

Bitcoin Versus Electronic Money

Bitcoin has had a volatile journey since it was launched in 2009, attracting attention among conventional investors as well as the black market. Regulators and policy makers are also following Bitcoin, raising the occasional eyebrow as they evaluate Bitcoin's risks and benefits and how to regulate this little understood virtual currency. Some media reports have confused Bitcoin with more popular electronic money (e-money) schemes used in many low-income countries to reach the unbanked. But the two are markedly different and should not be conflated. This Brief provides information about Bitcoin and contrasts Bitcoin with e-money to avoid alarm about the former to the detriment of the latter.

Virtual Currency

One way to comprehend virtual currency is to first understand fiat currency. Fiat currency is any legal tender designated and issued by a central authority that people are willing to accept in exchange for goods and services because it is backed by regulation and because they trust this central authority. Fiat money is similar to commodity-backed money in appearance and usage, but differs in that it cannot be redeemed for a commodity, such as gold (European Central Bank 2012).¹

By contrast, virtual currency is "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community." Although there are different types of virtual currencies (European Central Bank 2012), this Brief will focus on virtual currencies with "bidirectional flow" since these currencies intersect most directly with the real economy. Virtual currencies with bidirectional flow may be bought and sold according to prevailing exchange rates and may be used to purchase both real and virtual goods and services.

Bitcoin

Bitcoin was launched in 2009 as an alternative to fiat currencies by an unknown computer scientist using the pseudonym Satoshi Nakamoto (n.d.). Bitcoins are not printed like fiat money, but instead are "mined" using computing power in a distributed global network of volunteer software developers. At its core, Bitcoin is nothing more than a digital file that lists every transaction that has ever happened in the network in its version of a general ledger called the "block chain." Bitcoin

is the first example of a growing category of money known as cryptocurrency in which open-source software solves complex mathematical calculations to mine more Bitcoins (Coin Desk 2013a). These "miners" make the Bitcoin network function by validating transactions and thereby creating new Bitcoins. This occurs when the Bitcoin network collects all the transactions made during a set period of time (usually every 10 minutes) into a list called a "block." Miners confirm these blocks of transactions and write them into the block chain by competing against each other to solve mathematical calculations. Every time a miner's system finds a solution that validates a block of transactions, that miner is awarded 25 Bitcoins (Coin Desk 2013b). Every four years, this reward is halved so that the total number of Bitcoins will never exceed 21 million.²

For a new user not interested in the mining process, the most popular way to obtain Bitcoins is through a traditional exchange where fiat currency is converted into Bitcoins and then stored in a Bitcoin wallet. Wallets come in many forms, including desktop access, mobile access, and online web-based access. Each has its own risks as both desktop and mobile access are susceptible to hackers, a hard drive crash, or a lost mobile device. Online access uses third parties that may also be hacked, cheat its users, or go bankrupt (Lee 2013).

Bitcoin wallets hold the digital private encryption keys, or secret codes, needed to carry out Bitcoin transactions. Let's say Person A wants to send five Bitcoins to Person B. Person A uses a private key to sign a message with the input (the Bitcoin address used to send Bitcoins to Person A in the first place), the amount (five Bitcoins), and the output (Person B's Bitcoin address). Person A sends this message

1 European Central Bank (2012) provides an excellent overview of virtual currencies, including two case studies on Bitcoin and Second Life's Linden Dollars.
 2 There are 210,000 10-minute increments over four years; therefore, the award is halved after 210,000 blocks have been written into the block chain. During the first four years of the Bitcoin network when the reward was 50 Bitcoins, 10.5 million Bitcoins were created (210,000 multiplied by 50 Bitcoins).

from Person's A Bitcoin wallet into the wider Bitcoin network from where miners verify the transaction once it becomes part of a block by solving a mathematical calculation (CoinDesk 2013c). The mathematical component of the system is important to prevent fraud by ensuring that a person cannot use the same Bitcoin for multiple transactions.

Bitcoin differs from fiat currency in the following key ways:

1. It is decentralized. Bitcoin is based on a decentralized, peer-to-peer network that does not have a central clearing house or any other intermediary. No single institution controls the Bitcoin network like a central bank does with fiat currency. Every machine that mines Bitcoins and processes transactions makes up a part of the network.
2. It is not inflationary. Unlike fiat currency, which can be printed to create more supply, Bitcoin was designed to have a maximum number of coins. Only 21 million will ever be created according to a predetermined algorithm. There are about 12 million Bitcoins currently in existence (Lee 2013). This represents 57 percent of all the Bitcoins that will ever be created, and by 2017, 75 percent will have been created. The last Bitcoin will be mined in 2140 (Hern 2013).
3. It is anonymous, sort of. Users can hold multiple public Bitcoin addresses, but they are not linked to names, physical addresses, or other identifying information. However, as discussed below, recent regulation of exchanges has made it more difficult to retain the anonymous aspect of Bitcoin. Researchers have also found ways to track transactions of public

addresses, but it is still difficult to link a public address to a person's identity.

4. It is transparent. Although Bitcoin transactions are somewhat anonymous, they are also transparent. Bitcoins are really only records of Bitcoin transactions between different addresses making up the block chain. Everyone on the network can see how many Bitcoins are stored at each public Bitcoin address, but they cannot easily identify to whom the address belongs.
5. It is irrevocable. There is no way to chargeback a Bitcoin transaction unless the recipient actually sends the coins back to the sender.

Bitcoin versus E-Money

E-money is commonly defined as value (i) stored electronically, (ii) issued on receipt of funds of an amount not less in value than the monetary value issued, and (iii) accepted as a means of payment by parties other than the issuer.³ In e-money schemes, the link between e-money and fiat currency against which it is issued remains intact, as funds are expressed in units of that currency (U.S. dollar [USD], Euro [EUR], Kenyan shilling [KES], etc.). In virtual currency schemes, by contrast, the unit of account has no physical fiat currency counterpart (European Central Bank 2012). See Table 1 for more information.

Aside from being digital in format, there are few similarities between Bitcoin and e-money. E-money, like many other digital forms of fiat currency, such as credit and debit cards, PayPal, and wire transfers, is simply one mechanism by which to interact with

Table 1. Comparison between e-money and Bitcoin

	E-Money	Bitcoin
Format	Digital	Digital
Unit of account	Fiat currencies (USD, EUR, KES)	Bitcoins (BTC)
Customer identification	Financial Action Task Force (FATF) standards apply for customer identification (though such standards permit simplified measures for lower risk financial products)	Anonymous
Means of production	Digitally issued against fiat currency of central authority	Mined/mathematically generated
Issuer	Legally established e-money issuer (which may be a financial institution)	Community of people/miners

Source: Adapted from European Central Bank (2012).

³ The European Commission Electronic Money Directive (2009/110/EC). http://ec.europa.eu/internal_market/payments/emoney/text/index_en.htm

that fiat currency. To mitigate against systemic and consumer protection risks, the cash against which e-money is issued typically must be deposited with fully prudentially regulated financial institutions (Tarazi and Breloff 2010). In contrast to Bitcoin, e-money is not a separate currency and is overseen by the same central authority as the underlying national currency. Confusion between the two may have arisen recently from a news story that inaccurately associated Bitcoin with M-PESA, the mobile payments service used by over 11 million customers in Kenya popular for its potential to provide financial services to the financially excluded.⁴

Risks

The abstract nature of Bitcoin poses a challenge to regulators. Like any form of monetary value, including cash, e-money, and credit cards, Bitcoin can be used for both legitimate and illicit purposes. The question is whether Bitcoin makes it easier for criminals to funnel money for illicit purposes, and how regulators should respond to these perceived or real risks.

Much of this discussion came to a head with the recent crackdown of Silk Road, an underground market launched in January 2011 that accepted Bitcoins exclusively for the purchase of illicit goods and services. With the double layer of anonymity created by Bitcoin and the Tor browsing system used by Silk Road, money on the Silk Road site was almost untraceable. Nevertheless, the U.S. Federal Bureau of Investigation was able to finally track down the founder of Silk Road in October 2013 (Time 2013). By the time it was shut down, Silk Road had processed sales totaling more than 9.5 million Bitcoins, worth about \$1.2 billion.⁵

Regulators in the United States have begun to take notice of the increasing use of Bitcoin. The Financial Crimes Enforcement Network (FinCEN), the Financial Intelligence Unit within the U.S. Treasury Department that focuses on all anti-money laundering (AML) and combatting the financing of terrorism (CFT) regulation, issued guidance in March 2013 defining the circumstances under which virtual currency users could be categorized as a money transmitting business (MTBs) (FinCEN 2013). Since MTBs must enforce AML

controls, this was an important step in addressing the risks presented by the anonymity of virtual currencies.

Silk Road aside, the biggest current risk of Bitcoin is uncertainty surrounding its future, which depends largely on the number of active users and accepting merchants. Since Bitcoins cannot currently be used to purchase many things directly,⁶ most users and merchants will convert them back into a fiat currency of choice. Conversion from fiat currency to Bitcoin and back again most regularly happens using an exchange. If exchanges begin to be more systematically regulated, as they are in the United States, then their use can be more closely monitored and controlled (Hoskinson 2013). Bitcoin users, however, can transact, buy, and sell outside of these exchanges, so not everyone will be monitored. The global nature of the Bitcoin network also needs to be considered. Many developing countries lack the regulatory framework or the capacity to track this new type of financial innovation. The largest Bitcoin exchange, for example, is now located in China.⁷ However, China's central bank recently barred financial institutions from handling Bitcoin transactions (Bloomberg News 2013).

The fluctuation of Bitcoin's value also adds to its risk. Bitcoin is not pegged to any real-world currency. Its value is determined by supply and demand and trust in the system. Following the closure of the underground market Silk Road in October 2013, the value of Bitcoin dropped from \$139 to \$109 in less than three hours and bottomed out at \$99 (Mattise 2013). This has led to Bitcoin being used more as a speculative investment tool than a currency or payment system. While there are now estimated to be 93,000 transactions per day, the majority of Bitcoins (around 55 percent) are not in circulation (Schrade 2013). Bitcoins are also not immune to fraud. As of November 2013, approximately 800,000 Bitcoins have been stolen (Schrade 2013). Since all Bitcoin transactions are irrevocable, there is no recourse for users who suspect they are or have been the victim of fraud. One can argue that consumers now have a choice: either pay higher fees for services that offer chargeback services in the case of fraud or pay lower fees for services with little to no recourse.

4 The article claimed that Kipochi (a Kenya-based Bitcoin wallet accessible via mobile phones) launched a product that allowed people in Africa to send and receive Bitcoins. Several statements in the article were misleading. It referred to Kipochi as being able to "convert [Bitcoins] to and from the Kenya currency M-PESA" (Spaven 2013). M-PESA is not a Kenyan currency, but simply a service that allows users to send e-money through an e-money account accessed through the mobile phone. M-PESA is not affiliated with Bitcoin, and there is no integration of the systems. Safaricom does not permit the sale and purchase of Bitcoins using M-PESA.

5 Interestingly, a Silk Road 2.0 website emerged just a month after the shutdown of the original website (Eha 2013).

6 One estimate is that fewer than 1,500 merchants accept Bitcoin globally (Schrade 2013).

7 Hearing "Beyond Silk Road—Potential Threats, Risks, and Promises of Virtual Currency" on 18 November 2013 (statement of Jeremy Allaire), testimony before the Senate Homeland Security and Governmental Affairs Committee, <http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies>.

Implications for the Unbanked

The current realities of Bitcoin mean it is still a long way off from reaching the unbanked. Only the financially included can access the Bitcoin system through the necessary digital connections to the Internet. The average transaction size to date is around \$2,000. But as with so many cutting-edge innovations, time will tell whether the benefits of Bitcoin can eventually impact mainstream populations around the world, and perhaps even those at the base of the pyramid. Advocates of the virtual currency believe that Bitcoin's peer-to-peer architecture and low barriers to entry will lead to the creation of a generation of innovative financial services, in much the same way as the Internet's open architecture led to new online services (Lee 2013). Proponents argue that Bitcoin provides a much cheaper and quicker payment system than what is currently available, especially for international transfers. That may be so, but it is also possible that five years from now Bitcoin will have disappeared or been replaced by other types of virtual or cryptocurrencies.

There is more clarity around e-money, with mounting evidence that it has brought previously excluded people into the formal financial system. Regulators and policy makers should take care not to confuse e-money with virtual currencies like Bitcoin and, in so doing, retract on the regulatory progress that has enabled e-money systems to flourish under risk-based proportionate regulation. E-money should continue to be regulated proportionately based on the size and nature of e-money transactions, continuing to open access to the formal financial system for many of the world's unbanked.

References

Arthur, Charles. 2011. "Bitcoin Value Crashes below Cost of Production as Broader Use Stutters." *theguardian.com*, 18 October. <http://www.theguardian.com/technology/2011/oct/18/bitcoin-value-crash-cryptocurrency>

Bloomberg News. 2013. "China Bans Financial Companies from Bitcoin Transactions." *Bloomberg Personal Finance*, 5 December. <http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html>

Brito, Jerry, and Andrea Castillo. 2013. "Bitcoin: A Primer for Policymakers." Mercatus Center: George Mason University. http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf

CoinDesk. 2013a. "What Is Bitcoin." 26 November. <http://www.coindesk.com/information/what-is-bitcoin/>

———. 2013b. "How Bitcoin Mining Works." 26 November. <http://www.coindesk.com/information/how-bitcoin-mining-works/>

———. 2013c. "How Do Bitcoin Transactions Work?" 26 November. <http://www.coindesk.com/information/how-do-bitcoin-transactions-work/>

Eha, Brian Patrick. 2013. "Could the Silk Road Closure Be Good for Bitcoin?" *The New Yorker*, 5 October. <http://www.newyorker.com/online/blogs/currency/2013/10/could-the-silk-road-closure-be-good-for-bitcoin.html>

European Central Bank. 2012. "Virtual Currency Schemes." October. <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

European Commission. 2009. European Commission Electronic Money Directive (2009/110/EC).

FATF (Financial Action Task Force). 2013. "FATF's Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services." <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>

FinCEN (Financial Crimes Enforcement Network). 2013. "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." 18 March. http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

Hern, Alex. 2013. "Is Bitcoin about to Change the World?" *The Guardian*, 25 November. http://www.theguardian.com/technology/2013/nov/25/is-bitcoin-about-to-change-the-world-peer-to-peer-cryptocurrency-virtual-wallet?CMP=fb_gu

Hoskinson, Charles. 2013. "The Mathematician's Defense of Bitcoin: It's Just Another Option." *PBS Newhour*, 9 October. <http://www.pbs.org/newshour/businessdesk/2013/10/the-mathematicians-defense-of.html>

Lee, Timothy B. 2013. "12 Questions about Bitcoin You Were Too Embarrassed to Ask." The Switch blog post. Washington Post, 19 November. <http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/>

Mattise, Nathan. 2013. "Amid Silk Road Uncertainty, Bitcoin Value Drops over 20% in 3 Hours." *arstechnica.com*, 2 October. <http://arstechnica.com/information-technology/2013/10/amid-silk-road-uncertainty-bitcoin-value-drops-over-20-in-3-hours/>

Nakamoto, Satoshi. n.d. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Bitcoin.org*. <http://bitcoin.org/bitcoin.pdf>

Schrade, Dirk. 2013. "Virtual Currency Schemes: Bitcoin—A Matter of Swim or Sink? Presentation at the Committee on Payment and Settlement Systems World Bank Conference, Cape Town, 3–4 December.

Spaven, Emily. 2013. "Kipochi Launches M-Pesa Integrated Bitcoin Wallet in Africa." *CoinDesk*, 9 July. <http://www.coindesk.com/kipochi-launches-m-pesa-integrated-bitcoin-wallet-in-africa/>

Tarazi, Michael, and Paul Breloff. 2010. "Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds." Focus Note 63. Washington, D.C.: CGAP, July.

Time Magazine. 2013. "The Deep Web." *Time Magazine*, 11 November.

January 2014

All CGAP publications are available on the CGAP Web site at www.cgap.org.

CGAP
1818 H Street, NW
MSN P3-300
Washington, DC
20433 USA

Tel: 202-473-9594
Fax: 202-522-3744

Email:
cgap@worldbank.org

© CGAP, 2014

AUTHOR:

Sarah Rotman