

There Are Two Sides to Every Coin—Even to the Bitcoin, a Virtual Currency

By Maria A. Arias and Yongseok Shin

Until recently, the popularity of the virtual currency bitcoin had largely been confined to the tech circles. It started to grab the attention of the mainstream media as its value against the U.S. dollar gyrated wildly earlier this year (see figure), fueled by speculative trades by several hedge funds. Today, bitcoins are more widely accepted and circulated than ever, often aiding illicit transactions. In this article, we describe the unique features of the bitcoin and explain how it works.

What Is Bitcoin?

Bitcoin is a decentralized virtual currency that uses a peer-to-peer consensus system to confirm and verify transactions. The Bitcoin network was designed and launched in January 2009 by an anonymous programmer (or a group of programmers) under the pseudonym of “Satoshi Nakamoto,” based on the concept of open-source cryptocurrency¹ described by cryptographer Wei Dai in 1998.

Central to Bitcoin is its independence from any institution or government, allowing any interested parties to engage in a direct monetary transaction at a low cost. Instead of trusting a financial intermediary to mediate and confirm a transaction, all valid transactions are encrypted into a single agreed-upon history or ledger of transactions. This effectively precludes anyone’s attempts to spend the same coin multiple times or to create counterfeit bitcoins.

How It Works

Without having a central authority or clearinghouse, pending transactions and money distributions are verified through network consensus. In short, pending transactions are

broadcast publicly in chronological order and are bundled into blocks. Individuals in the network devote computing power to decode the encrypted transactions (akin to solving a cryptographic puzzle) and verify that blocks contain only valid transactions. As blocks are confirmed, they are added to the network’s public ledger, called the “block chain.” The network verification requires that the majority of CPU power in the Bitcoin network deem the transaction to be valid.

The time stamp added to every transaction and the proof-of-work required to confirm

Central to Bitcoin is its independence from any institution or government, allowing any interested parties to engage in a direct monetary transaction at a low cost.

each block enhance the network’s security. Transactions are irreversible, as they cannot be changed once they are included in the block chain and other blocks are confirmed after it. If there are two competing block chains, the longer one is accepted to be the legitimate one. If an “attacker” wants to change a previous transaction or wants to insert an illegitimate one to the block chain, he or she would need an unrealistic amount of computing power to reproduce all the blocks including the said transaction and all those that came after, and to generate longer

block chains at a faster rate than all the other CPUs on the network. The probability of a successful attack to the Bitcoin network is virtually zero. (There have been breaches into providers of Bitcoin-related services—e.g., those that exchange bitcoins into real-world currencies or those that manage clients’ Bitcoin accounts.² However, such attacks are no more an attack on the Bitcoin network than a stickup at a grocery store is an attack on the food-supply chain.)

Mining a Predetermined Supply

The supply of bitcoins is increased by a preset amount each time a block is added to the block chain. These new bitcoins, as well as a small fee charged from the transactions that were confirmed within the block, are awarded to the individual who solved the cryptographic puzzle as an incentive for transactions to be confirmed and for the individuals to work in the network’s favor. This process of obtaining new bitcoins is called mining, and those who devote their computing resources to the process are called miners.

The rate at which the supply of bitcoins grows is hard-wired into the system. The difficulty of the puzzles is programmed to respond to the increase in the number of miners and the computing power in the network so that the amount of newly mined bitcoins halves roughly every four years. At this expansion schedule, the supply of bitcoins will reach its programmed limit of about 21 million bitcoins by the year 2140. Once the maximum supply of bitcoins is reached, the only incentive for miners is the fees collected from confirmed transactions, which are expected to increase as the number of users and, hence, the number of transactions to be confirmed increase.

Storage and Anonymity

One does not have to be a miner to obtain and spend bitcoins. Indeed, many bitcoin users simply purchase them at one of the competing online bitcoin exchanges. Anonymity and privacy are readily granted to all users since they can create unlimited Bitcoin accounts without having to validate their true identity. Bitcoin account information is stored in digital wallets that can be downloaded as software on a computer or on a smartphone; the wallets can be encrypted to keep their contents secure. The wallet contains private keys (or cryptographic signatures) linked to each of the user's Bitcoin account addresses. Nonetheless, transactions can be traced back and forth through the block chain, and account balances are public; so, it is up to the user to avoid revealing any information that can link a Bitcoin account to his or her true identity.³

Utopian Virtual Currency or Vehicle of Speculative Investment?

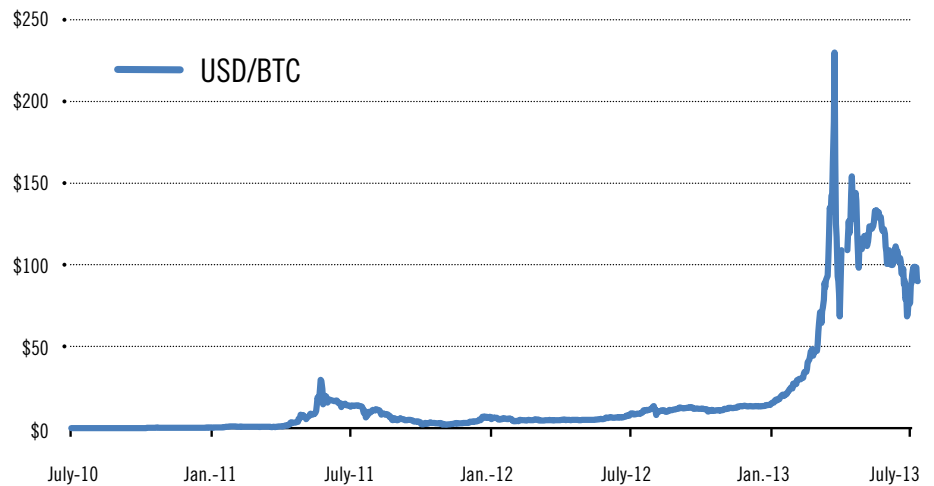
Two of Bitcoin's most distinctive properties are what have made it popular: (i) its supply is dictated by a pre-programmed mathematical formula that is thought to be impervious to politics or human error; and (ii) it allows for total anonymity/privacy in transactions.

The former particularly appeals to those who are afraid that the massive monetary easing by the world's central banks in the wake of the 2008 financial crisis would unleash hyperinflationary forces and devalue the purchasing power of fiat currencies. The latter appeals not only to those who intend to engage in illicit purchases of recreational drugs and weapons,⁴ but also to those who value discretion and privacy on the Internet. (Most bitcoin-friendly businesses operate online, but there now are a small but growing number of offline retailers that accept bitcoins, especially in California and New York.) Ultimately, users trust bitcoins will hold value and serve as a low-cost medium of transaction.

The present reality of Bitcoin is not as idyllic as its enthusiasts might acknowledge. The feared hyperinflation never materialized in the U.S.—the price level has remained relatively stable during the past five years. On the other hand, the bitcoin's value (measured as U.S. dollars per bitcoin in the figure) has been anything but stable. One bitcoin was worth about \$20 in the beginning of 2013,

FIGURE 1


U.S. Dollar Value of 1 Bitcoin



SOURCE: Mt. Gox Exchange.

Two of Bitcoin's most distinctive properties are what have made it popular: (i) its supply is dictated by a pre-programmed mathematical formula that is thought to be impervious to politics or human error; and (ii) it allows for total anonymity/privacy in transactions.

but its value skyrocketed to \$230 in April (an enormous deflation when prices are measured in bitcoin units) and then crashed back and settled in July at about \$100. The increase in value might have been good for those who had acquired bitcoins as a form of investment, but the volatility in its value (or purchasing power) makes it a poor choice as a store of value. In addition, the speculation on bitcoins, especially when coupled with their fixed supply in the long run, will curtail their usefulness as a medium of exchange. People may hoard bitcoins (instead of spending and circulating them), expecting their value would continue to increase. After all, nobody *has* to spend bitcoins since they can pay with the U.S. dollar.

Furthermore, concerns about the virtual currency's potential uses for criminal transactions and money laundering have been brought up by regulators, with the U.S. Treasury's Financial Crimes Enforcement Network being one of the first agencies to address the issue. It released guidance on regulatory responsibilities that money business services must abide by, including the requirement to register and report certain information to the bureau to avoid money laundering.⁵ However, Bitcoin presents a unique challenge for the regulatory agencies: There is no single central entity responsible for Bitcoin, nor is the network located somewhere; it is just a virtual network accessed by individuals throughout the world who use their computing power to solve complex cryptographic puzzles to manage transactions and mine coins. At the time of this writing, the U.S. regulators seem to focus on the intermediaries and exchanges that serve as the front-end of the Bitcoin network for the nonmining users. Only time will tell whether this is the beginning of the demise of Bitcoin. 

Yongseok Shin is an economist and Maria A. Arias is a research analyst, both at the Federal Reserve Bank of St. Louis. For more on Shin's work, see <http://research.stlouisfed.org/econ/shin>.

Bitcoin Essentials

Bitcoin works just like cash. Bitcoins can be bought or sold in currency exchanges, Mt. Gox being the most commonly used one.

Bitcoins can serve as payment for products or services at a growing number of businesses. A transaction is made by “sending” bitcoins to the address of the account to be credited. Once a transaction is made, it is broadcast publicly among the network, which is composed of individuals, known as “miners,” who devote computing power to decode the transactions.

These transactions are “pending” until the majority of the network verifies they are valid—just as a central authority would verify a banking transaction before it is confirmed. Then, the verified block is posted to the public block chain, and the network starts to decode the next transaction block.

To enhance anonymity, users are encouraged to create new addresses for each transaction to be received, yet the public block chain and account balances can be traced to link accounts and users.

ENDNOTES

- ¹ See www.weidai.com/bmoney.txt.
- ² See www.npr.org/blogs/money/2011/08/24/138673630/what-is-bitcoin-and www.npr.org/blogs/money/2011/06/21/137324088/the-bitcoin-mess for examples of attacks on third-party service providers.
- ³ Meiklejohn et al show that in some instances users—individuals and institutions that transact in bitcoins—could be identified by “clustering” public account records and transactions through the block chain.
- ⁴ See <http://bitcoinmagazine.com/the-silk-road-report/> and <http://gawker.com/5808314/everyone-wants-bitcoins-after-learning-they-can-buy-drugs-with-them>.
- ⁵ Money business services include businesses that deal or exchange currency, transmit money, and process money orders or checks. To quote the Financial Crimes Enforcement Network: “The guidance is in response to questions raised by financial institutions, law enforcement, and regulators concerning persons who use convertible virtual currencies or make a business out of exchanging, accepting, and transmitting them. ... MBSs [money business services] have registration requirements and a range of anti-money laundering, recordkeeping, and reporting responsibilities under Financial Crimes Enforcement Network’s regulations.”

REFERENCES

- Financial Crimes Enforcement Network. “FinCen Issues Guidance on Virtual Currencies and Regulatory Responsibilities.” Press Release. March 18, 2013. See www.fincen.gov/news_room/nr/pdf/20130318.pdf.
- Greenberg, Andy. “Follow the Bitcoins: How We Got Busted Buying Drugs on Silk Road’s Black Market.” *Forbes*, Sept. 5, 2013. See www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/.
- Meiklejohn, Sarah; Pomarole, Marjori; Jordan, Grant; Levchenko, Kirill; McCoy, Damon; Voelker, Geoffrey; and Savage, Stefan M. “A Fistful of Bitcoins: Characterizing Payments among Men with No Names.” Proceedings of the ACM Internet Measurement Conference, Barcelona, Spain, October 2013.
- Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” 2008. See <http://bitcoin.org/bitcoin.pdf>.