

Yermack, David

Article

The potential of digital currency and blockchains

NBER Reporter

Provided in Cooperation with:

National Bureau of Economic Research (NBER), Cambridge, Mass.

Suggested Citation: Yermack, David (2018) : The potential of digital currency and blockchains, NBER Reporter, National Bureau of Economic Research (NBER), Cambridge, MA, Iss. 1, pp. 14-17

This Version is available at:

<http://hdl.handle.net/10419/178763>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

The Potential of Digital Currency and Blockchains

David Yermack

Digital currencies such as bitcoin and the underlying blockchain technology are among the most exciting recent innovations in finance. During 2017, surging interest in cryptocurrencies drove their total market value above \$600 billion, an increase of more than 700 percent for the year, and major corporations and governments launched blockchain projects in diverse areas such as shipping and logistics, electric power distribution, and real estate title registration. Blockchain refers to a series of records, typically holding data such as financial transactions, protected by cryptographic tools and arranged sequentially, such that any attempt to change a prior entry throws off all entries after that point in the chain. This property makes blockchain ledgers resistant to tampering and provides much greater security than conventional double-entry bookkeeping.

In a series of papers, I have explored both the potential and the limitations of this emerging technology. Due to the libertarian free-market philosophy inherent in the stateless design of digital currencies,

the topic evokes neoclassical ideas from the institutional economics of the 19th and 20th centuries, reviving ideas behind such movements as the Jacksonian era of Free Banking, in which private currencies played a much larger role in the economy than government fiat currencies, and the 1930s Chicago Plan for a narrow banking system with a 100 percent reserve requirement.

This article summarizes my digital currency work in three areas: the suitability of bitcoin as a currency, how blockchain technology may impact central banking, and the potential for blockchain technology to disrupt the equity markets and the dynamics of corporate governance. This work draws upon finance and banking as well as law and economics, cryptography, macroeconomics, and other fields.

Bitcoin as a Currency

Bitcoin is described by its anonymous creator as “a peer-to-peer electronic cash system,” a stateless payment system that

does not rely upon a trusted intermediary such as a central bank or a mint.¹ Its money supply is regulated by transparent, open source computer code, and transactions are validated by a system of double-key cryptography and are entered into a decentralized, widely distributed ledger through a periodic competition known as mining. Since the first use of bitcoin to pay for two pizzas in May 2011, a gradually increasing network of merchants has begun accepting bitcoin as payment for goods and services in the real economy.

While its design is indisputably novel and clever, a natural question to investigate is how well bitcoin fulfills the classical roles of money. I began to explore that question in late 2013, when the value of a bitcoin soared above \$1,000 during an episode of feverish investor speculation² and concluded that bitcoin does not behave much like a currency, according to the criteria widely used by economists. Instead, bitcoin resembles a speculative investment similar to the internet stocks of the late 1990s.



David Yermack is a research associate of the NBER's Law and Economics Program, the Albert Fingerhut Professor of Finance and Business Transformation at New York University's Stern School of Business, and chair of the Stern School's finance department. He has been a member of the NYU faculty since 1994. He is also an adjunct professor of law and director of the law school's Pollack Center for Law and Business.

In 2014 Yermack began teaching the full semester course on Digital Currency and Blockchains at NYU with his law school colleague Geoffrey Miller. The course was the first in the world on this topic taught at a major research university, and it now enrolls more than 200 students annually.

In addition to his recent research on blockchains and digital currencies, Yermack has published some of the most cited papers in the fields of executive compensation and corporate governance. He has written papers on such diverse topics as options in baseball players' contracts, incentive compensation for clergymen, tobacco litigation, fraudulent charitable contributions, CEOs' mansions, and the fashion industry.

Yermack has been awarded five degrees from Harvard University: AB in 1995, MBA in 1991, JD in 1991, AM in 1993, and PhD in 1994. He has been a visiting professor at 12 international universities and a visiting scholar at the Federal Reserve Banks of New York and Philadelphia. He has given invited research seminars at more than 100 universities and institutes worldwide.

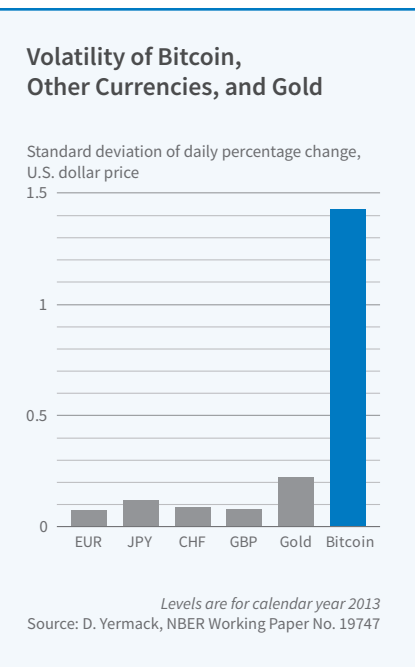


Figure 1

Money is typically defined by economists as having three attributes: It serves as a medium of exchange, a unit of account, and a store of value. Bitcoin somewhat meets the first of these criteria, because a growing number of merchants, especially in online markets, appear willing to accept it as a form of payment. However, the worldwide commercial use of bitcoin remains minuscule, indicating that few people use it widely as a medium of exchange, and those who do can be encumbered by security precautions and long delays needed to verify transactions.

Bitcoin also performs poorly as a unit of account, because merchants must quote the prices of common retail goods out to five or six decimal places with leading zeros, a practice rarely seen in consumer marketing and that is likely to confuse both sellers and buyers. In addition, bitcoin exhibits very high time series volatility, and it trades for different prices on different exchanges without the possibility of arbitrage. These characteristics undermine bitcoin's usefulness as a unit of account. Figure 1 shows the volatility of the daily bitcoin-U.S. dollar exchange rate in 2013, compared with that of other major currencies and gold. Bitcoin's volatility is an order of magni-

tude larger than that of other currencies and much higher than even the volatilities of risky growth stocks, which tend to top out in the range between 0.50 and 1.00. Many bitcoin enthusiasts have argued that its volatility should decline to more normal levels as the currency becomes more widely used, but Figure 2, which displays the volatility measured in a 120-day moving average over the six-year period 2012–17, shows that this has not occurred. Instead, bitcoin's volatility has gyrated; by late 2017, it had spiked to a level not seen since four years earlier.

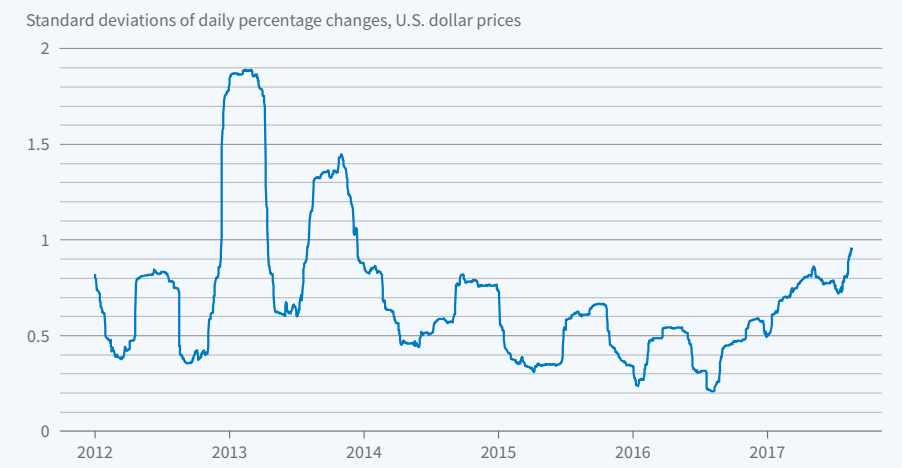
As a store of value, bitcoin faces great challenges due to rampant hacking attacks, thefts, and other security-related problems. Bitcoin's daily exchange rate with the U.S. dollar exhibits virtually zero correlation with the dollar's exchange rates against other prominent currencies such as the euro, yen, Swiss franc, and British pound, and also against gold. Because bitcoin's value is almost completely untethered from that of other assets, it is not a useful tool for risk management.

Bitcoin also lacks additional characteristics usually associated with currencies. It cannot be deposited in a bank, and instead must be possessed through a system of “digital wallets” that have proved both costly to maintain and vulnerable to

predators. No form of insurance has been developed for owners of bitcoin comparable to the deposit insurance relied on by bank customers in most economies. No lenders use bitcoin as the unit of account for standard consumer finance credit, auto loans, and mortgages, and to date no credit or debit cards have been denominated in bitcoin. Bitcoin cannot be sold short, and financial derivatives such as forward contracts and swaps that are routine for other currencies have not existed for bitcoin until very recently, when the major Chicago commodities exchanges began listing bitcoin futures in December 2017. A major price decline began very shortly after the inception of futures trading permitted speculators to bet for the first time against its further appreciation.

However, concluding that bitcoin does not meet standard criteria as a form of money implicitly raises the question of whether we have the right definition of money. An interesting alternative — “money is memory” — has been proposed in a provocative paper by Narayana R. Kocherlakota.³ This work, which predates the launch of bitcoin by more than a decade, follows a logic quite similar to the blockchain distributed ledger that underlies bitcoin and other digital currencies.

Volatility of Bitcoin, 120-Day Moving Average



Source: Researcher's calculations using data from Bitcoincharts.com

Figure 2

Central Bank Digital Currency

Although bitcoin and other digital currencies were created to bypass the control of central banks, the possibility of a central bank withdrawing its bills and notes from circulation and replacing them with its own blockchain-based digital currency has become an appealing topic of debate among monetary economists, and many central banks are openly investigating this possibility. Max Raskin and I review the most widely circulated proposals of this type and evaluate their potential costs and benefits.⁴

Most central bank digital currency proposals are a variant of the “Fedcoin” scheme advanced by a commentator in 2014.⁵ The Fedcoin ideas have been taken up and discussed in policy papers by top officials of the Bank of England, among others. Under the Fedcoin proposal, citizens and businesses would be permitted to open accounts at the central bank itself, rather than depositing their funds in commercial banks as is done today. Central bank digital accounts could initially be funded by permitting depositors to convert existing currency, presumably at a one-to-one rate, and the new digital currency would reside on a blockchain operated by the central bank. When depositors wished to spend their digital currency, they would convey it over the central bank’s blockchain to the account of another party.

By concentrating deposits in the central bank, Fedcoin schemes would implicitly end the practice of fractional reserve banking, “narrowing” the banking system so that depositors dealt directly with the central bank rather than with intermediary private banks. In many ways, Fedcoin represents a revival of the 1933 Chicago Plan, a widely discussed academic proposal to end fractional reserve banking in order to restore public confidence during the Great Depression.⁶

Monetary policy would become much easier for the central bank to implement under a digital currency sys-

tem. The bank could commit to an algorithmic monetary policy and control it precisely. Negative interest rates could be paid to depositors, who would not have the option of holding physical cash to defeat such a policy. The concept of open market operations would be superseded by direct manipulation of customer balances, which could be targeted finely toward certain geographical regions or distinct demographic or economic clienteles of depositors.

The implications of these innovations could be vast. The central bank would not be vulnerable to runs, and governments could stop providing deposit insurance and occasional bailouts as the lender of last resort to inadequately funded commercial banks. Commercial banks would no longer have to engage in “maturity transformation,” under which they raise funds from short-term demand deposits and lend them out in long-term mortgages and other loans, and they would presumably recapitalize themselves with long-term debt and equity securities. Risk-shifting and other moral hazard problems on the part of banks, which now receive free deposit insurance from the government, might be eliminated.

In macroeconomics, the main advantages to a central bank of having its own digital currency would come from giving the government more control and understanding of the financial system. Such control could facilitate policy intervention in response to the business cycle while also ensuring better individual compliance with tax collection and anti-money laundering statutes.

Blockchains and Corporate Finance

Blockchains appear to have great potential in corporate finance.⁷ In addition to virtual currencies, blockchains can also hold debt securities and financial derivatives, which can be executed autonomously as “smart contracts” — computer code written to execute the reciprocal promises of two par-

ties when agreed-upon contingencies are met. Companies could issue shares on a blockchain in several forms. A firm could operate and update its own private blockchain and sell shares directly to investors, who could then trade them on the same platform. A firm could also create a decentralized public blockchain similar to bitcoin’s, in which shares were issued as rewards to miners for doing the work of updating the ledger. A third alternative would be to use an existing blockchain and attach shares of stock to coin transactions, using the so-called “colored coins” approach, which refers to bitcoin transactions that include a data field conveying information about other assets, such as the CUSIP number of a Treasury bond, that a seller wishes to transfer to a buyer. Finally, an existing stock exchange might improve its operations by adopting blockchain technology for post-trade clearing and settlement, as the Sydney-based ASX exchange is slated to do this year.

Using blockchains to record stock ownership could solve many longstanding problems related to companies’ inability to keep accurate and timely records of who owns their shares. Perhaps most importantly, blockchains could provide unprecedented transparency to allow investors to identify the ownership positions of debt and equity investors, including the firm’s managers, and overcome corruption on the part of regulators, exchanges, and listed companies. If a firm elected to keep its financial records on a blockchain, opportunities for earnings management and other accounting gimmicks could drop dramatically, and related party transactions would become more transparent.

The greater transparency of ownership associated with recording stock ownership on blockchains could provide firms with an early warning system when activists or raiders begin to buy shares. This would effectively make blockchains into a type of takeover defense, by undercutting the element of surprise and raising the cost for active investors to acquire shares.

On blockchains such as Ethereum

that have more advanced capabilities than bitcoin’s, self-executing smart contracts could replicate contingent claims such as stock options held by employees or warrants owned by outside investors.⁸ These smart contracts could extend into areas such as the pre-contracted resolution of financial distress. Further applications appear promising in areas such as shareholder voting, where a number of national stock exchanges already have conducted successful pilot projects.

¹ S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” unpublished manuscript, October 2008, available at <https://bitcoin.org/bitcoin.pdf>. [Return to Text](#)

² D. Yermack, “Is Bitcoin a Real Currency? An Economic Appraisal,” NBER Working Paper No. 19747, December 2013, revised April 2014, and in Handbook of Digital Currency, Amsterdam, Elsevier, 2015, pp. 31–44. [Return to Text](#)

³ N.R. Kocherlakota, “Money Is Memory,” Journal of Economic Theory, 81(2), August 1998, pp. 232–51. [Return to Text](#)

⁴ M. Raskin and D. Yermack, “Digital Currencies, Decentralized Ledgers, and the Future of Central Banking,” NBER Working Paper No. 22238, May 2016, and in Research Handbook of Central Banking, Cheltenham, England, Elgar Publishing, 2018. [Return to Text](#)

⁵ J.P. Koning, “Fedcoin,” jpkoning.blogspot.com/2014/10/fedcoin.html. [Return to Text](#)

⁶ I. Fisher, “100% Money and the Public Debt,” Economic Forum, April–June 1936, pp. 406–20. [Return to Text](#)

⁷ D. Yermack, “Corporate Governance and Blockchains,” NBER Working Paper No. 21802, December 2015, revised October 2016, and Review of Finance, 21(1), March 2017, pp. 7–31. [Return to Text](#)

⁸ D. Yermack, “Smart Contracts and Corporate Governance,” Proceedings of the 44th Economics Conference of the Oesterreichische Nationalbank, 2017, pp. 94–99. [Return to Text](#)