THIRD WAY

REPORT *Published January 16, 2015 • 14 minute read*

Bitcoin: Back to the Future

Jim Kessler
Senior Vice President for Policy
@ThirdWayKessler

John Vahey

Matthew Caulfield

Who is right about Bitcoin? Marc Andreessen, the founder of Netscape, or Paul Krugman, the Nobel Prize winning economist and columnist for *The New York Times*? Does Bitcoin offer "a sweeping vista of the future" or is it simply "evil"? At just $64 million in daily transactions, compared to over $33 billion in daily credit card charges, is Bitcoin even relevant or is it just a passing fad like Chia Pets or Beanie Babies? And, by the way, what the heck is a bitcoin anyways?

What is Bitcoin?

Bitcoin is virtual money, meaning it has no physical form. Nobody is walking around with a pocketful of bitcoins, little bitcoins don't fall between the cushions of your sofa, and there is no bank vault full of bitcoins. The European Central Bank defines virtual currency as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community." [1]

The Bitcoin system was developed in 2008 by Satoshi Nakamoto—a pseudonym that refers to the person (or group of people) responsible for creating Bitcoin. According to a

presentation by the Federal Reserve Bank of St. Louis, Bitcoin —with a capital 'B'—refers to the "set of rules" that govern the Bitcoin software program which allows individuals to send, receive, and verify transactions in units called bitcoins. [2] The smallest unit of bitcoin, known as a *satoshi,* is .00000001 BTC.

Anyone with a device that runs the Bitcoin software can transact in bitcoins and be part of Bitcoin's virtual community. To get started, you just need to download a Bitcoin wallet. This web-based tool enables you to send and receive bitcoins. Secondly, you will need to swap a currency, like U.S. dollars, for bitcoins or sell a product and accept bitcoins as payment.

Many international retailers accept bitcoin and there are approximately 285,000 bitcoin transactions per day totaling around $64 million. [3] Bitcoin's stats are dwarfed by the transaction sizes and volumes of Visa, MasterCard, and American Express which handle around 408 million transactions per day totaling over $33 billion. [4] At the beginning of 2013, the dollar price per bitcoin was around $14. By November 2013, the market price of Bitcoin rose to over $1200 per bitcoin. [5] But over 2014, Bitcoin's value dropped steadily. As of January 2015, Bitcoin hovers around the $200 mark. [6] If Bitcoin market volatility continues, Bitcoin's popularity as a medium for exchange could suffer.

Cracking the Bitcoin code: 4 things that make Bitcoin unique

1. Cuts out the Middleman

Bitcoin is a decentralized peer-to-peer network.

Bitcoin is described as decentralized for two reasons. First, Bitcoin is not associated with a government or a central bank. In the United States, the U.S. Mint mints coins and prints dollars. The Federal Reserve is in charge of monitoring the amount of private dollar creation, credit expansion, and

inflation. Bitcoin consists of an international community of virtual users who are not associated with a central government responsible for establishing or managing bitcoin.

Secondly, transactions are not verified by a single, centralized, or controlling third party. Most online, digital transactions require a middleman. For example, PayPal or a bank will verify that you own the funds you are sending to someone else. These intermediaries facilitate the transfer of funds and protect against "double spending"—attempts to defraud by spending the same virtual funds more than once.

Bitcoin is special because it solves the double spending problem without a centralized third party. Digital currencies are similar to electronic dollar bills. Double spending would be like scanning and emailing an electronic copy of a dollar bill as payment. Without a system for verifying that the sender is the legitimate owner of the dollar, the receiver of the payment would not know if the sender had sent that same $1 file to 100 other people. Users on Bitcoin's peer-to-peer network work collectively to verify that the bitcoins you are attempting to spend are, in fact, yours.

Cutting out the middleman reduces the fees associated with facilitating bitcoin transactions compared with more old school payment methods. Some transactions, especially larger transactions, may include only a small fee to incentivize miners to add transactions to the "block chain"—Bitcoin's universal transaction ledger. The average Bitcoin transaction will typically include a fee of .0001 BTC or around 6 cents. By contrast, fees for transactions using traditional payment systems are typically 2-3% of the transaction size. [7]

2. Speaking in Code

Bitcoin uses public key cryptography.

Bitcoin is the world's first crypto-currency. Cryptography is defined as "the process of writing or reading secret messages or codes." [8] Bitcoin users rely on the willingness and ability of other members of the Bitcoin community to expend time,

money, and energy to verify encrypted messages. This is done (as we note later in the paper) in exchange for new bitcoins.

All Bitcoin transactions begin with a public broadcast of an encrypted transaction message that includes the sender's "public key"—a unique 33-digit identity that is associated with their Bitcoin wallet. A public key is a lot like a checking account number—a digital code associated with one individual or account.

The message is signed with the sender's "private key." A private key is like your online banking password. If you want to pay a bill online, you sign into your account with your public key (account number) and your private key (secret password). In a Bitcoin transaction, the public broadcast of a transaction message includes the user's public key and is signed by the user's private key.

Messages include the quantity of bitcoins to be sent, the public key associated with the recipient's wallet, and how many bitcoins the sender wants to receive in change. This information is publicly displayed to every Bitcoin user. Other users are then able to decrypt the message and verify that the user making the payment is the rightful owner of the bitcoins.

Bitcoin affords users a certain level of privacy and security as you only need to share your public digital identity with other users. Some see this level of privacy as a happy medium between credit cards, which require a lot of personal information (e.g. name, address, zip code), and cash, which is entirely anonymous.

Each completed Bitcoin transaction becomes part of a universal public ledger—or "block chain." This means that the transaction history of each bitcoin is publicly available. Therefore, Bitcoin users are able to trace the ownership history of each individual bitcoin from its very first transaction to its most recent transaction.

3. No Printing Press

Bitcoins are “mined,” not made.

So, without an association with a government or a printing press, how are bitcoins ‘made'? The answer is the Bitcoin protocol is designed to have new bitcoins enter circulation as reward or “bounty” payments to Bitcoin “miners.” Miners receive these awards for verifying Bitcoin transactions and adding new blocks of transactions to the Bitcoin ledger.

Bitcoin miners, like coal miners or gold miners, spend time, money, and energy prospecting for valuable items. Bitcoin miners don’t use drills or shovels. They use powerful, cutting edge computers to verify transactions. In return, they extract valuable new bitcoins. The Bitcoin mining process involves competing to solve a difficult math puzzle assigned by the Bitcoin software. Solving the puzzle requires miners to devote significant computing power and electricity to performing calculations over and over until they are successful. The puzzle is designed to be very difficult and costly to solve. If the puzzle was easy to solve that would inevitably lead to fraud—users attempting to verify illegitimate transactions in order to receive the bounty payment.

When a miner solves the puzzle, they broadcast the solution along with the new block of transactions to the Bitcoin community. This is known as a “proof of work.” It proves that the miner devoted time and energy to solving the problem. The new block of transactions is only added to the ledger if a majority of Bitcoin users agree that the difficult numerical problem is solved and the proof of work is legitimate. Once a new block is added, the whole process starts again.

In order to incentivize miners, the Bitcoin software is currently programmed to pay miners 25 bitcoins ($5,000 given an exchange rate of $200 per bitcoin) for adding a new block of transactions to the universal ledger. The system is designed to award 25 new bitcoins every 10 minutes. Currently, there are about 13.7 million bitcoins in circulation. [9] At a price of $200, that gives Bitcoin a total market value of $2.7 billion. Yet when Bitcoin was at its peak of $1242, its market value was $14.9 billion (taking into

account its slightly lower circulation of 12 million in late November 2013). [10] By contrast, in the United States there is $1.29 trillion in cash and coins in circulation. [11] But, the vast majority of dollars in a fractional reserve banking system are 'created' by banks making new loans and not via the U.S. Mint's printing press.

Striking Bitcoin gold isn't easy or cheap. The estimated total daily cost of electricity for all miners is $147,000. [12] *The New York Times* reported that mining operations have actually been set up in Iceland in order to take advantage of the free, frigid arctic air in order to cool overheating computers toiling in the virtual Bitcoin mines. [13]

4. Limited Time Only

There is a limited supply of bitcoins.

The Bitcoin program is designed to reward miners by supplying new bitcoins into circulation every 10 minutes. And every four years, the amount of bitcoins rewarded to miners for successfully adding blocks of transactions is programmed to be cut in half. Thus, at some point in the next four years, miners will be rewarded with 12 ½ bitcoins instead of 25 for adding blocks to the ledger. Obviously, cutting the reward in half is a big deal for miners, especially if the price of bitcoin falls.

To maintain the every-10-minute pace of expansion, the Bitcoin software automatically adjusts to make the proof of work riddle harder or easier to solve. When a lot of mining computers are competing to solve the puzzle, the difficulty of the math riddle is increased. Miners will need to expend greater energy and time solving the riddle and earning the 25 bitcoin bounty.

Ultimately, the Bitcoin system will be limited to 21 million bitcoins. It is estimated that in 2140 the reward payments will stop and no additional bitcoins will enter circulation. At that point, it is assumed, miners will be compensated with higher transaction fees. But, ultimately, the supply of bitcoins is limited. For many, this is part of the appeal of Bitcoin. Users

and investors in Bitcoin believe that the value of the virtual currency will increase in value over time.

Who Likes Bitcoin and why?

Speculators

The Winkelvoss twins ("The Winkelvii") own Bitcoin as an investment. They think the total market value of bitcoins will rise to $400 billion, about 148 times its January 2015 market value. [14] They express great confidence in the mathematical scheme that runs Bitcoin. They have even filed paperwork with the Securities and Exchange Commission (SEC) to establish an exchange traded fund (ETF) which would give investors exposure to Bitcoin's rise or fall.

Techies

Venture capitalist Marc Andreessen believes Bitcoin is a technological innovation whose effects will be "profound." Andreessen compares the current debate about Bitcoin's value to the debates about the long-term value of PCs in the early 1970's and the Internet in the early 1990's. In a *The New York Times* op-ed, "Why Bitcoin Matters," Andreessen states "Bitcoin offers a sweeping vista of opportunity to re-imagine how the financial system can and should work in the Internet era, and a catalyst to reshape that system in ways that are more powerful for individuals and businesses alike." [15]

Fed Skeptics

The fact that Bitcoin is not associated with a government or central bank is appealing to people in countries whose central banks and central governments are notorious currency inflators. The Argentine peso has been inflated repeatedly and its buying power was expected to fall by 38% in 2014. [16] Some merchants in Argentina actually prefer bitcoins to pesos. If they are paid in dollars they will convert that payment to bitcoin. They do this because the dollar-to-bitcoin exchange rate is actually better than the dollar-to-peso exchange rate set by the Argentine government. In June 2014, it was over 30% better. [17] By contrast, in the U.S., most

merchants that accept bitcoins exchange them for dollars immediately.

Cranks

For the cranks, Bitcoin is part of a social and political revolution. Amir Taaki and Cody Wilson, anarchists recently interviewed by Wired magazine, are developing Dark Wallet, a completely anonymous, untraceable platform to exchange anything—including murder for hire—for bitcoins. As Wired states, they have "dedicated their careers to building some of the most controversial software ever offered to the public." Wilson developed the 3-D printed gun so that, "Everywhere there's a computer, there would be the promise of a gun." [18] And Taaki describes the hacker's ethic as "Empower the small guy, privacy and anonymity, mistrust authority, promote decentralized alternatives, freedom of information. These are good principles. The individual against power." [19] This is the dark, anti-authority side of Bitcoin.

Who Doesn't like Bitcoin and why?

China

China employs strict capital controls and is not in love with the fact that it cannot control Bitcoin. Capital controls restrict the flow of capital and prevent domestic currency from flowing outside the controlling countries borders. For China, domestic savings deposited in Chinese banks fund cheap investments in China. Bitcoin—which could allow Chinese citizens to skirt capital controls—is a threat to domestic currency tranquility and cheap investment funding. In April 2014, in reaction to Bitcoin's growing popularity, China's central bank banned Chinese commercial banks and payment companies from having Bitcoin trading accounts.

Fed Friends

Paul Krugman really does not like Bitcoin nor does he believe in it as a currency, because it is not a reliable store of value. In a blog post subtly titled, "Bitcoin is Evil," Krugman agrees

with those that say Bitcoin is a part of a Libertarian, anti-Federal Reserve political agenda—like returning to the gold standard. Since some Bitcoin proponents believe (see Fed Skeptics) that Bitcoin will save them from central-bank-created inflation, Krugman points out episodes of hyperinflation have been quite rare since the end of the gold standard.

Deflation Fearers

Some critics point out that the fact that bitcoin is deflationary is a weakness of the Bitcoin system. In the very first Bitcoin transaction, two pizzas were purchased for 10,000 bitcoins. At the time, that was about $25 in bitcoins. Today, 10,000 bitcoins equal about $2 million. At $12.50 per pizza, you can afford 160,000 pizzas. So, the price of goods (pizza) per bitcoin has fallen dramatically. If the price of bitcoin consistently rises, holders of bitcoin will have every reason to hoard—instead of spend. As University of Chicago Law Professor Eric Posner states, “As the economy grows, a fixed-supply currency becomes worth more in terms of goods and services, and people begin to hoard it—expecting that if they wait a little longer, they will be able to buy more. Once hoarding takes over circulation ends, and with it the function of the currency.” [20]

Prosecutors

Bitcoin has drawn the attention of law enforcement because it has been used to pay for illegal goods and services. "Silk Road" was an online marketplace that allowed users to pay for illegal drugs, and counterfeit currencies, amongst other illicit items with bitcoins. It was shut down by federal law enforcement in 2013 but according to a study by the Digital Citizens Alliance, even after the closure of Silk Road, 40,000 illegal products are currently listed for sale on the ‘dark web.’ [21] And in this obscure corner of the Internet, Bitcoin is the preferred payment option. Due to Bitcoin’s privacy benefits, many see transactions as untraceable as cash. Though, as Johns Hopkins University computer science researcher Ian Miers remarked, “It doesn’t matter if the

bagman is wearing a mask and a hoodie if the bills are marked. With bitcoin, all the bills are marked." [22]

Conclusion

Are virtual currencies like Bitcoin the future? They may be. At this point, Bitcoin is an innovative and novel payment method. There is tremendous value in challenging traditional payment methods and reducing costs associated with making payments. This incentivizes traditional intermediaries to create new, cheaper, and more efficient payment methods in the future, making the future brighter for everyone. Or maybe not.

TOPICS

FINANCIAL SERVICES 70

END NOTES

1. "Virtual Currency Schemes," Report, European Central Bank, October 29, 2012, p. 5. Accessed July 29, 2014. Available at: https://www.ecb.europa.eu/pub/pubbydate/2012/html/index.en.html.

2. Louis Andolfatto, "Bitcoin and Beyond: The Possibilities and Pitfalls of Virtual Currencies," Presentation, The Federal Reserve Bank of St. Louis, March 31, 2014, p. 4. Accessed July 29, 2014. Available at: https://www.stlouisfed.org/dialogue-with-the-fed/bitcoin-and-beyond.cfm.

3. "Bitcoin Charts: Estimated Transaction Volume and Estimated USD Transaction Volume," Block Chain Info. Accessed January 16, 2015. Available at: https://blockchain.info/charts/. Note: Statistics based on an average computed over seven days.

4. Visa Inc. 2014 Annual Report, November 21, 2014. Accessed January 16, 2015. Available at: http://yahoo.brand.edgar-online.com/displayfilinginfo.aspx?FilingID=10321036-14831-53514&type=sect&TabIndex=2&dcn=0001403161-14-000017&nav=1&src=Yahoo.

5. Kitco News, "2013: Year of the Bitcoin," *Forbes*, December 10, 2013. Accessed January 15, 2015. Available at: http://www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/.

6. "Bitcoin Price Index Chart," CoinDesk. Accessed January 15, 2015. Available at: http://www.coindesk.com/price/.

7. Marc Andreessen, "Why Bitcoin Matters," Op-ed, *The New York Times*, January 21, 2014, Dealbook. Accessed July 29, 2014. Available at: http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

8. Merriam-Webster. Accessed July 29, 2014. Available at: http://www.merriam-webster.com/dictionary/cryptography.

9. "Total Bitcoins in Circulation," Blockchain Info. Accessed January 15, 2015. Available at: https://blockchain.info/charts/total-bitcoins.

10. "Total Bitcoins in Circulation," Blockchain Info. Accessed January 15, 2015. Available at: https://blockchain.info/charts/total-bitcoins.

11. "How much U.S. currency is in circulation?" FAQs, The Board of Governors of the Federal Reserve System, July 10, 2014. Accessed July 29, 2014. Available at: http://www.federalreserve.gov/faqs/currency_12773.htm.

12. Mark Gimein, "Virtual Bitcoin Mining Is a Real-World Environmental Disaster," *Bloomberg*, April 12, 2013. Accessed July 29, 2014. Available at: http://www.bloomberg.com/news/2013-04-12/virtual-bitcoin-mining-is-a-real-world-environmental-disaster.html.

13. Nathaniel Popper, "Into the Bitcoin Mines," *The New York Times*, December 21, 2013, Dealbook. Accessed July 29, 2014. Available at: http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/.

14. Agustino Fontevecchia, "Winklevoss Twins Say Bitcoin Market To Hit $400B, Urge Regulators Not To Push Innovation To China," *Forbes*, November 12, 2013. Accessed July 29, 2014. Available at: http://www.forbes.com/sites/afontevecchia/2013/11/12/winklevoss-twins-say-bitcoin-market-to-hit-400b-urge-regulators-not-to-push-innovation-to-china/.

15. Marc Andreessen, "Why Bitcoin Matters," Op-ed, *The New York Times*, January 21, 2014, Dealbook. Accessed July 29, 2014. Available at: http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

16. J.M.P., "If it can't make it there," *The Economist*, June 12, 2014. Accessed July 29, 2014. Available at: http://www.economist.com/blogs/schumpeter/2014/06/bitcoin-argentina.

17. Michael J. Casey, "BitBeat: Why Bitcoin's Scoring in Argentina," *The Wall Street Journal*, June 25, 2014, Money Beat. Accessed July 29, 2014. Available at: http://blogs.wsj.com/moneybeat/2014/06/25/bitbeat-why-bitcoins-scoring-goals-in-argentina/.

18. Andy Greenberg, "Waiting for Dark," *Wired*, July 11, 2014. Accessed July 29, 2014. Available at: http://www.wired.com/2014/07/inside-dark-wallet/.

19. Andy Greenberg, "Waiting for Dark," *Wired*, July 11, 2014. Accessed July 29, 2014. Available at: http://www.wired.com/2014/07/inside-dark-wallet/.

20. Eric Posner, "Fool's Gold," *Slate*, April 11, 2013. Accessed July 29, 2014. Available at: http://www.slate.com/articles/news_and_politics/view_from_chicago/2013/04/bitcoin_is_a_ponzi_scheme_the_internet_currency_will_collapse.html.

21. Andy Greenberg, "Waiting for Dark," *Wired*, July 11, 2014. Accessed July 29, 2014. Available at: http://www.wired.com/2014/07/inside-dark-wallet/.

22. Andy Greenberg, "Waiting for Dark," *Wired*, July 11, 2014. Accessed July 29, 2014. Available at: http://www.wired.com/2014/07/inside-dark-wallet/.