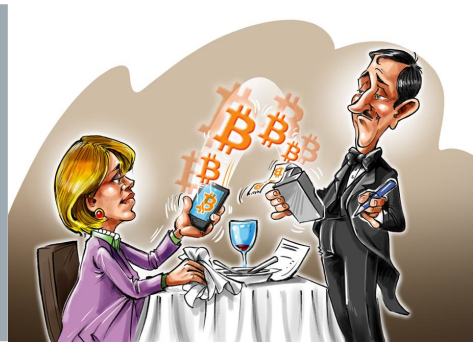
ECONOMIC NOTE

Montreal Economic Institute
Ideas for a More Prosperous Nation

Bitcoin: More Than a Currency, a Potential for Innovation

by **David Descôteaux**



Bitcoin digital currency has attracted the regular attention of the financial press for the past several months. Sold for a fraction of an American cent when it was introduced in 2009, the market value of a bitcoin exceeded one thousand US dollars in the fall of 2013, although it fell considerably in December (see Figure 1). Its price fluctuates enormously, influenced by new innovative developments but also by positive or negative decisions by governments and central banks concerning its use. Is the Bitcoin system here to stay and become an integral part of our economic lives?

Whatever the outcome of this particular experiment, the innovations made possible by new information technology have the potential to revolutionize monetary and financial matters. This *Economic Note* therefore offers an overview of the Bitcoin phenomenon in order to better understand the issues that it raises.

What is Bitcoin?

Bitcoin is both a payment system and a currency.[1] The currency is created electronically and exchanged between users without passing by a financial intermediary. By downloading free software (or a free application in the case of a mobile device), a user acquires a personal wallet that allows him or her to buy, send and receive bitcoins. Each wallet has a distinct alphanumeric address, somewhat like a bank account. Each transaction, whether it is a payment for goods and services, a purchase of bitcoins on an exchange or just a transfer of bitcoins between two people, is protected by a cryptographic signature (a private key associated with each wallet). If need be, the transaction can happen in a quasi-anonymous manner.[2]

What most distinguishes bitcoins from traditional currencies is that they are created and exchanged on a decentralized network that belongs to no one in particular. As in the case of sharing music files or films, Bitcoin uses a peer-to-peer data transfer protocol. The proper functioning of the network therefore does not rely on any authority, but rests instead on the reliability of its cryptographic protocol. This contains procedures for preventing people from spending other users' funds, double spending the same bitcoin, and ensuring new bitcoins are created in accordance to the rules of the system.

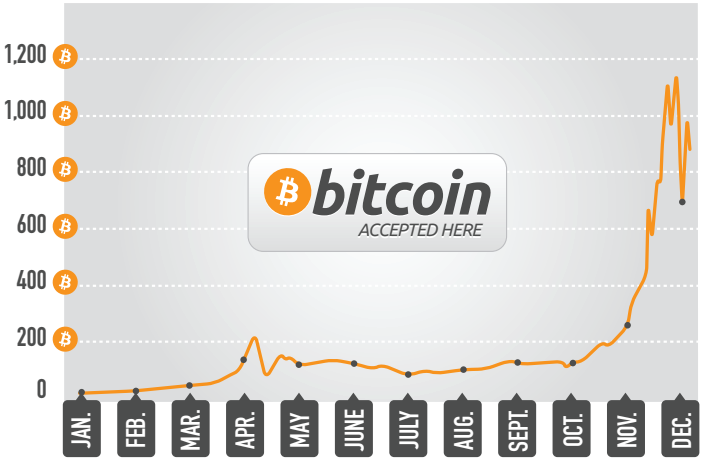
Concretely, these characteristics—a decentralized network and cryptographic security—ensure that users do not need to fill out forms with their personal information or pay transaction fees to third parties to process their payments (as is the case with transactions using Visa or PayPal, for example).

This does not make Bitcoin an opaque system, however. In some ways, it is even more transparent that our current monetary system. At the heart of Bitcoin is the "blockchain," a public transaction ledger

January 2014
Regulation Series

This *Economic Note* was prepared by **David Descôteaux**, associate researcher at the Montreal Economic Institute.

Figure 1 — Average daily price of a bitcoin in 2013, in US dollars



Source: *CoinDesk Bitcoin Price Index*, data extracted December 12, 2013. The *Bitcoin Price Index* represents the average price of a bitcoin based on the largest global exchange sites, namely Mt. Gox, Bitstamp and BTC-e.

on the Internet in which all transactions carried out on the network since it began are recorded chronologically. For a transaction to be included in the blockchain, it must first be validated, which requires the solving of a complex mathematical problem.

This is where the "miners" come into play, usually technophiles from all four corners of the globe equipped with powerful computer hardware. They validate the transactions and ensure the blockchain is valid and complete at each time instance. They are rewarded for their services in newly-created bitcoins[3] and with small fees they collect for confirming transactions.

This activity is called "mining" by analogy with the extraction of precious metals. The Bitcoin protocol is designed in such a way that new bitcoins are created at a fixed rate that decreases over time, until the creation of new monetary units stops completely once 21 million bitcoins have been put into circulation.[4]

For this reason, Bitcoin can be seen as an alternative to national currencies that are constantly being depreciated in countries with central banks that have a tendency to continually increase the money supply. It can also serve as a means of protection against the possibility that a government will impose capital controls, since Bitcoin cannot be controlled by any government.

Is bitcoin a "common currency"?

Does bitcoin have the potential to become a form of money that is widely used for day-to-day purchases, on the same level as the Canadian dollar? Generally speaking, a currency consists of an asset used regularly to buy goods and services. The value of a currency therefore depends on the utility that people bestow upon it. And this utility depends in turn on users' confidence in the currency and on its adoption by a large number of consumers, investors and merchants.

Bitcoins are accepted by a growing number of stores and businesses of all kinds, from hotels and restaurants in Europe to a laser eye surgery clinic in Colorado. A university in Cyprus allows students to use bitcoins to pay their tuition fees. And bitcoin ATMs are now in service in a few places around the world, including Vancouver.

The use of bitcoins nonetheless remains marginal compared to currencies like the US dollar and the euro. Recent developments, though, suggest that this use is bound to increase. In particular, the number of stores accepting bitcoins and the number of transactions carried out on one of the main processing sites both more or less doubled during the month of November, 2013.[5] As for the number of users of My Wallet, one of the most popular Bitcoin wallets in the world, it has grown by a factor of ten during the year 2013 (see Figure 2).

What most distinguishes bitcoins from traditional currencies is that they are created and exchanged on a decentralized network that belongs to no one in particular.

One of the main reasons for the growing popularity of Bitcoin among stores and consumers is that it reduces transaction costs. Banks, credit card companies and online payment services charge fees to retailers who offer their customers the opportunity to pay by debit or credit card, or with a PayPal account. A portion of these fees is generally passed on to consumers in the form of higher prices for goods and services. The use of bitcoins can therefore allow businesses that are more affected by such costs to reduce them.

The transfer of money across international borders (for example, remittances by foreign workers to their families still

living in their countries of origin), where transaction fees are relatively high, is also a promising avenue for Bitcoin, according to several specialists.[6] The use of bitcoins therefore has the potential to improve the supply of financial services insofar as transaction fees remain low and confirmation delays for these transactions remain short.

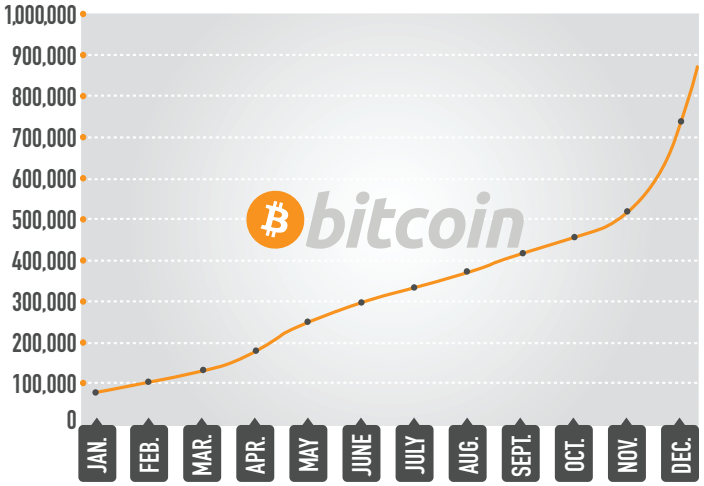
However, Bitcoin also has some disadvantages, commercially speaking. In particular, it may be difficult—if not impossible—to have any recourse in case of fraud, because transactions are irreversible once they have been confirmed in the blockchain (unless the person you are dealing with agrees to reimburse you).[7] Of course, the strength of Bitcoin being that it is a technological platform to which many new applications can attach themselves, we can expect that various consumer protection services will be offered by technology companies in the near future.[8]

One recent example of this kind of innovation has helped minimize problems related to the current high volatility of the value of bitcoins. This volatility has been a stumbling block for their adoption by retailers, who are afraid to accept payments in bitcoins and then see their value take a major hit a few minutes or a few hours later. Several companies are now offering to make it easier for merchants to use bitcoins for their transactions, and guaranteeing them a conversion rate in US dollars, for a small fee.[9]

One of the main reasons for the growing popularity of Bitcoin among stores and consumers is that it reduces transaction costs.

This kind of innovation, built on the Bitcoin protocol, could also turn out to be promising for banks and the financial sector in general. Thanks to its innovative character, the Bitcoin infrastructure could serve as a technological platform for equity markets, insurance markets and any other banking product or service. This therefore opens up numerous opportunities for financial institutions to improve their selection of products.[10] In the words of a US Federal Reserve economist, Bitcoin "represents a remarkable conceptual and technical achievement, which may well be used by existing financial institutions ... or even by governments themselves."[11]

Figure 2 — Number of users of My Wallet Bitcoin wallet in 2013



Source: Blockchain.info, My Wallet Number of Users, data extracted from the www.blockchain.info website on December 17, 2013.

Disadvantages to be overcome

Despite its numerous advantages, Bitcoin suffers from a few major shortcomings that are still hampering its development.

The ease with which transactions can be carried out quasi-anonymously with bitcoins allows them to be used for illegal activities like fraud and money laundering. In October 2013, for example, the FBI shut down Silk Road, a market where illicit products were sold and that used Bitcoin as its method of payment. Bitcoin can also facilitate tax evasion if transactions are not declared to the tax authorities. Finally, users are not fully protected from hackers and electronic theft.

It is important to note, however, that these risks are not so far removed from those associated with cash—which remains more anonymous than Bitcoin—or credit cards. It is also important to put into perspective the scope of potentially illegal actions carried out with the help of bitcoins, for example by comparing these with the black market in general, which is thought to total $2 trillion ($2,000 billion) in the United States.[12]

During the recent Senate hearings on the subject of virtual currencies, a representative of the American Secret Service minimized the importance of the use of bitcoins for criminal purposes, stating that "within what we see in our investigations, the online cybercriminals, the high-level international

cybercriminals we are talking about, have not, by and large, gravitated towards the peer-to-peer crypto-currencies such as Bitcoin."[13] This does not mean that this trend will not increase in time, however.

The volatility of the value of bitcoins also entails costs and risks. This volatility should diminish, however, as the use of bitcoins as a medium of exchange spreads, which will reduce the ability of a small number of actors to influence their price.

For the development of Bitcoin to continue, an appropriate legal and regulatory framework will need to be adopted to mitigate the risks and concerns that still exist.

Finally, and more crucially, Bitcoin is currently operating in a legal grey zone. Several central banks, like China's and France's, have expressed serious reservations about it. In other countries, the authorities have shown greater openness. In Germany, for example, the government has officially recognized Bitcoin as a private currency, and therefore as legitimate and subject to tax law.[14] Revenue Canada, the only Canadian governmental authority to have officially addressed Bitcoin, only issued a short press release to the effect that it considered bitcoins to be simple goods traded under a barter system, and not a currency or a financial asset. In other words, Canada has not yet officially spelled out a detailed position on the matter.[15]

For the development of Bitcoin to continue, an appropriate legal and regulatory framework will need to be adopted to mitigate the risks and concerns that still exist.[16] Such a framework could strengthen consumers', retailers' and investors' confidence in Bitcoin, and hence encourage its use on a large scale.

References

1. The invention of Bitcoin is attributed to an individual or a group that went by the pseudonym Satoshi Nakamoto, but his or her (or their) real identity has never been confirmed. In 2008, Nakamoto published a document describing the Bitcoin protocol.
2. Although anonymity can be reinforced through a series of measures that users can take, it will never be perfect. Researchers at a Swiss university showed, using a simulation, that the profiles of around 40% of users could be discovered even if they were to adopt the confidentiality measures recommended by the Bitcoin community. See Elli Androulaki *et al.*, "Evaluating User Privacy in Bitcoin," *Lecture Notes in Computer Science*, Vol. 7859, 2013, p. 34.
3. The total number of bitcoins increases by a pre-established amount each time a block is added to the blockchain. These new bitcoins are given to those who solve the related mathematical problems. See Maria A. Arias and Yongseok Shin, "There Are Two Sides to Every Coin—Even to the Bitcoin, a Virtual Currency," *The Regional Economist*, Federal Reserve Bank of St. Louis, October 2013, p. 1.
4. There were, as of December 6, 2013, over 12 million bitcoins in circulation according to the Bitcoinscharts.com website.
5. Joon Ian Wong, "CoinMap: Bitcoin-Accepting Merchants Increased 81% in November," *Coindesk*, November 28, 2013; Joon Ian Wong, "BitPay Sees 6,260% Increase in Bitcoin Black Friday Sales," *Coindesk*, December 3, 2013.
6. Among others, David Woo of Bank of America Merrill Lynch. See Joe Weisenthal, "This Is, Quite Simply, The Biggest Endorsement That Bitcoin Has Ever Received," *Business Insider*, December 5, 2013.
7. As a Desjardins Group study notes, "If the fees for account maintenance, currency exchanges and transactions remain low for cryptocurrencies, it is largely because there are no safeguards in place or recourse for users who suffer damages. Our traditional monetary system offers several ways to protect citizens, but these structures come at a price." Hendrix Vachon, "The limits of currencies like Bitcoin," *Economic Studies*, Desjardin Group, November 21, 2013, p. 4.
8. A new company, Bitrated, already launched this type of service in December 2013. Vitalik Buterin, "Bitrated: You Can No Longer Say Bitcoin Has No Consumer Protection," *BITCOIN Magazine*, December 10, 2013.
9. Bitpay, among others, states on its website that it is providing this service to over 12,000 merchants and charities (as of December 2013).
10. Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers*, Mercatus Center at George Mason University, 2013, p. 16.
11. François Velde, "Bitcoin: A Primer," *Chicago Fed Letter*, Federal Reserve Bank of Chicago, December 2013, p. 4.
12. Richard Cebula and Edgar L. Feige, "America's Underground Economy: Measuring the Size, Growth and Determinants of Income Tax Evasion in the U.S.," MPRA Paper No. 29672, University Library of Munich, 2011, p. 17.
13. Testimony of Edward Lowery, Special Agent for the American Secret Service, before a Senate committee on virtual currencies, November 18, 2013.
14. "Germany lends real value to bitcoin virtual money," Deutsche Welle, August 22, 2013.
15. Canada Revenue Agency, "What you should know about digital currency," Press release, November 5, 2013.
16. The MEI will explore these challenges in more detail in a *Research Paper* to be published between now and the fall of 2014.

910 Peel Street, Suite 600
Montreal (Quebec) H3C 2H8, Canada
Telephone: 514-273-0969
Fax: 514-273-2581
Website: www.iedm.org