

Financial Technology**Blockchain Has Stolen Much of Bitcoin's Spotlight**

By Gregory Roberts

Feb. 22 — In the beginning, the buzz was all about bitcoin, the virtual currency that promised to revolutionize getting and spending on a global scale.

Now the spotlight shines on the blockchain, the recordkeeping software that underpins bitcoins and served as their *raison d'être*. Big companies such as IBM and JPMorgan Chase are scrambling to invest in blockchain

technology.

So what happens to bitcoin, the cryptocurrency that's easy to find depicted on the Internet — usually as a gleaming gold disk stamped with a symbol that combines a capital B and a dollar sign — but that no one has ever actually seen, felt or heard jingling in pocket or purse?

"I think bitcoin still has a very bright future," New York Law School Professor Houman Shadab told Bloomberg BNA, "but its growth and adoption may be slower than was predicted and hoped for."

James Angel, a business school professor at Georgetown University, told Bloomberg BNA, "I'm definitely a skeptic."

Angel said he has long believed that bitcoin will go the way of bitnet, a 1980s-vintage computer network eclipsed by the Internet.

Somewhere in between is David Sica, vice president of Nyca Partners LLC, a venture-capital firm concentrating on new technology in financial services.

"If you look at consumer payment ideas that have really done well, they solve a problem for which there was no other solution," Sica told Bloomberg BNA. "You need a content that's compelling enough."

Bitcoin isn't there yet, Sica said. "It also seems logical that if it doesn't find a legitimate use," he said, "it's going to go pure black-market."

Satoshi and the Byzantine Generals

The father of bitcoin is Satoshi Nakamoto — or maybe the mother, or the parents: the name is a pseudonym for a still-anonymous computer programmer or team of programmers. In 2009, Nakamoto made public the software that gave birth to the first bitcoins. That software created a blockchain, an electronic ledger that keeps a record of all bitcoin transactions since Day One.

Nakamoto's blockchain apparently solved what's called the Byzantine Generals' Problem. Drawing on an imaginary scenario involving multiple military commanders from the notoriously devious Byzantine Empire participating in the same campaign, the problem has to do with ensuring reliable and verifiable communications among people who are scattered geographically and who aren't all necessarily trustworthy — in short, the Internet.

Nakamoto's solution called for encrypting each message, or transaction, with each subsequent transaction encrypting the one before it — and with the record publicly available online. So the encryption for Transaction 2 would include an encryption of Transaction 1; the encryption of Transaction 3 would include an encryption of Transaction 2 (which already included an encryption of Transaction 1), and so on.

As transactions occur, they are bundled in blocks, and the blocks are posted online and attached to one another in sequence: the blockchain. Computer operators can examine each transaction and determine if it accurately reflects and incorporates the preceding transactions, meaning that any attempt to tamper with

BNA Snapshot

Development: Bitcoins may be losing their allure as investors focus on the cryptocurrency's running buddy, the blockchain.

Next Step: Businesses and institutions will try out blockchain variations and their potential to save time and money.

messages and alter the record would be detected.

Those examinations take time and they also take money, to pay for the advanced computer hardware required and the large amounts of electricity needed to power it. To provide an incentive for computer operators to perform the verifications necessary for entering transactions on the record, Nakamoto offered bitcoins.

The first bitcoins went to the original solvers of an invented cryptographic problem. The accumulation and movement of bitcoins online generated subsequent transactions entered in the blockchain, the verification of which generated additional bitcoins for the verifiers, with bitcoin accounts debited and credited in the system as the virtual currency changed hands — a process that goes on today. With the operation open to everyone across the Internet, the number of verifiers, or “miners,” is large and diverse enough to deter efforts at organized fraud.

Pizza and Fiat Currency

But what good are bitcoins? They exist only in cyberspace and lack any intrinsic value. And unlike U.S. dollars or Swiss francs or Japanese yen, no government pledges by declaration, or fiat, to honor them as a medium of exchange.

Any currency, crypto or otherwise, has value only to the extent that those who exchange it accord it value in the real world. The breakthrough for bitcoin, according to bitcoin lore, came in May 2010, when a bitcoin account-holder with the user ID laszlo offered in an online forum to transfer 10,000 bitcoins to anyone who would pay for the delivery of two large pizzas to his home in Jacksonville, Florida. Someone took him up on it, and bitcoins were worth something.

Since then, bitcoins have acquired more of the characteristics of familiar fiat currencies. There is a growing number of merchants who will accept bitcoins as direct payment for goods and services. There are consumer financial-services companies that will provide mobile wallets based on accounts denominated in bitcoins, with users transferring them around the world or translating them into fiat currencies for purchases at local stores via their smartphones. There are bitcoin currency exchanges: The 10,000 bitcoins laszlo spent to buy two pizzas in 2010 could fetch him about \$4.2 million today, and the exchange value of a single bitcoin peaked at close to \$1,000 in November 2013.

There have been bumps along the way. The volatility reflected in that peak-price spike in 2013 followed by a plunge to below \$220 in January 2015 scares away some potential users of bitcoins. There have been scandals, too. In 2013, the FBI shut down the Silk Road site on the “dark web” that was a locus for illegal drug sales, with bitcoins as the medium of exchange. In 2014, Mt. Gox, a Japanese bitcoin exchange that reportedly had controlled 70 percent of the global market, filed for bankruptcy and reported that 750,000 of its customers' bitcoins had gone missing.

Bitcoin boosters tout the speed, accessibility, anonymity and low transaction costs of the bitcoin network.

“It's not just some asset class that's super volatile and speculative,” Jason Leibowitz, a bitcoin investor who wrote a widely circulated primer on bitcoins, told Bloomberg BNA. “It's more of a problem-solver.”

One problem it solves, he said, is the difficulty of transferring money internationally, especially to people who lack connections to an established banking system, many of them living in developing countries. Anyone with a smartphone can tap into the online bitcoin network, he said.

“You now have a way to send, receive and store money essentially in the cloud,” he said.

Competitors Emerge

Bitcoin adopters worldwide number 5 million to 7 million, Leibowitz said. While that's a tiny slice of the global population of 7.4 billion, “when millions of people are using a decentralized new currency, it's worth taking note,” he said.

“It's already had a huge impact,” Campbell Harvey, a business school professor at Duke University, told Bloomberg BNA. “Even if bitcoin is not the dominant cryptocurrency in the future, no one can deny the substantial disruptive effect it's had.”

The website coinmarketcap.com lists more than 500 cryptocurrencies, each with its own blockchain variation, although bitcoins account for 85 percent of the currencies' collective value.

Harvey predicts that national central banks will follow the lead of the existing cryptocurrencies and issue

their own, fiat versions of them.

Bitcoin faces technical obstacles in terms of scaling up to function effectively in international finance and governance issues concerning who controls the system's protocols, Angel said.

But the bigger issue is competition from operators that are on sounder footing, even if they, too, are emerging, Angel said. Cellphone companies in Kenya have pioneered in developing mPesa, a fiat-currency mobile payment system utilized by the "unbanked." Venmo and other providers offer Internet-based money transfers. And firms such as Apple and PayPal are expanding into mobile wallets.

"At least in the short and medium term, bitcoin faces a lot of competition from alternative electronic payment methods," Shadab said.

One market niche bitcoin potentially could exploit is micropayments, amounting to less than a dollar online, Sica said. Those amounts, which are not cost-effective for existing payment systems to process, possibly could be handled by bitcoins, which involve little or no overhead and can be subdivided into tiny fractions. Applications could include payment for article views on news sites, or gratuities for favorite bloggers.

From Bitcoin to Blockchain

It's the concept of the blockchain that's firing recent interest from investors, who envision enormous savings in time and money via high-speed, low-cost, verifiable recordkeeping, for stock market settlements, currency transactions and myriad other applications that rely on accurate ledgers.

"Blockchains offer tremendous potential to improve financial services, as well as more broadly in the economy," Shadab said.

The bitcoin blockchain is the largest and most widely distributed, but it is not the only one. "There are many other blockchains that are possible that serve a different purpose," Harvey said.

Variations on the blockchain could adopt a proprietary governance structure, limit access and provide for different incentives for miners, such as payments for service, much as companies hire bookkeepers and accountants now.

"It's a generally accepted belief that Wall Street's infrastructure, and frankly, most large companies' infrastructure, is out of date." Sica said. "If you were to build it today, you would use new technology."

One piece of that new technology could be blockchain, at least potentially, Sica said: "It's still the early innings."

To contact the reporter on this story: Gregory Roberts in Washington at groberts@bna.com

To contact the editor responsible for this story: Mike Ferullo in Washington at mferullo@bna.com

Contact us at <http://www.bna.com/contact-us> or call 1-800-372-1033

ISSN 1526-5013

Copyright © 2016, The Bureau of National Affairs, Inc.. Reproduction or redistribution, in whole or in part, and in any form, without express written permission, is prohibited except as permitted by the BNA Copyright Policy.