Journal of Institutional Economics (2020), **16**, 433–444
doi:10.1017/S1744137420000107

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Is Bitcoin a decentralized payment mechanism?

William J. Luther[1]* and Sean Stein Smith[2]

[1]Department of Economics, Florida Atlantic University, Boca Raton, FL 33431, USA and [2]Department of Economics and Business, Lehman College, City University of New York, Bronx, NY 10468, USA
*Corresponding author. Email: wluther@fau.edu

(Received 3 January 2020; revised 13 February 2020; accepted 17 February 2020; first published online 20 March 2020)

Abstract
We make a distinction between centralized, decentralized, and distributed payment mechanisms. A centralized payment mechanism processes a transaction using a trusted third party. A decentralized payment mechanism processes a transaction between the parties to the transaction. A distributed payment mechanism relies on the network of users to process a transaction on a shared ledger. We maintain that bitcoin is neither a centralized nor a decentralized payment mechanism. It is, instead, a distributed payment mechanism. We then consider decentralized and centralized aspects of the broader bitcoin payment space.

Keywords: Bitcoin; centralized; consensus; decentralized; distributed; e-wallet; exchange; governance; payments

JEL classification: E40; E41; E42

Bitcoin is often described as a decentralized cryptocurrency that enables private transactions between users. When the pseudonymous Satoshi Nakamoto announced the first release of bitcoin, in January 2009, he referred to it as 'a new electronic cash system that uses a peer-to-peer network to prevent double-spending' that is 'completely decentralized with no server or central authority'.[1] More recently, Erik Voorhees (2015), the CEO and founder of ShapeShift.io, a digital asset exchange, writes that bitcoin insiders 'understand that one of Bitcoin's most important features – and perhaps its true core innovation – is its decentralized structure'.[2] Others describe bitcoin and the many alt-coins it inspired as 'decentralized digital currencies' (Tschorsch and Scheuermann, 2016) or 'decentralized public-ledger currency platforms' (Evans, 2014) or refer to bitcoin's underlying blockchain technology as a 'decentralized ledger' (Reyes, 2016). Indeed, the subtitle of a recent popular book by Ammous (2018) bills bitcoin as *The Decentralized Alternative to Central Banking*.

There is some basis for this view. The bitcoin protocol does not process transactions like a centralized clearinghouse; is not governed nor regulated by any central entity like a bank or nation-state; and, in many cases, enables a greater degree of financial privacy than payment mechanisms relying on centralized clearing.[3] But that basis is insufficient. The bitcoin protocol does not employ decentralized clearing to process transactions and, in many cases, offers less financial privacy than payment mechanisms that do.

In what follows, we make a distinction between centralized, decentralized, and distributed payment mechanisms.[4] A centralized payment mechanism processes – or, clears – a transaction using a trusted

[1]Luther (2019) reviews the communication between early users on the Bitcoin Mailing List.

[2]Voorhees (2015) goes on to discuss centralized ancillary services, like Coinbase, while maintaining that they do not undermine the core claim that bitcoin is decentralized. We consider these issues in Section 2.

[3]Along these lines, Luther and Salter (2017) consider the extent to which people switch to bitcoin following a collapse in confidence in payment mechanisms relying on centralized clearing.

[4]Baran (1964) makes a similar distinction in the context of communication networks. See also Bashir (2018).

third party. A decentralized payment mechanism processes a transaction between the parties to the transaction. A distributed payment mechanisms relies on the network of users – not just the parties to the transaction – to process a transaction on a shared ledger. We maintain that bitcoin is neither a centralized nor decentralized payment mechanism. It is, instead, a distributed payment mechanism. We then consider decentralized and centralized aspects of the broader bitcoin payment space.

1. Three types of payment mechanisms

Payment mechanisms are useful, at least in part, because transactors lack the trust required to establish and sustain gift-exchange (Aliprantis *et al.*, 2007; Kiyotaki and Moore, 2002; Lagos and Wright, 2008).[5] But payment mechanisms do not eliminate the need to trust altogether. Rather, they shift some portion of the trust required to make a transaction from one entity or item to another.

In general, there are three types of payment mechanisms used to clear transactions: centralized, decentralized, and distributed. Since these payment mechanisms differ in the way they process transactions, they also differ in how they allocate the need to trust and the extent to which they promote financial privacy. We discuss each in turn.

1.1 Centralized payments

When two parties to an exchange employ a centralized payment mechanism, they rely on some third party to process the transaction. The third party acts as a central node, through which payments – and information about those payments – must pass. As such, the two parties to the exchange must place some trust in the third party. However, with many centralized payment mechanisms, some trust is still required between the two parties to the transaction – though perhaps less than would be required in the absence of the centralized payment mechanism.

A diagram of a centralized payment mechanism is shown in Figure 1. Each black node corresponds to an individual sending or receiving funds. The white node is a centralized clearing institution. The black connections represent the payment being sent from one individual node, through the centralized clearing institution, to another individual node.

Most digital payments today are processed using a centralized payment mechanism. When a customer swipes her debit card at a merchant terminal, for example, neither the customer nor the merchant clears the transaction. Rather, the two parties rely on a financial institution to debit the customer's account and credit the merchant's account. The financial institution acts as the centralized node, clearing the transaction taking place between the two parties.

In some cases, a single layer of centralized clearing is sufficient. When one Bank of America account holder transfers funds to another, for example, the bank can handle the transaction on its own – debiting one of its account holder's accounts and crediting the other's.

In many cases, however, there are multiple layers of centralized clearing. Consider, for example, when a Bank of America account holder transfers funds to a Chase account holder. Bank of America first debits its account holder's account and credits its own account. Then, it transfers funds to Chase – that is, some other trusted third party like the Clearinghouse Interbank Payment System (CHIPS) or Fedwire debits Bank of America's account and credits the account of Chase. Then, Chase debits its own account and credits the account of its account holder, finalizing the transaction. Hence, the payment and the corresponding information about the payment pass through three intermediaries, which are not parties to the original transaction.

A centralized payment mechanism transfers some of the trust required to make the transaction from the two parties to the transaction to the trusted third party (or, in the case of multi-layer centralized clearing, parties). The two parties must trust that the third party will debit and credit the corresponding accounts as instructed – and only as instructed. They must also trust the third party to

[5]Luther (2016*c*) surveys the literature on the essentiality of payments.

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

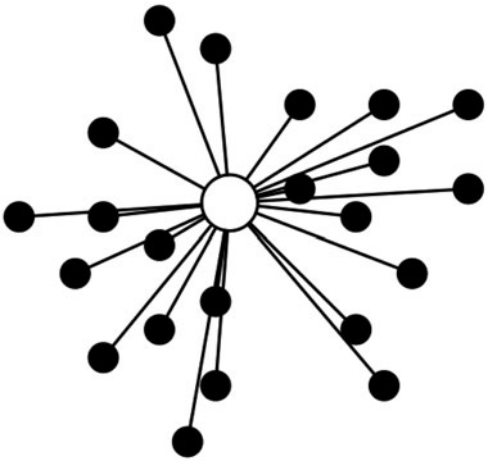

Figure 1. Centralized payment mechanism.

keep the corresponding information about the payment private. Such trust need not be absolute. The parties to the exchange might accept the risk that the funds will not be delivered to the recipient as instructed; that the sender's funds will be seized; or that information about the payment will be revealed to others. But, in general, the parties will be more inclined to rely on a centralized payment mechanism when it reduces their costs of transacting (e.g. by reducing the probability of theft or fraud, storage costs, etc.).

While the third party shoulders some of the trust required to make a transaction with a centralized payment mechanism, some trust usually remains with the parties to the original transaction. For example, the recipient of funds must trust that the sender will initiate the payment when goods and services are delivered in advance. Correspondingly, the sender of funds must trust that the recipient will deliver the goods or services as described when advance payment is agreed upon. And, in cases where the third party reserves the right to reverse the transaction, the recipient of funds must also trust that the sender will not file a claim with the financial institution to reverse the transaction after the goods or services have been delivered as described. Both must also trust that the other will not reveal information about the transaction, which they – along with the trusted third party – possess. In these ways, and others, the two parties must place some trust in one another while making a transaction, despite their reliance on a third party to clear the payment.

1.2 Decentralized payments

Those sending and receiving funds via a decentralized payment mechanism do not depend on some trusted third party to process payments, as they would with a centralized payment mechanism. Rather, with a decentralized payment mechanism, the parties to the transaction process the payment themselves. Since the payment does not pass through a centralized node, the information about the payment need not be shared with anyone other than the sender and receiver of funds. Hence, decentralized clearing tends to deliver a larger measure of financial privacy than centralized clearing, but also requires more trust between the exchanging parties.

A diagram of a decentralized payment mechanism is shown in Figure 2. As before, each black node corresponds to an individual sending or receiving funds. The black connections represent the payment being sent from one individual node to another individual node. Note the absence of any white nodes, or centralized clearing institutions, since the payments are cleared between the parties to the transaction. In other words, the payments are made in unique, pairwise transactions without requiring the parties to the transaction to interact with any other nodes on the system.

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

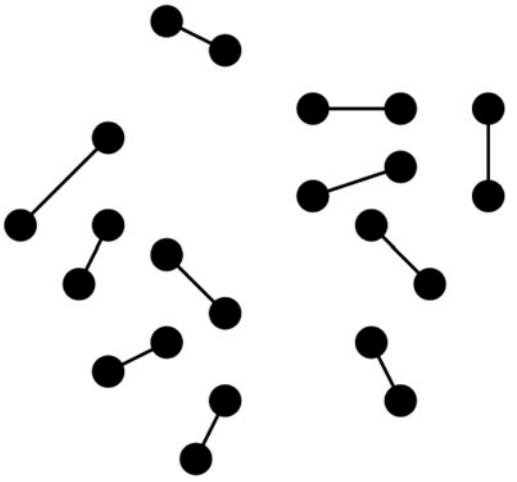

Figure 2. Decentralized payment mechanism.

Cash, or hand-to-hand currency, is perhaps the most familiar example of a decentralized payment mechanism. When a customer pays with cash, she debits her own account by taking the funds out of her wallet and handing them over to the merchant. Likewise, the merchant credits his own account by accepting the cash and placing it in the till. No third party is required to process the transaction.

Other, more technologically-advanced examples of decentralized payment mechanisms exist. But, at least to date, they have been much less popular than cash. Mondex, which was developed by the United Kingdom's National Westminster Bank in the early 1990s and later acquired by MasterCard International, offered a stored-value card that allowed users to transfer funds from one card to another without using a third-party to clear the transaction (White, 2007). Oyster card, which can be used to pay for public transit in and around London, similarly processes transactions between card and reader without the use of a trusted third party. But, unlike Mondex, the Oyster card reader later transmits all transactions data in batches to a central repository to serve as a record.[6]

Decentralized payments require a high degree of trust between the parties of the transaction. Again, such trust need not be absolute for the sender and recipient to agree to a particular payment mechanism. It need only be superior to the available alternatives.

What kind of trust is required with decentralized payment mechanisms? In cash transactions, the recipient must trust that the currency is legitimate (i.e. not counterfeit). If the sender holds more than the requisite balance for the transaction on hand, she must trust that the recipient does not take more cash than was agreed upon. Correspondingly, with Mondex cards, the sender (recipient) must trust that the card reader has not been manipulated in such a way as to transfer more (less) than stipulated. As with centralized payment mechanisms, both parties must trust the other will not reveal information about the transaction to others; but, for decentralized payments, they need not worry about some third party revealing that information, so long as the sender and recipient keep the transaction private. For this reason, we say that decentralized payment mechanisms tend to promote a greater degree of financial privacy than centralized payment mechanisms.

1.3 Distributed payments

Whereas centralized payments are cleared by some trusted third party and decentralized payments are cleared by the parties to the transaction, distributed payment mechanisms rely on the network of users to debit and credit the respective accounts. Distributed payment mechanisms employ a shared ledger

[6]Barclaycard was selected in 2006 to add e-money capabilities to the Oyster card, which might have resulted in use beyond the transit system. However, the project was shelved and the subsequent collaboration omitted e-money functionality.

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

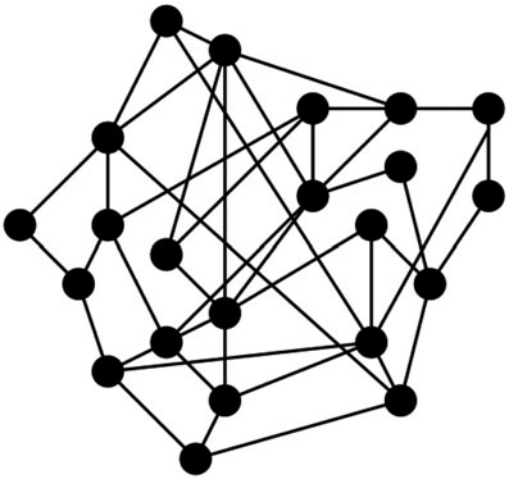

Figure 3. Distributed payment mechanism.

and a protocol for updating that ledger. In many cases, any individual user is capable of updating the ledger. However, the update – and, hence, the corresponding transactions – is only recognized as legitimate after confirmation from the network of users, as specified by the protocol.

A diagram of a distributed payment mechanism is shown in Figure 3. As before, each black node corresponds to an individual sending or receiving funds. The black connections represent the payment being sent from one individual node to another individual node. However, in the case of distributed clearing, the payment (and information about the payment) passes through all of the other nodes, as funds are debited and credited by the system on a shared ledger.

Bitcoin is arguably the most familiar example of a distributed payment mechanism.[7] When a bitcoin transaction is made, the sender effectively announces to the system that she (1) possesses a balance of bitcoin and (2) would like to send that balance to another user. She uses her private key to confirm (1) and the public key of the recipient to initiate (2). Her transaction is then bundled together with the other transactions being made around the same time and users running the bitcoin protocol race to process the block of transactions.

More specifically, computers running the protocol use a brute force approach to search for the input that corresponds to the given hashed output. The brute force approach, which is the best that anyone can do, reduces the odds that any individual user processes a batch of transactions to a random probability proportionate to his share of computing power on the system. Once a user finds the right input value, it can be easily confirmed by other users. The block of transactions is then added to the blockchain, or public ledger of all past transactions. Since the blockchain is, quite literally, a chain of all transaction blocks, future updates to the ledger serve to reconfirm the earlier transactions by building on the existing blockchain.[8]

In actuality, there are multiple versions of the shared bitcoin ledger, or blockchain, at any point in time. However, the bitcoin protocol specifies that the longest blockchain will be recognized as legitimate; so users tend to accept the longest blockchain and add subsequent blocks of transactions to that version of the ledger.[9] For this reason, many bitcoin users only recognize a transaction as being

[7]Bitcoin's underlying blockchain technology is often described as 'distributed ledger technology'. For symmetry, we use the term 'distributed payment mechanism'. Davidson *et al.* (2018), Allen *et al.* (2018), Berg *et al.* (2019), and Allen *et al.* (2020) consider the economics of the blockchain technology and its potential effects on institutions.

[8]Luther and Olson (2015) compare the shared ledger to the concept of memory in the monetary economics literature.

[9]An exception occurs when a fraudulent transaction is confirmed, in which case the honest nodes on the system band together to build on a legitimate version of the ledger. So long as the honest nodes hold a majority of the computing power on the system, they will ultimately be able to produce a longer blockchain than the dishonest nodes, thereby

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

legitimate once it is six blocks deep on the blockchain. More generally, the transaction is only recognized as legitimate because there is a consensus that the transaction is legitimate.

Distributed payment mechanisms allow one to send funds without trusting one's trading partner or some third party to clear the transaction. However, they require the parties trust the distributed payment mechanism – that is, the shared ledger and protocol for updating the ledger. With bitcoin, that requires trusting that no individual or group of individuals will acquire a majority of the computing power on the system and then abuse that power to their advantage.[10] It also requires trusting that the system will not be updated in such a way that one finds undesirable or otherwise reduces the purchasing power of one's bitcoin balance.

As with centralized and decentralized payment mechanisms, distributed payment mechanisms do not eliminate the need to trust one's trading partner entirely. Bitcoin payments are final, meaning they cannot be reversed without consent of the recipient. Hence, those sending funds in advance must trust the recipient to deliver goods and services as agreed upon. Likewise, the recipient of funds must trust the sender to relinquish those funds when goods and services are delivered in advance. And both must trust one another to keep the details of the transaction private. This is especially important when a shared ledger is employed, since identifying information for a party involved in one transaction might be used to identify that party in other transactions on the ledger that were initiated by or terminated in the same account. For this reason, distributed payment mechanisms like bitcoin tend to offer less financial privacy than decentralized payment mechanisms like cash, which lack a lasting record of transactions.[11]

2. Beyond bitcoin's payment mechanism

We maintain that bitcoin is neither a centralized nor a decentralized payment mechanism. Since it relies on the network of users to process transactions, it is best classified as a distributed payment mechanism. It is easy to understand why one might mischaracterize bitcoin as a decentralized payment mechanism, however. For starters, distributed payment mechanisms are relatively new. While most users are familiar with centralized and decentralized payment mechanisms, many do not realize there is a third way to process transactions. As a result, they classify each payment mechanism as either centralized or decentralized. And, since bitcoin has no central issuer or trusted third party clearing transactions, they erroneously conclude that it is a decentralized payment mechanism.

Moreover, the payment mechanism is just one aspect of the broader payment space. The nature of the broader payment space depends not merely on the way in which transactions are cleared (i.e. via a centralized, decentralized, or distributed payment mechanism). It also depends on how individual transactors interact with one another; the formal and informal rules governing those interactions; the governance structure in place for modifying the protocol; the extent to which individuals participate in that governance structure; and so on. Hence, one might reasonably conclude that the broader bitcoin payment space is relatively centralized or decentralized while recognizing that it processes transactions via a distributed payment mechanism.

Our focus on classifying bitcoin by the type of payment mechanism should not be taken to mean that there are no decentralized or centralized aspects of the broader bitcoin payment space. Again, we describe bitcoin as a distributed payment mechanism merely on the basis of how it clears

invalidating the fraudulent transaction. Indeed, the knowledge that fraudulent transactions will ultimately be reversed is sufficient to prevent most users from even attempting to make fraudulent payments.

[10]As Luther (2016*d*) notes, the mining pool GHash.io gained a majority of the computing power on the bitcoin network on 12 June 2014 and maintained it for 12 hours. However, it made no attempt to exploit that power. Indeed, it made a statement explaining that exploiting the temporary advantage would damage the long-term prospects of bitcoin and, hence, its own long-term interests in mining bitcoin.

[11]For an extended discussion of the relative financial privacy offered by bitcoin and cash, see Hendrickson and Luther (2017*b*).

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

transactions.[12] In an effort to remove any ambiguity on this point, we consider the extent to which one might describe the broader bitcoin payment space as centralized or decentralized. In brief, bitcoin's governance structure is relatively decentralized while ancillary services like exchanges and e-wallet providers act as centralized nodes in the broader bitcoin payment space.

2.1 Governance structure

While bitcoin is a distributed payment mechanism, its overarching governance structure is relatively decentralized.[13] At its core, bitcoin relies on consensus. The legitimate blockchain is made legitimate by consensus – those running the protocol accept it as the true version of the ledger. Likewise, the very nature of bitcoin – what it is, how it processes transactions, how its supply is determined, etc. – is fundamentally determined by consensus. Hence, any changes to the bitcoin protocol must be reached by consensus.

When a change to the bitcoin protocol is proposed, every user running the protocol effectively votes on whether to adopt the proposed change. Specifically, those accepting the proposed change will use the proposed protocol to process transactions. If those with a majority of the computing power running the protocol accept the change, blocks of transactions will be added to the blockchain using the proposed protocol and recognized as legitimate by consensus. If such a majority is not reached, those running the proposed protocol must choose to either abandon the proposed change, which the majority fails to recognize as legitimate, or fork the blockchain. In the latter case, those proposing the change essentially create a new cryptocurrency that has the same history as the bitcoin blockchain up until the point of the fork. To reiterate, a new cryptocurrency created by forking the bitcoin blockchain is not bitcoin, as the nature of bitcoin is determined by consensus and, in the case of a fork, the consensus has rejected the proposed change to the bitcoin protocol.

In practice, those proposing a change to the bitcoin protocol occasionally require more than a simple majority to see the change implemented. This is accomplished by writing the proposed protocol such that it is identical to the existing protocol up until the point when x percent of the blocks added to the blockchain over a given period of time are done so by users running the proposed protocol, where x is some number greater than 50 established by those proposing the change in advance.[14] The reason for imposing a supermajority on one's proposed change is straightforward. Since the value of bitcoin depends crucially on its network size, a narrow victory for one's proposed change might significantly reduce the value of one's bitcoin holdings if the losers opt to fork the blockchain by continuing to use the old protocol.

Some maintain that the bitcoin core development team and mining pools result in a more centralized bitcoin governance structure than many appreciate (Gervais *et al.*, 2014). The development team currently consists of 602 contributors. Wladimir J. van der Laan has served as lead developer since 8 April 2014, when he took over for Gavin Andresen. Van der Laan currently has 6,399 commits, or revisions made to the bitcoin core protocol.[15] Andreesen has 1,101. Only 49 contributors have 20 or more commits; 27 have 100 or more; nine have 500 or more; and four have 1,000 or more. Hence, most changes to the bitcoin protocol are made by a relatively small number of users.

[12]Bohme *et al.* (2015) offer a broader consideration of bitcoin. Luther (2016*b*), Hendrickson *et al.* (2016), Hendrickson and Luther (2017*a*), and Luther (2020) discuss obstacles to its adoption. White (2015), Yermack (2015), Smit *et al.* (2016), Frasser and Guzman (2020), and Hazlett and Luther (2020) assess whether, or to what extent, it is money. Selgin (2015) classifies it as a synthetic commodity money. Graf (2013) and Luther (2018) consider its intrinsic worth. Luther and White (2014), Luther (2016*a*), and Hendrickson and Luther (2020) discuss its future prospects.

[13]Berg *et al.* (2018*a*) consider the governance of blockchain protocols more generally.

[14]For example, an August 2015 proposal to raise the block size limit from one to eight megabytes and then double the limit every 2 years thereafter was scheduled to go into effect only after at least 75% of all blocks added to the blockchain were processed with the new protocol and, even then, no earlier than January 2016. The proposal ultimately failed to gain consensus.

[15]The term 'commit' is used on GitHub to denote an individual change to a file or set of files. It is similar to saving a file, except that a unique identifier is created to keep track of what changes were made, when they were made, and who made them.

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

Those not working on the bitcoin core development team might nonetheless influence its development by submitting a Bitcoin Improvement Proposal (BIP). BIPs, which specify proposed changes to be made, are assessed by the developers and, when supported by a developer, implemented for the network to consider.

Developers might choose to implement a proposal with little support. However, it is ultimately up to the network of users to adopt the revised protocol or continue on using the previous version. Likewise, developers might refuse to implement a proposal with broad support. In this case, someone not on the development team might offer a revised version of the protocol which users on the network could then adopt. Since the cost of coordination is non-trivial, some might be reluctant to reject changes proposed through the official channel or propose updates through non-official channels.[16] Hence, proposals with somewhat limited support might gain adoption and those with widespread support might fail to gain adoption.

Mining pools result when those running the bitcoin protocol band together to share the gains of processing transactions. Recall that processing a batch of transactions is essentially a random lottery, where the odds of winning correspond to one's share of computing power on the system. That makes the reward for processing a block of transactions uncertain.[17] Some miners will get lucky, expending relatively little energy before successfully processing a block. Others will run the protocol for a long time, and incur huge costs for electricity, wear and tear on mining rigs, etc., before seeing any return. By agreeing to split any rewards in accordance with each participants computing power, miners pooling their efforts can enjoy the same expected value at a much lower variance. It is no wonder, then, that mining pools have become so popular.

Since the members of a mining pool typically run the same version of the protocol, updates to the protocol can hinge on the support or disapproval of one or more pools. As such, some believe mining pools act as a centralizing force, concentrating power in the hands of a few users running pools. It should be recognized, however, that mining pools are loose coalitions: miners can join or exit pools as they see fit. A user supporting a BIP that is rejected by her pool or opposing a BIP supported by her pool can divert her computing power to another mining pool that is more closely aligned with her views on the proper bitcoin protocol. Hence, any centralizing effect of mining pools is necessarily limited by the views of the individual users running the protocol.

As Craig and Kachovec (2019) note, the relatively decentralized nature of bitcoin's governance structure cuts both ways. On the one hand, it is capable of overcoming issues of time inconsistency. Users can reasonably expect the fundamental features of bitcoin to remain unchanged. And, since the software is open-source, they need not worry that the program 'be bought by a competing company and then not developed further because the program competes with another of the company's products, or […] shut down because the firm has decided that the software does not fit its new business model'.

On the other hand, it is relatively difficult to make some changes that would significantly improve the protocol. When such changes do occur, they will tend to be slower than might have been achieved with a more centralized governance structure. And, when such changes do not occur, they might divide the network by forking the blockchain. Craig and Kachovec (2019) cite the block size (or, transactions volume) debate, which ultimately forked the original protocol (now known as bitcoin core) to create bitcoin cash. The new cryptocurrency, bitcoin cash, resulted when a proposed change to increase the block size limit to eight megabytes in August 2017 failed to gain consensus among bitcoin users, but those supporting the change continued using the revised protocol.[18]

[16]Gervais *et al.* (2014) note that alert messages 'can only be sent by people that possess the appropriate cryptographic key', which is currently 'shared among the Bitcoin developers. This gives these entities privileged powers to reach out to users and urge them to adopt a given Bitcoin release'.

[17]The current reward for processing a block of transactions stands at 12.5 bitcoin. It will halve to 6.25 bitcoin in May 2020.

[18]In November 2018, the bitcoin cash blockchain suffered its own fork, creating bitcoin SV (short for Satoshi's Version) in the process. Some of the initial bitcoin cash supporters, including nChain's Chief Scientist Craig Wright and billionaire

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

Another effort to deal with the block size limit, and the corresponding congestion it causes on the bitcoin network, was the introduction of the lightning network. The lightning network is a second layer, or off-chain, payment protocol put forward on a white paper by Poon and Dryja (2016). It enables transactions between bitcoin users without immediately broadcasting those transactions to the bitcoin network and, hence, without immediately recording them on the bitcoin blockchain. The off-chain transactions executed on the lightning network are ultimately announced to and settled on the bitcoin blockchain in much the same way that historical circulating notes issued by private banks were ultimately settled in specie.[19] And, like historical banknotes, the lightning network permits a larger number of transactions to be made with a given quantity of base money. In general, the ability for users to propose and adopt second-layer solutions like the lightning network to first-layer deficiencies without achieving consensus makes the governance structure of the broader bitcoin payment space more decentralized than it otherwise would be.[20]

2.2 Ancillary services

As described in Section 1.3, the bitcoin protocol processes transactions without relying on trusted third parties. However, many users have nonetheless chosen to rely on third parties when buying, holding, and selling bitcoin. Exchanges and e-wallet providers, in particular, act as centralizing forces in the broader bitcoin payment space.

In principle, there are three ways to acquire bitcoin. One can run the bitcoin protocol and acquire a balance of bitcoin as a reward when she (or, if contributing to a mining pool, someone in her pool) processes a block of transactions. One can sell goods for bitcoin. Or, one can trade her domestic currency (e.g. dollars) for bitcoin. In practice, most users acquire bitcoin in the third way, typically by purchasing it from an exchange.

Why do most people opt for an exchange? For starters, few possess the specialized hardware and have access to relatively cheap electricity required to run the bitcoin protocol efficiently. Those attempting to mine without the requisite hardware or cheap electricity should expect to earn a balance of bitcoin worth less than the cost to acquire it. They do not sell goods and services for bitcoin because, at present, it is somewhat cumbersome for many would-be bitcoin users to find someone interested in purchasing the goods or services they produce with bitcoin. Finally, since bitcoin exchanges specialize in trading national currencies (and, in many cases, other cryptocurrencies) for bitcoin, they can typically transact at a lower cost than users offering one-off or small-scale exchange opportunities.

Bitcoin exchanges engage in many activities to lower transaction costs. They post exchange rates for the currencies they buy and sell, which can be easily compared with other exchanges or users offering to buy or sell bitcoin. They conduct many exchanges per day, which reduces the spread between the buying and selling prices. They build reputations and make costly real investments, both of which might be lost in the event of fraud, thereby making it less risky for others to trust them. And they build websites and purchase advertisements that make the process of acquiring or offloading bitcoin more user friendly.

Although exchanges lower the cost of buying and selling bitcoin for the typical user, they also act as centralized nodes that undermine the financial privacy of the broader bitcoin payment space. A user acquiring bitcoin by mining, selling goods or services, or purchasing bitcoin from another user could conceivably do so without linking her physical-world identity to her digital-world bitcoin address.[21]

gambling entrepreneur Calvin Ayre, proposed increasing the blockchain to 132 megabytes but failed to gain consensus among bitcoin cash users.

[19]On redeemable banknotes, see White (1984), Selgin (1988), Selgin and White (1994, 1987), and Smith (1990).

[20]In describing the lightning network as a second-layer solution, we do not mean to downplay its shortcomings. For example, off-chain payments are more susceptible to fraud than on-chain payments. Hence, transactions executed on the lightning network require more trust than those immediately broadcasted to the bitcoin network and recorded on the bitcoin blockchain. As a result, so-called watchtower nodes have emerged to monitor for such fraudulent spends.

[21]Berg *et al.* (2018*b*) consider the institutional economics of identity with specific reference to the blockchain technology.

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

But those acquiring bitcoin via an exchange often provide identifying information. In the United States, for example, the Financial Crimes Enforcement Network (2013) classifies bitcoin exchanges as a money services business, which means (among other things) that they must collect identifying information to comply with know-your-customer laws. And, even in jurisdictions where such laws are not applied to bitcoin exchanges, it is nonetheless commonplace to reveal one's identity when purchasing bitcoin from an exchange. Using a debit card, electronic funds transfer, or other payment mechanism tied to a traditional financial institution to purchase bitcoin from an exchange makes it easy to deanonymize a bitcoin user, since traditional financial institutions typically require identifying information when setting up an account.

Identifying information provided to a bitcoin exchange might be subpoenaed by the government, acquired by hackers in a data breach, or otherwise made available to others by the exchange. And, since the bitcoin blockchain is a public ledger, the acquisition of identifying information would allow one to trace all of the transactions associated with the identified account. Moreover, by tracing the identified user's transactions, one might be able to identify one or more of her trading partners as well. And, as with the initial identification, the transactions of subsequently identified users could be traced through the blockchain, potentially revealing the identities of still other users.

Unless it is sufficiently cheap to monitor whether one's potential trading partner has intentionally or unintentionally revealed her identity to an exchange, it is difficult to punish those users undermining the financial privacy of the system. As such, users are unlikely to take the risk of deanonymizing their future trading partners into consideration when choosing whether to buy or sell bitcoin via an exchange. Hence, by acting as centralized nodes whereby most users enter or exit the bitcoin payment space, exchanges undermine the financial privacy of the network.

Recall that bitcoin employs public key cryptography to keep transactions secure. In order to transfer a balance of bitcoin, the sender must sign the transaction request with her private key and indicate the recipient by his public key. While this cryptography prevents unauthorized transfers, it is only effective insofar as users keep their private keys private. Anyone with access to a user's private key can transfer funds from her account. It also requires that users prevent their private keys from becoming lost, since a user will not be able to demonstrate ownership and, hence, transfer funds from her account without access to her private key.[22]

Many users in the bitcoin payment space quite naturally worry about the loss or theft of their bitcoin. They are not specialists in securing private keys. Moreover, some users merely want the ability to send and receive bitcoin or the ability to realize a capital gain as demand for bitcoin increases over time. They are not interested in running the bitcoin protocol, which they view as unfamiliar and complicated. For these users, e-wallet service providers offer to secure one's private keys while also making it more convenient to send, receive, or store bitcoin.

To the extent that e-wallet providers are specialists in securing private keys, they reduce the risk of loss or theft. But such risks are not eliminated entirely. Users entrusting their private keys to an e-wallet provider must worry that it will fail to provide sufficient security. An e-wallet provider might hand over one's private keys when ordered to do so by the government. It might lose them to hackers in a data breach. Or, it might abscond with the private keys, defrauding its customers in the process. As such, e-wallet providers act as centralized nodes in the broader bitcoin payment space, introducing a trusted third-party where one need not exist.

While both exchanges and e-wallet providers act as centralizing forces, there is far less reason to be concerned with the latter. Those choosing to trust an e-wallet provider bear the costs and reap the rewards of doing so. There is no obvious externality. Any centralization occurring as a result of e-wallets is probably efficient. That is not the case with exchanges. As noted above, those using exchanges do not merely undermine their own financial privacy, but also the financial privacy of others. Hence,

[22]A private key can be lost if it is not properly secured, the hardware where one secures a private key fails, or it is not transferred in the event of one's death.

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

exchanges likely result in more centralization of the broader bitcoin payment space than is socially optimal.[23]

3. Conclusion

When bitcoin launched in 2009, it offered a fundamentally new way of processing transactions. Most digital payment mechanisms, like debit cards and electronic fund transfers, are centralized, employing a trusted third party to clear transactions. Other forms of payment, like cash, are decentralized, relying on the parties to the transaction to clear payments. Bitcoin, in contrast, employs a shared ledger and protocol for updating that ledger. As such, it is a distributed payment mechanism.

The distinction between centralized, decentralized, and distributed payment mechanisms is a meaningful distinction. Mistaking bitcoin for a decentralized payment mechanism makes one more likely to misattribute features to it and, as a result, misevaluate the extent to which it is likely to be an effective payment mechanism in a given context. Understanding what kind of payment mechanism bitcoin is helps one think about the kind of situations where bitcoin might be essential.

In particular, bitcoin is often supported on the grounds of promoting financial privacy. Mistaking bitcoin for a decentralized payment mechanism might lead one to believe – incorrectly, it turns out – that bitcoin offers a degree of financial privacy comparable to that of other decentralized payment mechanisms. In contrast, understanding that bitcoin is a distributed payment mechanism causes one to question that notion. As with decentralized payment mechanisms, the lack of reliance on a trusted third party means that distributed payment mechanisms generally provide *more* financial privacy than centralized payment mechanisms. However, their shared public ledger means that they tend to offer *less* financial privacy than decentralized payment mechanisms.

While the way in which bitcoin clears transactions requires classifying it as a distributed payment mechanism, there are nonetheless decentralized and centralized aspects of the broader bitcoin payment space. Its governance structure, which requires consensus, is relatively decentralized, though the bitcoin core development team and mining pools perhaps make it less decentralized than it otherwise would be. On the other hand, ancillary services, like exchanges and e-wallets, act as centralized nodes, undermining some of the financial privacy provided by the core distributed payment mechanism. The net effect is a unique institutional environment, which rivals traditional payment systems in some contexts.

References

Aliprantis, C. D., G. Camera and D. Puzzello (2007), 'Anonymous Markets and Monetary Trading', *Journal of Monetary Economics*, **540**(7): 1905–1928.

Allen, D. W. E., C. Berg, A. M. Lane and J. Potts (2018), 'Cryptodemocracy and its Institutional Possibilities', *The Review of Austrian Economics*, 1–12.

Allen, D. W. E., C. Berg, B. Markey-Towler, M. Novak and J. Potts (2020), 'Blockchain and the Evolution of Institutional Technologies: Implications for Innovation Policy', *Research Policy*, **490**(1): 1–8.

Ammous, S. (2018) *The Bitcoin Standard: The Decentralized Alternative to Central Banking*, Hoboken, NJ: John Wiley & Sons.

Baran, P. (1964), 'On Distributed Communications Networks', *IEEE Transactions on Communications Systems*, **120**(1): 1–9.

Bashir, I. (2018), *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*, Birmingham: Packt Publishing Ltd.

Berg, A., C. Berg and M. Novak (2018*a*), 'Crypto Public Choice'.

Berg, C., S. Davidson and J. Potts (2019), 'Capitalism after Satoshi: Blockchains, Dehierarchicalisation, Innovation Policy, and the Regulatory State', *Journal of Entrepreneurship and Public Policy*.

Berg, A., C. Berg, S. Davidson and J. Potts (2018*b*), 'The Institutional Economics of Identity'.

Bohme, R., N. Christin, B. Edelman and T. Moore (2015), 'Bitcoin: Economics, Technology, and Governance', *Journal of Economic Perspectives*, **290**(2): 213–238.

[23]In practice, it is perhaps less important to distinguish between the social desirability of exchanges and e-wallet providers than we have suggested, since economies of scope lead many exchanges to provide e-wallet services as well.

https://doi.org/10.1017/S1744137420000107 Published online by Cambridge University Press

Craig, B. R. and J. Kachovec (2019), 'Bitcoin's Decentralized Decision Structure', *Economic Commentary*, (2019-12): 1–5.
Davidson, S., P. De Filippi and J. Potts (2018), 'Blockchains and the Economic Institutions of Capitalism', *Journal of Institutional Economics*, **140**(4): 639–658.
Evans, D. S. (2014), 'Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms', *University of Chicago Coase-Sandor Institute for Law & Economics Research Paper*, 0(685).
Financial Crimes Enforcement Network (2013), 'Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies', Technical Report, March 2013. FIN-2013-G001.
Frasser, C. and G. Guzman (2020), 'What do we Call Money? An Appraisal of the Money or non-Money View', *Journal of Institutional Economics*, **16**(1): 25–40.
Gervais, A., G. O. Karame, V. Capkun and S. Capkun (2014), 'Is Bitcoin a Decentralized Currency?', *IEEE security & privacy*, **12**(3): 54–60.
Graf, K. (2013), 'On the Origins of Bitcoin: Stages of Monetary Evolution'.
Hazlett, P. K. and W. J. Luther (2020), 'Is Bitcoin Money? And What That Means', *Quarterly Review of Economics and Finance*.
Hendrickson, J. R. and W. J. Luther (2017*a*), 'Banning Bitcoin', *Journal of Economic Behavior & Organization*, **141**: 188–195.
Hendrickson, J. R. and W. J. Luther (2017*b*), 'Cash, Crime, and Cryptocurrency'.
Hendrickson, J. R. and W. J. Luther (2020), 'The Value of Bitcoin in the Year 2141 (and Beyond!)'.
Hendrickson, J. R., T. L. Hogan and W. J. Luther (2016), 'The Political Economy of Bitcoin', *Economic Inquiry*, **540**(2): 925–939.
Kiyotaki, N. and J. Moore (2002), 'Evil is the Root of all Money', *American Economic Review*, **920**(2): 62–66.
Lagos, R. and R. Wright (2008), 'When is Money Essential? A Comment on Aliprantis, Camera and Puzzello'.
Luther, W. J. (2016*a*), 'Bitcoin and the Future of Digital Payments', *Independent Review*, **200**(3): 397–404.
Luther, W. J. (2016*b*), 'Cryptocurrencies, Network Effects, and Switching Costs', *Contemporary Economic Policy*, **340**(3): 553–571.
Luther, W. J. (2016*c*), 'Mises and the Moderns on the Inessentiality of Money in Equilibrium', *Review of Austrian Economics*, **290**(1): 1–13.
Luther, W. J. (2016*d*), 'Regulating Bitcoin: On What Grounds?', in H. Peirce and B. Klutsey (eds.), *Reframing Financial Regulation: Enhancing Stability and Protecting Consumers*, Arlington, VA: Mercatus Center at George Mason University, pp. 391–415.
Luther, W. J. (2018), 'Is Bitcoin Intrinsically Worthless?', *Journal of Private Enterprise*, **330**(1): 31–45.
Luther, W. J. (2019), 'Getting of the Ground: The Case of Bitcoin', *Journal of Institutional Economics*, **150**(2): 189–205.
Luther, W. J. (2020), 'Regulatory Ambiguity in the Market for Bitcoin', *Review of Austrian Economics*.
Luther, W. J. and J. Olson (2015), 'Bitcoin is Memory', *Journal of Prices & Markets*, **30**(3): 22–33.
Luther, W. J. and A. W. Salter (2017), 'Bitcoin and the Bailout', *The Quarterly Review of Economics and Finance*, **66**: 50–56.
Luther, W. J. and L. H. White (2014), 'Can Bitcoin Become a Major Currency?', *Cayman Financial Review*, **36**: 78–79.
Poon, J. and T. Dryja (2016), 'The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments'.
Reyes, C. L. (2016), 'Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal', *Villanova Law Review*, **61**(1): 191.
Selgin, G. A. (1988), *The Theory of Free Banking: Money Supply Under Competitive Note Issue*, Lanham, MD: Rowman & Littlefield.
Selgin, G. A. (2015), 'Synthetic Commodity Money', *Journal of Financial Stability*, **17**: 92–99.
Selgin, G. A. and L. H. White (1987), 'The Evolution of a Free Banking System', *Economic Inquiry*, **250**(3): 439–457.
Selgin, G. A. and L. H. White (1994), 'How would the Invisible Hand Handle Money?', *Journal of Economic Literature*, **320**(4): 1718–1749.
Smit, J. P., F. Buekens and S. Du Plessis (2016), 'Cigarettes, Dollars and Bitcoins – An Essay on the Ontology of Money', *Journal of Institutional Economics*, **120**(2): 327–347.
Smith, V. C. (1990), *The Rationale of Central Banking and the Free Banking Alternative*, Indianapolis: Liberty Fund.
Tschorsch, F. and B. Scheuermann (2016), 'Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies', *IEEE Communications Surveys & Tutorials*, **180**(3): 2084–2123.
Voorhees, E. (2015), 'Is Bitcoin Truly Decentralized? Yes – and Here is Why It's Important', *Bitcoin Magazine*.
White, L. H. (1984), *Free Banking in Britain: Theory, Experience, and Debate, 1800–1845*, Cambridge: Cambridge University Press.
White, L. H. (2007), 'Payments System Innovations in the United States since 1945 and their Implications for Monetary Policy', in *Institutional Change in the Payments System and Monetary Policy*, London: Routledge, pp. 43–58.
White, L. H. (2015), 'The Market for Cryptocurrencies', *Cato Journal*, **350**(2): 383–402.
Yermack, D. (2015), 'Is Bitcoin a Real Currency? An Economic Appraisal', in D. L. K. Chuen (ed), *Handbook of Digital Currency*, Cambridge, MA: Academic Press, pp. 31–43.

Cite this article: Luther WJ, Stein Smith S (2020). Is Bitcoin a decentralized payment mechanism? *Journal of Institutional Economics* **16**, 433–444. https://doi.org/10.1017/S1744137420000107