KNOWLEDGE@WHARTON

FINANCE

Heads or Tails? What the Future Holds for Bitcoin and 'Altcoins'

Jul 09, 2014 North America

Has the shine worn off Bitcoin? The euphoria that greeted the cyber-currency last year, which drove prices from $13 to a high of more than $1,100, has given way to a more pragmatic view. Helping to cool down the fervor was the bankruptcy filing of Mt. Gox, once the largest Bitcoin exchange in the world. After getting hacked, the Tokyo-based firm lost a net 650,000 Bitcoins — worth $400 million at the market price of around $620 as of June 8, according to the CoinDesk Bitcoin Price Index. Two other major exchanges, BitStamp and BTC-e, were hacked as well and had to temporarily suspend transactions.

But fans such as venture capitalist Tim Draper are still enthusiastic about Bitcoin's prospects. Last week, Draper won the auction for the entire lot of nearly 30,000 Bitcoins seized by the government after closing down illegal drug site Silk Road. However, James Angel, a visiting finance professor at Wharton on leave from Georgetown University, believes venture capitalists mainly do not want to miss out on the next big tech trend. "When you talk to venture capitalists who are backing some of these ventures, they [are looking] at it like in the [early days of the] Internet — there's a revolution going on in the payment space, and this technology can be used for a lot of things other than crypto-money. So let's bankroll a couple of dozen different ventures, and one or two of them might pay off."

"The technology is brilliant," says Angel. "But not every elegant technology finds success in the marketplace." He points to the case of the Concorde supersonic jet, a technology that ultimately failed because of its economics. "So far, I haven't seen a value proposition [for Bitcoin] that makes me want to jump up and say, 'Yeah, this is going to work,'" Angel notes.

Bitcoin may be revolutionary, but it falls far short of being practical for most people. "Bitcoin has a lot of challenges it would need to overcome to become a part of the payment system," according to Angel. "It faces entrenched competition from other fiat currencies: the dollar, euro, yen and so forth." Indeed, there are many other payment options that would be easier and faster for consumers to use. Moreover, most hard currency is already electronic and therefore convenient to move around, he adds. A prime example is online banking. "The real question is, what does Bitcoin provide over other payment mechanisms?"

Angel predicts that Bitcoin eventually will be relegated to a niche in the world's financial systems — similar to Esperanto, a "politically neutral" language that was created in the late 19th century and which now exists on the fringes of linguistics. Bitcoin's inventor, Satoshi Nakamoto, designed the system to carry low fees and to allow users to stay virtually anonymous and shield transactions from political and regulatory manipulation. But this also exposes Bitcoin to several risks by allowing the currency to be abused for purposes such as drug trafficking and terrorist activity.

> **"Bitcoin has a lot of challenges it would need to overcome to become a part of the payment system."**
>
> –James Angel

But even Bitcoin cannot exist without being touched by traditional payment systems when it is exchanged in the real world. This is what Angel calls the "last mile" problem. For now, most people have to convert their hard currency into Bitcoin, transact in the cyber-currency and then re-convert it into hard currency. Not only does this add complexity, but also fees pile up in multiple transactions that negate any savings from the Bitcoin segment of the process. Using Bitcoin is the "cheapest part of the remittance. The problem is getting it into the electronic system and getting it out again at the other end," Angel says.

Transacting in the real world also attracts the increasing attention of regulators. Last week, the European Banking Authority recommended that financial institutions avoid virtual currencies until regulations to manage them are in place. In May, the U.S. Government Accountability Office (GAO) told Congress that closer collaboration among federal agencies is needed to ensure adequate consumer protection against cyber-currency risks. The IRS has also chimed in on the matter. In March, the agency said it would tax Bitcoin as property and require detailed recordkeeping and calculations.

Litecoin, Nxt and Darkcoin

While Bitcoin is getting much of the press, there actually are at least dozens of other cyber-currencies, according to the GAO. CoinMarketCap.com lists 363 so-called crypto-currencies. But Bitcoin remains the king. It is the most popular decentralized virtual currency in the world, with 12.6 million in circulation as of March 31, the GAO says. At a price of $620 apiece, the Bitcoin market is valued at $8 billion. Trailing way behind Bitcoin are Litecoin, Nxt, Darkcoin and Peercoin in the top five. Litecoin is trading at around $8 apiece and carries a market cap of around $230 million, while the rest fall off from there, according to CoinMarketCap.

Even as the largest, Bitcoin holdings remain miniscule compared to the $2.7 trillion in U.S. currency held by the public in the first quarter of this year, the GAO notes. Bitcoin transactions are tiny as well: Ranging from 29,000 to 102,000 daily in the past year compared to 44 million on

average processed each day by the Federal Reserve Banks. Many of these alternate cryto-currencies, or "altcoins," function similarly to Bitcoin, Angel says. Notably, Bitcoins are not physical coins but rather accounts in a virtual, public ledger. They are created when "miners" with computers compete to solve complex math problems and verify transactions in the ledger. The system is set up to yield only 21 million Bitcoins by 2040.

> **"It makes sense to have a fully digital, fully Internet-based mode of payment. It's not clear it can ever be a full substitute for [fiat] currency, but it certainly has potential."**
>
> — Nikolai Roussanov

Angel points to one cyber-currency, the Auroracoin created in Iceland, that he thinks is doing it right. "What they've basically done is the equivalent of Bank of America's mass credit card drops that launched the credit card industry," he says. The problem with adoption of payment systems is the "chicken and the egg" conundrum; you need people to use it, but enough merchants must accept it in order for them to do so. The Icelandic creators of Auroracoin got around this problem by giving everyone in the country some currency. At some point, they would all want to spend it. "If there's going to be a successful crypto-currency, there has to be mass buying by the population and the power structures," Angel notes.

Nikolai Roussanov, Wharton finance professor, nevertheless sees a limited role in the world for virtual currencies, especially in developed economies with established payment systems. "It makes sense to have a fully digital, fully Internet-based mode of payment," he says. "It's not clear it can ever be a full substitute for [fiat] currency, but it certainly has potential." If governments allow cyber-currencies to exist, there will likely be rules placed around them. "I can see a potentially viable crypto-currency being used in a somewhat more restricted way than we have now," he adds.

In the meantime, cyber-money would be more useful in countries with rampant inflation and stringent controls on money. "There is a demand by people to transact in a way that allows them to not necessarily pay the inflation tax that is effectively imposed by the combination of high inflation and capital controls," Roussanov notes. But then, crypto-currencies could be outlawed as well, as it has been in some nations. "We'll see," he says.

Bitcoin 2.0 and Beyond

David Yermack, finance and business transformation professor at New York University's Stern School of Business, notes that critical to the survival of a cyber-currency is government support. "I am skeptical that any form of money will be successful if it is not backed by a sovereign government. Without this sort of foundation, a currency really cannot be a form of property because it cannot be pledged as collateral, foreclosed upon, reassigned in bankruptcy and so forth," he says. "This will make it unattractive in a wide range of commercial settings."

> **"Governments can try to ban [Bitcoin], but unless they literally control every communication over the Internet, it seems impossible to prevent transactions."**
>
> –Ali Shourideh

In a recent working paper, Yermack wrote that Bitcoin does not behave like a currency according to criteria used by economists. Money should be a medium of exchange, a unit of account and a store of value. Bitcoin meets the first criterion because more merchants are accepting it as payment. But as a unit of account, it performs poorly because it requires businesses to quote prices to the fourth or fifth decimal place led by zeroes, which is impractical. Bitcoins also are quite volatile, with different exchanges quoting different prices without giving investors the ability to arbitrage. Finally, Bitcoin is a poor way to store value because it faces "rampant" hacking attacks and thefts, he points out. It also has virtually zero correlation to major currencies, so its value is "completely untethered" to them, making its risks "nearly impossible to hedge for businesses and customers and [rendering] it more or less useless as a tool for risk management," according to Yermack.

Then there are inherent flaws in the Bitcoin system itself. While the cyber-currency's proponents often crow about the lack of a regulatory body like a central bank controlling the supply of Bitcoins, Angel says that is largely a fallacy. "There are humans behind the Bitcoin protocol and miners to verify the transactions," he notes. "They're in control." It takes 51% of the miners in the network to set the standard, and mining pools are already being formed. That means these miners could amend the software to make more Bitcoins than the current ceiling of 21 million. "Do you trust them more than [Federal Reserve chairman] Janet Yellen?"

But the promise of "programmable" or "smart" money remains so alluring that it continues to fascinate Silicon Valley. For example, cyber-currencies can be programmed to be paid out only if certain conditions are met, such as when goods have been delivered to the buyer. In some applications, Bitcoins can be programmed to remove middlemen such as escrow companies from a transaction. Some quarters of the Bitcoin community have dubbed such applications as "Bitcoin 2.0," according to a recent story in *The Wall Street Journal*.

Angel suggests that the Fed and other central banks could create crypto-currencies based on their hard currencies to stay current with digital trends and still retain regulatory control. "The U.S. should do it to keep the dollar pre-eminent among the currencies of the world," he says. But even if governments do not join the bandwagon, it is too late to bottle up the idea of cyber-money. "Governments can try to ban it, but unless they literally control every communication over the Internet, it seems impossible to prevent transactions," notes Ali Shourideh, Wharton finance professor. If Bitcoin can somehow fix its perceived shortfalls, he adds, "it can claim to be one of the key financial innovations of our time."
