EasyChair Preprint

№ 7106

A Systematic Review on Bitcoin Transactions and it's System in India

Shanti Bhushan and Er. Prabhsharan Kaur

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

November 28, 2021

A Systematic Review on Bitcoin Transactions and it's System in India

Shanti Bhushan
University Institute of Computing
Chandigarh University, Punjab, India
shantibhushan619gmail.com

Er. Prabhsharan Kaur
University Institute of Computing
Chandigarh University, Punjab, India
prabhsharan.kaur13@gmail.com

***Abstract*— Cryptocurrencies like Bitcoin have been a big issue in the financial world in recent years. Cryptocurrency is a type of digital, virtual, or online currency that is secured by encryption. Cryptocurrency has wreaked havoc on the financial sector, with both good and bad consequences. Cryptocurrency is a difficult idea to grasp, but it is simple to utilise. It is thought to be. It's challenging since it's so different from our traditional currency that we've been using for so long. Following the global financial crisis of 2008, Bitcoin was designed to function independently of governments, central banks, and financial institutions. Since then, the structure of Bitcoin has been a problem to many policymakers, who have struggled to discover methods to bring it under control. As a result, some nations have banned or made it illegal, while others have remained vigilant, and the remainder have devised ways to tax and control its operations. This is a conceptual article that attempts to investigate the many elements of cryptocurrencies, beginning with their history, kinds, operation, benefits and drawbacks, problems and prospects. In addition, the study looks into the legal position of Bitcoin in India. The initial idea and inspiration, the manner of operation and various uses of cryptocurrencies, and blockchain technology are all covered in this article. We conclude that Bitcoin has a diverse set of applications and that cryptoassets are well positioned to become a significant asset class.**

***Index Terms*— Cryptocurrency, Bitcoin, India, Bank, Ban, Legal, Cash, Future**

I. INTRODUCTION

The instruments employed as exchange instruments to make trade transactions as simple as feasible based on market needs have evolved and changed dramatically[3]. Money refers to the instruments that are used to facilitate the exchange of products. Money is defined as a medium of trade, a monetary unit, and a store of value. Money is a means of trade in the sense that we all agree to accept it as payment for goods and services[1]. Employees agree to take money in exchange for their labour, while merchants agree to take money in exchange for their goods. Money serves as a straightforward means of identifying and expressing value as an accounting unit. Money is a store of value because it allows us to keep the fruits of our labour or business in a handy tool. From barter through commodity money, metal and coins, gold and silver, to modern monetary systems and checks, and finally to the most recent global currency advancements, such as the advent of cryptocurrencies like Bitcoin and Ethereum[4]. The emergence of cryptocurrencies has transformed the international payment system on a scale that was inconceivable only a few years ago. Cryptography is used to secure a cryptocurrency, which is a digital or virtual currency. David Chaum, an American cryptographer, invented e-cash, an anonymous cryptographic electronic money, in 1983. Later, in 1995, he put it into practice with Digicash, an early type of cryptographic electronic payments that needed user software to withdraw bank notes and select certain encrypted keys before they could be transmitted to a destination[14]. This made it impossible for the issuing bank, the government, or any other third party to track the digital currency. Because of its security characteristic, a cryptocurrency is impossible to forge. The fact that a cryptocurrency is not issued by a central authority is one of its distinguishing characteristics. It's entirely decentralized[5].

II. LITERATURE SURVEY

We did a narrative literature review using a variety of academic sources, including Google Scholar, Scopus, Web of Science, and Springer Link, to answer the study question. A narrative literature review is a methodological approach that tries to provide a full understanding and critical evaluation of knowledge related to a certain issue, as well as to potentially disclose flaws or problematize concepts, hypotheses, or claims that require additional investigation (Boell Cecez-Kecmanovic, 2015). A narrative literature review is not intended to be thorough; rather, it is selective in the content it incorporates, with the goal of furthering and contributing to theory development (Cronin et al., 2008). Unlike systematic literature studies, compiling a sample of data does not require it to be representative, because the most essential thing is to learn as much as possible about a topic (Wetherell Potter, 1992). Using a narrative literature review, we can look at the various ways that cryptocurrencies have been con-

ceptualized in previous studies and assess the theoretical underpinnings of this developing paradigm in finance.

III. Proposed Work

A. Bitcoin (BTC) :

Bitcoin is a cryptocurrency that was created in 2009. It is one of the most well-known currencies. It was released as open-source software in 2009[1]. Bitcoin allows users to conduct transparent peer-to-peer transactions using blockchain technology. These transactions are visible to all users, but they are protected by the blockchain's algorithm. While anybody may view the transaction, it can only be decrypted by the Bitcoin's owner using a "private key" that is supplied to each owner[9]. There is no central authority figure in Bitcoin, unlike a bank. Bitcoin users have complete control over the sending and receiving of money, allowing for anonymous transactions all over the world[3].

B. Litecoin (LTC) :

Litecoin was introduced in October 2011 as a Bitcoin alternative. Litecoin is a peer-to-peer cryptocurrency and open-source software project released under the MIT/X11 licence, similar to other cryptocurrencies. Its production and transmission are entirely based on an open source encryption technology. decentralised. In some aspects, Litecoin differs from Bitcoin[6]. The following are some of the differences between these digital currencies: The Litecoin network tries to process a block every 2.5 minutes, whereas Bitcoin takes 10 minutes to process. This helps Litecoin to confirm transactions more quickly. Bitcoin has a 21 million coin limit, while Litecoin has an 84 million coin limit[7][10]. Because it uses a new algorithm called scrypt and FPGA (Field Programmable Gate Array) and ASIC (Application Specific Integrated Circuit) devices intended for mining, experts think Litecoin is more difficult to create and more expensive to make[8].

C. Ethereum (ETH) :

Ethereum is a cryptocurrency that was introduced by Vitalik Buterin, a crypto currency researcher and programmer, in late 2013. It was first released in July of 2015. It's a free, open-source platform that uses blockchain technology[13]. While Ethereum blockchain concentrates on monitoring ownership of digital currency transactions, it also runs the computer code of any decentralised application, allowing application developers to use it to pay for transaction fees and services on the Ethereum network[12].

D. Introduction to Bitcoin :

Bitcoin, which was created by an unknown person or group of persons under the name Satoshi Nakamoto in 2008, is one of the most popular cryptocurrency wallets. Bitcoin is a type of digital currency known as a cryptocurrency[18]. It is a decentralised digital currency that may be sent from one user to another on the peer-to-peer Bitcoin network without the use of intermediaries, with transactions taking place on a public record known as blockchain and users' data being handled anonymously. Bitcoin is the most extensively used and accepted digital currency today, ten years after its introduction[15].

E. Features of Bitcoin :

Bitcoin is more than just a way to move money from one person to another. It has a number of characteristics that set it apart from other cryptocurrencies[13]. Control against fraud: It offers users the highest level of security against the most prevalent types of fraud, including as chargebacks and unauthorised charges. Users can encrypt their wallets and have complete control over their funds thanks to the security. As a result, there is no risk of fraud[17]. Bitcoin is globally accessible, allowing any bank, corporation, or individual to send and receive payments securely anywhere, at any time, in a matter of minutes. All forms of payment from across the world are accepted[20].

F. Working of Bitcoin :

Individuals can use Bitcoins to make payments to other individuals or merchants without the need for a third party to validate the transaction, such as a bank or financial institution. Instead, the blockchain is used to clear and validate transactions within the system. Blockchain technology underpins the majority of cryptocurrencies. In simple terms, it is a method for transferring and storing data or information generated during bitcoin transactions[11]. The blockchain is a public ledger that keeps track of all Bitcoin transactions and exposes them publicly. A block is a record of recent transactions that exists indefinitely. The blockchain, which dates back to the initial Bitcoin transaction, is made up of blocks of recorded data that build upon each other. The blockchain's transparency is critical for ensuring the validation process since it enables the community to monitor and self-police transaction behaviour. It also allows both the sender and the recipient to be verified, making double-spending of Bitcoin impossible[16]. A public key and a private key are generated when a Bitcoin wallet is created to hold Bitcoin. Public and private keys are a series of lengthy numbers and letters that function similarly to a user's username and password. If they wish to send money to them, they'll need their public key. Nobody needs to know their name or email address because it's just a series of numbers and digits. As a result, Bitcoin users are anonymous. However, the private key is kept hidden. The private key is one's identification on the blockchain. To use Bitcoin, you'll need a private key. Anyone who discovers it has the ability to take all of the Bitcoins in the account or wallet. A payment order in the Bitcoin system can be sent to any number of network nodes. The network nodes are connected in a loose network, and the message is forwarded until all nodes have been notified of the transaction[9].(Figure 1)

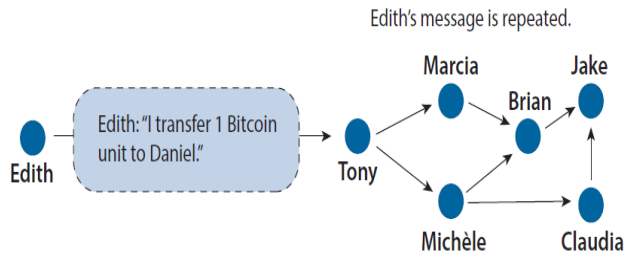

Fig. 1. Bitcoin Transaction Communicated to Network Nodes. The network nodes are connected in a loose network, and the message is forwarded until all nodes have been notified of the transaction.

G. Advantages of Bitcoin :

The ability to remain anonymous. When opening an account with a bank, users must present their identification. Anyone, everywhere in the globe, can send money to each other using Bitcoin. To open a Bitcoin wallet, there is no KYC (Know-Your-Customer) procedure. It is absolutely anonymous while while being completely transparent. Without regard for a corporation's name, address, or any other information, any company can generate an infinite number of Bitcoin addresses[14]. A peer-to-peer cryptocurrency network is one in which there is no one master server in charge of all activities. Information (in this case, money) is exchanged between two or more software clients. Users' program-wallets are all connected to the Bitcoin network. Each client keeps track of all committed transactions as well as the number of Bitcoins in their wallets. Hundreds of dispersed servers process transactions. Banks, taxes, and governments cannot regulate the flow of money between them. It's simple to use. Given that obtaining a bank account for a company in Ukraine is overly difficult and can be refused without explanation, businesses will find it more convenient to use Bitcoin. The company creates a BTC wallet in around 5 minutes and begins using it right away, without any questions or commissions[18].

H. Disadvantages of Bitcoin :

Traditional payment methods such as a credit card charge, bank draught, personal check, or wire transfer all benefit from being insured and revocable by the banks involved. Bitcoin transactions, on the other hand, are irreversible. When it comes to Bitcoins, the result is definitive every time they change hands and wallets. Your Bitcoin wallet, on the other hand, is not covered by insurance. Your wallet's contents are lost permanently if you lose your wallet's hard drive data or even your wallet password[14]. Bitcoin wallets cannot be confiscated, frozen, or audited by banks or law enforcement. Spending and withdrawal limits cannot be established on Bitcoin wallets. The owner of the Bitcoin wallet is the only one who can decide how the money is managed[15].

I. Opportunities of Bitcoin in India :

Entrepreneurs in the country see this as a natural opportunity for Bitcoin and other cryptocurrencies to spread across the country. According to reports, India presently has roughly 30,000 Bitcoin owners, with the number projected to rise. For customers, there is a payment system that does not require them to submit personal information. For marketers, it's a method to save transaction costs; for emigrants, it's a chance to send remittances for free[3].

J. Legal Status of Bitcoin in India

The legal status of Bitcoin and comparable crypto instruments varies significantly from country to country, and in many cases is currently unclear or evolving. While the majority of countries do not prohibit the use of Bitcoin, its position as money (or a commodity) varies, resulting in different regulatory ramifications. Some states have officially permitted its usage and trade, while others have outright prohibited or limited it. Likewise, Bitcoins have been categorized differently by various government agencies, departments, and courts[7]. However, Bitcoin is legal in India, Canada, Jordan, Vietnam, and Thailand, but banking is prohibited. The State Bank of Vietnam has declared that the issuance, supply, and use of Bitcoin and other similar virtual currencies is illegal as a form of payment and is punishable by fines ranging from 150 million to 200 million VND; however, the government does not prohibit Bitcoin trading as a form of virtual goods or assets. Bitcoins have been available in India since 2012, when it was first introduced. In his budget statement on February 1, 2018, Finance Minister Arun Jaitley indicated that the government will do everything possible to prevent the use of Bitcoin and other virtual currencies for illegal purposes in India[14]. He reaffirmed that India does not recognize them as legal cash and that blockchain technology will be encouraged in payment systems instead. People who use these forms of currencies should exercise caution, according to the Indian government, because they have no legal protection. People will not receive any assistance from the government if they are victims of fraud[16].

K. Challenges of Bitcoin in India :

Government Regulation: The Indian government's stance on Bitcoin is the most significant impediment to its growth. For the time being, the future of bitcoin in India is uncertain. In 2019, the Reserve Bank of India announced that cryptocurrencies will not be regarded legal cash. Due to the fact that it is fully decentralised[17].

Hackers and unscrupulous individuals can manufacture as much virtual currency as they want if they break the system and understand the technique of virtual currency generation. This will enable the creation of phoney virtual currency or the theft of virtual currency by simply changing account balances.

Negative influence on the Indian monetary system: Cryptocurrencies such as Bitcoin allow users to buy virtual

and real products and services using virtual currency, which may lower demand for actual money on some platforms. Users will no longer use actual money to purchase anything; instead, they will use virtual money. On the other hand, some sites allow users to trade their virtual currency for real money, which will raise demand for real money. The real monetary systems will be harmed by this demand-supply fluctuation[17].

Using Bitcoins for Criminal and Unlawful Operations: There have been several reports that Bitcoins have been used for illicit and illegal activities[13].

Security threats:If hackers and bad people can undermine the system and figure out how to manufacture virtual currency, they can make as much as they want. This will enable the creation of phoney virtual currency or the theft of virtual currency by simply changing account balances. Selling virtual objects and virtual currency in-game, for example, is against World of Warcraft (WoW) game policies. As a result, a large number of players visit WoW gold selling websites in order to purchase virtual gold in order to pay for virtual products that they require. Many WoW gold selling websites are untrustworthy and subject to hacking, and many customers have complained about spending real money for nothing or for phoney virtual currency[18].

Gold farming risks:In China and other emerging countries, the term "gold farming" is highly widespread. Gold farmers are those who play social games like World of Warcraft for the purpose of gaining gold, the game's virtual currency, and then selling it for real money. Players who do not have enough time to play and compete for virtual cash are the target purchasers. In truth, the gold farming operation generates a large amount of cash flow that is not controlled or regulated. When virtual currency is exchanged for real money in an uncertain environment, this will raise fraud and financial hazards[14].

Black market for cryptocurrency:Some social games, such as Second Life and World of Warcraft, have matured to the point that they can develop a black market for purchasing and selling their virtual currency. Because of the growing popularity of virtual currency in the online world, a robust illicit market for selling virtual currency for real money has emerged. Some fraud situations have been raised and debated among users after watching many social game forums. When a gamer decides to leave a game, for example, he or she may want to sell any virtual currency they have in the game's forums. The method of accepting money is dangerous since many malicious individuals may fail to complete the transaction or dispute the payment after it has been made. They will receive their money back as well as the virtual currency in this situation[12].

IV. CONCLUSIONS

Cryptocurrency in particular Bitcoin is a fresh, effective, and appealing payment method that can help businesses and operators increase their revenue. It also offers an alternative payment mechanism, in addition to real money, that allows users to conduct financial transactions like as buying, selling, transferring, and exchanging with ease. Cryptocurrency has the potential to bring additional good improvements to the e-Commerce and e-Payment industries. However, cryptocurrency has yet to gain widespread acceptance. Many cryptocurrency platforms have numerous concerns, obstacles, and issues. Users should exercise extra caution when utilizing cryptocurrencies until it is properly regulated and monitored. As a result, the lack of regulations is seen as the primary source of worry in cryptocurrency systems. The RBI's silence on the regulatory position of Bitcoins could be detrimental. In India, a whole economy has sprung up around Bitcoins, with traders, exchanges, and merchants accepting Bitcoin payments. Bitcoins have already achieved widespread popularity around the world; therefore, banning them in India is not an option. This industry would need to be regulated instead. The sooner you finish this, the better.

ACKNOWLEDGMENT

I would like to thank Er Prabhsharan Kaur for her valuable comments and suggestions to improve the quality of the paper. for helping me review my work regularly. I would also like to thank the University Institute of Computing, Chandigarh University, Punjab, India for providing me this opportunity.

REFERENCES

[1] Kapil Sharma, Deepakshi Jain, "Consensus Algorithms in Blockchain Technology: A Survey", Computing Communication and Networking Technologies (ICCCNT) 2019 10th International Conference on, pp. 1-7, 2019.

[2] M. Srikanth, R. N. V. Jagan Mohan, "Block-level based Query Data Access Service Availability for Query Process System", Computer Science Engineering and Applications (ICCSEA) 2020 International Conference on, pp. 1-9, 2020.

[3] Jash Rathod, Ashutosh Gupta, Dhiren Patel, "Using Blockchain Technology for Continuing Medical Education Credits System", Software Defined Systems (SDS) 2020 Seventh International Conference on, pp. 214-219, 2020.

[4] Sudeep Choudhari, Suman Kumar Das, Shubham Parasher, "Interoperable Blockchain Solution For Digital Identity Management", Convergence in Technology (I2CT) 2021 6th International Conference for, pp. 1-6, 2021.

[5] Shuang-Gen Liu, Wan-Qi Chen, Jia-Lu Liu, "An Efficient Double Parameter Elliptic Curve Digital Signature Algorithm for Blockchain", Access IEEE, vol. 9, pp. 77058-77066, 2021.

[6] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008

[7] Kiyotaki, Nobuhiro and Wright, Randall. "A Search-Theoretic Approach to Monetary Economics." American Economic Review, 1993, 83(1), pp. 63–77.

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

[9] Harwick, C. (2016). Cryptocurrency and the Problem of Intermediation. The Independent Review,20(4), 569- 588.

[10] Angel, J., McCabe, D. (2015). The Ethics of Payments: Paper, Plastic, or Bitcoin? Journal of Business Ethics,132(3), 603-611. Retrieved from http://www.jstor.org/stable/24703614

[11] Murali, J. (2013). A New Coinage: Can Bitcoin, the global online digital currency, be the precursor of a new monetary system? Economic and Political Weekly,48(38), 77-78.

[12] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in Bitcoin: A study of double-spending and accountability," ACM Trans. Inf. Syst. Secur., vol. 18, no. 1, 2015, Art. no. 2.

[13] P. K. Kaushal, A. Bagga, and R. Sobti, "Evolution of Bitcoin and security risk in Bitcoin wallets," in Proc. Int. Conf. Comput., Commun. Electron. (Comptelix), Jul. 2017, pp. 172–177.
[14] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries," in Proc. Workshop Econ. Inf. Secur. (WEIS), 2013, pp. 1–21
[15] P. M. Monamo, V. Marivate, and B. Twala, "A multifaceted approach to bitcoin fraud detection: Global and local outliers," in Proc. Int. Conf. Mach. Learn. Appl. (ICMLA), Dec. 2016, pp. 188–194.Systems (SDS) 2020 Seventh International Conference on, pp. 214-219, 2020.
[16] T. Pham and S. Lee. (2016). "Anomaly detection in Bitcoin network using unsupervised learning methods."
[17] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," IEEE Consum. Electron. Mag., vol. 7, no. 4, pp. 6–14, Jul. 2018
[18] B. Sengupta, S. Bag, S. Ruj, and K. Sakurai, "Retricoin: Bitcoin based on compact proofs of retrievability," in Proc. Int. Conf. Distrib. Comput. Netw. (ICDCN), 2016, Art. no. 14
[19] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in Bitcoin," in Proc. Int. Conf. Financial Cryptogr. Data Secur. San Juan, PR, USA: Springer, 2015, pp. 507–527.
[20] D. Zambre and A. Shah, "Analysis of Bitcoin network dataset for fraud," Stanford CS 224W Project Final Rep.-Group 30, Dec. 2013.