

© Tadeusz Ibram | Dreamstime.com

Might the Blockchain Outlive Bitcoin?

George Hurlburt, *STEMCorp*

Crypto-currency remains controversial. Bitcoin, a leading open source initiative to create an alternative form of currency, swirls at the center of this controversy. Bitcoin uses a brilliantly designed distributed ledger system, known as a *blockchain*. Validating blockchain transactions involves an eloquent mathematical hashing process, popularly called *mining*.

Where Does Crypto-Currency Stand?

The website <http://coinmarketcap.com> tracks crypto-currency market capitalizations and market trends:

- On 17 November 2013, the value of a Bitcoin peaked at US\$1,216.73 at the Mt. Gox exchange in Japan (<https://bitcoinhelp.net/know/more/price-chart-history>). According to coinmarketcap.com, on 14 August 2015, a single Bitcoin was valued at \$267.37; but by 21 January 2016, Bitcoin value climbed to \$416.93. By 5 February 2016, it was valued at \$388.59.
- On 14 August 2015, the website listed some 665 various types of available crypto-cur-

rencies, often called *altcoins*, for a total market capitalization of \$4,640,592,043. On that date, Bitcoin commanded 84 percent of this market capitalization and dominated with 89 percent in trade volume.

- On 21 January 2016, the market capitalization for the 658 listed altcoins had grown to \$6,945,858,793. Bitcoin had jumped to a 91 percent command of market capitalization, but trade volume had slipped to 86 percent.
- On 5 February 2016, the market capitalization for the 675 listed altcoins had shrunk by 3 percent to \$6,720,425,289. Bitcoin had a fallen to an 84 percent command on market valuation and maintained 92 percent by trade value.
- Of all of the altcoin offerings, 41 percent were not mineable by count, and 4 percent were not mineable by market capitalization value in January 2016.

At the moment, it appears that Bitcoin still has the edge in the crypto-currency field. In other terms, however, its viability teeters precipitously.

Blockchain advocates praise the lack of need for central governance, much less government regulation. Events, however, suggest that, lacking oversight, the quasi-anonymous bitcoin can and does breed illicit behavior:

- The former CEO of the then-troubled and now defunct Mt. Gox Bitcoin Exchange, Mark Karpeles, was arrested in Japan in August 2015, accused of \$387 million of theft in bitcoin valuation (www.aljazeera.com/news/2015/08/japan-arrests-mtgox-bitcoin-head-missing-387m-150801054245349.html).
- Ross Ulbricht, the Silk Road dark Web Bitcoin drug lord, was convicted in 2015. As soon as Silk Road was shut down, other bitcoin-based sites arose to sell illegal merchandise online.
- Two federal agents who tried to skim Bitcoin profits after Ulbricht's arrest were also indicted.¹
- Extortionists demanded Bitcoin payment from the hapless victims of the Ashley Madison infidelity site hack (<http://gizmodo.com/extortionists-are-after-the-ashley-madison-users-and-th-1725675204>).

JP Morgan and Bloomberg remain opposed to the very notion of crypto-currency. Nonetheless, a number of corporations began to embrace its use for business transactions during 2015:

- Firms such as Citi Corp, Goldman Sachs, Barclays, Overstock, and IBM have all announced initiatives surrounding crypto-currencies.
- Universal Air Travel Plan (UATP), an airline-owned payment network accepted by thousands of merchants for air, rail, hotel, and travel agencies, recently began accepting Bitcoin in payment for travel (www.economist.com/blogs/gulliver/2015/02/booking-flights-bitcoin).
- PayPal and Apple began accepting Bitcoin in 2015.

On the regulatory front, the reviews remain mixed, but lawmakers seemed to err on the side of caution in 2015. For example, the state of New York enacted legislation to open up the crypto-currency market for Bitcoin banking licensure. Unfortunately, the bill attached draconian requirements, including a separate license for each exchange service offered and complicated registration requirements. These rules forced many crypto-currency exchange entrepreneurs to suspended business in the state or to flee to other states. By some estimates, the state's rather modest \$5,000 registration fee could easily be offset by more than \$100,000 in requisite legal fees, depending on the size and scope of the firm.²

The international picture regarding Bitcoin regulation remained mixed in 2015:

- Russia is considering a total ban on Bitcoin.
- China and Brazil have defined rules on how crypto-currency,

particularly Bitcoin, shall be treated. At the same time, Bitcoin mining has become a growth industry in China.

- Australia is moving toward adopting Bitcoin as a currency.
- Other countries appear to be in a wait-and-see mode.
- Many countries, including the US, have declared Bitcoin taxable, while still not declaring it a currency per se.

Based on strong entrepreneurial movements fueled by aggressive venture capitalists, some speculate that the G7 nations will tend to eventually pave the regulatory way for digital crypto-currencies. If not, others speculate that developing nations in Africa, Latin America, and Asia will benefit, if the more developed nations exact too much restriction. Clearly, many of the world's regulatory bodies still remain in deliberation with regard to managing crypto-currency.³

Is Bitcoin Under Stress?

Leading Bitcoin developer Mike Hearn sold all of his Bitcoins in early 2016. In what has become a rift with fellow developers, he elected to move on, joining R3, a startup that exploits blockchain technology for business transactions. As he left, Hearn expressed serious concern over Bitcoin's long-term lack of efficiency and utility.⁴

Monopoly?

Like Bitcoin itself, the technology underlying it remains the subject of vigorous debate. The blockchain that chronicles all bitcoin transactions remains the heart of Bitcoin technology. A decentralized process known as mining establishes the veracity of all new blockchain links. This process uses a rigorous mathematical hash derived by competing miners, who use sophisticated computers to

verify the content of the new links before they are formally added to the blockchain.⁵

The ability to mine the blockchain is subject to inequities that favor monopolistic activities. Theoretically, the belief is that selfish miners will tend to band together in collusion and, through sheer force, will overtake the conventional miners who would need to join the selfish miner camp to survive. In such a scenario, monopolistic control is more likely. It was already the case that one mining node approached 51 percent of Bitcoin mining activity, which was prevented as a number of ethically minded miners left the group to get it back to size and prevent a monopolistic situation from occurring.⁶

While increasingly more powerful, some mining equipment can now be purchased via Walmart. Most mining equipment, however, falls into the corporate investment category for its sophistication. As Hearn alleged, miners in China have invested heavily in Bitcoin mining capability and now have the computational horsepower to monopolize Bitcoin.⁴

Transaction Rate

During 2015, Hearn led an initiative to change the size of the block as a way to hasten the verification process. The current block is limited to 1 Mbyte, allowing some rather anemic 300,000 transactions per day. In contrast, PayPal handles some 10 million transactions per day, while Visa handles 20,000 transactions per second. Hearn developed Bitcoin XT software as a way to increase block size and thus hasten processing speed to 24 transactions per second. By late 2015, 13 percent of the mining nodes had adopted Bitcoin XT. Once Bitcoin XT processes 75 percent of the links, the block size increases to 8 Mbytes and



Figure 1. Potential range of blockchain utility.

doubles every two years thereafter. Old-style miners would be pushed aside. This sparked fears that the validation process could grind to a halt, blocks would take far longer to resolve, the maximum bitcoin production could be reached way ahead of schedule, and the decrease in nodes could lead to more traditional and undesirable centrality of control. Hearn's critics warned of a failed initiative should enough bitcoin miners switch to Bitcoin XT.⁷ This disruptive fork, which represents a digression from the initial Bitcoin architecture, could wind up in a compromise that other developers have introduced—a more gradual approach known as Bitcoin Classic.⁴

Quasi Anonymous

Other critics note that the blockchain is, at best, semi-anonymous, in that the blockchain itself might be used mathematically to reveal the identity of the parties in any transaction. Others have established that, without specific protection, it is possible to link user

pseudonyms to the IP address where the transaction is generated for purposes of tracking parties involved in bitcoin transactions.⁸

End of the Line

In 2014, a successful miner earned 25 new bitcoins for each new 1-Mbyte block, averaging some 350 transactions successfully added to the blockchain. As the blockchain grows over time, the hashing algorithm, calibrated for 10-minute intervals from transaction time to the establishment of a new verified block, becomes more difficult. Finally, by design, bitcoin rewards diminish to zero after some 21 million bitcoins have been minted. This gives rise to the question of incentives to maintain the blockchain after the maximum number of bitcoins is attained, given that no new bitcoins will be minted. Ultimately, it could depend on the use of some form of transaction fees.⁹ Depending on how they're negotiated, such fees could suggest eventual centralization of this currently decentralized crypto-currency.

Where Might It All Lead?


Bitcoin as a crypto-currency clearly has both challengers and challenges. To truly appreciate the contribution of Bitcoin technology, however, perhaps one need look beyond the transactions that underlie crypto-currency. The blockchain, a means of accurately tracking any form of transaction, has significant value beyond the realm of monetary transfer. Some venture-backed firms are already working with transactions surrounding derivatives, bonds, loans, and contracts.¹⁰ Other startups are experimenting with many other types of transaction. In fact, blockchain utility can be traced to one or more startup firms working in each of the taxonomical elements shown in Figure 1. The figure defines four arbitrary areas of general endeavor with subdivisions within each.

Some have gone so far as to note that the Internet of Things (IoT)—or, perhaps better, the Internet of Anything (IoA)—would benefit the most from applied transaction blockchains. Comprising all manner of hardware-based sensors and their related actuators, the IoA was estimated to connect to some 9.8 billion devices in 2013, already exceeding the number of people residing on the planet (see Figure 2). It is envisioned that it will have connected 50 billion sensors by 2015. The IoA extends from wearable technology to vehicles, to homes, to public resources such as cities, roads, and shared infrastructure, to commerce, and even to broader industrial endeavors.¹¹

As sensors continue to multiply, the criticality of their interaction becomes increasingly important to preserve safety and security. Consider two autonomous vehicles approaching one another. It would be desirable

to have a record of the transactions between these vehicles as they safely pass one another or one stops to allow the other to pass. In another instance, the blockchain could also build a secure relationship between a car owner's key fob, the dealership, and the car itself. IBM is experimenting with a system called Adept that permits exchange among billions of interconnected devices using a blockchain approach.¹²

Unfortunately, new technology brings new challenges, and the adapted blockchain is a case in point. It is likely that services might be tracked by some specialized variations of the blockchain. An incentive for maintaining a decentralized pool of miners, however, represents a challenge. Miners would still need to be rewarded for their efforts, likely in some form of crypto-currency, even if the blockchain is not oriented around crypto-currency per se.¹³ Once again, the advantages of decentralization must be weighed against monopolistic behaviors in terms of efficiency and fairness.

Finally, the blockchain is not immune from malicious attack. Game-theoretic modeling establishes when mining pools are incentivized to attack other mining pools, thus significantly disrupting both short- and long-term equilibrium among miners.¹⁴ Before blockchains become a commonplace replacement for traditional transaction databases, strict standards, including acceptable behavioral guidelines, must be laid out. This more neatly fits a successful open source model in which infrastructure is served by a structured solution that has been thought through. 

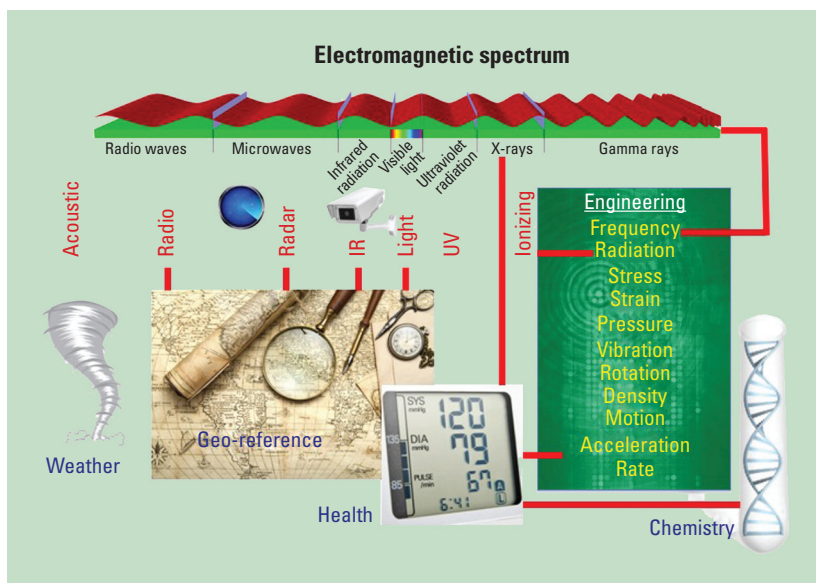


Figure 2. A sampling of the ubiquity of sensors feeding the Internet of Anything.

References

1. E. Perez, "2 Former Federal Agents Charged with Stealing Bitcoin During Silk Road Probe," *CNN*, 30 Mar. 2015; www.cnn.com/2015/03/30/politics/federal-agents-charged-with-stealing-bitcoin/.
2. D. Roberts, "Here's Why a Slew of Bitcoin Startups Fled New York This Week," *Fortune*, 14 Aug. 2015; <http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/>.
3. B.P. Eha, "How the World's Richest Nations Are Regulating Bitcoin," *Entrepreneur*, 7 Feb. 2014; www.entrepreneur.com/article/231294.
4. N. Popper, "A Bitcoin Believer's Crisis of Faith," *New York Times*, Dealbook blog, 14 Jan. 2016.
5. G. Hurlburt and I. Bojanova, "Bitcoin, Benefit or Curse?" *IT Professional*, vol. 16, no. 3, 2014, pp. 10–15.
6. I. Eyal and E. Gün Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," Dept. of Computer Science, Cornell Univ., Nov. 2015.
7. "Forking Hell: A Spat Between Programmers May Split Bitcoin," *The Economist*, 18 Aug. 2015; www.economist.com/news/business-and-finance/21661404-spat-between-developers-may-split-digital-currency-forking-hell.
8. A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of Clients in Bitcoin P2P Network," *Proc. 2014 ACM SIGSAC Conf. Computer and Communications Security*, 2014, pp. 15–29.
9. J. Kelleher, "What Is Bitcoin Mining?" *Forbes*, 8 May 2014; www.forbes.com/sites/investopedia/2014/05/08/what-is-bitcoin-mining/.
10. M. Leising, "Wall Street Embraces Blockchain as the Future," *Sidney Morning Herald*, 5 Aug. 2015; www.smh.com.au/business/markets/wall-street-embraces-blockchain-as-the-future-20150804-girpzo.html.
11. J. Parkinson, "IoT Mapped: The Emerging Landscape of Smart Things," *Venturebeat*, 23 Aug. 2015; <http://venturebeat.com/2015/08/23/iot-mapped-the-emerging-landscape-of-smart-things/>.
12. L. Greenemeier, "Bitcoin-Based Blockchain Breaks Out," *Scientific Am.*, 1 Apr. 2015; www.scientificamerican.com/article/bitcoin-based-blockchain-breaks-out/.
13. M. Orcutt, "The Most Valuable Aspect of Bitcoin: Its Versatile Ledger Technology," *MIT Technology Rev.*, 8 May 2015; www.mitre.org.

technologyreview.com/news/537246/why-bitcoin-could-be-much-more-than-a-currency/

14. A. Laska, B. Johnson, and J. Grossklags, "When Bitcoin Mining Pools Run Dry: A Game-Theoretic Analysis of the Long-Term Impact of Attacks Between Mining Pools,"

Financial Cryptography and Data Security, LNCS 8976, 2015, pp. 63–77.

George Hurlburt is the chief scientist at *STEMCorp*, a nonprofit 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.

cn Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.

CONFERENCES *in the Palm of Your Hand*

IEEE Computer Society's Conference Publishing Services (CPS) is now offering conference program mobile apps! Let your attendees have their conference schedule, conference information, and paper listings in the palm of their hands.

The conference program mobile app works for **Android** devices, **iPhone**, **iPad**, and the **Kindle Fire**.



For more information please contact cps@computer.org

