

A Brief Survey of Cryptocurrency Systems

Sushma Malik¹#, Anamika Rana²*

Assistant professor (IT), Institute of Innovation in Technology and Management, Janak Puri, New Delhi, India

* *Assistant professor (IT), Maharaja Surajmal Institute of Technology, Janak Puri, New Delhi, India*

¹sushmamalikiitm@gmail.com, ²anamika.rana@gmail.com

Abstract—Information and communication Technology (ICT) have change the state of life from the last few years because many activities of daily life have been merged online and they become more productive. Cryptocurrency is specific type of virtual currency which works on the principles of cryptography and electronic medium communication. It gain lots of attention in the recent years. Cryptocurrency has decentralized control and is controlled by non-government bodies. It opposes the centralized digital currency and central banking system because of its decentralized feature. It revolutionizes the digital trade market by creating a free flow trading system which works without any third party. The usage of virtual money or currency has widespread in recent years. this paper highlight the introduction of cryptocurrency, its history , some aspects of it ,working of cryptocurrency and also highlight the future of cryptocurrency in India.

Key words: Cryptocurrency, Bitcoin, cryptography, decentralize, centralized, digital currency

I. INTRODUCTION

There is no doubt that this is an era of information and communication technologies because of which many opportunities have been created. Financial and business sector are one of the biggest Sector which took the benefits from this technology. A large

number of online users have activated virtual world concepts and creating a new business phenomenon, a result of this new type trading the transactions and currencies have been arising. One of the biggest financial forms that have been emerged in past few years is Cryptocurrency. It is a digital currency created with controlling its creation and protecting transactions, with hiding the identity of the user (Jani, 2018). Cryptocurrency is the combination of crypto and currency. Crypto- is short form of “cryptography”, computer technology which is used for security, hiding information, identities. Currency simple means “money mostly in use”. It is a digital form of cash which is designed to work faster, to provide more reliability and to be cheaper than our government issued money or the legal tender.

The basic principle of cryptocurrency is that no individual or organization may control the production of a given currency. The certain pre defined amount of cryptocurrency is produced by the entire cryptocurrency system. The rate of production is set by a value defined earlier and is publically known. It provides the permission to transfer the virtual costless cryptocurrency units which also called coins between client applications through peer to peer network (Vejacka, 2014). Instead of trusting a government to create your money and banks for storing, sending, receiving money users transact directly with each other without any intermediate (government) between

them and they can store their money themselves. As peoples can directly send, for the purpose of prevention from fraud and manipulation, every user of a cryptocurrency can simultaneously record and verify their own transactions and others transactions as well. Ledger is very well known by the commerce students and even it is known by many of us.

Cryptocurrency also used the ledger to store the digital transaction records and it is publicly available to everyone, means anyone can verify the transactions which is done by others. With this public ledger transactions become secure, transparent, efficient and permanent. With the help of this ledger, user don't need to trust a bank to hold cryptocurrency and also don't require to trust the person with user doing the business to actually pay to user. Instead user can see by them the money being sent, received, verified and recorded by thousands of people. This system not required a middleman for transactions and transactions are usually very affordable and fast (Li & Wang, 2016).

It was mostly used to do illegal deals by drug dealers, smugglers and black marketers for the transaction of their funds as it is the safest, untraceable and fastest method to do all over the world (Kashyap & Chand, 2018).

Characteristics of Cryptocurrency technology platform (Thackeray, 2018):

Irreversible: After confirmation of transaction, a transaction cannot be reversed.

Unidentified: it works on the decentralized principle, so neither transactions nor accounts are connected to real-world identities. Everything is digitalized with access by means of the internet.



Figure 1: Characteristics of Cryptocurrency Platform

Global Speed: Transactions are done on the network and are confirmed in a couple of minutes. for verification and validation, there are no involvement of third parties.

Secure: it become secure with the implementation of strong cryptography algorithms which makes it impossible to break this scheme.

No Gatekeeper: Software is freely available for download. After installed anyone can receive and send Bitcoins or other cryptocurrencies.

II. HISTORY OF CRYPTOCURRENCY

The first cryptocurrency was launched in 2009 named as Bitcoin by Satoshi Nakamoto, Bitcoin was not regulated by a government or institution and no third

party was involved, it was open source from peer to peer transfer. This cryptocurrency used blockchain technology.

In the 19th century, there have been many attempts to create digital money, but they all failed. After seeing all the failures Satoshi tried to build a digital cash system which is decentralized. Like peer to peer network file sharing (Mukhopadhyay, Skjellum, Hambolu, Oakley, Yu, & Brooks, 2016).

III. BLOCKCHAIN OVERVIEW

The public ledger which stores the transactions of cryptocurrency is called the blockchain. Each and every transaction is stored in a block and each block consists of variable number of verified transactions. in each cryptocurrency system, the size of block is fixed by providing the upper bound number of transactions. For example the maximum size of bitcoin block is 1MB (Mukhopadhyay, Skjellum, Hambolu, Oakley, Yu, & Brooks, 2016).

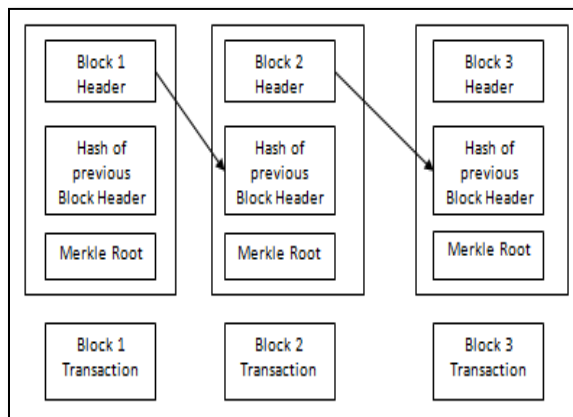


Figure 2: Blockchain

Blocks in n the blockchain are made up of digital pieces of information. Blocks mainly made up of three parts like:

1. Block store the transaction related information like date, time and amount of dollar which user recent purchase.
2. It also stores the user information who did the transaction. it using digital signature of the user instead of user name.
3. Each block store a unique code called a hash that differentiates the block from every other block. Hash is basically the cryptographic codes which created with some algorithms (Reiff, 2020)

IV. TYPES OF CRYPTOCURRENCIES

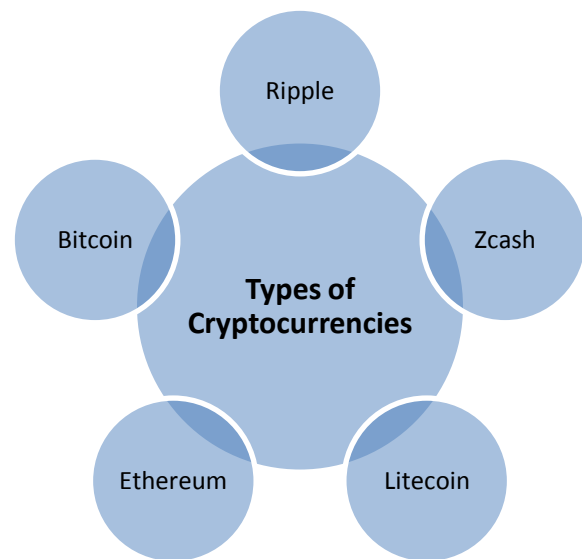


Figure 3: Types of Cryptocurrency

Bitcoin: Bitcoin is the main cryptocurrency type which is worldwide used in payment system. It is the decentralized digital currency and there is no administrator which controls it functioning. There is peer to peer networking and all the transfer of digital currency took place without any help of third party. Transfer in bitcoin is verified by the network codes

which use the special algorithm of cryptography and blockchain record has been made for the ledger of the public distribution (Kashyap & Chand, 2018).

Block of Bitcoin consists of following 5 fields:

1. Magic Number: This is fixed
2. Block Size
3. Block Header: It store the hash of previous block, time stamp and block version number.
4. Transaction counter: This field consist the number of transaction.
5. Transactions: The enumerated set of verified transactions.

Ethereum: Ethereum can be called Ether because of its generation on the platform of Ethereum. it is launched in 2013 by Vitalik Buterin, a computer programmer and researcher in cryptocurrency. Smart scripting facility is also available in it. It works based on the version which is modified in cryptocurrency and has transaction-based payment system. It is the open source platform based cryptocurrency on blockchain technology (Kashyap & Chand, 2018). It focuses on running the programming code of any decentralized application code while tracking the ownership of binary transactions.

Litecoin: Litecoin founded in the year 2011 by Charles Lee. It is a peer- to –peer currency which is used in global payment network. Litecoin mining process can be execute on the normal desktop computer with slow processing (Kashyap & Chand, 2018).

Ripple: Ripple was released in 2012 by a company named OpenCoin with its founder Chris Larsen. It acts as both a cryptocurrency and digital payment

network for financial transactions. The payment method mechanism of ripple is very fast, secure and low cost method of money transferring (Kashyap & Chand, 2018).

Zcash (ZEC): Zcash is a digital currency which is based on the original Bitcoin code base. It was designed by scientists Jihn Hopkins at MIT. The main feature of Zcash is it privacy because users can send and receive Zcash without disclosing the sender, receiver or the amount transacted. (Types of Cryptocurrency Explained, 2018).

V. THREATS IN CRYPTOCURRENCY

There are many risk involve in investing cryptocurrency. Some of them are listed here:

Entrance is wide, but exit is narrow: It is very clear with the heading that it is easy to invest in the cryptocurrency. The main reason of easy investment its digitally performance. all the transactions have been done digitally so it creates a less barrier for the cryptocurrency and a very high risk to exist from the digital world of cryptocurrency (Kashyap & Chand, 2018).

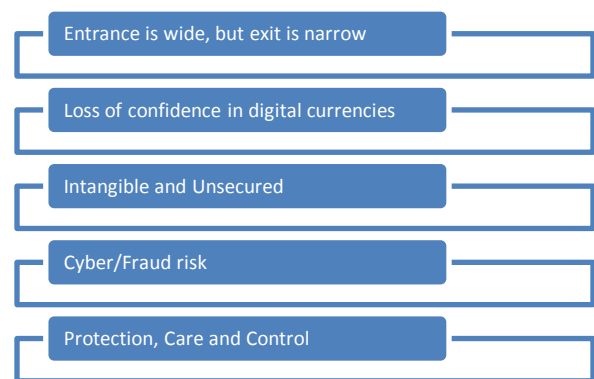


Figure 4: Threats in Cryptocurrency

Loss of confidence in digital currencies: The nascent nature of the currencies is subject to a high degree of uncertainty. Cryptocurrency is work on the

decentralized principle so there is no involvement of central bank. The assets and their value is strictly determined by the value that market participants place on them through their transactions, which means that loss of confidence may bring about a collapse of trading activities and an abrupt drop in value (Thackeray, 2018).

Intangible and Unsecured: The intangible nature of cryptocurrency makes it unsecured. There is no involvement of bank and banker, who act as intermediaries in between to solve the issues of cryptocurrency but this kind of security can be assured by banks (Kashyap & Chand, 2018).

Cyber/Fraud risk: It is the attraction point of the criminal community because of its cash currency nature. Criminals can crack the cryptography algorithm and drain out the crypto wallets and steal cryptocurrency. As all the transaction of cryptocurrency are conducted on the internet, the hackers target the user, handle the services and storage areas with the help of spoofing/phishing and malware (Thackeray, 2018).

Protection, Care and Control: Cryptocurrency intangible nature and act as an asset in digital form became the biggest issues for the care, control and custody of the cryptocurrency. The experienced investors will provide the security to their cryptocurrency but who are not aware about the security concerns are become the easily target of the frauds and hackers are easily steal their cryptocurrency (Kashyap & Chand, 2018).

VI. WORKING OF CRYPTOCURRENCY

Blockchain technology makes cryptocurrency a transparent system and a self-run decentralized

system. Here, when a transaction is carried out from A to B, then a record of transaction is put on the ledger and the ledger is owned by every user of the cryptocurrency. The record of transaction is put on the ledger after verification process. Verification of transactions is done by miners who verify the transaction and then adds it to the public ledger. For verifying transactions miners are rewarded with cryptocurrencies. Mining involves high quality tools and a very strong computing system.

Steps involved in mining are as follows:

1. A miner performs a resource-intensive task and produces a proof that the work has been done. This task prevents a malicious miner from forming false identities and manipulating.
2. The proof produced is verified to confirm that the task has been performed.
3. The miner then checks for the validity of the transactions, and if all the transactions in the block prove valid, the block is posted in the Blockchain.

VII. REASONS WHY SHOULD GO FOR CRYPTOCURRENCY

The global economy is moving toward the usage of digital eco system. In this internet era, investment to money transfer is going to paperless means can be implemented through internet. The newest and most promising method in the digital payment sector is cryptocurrency. Cryptocurrency is the medium of exchange in digital form. From the last few years, usage of digital currency is increased. Some reasons are highlighted here (Online, 2017):

1. **Fraud-proof:** Currency in cryptocurrency are decentralized neither government nor bank has any control over it, user just own it. All confirmed transactions are stored in public ledger. All identities of coin owners are encrypted to ensure the legitimacy of record keeping.
2. **Identity Theft:** the public ledger in cryptocurrency is called the blockchain. Blockchain ensure secure the transactions of digital currency by the implementation of encryption algorithms and make the entity virtually nonhackable and void the fraud cases.
3. **Instant Settlement:** after the implementation of blockchain, cryptocurrency get the importance. User just need the smart devices with internet and become the owner of own bank making payments and money transfer.
4. **Accessible:** This virtual kind of bank are easily accessible by the user from any time and from anywhere with the help of internet.
5. **Users become the owner:** User become the owner of this virtual bank and own perform the transactions without the usage of third part.

VIII. CRYPTOCURRENCY IN INDIA

Cryptocurrency in the form of bitcoin was introduced in 2012. But now RBI has banned the transaction of Bitcoins in India. That's why digital money cannot be used for the transaction and payment of goods and services. In the union budget of 2018, the Indian Government declared that usage of cryptocurrency such as bitcoin were illegal in India. There is no security and protection available to those using and

trading them or dealing them. Government also said that cryptocurrency is being used by the illegal activities such as drug dealing, terrorism and many more. According to Indian government, people who dealing with cryptocurrency should careful and take caution because there is no lawful protection of this kind of currency and no help can be given by the government side if any fraud is faced by the people (Singh & Singh, 2018).

IX. CONCLUSION

Cryptocurrency offers a new and attractive mode of payment that can enhance the revenues of companies. Virtual money enables the user to perform financial activities like buying, selling, transferring and exchanging easily apart from the real money. Virtual money like cryptocurrency are very recent topic in economy of the country. This paper tries to provide the overview of cryptocurrency and blockchain technology. Also highlight the threats which are included while using the cryptocurrency and also include the some reasons why cryptocurrency get popularity. After the popularity of this kind of virtual money, Indian government has ban its usage in India. Indian government cannot provide any kind of help to the people if fraud case can happen while using cryptocurrency.

REFERENCES

- [1] Jani, S. (2018). The Growth of Cryptocurrency in India: Its Challenges & Potential Impacts on Legislation. *ResearchGate*.
- [2] Kashyap, S., & Chand, K. (2018). Impact of Cryptocurrency in India. *International Journal of Law Management & Humanities*, 2 (1), 1-10.
- [3] Li, X., & Wang, C. (2016). The Technology and Economic Determinants of

- Cryptocurrency Exchange Rates: The Case of Bitcoin. *Decision Support System* .
- [4] Mukhopadhyay, U., Skjellum, A., Hambolu, O., Oakley, J., Yu, L., & Brooks, R. (2016). A Brief Survey of Cryptocurrency Systems. *14th Annual Conference on Privacy, Security and Trust*. IEEE.
- [5] Online, E. (2017, 10 25). *5 Reasons why you should go for cryptocurrency*. Retrieved 05 15, 2020, from [economictimes.indiatimes.com: https://economictimes.indiatimes.com/industry/banking/finance/5-reasons-why-you-should-go-for-cryptocurrency/articleshow/61184608.cms?from=mdr](https://economictimes.indiatimes.com/industry/banking/finance/5-reasons-why-you-should-go-for-cryptocurrency/articleshow/61184608.cms?from=mdr)
- [6] Reiff, N. (2020, 2 1). *Blockchain Explained*. Retrieved 5 13, 2020, from investopedia: <https://www.investopedia.com/terms/b/blockchain.asp>
- [7] Singh, A. K., & Singh, K. V. (2018). Cryptocurrency In India-Its Effect and Future on Economy With Special Refernce to Bitcoin. *Journal of Advance Management Research* , 6 (2), 262-274.
- [8] Thackeray, J. (2018, 07 17). *5 Inherent Risks of Cryptocurrency*. Retrieved 05 15, 2020, from Financial Executive International: <https://daily.financialexecutives.org/FEI-Daily/July-2018/5-Inherent-Risks-of-Cryptocurrency.aspx>
- [9] *Types of Cryptocurrency Explained*. (2018, September 21). Retrieved 05 15, 2020, from <https://www.trustetc.com/>: <https://www.trustetc.com/blog/cryptocurrency-types/>
- [10] Vejacka, M. (2014). Basic Aspects of Cryptocurrencies. *Journal of Economy, Business and Financing* , 2 (2), 75-83.