March 7, 2014

WELLS FARGO SECURITIES

*Foreign Exchange Research*

# Special Edition

**Nick Bennenbroek, Head of Currency Strategy**
nicholas.bennenbroek@wellsfargo.com
1-212-214-5636

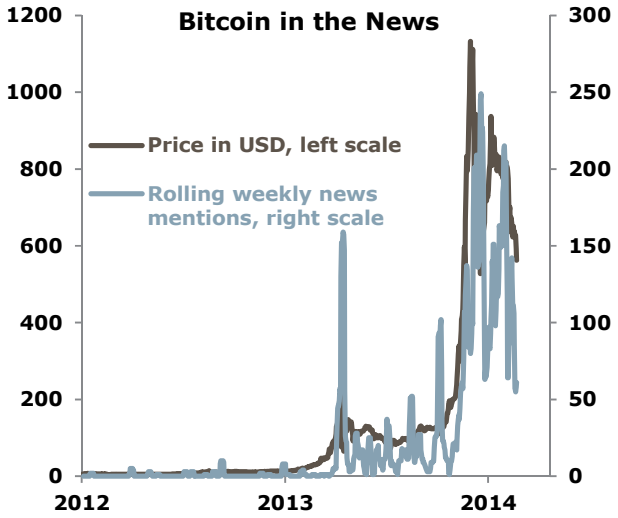
## Bitcoin 101: A Primer




Together we'll go far

### *Summary*

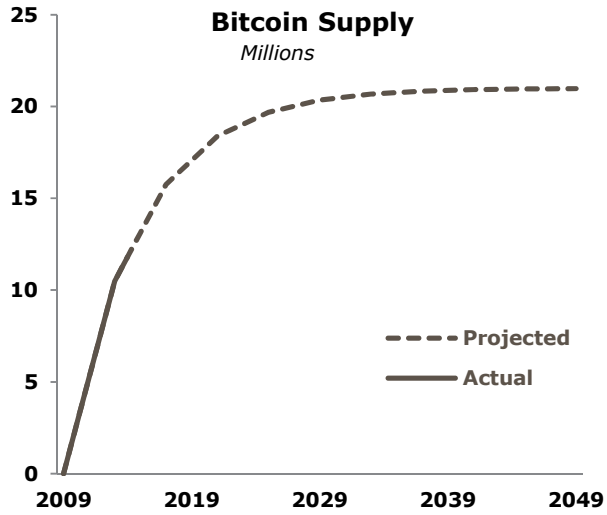
The "digital currency" Bitcoin has attracted the attention of markets and the general public. Media reports on the virtual currency have surged, as Bitcoin has experienced large and sometimes dramatic price swings, and has been affected by some high-profile difficulties. In this report, we provide an introduction to Bitcoin—what it is and how it works—the potential, the problems and the price swings.




Source: Bloomberg, www.Bitcoincharts.com, Wells Fargo Securities, LLC

### *What is Bitcoin?*

Bitcoin is decentralized digital currency that enables online payments to be made directly from one party to another, without the need for a central third-party intermediary to verify the transaction. Bitcoin is a peer-to-peer payments network that was created in open-source C++ programming code in early 2009 by the programmer or group of programmers known as Satoshi Nakamoto. In terms of the infrastructure, Bitcoin is a public, Internet-wide ledger. The ledger contains every transaction ever processed. The Bitcoins themselves are just the slots in the ledger, to which one claims ownership. Bitcoins are divisible to eight decimal places, theoretically allowing for transactions as small as 6/10,000ths of a cent at current Bitcoin prices. Bitcoins, or ownership of the specified ledger slots (or fractions of ledger slots) can be obtained through various methods. These include paying cash for Bitcoin, providing a good or service in exchange for Bitcoin, or verifying other Bitcoin transactions (a process known as "mining"), which rewards the verifier with Bitcoins. Because Bitcoin transactions do not require a centralized intermediary, payments can be processed at very low cost.




Source: https://en.Bitcoin.it/wiki/Controlled_supply

### *Predictable Rate of Increase in Supply*

The global supply of Bitcoins is increasing at a predictable and relatively predetermined pace. Currently, the total supply of the digital currency is around 12,500,000 Bitcoins[1], while overall supply will reach a maximum of 21,000,000 Bitcoins, which is expected to happen around 2140. The supply of Bitcoin increases through the process of mining, which we will briefly address later when discussing the mechanics of a transaction. The predictable rate of increase in supply has been cited by some as an advantage of Bitcoin, in that the supply and price of the digital currency cannot be influenced or managed by governments or central banks. Such concerns about the government management of currencies has become more visible and been expressed more frequently in the wake of the 2008 global financial crisis, as several of the world's major central banks (Federal Reserve, Bank of Japan and Bank of England) have implemented quantitative easing (the outright purchase of government bonds and other assets). This has led to a rapid increase in the size of central bank balance sheets, and more rapid growth in the global money supply, leading some to question the soundness and stability of traditional fiat (i.e., paper) currencies.

### *Overview of a Bitcoin Transaction*

A Bitcoin transaction entails transferring the ownership of a specified number of slots of the Internet-wide ledger from one party to another. The transfer of Bitcoins is enabled using a Bitcoin wallet, options for which could be a computer-based program or mobile device-based application, which can be used to send and receive Bitcoins.

[1] www.Bitcoincharts.com

**Public and Private Keys.** Regarding the transaction, each slot or address in the Internet-wide ledger has a public key that serves as a pseudonym (users can have several public keys, which do not need to be tied to each other, or to the users' real-life identity). Each slot or address in the ledger also has a private key, which the owner must keep secret. In each transaction the previous owner signs—using the private key that corresponds to the public key/ledger slot—a hash of the transaction in which the Bitcoin was received, as well as the public key of the next owner. This transaction can then be added to the set of transactions that constitutes the Bitcoin, and because each transaction references the previous transaction, those transactions form a chain.

**Wallets and Miners.** Once the sender and receiver have carried out the transaction via their Bitcoin wallets, the "wallet" broadcasts the proposed transaction to other Bitcoin users. To verify the validity of a Bitcoin, a user can check the validity of each transaction in the chain. To avoid double spending, each user in the system needs to be aware of all transactions. Double spending could occur if a user attempts to transfer a Bitcoin after they have already done so. To determine which transaction comes first they are grouped into "blocks" and time-stamped. Eventually, the broadcasts of the transactions reach a "miner." This is a user, or group of users, who solve a difficult mathematical problem that is costly in terms of computer power required, (electricity and time), but verifies that the transaction is legitimate (that is, the sender owns the Bitcoin and has not spent it previously).

**Blocks and Block Chains.** The miner who first finds the solution broadcasts it to other miners. Once verified by other miners (i.e., accepted by a majority), the new block of transactions is added. These blocks are also then formed into a chain, with each block referencing the previous one, again further confirming the validity of each transaction. The process yields a "block chain," which is available for all users in the system. In this manner, and as we stated earlier, the public Internet-wide ledger contains every transaction ever processed. Typically, it takes 10 minutes for Bitcoin payments to be confirmed, although for larger transactions, it is customary to wait up to 60 minutes. The successful miner who first finds the solution is awarded additional Bitcoin(s), hence the analogy to "mining" for Bitcoins. The sender/payer of a Bitcoin may also include as part of that transaction a small fee, to incent a miner to process their transaction more rapidly. That fee will also be necessary to compensate miners once the supply of Bitcoin has reached its maximum amount.

## *Potential Growth Opportunities Created by Bitcoin*

In our view, the primary opportunity for Bitcoin appears to be as a low-cost payments mechanism. Because there is no centralized intermediary involved in the transaction, and because of the competitive nature by which transactions are verified, transactions via Bitcoin generally take place at very low cost.

**Low-Cost Processing, Irrevocable Payments and Pseudonymous Transactions.** For merchants, the current low cost of processing Bitcoin payments compares favorably to the fees charged by credit card companies or other financial institutions. For the U.S. in 2012, the average margin on card-based transactions was 1.5%, which amounts to $66.5 billion in processing fees. For low-margin businesses, the ability to securely process payments could be especially beneficial. Bitcoin payments are also irrevocable, an advantage for business, albeit a disadvantage for consumers. Eventually, the processing cost for Bitcoin payments will likely increase to some extent, since "miners" will need to be compensated for their efforts once the supply of Bitcoins is exhausted, and as Bitcoin-related services impose or increase their own fees. That should diminish the cost advantage Bitcoin enjoys compared to traditional payments systems, but it might not eliminate that advantage completely. Another advantage of Bitcoin as a payments systems is in deterring and preventing identity theft, given that Bitcoin transactions are pseudonymous and do not include any identifying personal information. For 2012, fraud on card-based payments was estimated at $11.3 billion across $21.604 trillion of purchase volume and cash withdrawals made with payment cards on a global basis. Also notable were breaches at TJ Maxx (2007—$256 million cost and 100 million cards); Target (2013—40-100 million cards, cost undetermined); and Michael's has had two. There were also data breaches at Heartland Payment (2009—cost of $147 million) and Global Payments (2012—cost of roughly $94 million). In terms of merchant usage, according to coinmap.org, there are currently around 3,300 physical businesses accepting Bitcoin globally, a small but growing number.

**Alternative to Foreign Exchange Payments.** Another opportunity for Bitcoin is lower-cost foreign exchange and international payments. At the retail level, the margins charged for electronic foreign exchange payments are often in the range of 2-4%, while the margins on international remittances are often in the range of 1-2%. Since Bitcoin can be used to send and receive payments internationally, it provides a cost-effective alternative, even if one allows for the need to exchange Bitcoin to a legally recognized fiat currency at either end of the transaction. Additionally, Bitcoin could prove attractive to citizens subject to capital controls, given the ability to access the digital currency globally. Examples of capital controls could include limits on the amount of physical currency that can be carried across borders or limits on electronic withdrawals from bank accounts. Bitcoin has also been cited as a possible alternative to emerging currencies, which are susceptible to inflationary episodes and loss of purchasing power.

There is potential for Bitcoin in the area of international payments. However, unless or until Bitcoins become widely accepted, the value of the market could be limited unless there is an ability to exchange Bitcoins into a legal currency. While this may not pose difficulties in exchanging U.S dollars into

the euro or the Chinese renminbi, it could pose challenges for currencies such as the Venezuelan bolivar or Argentine peso. We are unaware of exchanges that currently accept payment for Bitcoin in those currencies.

**Micropayments Potential.** A third area of opportunity for Bitcoin could be in the area of micropayments. Given that Bitcoins are divisible to eight decimal places, and given that the cost of processing transactions is very low, it allows for payments and transactions that would not be economically practical through banks or other traditional payments systems. In particular, this could lend itself to transactions for media and other internet-based content. The ability to transact in very small amounts could open up the possibility for content providers to charge for much smaller slices of information: per news article, per page view, or per hours or minutes viewed. That said, the short delay in confirming transactions may not make it suitable for small in-person payments, but more for online payments.

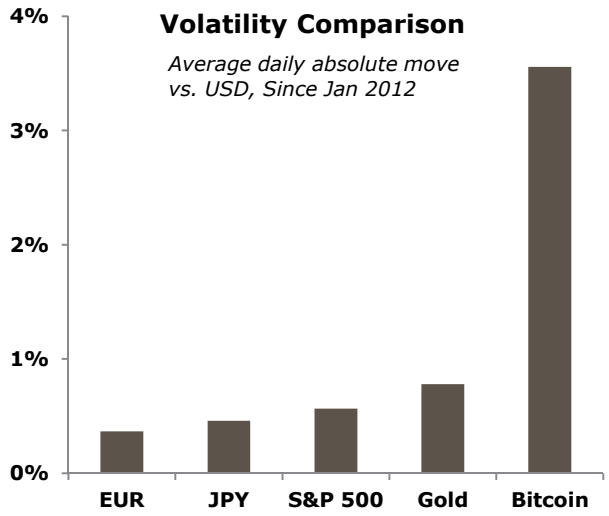
Another advantage and opportunity for Bitcoin is its prevalence as a digital currency. Some estimates suggest that Bitcoin accounts for around 65% of all digital currency payments, with its relatively broad network supporting its attractiveness relative to other, lesser-used digital currency alternatives. Finally, the Bitcoin platform itself—the protocol and encryption methods—might also have potential and application in securely transferring other forms of digital information, such as digital contracts, digital ownership documents, and so on.

### *Issues and Risks for Bitcoin*

Balanced against the opportunities for Bitcoin as a payments system, there are several issues and risks that could affect the digital currency—some of them transitory and some of them more permanent. We address some of the more notable of these issues below.

**Bitcoin Price Volatility.** A significant issue for Bitcoin is the large price movements that the digital currency exhibits on a daily basis, a factor that could inhibit its broader acceptance as an alternative currency to the existing, government-backed, paper currencies. Money, or a currency is typically thought of as having three characteristics: (1) that it functions as a medium of exchange, (2) a unit of account, and (3) a store of value. As we highlighted previously, there is certainly potential for Bitcoin to function as a medium of exchange (i.e., its greatest potential is as an alternative payments system). However, the price volatility of Bitcoin limits its usefulness as a unit of account and, especially, as a store of value. Since the beginning of 2012, the average daily price move for Bitcoin has been around 3.5%, far in excess of gold (0.8%), and the S&P 500 equity index, and less than 1% for the euro/U.S. dollar exchange rate and the U.S. dollar/yen exchange rate (around 0.5% or less).

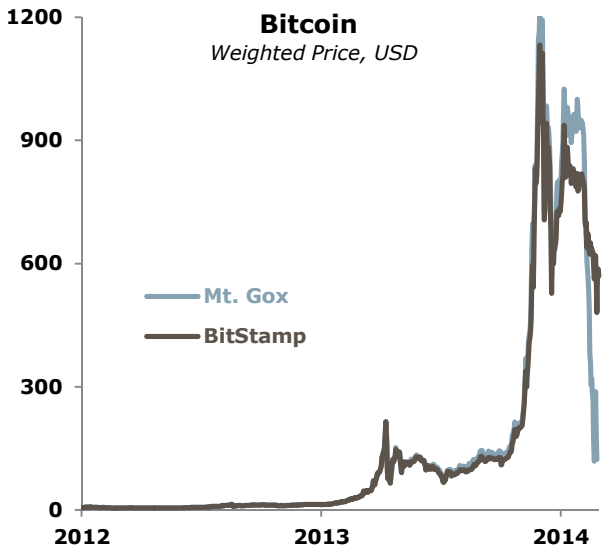
While the price volatility of Bitcoin may lessen if the digital currency matures and gains wider acceptance, we expect it will likely still exhibit greater volatility than the traditional fiat currencies. While the absence of government management has been cited as an advantage of Bitcoin, it also means there is no centralized authority to manage or smooth out the price fluctuations or overall supply of the digital currency. Accordingly, the long-term price volatility of Bitcoin is likely to remain somewhat elevated, in the same way that volatility in gold or other commodities prices is elevated. This ongoing volatility of prices could limit its usefulness as a unit of account. More importantly however, in our opinion, it means Bitcoin is unlikely to become a stable store of value and satisfy that particular currency criteria. While consumers and businesses may be willing to transact in Bitcoins, we think they might be less willing to hold on to those Bitcoins, unless as an asset or investment, rather than purely as "money." This of course could limit Bitcoin's acceptance with the wider public.




Source: Bloomberg, www.Bitcoincharts.com, Wells Fargo Securities, LLC

**Technology and Exchange Risk.** Like other electronic systems, Bitcoin is susceptible to hackers. There is also the known issue of transaction malleability (under certain limited conditions, changes can be made to a transaction to make it appear as if the transfer didn't go through). More broadly, a significant concern for users is the safety and security of assets held at Bitcoin exchanges. As we mentioned previously, payment in cash is one way to obtain Bitcoins. Bitcoin exchanges help fulfill that function, allowing members to convert fiat currency into Bitcoins and vice versa. In transacting through these exchanges, individuals are exposed to potential fraud, take on credit risk related to the exchange, and are relying on the competence of management. There have been several examples of Bitcoin exchanges that have been hacked, as well as denial-of-service attacks on exchanges, which have consequently either suspended withdrawals or halted transactions in response. The most high-profile

instance of these exchange difficulties was the recent shutdown and bankruptcy declaration by the Tokyo-based Mt. Gox, once the world's largest Bitcoin exchange.[2] The company said it has lost 850,000 Bitcoins (which equates to a total value of $470 million. The company said that 750,000 of those Bitcoins belonged to customers, and 100,000 were its own, and that it believes there is a high probability that the Bitcoins were stolen. Mt. Gox had also been beset by other difficulties in the past few weeks, prompting the price of "Mt. Gox" Bitcoins to trade at a discount to other exchanges (see chart below). While the difficulties of one exchange are not necessarily systemic across the industry, it does highlight the need for sound management and proper oversight and controls, particularly considering the current regulatory and legal situation, as we discuss below.




Source: www.Bitcoincharts.com, Wells Fargo Securities, LLC

**Regulatory and Legal Issues.** Bitcoin is likely to come under increasing regulatory scrutiny, especially if it gains wider acceptance. Authorities could be motivated to increase their scrutiny and oversight of the digital currency to assist with law enforcement efforts in addressing "black-market" activities, as well as taxing more legitimate Bitcoin related activities. Such regulatory efforts will almost certainly increase Bitcoin's transaction processing costs, diminishing one of its key advantages.

Given the current lack of regulation, legal recourse, as it relates to Bitcoin, remains unclear. There is little to no legal recourse in the event that a user is hacked or otherwise subjected to fraud. Additionally, there are no broadly adopted consumer protection mechanisms in place, a key shortcoming relative to legal currency, which is backed by the full faith and credit of the issuing authority. However, some initial private-sector efforts to provide some form of protection are underway. That said, the lack of regulation, the unclear legal situation, and the lack of consumer protection heighten the risks attached to transacting in the Bitcoin market in these early stages.

**Infrastructure Issues.** In part related to the regulatory and legal issues, but broader in scope, is the need for Bitcoin to develop a comprehensive payments system with robust rules, enforcement and processing frameworks. This would allow for enforcement of customer protections (unauthorized activity, asset protection, fraud, pricing and disclosure), and allow for government activities (as mentioned previously, taxation and law enforcement), while also helping to guarantee the safety and soundness of the financial system. The process of comprehensively developing an infrastructure could take multiple years.

**Cautious Initial Stance by Government Authorities.** Government authorities have adopted a very cautious stance on digital currency thus far. Among some of the recent announcements, China's central bank warned in mid-December about the risks of Bitcoin, and said that financial institutions should not engage in business with Bitcoin-related companies. In February, Russian authorities pointed to the risks of money laundering and financing terrorism and declared that cyber currencies are money substitutes and "cannot be used by individuals or legal entities." Just before the bankruptcy of Mt. Gox, Japanese Finance Minister Taro Aso told reporters, "no one recognizes them as real currency." The stance of the Federal Reserve has been more even handed, but hardly embracing. Fed Chair Yellen, in response to questions at her recent testimony, said the Fed "simply does not have the authority to supervise or regulate Bitcoin in any way."

**Reputational Issues.** Another issue for Bitcoin currently, albeit possibly a transitory issue, is its perceived association with illicit activities. The anonymity of payments through Bitcoin has led some to argue that the currency could be used to support illegal activities. One of the best-known examples is the Silk Road marketplace for illegal drugs, malicious software, and other illegal products, where Bitcoin is the payment of choice. Association with such activities could, at least initially, slow the acceptance of Bitcoin by the wider public.

### *Bitcoin Demand as an Alternative Currency*

One final point is the extent of broader public demand for an alternative "hard" currency to the U.S. dollar. While there are certainly vocal segments of the population that have expressed their concerns about perceived government undermining of currencies, it is difficult to assess, how widespread those views are. While the U.S. dollar is by no means strong, based on the Fed's broad trade-weighted index (i.e., the dollar's value against both major and emerging currencies), the greenback is

[2] Mt. Gox Files for Bankruptcy After $470 Million Bitcoin Loss, Bloomberg, 28 February 2014.

at least off the lows seen in 2008 and 2011. Moreover, since at least 2010, consumer price inflation has been reasonably modest, within a 1-4% range. On that basis, it is far from clear-cut that the government's efforts have undermined the currency. Should demand for Bitcoin as a "hard" currency prove limited, the digital currency's price appreciation would also be limited.


Source: Bloomberg, Wells Fargo Securities, LLC

### *Final Thoughts*

The ability for payments to be processed via Bitcoin offers a potentially significant opportunity for the digital currency to fulfill a market niche with applicability in the areas of general merchant payments, international payments, and micropayments. Balanced against this potential opportunity for Bitcoin are several issues or risks. Some of these are likely to be permanent, such as what we perceive as the inherent instability of the digital currency. While other issues may eventually be addressed (for example, security concerns of Bitcoin exchanges, regulatory and legal issues, and the development of payments system infrastructure), the expense of doing so could clearly diminish the cost advantage Bitcoin currently enjoys relative to traditional payments systems. It is not clear at that point whether the remaining cost advantage would necessarily outweigh the remaining issues. Thus, while we think Bitcoin clearly has some potential as an alternative payments system, it is probably too early to assess its long-term potential and sustainability. The extent of public demand for an alternative currency is unclear (and there are other choices for hard assets, such as gold). Also, we expect the inherent volatility of Bitcoin to restrain wider public acceptance.

*Source for cover image: © iStockphoto.com*

## Wells Fargo Securities, LLC Economics Group


| | | | |
|---|---|---|---|
| Diane Schumaker-Krieg | Global Head of Research, Economics & Strategy | (704) 410-1801<br>(212) 214-5070 | diane.schumaker@wellsfargo.com |
| John E. Silvia, Ph.D. | Chief Economist | (704) 410-3275 | john.silvia@wellsfargo.com |
| Mark Vitner | Senior Economist | (704) 410-3277 | mark.vitner@wellsfargo.com |
| Jay H. Bryson, Ph.D. | Global Economist | (704) 410-3274 | jay.bryson@wellsfargo.com |
| Sam Bullard | Senior Economist | (704) 410-3280 | sam.bullard@wellsfargo.com |
| Nick Bennenbroek | Currency Strategist | (212) 214-5636 | nicholas.bennenbroek@wellsfargo.com |
| Eugenio J. Alemán, Ph.D. | Senior Economist | (704) 410-3273 | eugenio.j.aleman@wellsfargo.com |
| Anika R. Khan | Senior Economist | (704) 410-3271 | anika.khan@wellsfargo.com |
| Azhar Iqbal | Econometrician | (704) 410-3270 | azhar.iqbal@wellsfargo.com |
| Tim Quinlan | Economist | (704) 410-3283 | tim.quinlan@wellsfargo.com |
| Eric Viloria, CFA | Currency Strategist | (212) 214-5637 | eric.viloria@wellsfargo.com |
| Michael A. Brown | Economist | (704) 410-3278 | michael.a.brown@wellsfargo.com |
| Sarah Watt House | Economist | (704) 410-3282 | sarah.house@wellsfargo.com |
| Michael T. Wolf | Economist | (704) 410-3286 | michael.t.wolf@wellsfargo.com |
| Zachary Griffiths | Economic Analyst | (704) 410-3284 | zachary.griffiths@wellsfargo.com |
| Mackenzie Miller | Economic Analyst | (704) 410-3358 | mackenzie.miller@wellsfargo.com |
| Blaire Zachary | Economic Analyst | (704) 410-3359 | blaire.a.zachary@wellsfargo.com |
| Peg Gavin | Executive Assistant | (704) 410-3279 | peg.gavin@wellsfargo.com |
| Cyndi Burris | Senior Admin. Assistant | (704) 410-3272 | cyndi.burris@wellsfargo.com |