International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072

GROWTH OF CRYPTOCURRENCY

Dr. Dashrath Mane[1], Ms. Aishwarya Dhuri[2], Ms. Swati Mishra[3]

[1]Assistant Professor, VESIT, Mumbai University, Mumbai, Maharashtra, India.
[2]MCA Final Year Student, VESIT, Mumbai University, Mumbai, Maharashtra, India,
[3]MCA Final Year Student, VESIT, Mumbai University, Mumbai, Maharashtra, India.

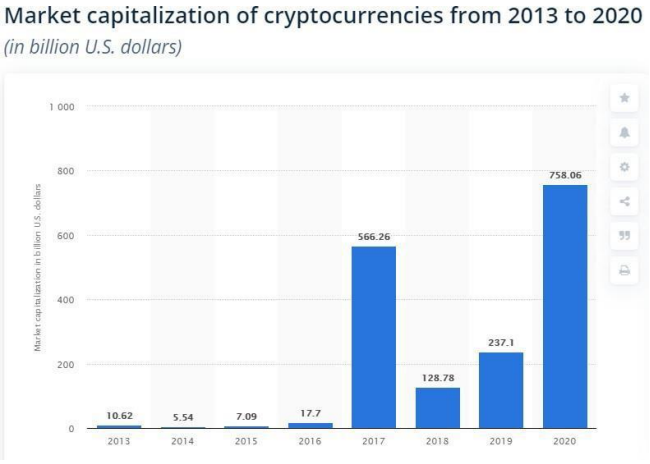
Abstract - *Advancement in technology has replace the traditional cash payment method with online payments but Now-a-days there is new term whichiscalled as Cryptocurrency. Cryptocurrency is a digital form of cash which is used for transactions .It uses Blockchain and cryptography for transactions. Cryptocurrency can be called as alternate to traditional system of money. It has not yet established trust asa new currency system in the world and people are still cynical about its worth. This paper is research on the technologies used in creation of cryptocurrency and types ofcryptocurrencies.*

Key Words: **Blockchain,Cryptography,Cryptocurrency**

1.INTRODUCTION

Money is important for every living human being on this planet and if we look back in history people used to buy goods with help of silver or gold coins but before that Barter System was used which means people used to exchange their goods with the goods they required. Gradually, Barter System was replaced by Monetary System. The metal coins were replaced by Paper Money as it was easy to carry around. Gradually, the use of cash transactions was limited as people started using Plastic cash i.e. credit cards and debit cards. Era of internet gave birth to Internet banking and due to further advancement of mobile phone technology, we can easily avail the facilities like mobile banking or mobile payment. But this all things are possible with help of a bank which is monitored by Government which is a kind of Centralized system. But due to development in technologies, new Decentralized form ofcurrencyis introduced which is Cryptocurrency.

Cryptocurrency is like a virtual currency which can replace the traditional method of currency.The bank or any financial institute cannot control or regulate it. Cryptocurrency named as Bitcoin was first created by Satoshi Nakamoto in 2009 which is completely decentralized. Some people use cryptocurrency as investment or alternate currency but mainly it is used as investment just like gold. Along with the most popular cryptocurrency Bitcoin, there are more cryptocurrency such as Litecoins, Zcash, Ethereum, Monero, Auroracoin, etc. There are more than 1600 cryptocurrencies which are available tilldate.



Apart from benefits of cryptography there are technical challenges to use them for day to day transactions. Also, there are many cases of money laundering ,theft, hacking etc. But slowly many countries are making Cryptocurrency legal.

1) Japan's government has allows some cryptocurrencies for payment and trading purposes and for that they have Payment Services Act which is based on a framework.
2) In 2013, US government accepted bitcoin for transactions.
3) Germany has allowed cryptocurrencies and also started the development of blockchain solutions.
4) France from 11th July 2014 has legalized cryptocurrency exchanges, taxation and permitted those who are involved in trading and use of such currencies such as bitcoin.
5) Malta has finally accepted few cryptocurrencies for digital transactions.
6) The Canadian government uses legalized cryptocurrency called impak coin
7) There is a region in Holland called "Bitcoin City" where transactions including purchases, trading and business are

legal with bitcoin. But government has not yet officially legalized the use of any cryptocurrency.

8) In Vietnam, cryptocurrency isn't consider payment tool but purchase of same are legal.

9) From 2017, The bank of Thailand has legalized the use of bitcoin.

10) India has finally legalized cryptocurrency i.e. bitcoin. India has made some provisions and has recently decided to levy a tax on cryptocurrency trading.

11) From November 2016, The Federal Tax Service of Russia has legalized bitcoins.

2. LITERATURE REVIEW

1. Akshay A., ShivashankaracharY. - "A Study On Security Issues In Investments And Transactions In Bitcoins And Cryptocurrencies" In this paper, they have highlighted the features of Bitcoin as a Cryptocurrency and the issues related with the transaction and investment of Bitcoins. As Bitcoins are related to currency and their value is increasing rapidly in the market, it's security is a point of concern. To establish a secured channel for transaction of bitcoins it is important to focus on it's security. Point of consideration related to the security of Bitcoins are their storage, extraction and transaction. The contemplate about online storage of Bitcoins is required. This paper also highlighted other risks associated with Bitcoins like no regulation regarding its transaction in India.

2. Everett J. & Team, Department of US Treasury - "Risks & Vulnerabilities of Virtual Currency-/Cryptocurrency as a Payment Method". In this paper, they have pointed out the practical approach towards the evolution of currency. The have led emphasis on the threats and difficulties that will arise in emergence of cryptocurrencies for illicit users, consumers, the official sector, and financial institutions. By observing the cryptocurrency needs and requirements for each set of people, it is comprehensible which set of people are most likely to steer to a specific cryptocurrency, and then find an appropriate response. The transformation from traditional currency to cryptocurrency as a new method of payment has many implications for financial sectors, illicit users, official sector and consumers. Before implementing the method of cryptocurrencies to proceed financial transaction on large scale, the threats and difficulties related to their security should be taken care. This adoption will require assimilation of the cryptocurrency protocols and regulation to cope up with all the risks and challenges.

3. Christian Catalini, MIT Expert- "Blockchain, Explained" In this Blog (MIT Digital),a brief up about Blockchain Technology and its origin is given. Its connection with the origin of Cryptocurrency is explained. According to him, the blockchain technology is the intrinsic root of Cryptocurrency which provide features like less cost for verification and networking, privacy and security etc. He has also led emphasis on the aspects like the disruption caused by blockchain technology in other sectors like Banking, Finance, Money Transfer, Money Payments, Identity & Privacy, Internet of Things, Robotics, Artificial Intelligence etc. He has also estimated that in coming decade Cryptocurrency will establish its root throughout the globe.

4. World Crypto Index (Cryptocurrency Guide, News and Reviews) All the knowledge about Cryptocurrency and its updates related to its core to advanced are available in this online platform. It focuses on main areas of the cryptocurrency and blockchain worlds:news, reviews, and learning guide.World Crypto Index gives latest information in cryptocurrency like Bitcoin. It has led emphasis on the security aspects related to Cryptocurrency. It gives price chart that helps to know about various cryptocurrency, of their working and the technology they use. it also provides a thorough Cryptocurrency Learning Guide which consists of useful information for beginners as well as for the experienced enthusiasts.

5. Sudhir Khatwani (CoinSutra) – "Future of Bitcoin and other Cryptocurrencies in India after RBI's Ban" In this article, the author has highlighted the framework of Bitcoins and other Cryptocurrencies in Indian Market after the RBI's ban of transaction of these virtual currencies in INR (at money) through its own entities like banks and other financial institutions. The author emphasized over the various implications against the ban of the transactions of these cryptocurrencies through banks. He has marked the past events related to the ban of cryptocurrency by Chinese Government which resulted in upsurge demand of cryptocurrencies by crypto investors through other channels. The same can happen in India also because India has a large number of platforms and transaction facilities which makes buying and selling of cryptocurrencies in India possible. He has also discussed the innovative technology associated with the origin of Cryptocurrency, i.e. Blockchain which is going to be the new Dot Com Boom in the world in coming decade and by banning the Cryptocurrency in India, the millennial investors and technocrats will miss a chance to establish themselves in this field.

3.CRYPTOCURRENCY

Cryptocurrency uses cryptography and blockchain technology for securely exchanging keeping track of transactions.

Blockchain

A Blockchain differs from a typical database. .A blockchain is chain of blocks that contain information in encrypted format. Its a distributed ledger completely available to anyone and has real-time access. Once data is recorded inside of the blockchain, to make changes in it is very difficult. Blockchain have Blocks, Nodes and Miners.

Blocks consist of data, nonce and hash. Blocks consists majorly of Hash, Data, Nonce. The data stored inside of a block depends on the type of Block. Nonce is randomly generated which is 32-bit and hash(256-bit) is joined to nonce. When blockchain is created, nonce generates hash and its not changed until data is mined. Miners generates blocks by mining. Since every block has unique nonce and hash, its not easy to do mining. Miners use complex computation to find nonce that will generate the hash.
When miner finds the correct nonce, its distributed among the nodes and if they approve it, the block is added to the chain and miner is rewarded. Finding correct nonce requires lots of time and computing power.

Since blockchain is decentralized, nodes are connected to block chain. These nodes can be devices that maintains the functioning of blockchain. Each node has a copy of its own blockchain and network must automatically approve the new block to update and verify.

Cryptography

Using cryptography, user can send secure messages to different users. This encryption is done using a key and algorithm. When encrypted message is received by receiver, they decrypt it to generate original message. This technique makes the data or transaction unreadable for unauthorized user and can only processed using a key. For transaction or sending message many cryptocurrencies use various forms of cryptography.Symmetric Encryption Cryptography use same key to encrypt as well as decrypt a message. An example of same- A = '1', B= '2' and so on.
Encrypted message such as "HELLO" becomes 85121215" receiver will decrypt by reversing it. Complex variations also exists for security. Asymmetric Encryption Cryptography is another method, which use two different keys private and public - to encrypt &decrypt the data provided. The public key is kept in open , while only the owner knows the private key. In this way, the owner can encrypt the message using public key of the receiver, but the decryption can only be done by using private key of the receiver. another method is known as Hashing, in which it maintains the blockchain data structure, addresses are encoded, it is also an important part for encrypting of transaction that are made between accounts, and which in turns make block mining possible, Digital Signatures are used by many various cryptography process to allow authenticate users to network. Multiple methods of cryptography exists with many customization are used in cryptocurrency.

Transaction Process of Cryptocurrency

Cryptocurrency is created as alternate for transaction as a normal currency. Cryptocurrency used Blockchain and cryptography for tracking transactions. The transaction of cryptocurrency can be explained as follows

1. A person needs to send money to other person.
2. This transaction is called “block”.
3. Block is shared with everyone inside the network.
4. Those who are part of the network could approve the valid transaction.
5. After a Block is added in the chain, then it provides transparent transaction.
6. The money goes from the sender to receiver after this process.

Advantages

✓ No limit on coins.
✓ Easy verification of transactions.
✓ Operating independent of bank.
✓ Almost no transaction cost.
✓ All time access to money.
✓ No limits on particular withdrawal.
✓ Freedom for anyone to use not specific to country.
✓ International transactions are faster.

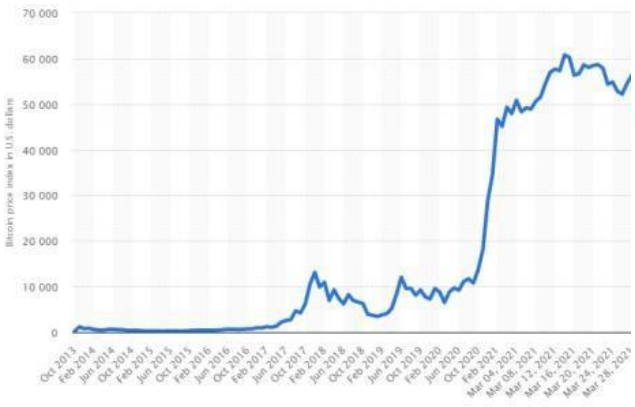
Disadvantages

✓ Money laundering and thefts.
✓ Hacking .
✓ On dark web, people are using it to buy weapons and drugs.
✓ Difficulty to track transactions as theseareoutside traditional financial system.
✓ Anyone can create own cryptocurrency.

Different Types of Cryptocurrency

Bitcoins

Bitcoin is form of digital currency and is decentralized without central bank. It uses blockchain to perform transactions on pee- to-peer network. Its transactions are manual. It uses 10 minutes to perform transaction .There's a limit to how many bitcoins can exist:21,000,000. It uses SHA256 algorithm for hashing. The price of Bitcoin reached $52,500 in February 2021.



Litecoins

Litecoin is fully decentralized global payment network. It went live on october13,2011.As of march 2021, Litecoin has value of

$13.7billion. Minors are currently awarded 12.5 new litecoins per block. Litecoin uses scrypt algorithm due to this FPGA and ASIC devices used for mining are complicated and expensive to produce than bitcoin. he advantage of Litecoin that it can process the block in 2 minutes and 30 seconds where it takes 10 minutes by Bitcoin.

Ethereum

Ether is a currency that's accepted in Ethereum network. It works on blockchain technology. It takes 20 seconds to finish transactions. Also transactions are manual or automatic. Expected to be continuous but not expected to exceed 100,000,000.It uses ethash algorithm for hashing.

Namecoin

Namecoin is storing system based on bitcoin. Namecoin utilizes the same proof-of-work (PoW) algorithm as Bitcoin. The mining of Namecoin is same as of Bitcoin, and limit issued of coins is 21million. The major difference are possible of storing data inside it's own Blockchain transaction database and registering a unique Domain name along with .bit address but the main issue with this appears to be with the choices of name just it may happen that it can be already taken. It is currently priced at 0.407581 US. It is currently ran 629th rank. It was developed for increasing privacy and security.

Ripple

Ripple is also called as XRP. RippleNet uses RTXP for moving value around world.XRP is a technology which is known for its digital payment network and protocol. XRP is a technology is known for it's protocol & payment with digital mode. Ripple is known for asset exchange, Remittance system and payment settlement. XRP has 100 billion pre-mined cryptocoins.

Auroracoin

Auroracoin was released in 2014 in Iceland and it is decentralized, peer-to-peer, and secure cryptocurrency. It is based on Blockchain and was created to bypass governmental restrictions associated with the national at currency. Auroracoin uses Scrypt algorithm, and is a clone of the popular cryptocurrency Litecoin. Auroracoin has a current supply of 18,078,319.753. The last known price is $0.028883 USD

Monero

Monero is an open source decentralized cryptocurrency which was launched in April 2014. It's transaction is untracable and not linkable as coins which are received by the recipient are rerouted through address that is randomly generated to be used specially for this transaction.

Zcash

ZCash has a decentralized blockchain which keeps its users and their transactions anonymous. ZCash uses zero-knowledge proofs (zk-SNARKs) for validating transactions and it doesn't reveal information of users. ZCash's total market capitalization is $403 million as per April 30, 2020.

Bit coin cash

This was started back in August 2017 by miners and developers of Bitcoin which is known as Hard Fork, in a way they created a new currency known as BCH. It has their own specification and Blockchain and the major difference is BCH has block size of 8 MB. Bitcoin owners at time of creation of fork are owners of bitcoincash.

Bitcoin private

Bitcoin Private was released in March 2018.Even if Bitcoin Private sender, recipient and other transactional metadata remain unidentifiable its payments gets published on a

public blockchain. Bitcoins private was created from a copyofadigital currency known as zclassic.

4. CONCLUSIONS

Cryptocurrency is new age attractive mode of payment that can increase companies revenues. This is opening a new door for paying that will enable the user to make financial activities as selling, exchanging, transferring and buying easy but they aren't regulated and controlled as they are deserved to be. My analysis indicates that cryptocurrency is that People are aware of Cryptocurrency but see it as an investment because of good returns but due to lack of regulations and laws they are not willing to invest in it. But as many countries are making cryptocurrency legal , there is a chance of replacing it with monetary system. In the future the concept of cryptocurrency is much promising it will give positive evolution to e-Business and e-Payment sector. With constant development in field of cryptocurrency and technology will reach new heights.

REFERENCES

[1] https://www.weforum.org/reports/the-future-of- financialinfrastructure-an-ambitious-look-at- howblockchain-can-reshape-financial-services
[2] Paul Vigna, Michael J. Casey, “The Age of Cryptocurrency”
[3] Dominic Frisby, “Bitcoin: the Future of Money?”
[4] Deepika Chawla, Neena Sondhi, “Research Methodology – Concepts and Cases”
[5] https://blockgeeks.com/guides/what-is- cryptocurrency/
[6] http://empirica.io/blog/different-types- cryptocurrency/
[7] https://en.wikipedia.org/wiki/List_of_cryptocurrencie s
[8] https://www.statista.com/statistics/326707/bitcoin- price-index/
[9] https://www.investopedia.com/terms/c/cryptocurren cy.asp
[10] https://www.researchgate.net/publication/316656878_An_Analysis_of_Cryptocurrency_Bitcoin_and_the_Future