

# THE EVOLUTION OF BITCOIN AND OTHER CRYPTOCURRENCIES

Prashant Bhatt<sup>1</sup>, Maan Singh Choudhary<sup>2</sup>

<sup>1</sup>Department of Computer Application, Uttaranchal University, Dehradun, India, E-mail : prashantbhatt198@gmail.com

<sup>2</sup>Department of Computer Application, Uttaranchal University, Dehradun, India, E-mail : maanchoudhary400@gmail.com

**Abstract-** *Cryptocurrency is a digital or virtual money or asset that is meant to function as a means of exchange and is safeguarded by encryption. Although Bitcoin was not the first effort at digital money, it has proven to be the most successful, and it is currently accepted by the majority of big businesses. Bitcoin is a peer-to-peer cryptocurrency that works on a peer-to-peer network. Its security is ensured by cryptographic algorithms rather by governments, and it has the potential to become a significant method of payment for e-commerce, as well as a credible competitor to existing money-transfer services.*

**Keywords -** *Digital Currency, Bitcoin, Cryptographic Currencies, Cryptographic Algorithm, Cryptocurrency, Blockchain*

## 1. INTRODUCTION

Rose, C. (2015). When you compare two pieces of money from the 19th century, you'll see a silver coin and paper money that could be traded for an equal coin at the time. Paper rupee banknotes were backed by silver more than a century ago, a precious metal that should theoretically always have value. However, this has altered in recent years, and modern money is now backed only by the Indian government's word. As a result, the government can do anything they want; they can manufacture more folding money, devalue the currency whenever they want, and, while improbable, the currency may even vanish entirely.

Although the phrases virtual money, digital currency, and cryptocurrency are sometimes used interchangeably, there is a fundamental distinction between them.

**Virtual Currency:** A virtual currency, according to the ECU financial organization, is "a kind of unregulated, digital money that is produced and often controlled by its creators, and used and accepted among members of a specific virtual community." Although a digital currency functions similarly to a traditional money, it does not have the same characteristics, according to the US Department of Treasury.

**Digital Currency:** may be a kind of virtual money that is produced and held electronically. Cryptocurrencies are some, but not all, digital currencies.

**Cryptocurrency:** may be a subset of digital currencies, however, it uses cryptography for security so this makes it extremely difficult to counterfeit (Gilpin, 2014).

One of the most essential aspects of cryptocurrencies is that they are not issued by any central body and are not backed by regular banks. Many people do not believe them to be money, despite the fact that they may someday pose a serious threat to conventional money. Many individuals do not trust in the rupee, the dollar, the ruble, the yen, or any other official money; instead, they trust in gold and silver. However, many of us are starting to trust in cryptocurrencies. "Bitcoin was designed to take power away from the government and central bankers and put it in the hands of the people." (Gilpin, 2014).



## 2. DEVELOPMENT

A programmer (or potentially a group of programmers) known as Satoshi Nakamoto wrote a paper outlining digital currency in 2008, and the Bitcoin network was built the following year (Metz, 2013). Unlike official currencies, Bitcoin is not backed by a financial institution, and anybody with a computer or an Application-Specific Microcircuit (ASIC), which is a specialized processor designed exclusively for the purpose, may generate a Bitcoin via a process known as mining. Because each member in Bitcoin has theoretically equal authority, it is relatively quick, inexpensive, and simple to attempt. Because there are no banks and hence no bankers, everyone saves their own Bitcoin in a virtual account known as a wallet. Users have complete control over their funds, and they may transfer micropayments as tiny as one Satoshi, or 0.00000001BTC (a Bitcoin to eight decimal places), or around 0.028 Indian Rupee today. The value of a Bitcoin, like the value of any other money, is determined by the customer's willingness to pay. Bitcoin may not have any worth if no one used it, but it may have any price, and volatility is widespread, making and losing fortunes for many individuals in the process (Kelion, 2013).

Because no one controls the network, no one, organization, or government can guarantee Bitcoin. This implies that there is no assurance that Bitcoin will maintain a stable connection with any traditional currency. Bitcoin fluctuates in value versus traditional currencies, rising from less than a dollar in 2011 to about \$1,200 in 2013 and now hovering around \$38,000. Furthermore, since Bitcoin is open source, anybody can take the ASCII text file, make minimal changes, and establish a network that is similar to Bitcoin's, resulting in the creation of their own money. Because the basic Bitcoin protocol is exceedingly difficult to change owing to the network's decentralization, if someone feels they need a significantly superior virtual currency, it's far simpler to establish their own than to persuade Bitcoin users to change (Lee, 2013).

Thousands of participants compete in Bitcoin mining to solve a mathematically complicated repetitious issue. If a person solves the problem, they will be given the ability to add a block to the Bitcoin global transaction registry as well as 25 Bitcoins as a prize. However, since it requires so much processing power, the most common method is to join a mining pool of thousands of users who individually contribute their processing power to solving the issue in exchange for a piece of the earnings. Originally, it was expected that Bitcoin would be the "people's money," with decentralized processing power and everyone having an equal chance of solving the Bitcoin issue, known as a hash function. However, specialist technology created expressly for this purpose has emerged to solve this hash function more efficiently. What happened is that instead of the average person attempting to mine Bitcoin with their computer, it's now the domain of people or groups of persons spending tens of thousands of dollars on specialized gear with just one purpose: to unravel the hash function (Lee, 2013). Because every Bitcoin transaction is public, it's simple to track down individuals or groups of persons who are mining Bitcoin for \$3,000 per day or \$1 million per year.

Using these AICS is so much more efficient that it's worth it. The banking system is currently sluggish, and it relies on antiquated infrastructure to transmit money across the globe, which may take days or weeks. Banks were only able to provide same-day payments after the Office of Fair Trading "dragged them into the nineteenth century." Metro Bank acquired the first new UK banking license in 150 years when it started in 2010." (Kelion, 2013).

Bitcoin might be a new economic system created by and for the people, with everyone having equal authority. People manage their own money, and as a result, the Bitcoin system's laws are imposed on everyone via mutual mistrust (Kelion, 2013). Except in the rare circumstance of controlling 51 percent of the whole network, no one can tamper with or affect the system.

## 3. VALUE

Rose, C. (2015). Bitcoin was once of little interest to the general public, since only cryptographers, hackers, and mathematicians understood its purpose and use. It's produced by an algorithm, it's hard to forge, it's mostly anonymous, and there are no extra costs from intermediaries like banks since it's a peer-to-peer network. Indeed, these are the characteristics of a money that is well suited to our current digital economy. Although the value of Bitcoin may be a mix of speculation on future value and true, irrefutable use, the dramatic price fluctuations Bitcoin has seen are a logical response to the massive worldwide interest in a pool of currency that is very small in comparison to its government-backed rivals.

However, Bitcoin's unpredictable fluctuations are preventing it from fulfilling its true potential as a creative new kind of money. Although many businesses have declared that they accept Bitcoin, from PayPal to Dell to Newegg to Lamborghini dealers to Virgin Galactic, it's difficult to simply accept a payment that could lose half its value overnight or double in the next week, and even though it has the potential to become the essential medium of exchange on the internet "its high volatility, a result of speculative activities (Popper, 2013).

Network externalities exist with virtual currencies; the more individuals who use them, the more valuable they become. Because Bitcoin was the first digital money to be accepted, it has a significant advantage. Bitcoin receives the greatest attention and has the most supporters and merchants, as well as the most users involved in it. Bitcoin has the potential to be the most significant digital money eternally as long as it continues to meet the needs of users. And, although many suggested Bitcoin upgrades are conceptually appealing, none seem to be ready to persuade consumers to change in substantial numbers (Lee, 2013). "Bitcoin has the potential to become a substantial e-commerce payment method and a major rival to established money-transfer services. Bitcoin, as a means of trade, has a lot of room for development, in our opinion " (Popper, 2013).

#### 4. HOW IT WORKS

C. Rose (2015). Bitcoin is a peer-to-peer electronic cash system. In a traditional payment system, such as Paytm, Visa, MasterCard, or PayPal, there is a business in the middle, a for-profit organization that centralizes payments, manages the network, and ensures its security and reliability. Bitcoin, on the other hand, follows a totally different model: rather than being guaranteed by a government or governments, its security is assured by a cryptographic technique, the Secure Hash Algorithm (SHA) which is 256 bits (SHA-256). If you put one dollar into PayPal, for example, the PayPal network will ensure that you will be able to withdraw one dollar anytime you want. Using a regular PC to mine Bitcoin is no longer cost-effective, since the power used is equal to the value of the Bitcoin mined. Instead, massive groups of users form, with these groups controlling the majority of the network's computational capacity. Litecoin (often referred to as the silver to Bitcoin's gold) is a popular alternative to Bitcoin that employs the Scrypt algorithm, which is said to be more difficult to automate. However, given the amount of money that might be earned, it was unavoidable that specialised equipment for the Scrypt algorithm be developed, and since 2014, there have been various Scrypt ASIC devices available on the market.

#### 5. LEGALITY

"The Department of Justice understands that many virtual currency systems provide lawful financial services and have the potential to enable more efficient global commerce," according to the Justice Department. Ribeiro (Ribeiro, 2013). You may buy anything from "beer in Berlin, pizza in Amsterdam, a cab in Edinburgh, a dental check-up in Ljubljana, a degree in Nicosia, Alpaca socks from Massachusetts - or maybe even a space flight with Virgin Galactic" (Kelion, 2013).

Laszlo Hanyecz, a Florida programmer, used 10,000 Bitcoin to buy two pepperoni pizzas from Papa John's in May 2010. This was the first commercial transaction utilizing Bitcoin. Hanyecz estimated that \$60 worth of Bitcoin was enough for two pizzas and remuneration for someone's work at the time, but that quantity of Bitcoin is now worth roughly \$5 million (Griswold, 2014).

Bitcoin is a significant advancement in the history of money that is predicted to grow in popularity as the number of organizations and individuals who accept Bitcoin as payment grows. To bring Bitcoin into the mainstream, everyone must be persuaded that it is genuine, secure, and valuable. "It's like being on the cutting edge of the Internet 20 years ago,"... "Bitcoin will be transformational" (Leinwand, 2013) However, since it is almost untraceable, it has been utilized for a variety of illicit objectives. "However, we have noticed that some elements of virtual currencies appeal to criminals, posing a variety of new enforcement challenges," says the report. Ribeiro (Ribeiro, 2013).

#### 6. CONCLUSION

C. Rose (2015). If you see someone promoting Bitcoin at a university, they are most likely from the computer science department, and if you see someone condemning Bitcoin, they are most likely from the economics department. The reason for this is because the long-term prospects for Bitcoin are bleak. Starting an altogether new idea that relies on a large number of people adopting and adopting it is incredibly tough, and it's much more difficult when the new idea involves a whole new payment and monetary system. There are a plethora of reasons that Bitcoin might fail. "The technology is broken. Excessive speculation results in an unrecoverable crash. The pricing is never stable. Liquidity is obliterated by deflationary pressure. It is shut down by the government. It becomes outdated as a result of the introduction of a new currency. Users forsake it for a variety of reasons" (Jeffries, 2013). Economists have never had to think about a system like Bitcoin before it was created, and they are just now starting to analyze the implications. Some economists say Bitcoin will fail because the cost of making a Bitcoin clone is negligible, but Bitcoin might potentially destabilize the whole monetary system.

Money should be a trustworthy means of trade as well as a secure store of value. Money that is a dependable store of value is generally supported by a government or other central authority, or it's intrinsic worth, such as gold or silver, which gives most economists issues. People will not trust it over time if it lacks support and genuine worth (Jeffries, 2013). Bitcoin, on the other hand, has a finite quantity; after 21 million Bitcoins have been generated, no more will be generated. As a result, Bitcoin's availability is much more inelastic than gold's, and its supply is also significantly more visible than gold's. Bitcoin, like gold, can not depreciate and is perfectly divisible; it has no issuing authority or nation of origin, making it a truly global currency that may be used to transact between any two parties anywhere on the planet. Because there is no central authority or bank, it is also the final word in disintermediation. It is both a monetary mainstay and a payment method in one and needs no storage. Either Bitcoin fails and becomes worthless, or it succeeds and each Bitcoin is worth hundreds of thousands, if not millions, of dollars in conventional currency. Those who invest in Bitcoin should consider it a speculative bet on the success of cryptocurrencies in the future (Schlichter, 2013).

#### REFERENCES

- [1] Rose, C. (2015). The Evolution Of Digital Currencies: Bitcoin, A Cryptocurrency Causing A Monetary Revolution. *International Business & Economics Research Journal (IBER)*, 14(4), 617-622. <https://doi.org/10.19030/iber.v14i4.9353>

- [2] Gilpin, L. (2014) 10 things you should know about Bitcoin and digital currencies. TechRepublic. Retrieved 20/5/2021 from <http://www.techrepublic.com/article/10-things-you-should-know-about-bitcoin-and-digital-currencies/>
- [3] Griswold, A. (2014) The First-Ever Bitcoin Purchase Was Remarkably Inglorious. Slate.com. Retrieved 6/4/2021 from [http://www.slate.com/blogs/moneybox/2014/05/23/first\\_bitcoin\\_purchase\\_two\\_pepperoni\\_pizzas\\_from\\_papa\\_john\\_s.html](http://www.slate.com/blogs/moneybox/2014/05/23/first_bitcoin_purchase_two_pepperoni_pizzas_from_papa_john_s.html)
- [4] Metz, C. (2013) For Bitcoin's Biggest Believers, Digital Currency Is Better Than Gold. Wired. Retrieved 14/4/2021 from <http://www.wired.com/2013/10/bitcoin-in-japan/>
- [5] Ribeiro, J. (2013) US agencies see some benefits in virtual currencies. PCWorld. Retrieved 5/5/2021 from <http://www.pcworld.com/article/2064800/us-agencies-coming-around-cautiously-to-seeing-benefits-in-virtual-currencies.html>
- [6] Jeffries, A. (2013) The Verge. Why don't economists like Bitcoin? Retrieved 1/4/2021 from <http://www.theverge.com/2013/12/31/5260534/krugman-bitcoin-evil-economists.html>
- [7] Leinwand, D. USA Today. Bitcoin: Super currency or super fad? Retrieved 12/4/2021 from <http://www.usatoday.com/story/news/nation/2013/12/10/bitcoin-entrepreneurs-seek-mainstream-acceptance.html>
- [8] Metz, C. (2013) For Bitcoin's Biggest Believers, Digital Currency Is Better Than Gold. Wired. Retrieved 7/5/2021 from <http://www.wired.com/2013/10/bitcoin-in-japan.html>
- [9] Popper, b. (2013) The Verge. Bitcoin is too cheap for its own good. Retrieved 17/4/2021 from <http://www.theverge.com/2013/12/9/5192054/bitcoin-boom-bust-bubble-currency-technology>
- [10] Schlichter, D. (2013) Could Bitcoin be the money of the future? Retrieved 4/4/2021 from <http://detlevschlichter.com/2013/04/could-bitcoin-be-the-money-of-the-future>