BITCOIN: A PRIMER FOR POLICYMAKERS

Crypto-currencies promise to lower the cost of payments but are threatened by excessive regulation, say **Jerry Brito** and **Andrea Castillo**

Bitcoin is an open-source, peer-to-peer digital currency. Among many other things, what makes Bitcoin unique is that it is the world's first completely decentralised digital-payments system. This may sound complicated, but the underlying concepts are not difficult to understand.

Overview

Until Bitcoin's invention in 2008 by the unidentified programmer known as Satoshi Nakamoto, online transactions always required a trusted third-party intermediary. For example, if Alice wanted to send $100 to Bob over the Internet, she would have had to rely on a third-party service like PayPal or MasterCard. Intermediaries like PayPal keep a ledger of account holders' balances. When Alice sends Bob $100, PayPal deducts the amount from her account and adds it to Bob's account.

Without such intermediaries, digital money could be spent twice. Imagine there are no intermediaries with ledgers, and digital cash is simply a computer file, just as digital documents are computer files. Alice could send $100 to Bob by attaching a money file to a message. But just as with email, sending an attachment does not remove it from one's computer. Alice would retain a copy of the money file after she had sent it. She could then easily send the *same* $100 to Charlie. In computer science, this is known as the 'double-spending' problem,[1] and until Bitcoin it could only be solved by employing a ledger-keeping trusted third party.

Bitcoin's invention is revolutionary because for the first time the double-spending problem can be solved without the need for a third party. Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network. Every transaction that occurs in the bitcoin economy is registered in a public, distributed ledger, which is called the block chain. New transactions are checked against the block chain to ensure that the same bitcoins haven't been previously spent, thus eliminating the double-spending problem. The global peer-to-peer network, composed of thousands of users, takes the place of an intermediary; Alice and Bob can transact without PayPal.

One thing to note right away is that transactions on the Bitcoin network are not denominated in dollars or euros or yen as they are on PayPal, but are

Jerry Brito is a Senior Research Fellow at the Mercatus Center at George Mason University and Director of its Technology Policy Program.
Andrea Castillo is a Program Associate for Spending and Budget Initiative at the Mercatus Center.
This article is reproduced here with permission of the Mercatus Center.

instead denominated in bitcoins. This makes it a virtual currency in addition to a decentralised pay-ments network. The value of the currency is not derived from gold or government fiat, but from the value that people assign to it. The dollar value of a bitcoin is determined on an open market, just as is the exchange rate between different world currencies.[2]

Because Bitcoin is a peer-to-peer network, there is no central authority charged with either creating currency units or verifying transactions.

Operation

So far we have discussed what Bitcoin is: a decentralised peer-to-peer payments network and a virtual currency that essentially operates as online cash. Now we will take a closer look at how Bitcoin works.

Transactions are verified, and double-spending is prevented, through the clever use of public-key cryptography.[3] Public-key cryptography requires that each user be assigned two 'keys,' one private key that is kept secret like a password, and one public key that can be shared with the world. When Alice decides to transfer bitcoins to Bob, she creates a message, called a 'transaction,' which contains Bob's public key, and she 'signs' it with her private key. By looking at Alice's public key, anyone can verify that the transaction was indeed signed with her private key, that it is an authentic exchange, and that Bob is the new owner of the funds. The transaction—and thus the transfer of ownership of the bitcoins—is recorded, time-stamped and displayed in one 'block' of the block chain. Public-key cryptography ensures that all computers in the network have a constantly updated and *verified* record of all transactions within the Bitcoin network, which prevents double-spending and fraud.

What does it mean when we say that 'the network' verifies transactions and reconciles the ledger? And how exactly are new bitcoins created and introduced into the money supply? As we have already seen, because Bitcoin is a peer-to-peer network, there is no central authority charged with either creating currency units or verifying transactions. This network depends on users who provide their computing power to do the logging and reconciling of transactions. These users are called 'miners'[4] because they are rewarded for their work with newly created bitcoins. Bitcoins are created, or 'mined,' as thousands of dispersed computers solve complex math problems that verify the transactions in the block chain. As one commentator has put it:

> The actual mining of Bitcoins is by a purely mathematical process. A useful analogy is with the search for prime numbers: it used to be fairly easy to find the small ones (Eratosthenes in Ancient Greece produced the first algorithm for finding them). But as they were found it got harder to find the larger ones. Nowadays researchers use advanced high-performance computers to find them and their achievements are noted by the mathematical community (for example, the University of Tennessee maintains a list of the highest 5,000).
>
> For Bitcoins the search is not actually for prime numbers but to find a sequence of data (called a 'block') that produces a particular pattern when the Bitcoin 'hash' algorithm is applied to the data. When a match occurs the miner obtains a bounty of Bitcoins (and also a fee if that block was used to certify a transaction). The size of the bounty reduces as Bitcoins around the world are mined.
>
> The difficulty of the search is also increased so that it becomes computationally more difficult to find a match. These two effects combine to reduce over time the rate at which Bitcoins are produced and mimic the production rate of a commodity like gold. At some point new Bitcoins will not be produced and the only incentive for miners will be transaction fees.[5]

So, the protocol was designed so that each miner contributes a computer's processing power toward

maintaining the infrastructure needed to support and authenticate the currency network. Miners are awarded newly created bitcoins for contributing their processing power toward maintaining the network and verifying transactions in the block chain. And as more processing power is dedicated to mining, the protocol will increase the difficulty of the math problem, ensuring that bitcoins are always mined at a predictable and limited rate.

This process of mining bitcoins will not continue forever. Bitcoin was designed to mimic the extraction of gold or other precious metals from the earth—only a limited, known number of bitcoins can ever be mined. The arbitrary number chosen to be the cap is 21 million bitcoins. Miners are projected to painstakingly harvest the last 'satoshi,' or 0.00000001 of a bitcoin, in the year 2140. If the total mining power scales to a high enough level, the difficulty in mining bitcoins will have increased so much that procuring this last satoshi will be quite a challenging digital undertaking. Once the last satoshi has been mined, miners who contribute their processing power toward verifying transactions will be rewarded through transaction fees rather than mined bitcoins. This ensures that miners still have an incentive to keep the network running after the last bitcoin is mined.

Pseudonymity

A great deal of attention given to Bitcoin in the media centres on the anonymity that the digital currency is supposed to lend its users. This idea stems from a mistaken understanding of the currency, however.

Because online transactions to date have required a third-party intermediary, they have not been anonymous. PayPal, for example, will have a record of every time Alice has sent Bob money. And because Alice's and Bob's PayPal accounts are tied to their respective bank accounts, their identities are likely known. In contrast, if Alice gives Bob a $100 bill in cash, there is no intermediary and no record of the transaction. And if Alice and Bob don't know each other's identities, we can say the transaction is completely anonymous.

Bitcoin falls somewhere between these two extremes. On the one hand, bitcoins are like cash in that once Alice gives bitcoins to Bob, she no longer has them and Bob does, and there is no third-party intermediary between them who knows their respective identities. On the other hand, unlike cash, the fact that a transaction took place between two public keys, the time, the amount, and other information is recorded in the block chain. Indeed, every transaction that has ever occurred in the history of the bitcoin economy is publicly viewable in the block chain.[6]

While the public keys for all transactions—also known as 'Bitcoin addresses'[7]—are recorded in the block chain, those public keys are not tied to anyone's identity. Yet if a person's identity were linked to a public key, one could look through the recorded transactions in the block chain and easily see all transactions associated with that key. So, while Bitcoin is very similar to cash in that parties can transact without disclosing their identities to a third party or to each other, it is unlike cash in that all the transactions to and from a particular Bitcoin address can be traced. In this way, Bitcoin is not anonymous but pseudonymous.

This process of mining bitcoins will not continue forever. Bitcoin was designed to mimic the extraction of gold or other precious metals.

Tying a real-world identity to a pseudonymous Bitcoin address is not as difficult as some might imagine. For one thing, a person's identity (or at least identifying information, such as an IP address) is often recorded when the person makes a Bitcoin transaction at a website, or exchanges dollars for bitcoins at a bitcoin exchange. To increase the chances of remaining pseudonymous, one would have to employ anonymising software like Tor, and take care never to transact with Bitcoin addresses that could be tied back to one's identity.

Finally, it is also possible to glean identities simply by looking at the block chain. One study found that behaviour-based clustering techniques could reveal the identities of 40% of Bitcoin users in their simulated Bitcoin experiment.[8] An early analysis of the statistical properties of the Bitcoin transaction graph showed how a passive network

analysis with the appropriate tools can divulge the financial activity and identities of Bitcoin users.[9] A later analysis of the statistical properties of the Bitcoin transaction graph garnered similar results with a larger dataset.[10] Another analysis of the Bitcoin transaction graph reiterated that observers using 'entity merging'[11] can observe structural patterns in user behavior and emphasised that this is 'one of the most important challenges to Bitcoin anonymity.'[12] In spite of this, Bitcoin users do enjoy a much higher level of privacy than do users of traditional digital-transfer services, who must provide detailed personal information to the third-party financial intermediaries that facilitate the exchange.

Although Bitcoin is frequently referred to as an 'anonymous' currency, in reality, it is very difficult to stay anonymous in the Bitcoin network. Pseudonyms tied to transactions recorded in the public ledger can be identified years after an exchange is made. Once Bitcoin intermediaries are fully compliant with the bank-secrecy regulations required of traditional financial intermediaries, anonymity will be even less guaranteed, because Bitcoin intermediaries will be required to collect personal data on their customers.

Although Bitcoin is frequently referred to as an 'anonymous' currency, in reality, it is very difficult to stay anonymous in the Bitcoin network.

Benefits

The first question that many people have when they learn about Bitcoin is, 'Why would I want to use bitcoins when I can use dollars?' Bitcoin is still a new and fluctuating currency that is not accepted by many merchants, so the uses for Bitcoin may seem mostly experimental. To better understand why people might want to use Bitcoin, it helps to think of it not necessarily as a replacement for traditional currencies, but rather as a new payments system.

Lower transaction costs

Because there is no third-party intermediary, Bitcoin transactions are substantially cheaper and quicker than traditional payment networks. And because transactions are cheaper, Bitcoin makes micropayments and other innovations possible. Additionally, Bitcoin holds much promise as a way to lower transaction costs for small businesses and global remittances, alleviate global poverty by improving access to capital, protect individuals against capital controls and censorship, ensure financial privacy for oppressed groups, and spur innovation (within and on top of the Bitcoin protocol). On the other hand, Bitcoin's decentralised nature also presents opportunities for crime. The challenge, then, is to develop processes that diminish the opportunities for criminality while maintaining the benefits that Bitcoin can provide.

First, Bitcoin is attractive to cost-conscious small businesses looking for ways to lower the transaction costs of doing business. Credit cards have greatly expanded the ease of transacting, but their use comes with considerable costs to merchants. Businesses that wish to offer the option of credit card payments to their customers must first pay for a merchant account with each credit card company. Depending on the terms of agreement with each credit card company, businesses must then pay a variety of authorisation fees, transaction fees, statement fees, interchange fees, and customer-service fees, among other charges. These fees quickly add up and significantly increase the cost of doing business. However, if a merchant neglects to accept credit card payments to save on fees, he or she could lose a considerable amount of business from customers who enjoy the ease of credit cards.

Since Bitcoin facilitates direct transactions without a third party, it removes costly charges that accompany credit card transactions. The Founders Fund, the venture capital fund headed by Peter Thiel of PayPal and Facebook fame, recently invested $3 million in the payment-processing company BitPay because of the service's ability to lower the costs of doing online commerce across borders.[13] In fact, small businesses have already started to accept bitcoins as a way to avoid the costs of doing business with credit card companies.[14] Others have adopted the currency for its speed and efficiency in facilitating transactions.[15] Bitcoin will likely continue to lower transaction costs for

businesses that accept it as more people adopt the currency.

Accepting credit card payments also puts businesses on the hook for charge-back fraud. Merchants have long been plagued by fraudulent 'charge-backs,' or consumer-initiated payment reversals based on a false claim that a product has not been delivered.[16] Merchants therefore can lose the payment for the item and the item itself, and also have to pay a fee for the charge-back. As a nonreversible payment system, Bitcoin eliminates the 'friendly fraud' wrought by the misuse of consumer charge-backs. This can be very important for small businesses.

Consumers like charge-backs, however, because that system protects them from unscrupulous merchants or merchant errors. Consumers may also enjoy other benefits that merchant-account fees help fund. Indeed, many consumers and merchants will probably stick to traditional credit card services even if Bitcoin payments become available. Still, the expanded choices in payment options would benefit people of all preferences.

Those who want the protection and perks of using a credit card can continue to do so, even if they pay a little more. Those who are more price- or privacy-conscious can use bitcoins instead. Not having to pay merchant fees means that merchants who accept Bitcoin have the option to pass the savings on to consumers. That is the business model of the Bitcoin Store,[17] which sells thousands of consumer electronics at discounted prices and only accepts bitcoins. The same Samsung Galaxy Note tablet that sells on Amazon for $779 plus shipping[18] sells at the Bitcoin Store for a mere $480.[19] In this way, Bitcoin provides more low-cost options to bargain hunters and small businesses without detracting from the traditional credit card services that some consumers prefer.

As an inexpensive funds-transfer system, Bitcoin also holds promise for the future of low-cost remittances. In 2012, immigrants to developed countries sent at least $401 billion in remittances back to relatives living in developing countries.[20] The amount of remittances is projected to increase to $515 billion by 2015.[21] Most of these remittances are sent using traditional brick-and-mortar wire services such as Western Union and MoneyGram, which charge steep fees for the service and can take several business days to transfer the funds.[22] In the first quarter of 2013, the global average fee for sending remittances was 9.05%.[23] In contrast, transaction fees on the Bitcoin network tend to be less than 0.0005 BTC,[24] or 1% of the transaction.[25] This entrepreneurial opportunity to improve money transfers has attracted investments from big-name venture capitalists.[26] Even MoneyGram and Western Union are contemplating whether to integrate Bitcoin into their business models.[27] Bitcoin allows for instantaneous, inexpensive remittances, and the reduction in the cost of global remittances for consumers could be considerable.

Bitcoin has the potential to improve the quality of life for the world's poorest. Improving access to basic financial services is a promising antipoverty technique.

Potential to combat poverty and oppression

Bitcoin also has the potential to improve the quality of life for the world's poorest. Improving access to basic financial services is a promising antipoverty technique.[28] According to one estimate, 64% of people living in developing countries lack access to these services, perhaps because it is too costly for traditional financial institutions to serve poor, rural areas.[29] Because of the impediments to developing traditional branch banking in poor areas, people in developing countries have turned to mobile banking services for their financial needs. The closed-system mobile payment service M-Pesa has been particularly successful in countries such as Kenya, Tanzania and Afghanistan.[30] Entrepreneurs are already moving to this model; the Bitcoin wallet service Kipochi recently developed a product that allows M-Pesa users to exchange bitcoins.[31] Mobile banking services in developing countries can be further augmented by the adoption of Bitcoin. As an open-system payment service, Bitcoin can provide people in developing countries with inexpensive access to financial services on a global scale.

Bitcoin might also provide relief to people living in countries with strict capital controls.

The total number of bitcoins that can be mined is capped and cannot be manipulated. There is no central authority that can reverse transactions or prevent the exchange of bitcoins between countries. Bitcoin therefore provides an escape hatch for people who desire an alternative to their country's devalued currencies or frozen capital markets. We have already seen examples of people turning to Bitcoin to evade the harmful effects of capital controls and central-bank mismanagement. Some Argentines, for instance, have adopted Bitcoin in response to the country's dual burdens of a 25% inflation rate and strict capital controls.[32] Demand for bitcoins is so strong in Argentina that one popular bitcoin exchange is planning to open an Argentine office.[33] Argentine Bitcoin use continues to surge in the face of Argentina's capital mismanagement.[34]

Bitcoin might also provide relief to people living in countries with strict capital controls. The total number of bitcoins that can be mined is capped and cannot be manipulated.

Individuals in oppressive or emergency situations might also benefit from the financial privacy that Bitcoin can provide. There are many legitimate reasons why people seek privacy in their financial transactions. Spouses fleeing abusive partners need some way to discreetly spend money without being tracked. People seeking controversial health services desire financial privacy from family members, employers and others who might judge their decisions. Recent experiences with despotic governments suggest that oppressed citizens would benefit greatly from the ability to make private transactions free from the grabbing hands of tyrants. Bitcoin provides some of the privacy that has traditionally been afforded through cash—with the added convenience of digital transfer.

Stimulus for financial innovation

One of the most promising applications of Bitcoin is as a platform for financial innovation. The Bitcoin protocol contains the digital blueprints for a number of useful financial and legal services that programmers can easily develop. Since bitcoins are, at their core, simply packets of data, they can be used to transfer not only currencies but also stocks, bets and sensitive information.[35] Some of the features that are built into the Bitcoin protocol include micropayments, dispute mediations, assurance contracts, and smart property.[36] These features would allow for the easy development of Internet translation services, instantaneous processing for small transactions (like automatically metering Wi-Fi access), and Kickstarter-like crowdfunding services.

Additionally, programmers can develop alternative protocols on top of the Bitcoin protocol in the same way that the Web and email are run on top of the Internet's TCP/IP protocol. One programmer has already proposed a new protocol layer to add on top of the Bitcoin protocol that can improve the network's stability and security.[37] Another programmer created a digital notary service to anonymously and securely store a 'proof of existence' for private documents on top of the Bitcoin protocol.[38] Other programmers have adopted the Bitcoin model as a way to encrypt email communications.[39] Another group of developers has outlined an add-on protocol that will improve the privacy of the network.[40] Bitcoin is thus the foundation upon which other layers of functionality can be built. The Bitcoin project can be best thought of as a process of financial and communicative experimentation. Policymakers should take care that their directives do not quash the promising innovations developing within and on top of this fledgling protocol.

Challenges

Despite the benefits that it presents, Bitcoin has some downsides for potential users to consider. It has exhibited considerable price volatility throughout its existence. New users are at risk of improperly securing or even accidentally deleting their bitcoins if they are not cautious. Additionally, there are concerns about whether hacking could compromise the bitcoin economy.

Volatility

Bitcoin has weathered at least five significant price adjustments since 2011.[41] These adjustments

resemble traditional speculative bubbles: overoptimistic media coverage of Bitcoin prompts waves of novice investors to pump up Bitcoin prices.[42] The exuberance reaches a tipping point, and the value eventually plummets. Newcomer investors eager to participate run the risk of overvaluing the currency and losing their money in a crash. Bitcoin's fluctuating value makes many observers sceptical of the currency's future.

Does this volatility foretell the end of Bitcoin? Some commentators believe so.[43] Others suggest that these fluctuations are stress-testing the currency and might eventually decrease in frequency as mechanisms develop to counteract volatility.[44] If bitcoins were only used as stores of value or units of account, the currency's volatility could indeed endanger its future. It does not make sense to manage business finances or keep savings in bitcoins if the market price swings wildly and unpredictably. When Bitcoin is used as a medium of exchange, however, volatility is less of a problem.[45] Merchants can price their wares in terms of a traditional currency and accept the equivalent number of bitcoins. Customers who purchase bitcoins to make a one-time purchase don't care about what the exchange rate will look like tomorrow; they simply care that Bitcoin can lower transaction costs in the present. Bitcoin's usefulness as a medium of exchange might explain why the currency has grown more popular among merchants in spite of its price volatility.[46] It is also possible that the value of bitcoins will become less volatile as more people become familiar with the Bitcoin technology and develop realistic expectations about its future.

Security breaches

As a digital currency, Bitcoin presents some specific security challenges.[47] If people are not careful, they can inadvertently delete or misplace their bitcoins. Once the digital file is lost, the money is lost, just as with paper cash. If people do not protect their private Bitcoin addresses, they can leave themselves open to theft. Bitcoin wallets can now be protected by encryption, but users must choose to activate the encryption. If a user does not encrypt his or her wallet, bitcoins could be stolen through malware.[48] Bitcoin exchanges, too, have at times struggled with security; hackers successfully stole 24,000 BTC ($250,000) from a bitcoin exchange called Bitfloor in 2012[49] and mounted a massive series of distributed denial-of-service (DDoS) attacks against the most popular bitcoin exchange, Mt.Gox, in 2013.[50] (Bitfloor eventually repaid the stolen funds to its customers, and Mt.Gox ultimately recovered from the DDoS attacks.) Of course, many of the security risks facing Bitcoin are similar to those facing traditional currencies. Dollar bills can be destroyed or lost, personal financial information can be stolen and used by criminals, and banks can be robbed or targeted by DDoS attacks. Bitcoin users should take care to learn about and prepare for security concerns just as they currently do for other financial activities.

When Bitcoin is used as a medium of exchange, however, volatility is less of a problem. Merchants can price their wares in terms of a traditional currency and accept the equivalent number of bitcoins.

Criminal uses

There are also reasons for policymakers to be apprehensive about some of Bitcoin's exaptations. Because Bitcoin is pseudonymous, policymakers and journalists have questioned whether criminals can use it to launder money and accept payment for illicit goods and services. Indeed, like cash, it can be used for ill as well as for good.

For one example, we can look at the infamous Deep Web[51] black market site known as 'Silk Road.' Silk Road takes advantage of the anonymising network Tor and the pseudonymous nature of Bitcoin to make available a vast digital marketplace where one can mail order drugs and other licit and illicit wares. Although Silk Road administrators do not allow the exchange of any goods that resulted from fraud or harm, like stolen credit card information or photographs of child exploitation, they do allow merchants to sell illegal products like forged identity documents and illicit drugs. The pseudonymous nature of Bitcoin allows buyers to purchase illegal goods online in the same way that cash has been traditionally used to

facilitate illicit purchases in person. One study estimated the total monthly Silk Road transactions amount to be approximately $1.2 million.[52] But the Bitcoin market amassed $770 million in transactions during June 2013; Silk Road sales constitute a small drop in the total bitcoin economy bucket.[53]

Bitcoin's association with Silk Road has tarnished its reputation. Following the publication of an article on Silk Road in 2011,[54] senators Charles Schumer and Joe Manchin sent a letter to Attorney-General Eric Holder and the Drug Enforcement Administration's administrator Michele Leonhart calling for a crackdown on Silk Road, the anonymising software Tor, and Bitcoin.[55]

Many of the potential downsides of Bitcoin are the same as those facing traditional cash. Cash has historically been the vehicle of choice for drug traffickers and money launderers, but policymakers would never seriously consider banning cash.

Another concern is that Bitcoin can be used to launder money for financing terrorism and trafficking in illegal goods. Although these worries are currently more theoretical than evidential, Bitcoin could indeed be an option for those who wish to discreetly move ill-gotten money. Concerns about Bitcoin's potential to facilitate money laundering were stoked after Liberty Reserve, a private, centralised digital-currency service based in Costa Rica, was shut down by authorities on charges of money laundering.[56]

While Liberty Reserve and Bitcoin appear similar because they both provide digital currencies, there are important differences between the two. Liberty Reserve was a centralised currency service created and owned by a private company, allegedly for the express purpose of facilitating money laundering. Bitcoin is not. The transactions within the Liberty Reserve economy were not transparent. Indeed, Liberty Reserve promised its customers anonymity. Bitcoin, on the other hand, is a decentralised open currency that provides a public record of all transactions. Money launderers may attempt to protect their Bitcoin addresses and identities, but their transaction records will always be public and accessible at any time by law enforcement. Laundering money through Bitcoin, then, can be seen as a much riskier undertaking than using a centralised system like Liberty Reserve. Additionally, several bitcoin exchanges have taken steps to comply with anti-money laundering recordkeeping and reporting requirements.[57] The combination of a public ledger system and the cooperation of bitcoin exchanges in collecting information on their customers will likely make Bitcoin less attractive to launderers relative to private anonymous virtual currencies.

It is also important to note that many of the potential downsides of Bitcoin are the same as those facing traditional cash. Cash has historically been the vehicle of choice for drug traffickers and money launderers, but policymakers would never seriously consider banning cash. As regulators begin to contemplate Bitcoin, they should be wary of the perils of overregulation. In the worst-case scenario, regulators could prevent legitimate businesses from benefitting from the Bitcoin network without preventing money launderers and drug traffickers from using bitcoins. If bitcoin exchanges are overburdened by regulation and shut down, for instance, money launderers and drug traffickers could still put money into the network by paying a person in cash to transfer his or her bitcoins into their virtual wallets. In this scenario, beneficial transactions are prevented by overregulation while the targeted activities are still able to occur. The challenge for policymakers and regulators is how to develop a system of oversight that assuages their twin concerns about money laundering and illicit purchases without smothering the benefits that Bitcoin is poised to provide to legitimate users in their everyday lives.

Conclusion

Bitcoin is an exciting innovation that has the potential to greatly improve human welfare and jumpstart beneficial and potentially revolutionary developments in payments, communications and business. Bitcoin's clever use of public-key encryption and peer-to-peer networking solves the double-spending problem that had previously made decentralised digital currencies impossible.

These properties combine to create a payment system that could lower transactions costs in business and remittances, alleviate poverty, provide an escape from capital controls and monetary mismanagement, allow for legitimate financial privacy online, and spur new financial innovations. On the other hand, as 'digital cash,' Bitcoin can be used for money laundering and illicit trade. Banning Bitcoin is not the solution to ending money laundering and illicit trade, just as banning cash is not a solution to these same ills.

Bitcoin could ultimately fail as an experimental digital currency and payment system. An unanticipated problem could arise and undermine the bitcoin economy. A superior cryptocurrency could outcompete and replace Bitcoin. It could simply fizzle out as a fad. The possibilities for failure are endless, but one reason for failure should not be that policymakers did not understand its workings and potential. We are ultimately advocating not for Bitcoin but for innovation. It is important that policymakers allow this experimentation to continue. Policymakers should work to clarify how Bitcoin is regulated and to normalise its regulation so that we have the opportunity to learn just how innovative Bitcoin can be.

Endnotes

1 David Chaum, 'Achieving Electronic Privacy,' *Scientific American* (August 1992), 96–101.
2 'Markets,' Bitcoincharts, http://bitcoincharts.com/markets/.
3 Christof Paar, Jan Pelzl, and Bart Preneel, 'Introduction to Public-Key Cryptography,' in Christof Paar and Jan Pelzl (eds), *Understanding Cryptography: A Textbook for Students and Practitioners* (New York: Springer, 2010), Chapter 6. Sample available at http://wiki.crypto.rub.de/Buch/download/Understanding-Cryptography-Chapter6.pdf.
4 Miners tend to be ordinary computer enthusiasts, but as mining becomes more difficult and expensive, the activity will likely become somewhat professionalised. For more information, see Alec Liu, 'A Guide to Bitcoin Mining,' *Motherboard* (22 March 2013).
5 Ken Tindell, 'Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995,' *Business Insider* (5 April 2013).
6 Note that this might be a boon to economic researchers.
7 *Bitcoin wiki*, s.v. 'Address,' https://en.bitcoin.it/wiki/Address.
8 Elli Androulaki, et al. 'Evaluating User Privacy in Bitcoin,' *IACR Cryptology ePrint Archive* 596 (2012).
9 Fergal Reid and Martin Harrigan, 'An Analysis of Anonymity in the Bitcoin System,' in Yaniv Altshuler, et al. (eds) *Security and Privacy in Social Networks* (New York: Springer, 2013), http://arxiv.org/pdf/1107.4524v2.pdf.
10 Dorit Ron and Adi Shamir, 'Quantitative Analysis of the Full Bitcoin Transaction Graph,' *IACR Cryptology ePrint Archive* 584 (2012).
11 Entity merging is the process of observing two or more public keys used as an input to one transaction at the same time. In this way, even if a user has several different public keys, an observer can gradually link them together and remove the ostensible anonymity that multiple public keys is thought to provide.
12 Micha Ober, Stefan Katzenbeisser, and Kay Hamacher, 'Structure and Anonymity of the Bitcoin Transaction Graph,' *Future Internet* 5:2 (2013).
13 Tom Simonite, 'Bitcoin Hits the Big Time, to the Regret of Some Early Boosters,' *MIT Technology Review* (22 May 2013).
14 Gabrielle Karol, 'Small Business Owners Say Bitcoins Better Than Credit Cards,' *FOX Business, Small Business Center* (12 April 2013).
15 Bailey Reutzel, 'Why Some Merchants Accept Bitcoin Despite the Risks,' *Payments Source* (21 May 2013).
16 Emily Maltby, 'Chargebacks create business headaches,' *The Wall Street Journal* (10 February 2011). One such scam involves Alice sending Bob a PayPal payment for a laptop that Bob has listed on Craigslist. Alice comes by Bob's house, picks up the laptop, and soon thereafter initiates a 'charge-back' (i.e. reverses the payment). PayPal generally requires proof of shipment before reversing a charge-back, so Bob is out of luck.
17 Vitalik Buterin, 'Bitcoin Store Opens: All Your Electronics Cheaper with Bitcoins,' *Bitcoin Magazine* (5 November 2012).
18 Amazon listing for a Samsung Galaxy Note tablet, http://amzn.com/B00BJXNGIK.
19 Bitcoin store listing for a Samsung Galaxy Note tablet, www.bitcoinstore.com/samsung-galaxy-note-gt-n8013-10-1-32-gb-tablet-wi-fi-1-40-ghz-deep-gray.html. Products on the Bitcoin store are priced in both bitcoins and US dollars. At the point of purchase, Bitpay, a Bitcoin payment processing company, determines the currency conversion rate and holds that price for 15 minutes. See the Bitcoin Store FAQ, www.bitcoinstore.com/faq.
20 World Bank Payment Systems Development Group, *Remittance Prices Worldwide: An Analysis of Trends in the Average Total Cost of Migrant Remittance Services* (Washington, DC: World Bank, 2013).
21 As above.
22 Jessica Silver-Greenberg, 'New rules for money transfers, but few limits,' *The New York Times* (1 June 2012).

23 World Bank, *Remittance Prices*.
24 *Bitcoin wiki*, s.v. 'Transaction fees,' https://en.bitcoin.it/wiki/Transaction_fees.
25 Andrew Paul, 'Is Bitcoin the Next Generation of Online Payments?' *Yahoo! Small Business Advisor* (24 May 2013).
26 Simonite, 'Bitcoin Hits the Big Time.'
27 Andrew R. Johnson, 'Money transfers in bitcoins? Western Union, MoneyGram weigh the option,' *The Wall Street Journal* (18 April 2013).
28 Muhammad Yunus, *Banker to the Poor: Micro-lending and the Battle Against World Poverty* (New York: Public Affairs, 2003).
29 Oya Pinar Ardic, Maximilien Heimann, and Nataliya Mylenko, 'Access to Financial Services and the Financial Inclusion Agenda around the World' (Policy Research Working Paper, World Bank Financial and Private Sector Development Consultative Group to Assist the Poor, 2011).
30 Jeff Fong, 'How Bitcoin Could Help the World's Poorest People,' *PolicyMic* (May 2013).
31 Emily Spaven, 'Kipochi launches M-Pesa Integrated Bitcoin Wallet in Africa,' *CoinDesk* (19 July 2013).
32 Jon Matonis, 'Bitcoin's Promise in Argentina,' *Forbes* (27 April 2013).
33 Camila Russo, 'Bitcoin Dreams Endure to Savers Crushed by CPI: Argentina Credit,' *Bloomberg* (16 April 2013).
34 Georgia Wells, 'Bitcoin downloads surge in Argentina,' *The Wall Street Journal Money Beat* (17 July 2013).
35 Jerry Brito, 'The Top 3 Things I Learned at the Bitcoin Conference,' *Reason* (20 May 2013).
36 Mike Hearn, 'Bitcoin 2012 London: Mike Hearn,' YouTube video, 28:19, posted by 'QueuePolitely' (27 September 2012), www.youtube.com/watch?v=mD4L7xDNCmA. Smart property is a concept to control ownership of an item through agreements made in the Bitcoin block chain. Smart property allows people to exchange ownership of a good or service once a condition is met using cryptography. Although smart property is still theoretical, the basic mechanisms are built into the Bitcoin protocol. See *Bitcoin wiki*, s.v., 'Smart Property,' https://en.bitcoin.it/wiki/Smart_Property.
37 J.R. Willett, 'The Second Bitcoin Whitepaper' (2013), https://sites.google.com/site/2ndbtcwpaper/2ndBitcoinWhitepaper.pdf.
38 Jeremy Kirk, 'Could the Bitcoin Network Be Used as an Ultrasecure Notary Service?' *ComputerWorld* (23 May 2013).
39 Jonathan Warren, 'Bitmessage: A Peer-to-Peer Message Authentication and Delivery System,' white paper (27 November 2012), https://bitmessage.org/bitmessage.pdf.
40 Ian Miers, et al. 'Zerocoin: Anonymous Distributed E-Cash from Bitcoin,' working paper (Johns Hopkins University Department of Computer Science, Baltimore, MD, 2013).
41 Timothy B. Lee, 'An Illustrated History of Bitcoin Crashes,' *Forbes* (11 April 2013).
42 Felix Salmon, 'The Bitcoin Bubble and the Future of Currency,' *Medium* (3 April 2013).
43 Maureen Farrell, 'Strategist Predicts End of Bitcoin,' *CNNMoney* (14 May 2013).
44 Adam Gurri, 'Bitcoins, Free Banking, and the Optional Clause,' *Ümlaut* (6 May 2013).
45 Jerry Brito, 'Why Bitcoin's Valuation Really Doesn't Matter,' *Technology Liberation Front* (5 April 2013).
46 Today, merchant service providers accept the risk presented by the volatility and nevertheless maintain low fees. It remains to be seen whether this model will be sustainable in the long run.
47 Most of the security challenges concern wallet services and bitcoin exchanges. The protocol itself has proven to be considerably resilient to hacking and security risks. Renowned security researcher Dan Kaminsky tried, but failed, to hack the Bitcoin protocol in 2011. See Dan Kaminsky, 'I Tried Hacking Bitcoin and I Failed,' *Business Insider* (12 April 2013).
48 Stephen Doherty, 'All Your Bitcoins Are Ours …' *Symantec Blog* (16 June 2011).
49 Devin Coldewey, '$250,000 Worth of Bitcoins Stolen in Net Heist,' *NBC News* (5 September 2012).
50 Meghan Kelly, 'Fool Me Once: Bitcoin Exchange Mt.Gox Falls after Third DDoS Attack This Month,' *VentureBeat* (21 April 2013).
51 *Wikipedia*, s.v. 'Deep Web,' http://en.wikipedia.org/wiki/Deep_Web.
52 Nicolas Christin, 'Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace,' *Carnegie Mellon CyLab Technical Reports: CMU-CyLab-12-018* (30 July 2012).
53 Jerry Brito, '*National Review* Gets Bitcoin Very Wrong,' *Technology Liberation Front* (20 June 2013).
54 Adrian Chen, 'The Underground Website Where You Can Buy Any Drug Imaginable,' *Gizmodo* (1 June 2011).
55 Brett Wolf, 'Senators Seek Crackdown on "Bitcoin" Currency,' *Reuters* (8 June 2011).
56 'Liberty Reserve Digital Money Service Forced Offline,' *BBC News—Technology* (27 May 2013).
57 Jeffrey Sparshott, 'Bitcoin exchange makes apparent move to play by U.S. money-laundering rules,' *The Wall Street Journal* (28 June 2013).