IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

A Review on Evolution of Cryptocurrencies using Blockchain

K. Hema[1*], A. Ravi Prasad[2], J. Kishore Kumar[3]

[1]Dept. of MCA, SVCE, Tirupati, Chittoor District, Andhra Pradesh, India
[2,3]Dept. of Computer Applications, SGGDC, Piler, Chittoor District, Andhra Pradesh, India

[*]*Corresponding Author: goldenhema@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7si6.8286 | Available online at: www.ijcseonline.org

***Abstract* :** Cryptocurrency, which operates as a Peer to Peer Electronic Cash System. Cryptocurrency has a potential to be a major means of payment for e-commerce. In Cryptocurrency the word -"Crypto" refers to various encryption algorithms and cryptographic techniques are employed. Cryptocurrency has numerous latent value propositions and long-term use cases including Distributed Ledger Technology (DLT) and Blockchain innovations. This technology is not issued by any central authority and it is theoretically not effecting to any Government interference. The first Cryptocurrency based on Blockchain was Bitcoin, which is still the most popular and valuable. The success of Bitcoin brought number of competing Cryptocurrencies like -Altcoins. For example Altcoins are- Litecoin, Namecoin, Ethereum, Peercoin, Dogecoin, Monero, EOS, and Cardano etc., At present there are literally thousands of Cryptocurrencies in existence, with an aggregate market value around $200 billion. But the future of Cryptocurrency is impossible to predict, and although it is unlikely that Cryptocurrency will eliminate trusted intermediaries like Financial Payments, Settlements, Clearing, Supply Chain, Agriculture, Voting, Data Protection Mechanisms, Crowd-funding, Decentralized business applications and Services. There may be benefits of Cryptocurrencies towards hype-financed research and development in DLT and Blockchain infrastructure. The main purpose of this study is to narrate the evolution of Cryptocurrency using Blockchain Technology. The study also includes the growth of technology and the challenges that are faced at the time of development. However there are inherent difficulties in regulating the cryptocurrency market, which will be discussed in detail in this paper.

***Keywords* --** *Cryptocurrency, Bitcoin, Blockchain Technology, Distributed Ledger Technology, Financial Payments.*

I. INTRODUCTION

A Cryptocurrency is a digital asset or virtual currency that uses Cryptography for security and to control the creation of new coins. Cryptocurrencies can be defined as a subset of digital currencies. The Government have the full control over the value of a currency but in case of cryptocurrency Government has no control because of decentralization [1]. The first Cryptocurrency- Bitcoin was launched in 2009 by Satoshi Nakamoto. Bitcoin functions uses Blockchain technology which stores all the transactions with some defined data structure and also organizes data into blocks and copied across all computers running Bitcoin software. Blockchain has applications for many industries like healthcare, insurance, pharmacy, manufacturing, healthcare, e-voting, legal contracts, tourism, energy, and travel industry [2] .

Blockchain is a technology which depends on Distributed Ledger. Distributed Ledgers use independent computers to refer it as nodes to record, share and synchronize transactions in their respective electronic ledgers. With the success of Bitcoin number of Cryptocurrencies are developed such as Altcoin , Ethereum, EOS and Cardano etc,. In this study the evolution of various Cryptocurrencies from Bitcoin is Studied.

II. SCOPE OF CRYPTOCURRENCY

With the effect of demonetization there has been a great bonding for Cryptocurrencies in India. Since five years Bitcoin made its debut in Indian Financial markets. Even though there has been number of notifications circulated by the finance ministry there has been a rapid rise in transactions of Cryptocurrencies. With this it is very clear that there is a bright future of Bitcoin in India . At present there are approximately 1548 Cryptocurrencies operating in the market alternative to Bitcoin. [3]

Scope of adopting Cryptocurrency in Indian market: In the present digital world, where technology is playing a crucial role in transforming the digital economy of the world, India is no different in taking baby steps while adopting the digital form of currencies such as Bitcoin's. At present, there exist an estimated total Bitcoin(Cryptocurrencies) turnover of Rs 300 crore in India with a huge user base of around 1,00,000 people. It is also being forecasted by industry experts that Bitcoin is all set to expand its user base steadily across different parts of India

with their adoption to grow at 200-300 per cent annually in order to bring a digital revolution. We are walking ahead in search of a planet where transactions could take place between user ends digitally and not through the same conventional way. All these transactions are verified by the network nodes that are recorded in a public Distributed Ledger called the Blockchain, which empowers and uses Bitcoin as its unit of account. It is nothing but a smart way to cross boundaries and check out an innovative as well as quick method to deal with your day to day financial transactions[4]. The virtual currency can be converted into physical form through various online exchange platforms. Taxing the cryptocurrency is another way to legalise this currency that's why It becomes a risky investment option.

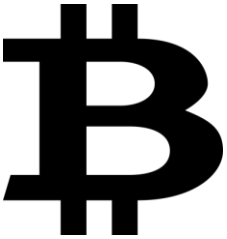

Fig 1: Symbol of Bitcoin [5]

Bitcoin is a tricky thing because of decentralisation and having no central authority. Government cannot track the moment of money via Bitcoin because of volatile nature. Apart from security issues, government has to take care of an individual's personal privacy and security from hacking into the individual account and transfer Bitcoin's(Fig 2). Still there are some reasons in legalising Bitcoin's in India and GOI is a step backward even though Bitcoin has its own set of features.

- Bitcoin is permission less.
- It is very fast and cheap to utilise.
- You can send money to anyone anywhere(24*7).
- No bank can deny your accounts, cards or transactions.

And now people have started to realised it. They are using Bitcoin's for accepting payments, recharging their mobile phones, paying their electricity bills. Government may not stop this behaviour. It is better to regulate it than let it flourish without any government control [6].

III. CRYPTOCURRENCIES: AFTER BITCOIN

In this study we will see the evolution of Cryptocurrencies after Bitcoin growing exponentially. After Bitcoin creation the first Altcoin came out after two years. Then the rate of Altcoin started to grow from 2013 onwards and increasing till now.

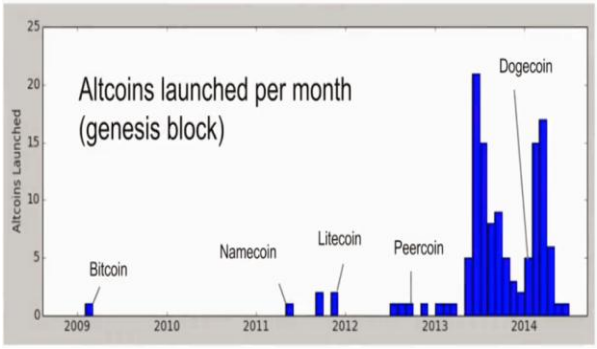

Fig 2: Types of Altcoins[7]

ALTCOIN CLASSIFICATIONS:

Altcoins classification rely on Altcoins genealogy. There are many Bitcoin-like alternatives like Litecoin, Namecoin, Peercoin, Dogecoin, Monero, Cardano and Ethereum etc,. However, there will be differences between each Altcoin such as transactions management, differences in the scripting language, additional features like security, whether it is mining-based or not, it is with different consensus algorithms and so on. Why because they have different built in parameters they differ from Bitcoin [7].

Namecoin: Namecoin is a decentralized domain name management. Namecoin-the first Altcoin evolved in 2011, after two years of Bitcoin evolution. The purpose of Namecoin was to replace the domain name system in a decentralized way. A specific plug-in for Firefox or Chrome is available to access any website ending with ".bit". It will automatically take you to the right location suggested by the registry stored on Namecoin. To register a domain in Namecoin and to continue, it is necessary to send a transaction information to the Namecoin system. Some of the properties of Namecoin are-

- It gives the possibility to register a unique domain name which is not already in use for a small fee.
- It is not necessary to renewal and pay the fee to keep the domain and it is enough to publish every six months a transaction that pings the domain name under your control.
- Namecoin also manages sub domains in the same way as current domain system maintains. For example, if you have registered in mywebsite.bit, you have accessibility to all its sub domains.
- It is also possible to transfer domains to other people by selling them in exchange of some Namecoins.
- It was the first Altcoin having the feature of merge-mining.

Fig 3: Symbol of Namecoin[7]

Litecoin: Litecoin is the first memory-hard mining puzzle in the Altcoins. Litecoin was born in 2011 after Namecoin. For long time Litecoin was the second main Cryptocurrency after Bitcoin. The main technical difference between Litecoin and Bitcoin is its mining-puzzle. Litecoin uses a memory-hard mining puzzle, while the Bitcoin is a computation hard one. In 2011, Bitcoin mining already required GPUs and Litecoin purpose was to be GPU(Graphic Processing Units) resistant. Eventhough it is also possible to improve Litecoin mining first using GPUs and then with a specific Litecoin ASIC.
The progression of Bitcoin Mining went like this:
CPU Mining – It is a base standard in which everything began.
GPU Mining – Today a single GPU is roughly equal to 30 CPUs.
ASIC Mining – Today a single ASIC miner is approximately equal to 400 GPUs (12,000 CPUs).
Litecoin is the second most forked Cryptocurrency, it differs from Bitcoin just for some parameters change.

Fig 4: Symbol of Litecoin[7]

Peercoin: It is a first proof-of-stake mining puzzle
Peercoin was born towards the end of 2012 and it uses a very different mining puzzle- proof-of-stake. As we said in a previous study this method doesn't involve any computational work. But, it involves mining by making transactions using coins owned by the miner. Coins take more stake over time as long as the miner doesn't spend them. since it is an hybrid mining protocol Peercoin mining is a little more complicated, and supports proof-of-work also. In fact, the proof-of-work blocks aren't actually included in the calculation and it is not fully decentralized and we can't prove that proof-of-stake is a very secure mining protocol since Peercoin relies on the checkpoints.

Fig 5: Symbol of Peercoin[7]

Dogecoin: It is having fun with Cryptocurrency.
Dogecoin was born at the end of 2013. Besides that the main difference between Dogecoin and other currencies is that it was born with the purpose of having fun with Cryptocurrency. In fact, Dogecoin supported many marketing campaigns and public events, which became popular in a very short term after its launch. For example- It sponsored a NASCAR driver with Dogecoin logo on his car. The technical difference between Dogecoin and other Cryptocurrencies was the notion of random block rewards, rather than having a fixed block reward. Each block bonus is random. It depends on a pseudo-random function with block hash technique. So, miners know about the reward before the block insertion. If the reward was low, they can switch to other Cryptocurrencies mining. But now Dogecoin block reward is fixed and halved every two months.

Fig 4: Symbol of Dogecoin[7]

Ethereum: It is the first smart contract cryptocurrency. Ethereum birth takes place at the beginning of 2013 and allows the creation of smart contracts in a Turing-complete programming language. A contract is something which can be fulfilled and can be applied when a series of conditions are met. The smart contract Cryptocurrencies are computer programs installed on the peer-to-peer network. In order to run, they have to "pay" the computational power required through a token, called Ether, which therefore acts both as cryptocurrency and contract fuel. There are many examples of contracts that are already running on Ethereum network. For example, electoral systems, registration of domain names, financial markets, crowd funding platforms, intellectual property and so on.

Fig 4: Symbol of Ethereum[7]

Monero: It is having a higher privacy level. Monero uses a ring signature algorithm. A signature is a combinations of many participants signatures. So, it is possible to link a transaction to a users of group, but not to trace it back to the user who actually made it. In addition, Monero is fungible and hence we can say that every coin is completely identical to every other coin in circulation.

Fig 4: Symbol of Monero[7]

Cardano: It is a first provable secure proof-of-stake algorithm. Cardano is a decentralized public blockchain which aims to protect user privacy. It is a third generation cryptocurrency born in 2015. Its roadmap is still evolving and obtained the major successes in the second half of 2017. At the beginning of 2018 it was entered in the top 5 Market Cap Cryptocurrencies. The main Cardano features are:

- high speed: low speed is a point of failure of most early born Cryptocurrencies
- money ownership: the user owns his money unlike in bank accounts where the bank owns them
- pseudonimity
- security
- extensibility: supports the side chain concept, allowing to create specific purpose Cryptocurrencies for a particular aim in which participants hold tokens that are valuable on the main chain. Examples of these applications are identity management, gaming and gambling, and verifiable computations.

The main differences with Bitcoin are:

- Mainly mining relies on the first provable secure proof of stake algorithm called "Ouroboros".
- presence of layers.
- The Cardano cryptocurrency depends on Settlement layer where the users can make exchanges and also has support to Control layer extension serving as a trusted computation framework. The aim is to evaluate that a certain computation was correct. In gaming and gambling those systems serve for verifying honesty of random number generation and game outcomes.

Fig 7: Symbol of Cardano[7]

Ripple: Ripple was born in 2012. It has aim to help the authorities and not to substitute them. Such that Banks and financial services companies can incorporate Ripple protocol into their own systems. As the Ripple team says, the aim is- "do for payments what SMTP did for email, which enables the systems of different financial institutions to communicate directly." According to the Ripple network it is possible to make payments in XRP (Ripple internal currency) or in fiat currency. XRP transactions rely on Ripples internal Distributed Ledger. But for other currencies or assets, the ledger records only the owned amount. To perform the exchange of other assets, users have to specify a list of trusted users and to what amount payment between two users that trust each other can take place directly according to the maximum threshold. Meanwhile, a payment between users who don't trust each other directly goes through a path created linking users who have a mutual trust relationship. This type of payments mechanism through a network of trusted associates is named 'Rippling'.

Fig 8: Symbol of Cardano[7]

The study of cryptocurrency technology and its network have been endowed with many superior features due to its unique architecture. The total market value has reached hundreds of billions of US dollars with some experts suggesting it would hit a USD 1 trillion valuation this year [8]. In addition, there are new Cryptocurrencies in various sectors reaching nearly trillion valued market. As an encrypted digital currency, Cryptocurrencies are operated in such a system which cannot be materialized, and the well structured records of the network satisfy the 5 V feature of Big Data (volume, variety, velocity, veracity and value) [9]. On the other hand, technologies under Cryptocurrencies have proved its applicability to a wide range of subjects.

Considering the rapid development of payment and transactions over the last decade, although it is still not certain to claim that Cryptocurrency will be the future currency, its significance and possible influences should not be underestimated. Online payments are now the preferred form of transaction than it was years ago, and payment intermediary platforms like PayPal have further enhanced the security and privacy protection for online payments. However, the use of cryptocurrency can overcome many drawbacks of the existing transaction system by incorporating the cryptography technique [10] The most important features of cryptocurrency are that: it uses decentralized control system(i.e., peer-peer)whose records are irreversible. At Present many researchers are working and seeking the determinants of Bitcoin and have investigated several factors across disciplines, for example, policy uncertainty [11], market forces [12], global uncertainty [13], cost of production [14], user characteristics [15], financial regulations [16], and financial stress [17].

Emmanuel Silva reviewed that-The significant impact of cryptocurrency is inseparably linked with the blockchain technology. Since every single record will be time stamped, saved and shared in a transparent database, this prevents overwriting and damaging to the maximum extent because of decentralization and has real-time peer-to-peer operation, anonymity, transparency, irreversibility and integrity in a widely applicable manner. However, there are still vulnerabilities and challenges related to this technology that should not be neglected [18]. One of the limitations is its performance. Here the verification of every transaction

requires the acknowledgement of every node in the network, which substantially will take more time than the centralized system.

Researchers have been investigating on the solutions of overcoming its limitations and further improving this technology, we have found relatively new progressions like Tangle and Hash graph technologies that can substantially improve efficiency and reduce costs. At present there is no clear information in terms of full adaptation and the relevant processes for the adoption of cryptocurrency as mainstream currency or the adoption of the blockchain technology behind it [19]. There are still many potentials that remain untackled and are certainly worth exploring as future research.

IV. CONCLUSION

The study of the paper introduces the growth of Cryptocurrencies using blockchain technology. It provides the efficient decentralized peer to peer transaction system while retaining anonymity and privacy. Researchers have been investigating on the solutions of overcoming its limitations and for further improvement of this technology. In regard to the Cryptocurrency, we have reviewed the relevant developments in terms of security and privacy enhancements. There are still many potentials that remain untackled and are certainly worth exploring for future research. Instantly, the transaction records are not fully exploited, mainly due to the lack of usability of application programming interface. To understand where the current research on Cryptocurrency using Blockchain technology positions itself, we decided to map all relevant research by using the systematic mapping study process . We extracted and analyzed 13 primary papers from scientific databases.

Author Contributions: All authors have equally contributed substantially to the work reported.

REFERENCES

[1]. https://enterslice.com/learning/cryptocurrencies-challenges-india

[2]. S. Manski, "Building the blockchain world: Technological commonwealth or just more of the same?" Strategic Change, vol. 26, no. 5, 2017, pp. 511-522.

[3]. https://imarticus.org/the-scpe-of-cryptocurrency-technology-in-india/

[4]. https://www.dqindia.com/scope-of-adopting-bitcoin-in-indian-market/

[5]. https://en.bitcoin.it/wiki/Bitcoin_symbol

[6]. https://www.quora.com/What-is-the-scope-of-cryptocurrency-in-India-and-what-are-its-legal-consequences

[7]. http://learningspot.altervista.org/altcoins-history-and-main-features-and-differences-from-bitcoin/altcoin_history/

[8]. Browne, R.; Kharpal, A. Cryptocurrency Market Will Hit $1 Trillion Valuation This Year, CEO of Top Exchange Says. 2018. Available online: https://www.cnbc.com/2018/02/13/cryptocurrency-market-to-hit1-trillion-valuation-in-2018-kraken-ceo.html (accessed on 30 August 2018)

[9]. Wamba, S.F.; Akter, S.; Edwards, A.; Chopin, G.; Gnanzou, D. How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study. Int. J. Prod. Econ. 2015, 165, 234–246. [CrossRef]

[10]. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutor. 2016, 18, 2084–2123. [CrossRef]

[11]. Demir, E.; Gozgor, G.; Lau, C.K.M.; Vigne, S.A. Does economic policy uncertainty predict the Bitcoin returns? An empirical investigation. Financ. Res. Lett. 2018, 26, 145–149. [CrossRef]

[12]. Ciaian, P.; Rajcaniova, M.; Kancs, D.A. The economics of BitCoin price formation. Appl. Econ. 2016, 48, 1799–1815. [CrossRef]

[13]. Bouri, E.; Gupta, R.; Tiwari, A.K.; Roubaud, D. Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions. Financ. Res. Lett. 2017, 23, 87–95. [CrossRef]

[14]. Hayes, A.S. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. Telemat. Inf. 2017, 34, 1308–1321. [CrossRef]

[15]. Yelowitz, A.; Wilson, M. Characteristics of Bitcoin users: An analysis of Google search data. Appl. Econ. Lett. 2015, 22, 1030–1036. [CrossRef]

[16]. Pieters, G.; Vivanco, S. Financial regulations and price inconsistencies across Bitcoin markets. Inf. Econ. Policy 2017, 39, 1–14. [CrossRef]

[17]. Bouri, E.; Gupta, R.; Lau, C.K.M.; Roubaud, D.; Wang, S. Bitcoin and global financial stress: A copula-based approach to dependence and causality in the quantiles. Q. Rev. Econ. Financ. 2018, 69, 297–307. [CrossRef]

[18]. Berke, A. How Safe Are Blockchains? It Depends. Harvard Business Review. 2017. Available online: https://hbr.org/2017/03/how-safe-are-blockchains-it-depends (accessed on 30 August 2018)

[19]. Mendling, J.; Weber, I.; Aalst, W.V.D.; Brocke, J.V.; Cabanillas, C.; Daniel, F.; Debois, S.; Di Ciccio, C.; Dumas, M.; Gal, A.; et al. Blockchains for business process management-challenges and opportunities. ACM Trans. Manag. Inf. Syst. 2018, 9. [CrossRef] 63. Kikten

