Bitcoin: The Currency of Tomorrow – or Today?

Author: Joseph Budzyn, Senior Business Development Manager

Published: September 2014

Executive Summary

Enthusiasts call bitcoin a revolution in payment technology that will change the financial landscape. It will open new markets and have less government involvement. Detractors call bitcoin a scam and a good way to lose money. Governments can't seem to agree on how bitcoin should be treated. Already it has been classified as currency, property, a commodity, legal and illegal at different times. Yet nearly every day, companies are announcing they will accept this "digital cash."

Five years after the emergence of bitcoins, consumers are using them to buy everything from pizza to cars, from drugs to real estate. Political donations can even be made in bitcoin. But what are bitcoins exactly? How do they work? What are the risks associated with their usage?

What are Bitcoins?

Like traditional currency, bitcoins facilitate the exchange of goods or services. The advantages of bitcoin are fast payments worldwide with very low transaction costs. International monetary transactions can take three days to clear, whereas bitcoin transactions are considered settled after just one hour. Credit cards transaction fees are roughly two percent of the purchase price, while the minimum bitcoin transaction fee is 0.001 of the bitcoin's value.[1]

Bitcoin was released to the world in 2009 by someone going by the name "Satoshi Nakamoto." It is unclear who Satoshi is, if it is a pseudonym, or if it is really a group of people using the name.[2] Today the bitcoin software is maintained and improved by a group of developers.[3]

Bitcoin is a peer-to-peer payment system that uses a mathematical algorithm to limit the total number of bitcoins that exist and controls their rate of discovery. In total 21 million bitcoins will be produced.[4] This limit creates scarcity, and when coupled with supply and demand, determines the value of a bitcoin.[5]

Using bitcoin is somewhat similar to online banking. Software known as a "wallet" stores bitcoin addresses (similar to an account number) and handles transactions. The wallet can reside on any computing device, or on a website known as a "web wallet." Wallets securely store bitcoin using encryption, and can send them to an individual or company for payment.

A "hot wallet" is connected to the Internet and can be used for transactions. Wallets stored on devices without Internet connections are "cold wallets." A cold wallet is used for offline bitcoin storage and can be stored on a standalone USB device,[6] for example. Similar to an online bank account, the username and password must be protected from unauthorized access to protect the bitcoins within the wallet.

With an online bank account, anyone that has the username and password to the account can access it and remove money. In order to keep the bank account secure, the username and password must be protected from unauthorized access. Likewise, the bitcoin wallet and password must be protected from unauthorized access to protect the bitcoins within the wallet.

How does Bitcoin Work?

Bitcoin does not rely on banks to log transactions or track how many bitcoins are held in individual accounts. Instead the bitcoin network uses a "block chain" to perform these functions openly and publicly.

The block chain is a public ledger containing all confirmed transactions.[7] The integrity and chronological order of the block chain is maintained with encryption by the bitcoin network.[8] User identities are protected by recording the bitcoin address in the ledger instead of user names. As long as the bitcoin users do not identify themselves as the owner of a bitcoin address, their transactions remain anonymous.

No single entity or central bank controls the bitcoin network or sets economic policy. Instead bitcoin users control the bitcoin network, with a subgroup of bitcoin "miners" using their computers to process transactions and add them to the block chain by "mining."

Mining

Roughly every ten minutes the bitcoin network bundles recent transactions together and sends them to the miners.[9] The miners' computers perform complex calculations called a "proof of work." The proof is very hard to create and requires billions of calculations per second, turning the effort into a type of lottery.[10] The first miner to satisfy the proof of work calculations wins a reward of bitcoins. In 2014 the reward for adding one block to the block chain is 25 bitcoin.[11] The transactions combined with the proof of work and control data make up a block in the chain.

This incentive of accruing bitcoins is why miners participate in the bitcoin network. As the bitcoin network grows in computing power, it automatically adjusts the difficulty of the proof of work to ensure the calculations take roughly ten minutes.[12] This keeps mining very competitive and ensures that no one entity can control the network.[13]

The calculations for the proof of work are based off the previous block in the block chain to enforce chronological order. As more blocks are added to the chain, it becomes increasingly difficult to reverse previous transactions (i.e., improperly return the bitcoins to the original holder by undoing the transactions) since all subsequent blocks would require recalculation.[14]

There is the possibility that two blocks (containing different transactions) could be discovered by different miners at the same time. If this occurs, the bitcoin network determines which block to use as the official ledger.[15] The alternate block is discarded, creating a small risk that some transactions may be lost if they did not make it into the block added to the official ledger.

It takes roughly ten minutes for a transaction to be recorded in the public bitcoin ledger. For small transactions, ten minutes is likely long enough. In order be certain that a

transaction is permanently entered in the block chain, such as those for larger transactions, waiting until several blocks are added to the chain may be wise.[16]

Bitcoin Risks

As with any emerging technology, this new practice brings associated – and sometimes uncharted – risks.

- Like cash, if a bitcoin is lost, it is lost forever. There is no recourse to recover the bitcoin if the password to a bitcoin wallet is forgotten. The same is true if the wallet becomes corrupted due to hardware failure, or if the USB storage device containing a cold wallet is lost. Having good backups of the wallet is critical.[17]

  Additionally, bitcoin transactions are not reversible. Once a transaction has been confirmed in the block chain, it cannot be undone. This benefits merchants since chargeback fraud, (when someone purchases an item with their credit card, then petitions their credit card company for a refund claiming they never received the item), is not possible.[18]

  As a consumer, limit bitcoin transactions to trustworthy merchants. A reputable merchant can issue a refund as a separate transaction, while an unscrupulous one may simply keep the bitcoin and never fulfill the order.

- Transactions may be anonymous, but they are recorded. Bitcoin is popular with criminals since their identity is protected. However, every transaction is recorded in the public ledger.[19] This makes it possible for law enforcement to reconstruct past bitcoin transactions if the user's identity can be matched with bitcoin addresses.

  As an example, suppose a bitcoin address is used to ship a product to a residence from a well-known, legitimate website. Then the same bitcoin address is used to purchase something illegal. Law enforcement can now link both transactions to the same bitcoin user. If law enforcement can obtain the shipment address from the legitimate website, then a suspect identity begins to emerge.

  Once the identity is determined, the user's entire history of bitcoin use becomes available. The anonymity provided by bitcoin can be fragile, and easily lost.

- Acting too fast could result in lost payment. Bitcoin transactions can occur nearly instantly, however blocks are added to the block chain every ten minutes; it takes at least that long for the transaction to be confirmed by the bitcoin network.

  If an order is fulfilled before the transaction is confirmed, a company may find that product has been shipped, but payment never occurred. For particularly large transactions, waiting until several blocks are added to the chain may be wise.

- Bitcoin value is volatile. Bitcoin values have risen and fallen significantly over the last two years; starting around $5 per bitcoin, peaking above $1,100, and currently valued around $500 per bitcoin.[20] This makes storing value in bitcoins something of a gamble. Many companies that accept bitcoins immediately exchange them for their local currency, protecting their organizations from potential dramatic price swings.

- Laws and regulations are still emerging. In the United States, various government agencies and states disagree on how to classify bitcoins and regulate their use. At the federal level, for example, the IRS is treating bitcoin as property, not currency.[21] This means that capital gains and losses must be calculated and reported for tax purposes, thereby complicating everyday use since every purchase requires accounting documentation.

  Most states have not adopted a regulatory approach to digital currency. Texas has issued regulatory guidance on its decision to not treat bitcoin as currency.[22] New York is considering regulating virtual currency exchanges,[23] while Florida is applying existing laws to bitcoin exchanges, particularly money laundering laws.[24]

Besides limited regulations, there is little consumer protection in place. Unlike traditional currency deposits at banks, bitcoin deposits are not protected by anything similar to the Federal Deposit Insurance Corporation (FDIC).[25]

Until government agencies fully decide exactly what bitcoin is, insurers are unlikely to feel comfortable offering standardized coverages. Until then, companies seeking insurance can inquire about customized offerings.

Internationally, the legal landscape is just as complicated with many laws in development. Some countries, such as Iceland, have restricted the foreign exchange of bitcoin.[26] Others, such as Vietnam do not recognize the currency.[27] China has barred financial institutions from trading bitcoin[28], while India has advised the public to avoid the buying and selling of virtual currencies.[29] Russia appeared to ban bitcoin in January, but then clarified that bitcoin was not banned in February.[30]

As with any new technology, laws and regulations take time to formulate. The legal landscape is changing rapidly, but should become clearer as time passes.

- Malware can steal electricity. Malware that mines for bitcoins has been discovered on computers, tablets and cell phones. Mining for bitcoins is a computationally intensive process, stealing extra processing power can give an unscrupulous miner an edge; it can result in a larger electricity bill or drained batteries for the owners of these compromised computers. [31]
- Malware can steal bitcoins. Malware can also attack the wallet software itself and potentially drain the wallet of any bitcoins it contains.[32]
- Bitcoins can be lost to theft or exchange failure. In early 2014 hackers allegedly exploited weaknesses in several bitcoin exchange websites. By sending many copies of the same bitcoin payment, a vulnerable exchange would send out the requested bitcoins repeatedly.[33] Using this technique, hackers allegedly stole thousands of bitcoins, worth millions of dollars.[34,35] Unable to return bitcoins to their customers, the hacked exchanges closed. Since there is no FDIC-like insurance protecting the users of such exchanges, the only remedy is through the legal system.

Conclusion

Given all of the media coverage that bitcoin receives, it is important to remember that it emerged only five years ago. Will bitcoin revolutionize the financial world? Will it join other valueless currencies are only found in history books? It's too soon to know for certain. Should a company accept bitcoin as payment today? If approached thoughtfully as a means of transaction, accepting bitcoin can be a differentiator in today's competitive marketplace. If implemented poorly, accepting bitcoin can be risky. Taking appropriate steps to minimize risks will enable adopting virtual currencies and attracting the growing user base. And if nothing else, being educated about virtual currencies will ensure being prepared for the future – whichever direction it may take.

Contact Us

To learn more about how OneBeacon Technology Insurance can help you manage online and other technology risks, please contact Dan Bauman, Vice President of Risk Control for OneBeacon Technology Insurance at dbauman@onebeacontech.com or 262.966.2739.

References

[1] The Bitcoin Wiki (n.d.). "Transaction Fees – Bitcoin" The Bitcoin Wiki. Retrieved May 29, 2014, from https://en.bitcoin.it/wiki/Transaction_fees

[2] Bitcoin.org FAQ (n.d.). "FAQ – Bitcoin". Retrieved May 29, 2014 from https://bitcoin.org/en/faq#who-created-bitcoin

[3] Bitcoin.org Developers (n.d.). "Developers – Bitcoin". Retrieved May 29, 2014 from https://bitcoin.org/en/development

[4] Bitcoin.org FAQ (n.d.). "FAQ – Bitcoin". Retrieved May 29, 2014 from https://bitcoin.org/en/faq#how-are-bitcoins-created

[5] Butcoin.org FAQ (n.d.). "FAQ – Bitcoin". Retrieved May 29, 2014 from https://bitcoin.org/en/faq#why-do-bitcoins-have-value

[6] The Bitcoin Wiki (n.d.). "Securing Your Wallet – Bitcoin". Retrieved May 29, 2014 from https://en.bitcoin.it/wiki/Securing_your_wallet

[7] The Bitcoin Wiki (n.d.). "Block Chain – Bitcoin". Retrieved May 29, 2014 from https://en.bitcoin.it/wiki/Block_chain

[8] Bitcoin.org (n.d.). "How Does Bitcoin Work? – Bitcoin". Retrieved May 29, 2014 from https://bitcoin.org/en/how-it-works

[9] Bitcoin.org FAQ (n.d.). "FAQ –Bitcoin". Retrieved May 29, 2014 from https://bitcoin.org/en/faq#mining

[10] Nakamoto, Satoshi (May 24, 2009). "Bitcoin: A Peer to Peer Electronic Cash System". (https://bitcoin.org/bitcoin.pdf. Page 3.

[11] The Bitcoin Wiki (n.d.). "Controlled Supply – Bitcoin". Retrieved May 29, 2014 from https://en.bitcoin.it/wiki/Controlled_Currency_Supply

[12] Ibid 10.

[13] Ibid 10, Page 4.

[14] Ibid 10.

[15] Ibid 10.

[16] Bitcoin.org FAQ (n.d.). "FAQ – Bitcoin". Retrieved May 29, 2014 from https://bitcoin.org/en/faq#why-do-i-have-to-wait-10-minutes

[17] The Bitcoin Wiki (n.d.). "Wallet Security Dos and Don't's (general) – Bitcoin". Retrieved May 29, 2014 from https://en.bitcoin.it/wiki/Wallet_Security_Dos_and_Don%27ts_(general)

[18] Bitcoin.org FAQ (n.d.). "FAQ – Bitcoin". Retrieved May 29, 2014 from https://bitcoin.org/en/faq#what-are-the-advantages-of-bitcoin

[19] Ibid 10, Page 6.

[20] Bitcoin Charts (n.d.). "Bitcoin Charts / Charts". Retrieved May 29, 2014 from http://bitcoincharts.com/charts/bitstampUSD#rg730ztgCzm1g10zm2g25

[21] IRS (March 25, 2014). "IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply". Retrieved May 29, 2014 from http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance

[22] Cooper, Charles (April 3, 2014). "Supervisory Memorandum – 1037" Texas Department of Banking. http://www.dob.texas.gov/public/uploads/files/Laws-Regulations/New-Actions/sm1037.pdf

[23] Lawsky, Benjamin (March 11, 2014). "In the Matter of Virtual Currency Exchanges" New York State Department of Financial Services. http://www.dfs.ny.gov/about/po_vc_03112014.pdf

[24] Krebs on Security (February 14, 2014). "Florida Targets High-Value Bitcoin Exchangers – Krebs on Security" http://krebsonsecurity.com/2014/02/florida-targets-high-dollar-bitcoin-exchangers/#more-24742

[25] Mongiovi, Jamie (March 18, 2014). "Consumer Alert: Virtual Currencies", Florida Office of Financial Regulation (OFR). Retrieved May 29, 2014 from http://www.flofr.com/PressReleaseDetail.aspx?id=4251

[26] BitLegal (n.d.). "Iceland – BitLegal". Retrieved on May 29, 2014 from http://bitlegal.net/list.php

[27] VietNamNet (February 4, 2014). "First bitcoin online trading floor in Vietnam illegal- News VietNamNet". Retrieved May 29, 2014 from http://english.vietnamnet.vn/fms/business/98789/first-bitcoin-online-trading-floor-in-vietnam-illegal.html

[28] Song, Sophie (March 27, 2014). "The Rise And Fall Of Bitcoin In China: Central Bank Shuts Down All Chinese Bitcoin Exchanges". Retrieved on May 29, 2014 from http://www.ibtimes.com/rise-fall-bitcoin-china-central-bank-shuts-down-all-chinese-bitcoin-exchanges-1563826

[29] Srivas, Anuj (December 24, 2013). "Reserve Bank Warns against Bitcoin Use" The Hindu. Retrieved on May 29, 2014 from http://www.thehindu.com/business/Economy/reserve-bank-warns-against-bitcoin-use/article5497653.ece

[30] BitLegal (n.d.). "Russia – BitLegal". Retrieved on May 29, 2014 from http://bitlegal.net/list.php

[31] Pichel Abigail (n.d.). "Cybercriminals Unleash Bitcoin-Mining Malware" TrendMicro. Retrieved on May 29, 2014 from http://about-threats.trendmicro.com/us/webattack/93/Cybercriminals+Unleash+BitcoinMining+Malware

[32] Litke, Pat and Stewart, Joe (February 26, 2014). "Cryptocurrency-Stealing Malware Landscape", Dell SecureWorks. Retrieved on May 29, 2014 from http://www.secureworks.com/cyber-threat-intelligence/threats/cryptocurrency-stealing-malware-landscape/

[33] Felton, Ed (February 12, 2014). "Understanding Bitcoin's transaction malleability problem", Freedom to Tinker. Retrieved on May 29, 2014 from https://freedom-to-tinker.com/blog/felten/understanding-bitcoins-transaction-malleability-problem/

[34] McMillan, Robert (March 3, 2014). "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster", Wired. Retrieved on May 29, 2014 from http://www.wired.com/2014/03/bitcoin-exchange/

[35] Urquhart, Jim (March 5, 2014). "Bitcoin bank Flexcoin shuts after hacking theft", Reuters. Retrieved on May 29, 2014 from http://www.reuters.com/article/2014/03/05/us-bitcoin-flexcoin-idUSBREA2329B20140305