"BlockChain: The new crude oil or The Internet of 90's"

Ashutosh Pandya

B.Tech Scholar, Dept. of Computer Science Engineering

Shri Vaishnav Institute of Information Technology
Shri Vaishnav VidhyapeethVishwavidhyalaya,Indore-India

Abstract:

Blockchain technology is a comparatively new approach in the digital world. It is one of the most emerging technologies of the modern era. Blockchain is the base for the bitcoins and other cryptocurrencies. Blockchain's have an incorruptible digital ledger which is proving to be the backbone of digital transactions. Blockchain also omit's the middleman and the third party reliability .Its also helping in solving the concern of privacy over the Internet .The technology is of great potential and has the power of changing our lives. As a result a large scale investment is being made in the field Blockchain technology. This paper is meant to give a brief introduction to the underlying aspects of Blockchain and Cryptocurrency .The document also aims to showcase crypto market as a platform to earn money and shows Cryptocurrencies as "Digital Gem".

*Keywords:*Blockchain,Crpytocurrency,Earni ng money with Crpytocurrency, Bitcoin, Ripple,Litecoin, Ethereum.

1. Introduction to Blockchain:

Earlier data was recorded manually in ledgers. After digitalization, the same data was been recorded digitally in centralized systems which led to the security flaws in the system. Block chain technology is nothing but a decentralized digital ledger with a strong encryption algorithm.. Rather than using centralized databases, it uses decentralized way of storing data. Trust is the factor that affects the centralized systems as they are controlled by single level of authority. Block chain eliminates the man in middle. Cryptographic principles enable secure and trustworthy transactions with minimal chances of failure. No central authority is required hence it provides a distributed environment. Transparency is another aspect of the blockchain technology as information is circulated to each peer in the network.

Blockchain technology affects a vast variety of potential areas of application by revolutionizing the way transactions are accomplished. It allows digital information to be distributed and restricts the alteration of information as it would require an immense computational power. It isRevolutionizing the way we transact on internet and eliminates ownership.

2. Literature Review:

The document aims to throw light on Blockchain the foundation for the Bitcoin and other different cryptocurrency along with their history and evolution with time. The market captured by the different cryptocurrencies around the globe. The paper reviews some most popular articles and research paper related to Blockchain and Cryptocurrencies . Some of the research papers and articles we came across during our studyare:

"Bitcoin: A peer-to-peer electronic cash system" by S. Nakamoto[1].

In this paper S. Nakamoto has proposed a peer-to-peer system for electronic transactions which eliminates the third-party. This led to the introduction of Blockchain Technology.

"Top ways to earn money from cryptocurrencies" by Sudhir Khatwani, [22]

This article is about earning in cryptosphere.It showcases some of the best ways by which money can be earned using cryptocurrencies. Such methods can often lead to getting caught in scams. Methods such as Mining, Buying and Holding, Arbitrage, Masternodes, etc are reviewed as a method to earn money in this particular article.

"Crypto-currency market capitalizations," Available: https://coinmarketcap.com[18]

The market capitalizations of top 100 cryptocurrencies is reviewed in this article. The market capital of Bitcoin being the largest ($68,990,027,384)

3.Cryptocurrency: A brief review

Cryptocurrency is a digital currency that uses principle of cryptography that is difficult to counterfeit. Earlier, we used to transact digitally but the whole process was centralized . The whole scenario changed when a research paper named "Bitcoin: A Peer -to- Peer Electronic Cash System" got published by Satoshi Nakamoto in 2008(actual identity still unknown). The central idea of the paper laid emphasis on the fact that the digital transactions require proof instead of trust. There are more than 1600 cryptocurrencies available over the Internet and are still growing. Some of the commonly known currencies are Bitcoin, Litecoin, Ethereum, Ripple, Ethereum Classic,etc.

3.1 Cryptocurrency Mining: In the case of paper currency there is a central authority that regulates the various functionalities such as printing and distribution. Since there is no central authority in the case of Bitcoin, new blocks are added by miners using special dedicated softwares. Miners perform a very similar functionality like mastercard and visa but in a quite different style. Mastecard and Visa records different types of transaction and verifies them but the scope of whole process is private. In contrast miners do the same task and records the transaction in the public ledger which can be publically accessed. For adding a new block miner has to solve complex math problems which requires time, electricity and resources(for processing). A miner is issued a few Bitcoins as a reward for adding a new block. Mining plays an important role in providing data integrity which in turn provides safety, stability and security to the network and makes it trust worthy.

3.2 Proof-of-Work and HashCash:

 Proof-of-Work is the original congruity algorithm in a   block chain network. Bitcoin is underlayed by a strong foundation of distributed legder which prevents tampering. As the ledger is public any type of alteration made in the ledger would be quickly rejected by other users in the chain. The proof of work detects tampering through Hashes, any minute change in data would result in the totally changed hash. In a transaction of 2000 BTC if 0.0001 BTC are altered, the Hash generated would be detected as fraud and will be rejected.

3.3 Bitcoin:

Bitcoin was the first decentralized Cryptocurrency introduced in 2009.It initially had no value but by the end of 2010 it was valued $0.125 per BTC accounting to a highest value of $19,783.06 per BTC in December 2017.

In the initial span of 3 years the size of ledger was between 1 megabyte to 13,468 megabytes and it is growing at a surging rate. The size of the ledger by the end of 2018 was 1, 97,224megabytes.

Bitcoin uses a very powerful cryptographic technique. The aim is to provide data integrity. It uses SHA(Secure Hash Algorithm) such as SHA-256, SHA-512. Any type of string can be given as an

input to these hash functions and the output of the function is a string of fixed size(Hash).

The hash functions used are so sensitive that if a minute change is being made to the input then the whole hash changes significantly.

3.3.1 Legalisation of Bitcoin:

Bitcoin is a virtual currency. The fact associated is that the user is anonymous . In India, the government has declared Bitcoin(and other cryptocurrencies) as unauthorized(neither legal nor illegal).The major problem could be with the existing taxation system and traceability of transaction hence the decision is in "No Man's Land". Even though Bitcoin was developed with the aim to make it a single currency for the World, there are many absurd to the fact. Bitcoin also enables billions of people around the Globe to participate in world economy. The best part of the Bitcoin is that it does not react to the demand pressure like gold hence it is bestowed as "DIGITAL GOLD".

3.3.2 Market worth of Bitcoin around the globe: According to statistics, if we calculate the total number of Bitcoins in circulation to the price, the total value amounts to 66.18 billion (US dollar) with a maximum of 237.62 billion (US dollar) in December 2017 when the value of Bitcoin was skyrocketing . The United States of America trades the most in Bitcoins(22.77%) which is followed by Russia(16.55%) and United Kingdom(11.67%).

3.3.3 Bitcoincount:

Like gold Bitcoins cannot be created, they have to be mined in a similar fashion like gold but Bitcoins have to mined digitally using immense computational power .The number of Bitcoins that can be mined are predefined in the protocol which are around
21 million .This figure will not change unless there are changes being made in the existing protocol. Bitcoin miners have mined around 16.8 million Bitcoins which is around 80% of all the Bitcoins. If the rumors are true all the Bitcoins will be mined till 2140.

3.4 Ethereum:

The applications on Ethereum run on its platform .Although its far behind Bitcoin (BTC),the current market cap of ether (ETH) is now more than Ripple and Litecoin .In 2016, a malicious actor stole more than $50 million worth of funds. Since then Ethereum was splited into two separate blockchains - Ethereum, and Ethereum Classic. There are more ether coins in circulation than Bitcoins. In July 2018 Ethereum was the second-largest virtual currency on the market, following Bitcoin.

Ethereum is a platform based in block chain which uses ether as it's fuel. Autonomous smart contracts and decentralized apps are written on this platform. It is a kind of smart contract system and has significant technological implications. Once the code is written on the Ethereum blockchain, it can't be altered, tempered, or hacked. It is an incentive awarded by clients on completion of requested operation. Unlike Bitcoin, ethereun is a programming language that enables developers to build and publish distributed applications. The most powerful advantage is that Ethereum transactions are confirmed in seconds .It uses ethash algorithm.
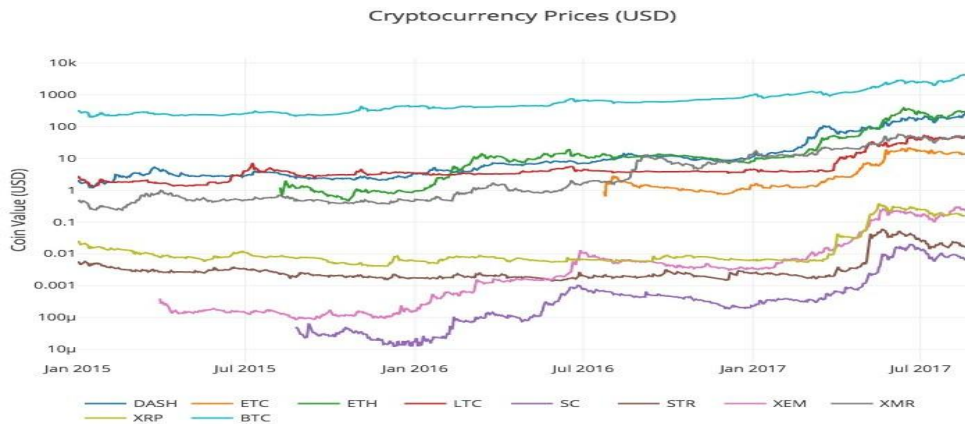
3.5 Litecoin:

Litecoin is one of the peer to peer Cryptocurrency through which user can transact instantly with a negligible transaction fee. Charlie Lee is the creator of Litecoin. It can be regarded as a more lighter form of Bitcoin. In comparison to Bitcoin, Litecoin is different in many ascpect such as Bitcoin uses SHA-256 while Litecoin uses Scrypt. In SHA-256 the processing is parallel while in the case of Scrypt there is a serialized processing which indeed saves a lot of memory. Litecoin's average mining time is 2.5 minutes which is lesser than that of Bitcoin's which is nearly 10 minutes. Litecoin's total

unit in the network are four times to that of Bitcoin's which is 84 million. Litecoin has gained a hooping of 7,291% to what its value was initially which is way ahead in the race from Bitcoin. The number of coins that are awarded are also double to that being awarded in Bitcoin. The market capital of Litecoin was valued around$540,274,528.26.

3.6 Ripple:

Ripple is also one of Cryptocurrency in the cryptoworld and also an open source platform . The main aim for designing was a fast and cheaper way of performing transactions. International transactions are very time consuming, following one after other payment gateway and a numerous middleman in the process making the process time consuming and unsecure. Even transporting money physically would be more time taking. Currently Ripple's chain has the fastest transaction speed of only 4 seconds. Moreover the number of transactions that can be verified are 1,500 transaction per second were as Ethereumcan handle only 15 transaction per second and Bitcoin only 3-6 transaction per second .Fast transaction speed along with more transactions per second is like cherry on the icing and makes transactions more scalable.

Prices of Different Cryptocurrencies

Top 5 Cryptocurrencies by Market Capitalization:

Name	Market Cap	Circulating Supply
Bitcoin	$68,622,176,528	17,575,350 BTC
Ethereum	$14,541,218,964	105,135,120 ETH
XRP	$13,075,163,918	41,432.141, 931XRP
EOS	$3,420,085,882	906,245,118 EOS
Litecoin	$3,375,655,346	60,772,611 LTC

4. How to Earn usingCryptocurrencies:

4.1 Mining: It's the most common and profitable form of earning cryptocurrencies till date. Mining requires an immense use of computational power. Cloud mining is the most efficient way of mining in which a share of mined currency is shared .Hosted mining is also becoming popular in the recent times.

In hosted mining, a mining machine is send to some that provides facility of electricity and cooling. Hosted Mining came into the scene as electricity rates for home usage were not veryefficient.

4.2Buying and holding: Like any other commodities, Bitcoins can be purchased and hold till there is an urge in the market price. This approach is identical to that of stock market in which shares are purchased and then sold at higher rates. Though the Cryptocurrencies have made incredible gains in the year 2017, it suffers from serious volatility. The issue of price fluctuation in Cryptocurrencies is of great concern and often lead to market risk.Still this strategy is quite effective when it comes to earning. It is well said, in the cryptosphere only those who can finally analyze the market or are day traders can make money.

4.3 Staking : Staking is a form of intensive mechanism along with mining. It is just like fixed deposit in which an interest is generated in a course of time. Similarly Stacking is the exercise of purchasing crypto coins and holding them in a Cryptocurrency wallet for a particular time period.

4.3.1 Proof of Stake(PoS):

According to the number of coins a person holds, mining and validating transactions cab be performed. PoS was created as a substitute to the proof of work(PoW).Mining power of an individual is determined by it. More the number of coins, more the minig power. The PoS addresses the issue of Pow. The percentage of coins a miner holds, attributes his mining power. A PoS miner instead of solving PoW puzzles by utilizing energy, is restricted to mine a proportion of transactions that is retrospective of his ownership stake. Peercoin was the first Cryptocurrency to adopt the PoS method followed by Blackcoin and Shadowcoin.

Despite of the fact that the fluctuations in Cryptocurrency price do affect the value of the stake, the value of cryptocoins that are staked through PoS does not depreciate with time.

4.4 Masternodes: The computer wallet keeps a real time full copy of blockchain. The developer of the Masternode isoften paid in lump sum. However for the development of the masternode the developer must have a minimun amount of coins. The range is usually between 1000 to 25,000 coins. The Masternode always communicates with other nodes so they are not standalone and make a decentralized network. Masternodes are not very profitable. When it comes to running a full node computer on a blockchain network, the increase in price and technical complexities leads to a decline in the number of full nodes.

4.5 Cryptocurrency Arbitrage: There was a time when cryptocurrencies were at its peak. Since then the cryptomarket is facinga decline and a good news is that even withsuch declination, money can be made on cryptocurrencies using arbitrage. It includes trading a coin when it is less valuable and selling it to another exchange when it gets more valuable. The two separate values encounter at a midpoint, and an interest from the amount of convergence is acquired.

A profit from the asset is made by buying it at lower price and then selling it at higher rice at to different exchanges. Inefficiency between exchanges and surge in trading volume leads to the rise in price differences.. Multiple strategies can be used by arbitrage traders such as-

Simple arbitrage- It includes trading in same coin on separate exchanges .

Triangular arbitrage- It includes trading in three currencies.

Convergence arbitrage- It includes trading a coin when it is less valuable and selling it to another exchange when it gets more valuable. The two separate values encounter at a midpoint, and an interest from the amount of convergence isacquired.

4.6 Cryptocurrency Faucets/Faucet Framing: Cryptocurrencies are the newer form of asset for the people around the globe. Faucet refers to small dipping water from tap. Similarly, Cryptocurrency

Faucets are the small rewards given for performing a small task , Cryptocurrency Faucets are one of the most popular form of earning Cryptocurrency The task can be anything from completing captcha to clicking links for increasing the traffic of the website. The amount that are received from the method are very less often about hundred of a million. The earliest rewards were in Bitcoins and with gaining popularity of ethers and Ripple the rewards are also being given in these currencies. The aim behind using faucet farming was to popularize the currency. Giving free coins provided an advantage that the interested user can start trading without risking money. Even the user can collect the coins and sell themwhen the prices reach highsky. Faucet Farming requires lesser time and brain. The stakes are also not so high infauceting.

4.7 Lending Cryptocurrencies: With the gaining popularity of cryptocurrencies, the amount of investments in the Cryptoworld is increasing subsequently. Similar to the traditional currency, cryptocurrencies can be lended to earn interests. The interest rate often varies from 3% to 8% annually. The lenders register on the platform and Cryptocurrency lending platform works by connecting borrowers to a network of lenders .In order to borrow, Collateral i.e. borrower's crypto asset needs to be deposited first on the platform. The lender lends amount to the borrower and earns interest over it. As the amount and interest is repaid, the borrower get back it's crypto asset. Some of the platforms are ethland, salt, bitfinex, poloniex,etc.

4.8 Cryptojacking:

Cryptojacking is the most brainy method used by hackers and miners to mine Cryptocurrency. The method involves usage of any of the computational device such as mobile, laptop, personal computer or cloud. The most typical part of the process is that it doesn't involves installing an application or program in the victim's device rather a java script file is being executed in the browser. The Hackers find cryptojacking a more interesting way of earning than other methods as the amount of resources used by the hacker is very less as compared to the profit earned. In contrast to stealing the data, the aim is to steal the processing resource. According to the reports there has been a
459 percent hike in the cases of Cryptojacking. There was a time when ransomware attacks were common but the share of Cryptojacking to the other stealth attacks is increasing at a surgical rate.

5.Conclusion:

Cryptocurrency and the blockchain technology have become everyday words. The Cryptocurrency market has grown from a market capitalization of $0.00 in 2010 to over $430 billion in 2017**.** There has been an absolute return of over one million percent which has driven interest in this technology. Bitcoin isn't a use case of internet like the e-commerce or social networking but it is as fundamental and parallel to internet. It has the potential to change our lives in the coming years same as the internet has done to us in the past 20 years.

Bitcoin is likely to experience more growth in the five-year time horizon. Ethereum,while having a lower expected value, it has wide range of outcomes, both positive and negative, indicates that it should be included in the investment portfolio. Litecoin can be preferred as a new investment option showing lesser variation than Ethereum.

The impact that these technologies will have on the world is still unpredictable but blockchain are too revolutionary. Governments may try to limit further innovation. Quantum Computing is said to be killing blockchain .With traditional computer using only two bits (0's and 1's) it's a trivial task to crack the encryption used in the blockchain but with quantum computers' being a 100 million times faster it would be a feasible task to break the encryptions used and thus exploiting the underlying of the blockchain.As the technology is not matured and wide spread there are much more chances for the survival of the blockchain. Blockchain Technology have a great potential and it will change the lives of the people like the internet in 90's did .The Business and investments made in the time turned out be a good assest. The technology when combined with others such as E-Commerce, Artificial Intelligence would symbiotically enhance their efficiency .Similar to the fundamentals of the crude of oil the

technology aims to be the fuel for the digital accounting across the globe.

References:

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.[Online].Available: https://bitcoin.org/bitcoin.pdf

[2] "State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available:http://www.coindesk.com/ state-of- blockchain-q1-2016/.

[3] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016.

[4]NRI, "Survey on blockchain technologies and related services," Tech. Rep., 2015. [Online].Available: http://www.meti.go.jp/english/press/ 2016/pdf/0531 01f.pdf

[5] "Antshares digital assets for everyone," 2016. [Online]. Available: https://www.antshares.org

[6] Raphael Auer, " Beyond the doomsday economics of "proof-ofwork" in cryptocurrencies" 2019 [Online] Available: https://www.bis.org/publ/work76 5.pdf.

[7] JakeFrankenfield,"Proofofstake",2018.[O nline]Available:https://www.investopedia.com/terms/p/proof-stake-pos.asp

[8] Jonathan Chiu, Thorsten Koeppl, "The Economics of Cryptocurrencies – Bitcoin and Beyond" 2017[Online] Available: https://www.chapman.edu/research/institutes -and-centers/economic-science- institute/_files/ifree-papers-and- photos/koeppel-april2017.pdf

[9]B. W. Akins, J. L. Chapman, and J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy," 2013. [Online]. Available: https://ssrn.com/abstract=2394738

[10] Chalmers Brown, "Benefits of Russia to legalize Bitcoins" 2016.[Online] Available: https://due.com/blog/benefits-for-russia-to- legalize-Bitcoins/

[11] Tom Alford, "Bitcoin Adoption: Trading Volume by Country" 2018[Online] Available: https://totalcrypto.io/Bitcoin- adoption-trading-volume-country/

[12] Dr. Gavin Wood, "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER" [Online] Available: https://gavwood.com/paper.pdf

[13] Frederik Armknecht , Ghassan O. Karame , Avikarsha Mandal , Franck Youssef, Erik Zenner,"Ripple:Overview and Outlook "2015,[Online]

[14] Vitalik Buterin, "Ehereum White Paper A NEXTGENERATION SMART CONTRACT AND DECENTRALIZED APPLICATION PLATFORM"2017 [Online]Available: https://whitepaperdataba se.com/ethereum-eth-whitepaper/

[15] https://litecoin.org/

[16] https://blockgeeks.com/guides/litecoin/

[17] Jorn van Zwanenburg, "Invest in blockchain" 2018.[Online] Available: https://www.investinblockchain.com/what- is-Ripple/

[18] "Crypto-currency market capitalizations," 2017. [Online]. Available: https://coinmarketcap.com

[19] https://cdn.patricktriest.com/blog/image s/posts/crypto-markets/plot- images/altcoin_prices_combined.png

[20] https://coinmarketcap.com/

[21] Charles Bovaird, "Bitcoin's Market Cap Is Now More Than $100 Billion" 2017.[Online]Available:https://www.forbes. com/sites/cbovaird/2017/10/20/Bitcoins- market-cap-is-now-more-than-100- billion/#72c3c5a82b8b

[22] Sudhir Khatwani, "Top ways to earn money from cryptocurrencies" 2018. [Online] Available: https://coinsutra.com/earn-money-from- cryptocurrencies/

[23] Prashant Ankalkoti, "A Relative Study On Bitcoin Mining"[Online] Available:https://www.researchgate.net/ publ ication/318850089_A_Relative_Study_on_ Bitcoin_Mining

[24] Sudhir Khatwani,"What Is A Masternode And How Is It Useful For Cryptocoin Investors".