3-1-2014

Digital Currency and Financial System: The Case of Bitcoin

Abdur Chowdhury
Marquette University, abdur.chowdhury@marquette.edu

Barry K. Mendelson
Capital Market Investments, Inc.

Published version. *Investments & Wealth Monitor,* (March/April 2014): 40-56. Permalink.

DIGITAL CURRENCY AND THE FINANCIAL SYSTEM: The Case of Bitcoin

By Abdur Chowdhury, PhD, and Barry K. Mendelson, CIMA®

Technological development and increased use of the Internet have led to the proliferation of virtual communities. Some of these communities have created and circulated their own currency for exchanging goods and services. Bitcoin is the most popular among these digital currencies and has been in the news recently because of wild fluctuations in its value and significant venture capital investment in entities associated with it.[1] Bitcoin is relevant in several areas of the financial system and is therefore of interest to central banks, consumers, and investors.

Digital currencies are part of a broader group of virtual currencies that include credit-card points, air miles, loyalty points, and coupons (see figure 1). Since the advent of the Internet, mobile devices, and detailed consumer information, companies increasingly are using digital currencies as marketing tools. As a result, the use of digital currencies has increased sharply, particularly among app-based coins and tokens, mobile coupons, and personal data exchanged for digital content. As these trends evolve, digital currencies have the potential to become more popular and compete with traditional currencies.

This article describes Bitcoin, its role in the financial system, its potential, its benefits, and its risks. We begin with a comprehensive overview and conclude with some recommendations about the future.

The Bitcoin Network

Bitcoin is the world's first completely decentralized peer-to-peer digital currency. A pseudonymous software developer published the Bitcoin Protocol (Nakamoto 2009), which outlined the theory of a decentralized currency. In January 2009 open-source Bitcoin software was released and mining of the first bitcoins began. Bitcoin rocketed to prominence in 2013, when its value soared more than 10-fold in a two-month period, from $22 in February to $266 in April (see figure 2).[2] The price of a bitcoin again rose to $710 on November 17, 2013, before falling to $600 shortly thereafter. Near-tripling of the price from early November 2013 to January 2014 was fueled by rising expectations that the virtual currency will continue to grow as an alternative to traditional methods of payment.[3] At its peak, based on more than 11.8 million bitcoins issued, this digital currency held a market value of more than $6 billion (figure 3).[4]

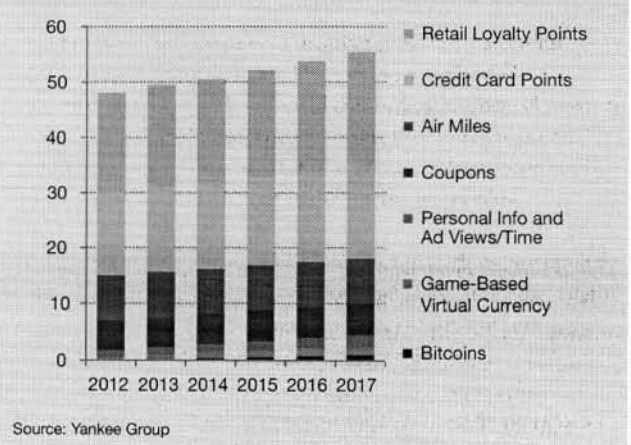
Since its creation, Bitcoin has evolved from a mathematical proof of concept to a rapidly expanding economic network. It is used in business transactions worldwide, and businesses big and small have shown interest in integrating the Bitcoin platform into their operations and providing new services within the Bitcoin economy. The momentum behind Bitcoin is growing as amateur investors, venture capitalists, and technology enthusiasts worldwide pump money into businesses that are trying to figure out how to use Bitcoin to buy and sell goods and services (see figure 4) (Needleman and Ante 2013). A growing number of merchants accept Bitcoin, because the associated transaction costs are generally lower than for credit or debit cards.

Instead of being produced on a printing press or by a central authority, bitcoins are generated by solving complicated algorithmic searches with powerful computers, a process known as mining.[5] Most Bitcoin users do not mine; they purchase or trade for bitcoins. Mining doesn't affect the average Bitcoin user much, but it is still an important part of the Bitcoin ecosystem.

All newly mined bitcoins, and all Bitcoin transactions, are publicly recorded. This record is known as the blockchain. The blockchain records transaction details, but it does not record any personal identifying information about senders or recipients.

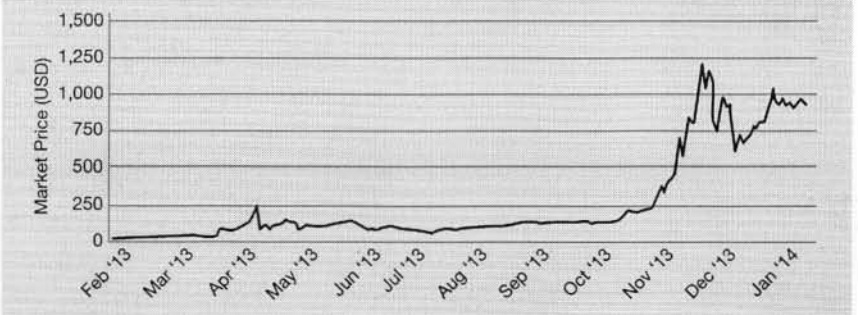
The blockchain is critical to maintaining the transparency of the Bitcoin system, and it makes counterfeiting or double spending impossible.

Figure 1: Virtual Currency Growth US$BN



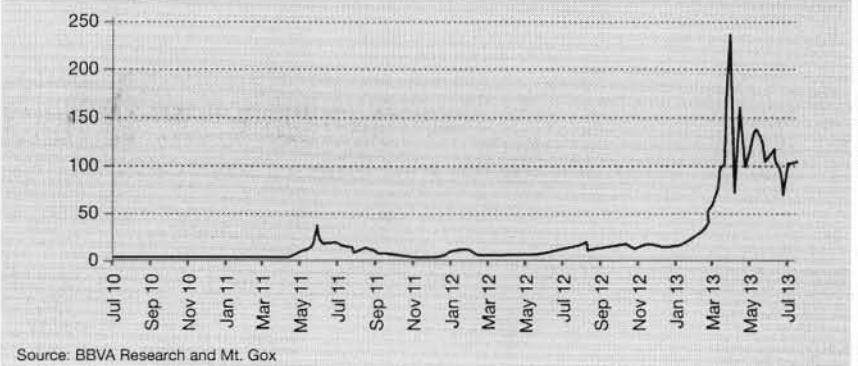
Source: Yankee Group

Figure 2: Market Price of Bitcoin



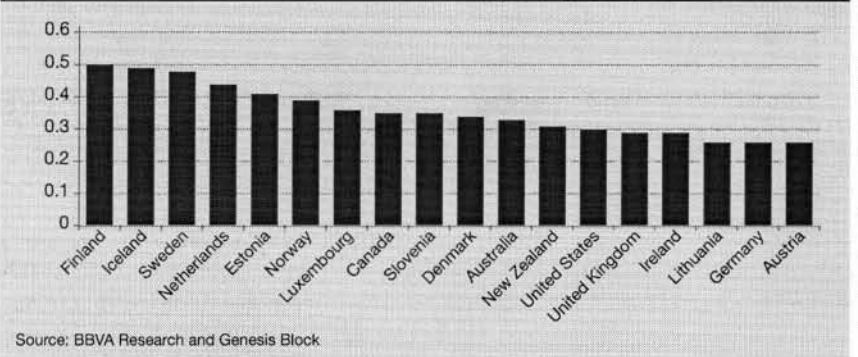
Source: http://blockchain.info/charts (accessed on January 25, 2014)

Figure 3: Bitcoin/USD Exchange Rate



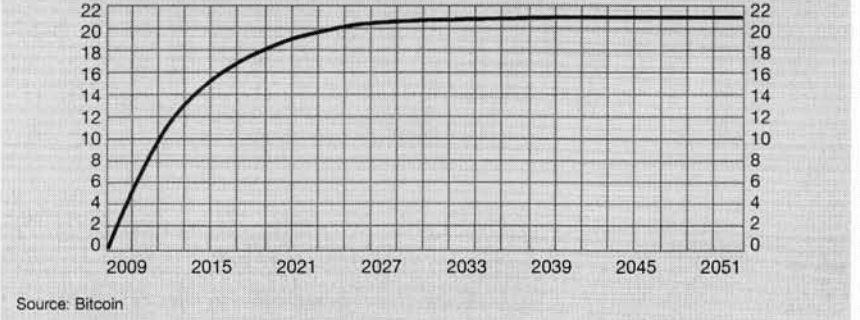
Source: BBVA Research and Mt. Gox

Figure 4: Bitcoin Penetration, Downloads Per Capita (%)



Source: BBVA Research and Genesis Block

Figure 5: Total Bitcoins (in millions)



Source: Bitcoin

Mining bitcoins is getting more complicated and more expensive as companies and technology fans race to build the powerful computers required for bitcoin production. The number of bitcoins that can be mined is limited. After the year 2040, no more bitcoins will be created, and the total amount that will ever be available is fixed at 21 million—more than half of which already have been mined (see figure 5). The Bitcoin scheme is technically designed so that its supply will increase at a particular pace.

A recent event highlights the vulnerabilities of a computer-driven virtual currency such as Bitcoin. On February 10, 2014, hackers began attacking the world's largest exchanges (Tokyo-based Mt. Gox, Cyprus-based BTC-exchange, and Slovenia-based Bitstamp) to exploit a flaw in the code that allowed users to send false requests to resend payments. The attacks forced the exchanges to suspend customer withdrawals. Later that day, Bitcoin's core developers discovered a bug in its digital infrastructure. The next morning, hackers exploited the bug and sent a barrage of mutated transactions that crippled Bitstamp and BTC-exchange. The hacker took every transaction occurring on the entire Bitcoin network and duplicated it under new identification codes, thus overwhelming and confusing the exchanges' computer systems. The major exchanges resumed processing withdrawals after several days once the software code was fixed. Mt. Gox, for its part, announced plans to introduce a new identification system for tracking bitcoin withdrawals, a move intended to protect against attack and restore operations.

Challenges Facing Bitcoin Users

Bitcoin proponents say that it promises to lower transaction costs for small businesses and global remittances, help alleviate global poverty by improving access to capital, protect individuals against capital controls and censorship, ensure financial privacy for oppressed groups, and spur innovation (Brito and Castillo 2013).

But potential users also should consider Bitcoin's downside risks, many of which are similar to the risks of using traditional

cash. First, based on Lee (2013) and our calculations, Bitcoin has weathered at least six significant price adjustments since 2011. These adjustments resemble traditional speculative bubbles: Overoptimistic media coverage of Bitcoin prompts waves of novice investors to pump up bitcoin prices (Salmon 2013). The exuberance reaches a tipping point, and the value eventually plummets (Brito and Castillo 2013).

Secondly, Bitcoin presents some specific security challenges.[6] If people are not careful, they can inadvertently delete or misplace their bitcoins because the currency is virtual, not physical. Once the digital file is lost, the money is lost, just like cash. Because of their pseudonymous nature, bitcoins could be used for illegal transactions. In October 2013, the U.S. government accused Silk Road of making available a vast digital marketplace where one could buy drugs and other illicit goods.

Another concern is that Bitcoin may be used to launder money for financing terrorism and trafficking in illegal goods. These worries appear to be more theoretical than practical right now, but it is conceivable that Bitcoin could be used by those who wish to discreetly move ill-gotten money.[7]

Is Bitcoin Money?

In its simplest form a traditional currency serves three purposes: medium of exchange, unit of account, and store of value. Bitcoin serves a role as a peer-to-peer network and a digital currency. However, it is not a traditional currency in the strictest sense. As a medium of exchange, Bitcoin satisfies the condition of coincidence of wants; however, it lacks liquidity because it has not been widely accepted. Its role as a unit of account is confined to a small group of businesses and individuals. Finally, Bitcoin's volatility makes it hard to predict, and thus it can be a risky instrument for storing value.[8]

Bitcoin and the Financial System

Because it has drawbacks as a currency, Bitcoin's insertion into the financial system has not been smooth. The supply of bitcoins cannot be controlled, regulated, or supervised by any public authority, and although businesses using bitcoins can be regulated, Bitcoin transactions and mining cannot. Bitcoin derives its value from decentralization and anonymity. Anonymity makes it difficult to manage credit, counterparty, liquidity, market, operational, and legal risks. Therefore in its current format, Bitcoin is not compatible with the demands of banks and regulators for transparency and accountability.

Consequently, the involvement of banks in the Bitcoin environment has been marginal and confined to those servicing businesses that operate with bitcoins. In most countries, banks are required to know their customers and comply with anti-money-laundering regulations, which are difficult to comply with in the Bitcoin network.[9]

Ultimately, lack of government support and vulnerability to money laundering make it difficult for Bitcoin to become a true competitor of benchmark currencies. Without the backing of governments and monetary authorities, Bitcoin's role in the global financial system will be limited to a niche currency or a digital commodity.

Bitcoin's limited supply and anonymity make it an attractive option for supporters of a decentralized monetary policy system and people who have lost trust in the financial system after the recent global crisis. In addition, it could be attractive for individuals looking to hedge against unstable local currencies.

From an institutional perspective, today's money is moving increasingly in an electronic environment, albeit one that is managed by the banking industry. However, in its purest form, digital peer-to-peer currencies eliminate the need for banking intermediation and sovereign guarantees. A decentralized digital currency challenges the entire monetary and banking system (BBVA 2013).[10]

For digital currencies to succeed they have to be trustworthy, and that necessarily implies the recognition of governments and financial institutions. Achieving such recognition will be hard for digital currencies such as Bitcoin, which by design are anti-establishment.[11]

Bitcoin and Monetary Policy

The Bitcoin scheme is designed as a decentralized system with no involvement of a central monetary authority. Bitcoins can be bought on different platforms. However, new bitcoins are created and introduced into the system only through mining, i.e., as a reward for the miners who perform the crucial role of validating all the transactions involved in the bitcoin creation process.

Therefore, the supply of money does not depend on the monetary policy of any virtual central bank; rather, it evolves based on interested users performing a specific activity. According to Bitcoin, the scheme has been designed so the money supply will develop at a predictable pace. The number of bitcoins in existence will reach its maximum limit of 21 million in 2040. From this point onward, miners are expected to finance themselves via transaction fees.

The fact that the supply of money is clearly determined implies that, in theory, it could not be changed by any central authority or participant wanting to "print" extra money. According to Bitcoin proponents, the system is designed to resist inflation as well as the business cycles that originate from extensive money creation. However, critics have suggested that the system leads to a deflationary spiral. The total supply of bitcoins is expected to grow geometrically until it reaches a finite limit of 21 million. If, however, the number of users starts growing exponentially for any reason, and assuming that the velocity of money does not increase proportionally, a long-term appreciation of the currency can be expected. This would imply a depreciation of the prices of the goods and services quoted in bitcoins. People would have an incentive to hold bitcoins and delay consumption, thereby exacerbating the deflationary spiral.

Brito and Castillo (2013) have pointed out, however, that the extent to which this could

HOW BITCOIN WORKS

Mining

Bitcoins enter circulation through a process called "mining." A miner's computer solves complex equations for the Bitcoin network. If it successfully solves an equation, the miner receives bitcoins, which come in the form of a long string of numbers and letters known as an "address."

Wallets

The miner stores bitcoins in a virtual "wallet," which saves the addresses on a hard drive or the Internet. Wallets can hold multiple Bitcoin addresses that each hold a balance of bitcoins.

Making a Purchase

Say a bitcoin owner wants to use coins to purchase a muffin. The muffin retailer gives the owner a bitcoin address, to which the muffin buyer sends the bitcoin or fraction of a bitcoin.

Verification

The bitcoin-mining community verifies the transaction and stores it in a public ledger, making the transaction irreversible. In return for processing transactions, miners can be rewarded with bitcoins.

Source: Adapted from a U.S. Government Accountability Office report

be a problem in reality is not clear. First, as highlighted by the *Economist* (2013), the deflation hypothesis assumes that many more people want bitcoins in exchange for goods or paper money, but Bitcoin is immature and illiquid—a clear disincentive for its use. Second, Bitcoin is not the currency of a country or currency area and therefore is not directly linked to the goods and services produced in a specific economy; bitcoins are linked to the goods and services provided by merchants who accept bitcoins. These merchants may also accept another currency (e.g., U.S. dollars) and therefore, the fact that deflation is anticipated could give rise to a situation where merchants adapt the prices of their goods and services in bitcoins.

Concluding Remarks

Successful virtual currencies must balance convenience and compliance (BBVA 2013). Trust in the U.S. dollar comes from the strength of the U.S. economy and its institutions. Would people trust a currency that is backed by a private entity or an unknown developer? Would the average person put savings in a digital wallet rather than a bank account that is insured by a deposit guarantee fund? Who will be accountable for a failure in the systems that create the digital currencies? These and other serious questions need to be considered by developers of virtual currencies.

On the other hand, governments and financial institutions should recognize that it is only a matter of time before new models of virtual currency such as Bitcoin become more mainstream. So the challenge for policymakers will be to foster Bitcoin's beneficial uses while minimizing its negative consequences.

Since this article was written, Bitcoin has been in the news a great deal. In February 2014, after weeks marked by technological breakdowns, regulatory issues, and general questions over its viability, Bitcoin was in turmoil. And on February 28, 2014, the Mt. Gox exchange filed for bankruptcy protection (Takemoto and Knight 2014). The way Bitcoin and its ecosystem react could determine whether the whole experiment goes the way of Dutch tulips in the 1600s or becomes a historic technological breakthrough such as e-mail (Guerrera 2014).

Bitcoin's strength has been predicated on three supposed qualities: It is anonymous, or at least pseudonymous (transactions are recorded but the identity of the parties is encrypted); it is difficult to hack; and it cuts out financial middlemen such as banks.

Of late, though, Bitcoin's three bulwarks have come under fire. Its anonymity has caught the attention of regulators and law-enforcement agencies because of alleged money laundering. Its immunity to cyberattacks was called into question in February 2014 when the three main Bitcoin exchanges were hacked. And the currency's place on the fringes of the financial system has proved a limitation because most banks refuse to facilitate transactions in bitcoins. Indeed, the price of a bitcoin now is almost half of its peak.

The world is not short of currencies, so what problem is this new digital currency solving? To thrive, Bitcoin must be more useful than current payment systems. Virtual currencies could embed into the financial infrastructure as complements to existing forms of payment in two ways (Guerrera 2014). The first is as a conduit for small international transactions such as remittances from foreign workers. A currency such as Bitcoin could reduce both the cost and the time required for such payments.

The second potential use is further into the future. Bitcoin is an open financial platform that could house data in a secure and universal ledger. From payments for road tolls to proof of ownership for cars and houses, Bitcoin could be an independent, secure, and reliable host of financial and personal information. It sounds far-fetched and even its supporters concede that this could only happen if three conditions materialize.

First, the current infrastructure—largely anonymous, anchored by unregulated overseas exchanges, and vulnerable to manipulation by criminals—must be overhauled through the creation of U.S. exchanges overseen by financial watchdogs. Second, institutional money such as pension funds must invest in Bitcoin to curb its wild price volatility. And, third, banks will have to view Bitcoin as legitimate and enable customers to exchange it for dollars and cents.

Continued on page 56

"I completed the self-study portion in IMCA's virtual classroom, studying at some very odd times, but I really wanted to absorb the material so I could start using it immediately with my clients," she recalls. After completing the online curriculum, Moore joined ot-her candidates at a week-long session at The University of Chicago Booth School of Business, followed by the certification exam. "I really like the way IMCA has structured the program to work for someone like me with a fully established practice," she says.

Moore also believes in giving back. She is a self-described "Air Force brat," and her father, husband, brother, grandfather, uncles, and nephew are veterans. One nephew currently serves in the U.S. Coast Guard; another is in the Air Force ROTC. Moore and her husband are former board members of Honor Flight Michigan, a charitable organization that transports World War II veterans to visit the WWII Memorial in Washington, DC. Today they raise money and awareness to support the charitable efforts of three organizations: Homes for Our Troops, Help for Our Disabled Troops, and Operation Never Forgotten. "We wouldn't have the freedoms we have today without the sacrifice and commitment of our military," she says. "Service to country is what that's all about, and is a core principle for both my husband and me."

Moore also mentors women moving up the career ladder at Wells Fargo Advisors and elsewhere in financial services. "If I can be part of shaping this industry to better meet the needs of clients and make it a friendlier place for women and minorities, by all means I'm going to do it," she says. "Every morning when I get up, I can be one of two things: part of the problem or part of the solution. I choose to be part of the solution."

She credits IMCA with being part of the solution as well. "IMCA supports my pursuit of excellence—in the credentials it offers, the standards it sets, and the education it provides," she says. "IMCA challenges me to step up and become a better financial professional for my clients, and to present financial services in a positive way. IMCA's ultimate goal is to help us make our industry better." ●

Interview by Ryan Hoffman, Investment Management Consultants Association® (IMCA®).

THE CASE OF BITCOIN

Continued from page 43

None of these conditions is a given, and none would make Bitcoin a replacement for the dollar. But Bitcoin likely will play more than a bit part in the financial industry of the future. ●

Abdur Chowdhury, PhD, is a professor in the Department of Economics at Marquette University and chief economist with Capital Market Consultants in Milwaukee, WI. He earned a BA (Honors) and an MA in economics, both from the University of Dhaka in Bangladesh, and MA and PhD degrees in economics from the University of Kentucky. Contact him at abdur@cmarkc.com.

Barry Mendelson, CIMA®, is chief executive officer and senior investment analyst with Capital Market Consultants in Milwaukee, WI. He earned a BS from Palmer College. Contact him at barry@cmarkc.com.

Endnotes

1. Bitcoin is not the only digital currency on the Web. Others include Ripple, a new currency from the startup OpenCoin.com.
2. Bitcoins come in whole or fractional form. Each bitcoin is subdivided into 100 million smaller units called satoshis, defined by eight decimal places.
3. The prices are as of November 17, 2013, on the Tokyo-based Mt. Gox exchange and on the Slovenia-based Bitstamp Exchange.
4. The Bitcoin economy exceeded $8 billion at one point in November 2013, and investors and the U.S. Treasury are beginning to give the virtual currency legitimacy.
5. Mining is the calculation of a hash of a block header, which includes, among other things, a reference to the previous block, a hash of a set of transactions, and a nonce (a 32-bit/4-byte field with a value set so that the hash of the block will contain a run of zeros). If the hash value is found to be less than the current target (which is inversely proportional to the difficulty), a new block is formed and the miner gets 50 newly generated bitcoins. If the hash is not less than the current target, a new nonce is tried, and a new hash is calculated. This is done millions of times per second by each miner.
6. Most security challenges concern wallet services and Bitcoin exchanges. The protocol itself has proven to be considerably resilient to hacking and security risks. See Kaminsky (2013).
7. Concerns about Bitcoin's money-laundering potential were stoked after authorities shut down Liberty Reserve, a private, centralized digital-currency service based in Costa Rica, on charges of money laundering. Unlike Bitcoin, however, Liberty Reserve was a centralized currency service created and owned by a private company.
8. Sharp buying and selling due to the Cyprus bail-in showed Bitcoin's vulnerability to speculation and highlights how unpredictable its value can be.
9. For example, the U.S. Department of Homeland Security seized Mt. Gox's bank account at Wells Fargo, alleging violations of anti-money-laundering regulations. Likewise, Barclays and Royal Bank of Canada have frozen or shut down bank accounts tied to Bitcoin businesses.
10. Ripple, created by a private company, was designed to serve a dual function as a currency and a payment system, allowing for faster processing times and lower fees.
11. In March 2013, the U.S. Financial Crimes Enforcement Network clarified rules set in 2008's Bank Secrecy Act (BSA), which governs digital currencies. Under the BSA, exchanges and administrators of digital currencies are considered money-services businesses, which require federal and state registration.

References

Banco Bilbao Vizcaya Argentaria (BBVA). 2013. Bitcoin: A Chapter in Digital Currency Adoption. BBVA Research (July 31). http://www.bbvaresearch.com/KETD/fbin/mult/130731_EconomicWatchEEUU_Bitcoin_tcm348-398292.pdf?ts=2082013.

Brito, Jerry, and Andrea Castillo. 2013. Bitcoin: A Primer for Policymakers. Mercatus Center, George Mason University. http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_v1.2.pdf.

Economist. 2013. How Does Bitcoin Work? (April 11). http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-does-bitcoin-work.

Guerrera, Francesco. 2014. Bitcoin's Crisis Is Turning Point for Currency. *Wall Street Journal* (February 17).

Kaminsky, Dan. 2013. I Tried Hacking Bitcoin and I Failed. *Business Insider* (April 12). http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4.

Lee, Timothy B. 2013. An Illustrated History of Bitcoin Crashes. *Forbes* (April 11). http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/.

Nakamoto, Satoshi. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf.

Needleman, Sarah, and Spencer Ante. 2013. Bitcoin Startups Begin to Attract Real Cash. *Wall Street Journal* (May 8). http://online.wsj.com/news/articles/SB10001424127887323687604578469012375269952.

Salmon, Felix. 2013. The Bitcoin Bubble and the Future of Currency. *Medium* (April 3). https://medium.com/money-banking/2b5ef79482cb.

Takemoto, Yoshifumi, and Sophie Knight. 2014. Mt. Gox Files for Bankruptcy, Hit with Lawsuit. Reuters (February 28). http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228.