Bitcoin: The Future of Digital Payments?

Prateek Vachher vachh007@umn.edu

In just a meager ten years, Bitcoin has gone from being a relatively obscure piece of code to an internationally recognized form of payment. Yet, opinions about Bitcoin's future are mixed. After considering the major factors affecting Bitcoin's future use, the research paper offers some trend and attribute analysis which acts as modest predictions. Both systems are currently co-existing alongside each other. Both look like they are here to stay for the foreseeable future, although the rise of Bitcoin is causing banks to rethink certain areas like transaction fees and how they link between countries, among other things.

1. About Virtual Currencies

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." Attributes of a real currency, as defined in 2011 in the Code of Federal Regulations, such as real paper money and real coins are simply that they act as legal tender and circulate "customarily". The IRS decided in March 2014, to treat Bitcoin and other virtual currencies as property for tax purposes, not as currency. Some have suggested that this makes Bitcoins not fungible—that is one Bitcoin is not identical to another Bitcoin, unlike one gallon of crude oil is identical to another gallon of crude oil—making Bitcoin unworkable as a currency. Examples of Virtual Currencies: Bitcoin, Litecoin, Dogecoin, etc.

1.1. About Bitcoin

Bitcoin is a virtual cryptographically secured currency that was created in the year 2009. Bitcoin is not owned by a company or any one person, in fact, the creator of Bitcoin is completely anonymous and still unknown to this day. Bitcoin is an alternative to fiat currencies by an unknowing computer scientist using the pseudonym Satoshi Nakamoto. Instead, Bitcoin is simply owned by all of the people who own Bitcoin, there is no central server, database, or website. Several online retailers such as Microsoft Store, Steam, Expedia, NewEgg, etc. have been accepting Bitcoins for store purchases from users in the United States. Transactions were supported and processed through several partner vendors for Bitcoin such as BitPay, CoinBase, etc.

One theory for the move was that with Bitcoin priced over $15,000, new participants in crypto markets who deposit a few thousand dollars are able to afford only a fraction of a Bitcoin. There's something psychologically unsatisfying about owning a fraction of something. But that same small deposit can buy hundreds or thousands of cheaper coins, fueling rallies in the upcoming cryptocurrencies. Seeing previously unknown or undiscovered coins rally like Bitcoin creates a new psychological element for participants who are now hoping to find "the next Bitcoin."

1.2. History of Bitcoin

On 18 August 2008, the domain name Bitcoin.org was registered. Later that year on 31 October, a link to a paper authored by Satoshi Nakamoto titled Bitcoin: A Peer-to-Peer Electronic Cash System (Nakamoto) was posted to a cryptography mailing list. This paper detailed methods of using a peer-to-peer network to generate what was described as "a system for electronic

transactions without relying on trust". On 3 January 2009, the Bitcoin network came into existence with Satoshi Nakamoto mining the genesis block of Bitcoin (block number 0), which had a reward of 50 Bitcoins. Embedded in the Coinbase of this block was the text:

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

The first open source Bitcoin client was released on 9 January 2009. Eventually as Bitcoin started becoming popular, a major vulnerability in the Bitcoin protocol was spotted. Transactions weren't properly verified before they were included in the transaction log or blockchain, which let users bypass Bitcoin's economic restrictions and create an indefinite number of Bitcoins.

the vulnerability was exploited on 15 August 2009; over 184 billion bitcoins were generated in a transaction and sent to two addresses on the network. Within hours, the transaction was spotted and erased from the transaction log after the bug was fixed and the network forked to an updated version of the Bitcoin protocol.

1.3. Working of Bitcoin

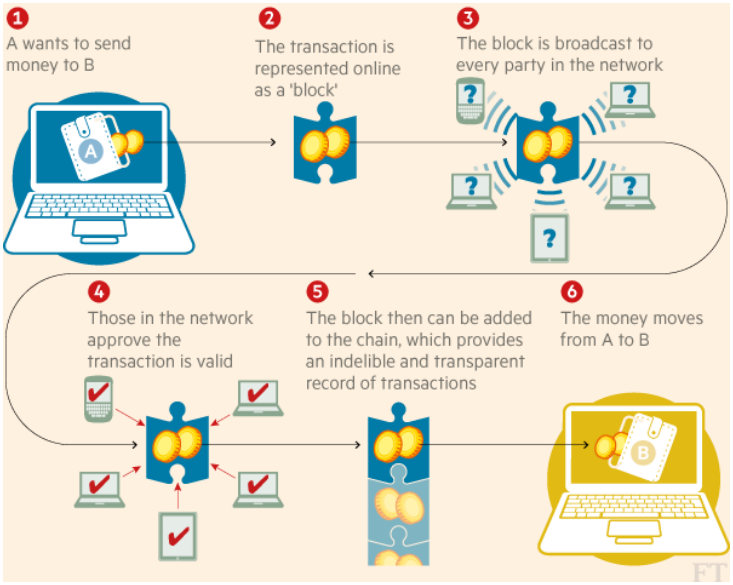
Bitcoins are not printed like fiat money, but instead, are “mined” using computing power in a distributed global network of volunteer software developers. At the core, Bitcoin is nothing more than a digital file that lists every transaction that has ever happened in the network in its version of a general ledger called the “blockchain”.

The “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 (mostly every 10 minutes) into a list called a “block”.

Mines confirm these blocks of transactions and write them into the blockchain 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 (Coindesk). Every four years, this reward is halved so that the total number of Bitcoins will never exceed 21 million[1]. Let's say Person A wants to send give Bitcoins to Person B. Person A uses a private key to sign a message with the input, the amount and the output. Person A sends this message from Person's A Bitcoin wallet into the wider Bitcoin network from where miners verify the transactions once it becomes part of a block by solving a mathematical calculation (CoinDesk). The mathematical component of the system is important to prevent fraud by ensuring that a person cannot use the same Bitcoin for multiple transactions.

Figure 2. is an image representing the working of Bitcoin.



1 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 times 50 Bitcoins)

1.4. Incidents regarding Bitcoin

Criminals have taken to Bitcoin because anyone can open a Bitcoin address and start sending and receiving Bitcoins without giving a name or identity. There is no central authority that could collect this information. Bitcoin first took off in 2011 after drug dealers began taking payments in Bitcoin on the black-market website known as the Silk Road, drug market. The U.S. Justice Department has claimed the proceeds from the sale of 144,336 bitcoins, valued at just over $48 million, that it obtained after shutting down the notorious online drug market (Roberts).

According to Digiconomist, the estimated power use of the Bitcoin network, which is responsible for verifying transactions made with the cryptocurrency, is 30.14TWh a year, which exceeds that of 19 other European countries (Digiconomist). At a continuous power drain of 3.4GW, it means the network consumes five times more electricity than is produced by the largest wind farm in Europe, the London Array in the outer Thames Estuary, at 630MW.

2. Bitcoin versus E-Money

Money, in itself, is largely worthless. It is simply a piece of printed paper or cheaply made coin used as a token to represent a given transaction. Yet, despite the apparent insubstantiality of money, few things stand shoulder to shoulder to absolute reality today than cold hard cash. From bankers to retailers, craftspeople selling their wares, or agents of the nefarious underworld, the undeniable reality of money speaks loud and clear. Today's world is bound by monetary ties, and cash flows like lifeblood around these binds.

Bitcoin shuddered into existence back in 2009, just as financial markets floundered amidst one of the worst economic recessions in recorded history. Bitcoin belongs to a subset of the digital currency known as cryptocurrency. It is so deemed because it relies on cryptography to

facilitate secure transactions, as well as the creation of new currency units to be added to an ever-increasing ledger.

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).

Table 1 provides a comprehensive comparison between e-money (traditional banking) and Bitcoin. It compares the two entities based on format (Digital), a unit of account, means for customer identification, means of production and issuing authority.

3. Key Differentiating Factors between Bitcoin and E-Money

3.1. Security

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.

Bitcoin is potentially the start of the fall of the manipulated banking system and allows a safe place to store savings and cash away from prying eyes, it is easier to conceal a private key than it is to hide funds in bank accounts. This could protect people in the event of malicious legal

cases, as there is no link between the two systems is proven and no laws are broken. In traditional banking your every action can be audited and picked up by governments, for both good and ill.

3.2. Governance

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.

Since Bitcoins cannot currently be used to purchase many things directly, 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 (Solman).

3.3. Economic

Unlike the 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). 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).

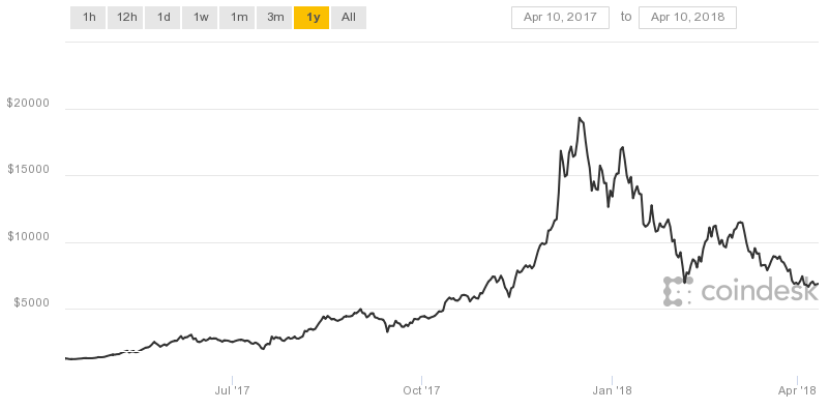


Figure 4 provides an insight into the drastic growth and decrement in the conversion rate between USD (US Dollar) and BTC (Bitcoin). At the recent Bitcoin price peak, Bitcoin had a value of 1BTC = $20,078.40.

The price of Bitcoin fluctuates in a similar way to a stock in terms of which things can cause the price to rise and fall, but unlike a stock, it is extremely unpredictable and much riskier to invest in, but also can have a bigger upside. People in countries with high inflation, like Argentina and Venezuela, have bought Bitcoin with their local currency to avoid losing their savings to inflation.

In 2010 the first documented purchase with Bitcoin occurred when one man paid the delivery guy 10,000 bitcoins in exchange for 2 large pepperoni pizzas. At the time this equaled about $21, but today those pizzas would be worth a whopping $45 million USD! This will be forever known in the Bitcoin community as "*The Bitcoin Pizza*".

3.4. Technological

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 make up a part of the network.

On the other hand, the traditional banking system has an already established system, and their bank cards are accepted nearly everywhere in the world. Use of cash doesn't require a network connection or electricity.

Conclusion

Both systems are currently co-existing alongside each other. Both look like they are here to stay for the foreseeable future, although the rise of Bitcoin is causing banks to rethink certain areas like transaction fees and how they link between countries, among other things. The banking system is open to manipulation while Bitcoin is pretty much tamper proof and allows the control of no one individual or corporation.

The chances are the adoption of Bitcoin or other decentralized currencies will increase due to its ease of use and the advantage of being tamper proof. The developers and community are working on capacity issues which would when the solutions are implemented, and conscious agreed, solve this hurdle. In poor countries with limited access to the internet or areas without electricity such as many places in rural India for example, there are still hurdles to cross there.

Bibliography

Ashford, Karen. “The Ripple Effect of Holden’s Closure.” *Forbes*, 2013, https://www.forbes.com/sites/forbesproductgroup/2018/01/11/the-ripple-effect-of-cryptocurrencies/#23abcee16080.

Böhme, Rainer, et al. “Bitcoin: Economics, Technology, and Governance.” *Journal of Economic Perspectives*, vol. 29, no. 2, 2015, pp. 213–38, doi:10.1257/jep.29.2.213.

Coindesk. “How Do Bitcoin Transactions Work?” *Coindesk*, 2015, pp. 1–5, https://www.coindesk.com/information/how-do-Bitcoin-transactions-work/.

Digiconomist. “Bitcoin Energy Consumption Index - Digiconomist.” *Digiconomist*, 2018, pp. 1–8, https://digiconomist.net/Bitcoin-energy-consumption.

Gervais, Arthur, et al. “Is Bitcoin a Decentralized Currency?” *IEEE Security and Privacy*, vol. 12, no. 3, 2014, pp. 54–60, doi:10.1109/MSP.2014.49.

Giungato, Pasquale, et al. “Current Trends in Sustainability of Bitcoins and Related Blockchain Technology.” *Sustainability (Switzerland)*, vol. 9, no. 12, 30 Nov. 2017, p. 2214, doi:10.3390/su9122214.

Hern, Alex. “Is Bitcoin About to Change the World?” *The Guardian*, 2013, https://www.theguardian.com/technology/2013/nov/25/is-Bitcoin-about-to-change-the-world-peer-to-peer-cryptocurrency-virtual-wallet.

How Cryptocurrency Is Disrupting the Global Economy. https://medium.com/the-mission/how-cryptocurrency-is-disrupting-the-global-economy-89347581aa93. Accessed 5 Apr. 2018.

Lee, Timothy. *12 Questions about Bitcoin You Were Too Embarrassed to Ask - The Washington Post*. 2013, https://www.expressnews.com/business/national/article/12-questions-about-Bitcoin-you-were-too-5022610.php.

Luther, William J. "Bitcoin and the Future of Digital Payments." *Independent Review*, vol. 20, no. 3, 2016, pp. 397–404, doi:10.2139/ssrn.2631314.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *Www.Bitcoin.org*, 2008, p. 9, doi:10.1007/s10838-008-9062-0.

Popper, Nathaniel. "What Is Bitcoin, and How Does It Work? - The New York Times." *The New York Times*, 2017, https://www.nytimes.com/2017/10/01/technology/what-is-Bitcoin-price.html%0Ahttps://www.nytimes.com/2017/10/01/technology/what-is-Bitcoin-price.html%0Anyti.ms/2iXKYLw.

Popper, Nathaniel. "What Is Bitcoin, and How Does It Work? - The New York Times." *The New York Times*, 2017, https://www.nytimes.com/2017/10/01/technology/what-is-Bitcoin-price.html.

Roberts, Jeff John. "Silk Road Bitcoin Sale: U.S. Makes $48 Million | Fortune." *Fortune*, 2017, http://fortune.com/2017/10/02/Bitcoin-sale-silk-road/.

Sen, Conner. “Cryptocurrencies Are Starting to Affect the Real Economy.” *Bloomberg*, 2017, https://www.bloomberg.com/view/articles/2017-12-18/cryptocurrencies-are-starting-to-affect-the-real-economy.

Solman, Paul. “The Mathematician’s Defense of Bitcoin: It’s Just Another Option | PBS NewsHour.” *PBS NewsHour*, 2013, https://www.pbs.org/newshour/economy/the-mathematicians-defense-of-Bitcoin-its-just-another-option.

Vasek, M. “The Age of Cryptocurrency.” *Science*, vol. 348, no. 6241, American Association for the Advancement of Science, June 2015, pp. 1308–09, doi:10.1126/science.aab2001.