Bitcoin is an online communication protocol that facilitates the use of a virtual currency, including electronic payments. Since its inception in 2009 by an anonymous group of developers (Nakamoto 2008), Bitcoin has served approximately 62.5 million transactions between 109 million accounts. As of March 2015, the daily transaction volume was approximately 200,000 bitcoins—roughly $50 million at market exchange rates—and the total market value of all bitcoins in circulation was $3.5 billion (Blockchain.info 2015). Table 1 summarizes Bitcoin activity to date. (We will follow the convention in the computer science literature of using capital-B Bitcoin to refer to the system, and lower-b bitcoin to refer to the unit of account.)

Bitcoin’s rules were designed by engineers with no apparent influence from lawyers or regulators. Rather than store transactions on any single server or set of servers, Bitcoin is built on a transaction log that is distributed across a network of participating computers. It includes mechanisms to reward honest participation, to bootstrap acceptance by early adopters, and to guard against concentrations of power. Bitcoin’s design allows for irreversible transactions, a prescribed path of money creation over time, and a public transaction history. Anyone can create a

Rainer Böhme is Professor of Security and Privacy, University of Innsbruck, Innsbruck, Austria. Nicolas Christin is Assistant Research Professor, Department of Electrical and Computer Engineering and CyLab, Carnegie Mellon University, Pittsburgh, Pennsylvania. Benjamin Edelman is Associate Professor of Business Administration, Harvard Business School, Boston, Massachusetts. Tyler Moore is Assistant Professor of Computer Science and Engineering, Southern Methodist University, Dallas, Texas. Their email addresses are rainer.boehme@uibk.ac.at, nicolasc@cmu.edu, bedelman@hbs.edu, and tylerm@smu.edu.

To access the disclosure statements, visit http://dx.doi.org/10.1257/jep.29.2.213 doi=10.1257/jep.29.2.213
Bitcoin account, without charge and without any centralized vetting procedure—or even a requirement to provide a real name. Collectively, these rules yield a system that is understood to be more flexible, more private, and less amenable to regulatory oversight than other forms of payment—though as we discuss in subsequent sections, all these benefits face important limits.

Bitcoin is of interest to economists as a virtual currency with potential to disrupt existing payment systems and perhaps even monetary systems. Even at their current early stage, such virtual currencies provide a variety of insights about market design and the behavior of buyers and sellers. This article presents the platform’s design principles and properties for a nontechnical audience; reviews its past, present, and future uses; and points out risks and regulatory issues as Bitcoin interacts with the conventional financial system and the real economy.
**Bitcoin Design Principles**

Scarcity is a prerequisite for ascribing value to any form of money. At a micro level, scarcity protects against counterfeiting. More broadly, scarcity bounds the growth path of the monetary base and facilitates price stability. In modern economies, where money is held in electronic forms, scarcity is preserved by legal rules ensuring the correctness of bookkeeping records: that is, electronic money involves a financial system in which transactions trigger a credit for one account and a corresponding debit to another. Central banks hold the power to adjust the absolute quantity of money in circulation.

Against this backdrop, Bitcoin can be understood as the first widely adopted mechanism to provide absolute scarcity of a money supply. By design, Bitcoin lacks a centralized authority to distribute coins or to track who holds which coins. Consequently, the process of issuing currency and verifying transactions is considerably more difficult than in classic bookkeeping systems. Meanwhile, Bitcoin issues new currency to private parties at a controlled pace in order to provide an incentive for those parties to maintain its bookkeeping system, including verifying the validity of transactions.

**Enabling Technologies and Processes**

The “Bitcoin core” software can be freely downloaded at https://bitcoin.org/en/choose-your-wallet. The standard Bitcoin implementation includes a number of features. Typically, it creates a “wallet” file for the user that can store bitcoins (without giving a name or proof of identity); it creates an individual node for the user in the peer-to-peer Bitcoin network that can be used with a standard Internet connection; and it provides access to the “block chain” data structure that verifies all past Bitcoin activity.

**Transactions and the Block Chain**

Bitcoins are recorded as transactions. For instance, some user Charlie does not simply “hold” three bitcoins. Rather, Charlie participates in a publicly verifiable transaction showing that he received three bitcoins from Bob. Charlie was able to verify that Bob could make that payment because there was a prior transaction in which Bob received three bitcoins from Alice and there was no prior transaction in which Bob spent these three bitcoins. Figure 1 illustrates these interactions.

Indeed, each individual bitcoin can readily be traced back through all transactions in which it was used, and thus to the start of its circulation. All Bitcoin transactions are readable by everyone in records stored in a widely replicated data structure. In general, transactions are ordered recursively by having the input of a transaction (roughly, the source of funds) refer to the output of a previous transaction. (For example, the transaction might reveal that Bob pays Charlie using bitcoin he received from Alice.)
Bitcoin relies on two fundamental technologies from cryptography: public-private key cryptography to store and spend money; and cryptographic validation of transactions. Standard public-private key cryptography lets anyone create a public key and an associated private key (Diffie and Hellman 1976). Public keys are designed to be widely shared—hence the name. Messages encrypted with a public key can only be descrambled by someone who possesses the corresponding private key, allowing anyone to encrypt a message that only the specified recipient can read. Similarly, messages encrypted with a private key can only be descrambled with the corresponding public key, allowing a specified sender to create a message that can be confirmed to be authentic. Public-private key cryptography is widely used: in the best-known example, web browsers on a HTTPS “secure website” encrypt communications with that site’s advertised public key in order to begin a secure connection. In Bitcoin, similar encryption fundamentals authenticate instructions to transfer money to other participants. Such an instruction is encrypted using the sender’s private key, confirming for everyone that the instruction in fact came from the sender.

**Figure 1**

**Bitcoin’s Approach to Transaction Flow and Validation**

Miners append blocks of transactions by solving mathematical puzzles of increasing difficulty.

*Source: Authors.*
Suppose that Alice has three bitcoins that she wants to give to Bob. She publishes a message in the Bitcoin network indicating that she is transferring three of her existing bitcoins, along with a reference to the transaction where she had received those bitcoins. Part of this message is encrypted by Alice’s private key to prove that the instruction came from her, in a method akin to a signature on a paper check. Later, if Bob wants to send bitcoins to Charlie, he publishes a message, again encrypted with his private key, indicating that he got his bitcoins from Alice and what he wants to send to whom. The Bitcoin network identifies Alice, Bob, and Charlie only by their public keys, which serve as account numbers.

Every new transaction that is published to the Bitcoin network is periodically grouped together in a “block” of recent transactions. To make sure no unauthorized transactions have been inserted, the block itself is compared to the most recently published block—yielding a linked sequence of blocks, or “block chain.” A new block is added to the chain roughly every ten minutes. With this data structure in place, any Bitcoin user can verify that a prior transaction did in fact occur.

Keeping the transaction record operational and updated is a public good, as it is the foundation of the entire Bitcoin system. To encourage users to assist, the Bitcoin system periodically awards newly minted bitcoins to the user who solves a mathematical puzzle that is based on the pre-existing contents of the block (which prevents tampering with the block and hence modifying prior transactions) and which can only be solved by computationally intensive methods that include a random component. Thus, faster computing is more likely to solve a given problem and will solve a greater number of these problems, but speed alone will not guarantee success.

Upon solving the puzzle, the user publishes a “block” which contains a proof-of-work that a solution was carried out along with all observed transactions that have taken place since the last puzzle solution was announced and a reference to the previous complete block. After other users verify the solution, they start working on a new block containing new outstanding transactions. This process is called “mining” and recursively ensures that the total historical ordering on all blocks (“chain”) is agreed by the entire network.

A Bitcoin transaction does not clear (and hence is not final) until it has been added to the consensus block chain. Transaction batches are added every ten minutes on average. However, miners are continuously working on adding blocks of transactions, and building on previous transactions. By continually presenting their solutions to the puzzles, with the associated new tail of the block chain, miners are in effect “voting” on the correct record of Bitcoin transactions, and in that way verifying the transactions. In some cases, a transaction batch will be added to the block chain, but then a few minutes later it will be altered because a majority of miners reached a different solution. Sources typically recommend considering a Bitcoin transaction final only after six confirmations, to assure that the transaction is truly recorded in a permanent part of the block chain. While this provides greater assurance, it creates a delay of approximately one hour before a Bitcoin transaction is finally validated.
As miners update the block chain, their computational efforts carry significant costs. In particular, the computerized proof-of-work calculations are quite power-intensive, consuming more than 173 megawatts of electricity continuously. For perspective, that amount is approximately 20 percent of an average nuclear power plant (World Nuclear Association 2015), or approximately $178 million per year at average US residential electricity prices. These computational costs have grown sharply and may rise further because Bitcoin automatically adjusts puzzle difficulty so that the time interval between two blocks remains roughly ten minutes. As more computing power joins the Bitcoin system, the puzzles automatically become more difficult, increasing computing and electricity requirements. In fact, an arms race ensued as the price of bitcoin rose. Taylor (2013) compares the difficulty of solving the puzzle to the bitcoin-dollar exchange rate, finding that spikes in the exchange rate—bitcoins becoming more valuable in terms of US dollars—have been followed by increases in computational difficulty.

**Built-in Incentives**

Bitcoin includes several built-in incentives to encourage useful behavior. The miners who verify the block chain are rewarded with—what else?—bitcoins. At first, miners solving the puzzle received a reward of 50 bitcoins. This reward is periodically cut in half, and it stands at 25 as of March 2015. After 21 million bitcoins have been minted, the reward falls to zero and no further bitcoins will be created. Hence, the protocol design for Bitcoin sets a controlled pace for the expansion of the currency and an ultimate limit to the number of bitcoins issued.

Miners have a second potential source of revenue (which will become the only source of revenue once all bitcoins have been created). When listing a transaction, the buyer and seller can also offer to pay a “transaction fee,” which is a bonus payment to whatever miner solves the puzzle that verifies the transaction. These fees are optional, but 97 percent of the transactions in 2014 include a fee, most often set at the default rate of the standard client software, 0.0001 bitcoin. In relative terms, the transaction fees are below 0.1 percent of total transaction value (Möser and Böhme 2014). However, as the mathematical puzzles become harder, there will presumably be a point where the automatic reward for solving the puzzle drops below the cost of doing so. At that point, one possibility is that those who wanted a Bitcoin transaction could bid up the optional fees. Houy (2014a) models equilibria for the level of transaction when the minting reward drops below the cost of mining.

Early in Bitcoin’s operation, updating the block chain yielded bitcoins more often and hence more readily per unit of computing power provided. This design benefited those who ran the Bitcoin platform at the outset—helping to create the critical mass needed to bootstrap the platform (Böhme 2013). Today, some users still find mining profitable, but effective mining now requires specialized hardware (particularly well-suited to solving the mathematical puzzles at issue) as well as access to low-cost electricity.

Requiring miners to solve a puzzle helps avoid certain types of fraud. In principle, a system like Bitcoin could validate transactions using a simple consensus by
majority vote, with a majority of connected users able to affirm that a given trans-
action in fact occurred. But then an attacker could game the system by creating
numerous fake identities. In response, the Bitcoin protocol makes it costly to submit
fake votes. Consistent with the Internet’s open architecture, anyone can connect
multiple computers to the Bitcoin system. But voting on the authenticity of a trans-
action requires first working to solve a mathematical puzzle that is computationally
hard to solve (although easy to verify). Solving the puzzle provides “proof of work”;
in lieu of “one person, one vote,” Bitcoin thus implements the principle of “one
computational cycle, one vote.” Through this design, the proof-of-work mechanism
simultaneously discourages creating numerous fake identities and also provides
incentives to participate in verifying the block chain.

What Bitcoin Doesn’t Have

Compared with conventional payment systems, Bitcoin lacks a governance
structure other than its underlying software. This has several implications for
the functioning of the system. First, Bitcoin imposes no obligation for a financial
institution, payment processor, or other intermediary to verify a user’s identity
or cross-check with watch-lists or embargoed countries. Second, Bitcoin imposes
no prohibition on sales of particular items; in contrast, for example, credit card
networks typically disallow all manner of transactions unlawful in the place of sale
(MacCarthy 2010). Finally, Bitcoin payments are irreversible in that the protocol
provides no way for a payer to reverse an accidental or unwanted purchase, whereas
other payment platforms, such as credit cards, do include such procedures. As
discussed in subsequent sections, these design decisions are intentional—simpli-
fying the Bitcoin platform and reducing the need for central arbiters, albeit raising
concerns for some users.

Centralization and Decentralization in the Bitcoin Ecosystem

The key innovation in Bitcoin, compared to other forms of cryptographic cash
(Chaum 1983) or virtual currencies (European Central Bank 2012), is its decentral-
ized core technologies. Early adopters praised decentralization and by all indications
chose Bitcoin because they wanted to use a decentralized system (Raskin 2013).
Decentralization offers certain advantages. It avoids concentrations of power that
could let a single person or organization take control. It often promotes availability
and resiliency of a computer system, avoiding a central point of failure. It offers
at least the appearance of greater privacy for users (and perhaps greater genuine
privacy) because in theory an eavesdropping adversary cannot observe transactions
across the system by targeting any single point or any single server. (However, as we
discuss below, significant privacy concerns remain.)

Nonetheless, the decentralization touted by Bitcoin has not fully come to frui-
tion. While the Bitcoin protocol supports complete decentralization (including the
possibility of all participants acting as miners), significant economic forces push
towards de facto centralization and concentration among a small number of intermediaries at various levels of the Bitcoin ecosystem. We review four key categories of intermediaries that have shaped Bitcoin’s evolution: currency exchanges, digital wallet services, mixers, and mining pools. A fifth type of intermediary, payment processors, is discussed further below.

Currency Exchanges

Currency exchanges allow users to trade bitcoins for traditional currencies or other virtual currencies. Most operate double auctions with bids and asks much like traditional financial markets, and charge a commission ranging from 0.2 to 2 percent. Some exchanges offer more advanced trading tools, such as limit or stop orders. To date, derivatives markets and short-selling remain rare.

At present, many trades in bitcoin are accompanied by one or even two conversions from and/or to conventional currencies. Furthermore, price quotes in bitcoin are almost always computed in real time by reference to a fixed amount of conventional currency. Thus, Bitcoin today resembles more a payment platform than what economists consider a currency.

While few technical barriers impede setting up intermediaries in the Bitcoin ecosystem, there are significant regulatory requirements. In the United States, currency exchanges generally operate as “money transmitters” and thus must register with the Financial Crimes Enforcement Network (FinCEN) as money services businesses. Registration includes a state-by-state licensing requiring both legal fees and posting bonds. Certification in a single state often costs at least $10,000, so nationwide participation can easily reach six figures on fees alone. Other countries have broadly similar rules. In Germany, currency exchanges that manage deposits on behalf of clients are viewed as “deposit banks” with a minimum capital requirement of €5 million.

In addition, currency exchanges need online infrastructure capable of withstanding attacks including hacking and denial-of-service attacks. For these reasons, the number of Bitcoin exchanges has remained modest, and the number of Bitcoin exchanges with significant volume has been even smaller. In spring 2012, the Japan-based Mt. Gox exchange served over 80 percent of all Bitcoin transactions. However, Mt. Gox collapsed in early 2014 and reported in its bankruptcy filing “losing” 754,000 of its customers’ bitcoins worth approximately $450 million at the time of closure (Abrams, Matthew, and Tabuchi 2014). In March 2015, the seven largest exchanges were BTC China, OKCoin, Huobi, Bitfinex, LakeBTC, Bitstamp, and BTC-e, which jointly served more than 95 percent of all bitcoin trade from October 2014 to March 2015 (Bitcoinity.org 2015).

Digital Wallet Services

Bitcoin wallets are data files that include Bitcoin accounts, recorded transactions, and private keys necessary to spend or transfer the stored value. Some users install specialized wallet software (such as Armory, Electrum, or Hive) on their personal devices to maintain control over their bitcoins. However, many users find
this task unappealing. Bitcoin wallet software can be difficult to install, and can impose onerous technical requirements—such as storing a copy of the entire block chain, which was 30 gigabytes as of March 2015. (Not all participants need to download the entire chain, but the system does rely on some users electing to do so.) Other users worry about security: a crash or attack on the computer holding the digital wallet could cause the loss of a user’s bitcoins.

As a result, many users rely on a digital wallet service that keeps the required files on a shared server with access via the web or via phone-based apps. A key distinction among digital wallet services is whether the service knows the account’s private key. Some services (including Blockchain.info, StrongCoin, and CoinPunk) let the user maintain control over private keys, meaning that the service is incapable of spending the user’s bitcoin (nor could hackers do so even if they fully infiltrated the wallet service). For such firms, the user must keep and present the private key when needed, and a user who loses the key or allows it to be compromised is at high risk. In contrast, other services (such as Coinbase and Xapo) require users to let the service store their private keys, which increases risk if the digital wallet service is compromised. In practice, digital wallet services tend to increase centralization—either expanding the role and importance of exchanges, or adding an additional service that is likely to be centralized due to high fixed costs, low marginal costs, and limited diversity in users’ needs.

Mixers

As initially envisioned, the Bitcoin transaction log shows each transaction made from each payer to each payee, along with the public keys serving as pseudonyms of each. As a result, anyone who knows the identity of any user from any transaction—perhaps the mailing address used for delivery of purchased goods, or the bank account used to purchase bitcoins—can track that user’s other transactions made with the same pseudonym, both before and since.

To preserve privacy against this tactic, mixers let users pool sets of transactions in unpredictable combinations, thus preventing tracking across transactions. Suppose Alice wants to pay Bob one bitcoin, and Charles wants to pay Daisy one bitcoin. To mislead an observer who tracks these payments, Alice and Charles could both pay a mixer “Minnie” and provide additional confidential instructions for Minnie to pay Bob and Daisy one bitcoin each. An observer would see flows from Alice and Charles to Minnie, and from Minnie to Bob and Daisy, but would not be able to tell whether it was Alice or Charlie who sent money to Bob. In practice, mixers must ensure that timing does not yield clues about money flows, which is particularly difficult since it is rare for different users to seek to transmit the exact same amount. Mixers have been used to promote anonymity in online communications, most famously by the Tor network, so their limitations are now widely known (Danezis and Diaz 2008). In addition to standalone services, some mixers are incorporated as a feature provided by digital wallets.

While mixers seem to improve privacy, they create additional challenges. For one, the finality of Bitcoin payments leaves payers with little recourse if a mixer
absconds with their funds. Furthermore, mixing protocols are usually not public, so their effectiveness cannot be proven. Indeed, correlations in timing might still reveal transaction counterparts, particularly at little-used mixers (Möser, Böhme, and Breuker 2013). Finally, mixers charge 1 to 3 percent of the amount sent, increasing costs for those who choose to use them.

**Mining Pools**

As discussed above, bitcoins are created when a miner successfully solves a mathematical puzzle. The puzzles have become significantly more difficult over time, and lumpy rewards mean a lone miner is now at risk of contributing resources in an attempt to solve a puzzle but then receiving no reward. In response, mining pools now combine resources from numerous miners. Miners work independently, but upon winning a miner shares earnings with others in the pool (much like consumers sharing resources to buy lottery tickets). As of March 2015, the two largest pools are AntPool and F2Pool, which together account for around one-third of Bitcoin mining activities.

Oversized mining pools threaten the decentralization that underpins Bitcoin’s trustworthiness. In several instances including a twelve-hour interval in June 2014, GHash briefly held more than 50 percent of total mining power, which could have allowed GHash pool operators to attempt manipulations. An attacker who holds a majority of Bitcoin’s computational resources can alter some of the system’s records, including inserting false transactions and rejecting actual transactions (albeit with a strong chance that others will notice), or deviate from the protocol rules.

**Uses of Bitcoin**

**Early: Silk Road and Other Illicit Activities**

After early proof-of-concept transactions, the first notable adopters of Bitcoin were businesses that sought features not easily available through alternatives: greater anonymity and the absence of rules concerning what could be bought or sold.

One prominent example involved the online sale of narcotics including marijuana, prescription drugs, and benzodiazepines (a class of psychoactive drugs). Drugs had been sold online for years, typically on informal bulletin boards and on websites such as “The Farmer’s Market,” a website that listed various narcotics available for purchase with payment using other services including PayPal (Kim 2014). When Bitcoin is used with tools to anonymize network traffic such as Tor (Dingledine, Mathewson, and Syverson 2004), marketplaces could provide stronger assurances of anonymity. Transaction volume grew sharply: Christin (2013) estimates that the turnover on the Silk Road anonymous online marketplace, the first to support Bitcoin transactions exclusively, reached $15 million per year just one year after it began operation. Silk Road’s own category classifications confirm the prevalence of narcotics items, which dominated Silk Road’s top categories as shown in Table 2. Examining 30 months of Silk Road data from February 2011 to July 2013,
the government evidence in the case against Ross Ulbricht lists 9.9 million bitcoins of transactions, which, accounting for the varying exchange rates, corresponds to $214 million (US v. Ulbricht, 2014, Government Exhibit 940). After the demise of Silk Road at the hands of law enforcement (discussed further below), alternative markets opened in its stead—a “new” Silk Road, as well as more than 30 competitors—and it is unclear whether the Silk Road takedown actually reduced contraband activity using Bitcoin.

While litigation documents largely focus on Silk Road as a marketplace for drugs and other contraband, the site’s general-purpose platform stood ready to sell anything. Reputation systems ensured trustworthiness of the transaction parties; escrow services mitigated counterparty risk; and, in some cases, hedges protected customers against currency volatility. Criminal charges criticized Silk Road’s fees: for escrow service, these averaged 8 percent in comparison to credit card system fees of approximately 3 percent—allegedly an indicator of Silk Road’s distinctive profit from misbehavior. But eBay’s fees typically somewhat exceed Silk Road’s fees, calling into question whether high fees in and of themselves indicate a platform’s purpose or responsibility.

Silk Road sellers appear to have exploited some arbitrage opportunities. For instance, marijuana is generally cheaper in the Netherlands than in Australia, providing Netherlands-based Silk Road sellers an opportunity to compete advantageously with street sellers in Australia. Numerous online discussions flagged this opportunity and the sellers who invoked it, and analysis of Silk Road’s transactions confirms disproportionate items sold from the Netherlands.

Gambling sites also turned to Bitcoin, both to protect customer privacy and to receive funds from customers unable to use other payment methods. The most popular single Bitcoin gambling game is Satoshi Dice, a simple betting game in which a player wins if a dice roll is less than the player’s chosen number. This service reported 2012 earnings of approximately 33,000 bitcoins (or roughly $403,000 at

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of items</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weed</td>
<td>3,338</td>
<td>13.7%</td>
</tr>
<tr>
<td>Drugs</td>
<td>2,193</td>
<td>9.0%</td>
</tr>
<tr>
<td>Prescription</td>
<td>1,784</td>
<td>7.3%</td>
</tr>
<tr>
<td>Benzodiazepines</td>
<td>1,193</td>
<td>4.9%</td>
</tr>
<tr>
<td>Books</td>
<td>955</td>
<td>3.9%</td>
</tr>
<tr>
<td>Cannabis</td>
<td>877</td>
<td>3.6%</td>
</tr>
<tr>
<td>Hash</td>
<td>820</td>
<td>3.4%</td>
</tr>
<tr>
<td>Cocaine</td>
<td>630</td>
<td>2.6%</td>
</tr>
<tr>
<td>Pills</td>
<td>473</td>
<td>1.9%</td>
</tr>
</tbody>
</table>

*Source: Christin (2013).*  
*Note: Categories are self-reported by sellers.*
then-applicable rates) with an average monthly growth of 78 percent at the time (Matonis 2013). For several months, the service’s (low value) payments accounted for up to 80 percent of total Bitcoin transactions (Möser and Böhme 2014). The Bitcoin Wiki (2015a) now reports around 100 casinos, poker sites, dice games, lotteries, and betting services.

Bitcoin can also be used to evade international capital controls. In December 2013, the People’s Bank of China, the central bank of China, banned Chinese banks from relationships with Bitcoin exchanges, a decision which the Economist magazine attributed to a desire to prevent yuan from being moved overseas via Bitcoin (D.K. 2013). Similarly, interest in Bitcoin appears to be particularly high in Argentina, where government policy strictly limits transfers to other currencies (McLeod 2013).

**Current: Consumer Payments, Buy-and-Hold**

In light of widespread criticism of the fees charged by credit and debit card networks (Anderson 2012), Bitcoin could offer an alternative that might pressure card networks to lower their prices to merchants. Some early evidence seems to confirm that Bitcoin may have this effect. Overstock.com, an online retailer, began to receive payments by Bitcoin in January 2014. Overstock reported a favorable response, including significant revenue gains, large average order sizes, and desirable customer demographics (Sidel 2014). Other merchants subsequently added Bitcoin support, including Expedia (travel), Newegg (electronics), Foodler (restaurant delivery and takeout), Gyft (gift cards for dozens of merchants), and TigerDirect (electronics). Payment processors help online merchants adjust their websites to accept Bitcoin. Early user reviews are mixed: users seem largely satisfied, though technical glitches sometimes occur. Merchants appear particularly pleased because Bitcoin payment processing is strikingly low-cost for them. For example, Coinbase (a payment processing firm) currently charges zero percent on incoming payments up to $1 million per merchant per annum, and 1 percent thereafter, which is considerably lower than the fees that merchants bear when a credit card is used to pay for a purchase.

It is less clear that consumers benefit from paying by Bitcoin. Many credit cards provide consumers with rebates of 1 percent, 2 percent or even more, as well as benefits of similar value such as frequent flyer points and merchandise credits. A consumer who pays by Bitcoin loses such rebates or bonuses. Edelman (2014) points out that even if a consumer already has bitcoins, the consumer would be better off making a purchase with a 1.5 percent cashback credit card, paying a 1 percent fee to convert bitcoins to dollars, then using those dollars to pay the credit card bill. Some merchants have responded by providing additional benefits to consumers who pay by Bitcoin: for example, Overstock provides a 1 percent rebate. However, if competing Bitcoin exchanges bid the 1 percent fee for converting from currency to bitcoin downwards, there could be room to make both consumers and merchants better off than through payments by credit card.

The block chain poses a further barrier to using Bitcoin for general-purpose payments. Every Bitcoin transaction, large or small, must be copied into all future
versions of the block chain. If Bitcoin expanded to include a huge volume of trans-
actions—as from millions of users’ small day-to-day payments—the storage burden
would need to be addressed. Furthermore, updating the block chain entails an
undesirable delay, making Bitcoin too slow for many in-person retail payments.

Meanwhile, other users appear to be buying bitcoins not to use them but to
hold them in appreciation. Meiklejohn, Pomarole, Jordan, Levchenko, McCoy,
Voelker, and Savage (2013) finds that of the bitcoins mined in 2009–2010, more
than 60 percent remain unspent or took more than one year to be spent.

Overall, some question whether the growth of Bitcoin payments is actually as
rapid as one might expect for a successful payments service. Evans (2014) compares
Bitcoin’s growth to that of mPesa, a widely used person-to-person payment system
using mobile phones in Kenya. Aligning the services based on months since launch,
Evans finds Bitcoin’s adoption less than one-twentieth as rapid.

Possible and Future: General-Purpose Payments, Mainstream Store of Value, and
Enabling Technology

Some proponents envision Bitcoin evolving into an all-purpose payment mech-
anism. If a payer already held bitcoins and if a payee was content to retain bitcoins
rather than convert to a traditional currency, fees would be relatively low: the only
costs are transaction fees paid to the successful miner who solved that block’s puzzle
(and perhaps also a small minting reward). However, to date most payments entail
at least one party needing to convert to or from bitcoin, which adds to transac-
tion costs. Overstock.com, the first prominent retailer to accept bitcoins, reports
keeping 10 percent of its bitcoin gross receipts in that form (Sidel 2014), but given
Overstock’s net margin of 0.6 percent (per its 2014 SEC 10-K), this effectively
requires transferring profits from the company’s other operations.

It might seem natural for consumers to use Bitcoin for international remit-
tances, which may sometimes cost $50 or more, rather than as a substitute for
credit card payments where consumers often receive a rebate. But so far, there is
little sign of Bitcoin use in this area. The fees from services such as Western Union
may appear high at first glance. But Western Union also offers a suite of services
including accepting and dispensing cash, which is distinctively useful in low-income
countries where transfer from bitcoin to local currency is likely to be difficult and
where merchants are unlikely to accept payment by Bitcoin.

Some computer scientists and entrepreneurs report excitement at Bitcoin not
for its role in facilitating payments, but for its ability to create a decentralized record
of almost anything. Marc Andreessen (2014), best known as coauthor of Mosaic
(the first widely-used web browser), presented the rationale:

Bitcoin gives us, for the first time, a way for one Internet user to transfer a
unique piece of digital property to another Internet user, such that the trans-
fer is guaranteed to be safe and secure, everyone knows that the transfer has
taken place, and nobody can challenge the legitimacy of the transfer. . . . All
these are exchanged through a distributed network of trust that does not
require or rely upon a central intermediary like a bank or broker. What kinds of digital property might be transferred in this way? Think about digital signatures, digital contracts, digital keys (to physical locks, or to online lockers), digital ownership of physical assets such as cars and houses, digital stocks and bonds . . . and digital money.

To date, there has been only limited use of the Bitcoin platform to provide services other than payment. Entrants building on the Bitcoin platform include Namecoin, an alternative domain name system; Colored Coins, a means to manage virtual property rights (Rosenfeld 2012); CommitCoin, a secure commitment scheme (Clark and Essex 2012), a timed version of which can be repurposed to ensure fairness in multi-party computation (Andrychowicz, Dziembowski, Malinowski, and Mazurek 2014) in order to run auctions without an auctioneer; and FutureCoin (Clark, Bonneau, Felton, Kroll, Miller, and Narayanan 2014), which enables decentralized prediction markets. However, none of these startups has attracted large-scale use to date, and each faces significant competition from firms and processes using more traditional system design.

**Risks in Bitcoin**

Bitcoin’s design presents distinctive risks that differ from other payment methods and stores of value. Here, we review market risk, the shallow market problem, counterparty risk, transaction risk, operational risk, privacy-related risk, and legal and regulatory risks.

Any user holding bitcoins faces **market risk** via fluctuation in the exchange rate between bitcoin and other currencies. Figure 2 plots the average US dollar–bitcoin exchange rate at the largest exchanges, along with the weekly trade volumes. A user might dismiss the short-term price spikes before mid-2013 as part of the price of using a new currency. But the sharp movements from late 2013 through 2015 would be a source of concern, both for users considering Bitcoin for transactions and for those using it as a store of value.

The relatively low weekly trade volumes suggest that Bitcoin users also experience a **shallow markets problem**: for example, a person seeking to trade a large amount of bitcoin typically cannot do so quickly without affecting the market price.

Given centralization in the Bitcoin ecosystem, **counterparty risk** has become substantial. Exchanges often act as de facto banks, as users convert currency to bitcoin but then leave the bitcoin in the exchange. However, 45 percent of the Bitcoin currency exchanges studied by Moore and Christin (2013) ultimately ceased operation. High-volume exchanges were more likely to close because of a security breach, while operators of low-volume exchanges were more likely to abscond without explanation. Of the exchanges that closed, 46 percent did not reimburse their customers after shutting down. If users avoid holding their bitcoins in an exchange and instead use a digital wallet service, other risks arise, as these firms
have become a lucrative target for cybercriminals. Examples include 4,100 bitcoins (valued at $1.2 million at then-applicable rates) taken from Bitcoin wallet inputs.io in November 2013, leading to that company’s default (McMillan 2013) as well as 1,295 bitcoins ($1 million) taken from Bitcoin payment processor BIPS the next month following denial-of-service attacks (Southurst 2013).

The irreversibility of Bitcoin payments creates heightened transaction risk. If bitcoins are sent due to error or fraud, the Bitcoin system offers no built-in mechanism to undo the error. Of course, a buyer and seller can voluntarily agree to correct errors, but the Bitcoin protocol has no mechanism to retake the funds by force. In a world of competing payment methods, irreversibility puts Bitcoin at a disadvantage: all else equal, consumers should favor a payment system that allows reversal of unwanted or mistaken charges.

Transaction risk also arises when receiving payments. As discussed above, Bitcoin transactions do not clear (and hence are not final) until they have been added to the authoritative block chain. Transaction batches are only added every ten minutes on average. This creates at least two potential avenues for abuse. First, there is a low but persistent risk that what was once viewed as the authoritative block chain will later be cast aside, as voted on by a majority of participants, canceling any transactions recorded in that version of the block chain. Second, malevolent participants could double-spend bitcoins, particularly through rapid transactions before the block chain is updated. The protocol has taken steps to mitigate this possibility, but researchers have demonstrated viable attacks if Bitcoin is used for faster payments than intended by design (Karame, Androulaki, and Capkun 2012).

---

**Figure 2**

US Dollar–Bitcoin Exchange Rate, January 2012–March 2015, along with Daily Bitcoin Trade Volume (in US Dollar Equivalent) at Four Top Currency Exchanges

*Source: Authors using data from Blockchain.info and Quandl.com.*
A separate transaction risk arises from proposals to blacklist tainted Bitcoins, specifically those that have been obtained through theft. Some set of arbiters would publicly announce the ill-gotten bitcoins (much like a list of serial numbers on stolen paper currency), and the proposals call on the community to refuse incoming payments appearing on the blacklist. However, blacklists are controversial within the Bitcoin community (Bradbury 2013). After all, blacklists create the prospect of rejecting transactions that have already occurred—transferring losses to those who had unknowingly accepted bitcoin that later turned out to be ill-gotten. Blacklists add significant complexity and create a risk of abuse by those who manage the blacklists. Finally, widespread use of blacklists could undermine the fungibility of bitcoins. With the block chain available for public inspection, each bitcoin can be traced to its unique transaction history, and in principle market participants could place varying values on bitcoins according to their apparent risk of future blacklisting.

Operational risk encompasses any action that undermines Bitcoin’s technical infrastructure and security assumptions. For example, despite a user’s efforts to keep a private key secure, vulnerabilities are to be expected—including operator error, security flaws, and malware that scours hard drives in search of wallet credentials and private keys. At least as worrisome, the Bitcoin platform faces operational risks through potential vulnerabilities in the protocol design or breakthroughs in cryptanalysis. Community attention has focused on the so-called “51 percent attack,” in which if some group can reliably control more than half the computational power, they can seize control of the system (Barber, Boyen, Shi, and Uzen 2012). If such attacks arose, the Bitcoin community might devise defenses, but the conflict and transition would be chaotic and would probably undermine trust in Bitcoin.

Denial-of-service attacks form a particularly prominent operational risk, particularly large for those who use Bitcoin through various intermediaries. Denial-of-service attacks entail swamping a target firm with messages and requests in such volume that it becomes unusable or very slow. Such attacks have diverse motivations. For example, an attack on a mining pool can prevent a pool’s participants from solving the current puzzle and thus give an advantage to all other miners (Johnson, Laszka, Grossklags, Vasek, and Moore 2014). News of an attack can undermine trust in an exchange or even in Bitcoin itself—allowing an attacker to buy bitcoin at lower prices. Finally, attackers can demand ransom from service providers (such as exchanges), threatening attacks that would undermine the service’s operation and customers’ confidence. Figure 3 plots the number of denial-of-service attacks reported by users on the popular bitcointalk.org forum in 2011 to 2013, showing progression from attacks on mining pools to attacks on exchanges. While denial-of-service attacks occur throughout the web, they seem to be particularly effective in the Bitcoin ecosystem due to the relative ease of monetizing the attacks.

Bitcoin raises certain privacy risks, most notably the risk that transactions can be linked back to the people who made them. Bitcoin transactions are not truly anonymous: instead, they are pseudonymous, in that each transaction specifies account information (the user’s public key) albeit without personal names, and the block
Figure 3
Reported (Distributed Denial of Service) DDoS Attacks on Bitcoin Services over Time


chain publishes transactions by that user identifier. Moreover, transactions made using Bitcoin often reveal real names—for example, as funds are converted to or from currencies in traditional banks, or when purchases from retailers reveal a customer name and mailing address. In principle, a Bitcoin user’s identity could be obtained from one such source and then associated with the user’s other transactions—flouting the widespread expectation of privacy.

Finally, Bitcoin systems face numerous legal and regulatory risks across countries. For example, a law-abiding user could lose funds in an exchange that is frozen or seized due to criminal activity—even if only a portion of the exchange’s customers were in fact engaged in such activity. Furthermore, uncertain tax treatment of Bitcoin gains and losses hinders tax planning. We explore these questions in the next section.

Regulating Virtual Currencies

The original vision of Bitcoin is broadly in tension with regulation and government control. In this respect Bitcoin extends a line of cyber-libertarianism, traced
back at least to John Perry Barlow’s 1996 “Declaration of the Independence of Cyberspace,” denying the role of governments in overseeing online communications. But contrary to the initial view that Bitcoin’s decentralization made it impossible to regulate, there now appears to be ample possibility of regulatory oversight, as well as circumstances in which such intervention could be useful.

**Fighting Crime**

Bitcoin receives regulatory scrutiny for three classes of criminal concerns: Bitcoin-specific crime, money laundering, and Bitcoin-facilitated crime.

**Bitcoin-specific crimes** are attacks on the currency and its infrastructure like bitcoin theft, attacks on mining pools, and denial-of-service attacks on exchanges to manipulate exchange rates. Law enforcement often struggles to prevent or solve these crimes due to their novelty, lack of clarity on which agency and jurisdiction are responsible, technical complexity, procedural uncertainty, and limited resources.

Second, Bitcoin can be used for **money laundering**. Bitcoin money laundering could evolve to become more difficult to trace, particularly when funds are routed through mixers, with mixing records concealed from the public and perhaps unavailable to law enforcement. These characteristics might assist perpetrators in concealing or mischaracterizing the proceeds of crime. That said, Bitcoin also includes design elements that could facilitate the tracing of funds, including publication of the block chain (providing permanent publicly available records of what funds moved where).

Finally, **Bitcoin-facilitated crime** entails payment for unlawful services delivered (or purportedly delivered) offline, like the illegal goods and services sold on Silk Road and payment of funds in extortion. Criminals may be drawn to virtual currencies because they perceive a lack of regulatory oversight, because they distinctively value irreversible transactions, or because they have been banned or ejected from other payment mechanisms.

**Consumer Protection**

A related justification for regulatory action is the need for consumer protection. Such discussions were particularly frequent after the February 2014 failure of Bitcoin exchange Mt. Gox, which lost bitcoins valued at more than $300 million. In light of this failure and others (Moore and Christin 2013), it is desirable to have orderly processes that distribute any remaining assets equitably. The risk of collapse also calls for disclosures to help consumers understand the products they are buying.

Broader consumer protection concerns result from irreversibility of Bitcoin transfers. Most electronic payment systems provide mechanisms to protect consumers against unauthorized transfers, and indeed such protections are often codified into law. (For example, credit card dispute rights are guaranteed by the US Fair Credit and Billing Act, 15 USC § 1666.) The absence of such protections in Bitcoin therefore appears to be contrary to longstanding public policy.
Regulatory Options

A key challenge for prospective regulators is where to impose constraints. It is infeasible to regulate all peers in the Bitcoin network due to their quantity, their geographic distribution, and the privacy protections in the network. Instead, regulators are naturally drawn to key intermediaries. But intermediaries raise predictable defenses. Why, they ask, should they face liability for the conduct of third-party users, customers, or suppliers? Furthermore, some users will anticipate regulators targeting intermediaries and will act to avoid such scrutiny, just as criminals can pay each other in cash to hide illegal activities from financial institutions.

The FBI takedown of Silk Road in 2013 illustrates both the challenges of regulation and regulators’ ultimate power. Silk Road was hosted as a “hidden service” on Tor, a system which is purpose-built for anonymity of both visitors and operators. Payments were only accepted in bitcoin. However, the Silk Road domain site was seized by the FBI when the site’s alleged operator, Ross Ulbricht, was arrested on charges of conspiracy to distribute controlled substances, computer hacking, money laundering, and murder-for-hire charges. The private keys associated with Ulbricht’s 144,000 bitcoins were also seized by the FBI (Greenberg 2013). Investigators targeted large merchants and administrators on Silk Road, exploiting poor operational security tactics to find their real identities. Ulbricht himself was identified by finding an early Silk Road advertisement posted on an online forum using his personal Gmail address (Zetter 2013). Silk Road’s online presence and electronic records in some respects made it an easier target than, say, a small-time dealer of drugs or weapons.

Transfers through currency exchanges are also within regulators’ grasp. In March 2013, the US Financial Crimes Enforcement Network issued guidance on when virtual currency operators should be classified as money-services businesses, requiring certain registration, reporting, and recordkeeping obligations. As exchanges complied, account details became available to regulators, and two months later, a US judge signed a seizure warrant for an account at the Mt. Gox exchange. In China, a December 2013 policy was broadly similar, requiring that Bitcoin intermediaries implement know-your-customer registrations for account-holders (People’s Bank of China and Five Associated Ministries 2013). These regulatory requirements will not impede peer-to-peer bitcoin transactions that are not facilitated by currency exchanges. But it seems longstanding reporting requirements can provide a level of compliance for virtual currencies similar to what has been achieved for traditional currencies.

In principle, Bitcoin’s electronic implementation in some ways makes it easier to regulate than offline equivalents. Consider the problem of theft. Once stolen cash enters circulation, little can be done to reclaim it. In contrast, Bitcoin blacklists could let law enforcement claw back all ill-gotten or stolen bitcoins—albeit with the problems discussed earlier.

Tax treatment of Bitcoin remains unsettled. In March 2014, the Internal Revenue Service (2014) issued guidance that transactions to and from virtual currencies may create taxable events for federal tax purposes. Thus, if a user converts...
dollars to bitcoin at one exchange rate, then later converts back at a higher rate, the user may owe tax on the appreciation; conversely, losses could offset gains elsewhere. Depending on the user’s purpose and primary activity, the gains and losses could be ordinary income or capital (Notice 2014-21). While this guidance seems well-grounded in longstanding principles of US tax law, it was criticized for creating additional record-keeping and complexity, particularly for those whose conversions are frequent.

While Bitcoin now appears to be subject to regulatory oversight, the authority of regulators faces certain limits. For example, if one country places too large a burden on Bitcoin services based there, services are likely to develop elsewhere. If many countries impede use of Bitcoin, some users will resort to services like Zerocash with even stronger security precautions—likely letting criminals continue to use the service yet, perhaps, adding too much complexity for mainstream consumers. The overall regulatory goal should not take aim at Bitcoin or any other specific system or company, but instead should consider regulations in the broader context of a global market for virtual currency services.

**Bitcoin as a Social Science Laboratory**

Bitcoin has the potential to be a fertile area for social science research. Scholars should appreciate Bitcoin’s contained environment with a clear set of rules (albeit not free from frictions), the publicly available record of transactions (unusual for most means of exchange), and the general availability of data even beyond the block chain (including market prices and trading volumes). To date, researchers have considered diverse questions ranging from design of financial markets to user behavior along with myriad questions of law and regulation. This research is of course quite recent, and much of it is still in working paper form. Many questions remain open, particularly to researchers who combine a deep understanding of Bitcoin with technical skills to collect data and a solid background in social science. Here are some of the issues this research has tackled and could approach in the future.

**Bitcoin as a Financial Asset**

After comparing exchange-traded volume of bitcoins to total transaction volume within the Bitcoin network, Glaser, Zimmerman, Haferkorn, Weber, and Sterling (2014) conclude that most users (by volume) treat their bitcoin investments as speculative assets rather than as means of payment. Bitcoin investments seem to offer diversification benefits according to Brière, Oosterlinck, and Szafarz (2013), who study correlations between bitcoin and other asset classes. Gandal and Halaburda (2014) examine exchange rates of different virtual currencies to observe comovement and identify opportunities for triangular arbitrage. Preliminary results on daily “closing” prices indicate little opportunity, although this may reflect that the arbitrageurs operate faster than the frequency of data points. Of course, given
ongoing fluctuations in bitcoin prices and innovations in other virtual currencies, new data is already available for these kinds of studies.

**Incentive-compatibility in Bitcoin Protocols**

When confronted by a set of protocols, economic agents naturally look for ways to participate that increase their own gains. For example, early mining pools faced selfish behavior in the form of “pool hopping”: Miners opted out of the pool in long rounds, in which the potential block reward has to be shared with a larger group. This drew attention to the mechanism design problem of keeping the expected payoff constant over time (Rosenfeld 2011).

Overall, the standard Bitcoin client software does not always act in the best interest of its principal. Both on the peer-to-peer network layer (Babaioff, Dobzinski, Oren, and Zohar 2012) and for the block mining protocol (Eyal and Sirer 2014), the prescribed rules are not equilibrium strategies if one considers the option to withhold information on a selective and temporary basis. Furthermore, Houy (2014b) observes that larger blocks are less likely to win a block race than smaller ones, meaning that a miner reduces the chance of collecting a reward when including new transactions into blocks—raising the question of why miners include transactions into blocks at all. So far, these concerns are theoretical. We are not aware of empirical evidence demonstrating substantial deviations from the suboptimal rules.

**Privacy and Anonymity**

The protection of online privacy and personal information arises in many contexts, and Bitcoin offers a specific set of rules and firms like the “mixers” that seek to offer privacy—although as we have seen, the privacy protections can be breached in various ways. Several papers analyze the public Bitcoin transaction history (Reid and Harrigan 2012; Ober, Katzenbeisser, and Hamacher 2013; Ron and Shamir 2013), finding a set of heuristics that can help to link Bitcoin accounts with real-world identities as long as some additional information is available for a related transaction. Androulaki, Karame, Roeschlin, Scherer, and Čapkun (2013) quantify the anonymity in a simulated environment similar to Bitcoin, finding that almost half of the users can be identified by their transaction patterns.

**Monetary Policy**

In a broad sense, the Bitcoin economy implements a variant of Milton Friedman’s (1960, p. 90) “% 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 keys. This raises one of the classic questions in monetary policy: What happens when the size of an economy grows at a different rate than the quantity of money in that economy? Or if viewing Bitcoin as a social science laboratory, what happens if the Bitcoin economy grows faster than the supply of bitcoins?
Just as overly rapid growth of a money supply is classically linked to inflation, the fixed slow growth rate of Bitcoin creates the possibility of deflation if Bitcoin was to be used widely, as Krugman (2011) noted while comparing the Bitcoin economy to the gold standard. In response to this risk, developers proposed alternative system rules. For example, Primecoin and Peercoin modify Bitcoin to provide an unlimited money supply, with $k$ fixed to approximately 1 percent for Peercoin.

It remains unclear whether decentralized cryptographic currencies can be designed with monetary policies that include feedback or even discretion. Bitcoin’s design embodies a basic version of monetary policy that does not consider the state of the real economy. We note that Bitcoin’s block chain presents a crude measure of monetary indicators—specifically the number of transactions and their nominal amount—but offers no information about what value was actually provided in exchange for payment. The block chain thus lays the groundwork for automatic monetary policy based solely in nominal data, but does not facilitate any policy based on real economic activity. Human arbiters could presumably add information about economic conditions or could introduce discretion by judgment, but they would also introduce the governance questions Bitcoin set out to overcome. Further experience with Bitcoin and other virtual currencies may illuminate some of the longstanding issues on the conduct and effects of monetary policy.

**Looking Ahead**

What is the future of Bitcoin and other virtual currencies? To replace credit cards for everyday consumer payments? To displace Western Union and other firms for international cash payments? To supplant banks for short-term deposits? Will Bitcoin and other virtual currencies favor low costs (to undercut competitors), privacy (to serve users who distinctively seek that benefit), or decentralization (to avoid a single point of control)? When disputes arise, do Bitcoin service providers protect sellers (who seek finality) or buyers (who often want refunds)? The original vision of Bitcoin offered one set of answers, but as new constituents approach the service, it becomes less clear that early design decisions meet prevailing requirements. It is also uncertain whether a single service can serve all needs. For example, those who seek greater privacy may be prepared to accept greater technical complexity and perhaps higher fees. However, recruiting mainstream consumers and merchants seems to call for a focus on simplicity and lower prices.

Bitcoin may be able to accommodate a community of experimentation built on its foundations. Mixers already close the most obvious privacy shortcomings in Bitcoin’s early design, while pools help reduce risk for miners, and wallets address some of consumers’ usability and security concerns.

Other aspects of Bitcoin architecture are largely locked in place through its protocol design. For example, the block chain is the essence of Bitcoin. There is no clear way for Bitcoin to substitute a different approach to record-keeping while retaining installed Bitcoin software, remaining compatible with intermediary
systems, and, most importantly, retaining the overall consensus that has coordinated around Bitcoin. Instantaneous transaction confirmations seem to require equally fundamental changes. In these and other respects, Bitcoin will struggle to make adjustments.

Numerous competing virtual currencies are waiting in the wings. For example, Litecoin confirms transactions four times faster than Bitcoin, potentially facilitating retail use and other time-sensitive transactions. NXT reduces the electrical and computational burden of Bitcoin mining by replacing proof-of-work mining with proof-of-stake, assigning block chain duties in proportion to coin holdings. Zerocash (Ben-Sasson et al. 2014), which is not yet operational, will seek to improve privacy protections by concealing identifiers in the public transaction history. Peercoin allows a perpetual 1 percent annual increase in the money supply.

To offer their competing design decisions, alternative virtual currencies would first need to achieve confidence in their value and adoption. Bitcoin benefited from early excitement for its service, buyers and sellers at Silk Road, and favorable press coverage. A replacement virtual currency would struggle to obtain this combination of advantages, but without favorable expectations for growth, few would be willing to convert traditional currency into a competing coin. Whether or not Bitcoin expands as its proponents envision, it offers a remarkable experiment, a lab for researchers, and an attractive means of exchange for a subset of merchants and consumers.

References


United States of America v. Ross William


This article has been cited by:

1. Francisco Javier García-Corral, José Antonio Cordero-García, Jaime de Pablo-Valenciano, Juan Uribe-Toril. 2022. A bibliometric review of cryptocurrencies: how have they grown?. *Financial Innovation* **8**:1. [Crossref]


3. Yannick Hoga. 2022. Quantifying the data-dredging bias in structural break tests. *Statistical Papers* **63**:1, 143-155. [Crossref]


10. Martin Cimiterra, Jackie Krafft, Lionel Nesta. 2022. Blockchain as Schumpeter Mark 1 or Mark 2? An empirical analysis of blockchain job offers in France and Germany. *Industrial and Corporate Change* **30**:6, 1388-1402. [Crossref]


13. Shanu Khare, Azher Ashraf, Mir Mohammad Yousuf, Mamoon Rashid. Blockchain: Structure, Uses, and Applications in IoT 131-144. [Crossref]


15. Oscar Lage, Maria Saíz-Santos, José Manuel Zarzuelo. The Value and Applications of Blockchain Technology in Business: A Systematic Review of Real Use Cases 149-160. [Crossref]

16. Vanita Jain, Akanshu Raj, Abhishek Tanwar, Mridul Khurana, Achin Jain. Coin Drop—A Decentralised Exchange Platform 391-399. [Crossref]
17. Ashraf Jaradat, Omar Ali, Ahmad AlAhmad. Blockchain Technology: A Fundamental Overview 1-24. [Crossref]


19. Swati Mathur, Lokesh Vijayvargy. The Study of Blockchain Technology to Enhance the Organizational Performance: Theoretical Perception 227-240. [Crossref]

20. Mohamed Sohail, Said Tabet, Mohamed Loey, Nour Eldeen M. Khalifa. Using Blockchain-Based Attestation Architecture for Securing IoT 175-191. [Crossref]


22. Syed Jawad Hussain Shahzad, Elie Bouri, Moeen Ur Rehman, David Roubaud. 2022. The hedge asset for BRICS stock markets: Bitcoin, gold or VIX. *The World Economy* 45:1, 292-316. [Crossref]


34. David Vidal-Tomás. 2021. The entry and exit dynamics of the cryptocurrency market. *Research in International Business and Finance* 58, 101504. [Crossref]


42. Raja Wasim Ahmad, Haya Hasan, Raja Jayaraman, Khaled Salah, Mohammed Omar. 2021. Blockchain applications and architectures for port operations and logistics management. *Research in Transportation Business & Management* 41, 100620. [Crossref]


47. Xucan Chen, Wei Cheng, Marie Ouellet, Yuan Li, David Maimon, Yubao Wu. Identifying Darknet Vendor Wallets by Matching Feedback Reviews with Bitcoin Transactions 788-797. [Crossref]


50. Fairouz Mustafa, Suman Lodh, Monomita Nandy, Vikas Kumar. 2021. Coupling of cryptocurrency trading with the sustainable environmental goals: Is it on the cards?. *Business Strategy and the Environment* 46. [Crossref]

58. Andrew M. Bailey, Bradley Rettler, Craig Wärnke. 2021. Philosophy, politics, and economics of cryptocurrency I: Money without state. *Philosophy Compass* 16:11. [Crossref]
59. Priyanka Chand Bhatt, Vimal Kumar, Tzu-Chuen Lu, Tugrul Daim. 2021. Technology convergence assessment: Case of blockchain within the IR 4.0 platform. *Technology in Society* 67, 101709. [Crossref]
63. Andrew Spurr, Marcel Ausloos. 2021. Challenging practical features of Bitcoin by the main altcoins. *Quality & Quantity* 55:5, 1541-1559. [Crossref]
65. Liam Hickey, Martin Harrigan. 2021. The Bisq decentralised exchange: On the privacy cost of participation. *Blockchain: Research and Applications* 29, 100029. [Crossref]


74. Don M. Autore, Nicholas Clarke, Danling Jiang. 2021. Blockchain speculation or value creation? Evidence from corporate investments. Financial Management 50:3, 727-746. [Crossref]


80. Klaus Grobys. 2021. When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market. Quantitative Finance 21:8, 1267-1279. [Crossref]


82. Ehsan Rehman, Muhammad Asghar Khan, Tariq Rahim Soomro, Nasser Taleb, Mohammad A. Afifi, Täher M. Ghazal. 2021. Using Blockchain to Ensure Trust between Donor Agencies and NGOs in Under-Developed Countries. Computers 10:8, 98. [Crossref]


86. Ilya Ivaninskiy, Irina Ivashkovskaya, Joseph A. McCahery. 2021. Does digitalization mitigate or intensify the principal-agent conflict in a firm?. Journal of Management and Governance 103. [Crossref]


88. Hesam Hamledari, Martin Fischer. 2021. The application of blockchain-based crypto assets for integrating the physical and financial supply chains in the construction & engineering industry. Automation in Construction 127, 103711. [Crossref]
89. Ashish Rajendra Sai, Jim Buckley, Brian Fitzgerald, Andrew Le Gear. 2021. Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management* **58**:4, 102584. [Crossref]


100. Chao Liu, Xiaoshuai Zhang, Kok Koeng Chai, Jonathan Loo, Yue Chen. 2021. A survey on blockchain-enabled smart grids: Advances, applications and challenges. *IET Smart Cities* **3**:2, 56-78. [Crossref]


102. Ajay Kumar, Kumar Abhishek, Pranav Nerurkar, Mohammad R. Khosravi, Muhammad Rukanuddin Ghalib, Achyut Shankar. 2021. Big data analytics to identify illegal activities on Bitcoin Blockchain for IoMT. *Personal and Ubiquitous Computing* **17**, . [Crossref]


107. Dejian Yu, Tianxing Pan. 2021. Tracing the main path of interdisciplinary research considering citation preference: A case from blockchain domain. Journal of Informetrics 15:2, 101136. [Crossref]


110. Anushree Tandon, Puneet Kaur, Matti Mäntymäki, Amandeep Dhir. 2021. Blockchain applications in management: A bibliometric analysis and literature review. Technological Forecasting and Social Change 166, 120649. [Crossref]

111. Lan van Wassenaer, Cor Verdouw, Sjaak Wolfert. 2021. What Blockchain Are We Talking About? An Analytical Framework for Understanding Blockchain Applications in Agriculture and Food. Frontiers in Blockchain 4. [Crossref]


113. Natkamon Tovanich, Nicolas Soulie, Petra Isenberg. Visual Analytics of Bitcoin Mining Pool Evolution: On the Road Toward Stability? 1-5. [Crossref]


120. TOAN LUU DUC HUYNH, MEI WANG, VINH XUAN VO. 2021. ECONOMIC POLICY UNCERTAINTY AND THE BITCOIN MARKET: AN INVESTIGATION IN THE COVID-19 PANDEMIC WITH TRANSFER ENTROPY. The Singapore Economic Review 16, 1–27. [Crossref]


122. Rong Li, Sufang Li, Di Yuan, Huiming Zhu. 2021. Investor attention and cryptocurrency: Evidence from wavelet-based quantile Granger causality analysis. Research in International Business and Finance 56, 101389. [Crossref]


125. Nitin Mittal, Srishty Pal, Anjali Joshi, Ashish Sharma, Sandeep Tayal, Yogesh Sharma. Comparative Analysis of Various Platforms of Blockchain 323-340. [Crossref]


139. Rameez Yousuf, Zubair Jeelani, Dawood Ashraf Khan, Owais Bhat, Tawseef Ahmed Teli. Consensus Algorithms in Blockchain-Based Cryptocurrencies 1-6. [Crossref]

140. Bhavya Ahuja Grover, Bawna Chaudhary, Nikhil Kumar Rajput, Om Dukiya. Blockchain and Governance: Theory, Applications and Challenges 113-139. [Crossref]
147. Apostolos Ampountolas, Elizabeth Chiffer. 2021. Will blockchain shift Online Travel Agencies toward growth or to an end?. *Tourism Economics* 60, 135481662098537.  

[Crossref]

160. Pierluigi Martino. Blockchain Technology: Key Features and Main Applications 9-31. [Crossref]

161. Yun Joo An, Paul Moon Sub Choi, Seth H. Huang. Blockchain, Cryptocurrency, and Artificial Intelligence in Finance 1-34. [Crossref]

162. Pratyusa Mukherjee, Chittaranjan Pradhan. Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology 29-49. [Crossref]

163. Raja Wasim Ahmad, Khaled Salah, Raja Jayaraman, Ibrar Yaqoob, Samer Ellahham, Mohammed Omar. 2021. The Role of Blockchain Technology in Telehealth and Telemedicine. International Journal of Medical Informatics 8, 104399. [Crossref]


166. Ekaterina Kostikova, Diana Alekseeva, Svetlana Rybakova, Anna Savina. 2021. Prospects of legal regulation and use of the digital rouble. SHS Web of Conferences 109, 01018. [Crossref]

167. Andria van der Merwe. Cryptocurrencies and Other Digital Asset Investments 445-471. [Crossref]

168. Evripidis Rizos. The Nature of Rights Upon Cryptocurrencies 605-627. [Crossref]


171. Jona Stinner, Marcel Tyrell. The New World of Blockchain Economics: Consensus Mechanism as a Core Element 9-19. [Crossref]


174. Yudi Fernando, Mohd Ridzuan Darun, Ahmed Zainul Abideen, Daing Nasir Ibrahim, Marco Tieman, Fazeeda Mohamad. Adoption of Blockchain Technology to Improve Integrity of Halal Supply Chain Management 2488-2496. [Crossref]

175. Thomas Tribunella, Heidi R. Tribunella. A Maturity Model for Understanding and Evaluating Digital Money 385–405. [Crossref]

176. Hayden Covington, Young B. Choi. Blockchain and Bitcoin 605-617. [Crossref]

177. Yousef Alabbasi, Kamaljeet Sandhu. Blockchain Technologically Driven Innovation at the Gulf Cooperation Council Countries 1202-1217. [Crossref]

178. Santosh Kumar Pani, Rajdeep Chatterjee, Nihar Ranjan Mahapatra. Towards Trusted, Transparent and Motivational Professional Education System Through Blockchain 1218-1230. [Crossref]


180. Teck Ming Tan, Jari Salo, Petri Ahokangas, Veikko Seppänen, Philipp Sandner. Revealing the Disintermediation Concept of Blockchain Technology 88–102. [Crossref]
181. Nozha Erragcha, Hanene Babay. Blockchain Towards Decentralized Digital Marketing 32-51. [Crossref]
182. Paul C. van Oorschot. Bitcoin, Blockchains and Ethereum 375-409. [Crossref]
184. Dmytro Matskevych, Inna Granovska. 2021. MEDIA EFFECT ON CRYPTOCURRENCY POPULARITY AND PRICING. PROBLEMS OF SYSTEMIC APPROACH IN THE ECONOMY :4(84). . [Crossref]
185. Gilles Hilary, Laura Xiaolei Liu. Blockchain and Other Distributed Ledger Technologies in Finance 243-268. [Crossref]
186. Zixian Tang, Qiang Wang, Wenhao Li, Huaifeng Bao, Feng Liu, Wen Wang. Mining Trojan Detection Based on Multi-dimensional Static Features 51-65. [Crossref]
187. Khaled Gubran Al-Hashedi, Pritheega Magalingam, Nurazeen Maarop, Ganthan Narayana Samy, Azizah Abdul Manaf. A Conceptual Model to Identify Illegal Activities on the Bitcoin System 18-34. [Crossref]
188. Bibliography 1061-1141. [Crossref]
190. Shakshi Sharma, Rajesh Sharma. Forecasting Transactional Amount in Bitcoin Network Using Temporal GNN Approach 478-485. [Crossref]
192. Wei Zhang, Yi Li. 2020. Is idiosyncratic volatility priced in cryptocurrency markets?. Research in International Business and Finance 54, 101252. [Crossref]
196. Randy Priem. 2020. Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications. Financial Innovation 6:1. . [Crossref]
201. Hee Jin Kim, Ji Sun Hong, Hyun Chan Hwang, Sun Mi Kim, Doug Hyun Han. 2020. Comparison of Psychological Status and Investment Style Between Bitcoin Investors and Share Investors. *Frontiers in Psychology* 11. [Crossref]


203. NIKOLAOS A. KYRIAZIS. 2020. THE EFFECTS OF GOLD, STOCK MARKETS AND GEOPOLITICAL UNCERTAINTY ON BITCOIN PRICES AND VOLATILITY. *Global Economy Journal* 2050020. [Crossref]


207. Dalila Boughaci, Abdullah A.K. Alkhawaldeh. Enhancing the security of financial transactions in Blockchain by using machine learning techniques: towards a sophisticated security tool for banking and finance 110-115. [Crossref]

208. Hafsa Benaddi, Khalil Ibrahimi. A Review: Collaborative Intrusion Detection for IoT integrating the Blockchain technologies 1-6. [Crossref]


211. Waleed Rashideh. 2020. Blockchain technology framework: Current and future perspectives for the tourism industry. *Tourism Management* 80, 104125. [Crossref]


214. Kyeongsik Yoo, Kunwoo Bae, Eunil Park, Taeyong Yang. 2020. Understanding the diffusion and adoption of Bitcoin transaction services: The integrated approach. *Telematics and Informatics* 53, 101302. [Crossref]


216. Omar Ali, Mustafa Ally, Clutterbuck, Yogesh Dwivedi. 2020. The state of play of blockchain technology in the financial services sector: A systematic literature review. *International Journal of Information Management* 54, 102199. [Crossref]


221. Bibliography 287-290. [Crossref]


230. William J. Luther, Sean Stein Smith. 2020. Is Bitcoin a decentralized payment mechanism?. *Journal of Institutional Economics* **16**:4, 433-444. [Crossref]


235. Umut UYAR, Gökşal Selahatdin KELTEN, Tuncay MORALI. 2020. YATIRIMCILAR İÇİN TEKNİK ANALİZ: BITCOIN VE ETHEREUM UYGULAMALARI. *Finansal Araştırmalar ve Çalışmalar Dergisi* . [Crossref]

236. S. E. Galaitsi, Benjamin D. Trump, Igor Linkov. Governance for the Internet of Things 371-381. [Crossref]

237. İşılay TALAY, Orkun BAYRAM. 2020. Küresel Tedarik Zinciri Ve Uluslararası Ticaret Yönetiminde Verimli Ödeme Sistemi Seçimi. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi* . [Crossref]


241. Cihan SEÇİLMİŞ, Mustafa Çağatay KIZILTAŞ. 2020. TURİZM İŞLETMELERİNDE ÖDEME YÖNTEMİ OLARAK KRIPTO PARA KULLANIMININ TÜKETİCİ TERCİHLERİNİNE ETKİSİ. *İktisadi ve İdari Bilimler Fakültesi Dergisi* 22:1, 45-56. [Crossref]


244. P. Mary Jeyanthi. THEORIES OF CRYPTOCURRENCY, BLOCKCHAIN AND DISTRIBUTED SYSTEMS AND ENVIRONMENTAL IMPLICATIONS 215-238. [Crossref]

245. Sandeep Kr. Sharma, Rajiv Kumar Modanval, N. Gayathri, S. Rakesh Kumar, C. Ramesh. IMPACT OF APPLICATION OF BIG DATA ON CRYPTOCURRENCY 181-195. [Crossref]

246. K. Murugeswari, B. Balamurugan, G. Ganesan. BLOCKCHAIN AND BITCOIN SECURITY 149-156. [Crossref]

247. Avinash Kaur, Anand Nayyar, Parminder Singh. BLOCKCHAIN 25-42. [Crossref]


254. Winifred Huang, Michele Meoli, Silvio Vismara. 2020. The geography of initial coin offerings. *Small Business Economics* 55:1, 77-102. [Crossref]


256. Ingrid Bauer, Liudmila Zavolokina, Gerhard Schwabe. 2020. Is there a market for trusted car data?. *Electronic Markets* 30:2, 211-225. [Crossref]


259. WILKO BOLT, MAARTEN R.C. VAN OORDT. 2020. On the Value of Virtual Currencies. *Journal of Money, Credit and Banking* 52:4, 835-862. [Crossref]


262. Heshan Sameera Kankanam Pathiranage, Huilin Xiao, Weifeng Li. 2020. The inefficiencies of bitcoins in developing countries. *Applied Economics Letters* 1-5. [Crossref]

263. Oliver Entrop, Bart Frijns, Marco Seruset. 2020. The determinants of price discovery on bitcoin markets. *Journal of Futures Markets* 40:5, 816-837. [Crossref]


265. Viachaslau Filimonau, Elena Naumova. 2020. The blockchain technology and the scope of its application in hospitality operations. *International Journal of Hospitality Management* 87, 102383. [Crossref]


267. Tianlong Fei, Yuan Chang, Jiaqi Wang, Ning Lu, Wenbo Shi. Anonymous Bitcoin Mixing Scheme Based on Semi-Trusty Supervisor 845-850. [Crossref]

268. Janick Rueegger, Guilherme Sperb Machado. Rational Exchange: Incentives in Atomic Cross Chain Swaps 1-3. [Crossref]


270. Ahmet Şakir DOKUZ, Mete ÇELİK, Alper ECEMIŞ. 2020. DBSCAN Algoritması Kullanarak Bitcoin Fiyatlarında Anormallık Tespiti. *European Journal of Science and Technology* 436-443. [Crossref]


279. Xiaoyu Li, Jiahong Yuan, Yan Shi, Zilai Sun, Junhu Ruan. 2020. Emerging Trends and Innovation Modes of Internet Finance—Results from Co-Word and Co-Citation Networks. *Future Internet* **12**:3, 52. [Crossref]

280. Pamella Soares de Sousa, Nataniel Parente Nogueira, Rayane Celestino dos Santos, Paulo Henrique M. Maia, Jerffeson Teixeira de Souza. Building a prototype based on Microservices and Blockchain technologies for notary’s office: An academic experience report 122-129. [Crossref]


284. Syed Omer Husain, Alex Franklin, Dirk Roep. 2020. The political imaginaries of blockchain projects: discerning the expressions of an emerging ecosystem. *Sustainability Science* **15**:2, 379-394. [Crossref]


289. Shinji Kakinaka, Ken Umeno. 2020. Characterizing Cryptocurrency Market with Lévy’s Stable Distributions. *Journal of the Physical Society of Japan* **89**:2, 024802. [Crossref]


295. Reilly White, Yorgos Marinakis, Nazrul Islam, Steven Walsh. 2020. Is Bitcoin a currency, a technology-based product, or something else?. *Technological Forecasting and Social Change* **151**, 119877. [Crossref]


297. E. L. Sidorenko. Stablecoin as a New Financial Instrument 630-638. [Crossref]


301. Hazik Bin Mohamed, Norhanim Mat Sari. Artificial Intelligence and Blockchain-Driven Islamic Capital Markets 874-888. [Crossref]


303. Antonio Carnevale, Carmela Occhipinti. Ethics and Decisions in Distributed Technologies: A Problem of Trust and Governance Advocating Substantive Democracy 300-307. [Crossref]

304. William J. Luther, Sean Stein Smith. 2020. Is Bitcoin a Decentralized Payment Mechanism?. *SSRN Electronic Journal*. [Crossref]

305. Andreas Mann, Florian Oliver Knauer. Der Einsatz der Blockchain-Technologie im (Dialog-)Marketing 85-118. [Crossref]

306. Ioannis Antoniadis, Konstantinos Spinthiropoulos, Stamatis Kontsas. Blockchain Applications in Tourism and Tourism Marketing: A Short Review 375-384. [Crossref]

307. Abdullah Yalaman. Bitcoin Jumps and Speculations: Empirical Evidence from High-Frequency Data 617-629. [Crossref]

308. Ralf-Christian Härting, Christopher Reichstein. Potential Use of Bitcoin in B2C E-commerce 33-40. [Crossref]


312. Wout J. Hofman. Supply Chain Visibility Ledger 305-329. [Crossref]
313. Matthias Horn, Andreas Oehler, Stefan Wendt. FinTech for Consumers and Retail Investors: Opportunities and Risks of Digital Payment and Investment Services 309-327. [Crossref]


315. P. V. Siva Kumar, Sriramudu, Chaitanya Palli, J. Adarshavathi, Padmavathi Guddeti. A Proposed Blockchain Model to Enhance Student Knowledge 107-115. [Crossref]


318. Artemij Voskobojnikov, Borke Obada-Obieh, Yue Huang, Konstantin Beznosov. Surviving the Cryptojungle: Perception and Management of Risk Among North American Cryptocurrency (Non)Users 595–614. [Crossref]

319. Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry, Arthur Gervais. SoK: Layer-Two Blockchain Protocols 201–226. [Crossref]

320. Jun Yang, Zhiguang Li. Impact of Bitcoin’s Distributed Structure on the Construction of the Central Bank’s Digital Currency System 829–832. [Crossref]

321. Xiaochen Zheng, Jinzhi Lu, Shengjing Sun, Dimitris Kiritsis. Decentralized Industrial IoT Data Management Based on Blockchain and IPFS 222–229. [Crossref]

322. Saketh Aleti, Bruce Mizrach. 2020. Bitcoin Spot and Futures Market Microstructure. SSRN Electronic Journal. [Crossref]

323. Anjum Khurshid. 2020. Applying Blockchain Technology to Address the Crisis of Trust During the COVID-19 Pandemic. JMIR Medical Informatics 8:9, e20477. [Crossref]

324. Yepeng Ding, Hiroyuki Sato. Formalizing and Verifying Decentralized Systems with Extended Concurrent Separation Logic 480–494. [Crossref]

325. Tommy Crépélière, Stefan Zeisberger. 2020. Arbitrage in the Market for Cryptocurrencies. SSRN Electronic Journal. [Crossref]

326. Christian Rainero, Alessandro Migliavacca, Riccardo Coda. 2020. Accounting for pandemics and economic crises management: Moral hazard, blockchain, and smart-contracts. Corporate Ownership and Control 18:1, Special Issue, 301–309. [Crossref]

327. Ping He, Dunzhe Tang, Jingwen Wang. 2020. Stake Centralization in Decentralized Proof-of-Stake Blockchain Network. SSRN Electronic Journal. [Crossref]

328. Artur Meynkhard. Effect of Bitcoin Volatility on Altcoins Pricing 652–664. [Crossref]

329. Ben Krishna, Satish Krishnan. Explaining Variation in Adoption of FinTech Products and Services Among Citizens: A Multilevel Model 541–552. [Crossref]

330. Isaiah Hull, Or Sattath, Eleni Diamanti, Göran Wendin. 2020. Quantum Technology for Economists. SSRN Electronic Journal. [Crossref]

331. João Marinotti. 2020. Tangibility As Technology. SSRN Electronic Journal. [Crossref]

332. Junying Gao, Bo Li, Zhihuai Li. Blockchain Storage Analysis and Optimization of Bitcoin Miner Node 922–932. [Crossref]


336. Georgios Drakopoulos, Michail Marountas, Xenophon Liapakis, Giannis Tzimas, Phivos Mylonas, Spyros Sioutas. Blockchain for Mobile Health Applications Acceleration with GPU Computing 389-396. [Crossref]

337. Yang Li, Zilu Liu, Zibin Zheng. Quantitative Analysis of Bitcoin Transferred in Bitcoin Exchange 549-562. [Crossref]


341. Andrei O. J. Kwok, Sharon G. M. Koh. 2019. Is blockchain technology a watershed for tourism development?. *Current Issues in Tourism* 22:20, 2447-2452. [Crossref]


357. Seth Frey, P. M. Krafft, Brian C. Keegan. 2019. "This Place Does What It Was Built For". *Proceedings of the ACM on Human-Computer Interaction* 3:CSCW, 1-31. [Crossref]


360. M. Creydt, M. Fischer. 2019. Blockchain and more – Algorithm driven food traceability. *Food Control* 105, 45-51. [Crossref]


363. Hilmi Lazrag, Abdellah Chehri, Rachid Saadane, Moulay Driss Rahmani. A Blockchain-Based Approach for Optimal and Secure Routing in Wireless Sensor Networks and IoT 411-415. [Crossref]

364. Yuling Chen, Jinyi Guo, Changlou Li, Wei Ren. 2019. FaDe: A Blockchain-Based Fair Data Exchange Scheme for Big Data Sharing. *Future Internet* 11:11, 225. [Crossref]


373. Georgios Drakopoulos, Eleanna Kafeza, Haseena Al Katheeri. Proof Systems In Blockchains: A Survey 1-6. [Crossref]
374. Muhammad Imran Sarwar, Kashif Nisar, Amna Khan. Blockchain - From Cryptocurrency to Vertical Industries - A Deep Shift 1-4. [Crossref]
377. Yong Tang, Jason Xiong, Rafael Becerril-Arreola, Lakshmi Iyer. 2019. Ethics of blockchain. Information Technology & People 33:2, 602-632. [Crossref]
378. Ayana Aspembitova, Ling Feng, Valentin Melnikov, Lock Yue Chew. 2019. Fitness preferential attachment as a driving mechanism in bitcoin transaction network. PLOS ONE 14:8, e0219346. [Crossref]
382. ANDREA FLORI. 2019. CRYPTOCURRENCIES IN FINANCE: REVIEW AND APPLICATIONS. International Journal of Theoretical and Applied Finance 22:05, 1950020. [Crossref]
384. Alexander Hempfing. 2019. What’s left after the hype? An empirical approach comparing the distributional properties of traditional and virtual currency exchange rates. PLOS ONE 14:7, e0220070. [Crossref]
386. Sune Sandbeck, A.T. Kingsmith, Julian von Bargen. The block is hot 15-29. [Crossref]
390. Junqin Huang, Linghe Kong, Guihai Chen, Long Cheng, Kaishun Wu, Xue Liu. B-IoT: Blockchain Driven Internet of Things with Credit-Based Consensus Mechanism 1348-1357. [Crossref]
391. Jiaqi Liang, Linjing Li, Weiyun Chen, Daniel Zeng. Towards an Understanding of Cryptocurrency: A Comparative Analysis of Cryptocurrency, Foreign Exchange, and Stock 137-139. [Crossref]
392. MALCOLM CAMPBELL-VERDUYN, MARCEL GOGUEN. 2019. Blockchains, trust and action nets: extending the pathologies of financial globalization. Global Networks 19:3, 308-328. [Crossref]
394. Mini Sharma. Blockchain for Cybersecurity: Working Mechanism, Application areas and Security Challenges 1182-1187. [Crossref]

415. Avi Goldfarb, Catherine Tucker. 2019. Digital Economics. *Journal of Economic Literature* **57**:1, 3-43. [Abstract] [View PDF article] [PDF with links]

416. Christie Smith, Aaron Kumar. Crypto-Currencies - An Introduction to Not-So-Funny Moneys 351-381. [Crossref]


425. Barış ALNIAÇIK. 2019. KRİPTO PARALARIN DÜNYA VE TÜRKİYE'DEKİ GÜNCEL DURUMU ÜZERİNE BİR İNCELEME. *R&S - Research Studies Anatolia Journal* 2:4, 21-30. [Crossref]

426. Muhammet Şahin. 2019. KRİPTO PARA YENİ BİR VERGİ SIĞINAĞI MI? BİLİŞİM TEKNOLOJİLERİNDEKİ GELİŞMELER KAPSAMINDA BİR DEĞERLENDİRME. *Pamukkale University Journal of Social Sciences Institute* . [Crossref]

427. Fulya Teomete Yalabık, İsmet Yalabık. 2019. Anonymous Bitcoin v enforcement law. *International Review of Law, Computers & Technology* **33**:1, 34-52. [Crossref]

428. Damodaran Appukuttan Nair. 2019. The bitcoin innovation, crypto currencies and the Leviathan. *Innovation and Development* **9**:1, 85-103. [Crossref]


430. Irfan Syauqi Beik, Mohammad Soleh Nurzaman, Aisha Putrina Sari. Zakat Standard Framework of Halal Cryptocurrency 275-284. [Crossref]

431. Irfan Syauqi Beik, Muhammad Hasbi Zaenal, Priyesta Rizkiningsih. Waqf Led Halal Cryptocurrency Model 285-298. [Crossref]

432. Stefano Bistarelli, Alessandra Cretarola, Gianna Figà-Talamanca, Ivan Mercanti, Marco Patacca. Is Arbitrage Possible in the Bitcoin Market? (Work-In-Progress Paper) 243-251. [Crossref]

433. S. Niggol Seo. Economics of the Green Climate Fund, Paris Agreements, and Global Funds and Currencies: An Overview 1-33. [Crossref]
434. S. Niggol Seo. The Microbehavioral Economic Models of Adaptation Behaviors to Global Warming 67-104. [Crossref]
435. S. Niggol Seo. Economics and Evaluations of the Green Climate Fund 179-221. [Crossref]
436. S. Niggol Seo. Economics of Global Funds: United Nations Specialized Funds and Other Crypto, Crowdfunding, Green Funds 223-260. [Crossref]
437. Shaen Corbet, Brian Lucey, Maurice Peat, Samuel Vigne. What Sort of Asset? Bitcoin Analysed 52-65. [Crossref]
438. Yuezhong Wu, Rongrong Chen, Yanxi Tan, Zongmiao Shao. Research on Two-Dimensional Code Packaging Advertising and Anti-counterfeiting Based on Blockchain 28-36. [Crossref]
439. Sanket Kanjalkar, Joseph Kuo, Yunqi Li, Andrew Miller. Short Paper: I Can’t Believe It’s Not Stake! Resource Exhaustion Attacks on PoS 62-69. [Crossref]
440. Konny Light. Cryptocurrencies: Can They Live Together with National Currencies and What Impact Do They Have on National and Global Economies? 213-223. [Crossref]
441. Trevor Clohessy, Thomas Acton, Nichola Rogers. Blockchain Adoption: Technological, Organisational and Environmental Considerations 47-76. [Crossref]
442. Florian Glaser, Florian Hawlitschek, Benedikt Notheisen. Blockchain as a Platform 121-143. [Crossref]
443. Constantin Fischer, Ingo Fiedler, Lisa Babenko. Blockchain-Technologie im Handel der Zukunft 441-471. [Crossref]
448. Dionisis Philippas. 2019. Media Attention and Bitcoin Prices. SSRN Electronic Journal. [Crossref]
449. Sebastien Meunier, Danni Zhao-Meunier. 2019. Bitcoin, Distributed Ledgers and the Theory of the Firm. SSRN Electronic Journal. [Crossref]
456. . Buy/Hold/Trade or Sell/Divest/Disengage 121-202. [Crossref]
457. Alessandro Roncaglia. [Crossref]
458. Efe Caglar Cagli. The Causal Relationship Between Returns and Trading Volume in Cryptocurrency Markets: Recursive Evolving Approach 167-190. [Crossref]
459. Yakup Söylemez. Cryptocurrency Derivatives: The Case of Bitcoin 515-530. [Crossref]
460. Sovik Mukherjee. Existence of Speculative Bubbles for the US at Times of Two Major Financial Crises in the Recent Past: An Econometric Check of BitCoin Prices 475-486. [Crossref]
462. Rongxin Zheng, Cuiwen Ying, Jun Shao, Guiyi Wei, Hongyang Yan, Jianmin Kong, Yekun Ren, Hang Zhang, Weiguang Hou. New Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools with Defence Cost 567-580. [Crossref]
463. Lujain Alharbi, Dania Aljeaid. A Blockchain Review: A Comparative Study Between Public Key Infrastructure and Identity Based Encryption 69-81. [Crossref]
464. Dalila Boughaci, Omar Boughaci. A Comparative Study of Three Blockchain Emerging Technologies: Bitcoin, Ethereum and Hyperledger 3-7. [Crossref]
465. Don M. Autore, Nicholas Clarke, Danling Jiang. 2019. Bitcoin Speculation or Value Creation? Corporate Blockchain Investments and Stock Market Reactions. SSRN Electronic Journal . [Crossref]
466. Christian Pfister. 2019. 2. Les monnaies digitales, un nouvel univers ?. Regards croisés sur l’économie n°24:1, 40. [Crossref]
467. Pierangelo Rosati, Tilen Ćuk. Blockchain Beyond Cryptocurrencies 149-170. [Crossref]
469. Thomas Tribunella, Heidi R. Tribunella. A Maturity Model for Understanding and Evaluating Digital Money 220-245. [Crossref]
470. Yousef Alabbasi, Kamaljeet Sandhu. Blockchain Technologically Driven Innovation at the Gulf Cooperation Council Countries 89-110. [Crossref]
472. Ville Savolainen, Jorge Soria. 2019. Too Big to Cheat: Mining Pools' Incentives to Double Spend in Blockchain Based Cryptocurrencies. SSRN Electronic Journal . [Crossref]
474. Wolfgang K. Härdle, Campbell R. Harvey, Raphael C. G. Reule. 2019. Understanding Cryptocurrencies. SSRN Electronic Journal . [Crossref]
475. Sarah Azouvi, Mary Maller, Sarah Meiklejohn. Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance 127-143. [Crossref]
479. Daniel Monroy, Jorge Armando Corredor H. 2019. Regulando Fintech 2.0 y Fintech 3.0: Administración de riesgos y regulación prudencial (Regulating Fintech 2.0 and Fintech 3.0: Risk Management and Prudential Regulation). SSRN Electronic Journal 22. [Crossref]


481. Kee-Youn Kang. 2019. Cryptocurrency, Delivery Lag, and Double Spending History. SSRN Electronic Journal. [Crossref]

482. Hayden Covington, Young B. Choi. 2019. Blockchain and Bitcoin. International Journal of Cyber Research and Education 1:1, 27-37. [Crossref]


484. Sui Cheng, Sian-Jheng Lin. 2019. Mining Strategies for Completing the Longest Blockchain. IEEE Access 7, 173935-173943. [Crossref]

485. Jakob Müllner, Igor Filatotchev. Chapter 4 The Changing Face of International Business in the Information Age 91-121. [Crossref]

486. Lars Steinert, Christian Herff. 2018. Predicting altcoin returns using social media. PLOS ONE 13:12, e0208119. [Crossref]


489. Christie Smith, Aaron Kumar. 2018. CRYPTO-CURRENCIES - AN INTRODUCTION TO NOT-SO-FUNNY MONEYS. Journal of Economic Surveys 32:5, 1531-1559. [Crossref]

490. Francesco Parino, Mariano G. Beiró, Laetitia Gauvin. 2018. Analysis of the Bitcoin blockchain: socio-economic factors behind the adoption. EPJ Data Science 7:1. [Crossref]

491. Yang Lu. 2018. Blockchain: A Survey on Functions, Applications and Open Issues. Journal of Industrial Integration and Management 03:04, 1850015. [Crossref]


497. Zaheer Allam. 2018. On Smart Contracts and Organisational Performance: A Review of Smart Contracts through the Blockchain Technology. Review of Economic and Business Studies 11:2, 137-156. [Crossref]


521. Mohammad Jabeed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, Jun Han, Paul Sarda. Blockchain Versus Database: A Critical Analysis 1348-1353. [Crossref]

522. Arti Jain, Shashank Tripathi, Harsh Dhar Dwivedi, Pranav Saxena. Forecasting Price of Cryptocurrencies Using Tweets Sentiment Analysis 1-7. [Crossref]

523. Benjamin Johnson, Aron Laszka, Jens Grossklags, Tyler Moore. Economic Analyses of Security Investments on Cryptocurrency Exchanges 1253-1262. [Crossref]

524. George D. Webster, Ryan L. Harris, Zachary D. Hanif, Bruce A. Hembree, Jens Grossklags, Claudia Eckert. Sharing is Caring: Collaborative Analysis and Real-Time Enquiry for Security Analytics 1402-1409. [Crossref]

525. Yoshiaki Kawase, Shoji Kasahara. A Batch-Service Queueing System with General Input and Its Application to Analysis of Mining Process for Bitcoin Blockchain 1440-1447. [Crossref]

526. Abhishek Ray, Mario Ventresca, Hong Wan. A Mechanism Design Approach to Blockchain Protocols 1603-1608. [Crossref]

527. Yuan Zhao, Bob Duncan. The Impact of Crypto-Currency Risks on the Use of Blockchain for Cloud Security and Privacy 677-684. [Crossref]

528. Taiguarana Melo Tupinambas, Rafael Aerf Leao Cadence, Andre Paim Lemos. Cryptocurrencies Transactions Advisor Using a Genetic Mamdani-type Fuzzy Rules Based System 1-7. [Crossref]

529. Zhen Li, Qi Liao. Toward Socially Optimal Bitcoin Mining 582-586. [Crossref]

530. Haneffa Muchlis Gazali, Che Muhamad Hafiz Bin Che Ismail, Tamrin Amboala. Exploring the Intention to Invest in Cryptocurrency: The Case of Bitcoin 64-68. [Crossref]

531. Marianne Verdier. 2018. La blockchain et l’intermédiation financière. *Revue d’économie financière* N° **129**:1, 67-87. [Crossref]


537. Alan Litchfield, Jeff Herbert. 2018. ReSOLV: Applying Cryptocurrency Blockchain Methods to Enable Global Cross-Platform Software License Validation. *Cryptography* **2**:2, 10. [Crossref]


539. Nguyen B. Truong, Tai-Won Um, Bo Zhou, Gyu Myoung Lee. Strengthening the Blockchain-Based Internet of Value with Trust 1-7. [Crossref]

605. Sam Dallyn. 2017. Cryptocurrencies as market singularities: the strange case of Bitcoin. *Journal of Cultural Economy* 10:5, 462-473. [Crossref]


607. Marcus O’Dair, Zuleika Beaven. 2017. The networked record industry: How blockchain technology could transform the record industry. *Strategic Change* 26:5, 471-480. [Crossref]

608. Sarah Manski. 2017. Building the blockchain world: Technological commonwealth or just more of the same?. *Strategic Change* 26:5, 511-522. [Crossref]

609. John Gregor Fraser, Ahmed Bouridane. Have the security flaws surrounding BITCOIN effected the currency’s value? 50-55. [Crossref]


611. Stephan Wiefling, Luigi Lo Iacono, Frederik Sandbrink. 2017. Anwendung der Blockchain außerhalb von Geldwährungen. *Datenschutz und Datensicherheit - DuD* 41:8, 482-486. [Crossref]


617. Young Bin Kim, Jurim Lee, Nuri Park, Jaegul Choo, Jong-Hyun Kim, Chang Hun Kim. 2017. When Bitcoin encounters information in an online forum: Using text mining to analyse user opinions and predict value fluctuation. *PLOS ONE* 12:5, e0177630. [Crossref]

618. Malte Moser, Rainer Bohme. Anonymous Alone? Measuring Bitcoin’s Second-Generation Anonymization Techniques 32-41. [Crossref]

619. Xin Li, Chong Alex Wang. 2017. The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin. *Decision Support Systems* 95, 49-60. [Crossref]

620. Irene C.L. Ng, Susan Y.L. Wakenshaw. 2017. The Internet-of-Things: Review and research directions. *International Journal of Research in Marketing* 34:1, 3-21. [Crossref]


622. Swati Bhatt. The Sharing Economy: Information Cascades, Network Effects and Power Laws 105-118. [Crossref]

623. Alicja Mikolajewicz-Woźniak. Virtual Currencies as the Starting Point for Changes in Financial Ecosystem 79-95. [Crossref]

624. Gregor Dorfleitner, Lars Hornuf, Matthias Schmitt, Martina Weber. Definition of FinTech and Description of the FinTech Industry 5-10. [Crossref]
625. Stefan Seebacher, Ronny Schüritz. Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review 12-23. [Crossref]
626. Joost de Kruijff, Hans Weigand. Understanding the Blockchain Using Enterprise Ontology 29-43. [Crossref]
627. Timothy Johnson. Some Implications of a Pragmatic Approach to Finance 271-293. [Crossref]
628. Svein Ølnes, Arild Jansen. Blockchain Technology as a Support Infrastructure in e-Government 215-227. [Crossref]
630. Svetlana Abramova, Pascal Schöttle, Rainer Böhme. Mixing Coins of Different Quality: A Game-Theoretic Approach 280-297. [Crossref]
631. Marie Vasek, Joseph Bonneau, Ryan Castellucci, Cameron Keith, Tyler Moore. The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin Brain Wallets 609-618. [Crossref]
636. Ethan Kane. 2017. Is Blockchain a General Purpose Technology?. SSRN Electronic Journal . [Crossref]
641. Jason Potts, Ellie Rennie. 2017. A City Is a Data Pool: Blockchains and the Crypto-City. SSRN Electronic Journal . [Crossref]
645. Jonathan Chiu, Thorsten V. Koeppl. 2017. The Economics of Cryptocurrencies Bitcoin and Beyond. SSRN Electronic Journal . [Crossref]
648. Stefan Hubrich. 2017. 'Know When to Hodl Em, Know When to Fodl Em': An Investigation of Factor Based Investing in the Cryptocurrency Space. SSRN Electronic Journal . [Crossref]

671. Young Bin Kim, Jun Gi Kim, Wook Kim, Jae Ho Im, Tae Hyeong Kim, Shin Jin Kang, Chang Hun Kim. 2016. Predicting Fluctuations in Cryptocurrency Transactions Based on User Comments and Replies. *PLOS ONE* 11:8, e0161197. [Crossref]

672. William J. Luther. 2016. CRYPTO CURRENCIES, NETWORK EFFECTS, AND SWITCHING COSTS. *Contemporary Economic Policy* 34:3, 553-571. [Crossref]

673. Alessandro Acquisti, Curtis Taylor, Liad Wagman. 2016. The Economics of Privacy. *Journal of Economic Literature* 54:2, 442-492. [Abstract] [View PDF article] [PDF with links]


675. Trent J. MacDonald, Darcy W. E. Allen, Jason Potts. Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking 279-296. [Crossref]

676. Svein Ølnes. Beyond Bitcoin Enabling Smart Government Using Blockchain Technology 253-264. [Crossref]

677. Masooda Bashir, Beth Strickland, Jeremiah Bohr. What Motivates People to Use Bitcoin? 347-367. [Crossref]


679. Sinclair Davidson, Primavera De Filippi, Jason Potts. 2016. Economics of Blockchain. *SSRN Electronic Journal*. [Crossref]


691. Gregor Dorfleitner, Lars Hornuf, Matthias Schmitt, Martina Weber. 2016. The Fintech Market in Germany. SSRN Electronic Journal. [Crossref]

692. Michel Rauchs. 2016. Cryptocurrencies Meeting Business Ecosystems: The Case of Bitcoin. SSRN Electronic Journal. [Crossref]


694. Aaron W. Baur, Julian Bühler, Markus Bick, Charlotte S. Bonorden. Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co 63-80. [Crossref]

695. Alessandro Acquisti, Curtis R. Taylor, Liad Wagman. 2015. The Economics of Privacy. SSRN Electronic Journal. [Crossref]


699. David Yermack. 2015. Corporate Governance and Blockchains. SSRN Electronic Journal. [Crossref]

700. Gautam Vora. 2015. Cryptocurrencies: Are Disruptive Financial Innovations Here?. Modern Economy 06:07, 816-832. [Crossref]

701. Xin Li, Chong (Alex) Wang, Qi Wang. 2014. Exploring the Determinants of Bitcoin Exchange Rate. SSRN Electronic Journal. [Crossref]


703. Hal S. Scott. 2014. The Importance of the Retail Payment System. SSRN Electronic Journal. [Crossref]

704. Garrick Hileman. 2014. The Bitcoin Market Potential Index. SSRN Electronic Journal. [Crossref]


706. Dincer Atli. Cybercrimes via Virtual Currencies in International Business 105-122. [Crossref]