International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

An introduction about Cryptocurrencies

SHENBAGAVADIVU T [1, *], MADHUMITRA AP [2], PERARUL SELVAN D [2], PRASANTH R [2] and BALAJI R [2]

[1] *Department of Commerce Business Application, Sri Krishna arts and science college, Coimbatore.*
[2] *Master of International Business, Sri Krishna arts and science college, Coimbatore.*

International Journal of Science and Research Archive, 2023, 08(02), 305–308

Publication history: Received on 28 January 2023; revised on 11 March 2023; accepted on 14 March 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.8.2.0210

Abstract

The researchers provide a brief definition of bitcoin in this paper along with a quick introduction to cryptocurrencies. The study looks at the role cryptocurrencies play in modern technology and how bitcoin has evolved in relation to spot contracts.

Keywords: Cryptocurrencies; Block chain; Bitcoin; Digital Money

1. Introduction

The "Satoshi Nakamoto" white paper, which was released in 2008, is where Bitcoin first appeared. It looks like an academic work and was distributed via an email group for cryptography. The original goal of Bitcoin's developers was to create a cash-like payment system that would allow for electronic transactions while also retaining many of the beneficial aspects of actual cash. We will start our research by thinking about a straightforward cash transaction in order to better comprehend the unique characteristics of physical monetary units and the need to generate digital cash.

2. Review of Literature

The origin of bitcoin's value is among its most perplexing features. The regression theorem of Ludwig von Mises has been said to be violated by bitcoin (LeRoux, 2014).

The regression theorem shows that all money must ultimately derive its purchasing power from a historical connection to a commodity that was valued in a condition of barter, regardless of whether the money is government-backed fiat currency or a commodity like gold.

The value of money theory as such can only trace back the objective exchange value of money to the point where it ceases to be the value of money and becomes merely the value of a commodity,

According to Jeffrey Tucker (2014) in his article titled, "What Gave Bitcoin Its Value," published by the Foundation for Economic Education.

2.1. Digital Cash

A payment system that allows for the electronic transmission of money via cash data files would be perfect. Such monetary data files would be able to move freely over electronic networks while retaining the benefits of actual cash. This kind of data package could be distributed by email or social media.

* Corresponding author: T. Shenbagavadivu
Department of Commerce Business Application, Sri Krishna arts and science college, Coimbatore

Electronic data has the unique ability to be replicated numerous times for very little expense. For money, this feature is quite unwelcome. Cash data files cannot be utilised as a payment method if they may be copied and used as currency. The "double spending dilemma" is the name given to this issue.

3. Characteristics of Cryptocurrency

A cryptocurrency is a form of digital or virtual money that is secured by encryption. This security characteristic makes a cryptocurrency difficult to forge. The organic nature of a cryptocurrency is one of its distinguishing characteristics and possibly its most charming allure. Since it was not issued by a centralised authority, it is theoretically shielded from influence or manipulation by the government. It is built from the ground up to benefit from how the internet operates. Cryptocurrency transactions are confirmed by user computers connected to the currency's network, as opposed to traditional financial institutions that rely on them to do so. It becomes difficult to raise the money supply over a set algorithmic pace since the currency is secure and encrypted.

3.1. Bitcoin Transactions

The present material's intricacy is a result of its interdisciplinarity. Combining components from the three fields of economics, cryptography, and computer science is important to comprehend the Bitcoin system. After giving a general overview of the Bitcoin system, we will go into further detail on a few technical aspects of the system. Blockchain connects established technologies in a novel way using these technologies. For the first time, this combination enables the decentralised maintenance of a ledger.

3.2. Transaction Capability

A payment order can be sent to any number of network nodes in the Bitcoin system. The message is forwarded until all nodes have been informed of the transaction by the network nodes, which are connected in a loose network.

The system's decentralisation offers various benefits. In particular, it greatly strengthens the system. Both a targetable central point of failure and system-relevant nodes that could bring the system down are absent. The system can always create new connections and communication channels, so it can still operate even if certain network nodes are unavailable. Transaction Legitimacy:

A symmetric cryptography is used in the Bitcoin system to guarantee the legitimacy of transactions. The concept is based on the use of key pairs made up of a private key and a public key. Sharing a private key is not advised. It relates to a value chosen at random from an enormous collection of numbers.

On the other hand, a public key is created from that number and is open to sharing. It functions as an alias in the Bitcoin network. A message is encrypted using a private key, and can only be unlocked using the associated public key. Another name for this kind of encryption is "signature." The signature makes it clear that no information in the encrypted communication is hidden using this method.

A message is encrypted using a private key, and can only be unlocked using the associated public key. Another name for this kind of encryption is "signature." The signature makes it clear that no information in the encrypted communication is hidden using this method.

The signature, which is similar to a handwritten signature but far more secure, serves as evidence that the communication has been previously encrypted using its associated private key, despite the fact that anyone may easily decrypt a message using its public key.

3.3. Outlook

Like any fundamental invention, blockchain technology won't reach its full potential until many years, if not decades, after it is widely used.

Therefore, it is impossible to predict the industries in which blockchain technology will be most effective. However, we want to highlight a few areas where blockchain technology can be used as an infrastructure platform to support a wide range of exciting applications.

3.4. Crypto assets

The use of bitcoin as an asset is the most obvious. Crypto assets like Bitcoin are expected to become their own asset class, giving them the potential to grow into an intriguing investment and diversification tool. Over time, Bitcoin itself might come to play a similar role to gold.

Furthermore, there is significant potential for trading equities on a public blockchain. On the Bitcoin (or a comparable) Blockchain, so-called coloured coins can be traded and used in smart contracts, as will be discussed below.

3.5. Coloured coin

A promise of payment associated with a Bitcoin transaction is a coloured coin. This promise is made feasible by the Bitcoin network's communication protocol, which enables the tying of additional data to transactions. Promises to supply an ounce, for instance

A dividend payment or a purchase of gold can be included in a Bitcoin transaction and shown as such on the Bitcoin Blockchain. Of course, issuer risks apply to all of these assurances, and some degree of faith is necessary. Compared to native crypto assets like Bitcoin units, this is a stark contrast.

3.6. Smart Contracts

Self-executing contracts are smart contracts. 8 They can be used to specify that a Bitcoin payment will only be carried out when a specific requirement is satisfied. In terms of smart contracts, the Ethereum network is currently in the forefront. It uses blockchain technology, much like Bitcoin, and offers Ether, a native crypto asset. Ethereum offers a more adaptable scripting language than Bitcoin and has the ability to track contractual situations. E-voting systems, identity management, decentralised organisations, and various funding methods (like initial coin offerings) are just a few examples of potential uses.

3.7. Data Integrity

The ability to watch over data files is another use case for public blockchains. We've already demonstrated how crucial a role block candidates' fingerprints play in the Bitcoin network. All types of data files can be given fingerprints using the same technology, which can then be used to store them in a blockchain. The inclusion of a fingerprint assures that any effort at manipulation will be exposed because any modification to the data file will result in an entirely different hash value. A fingerprint can be used as evidence that a given data file existed at a specific moment and maintains the integrity of the data because it is very difficult to edit a blockchain retrospectively.

3.8. Risks

As with every significant invention, there are hazards associated with blockchain technology. Some of these risks will be discussed in the sections that follow. We would like to point out that this list is not exhaustive, as we said in Section 3.

3.9. Forks

If the network users, or at least a substantial number of them, agree on the proposed adjustment the Bitcoin protocol may be changed. Because different groups cannot agree on a revision, it is possible (and has actually happened) for a blockchain to split. Fork is the term used to describe a split that endures. The ideological split between Ethereum and Ethereum Classic and the Bitcoin Cash fork are the two most prominent examples of enduring splits.

3.10. Energy Wastage

Proof-of-work mining is costly since it consumes a lot of energy. Some critics of Bitcoin contend that a centralised accounting system is more effective since it enables consensus without requiring the allocation of enormous quantities of processing resources.

But from our vantage point, things are not so simple. The cost of centralised payment systems is likewise high. A central bank's explicit and implicit expenses would need to be determined in addition to those for infrastructure and operations. Payroll expenses should be included in the explicit costs, and the potential for currency monopoly fraud should be included in the implicit costs. Additionally, a lot of crypto assets employ alternative consensus mechanisms that don't (exclusively) rely on computational resources.

3.11. Bitcoin Price Volatility

The cost of Bitcoin fluctuates a lot. This raises the issue of whether Bitcoin's rigidly set supply is a desirable monetary policy in the sense that it results in a stable currency. The answer is no since overall demand also affects the price of bitcoin. Prices fluctuate when a consistent supply of money meets a changing total demand. In government-run fiat currency systems, the central bank seeks to stabilise the price level by adjusting the money supply in response to variations in aggregate demand for money. The Federal Reserve System was specifically established "to provide an elastic currency" to reduce price variations brought on by shifts in the overall demand for the US dollar. Since the current Bitcoin protocol lacks such a mechanism, it is quite likely that the Bitcoin unit will experience far greater short-term price swings than many types of government-issued fiat currency.

4. Conclusion

The goal of Bitcoin's developers was to create a decentralised electronic payment system that resembled cash. In this process, they had to overcome the basic difficulty of establishing and transferring a monetary unit's digital property rights in the absence of a central authority. Berentsen and Schär Federal Reserve Bank of St. Louis REVIEW First Quarter 2018 15 by creating the Bitcoin Blockchain, they overcame this difficulty. Similar to cash, this revolutionary technology enables us to keep and transfer money without the need for a central authority.

The suitability of Bitcoin as a payment method is regularly questioned because to price volatility and scaling problems. Bitcoin and other blockchain-based tokens should not be overlooked as an asset, nevertheless. The development enables the representation of digital property without the need for a central authority. This could result in the emergence of a brandnew asset class that develops into an important tool for portfolio diversification. Additionally, blockchain technology offers a foundation for a wide range of applications. The use of coloured currencies, smart contracts, and the potential use of fingerprints to secure the integrity of data files on a blockchain are all promising applications that have the potential to transform the financial industry and many other fields.

Compliance with ethical standards

Acknowledgments

We are grateful for those who assist us in the production of this review, special thanks to professor T. Shenbagavadivu.

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Aleksander Berentsen, "Monetary Policy Implications of Digital Money." 89–117; doi:10.1111/1467-6435.00039; Kyklos (International Review of Social Sciences), 1998, 51(1).

[2] Fabian Schär and Alexander Berentsen. A thorough introduction to Bitcoin, Blockchain, and Cryptoassets. Norderstedt, 2017's Books on Demand.

[3] William H. Furness is the author of The Island of Stone Money: Uap of the Carolines. 1910. Philadelphia: J. B. Lippincott.

[4] Randall Wright and Nobuhiro Kiyotaki. An analysis of monetary economics using search theory. 1993, 83(1), pp. 63–77 of the American Economic Review

[5] Sunita Nakamoto Bitcoin: An Electronic Cash System Used Between Peers. https://bitcoin.org/bitcoin.pdf; 2008

[6] 2018 First Quarter Berentsen and Schär 16 Bank of Federal Reserve of St. Louis REVIEW

[7] Guillaume Rocheteau and Ed Nosal. Payments, money, and liquidity. The MIT Press, 2011; https://doi.org/10.7551/mitpress/9780262016285.001.0001. Cambridge and London.

[8] Smart Contracts: A Misunderstood Technology with High Potential, Fabian Schär and Dominik Langer.