REVIEW ARTICLE

ADHYAYAN Volume 10, Issue 1, 2020 Print ISSN: 2249-1066 Online ISSN: 2455–8656

Crypto-Micropayments: Issues in Gaining Trustworthiness

Abhishek Srivastava*

Associate Professor and HOD, Department of Information Technology, Gopal Narayan Singh University, Rohtas-821305, Bihar, India

Abstract

Conducting businesses over Internet has now turned to necessity rather than just considering it as fashion and in the same context turns into an essential part of financial institutions serving as one of the trusted third parties to process electronic payments. Now a day, crypto-micropayments are playing major roles as world-shattering decentralized, trustless payment systems nevertheless used by many individual entities, as well as, business houses for the benefit of their own concerns. Logically, crypto-micropayments provide a digital alternative to government-issued fiat currencies, and thus, can be used in online marketplaces to buy everything from a needle to flight tickets. Although with the growing number of opponents, cryptocurrencies show fearless traversal over the internet against its challengers who are also gaining grip from such virtual currencies whose presence in this era foretell a matter of great distrust and concurrently all hastening to become the main teller for the upcoming future cashless world. Since, digital currencies are still in a state of flux, this paper tries to target the squashy curves associated with cryptocurrencies, as well as, its frailty in association with societal perspectives due to its anonymity and cross-border features. This paper also focuses on the need for radical overhauling of existing payment-related regulatory framework in India with special reference to crypto-micropayments.

Keywords: Bitcoin, Blockchain technologies, Crypto-Micropayments, Cryptocurrencies, Digital commodities, Digital currencies, Volatile currencies.

Adhyayan: A Journal of Management Sciences (2020); DOI: 10.21567/adhyayan.v10i1.7

Introduction

Online shopping has been almost entirely dependent on financial institutions operating as one of the most reliable third parties in the electronic payment process. Although the method fits well enough for most transactions, it also suffers from the trust-based models. What is required is an electronic payment mechanism focused on cryptographic evidence rather than trust, enabling any two consenting parties to freely transact with each other without the need for a reliable third party. Computationally unrealistic reverse transactions can shield sellers from theft, and routine issuer systems could be quickly added to shield buyers. Absolute non-reversible deals are not even feasible, since financial firms are inappropriate to resist conflict resolution. Mediation fees raise processing costs, reduce the minimum functional size of transactions and close off the likelihood of small casual purchases, and the lack of opportunity to accept non-reversible payments for non-reversible transactions entails a bigger expense. The need for trust expands with the risk of reversal (Cinerama, 2020). Merchants ought to be careful of their clients, disturbing them with more details than they otherwise ought. A certain proportion of fraud is considered an inevitable part of the transaction. However, using physical currency, these costs and payment uncertainties can be eliminated in person, but there is no system for making payments through the contact channel without a trusted party. Cryptocurrencies are considered as digital currencies of the 21st century, i.e., a mixture of digital assets, huge amounts of computing power, and a network of servers on which to store shared data (Srivastva & Kiran, 2016).

Cryptocurrencies are not at all considered as regular money, as they are not centralized, i.e., they are not

Corresponding Author: Abhishek Srivastava, Associate Professor and HOD, Department of Information Technology, Gopal Narayan Singh University, Rohtas-821305, Bihar, India, e-mail: inbox.abhishek@gmail.com

How to cite his article: Srivastava, A. (2020). Crypto-Micropayments: Issues in Gaining Trustworthiness. Adhyayan: A Journal of Management Sciences, 10(1):45-50.

Source of support: Nil

Conflict of interest: None

issued or assured by central banks, and therefore, they are out of the purview of regulators (Bhatia *et al*., 2019). Such cryptocurrencies are secured in nature as they are crypto graphed and thus, lesser chances of getting hacked or trapped from hackers. However, some criminal elements always hold a soft target against such currencies because of their decentralized nature (DeVries, 2016). There are many cryptocurrencies that have risen dramatically this year, including Ethereum, Ripple, Litecoin, Dash, and most prominently Bitcoin. Although India's Reserve Bank of India has already counseled cryptocurrency users and merchants of its hazards. In the year 2019, Prime Minister Narendra Modi participated in dialogues on crypto assets at the G20 Summit in Osaka, Japan. All the leaders of G20 countries jointly stated that they will be applying crypto standards set by the Financial Action Task Force (FATF), i.e., hold answerable for evolving global strategies in regions, such as, combating money laundering, which comprises of thirty seven-member jurisdictions, including India. Plans included digitizing government data, improving India's digital structure, and optimizing its online connectivity.

Cryptocurrency as a Side Product of Digital Cash

It is a digital currency, in which encryption methods are used to standardize the peers of elements of currency, and authenticate the allocation of funds, operating autonomously of a central bank. Decentralized cryptocurrencies, such as, Bitcoin now provide a vent for individual affluence that is elsewhere constraint and seizure (Liu & Tsyvinski, 2018). Very few ones know that cryptocurrencies emerged as a side product of another invention. Satoshi Nakamoto, the unknown inventor of bitcoin, the first and still most important cryptocurrency, has never intended to invent a currency.

In his announcement of Bitcoin in late 2008, Satoshi said he developed "a peer-to-peer electronic cash system." His goal was to invent something else that many people failed to create before digital cash.

Transactional Properties of Cryptocurrency

Irreversible

Once committed, a transaction cannot be reversed. If a user sends money to a wrong person or even if a hacker steals them from the user's computer, it is irreversible and cannot be brought back to its original user, and thus, there is no safety (Liu *et al*., 2019).

Spoofed Identity

Since every transaction, as well as, accounts are connected to real-world identities, using cryptocurrencies it is not necessarily possible to connect the real-world identity of users with those addresses which are associated with crypto transactions.

Globally Accepted

Transactions are accepted worldwide with the internet and are completed in a couple of minutes. It is not a matter of relevance that if a cryptocurrency has been sent to a neighbor or someone on the other side of the world (Krishna, 2020).

Secure

Cryptocurrency funds are secured with a public key cryptographic system, where the owner of the private key can only send cryptocurrency. Using a strong key for encrypting hash values, makes it impossible to break this scheme.

No Need for Permission

Users should not ask anyone to seek permission for its use and thus, everybody can download it for free. After the proper installation of the application, the user can receive and send cryptocurrencies.

How Miners Create Coins and Confirm Transactions

Let us have a look at the mechanism ruling the databases of cryptocurrencies. A cryptocurrency, like Bitcoin, consists of a network of peers. Every peer has a record of the complete history of all transactions, and thus, of the balance of every account.

A transaction is a file that says, "Bob gives X Bitcoin to Alice," and is signed by Bob's private key. It is basic public-key cryptography, nothing special at all. After signed, a transaction is broadcasted in the network, sent from one peer to every other peer.

How a Cryptocurrency Works

A. Initiated by a user, when he generates a request to transact with a cryptocurrency from his account to other's accounts over his digital device, i.e., either on a smartphone or on a laptop.
B. User's requests are acknowledged by cryptocurrency networks with network users, especially called "miners" who act as the main source behind its processing.

C. While mining process, transactions are packed into data blocks which are randomly assigned with a header (so, that each time it can be viewed, i.e., where it has been used earlier for transaction) network miners completes such process of matching block's header with a nonce (an arbitrary value only once used) to get a "hash value" after attempting hashing function, i.e., hiding original data with the use of such function.
D. After the successful generation of "hash value," the network has been awarded a cryptocurrency, which can be used for such transactions.
E. This cryptocurrency in the form of "hash value," then added to the next block's header and is now ready to get transacted, and thus, creating a blockchain, i.e., a general ledger of long list of blocks so that it can be acknowledged at any point over the networks and its authenticity can be testified (Borri, 2019).
F. The transaction with cryptocurrency takes a longer time than any other transaction (i.e., sometimes it takes 10 minutes to complete a single transaction), and once completed its irreversible.

Benefits of Cryptocurrencies

With respect to its uniqueness, we have some intrinsic benefits with such transactions are something that is very unique, and normal currencies do not have such characteristics in their entire span of time (Vigna & Casey, 2016). Cryptocurrencies are a relatively untested method of exchange, and therefore, their users should ensure its adaptability issues and must be careful to evaluate their paybacks and perils, few of its noted advantages are as follows:

Distinct User Identity

Purchase of cryptocurrencies are discrete in nature, and thus, the user's personal identity is never in the case of involvement in transactions, thus, his purchases are much like cash-only purchases, and therefore, cannot be traced back to him.

No Interludes

Governments, banks, and other financial mediators cannot interrupt users' transactions or places from where it has been made and to whom.

Tax-Free Purchases

Since third parties cannot trace or identify the transactions, therefore, it is difficult to track or intercept transactions that are initiated by cryptocurrencies, which turns to be the most important benefits of cryptocurrencies, and thus, sales taxes are not added onto any purchases based with this currency.

Very Low Cost of Transactions

Since there are no transitional institutions involved in transactions neither any country's government is involved, therefore, the costs of transactions are comparatively lesser.

Mobile Payments

The need for online payments based on cryptocurrencies only required internet access, and thus, purchasers just need a digital device for payments, and no physical bank or financial institutions are involved in such a case for the purchase of a product.

Where Cryptocurrencies are used

Mainly all cryptocurrencies are used outside the existing banking institutions on the internet as a medium of exchange and according to CoinMarketCap, the total number of cryptocurrencies is 5,563 with a total market cap of $271.58 billion (as of 10 June 2020) are recorded so far. Crypto-micropayments validity varies significantly from country to country and is still undefined or changing in many of them.

Wealth Management

Wealth management is one of the most exciting ways cryptocurrency can be used.

Digital Advertisers and Publishers

Digital advertisers and publishers are clamoring to find their ways to increase their pertinent presence with one another.

Ethical Business Practices

Since blockchain technology makes it possible to track every transaction with complete transparency, therefore, such cryptocurrency can also be used to encourage ethical business practices.

Battling Electoral Fraud

Another ethical application of cryptocurrency will be its ability to help battle electoral fraud.

Maintain Accountability

Cryptocurrency can be used to escape financial scams in altruistic organizations. Blockchain can eradicate countless hitches arising with donations, such as, fund leakages because of its capability to keep transparency in transactions.

Going Green

Users will be happy to perceive that cryptocurrency can be used to make the world greener by its digital presence.

Travel

Since if such currencies will be accepted by more and more retailers, then people will use these cryptocurrencies more frequently even on travel too.

Education

Even schools are now accepting cryptocurrencies in the form of tuition fees, and according to futurism.com, several universities in Switzerland, Germany, Cyprus, and the United States have started accepting payment in the form of Bitcoins (a type of cryptocurrency).

Fund-Raising

Many fundraising ideas are now evolved with the use of cryptocurrencies for their better services and products. Several fund-raising websites, such as, IndieGoGo or Kickstarter, startup leaders are looking for different cryptocurrency as a fundraiser.

Augmented Reality

Virtual reality games, like Pokemon, Go craze, and companies like Candy Lab, etc., are now switching their dependability on cryptocurrencies for accepting payments in the form of cryptocurrencies.

ISSUES ASSOCIATED WITH CRYPTOCURRENCIES

There are several fundamental and operational issues that arise from a variety of reasons, such as, its toddlers nature of the market, having a lack of appreciation over the cryptocurrency space, as well as, some pertinent issues associated with cryptocurrencies (Anthony, 2017). Few of them are as follows:

Hard to Understand

Cryptocurrencies are a digital currency, and thus, involve lots of technical issues and challenges especially for the non-technical individual which ultimately initiates ignorance, misinformation, and distrust for those who are new to such currencies.

User must be Proficient in Computers especially in Computer Security

Since cryptocurrencies are just a hash value, i.e., stored in form of a digital file and if this wallet file is lost or stolen, all of the people's cryptocurrencies are most likely gone forever.

Takes longer Time to realize Payments, thus, practically Difficult for Retail Transactions

In the case of cryptocurrencies, it usually takes a longer time to realize a payment because it involves two transactions, i.e., first one to one to pay the seller and a second transaction to pay themselves, in which the second transaction becomes permanently confirmed in the blockchain process. Thus, causing an inconvenient wait for both the buyer and seller.

Lack of Consum er Protection

Since transactions are irreversible, therefore, the buyer must trust sellers to deliver, and thus, sometimes payment processing company will often refund the buyer their funds.

Exposed to Vulnerable Threats

Several vulnerable threats involved with cryptocurrencies are as follows:

- Spoofing payment information and phishing
- Hacking a payment gateway
- User address error
- Insecure initial coin offering
- Spoofing a user address

Let us take an example of a cryptocurrency "Bitcoin," where it is hard to obtain the following:

- Where is the service located?
- Do they publish a physical address?
- Do they disclose their identities or are they operating anonymously?
- What are other people saying about them in forums and reviews?

Role of Reserve Bank of India on Cryptocurrency-Based Payment Mechanism

Recently, India has virtually banned cryptocurrencies, like Bitcoin, with the Reserve Bank of India barring regulated entities from providing services to any individual or business dealing in digital currencies. The central bank has given three months to regulated entities, like banks, to unwind their positions with the entities related to cryptocurrencies. Recent testimonials given by Indian officials over cryptocurrencies are as follows:

"The RBI has cautioned on at least three occasions members of the public and users of virtual currency regarding risks they are exposing themselves to through these cryptocurrencies,"

RBI Deputy Governor, B. P. Kanungo

"The Indian government doesn't consider crypto currencies as legal tender and will take all measures to eliminate payments using them."

Finance Minister, Arun Jaitley

"The move of Indian government on cryptocurrencies are like similar to demonetization like effect on cryptocurrencies. That effectively means people lose ability to conduct any trade or exchange, at least in the open market. These have become dead assets for people who are holding onto them. This is going to have huge repercussions. If you disallow trading there is no exit to this."

Vishal Gupta, co-founder, DABFI, India

"Risks exist in every system but we have solutions to each of those. So why not work with virtual currency traders in a similar way and create a risk-free system rather than indirectly shutting it down."

Navin Surya, Chairman of the Payment Council of India

"Central banks won't lose monopoly over currency for the simple reason that ultimately even if a virtual currency becomes popular at some point in time, the holders would like to convert it into normal currency,"

R. Gandhi, former Deputy Governor, RBI, India

The government of India has now compelled to take a decision against virtual currencies originating from different parts of the world just because of their unregulated nature. Bitcoin, the most popular cryptocurrency, triggered worries that such currencies could enable the whole kit and caboodle from money laundering to tax-evasion and fraud. Even for organizations, a platform must be built in an improved way to connect with its customers, including safer transactions including wallet or cryptocurrency-based online transactions, which have been watched carefully all the time with their comments and concerns (Srivastava & Pandey, 2013).

However, India is not giving up on the idea of a virtual currency completely, but they are in favor of its introduction as a legal digital currency that can be accepted worldwide without any hesitations and grudge. Accordingly, the RBI has constituted an interdepartmental committee that will submit a report on the feasibility of a fiat digital currency. The committee will submit its report by June-end.

Conclusion

After having a colossal growth up to $20 K, Bitcoin's nuptial looks like coming to an end because it has now back to $10 K. While other analysts from the rest of the world termed it as "Bitcoin bubble" who is now going to get burst anytime. Whatever be the reason, cryptocurrency market jumps by over $13 billion driven by bitcoin as the major technical event approaches in the last one month. A convention in bitcoin commanded the cryptocurrency market higher ahead of a foremost technical episode for the digital coin and as industry contributors reported an amplified concern from institutional stockholders.

Now we have both sides of the penny. Cryptocurrencies do have many advantages that physical currencies do not provide to its users but we must not forget about its drawbacks. It is mostly because cryptocurrencies are young and new currencies. People are more intent to know more about these currencies and more they need to comprehend their existence and maturity in the international market. Cryptocurrencies provide a referential price for the assets, especially with the unfettered market. Thus, without proper supervision from its authorized regulators, they are definitely considered to be the case of manipulation.

At last, it can be concluded that cryptocurrencies were designed on the ground of disbelief and uncertainty. Users must need to boost their confidence to generate, dispense, and to manage the money in the form of cryptocurrencies. Cryptocurrencies, thus entail more obligations from its user's part to be more educated about its belongings and safe usage just because it is a new and intricate impression; it will surely take sufficient time for its hassle-free operations.

References

Anthony Tu, (2017). Cryptocurrency: 5 Expert secrets for Beginners: Investing into Bitcoin, Createspace Independent Pub, ISBN: 978-1976158872

Back (2002). Hashcash-a denial of service counter-measure, Retrieved from http://www.hashcash.org/papers/hashcash.pdf.

Bayer, D., Haber, S., and Stornetta, W. S. (1993). Improving the efficiency and reliability of digital time-stamping. In Sequences Ii (pp. 329-334). Springer, New York, NY.

Bhatia, S., and Wright de Hernandez, A. D. (2019). Blockchain is already here. What does that mean for records management and archives?. Journal of Archival Organization, 16(1), 75-84.

Borri, N. (2019). Conditional tail-risk in cryptocurrency markets. Journal of Empirical Finance, 50, 1-19.

Chuen, D.L. K., Guo, L., and Wang, Y. (2017). Cryptocurrency: A new investment opportunity?. The Journal of Alternative Investments, 20(3), 16-40.

Cinerama, Despite Similarities, Is Blockchain Really The Next Internet?, https://www.bitcoinisle.com/2017/03/10/despite-similarities-is-blockchain-really-the-next-

internet/, accessed on April 10, 2020

DeVries, P. D. (2016). An analysis of cryptocurrency, bitcoin, and the future. International Journal of Business Management and Commerce, 1(2), 1-9.

Fry, J. (2018). Booms, busts and heavy-tails: The story of Bitcoin and cryptocurrency markets?. Economics Letters, 171, 225-229.

H. Massias, X.S. Avila, and J.-J. Quisquater (1999). Design of a secure timestamping service with minimal trust requirements, In 20th Symposium on Information Theory in the Benelux.

Hileman, G., and Rauchs, M. (2017). Global cryptocurrency benchmarking study. Cambridge Centre for Alternative Finance, 33, 33-113.

investopedia, What are the advantages of paying with Bitcoin?, https://www.investopedia.com/ask/answers/100314/what-are-advantages-paying-bitcoin.asp, accessed on April 9, 2020

Srivastva, A., and Kiran, P. (2016). Transforming Customer Experience in E-Commerce Market Place: A Smact Approach. Indian Journal of Science and Technology, 9, 32.

Liu, Y., and Tsyvinski, A. (2018). Risks and returns of cryptocurrency (No. w24877). National Bureau of Economic Research.

Liu, Y., Tsyvinski, A., and Wu, X. (2019). Common risk factors in cryptocurrency (No. w25882). National Bureau of Economic Research.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

Paul Vigna, Michael J. Casey, (2016), "The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order" ISBN 9781250081551

R.C. Merkle (1980). Protocols for public key cryptosystems, In Proc. Symposium on security and Privacy, IEEE Computer Society, pages 122-133.

Rakesh Sharma, Four Problems With Bitcoin Futures, https://www.investopedia.com/news/four-problems-bitcoin-futures/ accessed on April 8, 2020

Revati Krishna, Experts Want India To Take A Clear View On The Virtual Currency Debate, https://www.bloombergquint.com/global-economics/2018/04/08/experts-want-india-to-take-a-clear-view-on-the-virtual-currency-debate, accessed on 10 April 2020.

S. Haber, W.S. Stornetta (1991). How to time-stamp a digital document, In Journal of Cryptology, vol 3, no 2, pages 99-111.

S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications security, pages 28-35, April 1997.

Srivastava, A. and Pandey, K.M., (2013). Social Media Marketing: An Impeccable Approach to e-Commerce, Management Insight, Vol. 8, No. 2.

Vigna, P., and Casey, M. J. (2016). The age of cryptocurrency: how bitcoin and the blockchain are challenging the global economic order. Macmillan.