EDITOR: Irena Bojanova, University of Maryland University College, irena.bojanova@umuc.edu

© Tadeusz Ibrom | Dreamstime.com

Bitcoin: Benefit or Curse?

George F. Hurlburt, *STEMCorp*
Irena Bojanova, *University of Maryland University College*

The age of trading two pelts for a chunk of shiny metal—the barter system—ended when people minted shiny metals into coins. Coinage metrically equated to established value, thus promoting fair trade. Eventually, paper currency symbolically supplanted coinage and modern national currency systems arose, initially backed by stockpiles of precious metals and enabled by print technology. As technology matured, banknotes became an important medium of telegraphic exchange, enabling near real-time monetary transactions over long distances.

More recently, plastic has overtaken paper. The immediate extension of credit at the point of sale offers a far more sophisticated abstraction for global exchange. Precious metals lose their luster in the emergent global marketplace where valuations are increasingly volitile. Increased regulation in today's markets can help safeguard against fraud, yet this leads to regulators, brokers, and bankers deriving income through regulatory fees for services. Now, with mobile devices becoming ubiquitous, mobile technology can clearly support open, unregulated virtual currency, embodied by one of the leading contenders—bitcoin cryptocurrency.

Bitcoin: A Virtual Entity

Bitcoin is a digital currency system based on peer-to-peer virtual data. Individual bitcoins are negotiable instruments backed only by the perceived value of items exchanged. The concept has grown since its shadowy introduction in 2009, and bitcoin values have fluctuated from as low as US$2.95 to nearly $1,200 per bitcoin. To date, over 12 million bitcoins exist, with a rough aggregated valuation of around $6.3B in mid-April (see http://bitcoincharts.com).

To use bitcoins, individuals must establish a bitcoin "wallet" on a computer (see Table 1). The wallet contains nothing more than a regularly updated file, listing all bitcoin transactions ever made. Bitcoins can be transmitted to other user wallets using a combination of public and private key cryptology. The transaction contains the amount of bitcoins, including fractions, and a transaction-unique digital signature, protected by a private key. The receiver provides a public key, which serves as the sending address. The transactions' public keys ensure that everyone in the Bitcoin network receives and can validate new exchanges via their wallets. Transactional private keys preserve both the integrity and anonymity of each sender's digital signature.

No one knows how many bitcoins a given user possesses, so each transaction makes reference to the user's unspent incoming transactions to cover the amount of the outgoing transaction. The public and private key combinations permit a degree of privacy among those who exchange bitcoins. Privacy is allegedly further enhanced for those willing to secure their systems and data to protect their private keys.[1] If, however, the private key is lost due to a disk crash without backup, or if it becomes inadvertently malformed, the affected bitcoins are forever lost.[2] Buyer beware!

Resolving the Transaction Sequence

Although the wallet validates transactions, it doesn't record the order of transactions. Because TCP doesn't guarantee the order of

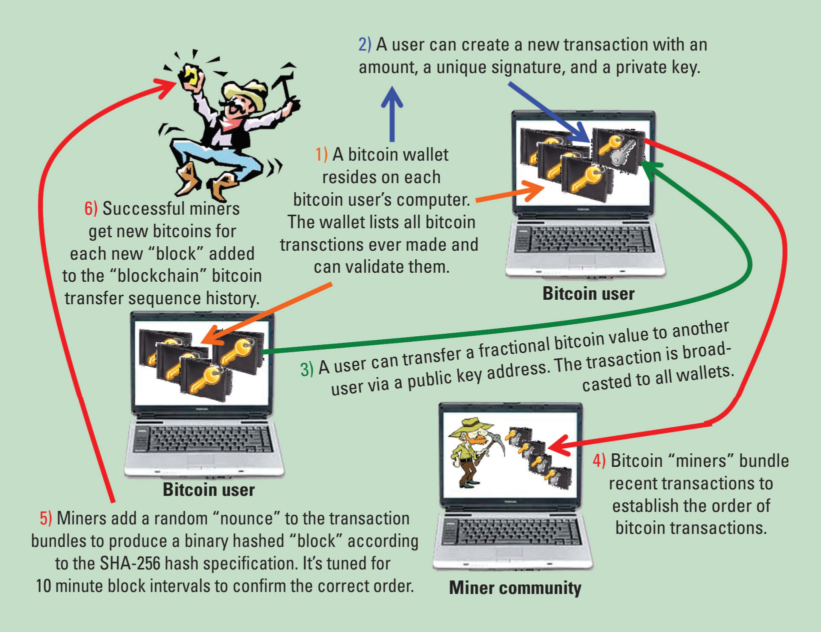
1520-9202/14/$31.00 © 2014 IEEE

Table 1. Establishing a bitcoin wallet.

Environment	Available wallets (for accepting and transferring payments, saving bitcoins, and making purchases)
Windows, Mac, and Linux	MultiBit—https://multibit.org BitcoinQT—https://bitcoin.org/en/download Armory—https://bitcoinarmory.com Electrum—https://electrum.org Hive—https://www.hivewallet.com
Android	Bitcoin Wallet— https://play.google.com/store/apps/details?id=de.schildbach.wallet Coinbase— https://coinbase.com
iOS	Coinbase— https://coinbase.com
QR code scan	NFC “Tap to pay” with Bitcoin Wallet—https://play.google.com/store/apps/details?id=de.schildbach.wallet
SMS	Text with Coinbase— https://coinbase.com
Web browsers	Coinbase— https://coinbase.com Blockchain—http://blockchain.info

arrival, it’s possible to nullify an initial transaction if a duplicate one hits its destination earlier than the original transaction. To prevent such duplication, some 20,000 distributed computers, operated by so-called bitcoin “miners,” gather recent transactions. The miners use Bitcoin mining software to apply a random number “nounce” to the transaction bundle and engage a rigorous hashing process to solve mathematical puzzles.

The hashing process is a random “guessing game” entailing more than 100,000 guesses with an acceptable digital string that fits a suitable pattern, according to the Secure Hash Algorithm (SHA)-256 standard. Successfully solving the mathematical puzzle ensures that acceptable sequence records, called blocks, are added to the growing historical record of all bitcoin transactions in proper order. Each block contains a record of recent transactions. A block’s hash identifier always points to the most recently accepted block. This ensures tamperproof sequencing. The sequence of blocks, universally available to all, is known as the *blockchain* and is near 3 Gbytes in size. Thus, as transaction blocks join the blockchain, receivers can confidently accept recent incoming transactions, as the probability of duplicative use of the same bitcoins is infinitesimal. This distributive mining process theoretically makes bitcoin a decentralized currency.



2) A user can create a new transaction with an amount, a unique signature, and a private key.
1) A bitcoin wallet resides on each bitcoin user’s computer. The wallet lists all bitcoin transctions ever made and can validate them.
6) Successful miners get new bitcoins for each new “block” added to the “blockchain” bitcoin transfer sequence history.
Bitcoin user
3) A user can transfer a fractional bitcoin value to another user via a public key address. The trasaction is broadcasted to all wallets.
Bitcoin user
4) Bitcoin “miners” bundle recent transactions to establish the order of bitcoin transactions.
5) Miners add a random “nounce” to the transaction bundles to produce a binary hashed “block” according to the SHA-256 hash specification. It’s tuned for 10 minute block intervals to confirm the correct order.
Miner community

Figure 1. How bitcoins are stored, transmitted, mined, and minted.

Minting the Bitcoins

Because of the random nature of hashing, achieving an acceptable block is never a guarantee. Thus, bitcoin mining is a competitive venture, where miners are awarded new bitcoins for each block successfully hashed and accepted in the blockchain. This is how the term “mining bitcoins” came to be, and it establishes how new bitcoins enter circulation. Figure 1 graphically depicts the transaction, blockchain creation, and bitcoin minting process.

The mathematical puzzle to be hashed is periodically modified both to increase complexity and ensure new block production remains regulated. This expanding complexity will continue until around the

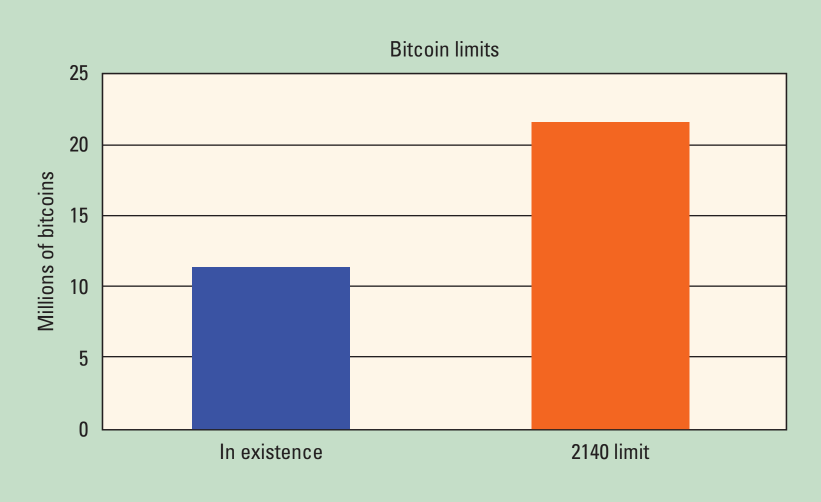


Figure 2. The bitcoin cap. In 2140, minting will hit a 21-million bitcoin cap.

year 2140, when minting will hit a 21-million bitcoin cap (Figure 2). The cap is governed by a diminishing payoff to miners at four-year intervals—the number of awarded bitcoins per block started at 50 and is halved every 210,000 blocks (or approximately every four years).

As the payout decreases, however, the complexity of the hashing puzzles increases to ensure 10-minute intervals between blocks. This demands increasingly sophisticated processing and requires more energy. Moore's Law appears to permit purposed-based Bitcoin mining technology to keep pace with this demand. Specialized commercial Bitcoin "mining rigs" are becoming more energy efficient, faster, and more accurate.[3] The price points for sophisticated "mining-rigs", however, require increasingly significant investments (regardless of whether the mining hardware is owned or rented in the cloud), thus fueling fears of eventual monopolistic mining operations. Should any single entity obtain 50 percent of the mining market, the odds of successful minting become a healthy (and somewhat controlling) 50 percent.

The Virtues of Bitcoin

The rapid ascent and seeming acceptance of Bitcoin suggests bottom-up virtual currency has staying power. It's open, yet it permits a degree of user anonymity, and it's relatively free of exorbitant transaction fees. Most importantly, it appears well suited to real-time, global mobile exchange. Table 2 outlines the pros and cons of Bitcoin.

Some assert that the bitcoin currency is attractive to the technically elite, who don't mind the risk, much less the extra effort required to acquire and manipulate bitcoins. Others note that over 200 million people are exposed to Bitcoin globally and, using social data mining, they can characterize Bitcoin users' personality traits.[4] For example, evidence shows that 64 percent of those who bought early bitcoins tended to initially keep them as speculative investments.[5] The number of bitcoin exchanges, where people store bitcoins, has grown. Interestingly, bitcoin activity rapidly shifted from hoarding to spending behavior when Satoshi Dice, a bitcoin gambling game, came into existence in April 2012. Bitcoin transactions grew by orders of magnitude as Satoshi Dice commanded some 60 percent of all initial bitcoin transactions.[5]

The transaction rate for bitcoin, however, is now branching out. The advent of ATMs and other mediated tools with built-in cash-to-bitcoin-to-cash conversions will ease bitcoin exchange. Furthermore, as online retailers, such as Overstock, aggressively encourage bitcoin trade, more consumers are likely to engage. Bitcoin—or more generally, digital currency—thus has the potential to become a worldwide disruptive technology. This trend is growing as Bitcoin communities, under the mantle of the College Cryptocurrency Network (CCN), appear increasingly on college campuses reminiscent of the growth of Facebook.[6]

A Forrester Research blogger recently asserted that bitcoin would survive, because of sluggish official response to the financial crisis, the borderless peer-to-peer nature of Bitcoin as a self-regulating financial system, and the democratic nature of the bitcoin movement.[7] Marc Andreessen, the Netscape developer turned venture capitalist, has invested over US$50M in bitcoin startups, and he recently advocated for bitcoins in the *New York Times*.[1] He argues the Bitcoin system is here to stay, because it represents a breakthrough technology that enables trusted exchange among otherwise untrustworthy participants. He further asserts that Bitcoin offers a basis for new business ventures to expand in the global economy. Even the Winklevoss twins of Facebook fame have filed for Securities and Exchange Commission acceptance of Bitcoin as a medium of market exchange. They've devised the "Winkdex" for valuation of Bitcoin as a market commodity.[8]

The Downside

Bitcoin, however, also has a dark side. The gambit of illicit activities associated with bitcoin cover a wide range, including sales of illegal goods, drugs, and weapons; assassinations; Ponzi schemes; money laundering; illegal mining; unlawful gambling; and outright theft. A recent spate of negative bitcoin

Table 2. Bitcoin pros and cons.

Pros	Cons
No costly regulation and overhead.	Lack of regulation to protect consumers.
Transactions are anonymous—cryptocurrency works like cash and cuts down on identity theft and credit card fraud.	Encourages illicit activity—money laundering, tax evasion, and illicit trade (for example, Silk Road[9]).
The first cryptocurrency that works.	Fluctuating valuation without backing—speculative ride can be wild, as only a limited number of bitcoins are in circulation.
Promotes a global economy—works everywhere, anytime, with minimal processing fees.	Not widely endorsed. Regulators in some countries have warned against or have taken concrete measures to discourage bitcoins use.
Trusted exchange.	Subject to malware (for example, Mt. Gox[14]).
Transactions are publically viewable to help protect against double spending.	Irreversible transactions—no refunds unless the receiver issues a new transaction to send bitcoins back.
Transactions are secure—military-grade cryptology protection is theoretically immune to government interference or manipulation.	Ostensibly anonymous users can be traced through network analysis.
Good for democracy.	Not good for established banking practices.
Cryptocurrency is produced collectively, at a rate bounded by a value both previously defined and publicly known.	Miners must invest in purpose-built Bitcoin hardware, which challenges the claim nobody owns or controls the network.
Users can have their own financial system—developers can integrate a Bitcoin server directly into their applications.	Balance of any user can be wiped out by a computer disk crash if a back-up copy of the holdings doesn't exist.

publicity has elicited strong emotions on all sides of the growing virtual currency debate. In the wake, the value of a bitcoin is currently declining.

Silk Road flourished as virtual business through the existence of bitcoins. It supported a highly profitable illegal drug trade, which thrived through seemingly untraceable transactions.[9] Silk Road ceased to exist, however, when Federal agents arrested its founder in a San Francisco Public Library in such a way that his laptop wouldn't be clam-shelled, thus denying access to its contents. This preserved incriminating transaction records on the laptop, including possible assassinations on adversaries.[9] Silk Road 2.0 quickly sprang up and resulted in a $2.7M loss when attacked by malware.[10]

Recent Distributed Denial of Service (DDoS) attacks have thwarted some of the leading bitcoin exchanges.[11] More ominously, Mt. Gox, a major bitcoin exchange in Japan,[12] was hit by a "transaction malleability" attack. This attack exploited Bitcoin software, allowing double payouts from the exchange. The resulting estimated $500M loss caused the exchange's value to plummet as Mt. Gox suspended bitcoin withdrawals and shortly thereafter sought bankruptcy protection[13] and subsequently liquidation.[14] The Canadian bitcoin exchange Flexcoin also lost $600k in a similar attack and had to shut down.[15]

Threatened by bitcoin's existence, both Apple and PayPal have carefully distanced themselves from fully endorsing it, and Amazon is creating its own digital coinage. Fearing an inability to regulate against fraud, China, Russia, Japan, and other nations have declared bitcoin a rogue currency, not to be nationally recognized. Ironically, Japan has also proposed taxing bitcoin use.[16] In the US, skeptical state lawmakers are calling for full bitcoin regulation for fear of widespread fraud and criminal activity or, at the very least, disruption of traditional regulation.[17] Subsequently, the US Internal Revenue Service declared bitcoins taxable as property, but not currency.[18] The wealthy and highly regarded investor, Warren Buffett, has declared bitcoin to be a "mirage."[19]

The Future of Virtual Currency

In many ways, the negative hype is overstated and not entirely accurate. The exploit that reduced Mt. Gox to bankruptcy protection resulted from an anticipated vulnerability, and the ability of federal investigators to isolate the Silk Road proponent, Ross Ulbricht, wasn't just a coincidence.[9]

Recent research reveals that bitcoin is "pseudonymous" (that is, the anonymity users think they have is fake). Pattern analysis, enabled through applied graph theoretical methods, can isolate individual users through refined heuristics. Transaction patterns contained in the blockchain and transaction wallets, when traversed as graphs can lead to solid inferential data as to who is doing what, despite private key protection. Such analysis even reveals sophisticated "peeling" techniques used to launder money anonymously by incrementally shedding small amounts through various exchanges.[10]

Table 3. Techniques and tools for engaging with bitcoin.

Activity	Description	Instructions
Use bitcoin	Establish wallets. Accept payments. Transfer payments. Save bitcoins in exchanges. Make purchases.	(See Table 1)
Join the network	Contribute computational power to the network by running full node software.*	Install the bitcoin client Bitcoin-Qt (https://bitcoin.org/en/download). Keep the bitcoin client running via an Internet connection.
Become a miner	Mine bitcoin blocks to help process transactions. Receive 50 bitcoins (halved each four years) for each successful blockchain link.	1. Invest in purpose-built Bitcoin mining hardware,** based on custom ASIC chips, Butterfly Labs (www.butterflylabs.com), or Avalon (http://avalon-asics.com), or rent Bitcoin mining hardware in the cloud (www.coindesk.com/information/cloud-mining-bitcoin-guide). 2. Install free Bitcoin mining software: CGminer (https://github.com/ckolivas/cgminer), BFGminer—command line (http://bfgminer.org), or the EasyMiner GUI for Windows/Linux/Android (http://easyminer1.software.informer.com). 3. Set up a user wallet to receive the bitcoins successfully mined. You might also use Bitcoin hardware wallets (www.hardwarewallets.com). 4. Join a mining pool to work with other miners to solve a block and share its rewards: eclipsemc (https://eclipsemc.com) or eligius (eligius.st/).
Development	Bitcoin is free software, still in active development, so you can become a bitcoin tester, developer, or entrepreneur—improving bitcoin or building new services or software that use bitcoin.	Use the GitHub repository (https://github.com/bitcoin/bitcoin). JoinThe GitHub discussions (https://github.com/bitcoin/bitcoin). Join the bitcoin-developmeWnt mailing list (http://sourceforge.net/p/bitcoin/mailman/bitcoin-development/).

** Note: Full nodes secure and relay all users' transactions – they comprise the backbone of the network.*

*** Computer CPUs, graphics card GPUs, or high speed video processor cards are no longer recommended—they consume more in electricity than you'll likely earn from mining.*

Virtual currencies, perhaps as a follow-on to bitcoin, will revolutionize finance, well exceeding the Internet's profound effect on how people interact with content. Sander Duivestein and Patrick Savalle speculate that disruptions might become increasingly abrupt,[20] fueled by the notion that peer-to-peer financial networking will become the trusted party, overtaking the traditional role of banking. With peer-to-peer finance, payments are sent directly from one party to another without going through a financial institution. If virtual currency begins to make banking as we know it obsolete, the trend could rapidly prove disruptive to the economy.

In essence, virtual currencies, currently represented by the bitcoin cryptocurrency model, have the potential to make money programmable. Eventually, financial APIs could unleash immense economic potential. This, in turn, gives further credence to trans-global, distributed, decentralized, and innovative companies and services.[20] A 20-year-old Canadian programmer is already promoting a language to codify online contract transactions.[21] The Mastercoin technology (www.mastercoin.it) enhances the Bitcoin blockchain with additional features. Others envision protocols that are currency agnostic, thus making fee-free, Internet-speed currency conversions straightforward.[20]

Significantly, virtual currencies enable economic value to be assigned to individual items, no matter what size. This is highly significant in the coming Internet of Anything. Imagine machine-to-machine markets allowing something as common as a soda machine to literally become its own enterprise, tracking its own inventory, ordering materials, and accounting for its own revenues. This logically leads to Decentralized Autonomous Corporations (DACs). As they emerge, DACs thrust the growing proliferation of autonomous systems to a new plateau. Here, the corporate mission is etched in code, not mediated by boards. This further suggests that corporations will rise quickly and die-hard as newer innovation rapidly overtakes current technology.[20]

Virtual currencies are the next logical step in financial operations and will likely prevail on a global scale. IT professionals must keep up with this major disruptive technology by, as Table 3 outlines, becoming involved as bitcoin users (paying with or accepting bitcoins), miners (running the computers that process and validate transactions), or developers and entrepreneurs (upgrading the system with new products and services). Minimally, we must become savvy about virtual currency and how it operates. We can't afford to stand on the sidelines because, as technical professionals, we will be the best prepared to act as ethical guardians when virtual currencies come to mass adoption.

References

1. M. Andreessen, "Why Bitcoin Matters," *New York Times*, 21 Jan. 2014; http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters.
2. Z. Miners, "3 Reasons Bitcoins Aren't in Your Wallet Yet," *Computerworld*, 2 Dec. 2013; www.pcworld.com/article/2071100/3-reasons-bitcoins-arent-in-your-wallet-yet.html.
3. M.B. Taylor, "Bitcoin and the Age of Bespoke Silicon," *Proc. 2013 Int'l Conf. Compilers, Architectures and Synthesis for Embedded Systems* (CASES 13), 2013, article no. 16; http://cseweb.ucsd.edu/~mbtaylor/papers/bitcoin_taylor_cases_2013.pdf.
4. M. Carney, "Bitcoiners Prefer Finance and Kindles to Sex: A Revealing Look into the Interest Graph of Crypto-Currency Users," *Pando*, 13 Feb. 2014; http://pando.com/2014/02/13/finance-kindles-but-no-sex-a-revealing-look-into-the-interest-graph-of-bitcoin-users.
5. S. Meiklejohn et al., "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *USENIX*, vol. 38, no. 6, 2013; http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.
6. B.P. Eha, "Meet the College Students Who Are Driving the Future of Bitcoin," *Entrepreneur*, 8 Apr. 2014; www.entrepreneur.com/article/232869#.
7. B. Hopkins, "Why Bitcoin Is Here to Stay," *ZDNet*, 29 Jan. 2014; www.zdnet.com/why-bitcoin-is-here-to-stay-7000025745.
8. K.L. Shandrow, "Winklevoss Twins Launch Winkdex Bitcoin Index," *Entrepreneur*, 20 Feb. 2014; www.entrepreneur.com/article/231658#.
9. D. Segal, "Eagle Scout. Idealist. Drug Trafficker," *New York Times*, 18 Jan. 2014; www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html.
10. "$2.7 Million-Worth of Bitcoin Stolen as Silk Road 2.0 is Hacked," *DailyMail*, 14 Feb. 2014; www.dailymail.co.uk/news/article-2559357/2-7-million-worth-Bitcoin-stolen-successor-dark-web-market-place-Silk-Road-hacked.html.
11. L. Kelion, "Cyber-Attack Disrupts Bitcoin Trades," British Broadcasting Corp, 12 Feb. 2014; www.samachar.com/Cyberattack-disrupts-Bitcoin-trades-ocqxTbgiajj.html.
12. M. Wheatly, "Mt. Gox at Death's Door? Bitcoin Price Slips Below $100, Before Rebounding Slightly," *Silicon Angle*, 21 Feb. 2014; http://siliconangle.com/blog/2014/02/21/mt-gox-at-deaths-door-bitcoin-price-slips-below-100-before-rebounding-slightly.
13. Y. Takemoto and S. Knight, "Mt. Gox Files for Bankruptcy, Hit with Lawsuit," Reuters, 28 Feb. 2014; www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228.
14. T. Mochizuki and K. Stech, "Mt. Gox Files for Liquidation", Wall Street Journal, 16 April 2014: http://online.wsj.com/news/articles/SB10001424052702303663604579504691512965308.
15. "Bitcoin Bank Flexcoin Shuts Down After Theft," Reuters, 4 Mar. 2013; www.reuters.com/article/2014/03/04/us-bitcoin-flexcoin-idUSBREA2329B20140304.
16. T. Mochizuki, "Japan Says Bitcoin Not A Currency, Government Also Says Commercial Banks Not Allowed To Provide Bitcoin As A Product," *Wall Street J.*, 6 Mar. 2014; http://Online.Wsj.Com/News/Articles/SB10001424052702303369904579423730757355014?Mg=Reno64-Wsj&Url=Http%3A%2F%2Fonline.Wsj.Com%2Farticle%2FSB10001424052702303369904579423730757355014.html.
17. Ingraham, Nathan, "Nine state regulators form Emerging Payments Task Force to Study Bitcoin," The Verge, Feb. 22, 2014: www.theverge.com/2014/2/22/5435202/nine-state-regulators-form-emerging-payments-task-force-to-study-bitcoin.
18. R. Arndt, "6 Big Questions About Bitcoin and the IRS," *Popular Mechanics*, 4 Apr. 2014; www.popularmechanics.com/technology/gadgets/news/6-big-questions-about-bitcoin-and-the-irs-16663447.
19. R. Wile, "Warren Buffett: 'Stay Away From Bitcoin. It's A Mirage,'" *Business Insider*, 14 Mar. 2014; www.businessinsider.com/warren-buffett-bitcoin-is-a-mirage-2014-3#ixzz2zAEMDK6n.
20. S. Duivestein and P. Savalle, "Bitcoin: It's the Platform, Not the Currency, Stupid!" *The Next Web*, 15 Feb. 2014; http://thenextweb.com/insider/2014/02/15/bitcoin-platform-currency
21. S. Melendez, "Could This 20-Year-Old Kid Make Bitcoin Obsolete?" *Fast Company*, 10 Feb. 2014; www.fastcolabs.com/3026271/could-this-20-year-old-kid-make-bitcoin-obsolete.

***George Hurlburt** is the chief scientist at* STEMCorp, *a non-profit corporation that works in the public sector to further economic development via adoption of network science to advance autonomous technologies as useful tools for human use. Contact him at ghurlburt@change-index.com.*

***Irena Bojanova** is a professor and program director of information and technology systems at the University of Maryland University College (UMUC). You can read her cloud computing blog at www.computer.org/portal/web/Irena-Bojanova. Contact her at irena.bojanova@umuc.edu.*