FBIC
Fung Business Intelligence Centre
GLOBAL RETAIL RESEARCH & INTELLIGENCE QUICK TAKE
FEBRUARY 3, 2015

IS BITCOIN'S BLOCKCHAIN THE NEW INTERNET?

- **As a currency and payment system, Bitcoin may be fatally flawed…**
- **… but its blockchain technology holds revolutionary potential**
- **IBM and Samsung unveil a blockchain-powered Internet of Things (IoT) at the 2015 Consumer Electronics Show (CES)**

DEBORAH WEINSWIG
EXECUTIVE DIRECTOR–HEAD GLOBAL RETAIL & TECHNOLOGY
FUNG BUSINESS INTELLIGENCE CENTRE
DEBORAHWEINSWIG@FUNG1937.COM NEW YORK: 646.839.7017

IS BITCOIN'S BLOCKCHAIN THE NEW INTERNET?

BITCOIN: THE GENESIS

On January 3, 2009, a mysterious figure (or group of figures) named Satoshi Nakamoto pushed a button and launched the world's first decentralized digital currency. An ingenious combination of cryptography, open-source software and a distributed public ledger to verify transactions, Bitcoin has been hailed by some as the future of money and derided by others as a dot-com-style investment scheme designed to line the pockets of early adopters. In its wake, the digital universe has been flooded with cryptocurrencies (roughly 500 at last count), many of which use Satoshi's code and protocol as a springboard.

Before Bitcoin, would-be developers of decentralized e-money foundered on the rocks of a dilemma known in computer science circles as the Byzantine Generals' Problem. Imagine that a group of generals are poised to attack a city, and know that they will succeed if at least half of them attack at the same time. However, they can only communicate by messenger, and there may be some traitorous generals who deliberately send fake messages. Without a central authority to coordinate them, how can they agree on a time of attack? In digital-currency terms, this problem can be restated as: How can a decentralized peer-to-peer network reach consensus on which transactions are valid, thus eliminating the possibility of counterfeiting and double spending?

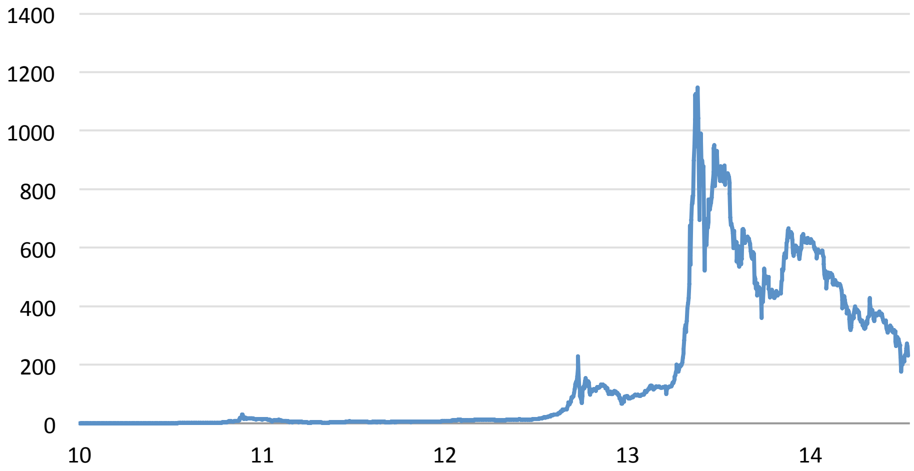
THE BLOCKCHAIN SOLUTION

Satoshi's solution was the so-called blockchain, a digital public ledger of every bitcoin transaction since the first ones were "mined" back in 2009. To put it simply, new bitcoin transactions are grouped together into "blocks" and then verified by volunteers in the peer-to-peer network who compete to solve a computationally intensive cryptographic problem. (The difficulty of the problem—which involves generating the correct target "hash," a string of letters and numbers that operates as a kind of digital fingerprint—is adjusted so that it generally takes about ten minutes to solve, regardless of the computer power thrown at it.) This is known as a proof-of-work system, as it is designed to ensure that a requisite amount of computer resources were used to complete a given task.

The first "miner" to solve the problem broadcasts it to the network. The block is then added to the chain of already verified and cryptographically sealed blocks. The miner is compensated with newly created bitcoins (currently 25, but set to decline by half every four years or so), which adds to the bitcoin money supply. The difficulty of the crypto problem means that faking a transaction would be virtually impossible unless one miner had more computing power than all the other miners combined. And copies of the complete blockchain ledger are spread across many nodes in the network, so that recordkeeping is no longer the responsibility of a single bookkeeper. (The transactions themselves use a private/public key encryption protocol that is also decentralized.)

In other words, Satoshi essentially created a fully distributed transaction processing engine, not only eliminating the need for a central authority but—even more radically—for a central server as well. A lot of people think this is a very big deal, and are overflowing with visions of blockchain technology as the key to everything from bankless banking to cloudless Internet of Things functionality. From that point of view, you could see bitcoin the currency (lower-case "b") as the first application of Bitcoin the technology (upper-case "B").

Figure 1. US Dollar Equivalent Value of Bitcoin



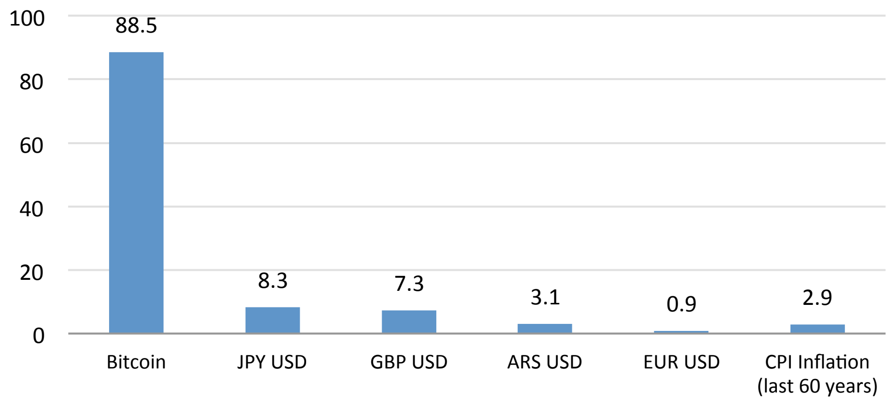
Through January 29, 2015
Source: CoinDesk.com

BITCOIN AS MONEY

The first vision of bitcoin was that it would offer a viable alternative to national "fiat" currencies. Aside from the minuscule size of its money supply (with a recent dollar value of around $3 billion, bitcoin represents only a fraction of the US M2 money supply of more than $11 trillion), the cryptocurrency must surmount some challenges before it can be considered a reliable unit of account or store of value, including:

- **Volatility.** The value of bitcoin has fluctuated wildly, partly because it has been treated mostly as a speculative asset and partly because the market is small and illiquid. In US dollar terms, bitcoin prices slid almost 60% in 2014 (and, according to PYMNTS.com, bitcoin was 48.1% more volatile than the Russian ruble). Bitcoin swooned again in January 2015, at one point losing roughly 36% of its value in a matter of days. One study pegged bitcoin's realized monthly volatility between May 2012 and May 2014 at 265% and its daily volatility at more than 200%. Annualized volatility has generally been around 90% (Figure 2), similar to that of a high-risk derivative or distressed equity. By contrast, typical emerging market currencies registered average volatilities of about 9% in the same period. Moreover, the fact that bitcoins do not seem to be correlated with other asset classes makes it virtually impossible to hedge against the risk.

Figure 2. 90-Day Volatility (%)



As of January 29, 2015
Source: Bloomberg

- **Uncertain legal status.** Bitcoin is currently suspended in a kind of legal no-man's land, as it is treated differently in virtually every nation in the world. Many countries simply ban all cryptocurrencies. Some just try to ring-fence them. In December 2013, China barred its financial institutions from dealing with bitcoin exchanges (possibly out of concern that citizens were using bitcoin to sneak wealth out of the country). Russia has begun to block bitcoin websites, which could be a prelude to a complete ban (the fear of which probably exacerbated the recent sell-off). More complicated is the tax situation. Last year, for example, the IRS declared that "virtual currency" like bitcoin will be treated as property for tax purposes. (It also stated that virtual currency derived from "mining" would be considered taxable gross income.) This could potentially result in confusing tax liabilities if the market value of a bitcoin is different when it used for payment that it was when received. In addition, bitcoin's widespread use in the criminal underworld is likely to inhibit its quest for legitimacy.

- **Lack of security.** While the blockchain has so far resisted attack, the same cannot be said of the infrastructure of third-party intermediaries that now surrounds bitcoin. This has not only introduced de facto centralization (as the bulk of transactions are now intermediated by a small number of exchanges and digital "wallet" services), but has increased the vulnerability of the Bitcoin system. The most notorious incident was the 2014 collapse of the largest bitcoin exchange, Mt. Gox, after the loss of 744,000 of its customers' bitcoins. Earlier this year, Bitstamp, another large exchange, briefly stopped trading after hackers made off with roughly 19,000 bitcoins. A follow-up to a 2013 study discovered that 45% of the exchanges originally examined had closed—and that 46% of the closed exchanges did not reimburse their customers after shutting their doors. Digital wallet companies (third parties that manage their customers' "wallets," software that holds bitcoins, addresses, and cryptographic keys) have also been compromised and are particularly tempting targets for cyber thieves. Ironically, bitcoin has given rise to an alternative banking system without the consumer protection or legal recourse that users of the mainstream system enjoy.

- **Miners face a capital crunch.** Rising bitcoin prices set off a spectacular mining arms race, and it now takes an immense amount of computing power to produce the winning "hash" in the required ten minutes. So bitcoin mining is now dominated by a handful of huge mining pools with tens of thousands of computers running hundreds of thousands of bitcoin-specific ASIC chips, which generally have to be replaced within four to five months. (A study in early 2014 estimated that bitcoin mining continuously consumes more than 100 megawatts of electricity, roughly 15% of the output of an average nuclear power plant.) But the collapse in bitcoin prices has made covering operational costs increasingly difficult and recently forced several miners to suspend operations. While the difficulty of the computational task is supposed to ease if miners start backing away, a sustained collapse in prices could threaten the mining infrastructure. (This also raises the question of how to incentivize participants in the Bitcoin network to verify transactions once bitcoin issuance comes to a halt.)
- **Inelastic supply.** The number of new bitcoins created per verified block is set to decrease at an exponential rate until the supply hits 21 million in around 2140. If it were the money supply of an actual sovereign state, this would be severely deflationary. As bitcoin is not a real money supply, it's difficult to understand the purpose of this constraint, if not to engineer an upward price squeeze. In practice, particularly if bitcoin remains a kind of token for transferring value, there will likely be little reason for not switching to another cryptocurrency or token.

Bitcoin:
Market Participants

- Miners
- Bitcoin exchanges and online wallet services (e.g. BitStamp, CoinBase)
- Companies accepting Bitcoin
  - Overstock, Wordpress, TigerDirect, etc.

Conventional Currency:
Market Participants

- Central banks
- Commercial banks
- Deposit insurance
- Financial regulatory authorities
- Payment services (e.g., Visa, PayPal)
- Auditing and consultancies
- All companies

BITCOIN AS A PAYMENT SYSTEM

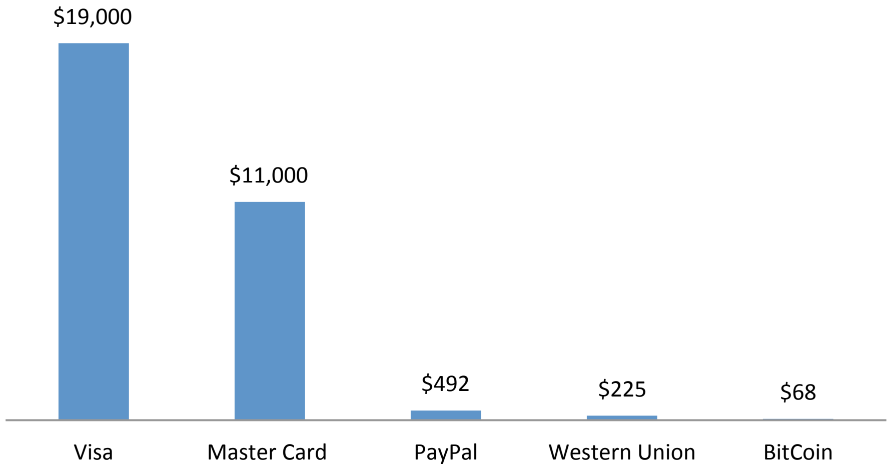
What about bitcoin as a payment system? While the Bitcoin economy has come a long way from its humble beginnings, it is far from reaching critical mass. For one thing, it hasn't exhibited the growth characteristics typical of successful payment systems. A 2014 study comparing bitcoin with M-Pesa, a payment system started in Kenya, found that bitcoin's adoption rate was less than one-twentieth as rapid. Moreover, the system is designed to handle seven transactions per second, whereas Visa handles about 10,000 per second (and has the capacity to handle as many as 47,000). Bitcoin transactions have been hovering at around 90,000 per day, versus about 21 million per day for Visa. (Remember that the bitcoin number covers all kinds of transactions, including buying and selling bitcoins, transferring bitcoins from one "wallet" to another, online gambling and criminal activity.) It's also worth noting that a 2014 Federal Reserve analysis suggested that fewer than 50% of all bitcoins in circulation are used in transactions, and about half of those involve values of less than $100.

Let's look at this issue from the perspectives of consumers and merchants:

- **Consumers.** Bitcoin probably wouldn't appeal to everyday consumers unless they were committed to the underlying philosophy. Transactions are anonymous (actually pseudonymous), but that attribute seems mostly attractive to criminals, such as the alleged Silk Road mastermind currently on trial in New York City. (Silk Road was an online black market shut down in 2013; its successor Silk Road 2.0 was busted in November 2014. Both of these markets operated solely with bitcoins.) There is no fraud protection (so the consumer, not the merchant, eats the cost of any loss) and transactions are irreversible (there are no cancellations or refunds). Moreover, as a 2014 Harvard Business School working paper pointed out, foregoing the rebates or cash-back bonuses offered by most credit cards could make bitcoin purchases a bad value for a lot of consumers. And if you lose the private key to one of the addresses in your wallet, or send a payment to a wrong address, the associated bitcoins are lost forever. The bitcoin system is also relatively inefficient, as it takes at least ten minutes to verify a bitcoin transaction (and one hour for the transaction to be considered finalized), whereas credit card verifications are virtually instantaneous. Finally, while paying transaction fees is considered "voluntary," miners routinely delay confirmation of no-fee or low-fee transactions.

- **Merchants.** The incentives for merchants are a lot clearer. First, most businesses that claim to accept bitcoins actually route buyers through a third-party processor like Coinbase, which converts bitcoins to dollars (for example) at an exchange rate and credits the merchant's account in dollars. But the fees are lower than what credit card companies demand (generally around 1%). In addition, there are no chargebacks, so the consumer's loss is the merchant's gain. Given bitcoin's price instability, prices are generally listed in the dominant currency, and some kind of frequently updated exchange rate is provided. (Overstock.com, for instance, lists the associated dollar price and updates the bitcoin prices every ten minutes.) So far, available evidence suggests that accepting bitcoins provides a public-relations bump, but not any significant additional sales beyond the first influx of bitcoin faithful.

Figure 3. Daily Transaction Volume (Millions of US Dollars)



Through December 31, 2013
Source: Fitch, company filings, blockchain.info, CoinDesk

WELCOME TO THE BLOCKCHAIN: LIFE BEYOND BITCOIN

While the media's attention remains focused on the ups and downs of bitcoin prices, Satoshi's real big invention—not a new kind of money, but a fully distributed transaction processing engine—is already beginning to find its way into new business models targeting areas such as property exchange, smart contracts, decentralized payment processing and even a new domain-name system for the Web.

Perhaps most intriguing is IBM's new "ADEPT" project (in collaboration with Samsung), which envisions using blockchain tech as the basis for building a robust platform for the Internet of Things. As Paul Brody , who spearheaded that project, put it in an October 2014 interview with *CoinDesk*, "I think that demand for the blockchain technology—the programmable ledger, autonomous distributed system—is going to be colossal."

There are people who view the blockchain as a uniquely powerful and adaptive platform that could serve as a foundation for a whole range of products and services, including decentralized apps. These visionaries see blockchain tech as a new value exchange protocol, and compare it to the Transmission Control Protocol/Internet Protocol (TCP/IP) communications architecture that underlies the current Internet. For now, it's best to remember that the blockchain is just a distributed public ledger, which makes it ideal for the registry and transfer of digital assets. A key concept in this new area is the idea of a "smart contract," a transaction that occurs only when certain real-world conditions are met (such as the delivery of a product by a supplier).

IBM AND SAMSUNG SEE THE BLOCKCHAIN AS THE IOT BACKBONE

As the Internet of Things starts to become more of a reality, it makes sense that blockchain tech would be seen as a better way to create a functioning distributed network, particularly as running a plethora of interconnected devices through central cloud servers is expensive, insecure and unwieldy. That's why IBM (in collaboration with Samsung) created its ADEPT system. (ADEPT is an acronym for Autonomous Decentralized Peer-to-Peer Telemetry.) The problems for IoT have always been maintaining a network of devices or appliances over the long run (who's going to ensure that your smart washer stays smart for 10 years?) and making the data collected secure if it all ends up on a central server.

As Paul Brody told *CoinDesk* back in October (Brody was an IBM VP and the North American leader for mobile and IoT; he recently left the company):

"As devices become smarter and smarter, why shouldn't they be able to manage themselves? The blockchain allows you to run a totally distributed platform. And by our calculation, if you use the blockchain, you can cut the cost of managing a high-volume device by 99%."

IBM and Samsung formally unveiled their prototype ADEPT network at the 2015 Consumer Electronics Show (CES) in Las Vegas. For the backbone of the system, they are working with: 1) nonprofit start-up Ethereum, which is building a non-Bitcoin blockchain-based platform for smart contracts supported by a new flexible programming language; 2) telehash, which provides P2P messaging and data transfer via mesh networking; and 3) BitTorrent, the file-sharing protocol. In a recently released white paper draft, IBM shared its vision of the blockchain-based ADEPT system as a kind of "ledger of existence" that would allow for decentralized transactions between billions of devices.

To quote from the paper:

"Applying the blockchain concept to the world of IoT offers fascinating possibilities. Right from the time a product completes final assembly, it can be registered by the manufacturer into a universal blockchain, representing its beginning of life. Once sold, a dealer or end customer can register it to a regional blockchain (a community, city, or state)."

The CES demonstration involved a Samsung washing machine that can use smart contracts to order and pay for detergent from a supplier (with the receipt sent to the owner's phone), perform its own maintenance, and potentially regulate its own water and power supplies. The authors of the white paper also hope that using ADEPT will allow the washer to negotiate "with other peer devices both in the home and outside to optimize its environment." And they note that all of this occurs "without a central controller."

At the moment, there is no clear way to implement this protocol on a broad enough scale to fulfill the ambitious vision sketched out in the white paper. (For one thing, Ethereum hasn't officially launched its platform yet, and it remains to be seen how scalable it is.) But this bold rethinking of IoT architecture does suggest that the promise of blockchain technology goes way beyond creating a handful of cryptocurrencies.

Deborah Weinswig, CPA
Executive Director – Head Global Retail and Technology
Fung Business Intelligence Centre Global (FBIC Global)
New York: 917.655.6790
Hong Kong: +852 6119 1779
deborahweinswig@fung1937.com

Marie Driscoll, CFA
mariedriscoll@fung1937.com

Christine Haggerty
christinehaggerty@fung1937.com

John Harmon, CFA
johnharmon@fung1937.com

Amy Hedrick
amyhedrick@fung1937.com

John Mercer
johnmercer@fung1937.com

Lan Rosengard
lanrosengard@fung1937.com

Jing Wang
jingwang@fung1937.com