PIIE PETERSON INSTITUTE FOR INTERNATIONAL ECONOMICS

POLICY BRIEF

17-13 Do Digital Currencies Pose a Threat to Sovereign Currencies and Central Banks?

Daniel Heller

April 2017

Daniel Heller *is visiting fellow at the Peterson Institute for International Economics.* *He thanks Olivier Blanchard, William Cline, Veronica Garcia, Marcus Noland, Simon Johnson, Adam Posen, Paolo Tasca, Nicolas Véron, and Steven Weisman for their encouragement and comments.*

Recent advances in information technology have led to the emergence of an entirely new form of money typically referred to as *digital currencies*. A distinguishing feature of digital currencies is that they are not issued by central banks (like banknotes) or commercial banks (like deposit accounts). Digital currencies are issued by a software protocol. They are not a liability of any institution or individual, and they are not backed by a government. These properties of digital currencies make them akin to commodities like gold (CPMI 2015).

By far the best known and most widely used digital currency is bitcoin, launched in 2009 as a peer-to-peer payment system for online purchases (Nakamoto 2008). The bitcoin system is open 24 hours, seven days a week. It has more than 13 million registered users. About $20 billion worth of bitcoin are in circulation; every second upto 10 payments are made in bitcoin. Several electronic exchanges have been established on which bitcoin is exchanged against some of the major sovereign currencies.

Users own the bitcoin system and can change the rules and protocol only by consensus or a supermajority of 95 percent. This communitarian ownership model and the fact that payments in bitcoin can be easily made from one end of the globe to another have led many to believe and hope that bitcoin will one day replace sovereign currencies—and the central banks that issue them. In addition, some observers see bitcoin as the origin of a fundamental transformation of the financial system toward a more decentralized structure.

This Policy Brief addresses the question of whether digital currencies pose a threat to sovereign currencies and their central banks. The first section introduces a taxonomy of money and compares the features of bitcoin with other forms of money. The second section provides a nontechnical introduction to how bitcoin is created and how the system works.[1] The third section presents some monetary, transactional, and technical statistics on the bitcoin system. The next two sections address money laundering and security. The sixth section assesses whether bitcoin meets the criteria economists usually apply to currencies (medium of exchange, unit of account, and store of value). The last section summarizes the main conclusions.

CLASSIFICATION OF MONEY AND MONETARY INSTRUMENTS

Many forms of money exist today (figure 1).[2] They can be divided into physical and electronic money. Physical money includes beads as well as banknotes and metal coins (cash), usually issued by a central bank. Electronic money includes (noncash) deposits of financial institutions at the central bank (central bank deposits), deposits of households and firms with commercial banks (commercial bank money), and e-money. E-money includes the monetary value stored on a chip card, such as a prepaid credit card, or a hard drive as well as digital currencies. Digital currencies can be issued by a central entity or in a decentralized way by a computer system. They are not denominated in a sovereign currency. Bitcoin is an example of a decentralized digital currency.

A distinct feature of a decentralized digital currency is that the settlement of a payment obligation takes place on a peer-to-peer basis, without the intermediation of a trusted third party, such as an automated clearinghouse, commer-

1. For descriptions of the bitcoin system, see Badev and Chen (2014), Eyal (2015), and Vigna and Casey (2015).

2. For a similar categorization, see IMF (2016).

Figure 1 Taxonomy of money

<table>
<tr><th colspan="3">Physical</th><th colspan="4">Electronic</th></tr>
<tr><td></td><td colspan="3">Money in the traditional sense (denominated in a sovereign currency)</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Physical tokens (beads, shells); privately issued notes</td><td colspan="2">Central bank money</td><td rowspan="2">Commercial bank money</td><td colspan="2">E-money (broad sense)</td></tr>
<tr><td>Cash (notes and coins)</td><td>Central bank deposits</td><td rowspan="2">Legally recognized e-money (e-money in the narrow sense)</td><td colspan="2">Digital currencies</td></tr>
<tr><td></td><td></td><td></td><td>Centrally issued</td><td>Decentralized or automatic issuance</td></tr>
<tr><td colspan="3">Peer-to-peer settlement</td><td colspan="2">Centralized settlement (trusted third party)</td><td>Peer-to-peer settlement</td></tr>
</table>

Source: Based on CPMI (2015).

cial bank, or central bank. This property is very similar to banknotes and metal coins. In fact, bitcoin founder Nakamoto (2008) claims that bitcoin transactions are as secure as settlement in bank notes and that no other "mechanism exists to make payments over a communications channel without a trusted third party."[3]

History of Paper Money and Deposits

The history of money is full of examples in which the private sector came up with innovations that successfully challenged the monopoly of the sovereign to issue money. The first paper money was issued by the private sector in the 10th century in China. It competed with copper coins of uncertain quality (Bernholz 2003). It took until the 17th century before paper money was introduced in Europe (Sweden), although private deposit accounts appeared in Northern Italy in the 12th century (Ferguson 2008). Many city-states and dukes had been issuing their own coins, often of poor and unknown quality, hindering trade and commerce in the region. Against this background, private money exchangers introduced deposit accounts against high-quality coins. These deposit accounts were then used to transfer money between clients as book entries, without the use of coins. Modern banking was born when these money exchangers also started providing loans.

In the 19th century, sovereign states frequently delegated the issuance of paper money to private-sector banks. In Canada, for instance, private banks began issuing notes in 1817—almost 50 years before provincial governments did so. The simultaneous circulation of private and government notes ended in Canada only in 1950 (Fung, Hendry, and Weber 2017). In the United States, only private banks issued bank notes until 1913, when the Federal Reserve System was established. Both private- and public-sector-issued notes were in circulation for about 20 years thereafter (Weber 2015).

Modern Electronic Payment and Settlement

Modern electronic payment and settlement processes are highly centralized and intermediated. Central banks issue sovereign currencies (fiat money) and provide settlement services, commercial banks specialize in taking deposits and making loans, central securities depositories electronically store securities, and central counterparties clear derivatives. This specialization is based on the existence of increasing returns to scale (Baltensperger 1980, Diamond 1984). An essential element for these intermediaries to assume their role and enhance the efficiency of the economy is that market participants trust them.

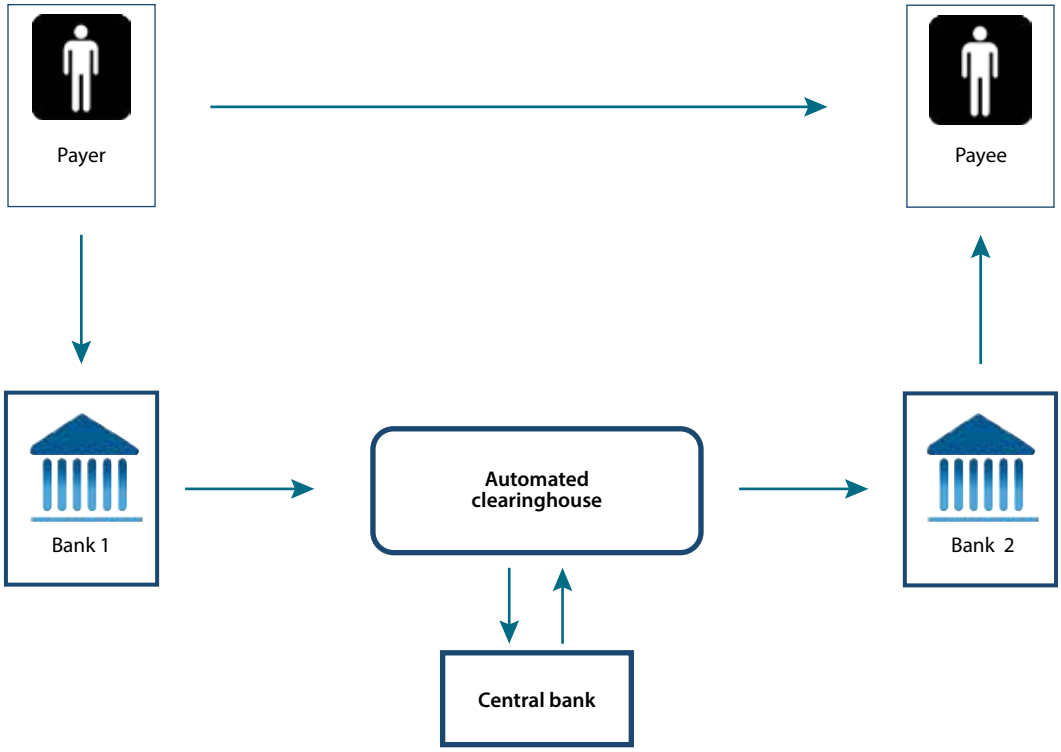
Figure 2 reveals the high degree of centralization and intermediation using the example of a recurring retail payment from a household (payer) to a merchant (payee). The payer sends a payment instruction to the bank where she holds a checking account (Bank 1). The bank authenticates the payer and checks whether she has enough funds in her account. If she does, the bank forwards the payment instruction to an automated clearinghouse, which aggregates and nets out the payment amounts it receives from participating banks.

At certain intervals—for instance, every two hours—the automated clearinghouse sends payment instructions for the net positions to the central bank for settlement (transfer of deposit balances). As soon as the central bank transfers the net debit balances of the participating bank, the payment is final (unconditional and irrevocable). Bank 2 then credits the account of the payee. The entire payment process usually lasts several hours, although it can take more than a day, depending on the payments infrastructure of a country.[4] For

3. The identity of Satoshi Nakamoto is a mystery as it is still not known which person or group hides behind this pseudoym. After frequent forum posts and exchanges of emails, Nakamoto vanished in 2011, saying that he or she "moved on to other things."

4. The process for large-value interbank payments is much faster. Interbank payments typically settle without delay and are immediately final. The processing speed of retail payments has increased markedly in recent years. In many countries retail payment systems provide immediate real-time finality (CPMI 2016a; Bech, Shimizu, and Wong 2017).

Figure 2 Traditional payment process with intermediation



cross-border payments, the process is even more complex and more time consuming, as it is likely to involve correspondent banks.

TRANSACTIONS IN THE BITCOIN SYSTEM

Payments in bitcoin take place without the intermediation of automated clearinghouses, commercial banks, or central banks. Figure 3 shows the settlement process. The process is initiated by the payer, who sends a payment instruction over the internet to participants in the bitcoin network, including the payee and "miners," who act as validators and record-keepers of all bitcoin transactions.

Transaction data are stored in electronic files called blocks. The entire history of transactions is recorded in a long sequence of blocks called a *blockchain*.[5] Every 10 minutes the bitcoin network packages the latest transactions into a new electronic block.[6] The right to create the next block that is added to the blockchain is assigned to only one miner. In order to determine which miner this will be, the system poses a complex cryptographic puzzle to the community of miners. The miner who is the first to solve this puzzle wins the right to generate the next block. A miner can influence her chances of being the first to solve this puzzle by increasing the amount of computational power she dedicates to the task. The winning miner receives a reward in the form of newly issued bitcoin, known as the *coinbase*. The market for mining is open to anyone with the required hardware and software. In recent years, high-speed processors have been developed especially for bitcoin mining. They can be purchased on the internet. The software is open source and can be downloaded for free.

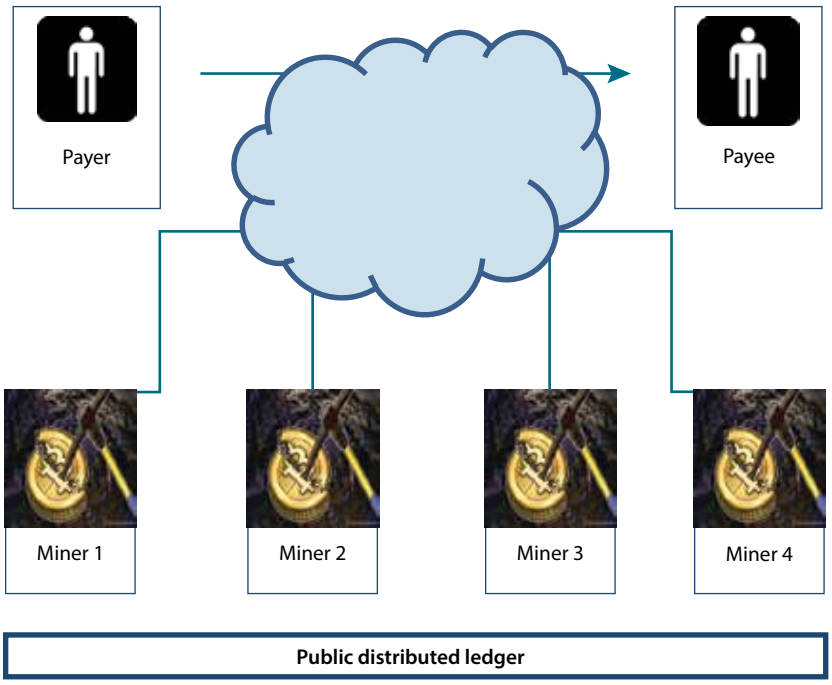
Vigna and Casey (2015) compare this competition among miners with participation in a lottery. The more tickets people buy, the higher their chances of winning. But no participant can ever be certain to win. Because new blocks are created every 10 minutes, miners can estimate their probability of wining and determine the expected value of winning a reward.

Once the system has determined the winning miner, the other miners assess whether the block propagated by the winner is valid. This validation is necessary to prevent fraud in the network. In particular, it is a means to prevent the same bitcoin (or a fraction of it) from being spent twice (so-called double spending). Miners provide trust in the system by serving as independent validators or notaries. If the majority

5. A blockchain is a type of distributed ledger, comprising unchangeable, digitally recorded data in packages or blocks. Each block is then "chained" to the next block, using a cryptographic signature.

6. Since the inception of the bitcoin system in 2009, more than 460,000 blocks have been created.

Figure 3 Peer-to-peer settlement in bitcoin



of miners (in terms of their computational power) agree that the transactions in a block are valid, identical copies of the block are distributed through the network, where they are stored in a decentralized way on the miners' computers.

It takes about an hour until the transactions of a block are considered final. This delay makes bitcoin unsuitable for large-value interbank payments, as the current real-time gross settlement systems eliminate settlement risk by providing immediate finality of payments.

Bitcoin is the first modern application of "distributed ledger" technology, a collective term that contains several components, including the use of blockchains, public key infrastructure, cryptographic signing, and hash functions, among others.[7] While the particular components required vary according to the problem being solved, in all distributed ledger applications a record of transactions or other data is stored across multiple entities (i.e., it is distributed) in a network, making the distributed ledger "a common, authoritative prime record—a single source of truth—to which multiple entities can refer and with which they can securely interact" (Digital Assets Holdings 2016).[8]

SOME STATISTICS ON BITCOIN

Every 10 minutes the bitcoin system issues new bitcoin as compensation for miners. The rate of bitcoin issuance is predetermined and exogenously given. Bitcoin "printing" decelerates over time, as issuance is cut by half every four years. The next time the block mining reward halves is in June 2020. The bitcoin reward per block will then decrease from 12.5 to 6.25. With the current block reward, the number of bitcoin in circulation increases by about 2 percent a year.

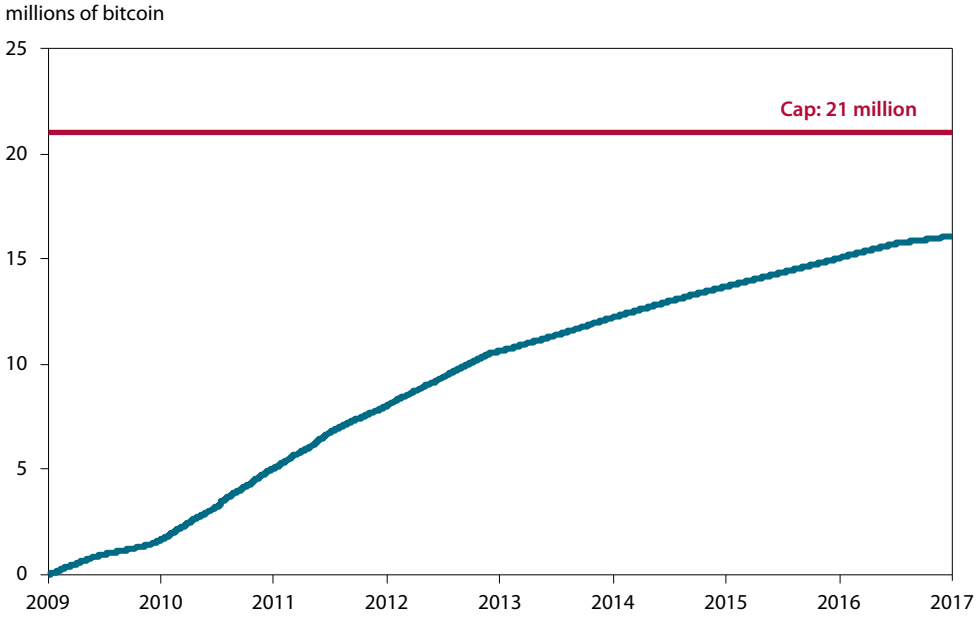
In addition, there is an upper limit of BTC21 million that can ever be generated. More than half of the lifetime supply of bitcoin was created in the first six years (figure 4). So far about 75 percent of the maximum number of bitcoin has been issued; about BTC5 million is left. The ceiling will be reached within 20 years.

In its early years, bitcoin traded below $1 (figure 5). In December 2013, the value of the bitcoin reached $1,150. In 2014 it depreciated to a low of $200. In March 2017 it appreciated to an all-time peak of $1,285. Since then, the price has oscillated between $940 and $1,200. According to the International Monetary Fund (IMF 2016), the price of bitcoin is more volatile than any other significant asset.

7. A hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of fixed size that is designed to be a one-way function (i.e., a function that is infeasible to invert).

8. In addition to bitcoin, distributed ledger technology can be used for smart or automated contracts—computerized protocols that automatically execute transactional events based on the terms of the contract. Issuance, ownership records, and coupon payments of financial assets like bonds could be administrated by smart contracts. For examples of applications of distributed ledger technology in payments, clearing, and settlement, see Federal Reserve Board (2016).

Figure 4 Volume of bitcoin in circulation, January 2009–February 2017

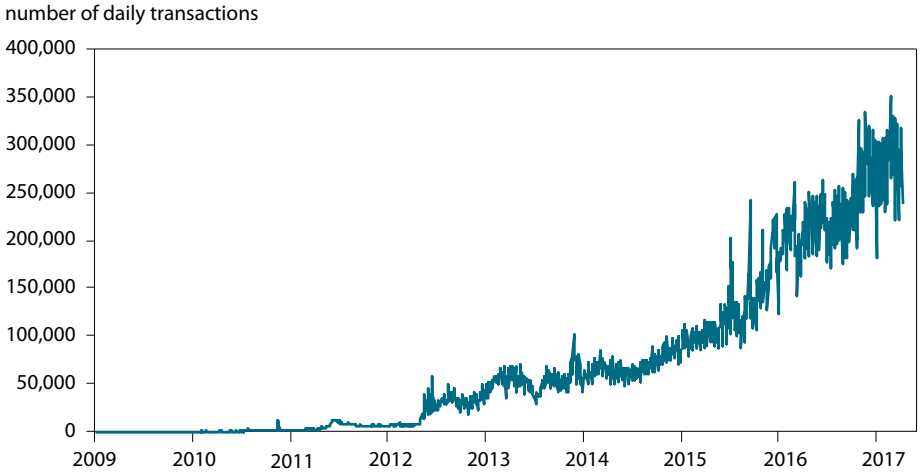


Source: blockchain.info.

Figure 5 Price of bitcoin in dollars, January 2009–April 2017

Source: blockchain.info.

Figure 6 Number of bitcoin transactions per day, January 2009–April 2017



Source: blockchain.info.

The total market value of bitcoin currently stands at $20 billion—about 35 percent of the value of banknotes in circulation in Australia, Brazil, Canada, and Hong Kong; 25 percent of the value of banknotes in Switzerland; and about 1 percent of the value of banknotes in the euro area and United States.[9] It is 2.3 times higher than the value of banknotes circulated by the Swedish Riksbank.

The number of transactions in bitcoin has steadily increased to about 350,000 per day (4 per second) (figure 6). As the maximum block size in bitcoin is 1 MB, the number of transactions that can be processed is limited. In fact, the system's capacity is fully exhausted and "faces a significant scalability barrier" (Eyal et al. 2015). Several short-term measures have been implemented. Once the block limit is reached, transactions are moved into a queue, from which they are released when there is space in a block. Processing is faster for transactions for which a transaction fee is charged.

In light of these binding capacity constraints, third-party custodians have emerged that settle bitcoin transactions internally (off-chain), in a manner akin to traditional clearinghouses (no data are available on the number of transactions processed off-chain). The bitcoin community is discussing and developing measures to increase the processing capacity in a sustainable way, including increasing the block size and introducing high-volume off-chain clearing for micropayments.

Figure 7 shows the trading volumes of bitcoin in various currencies. Until 2013 bitcoin was mostly traded against the dollar. A sudden surge of interest in bitcoin among Chinese investors led to a large shift in the trading activity. Since 2014, more than 95 percent of bitcoin trading has been against the Chinese renminbi. As the share of dollars (and all other currencies except the renminbi) was small until 2017, it is safe to conclude that bitcoin was not used to circumvent capital restrictions in China.

Trading against the renminbi collapsed in January 2017, after Chinese exchanges stopped margin trading and introduced trading fees. The dollar now accounts for about 50 percent of trading, followed by the renminbi, the euro, and the Japanese yen (each with a share of 12 to 14 percent).

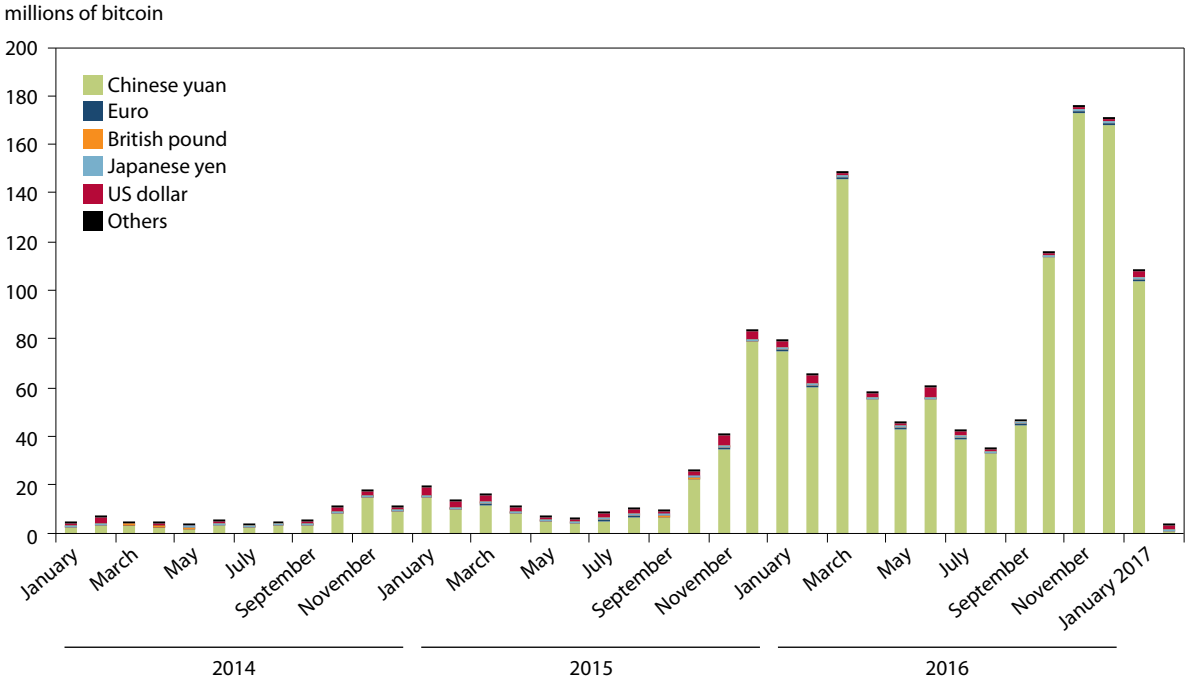
Since the halving of block rewards in July 2016, the costs per transactions have fluctuated between $4 and $10—about 0.5 to 1.5 percent of the value of the transaction. Bitcoin payments may thus not be less expensive than many conventional retail payments, including remittances.[10]

The collective mining efforts have increased rapidly in the past few years (figure 8), and the process has become industrialized, with the establishment of large commercial mining farms. Technological progress will lead to an increase in mining efforts over time. It has become standard practice for miners to form pools in which all members share the reward after one of them is selected to create the next block. Because mining consumes a great deal of electricity, miners typically locate where electricity is inexpensive, in particular in China, where about 60 percent of mining rewards are collected.

9. The latest data for bank notes in circulation are for the end of 2015 (CPMI 2016b).

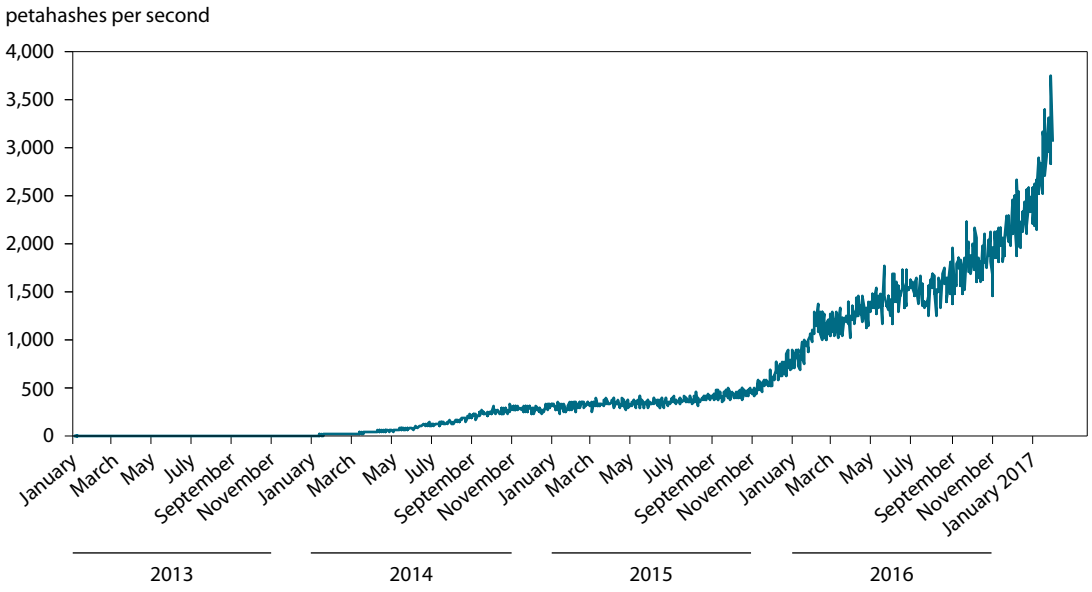
10. One of the larger exchanges charges a minimum fee of $15 for deposits and withdrawals of fiat currency. For a remittance of $200, this fee represents 15 percent. According to the World Bank's remittance prices database, the global average cost of sending a remittance of $200 is 7.4 percent.

Figure 7 Volume of bitcoin trading, by currency, January 2014–February 2017



Source: data.bitcoinity.org.

Figure 8 Computational power devoted to bitcoin mining, January 2013–February 2017



Note: 1 petahash per second is 1 quadrillion hashes (specific mathematical operations on a computer) per second.
Source: data.bitcoinity.org.

DOES BITCOIN FACILITATE MONEY LAUNDERING AND TERRORIST FINANCING?

Convertible digital currencies like bitcoin are potentially vulnerable to money laundering and terrorist financing (FATF 2014). Compared with noncash transactions in the regulated financial system, they provide much greater anonymity. Even though the bitcoin ledger is public, the payment instructions contain only the alphanumeric identifiers of the counterparties, but not their names (so-called pseudonymity). [11]

In 2015 the Financial Action Task Force (FATF), an intergovernmental body developing and promoting policies to combat money laundering and terrorist financing, developed international guidance. It states that measures regarding

As long as central banks continue to pursue stability-oriented monetary policies, they will have little reason to fear that the bitcoin system will replace them.

anti–money laundering (AML) and combating the financing of terrorism (CFT) need to be applied at the intersection between a digital currency and the regulated financial system. Digital currency exchanges have to ensure that the recommendations on AML/CFT are met. FATF (2015) provides guidance on how these exchanges can implement specific recommendations. The AML/CFT provisions are not applicable to the digital currency itself but to the infrastructures that convert it into sovereign currency.

The tax authorities view bitcoin as an asset that needs to be declared. In November 2016 the Internal Revenue Service was authorized to seek information about US taxpayers who conducted transactions in bitcoin and other digital currencies.[12]

11. The pseudonymity of the bitcoin system does not mean users can never be identified. In September 2013 the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a website selling illegal products, including weapons and drugs, on the dark net. In the course of the crackdown on Silk Road, US authorities seized more than BTC600,000 (about $16 million at the time). The prime suspect behind the site was sentenced to life in prison without parole.

12. See Department of Justice, "Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency," news release, November 30, 2016, www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used.

HOW SECURE IS BITCOIN?

Three features of distributed systems improve their security. First, they are fault tolerant, because they rely on many separate components. Second, they are attack resistant, because they are more expensive to attack and manipulate because of the absence of a central computer. Third, they are collusion resistant, because it is much harder for participants to collude and act in ways that benefit them at the expense of other participants (Buterin 2017).

These benefits notwithstanding, several potential security weaknesses have been identified. The first is typically referred to as a "51 percent attack." Bitcoin transactions are validated if the majority of miners agree that they are valid. It is possible for 51 percent (in terms of hash rates) of miners/validators to launch a coordinated attack. Given the relatively high past and current concentration in mining, the risk of such an attack exists (Garratt and Hayes 2014, Buterin 2017).

The second security risk is related to the fact that bitcoin is a bearer instrument, like cash or gold. Whoever holds the private (digital) key associated with a bitcoin wallet can spend its content. If an owner loses the key, he or she irrevocably loses access to the asset.

The risk of theft of private keys is not just hypothetical. Mt. Gox, a Tokyo-based bitcoin exchange that also stored private keys, was hacked twice in three years; about BTC850,000 ($450 million at the time) were stolen. Since then, the security of bitcoin wallets has been improved, for instance, by using two-factor authentication or multiple signatures. Nonetheless, a heist of BTC120,000 ($67 million at the time) occurred at the Bitfinex exchange in 2016.

HOW WELL DOES BITCOIN FUNCTION AS A CURRENCY?

Successful currencies meet three criteria: (1) they are in widespread use as medium of exchange, (2) they serve as unit of account, and (3) they are a stable store of value. Most sovereign currencies fully meet all three criteria. What about bitcoin?

Users are willing to accept a medium of exchange as payment only if they are confident that enough other users will be willing to accept it (Lo and Wang 2014). This willingness increases exponentially with the number of users in the network.

Various indicators, such as the number and value of transactions and the number of users and merchants, can be used to assess how widespread a currency is as a medium of exchange. Despite the growing number of transactions (see figure 6), bitcoin still plays a relatively minor role as a medium of exchange. For instance, the value of bitcoin

transactions is less than 1 percent of the value of card payments in China (CPMI 2016b). In terms of the aggregate value of transactions, the bitcoin network is about the size of Western Union (Tasca 2016).[13] Only 9,000 merchants accept bitcoin—a fraction of the 37 million outlets that accept Visa and MasterCard.[14] Virtually no Chinese merchants accept bitcoin, despite the high concentration of mining and trading in China.[15]

The majority of bitcoin are stored, not used to pay for goods and services (Tasca 2015; Baur, Hong, and Lee 2016). Bitcoin is thus held largely for speculative purposes, not as a medium of exchange.[16]

As a unit of account, a currency serves as the *numéraire* in which economic goods and activities are measured. It is used to indicate the prices in supermarkets and restaurants as well as wages in labor contracts. Here, too, bitcoin has gained little traction. As a unit of account, bitcoin is used only sporadically, in crowdfunding for blockchain startups or at gambling sites, for example.

A consumer price index based on exchange rate movements of bitcoin would have fallen in 2013 and soared in 2014 (see figure 5). More recently, it would have plummeted. If bitcoin had been the unit of account, the effects on the economy would have been disastrous.

A currency should be a good store of value. In order to be a good store of value, a currency needs to be stable. Bitcoin is far from stable. As its price fluctuates wildly, it is a high-risk asset.

Finally, since the supply of bitcoin is capped at the 21 million coins, an economy under a bitcoin currency standard would eventually operate in a deflationary environment (Tasca 2016). An imitator currency with a superior supply mechanism would soon arrive and replace bitcoin. The price of bitcoin would collapse leading to high inflation (Rogoff 2016).

CONCLUSIONS

Bitcoin is the first digital currency to have received widespread recognition and interest from users, developers, investors, central banks, and regulators, largely because of its distributed ledger technology, which allows it to provide relatively low-cost peer-to-peer transfers of money. As a medium of exchange bitcoin is still small compared with traditional channels, however, and it is held largely for speculation rather than transactions.

It is conceivable that bitcoin will find a niche role as a medium of exchange. But its lack of a mechanism for dampening the price effect of an increase in demand or reducing supply in case of a demand slump means that adopting bitcoin as a currency would be like reverting to a currency based on gold coins. As long as central banks continue to pursue stability-oriented monetary policies, they will have little reason to fear that the bitcoin system will replace them.

13. On an average day in 2015, Western Union transferred about $400 million; in January 2017 the bitcoin network settled about $300 million a day.

14. See www.fintech.finance.

15. See www.coinmap.org.

16. Online gambling accounts for many low-value transactions (Badev and Chen 2014).

REFERENCES

Badev, Anton, and Matthew Chen. 2014. *Bitcoin: Technical Background and Data Analysis*. Finance and Economics Discussion Series 2014-104. Washington: Federal Reserve Board.

Baltensperger, Ernst. 1980. Alternative Approaches to the Theory of the Banking Firm. *Journal of Monetary Economics* 6, no. 1: 1–37.

Baur, Dirk, Kihoon Hong, and Adrian Lee. 2016. *Virtual Currencies: Media of Exchange or Speculative Asset*. Working Paper 2014-007. London: SWIFT Institute.

Bech, Morten, Yuuki Shimizu, and Paul Wong. 2017. The Quest for Speed in Payments. *Quarterly Review* (March). Basel: Bank for International Settlements.

Bernholz, Peter. 2003. *Monetary Regimes and Inflation*. Cheltenham: Edward Elgar.

Buterin, Vitalik. 2017. *The Meaning of Decentralization.* Available at https://medium.com/@VitalikButerin/.

CPMI (Committee Payments and Market Infrastructures). 2015. *Digital Currencies*. Basel: Bank for International Settlements.

CPMI (Committee Payments and Market Infrastructures). 2016a. *Fast Payments: Enhancing the Speed and Availability of Retail Payments*. Basel: Bank for International Settlements.

CPMI (Committee Payments and Market Infrastructures). 2016b. *Statistics on Payments, Clearing and Settlement in CPMI Countries*. Basel: Bank for International Settlements.

Diamond, Douglas W. 1984. Financial Intermediation and Delegated Monitoring. *Review of Economic Studies* 51, no. 3: 393–414.

Digital Asset Holdings. 2016. *The Digital Asset Platform*. Nontechnical White Paper. Available at http://hub.digitalasset.com/hubfs/Documents/Digital%20Asset%20Platform%20-%20Non-technical%20White%20Paper.pdf?submissionGuid=19b3704a-4934-4661-9920-2270d03db39.

Eyal, Ittay. 2015. Bitcoin: *The Miner's Dilemma*. Working Paper 2014-006. London: SWIFT Institute.

Eyal, Ittay, Adem Efe Gencer, Emin Gün Sirer, and Robbert van Renesse. 2015. *Bitcoin-NG: A Scalable Blockchain Protocol*. Working Paper. Ithaca, NY: Cornell University. Available at https://arxiv.org/abs/1510.02037.

FATF (Financial Action Task Force). 2014. *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. Available at www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

FATF (Financial Action Task Force). 2015. *Guidance for a Risk-Based Approach: Virtual Currencies.* Available at www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

Federal Reserve Board. 2016. *Distributed Ledger Technology in Payments, Clearing, and Settlement*. Finance and Economics Discussion Series 2016-095. Washington

Ferguson, Niall. 2008. *The Ascent of Money*. London: Allen Lane.

Fung, Ben, Scott Hendry, and Warren Weber. 2017. *Canadian Bank Notes and Dominion Notes: Lessons for Digital Currencies*. Staff Working Paper 2017-5. Ottawa: Bank of Canada.

Garratt, Rod, and Rosa Hayes. 2014. *How Likely Is a 51 Percent Attack?* Liberty Street Economics. New York: Federal Reserve Bank of New York.

IMF (International Monetary Fund). 2016. *Virtual Currencies and Beyond: Initial Considerations*. Staff Discussion Note 16/3. Washington.

Lo, Stefanie, and J. Christina Wang. 2014. *Bitcoin as Money?* Current Policy Perspectives 14-4. Boston: Federal Reserve Bank of Boston.

Nakamoto, Satoshi. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at https://bitcoin.org/bitcoin.pdf.

Rogoff, Kenneth. 2016. *The Curse of Cash*. Princeton and Oxford: Princeton University Press.

Tasca, Paolo. 2015. *Digital Currencies: Principles, Trends, Opportunities, and Risks*. ECUREX Research Working Paper. Available at https://ssrn.com/abstract=2657598.

Tasca, Paolo. 2016. The Dual Nature of Bitcoin as Payment Network and Money. In *Cash on Trial*, ed. Christian Beer, Ernest Gnan, and Urs W. Birchler. Proceedings of the SUERF (Société Universitaire Européenne de Recherches Financières) Conference. Available at www.suerf.org/docx/SUERF_Conference_Proceedings_2016_1.pdf.

Vigna, Paul, and Michael J. Casey. 2015. *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. New York: St. Martin's Press

Weber, Warren. 2015. *Government and Private E-Money-Like Systems: Federal Reserve Notes and National Bank Notes*. Working Paper 2015-18. Ottawa: Bank of Canada.