Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2616-2624
Received 25 April 2021; Accepted 08 May 2021.

Cryptocurrency and Blockchain: A Comparative Study and Analysis

B. Naga Sudheer[1], Ch. Praneeth[2], K. Sarada[3], P. Radha Madhavi[4]

[1]Asst.Professor, Department of IT, Vignan's Foundation for Science, Technology & Research (Deemed to be University), Vadlamudi, Guntur, Andhra Pradesh, India. sudheer.bandlamudi44@gmail.com

[2]Asst.Professor, Department of IT, Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India. chpraneeth@hotmail.com

[3]Asst.Professor, Department of IT, Vignan's Foundation for Science, Technology & Research (Deemed to be University), Vadlamudi, Guntur, Andhra Pradesh, India. Saradakorrapati2009@gmail.com

[4]Department of IT, Vignan's Foundation for Science, Technology & Research (Deemed to be University), Vadlamudi, Guntur, Andhra Pradesh, India. radhansuresh@gmail.com

Abstract: When we look at our history, we people used “commodity currency.” Later Fiat currency was introduced as an alternative to this commodity currency and now, it is most leading form of currency. But this is not the end of economic history as they introduced Cryptocurrency. Cryptocurrency is neither commodity currency nor fiat currency but an experimental kind of currency. In recent years emerged lots of cryptocurrencies, starting from the most standard “Bitcoin” to the latest “Libra (Diem)”. In this paper we studied what cryptocurrency is and various policy makers, basic aspects of cryptocurrencies followed by characteristics and factors effecting the price of cryptocurrency. The main idea of cryptocurrency analysis is to provide an overall information about several cryptocurrency and helps focusing on the use of cryptocurrency in various fields.

Keywords: Cryptocurrency, Block chain, Bitcoin, Correlation, Smart Contracts, Master Nodes, Digital Currency, Virtual Currency, Wallet, Ledger, Cryptography, Policy Makers, Digital Signature, Public key and Private key.

1. Introduction

Creating a description for cryptocurrency is certainly not an easy job. The word “cryptocurrency” has grown into a “popular saying” to talk about that make use of a method identified as “cryptography”[1,2]. In modest expression, it is a practice of defending our data by changing into an indecipherable arrangement that can only be inferred by someone who owns a secret key. By using a resourceful structure of digital keys, cryptocurrencies are safeguarded. Now, we try to provide an appropriate description for cryptocurrency based on the analysis of the definitions and descriptions which are already developed by several concerned policy makers.

Policy Makers

1. **International Monetary Fund (IMF)** categorized cryptocurrency as digital assets and a digital depiction of price, distributed by secluded creators and denominated in their personal division of version.
2. **Bank for International Settlements (BIS)** recognized cryptocurrency as a digital currency with key features such as: They are digital assets of value based completely on supply and

demand factor which is very much alike to commodities such as gold and silver. Moreover, these do not functioned by any precise person or association.

3. **World Bank** defined cryptocurrency as a digital currency which is dependent on cryptographic practices to accomplish unanimity.
4. **Financial Action Task Force (FATF)** categorized cryptocurrency as a digital currency that can be virtually traded for real currency.

The core decision drawn from various standpoints: there is not any commonly acknowledged description for the word cryptocurrency. Most of them slant cryptocurrency with subclass or a practice of digital and virtual currency.

2. Cryptocurrency

As distinguished above, cryptocurrency can be treated as a money for electronic payment system. In common, the payment systems make use of the public ledgers to create an incognito account name which is known to whole network. A transaction ensues after two parties agree to transfer cryptocurrency from one incognito account to other starts with the purchasing person unlocking the payment by using their own private key, consenting the trading person uses their private key to lock it. In order to enter the cryptocurrency system, consumers should have a wallet with a cryptocurrency service provider[18,19,20]. This process is similar to approving a payment through online website that entails to enter an ID and passcode. Cryptocurrency platforms often use Block chain technology to validate changes to the public ledgers.

3. Block chain

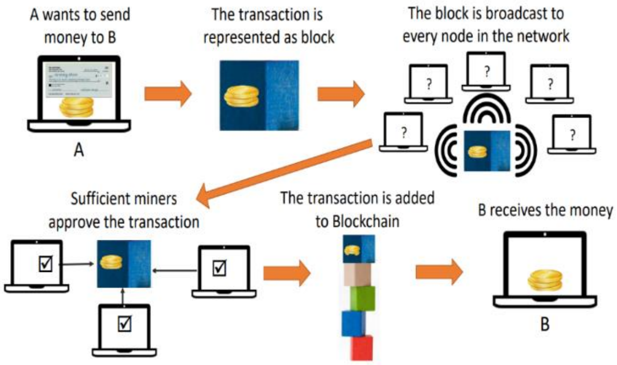
Block chain, which is a definite style of Distributed Ledger Technology (DLT) to store and allocate information across several public ledgers that are having same information which are mutually maintained and organized with the help of computer servers called nodes. These digital ledgers are executed without a fundamental repository and authority such as a bank, business, organization or government. At elementary level, with the group of community users they record the transactions information in a public shared ledger. In 2008, the concept of block chain technique was pooled with numerous additional methods and concepts to craft a contemporary cryptocurrency which are safe using these cryptographic techniques as a replacement for single controlling power. The initial cryptocurrency which is based on this block chain concept was Bitcoin.

Block chain is often defined with the term distributed-database[3]. We can add any Add-ons on this distributed-database by any person who generates a new “block” of information for holding all kinds of data. Then this newly generated block is publicized to everyone over the network as encoded format as any details regarding any transaction are not made available to the public. All the members in the network control the block’s validity by making use of a method algorithmic validation which is called with a name “consensus mechanism”. After the block validation, it is added to the block chain[5,6,7]. This results in updating the transaction ledger which is available

Received 25 April 2021; Accepted 08 May 2021.

over the entire network. The same mechanism can be used for any transaction that can be characterized in a digital format[11-14].

Every block is assigned with a digital signature by making use of a unique private key. Every user on this network has 2 keys. A public key is used as an address over block chain network and also used in the process of digital signature verification. A private key is used for creating a digital signature and a public key that is known to everybody over the block chain network. These both keys can be saved in a digital or e-wallet.


A wants to send money to B
A
The transaction is represented as block
The block is broadcast to every node in the network
?
Sufficient miners approve the transaction
The transaction is added to Blockchain
B receives the money
B

The core benefits of blockchain technique is simplification of any transaction execution that requires the involvement of a third party.

4. Cataloging Cryptocurrency

From 2017, the cryptocurrency market has risen steeply. Currently, there are numerous hundreds of coins in circulation and lot more continue to come in the future[4]. In order to understand and study the cryptocurrency market, we decided to analyze the basic assets of popular cryptocurrency.

The below mentioned study about cryptocurrencies are founded exclusively on the data accessible to public over internet.

Name	Market Cap	Circulating Supply	Price
Bitcoin	$911,167,346,274	18,710,662 BTC	$48,697.76
Ethereum	$449,937,562,690	115,882,346 ETH	$3,882.71
Litecoin	$20,776,757,531	66,752,415 LTC	$311.25
Monero	$7,634,509,301	17,909,861 XMR	$426.27
Dash	$3,575,285,832	10,131,651 DASH	$352.88

Zcash	$3,447,557,589	11,773,844 ZEC	$292.81
XRP	$47,379,438,928	35,108,326,973 XRP *	$1.35
Ethereum Classic	$11,887,969,801	116,313,299 ETC	$102.21
Decred	$2,458,432,979	12,927,455 DCR	$190.17
TRON	$8,658,504,537	71,659,657,369 TRX *	$0.1208

Table 1: Overview of Cryptocurrency (Up to May 2020)

1. **Bitcoin:** It was invented by an unidentified individual or a community of people using the name Satoshi Nakamoto which was started in 2009. This Bitcoin is a distributed digital currency without a sole proprietor which can be sent from one user to another user over bitcoin network. All the transactions are certified by the nodes and these transactions are recorded in a public ledger called a blockchain[8,9,10]. The major advantage of these bitcoins is that we cannot detect, trail or capture bitcoin transactions. There are no added taxes on any kind of purchases.
2. **Ethereum:** It is a universal, devolved policy for currency and different types of solicitations. Here, we have a flexibility of writing code which can controls money, and also to build various applications available everywhere over the world. It helps you to construct smart contracts and devolved applications without any interruption or any third-party intrusion. The major features of ethereum as it allows to upload and request programs to be executed, helps us to develop devolved applications which results in building effective organizations.
3. **Litecoin:** It functions in one logic as an online recompense system. Like PayPal or a bank's online network, we can use for transferring money to one another. This litecoin conducts transactions in units of litecoin. These are quicker handling and authorization of transactions. All the transaction costs are way lesser and adaptable. It has smaller competition in the mining as well as greater profit margin. Litecoin is very malleable meaning that we can simply buy it using other Cryptocurrencies like the Bitcoins or can be well-suited with maximum exchange platforms.
4. **Monero:** It is an open-source cryptocurrency that emphases based on the fungibility and privacy. It uses a clouded open ledger where everyone can broadcast or lead transactions, but no outside spectator can tell the basis, quantity or target. All Monero transactions are private and undetectable. It is an electronic money that permits fast, low-priced payments to and from everywhere in the world. Monero has no “pre-set” size bound which means malevolent miners can obstruct the system with excessively huge blocks. To preclude this, a block reward penalty is built into the system.

5. **Dash:** It is a digital currency that can be used to send or receive payments. It offers enhanced privacy and sophisticated transaction speed with the help of a distinctive model "Master nodes". These Master nodes act as exceptional servers that execute the acute functions on the Dash crypto network which are in control of Private Transactions. In this, master nodes controls all private transactions. Dash has a Private Send – a really unique feature that allows us to send funds confidentially by mingling it in between numerous additional transactions making it tough to detect any detailed transaction.
6. **Zcash**: It is a cryptocurrency that makes use of cryptography to provide boosted seclusion for its users compared to other cryptocurrencies. It uses a concept called zero-knowledge proofs that assurances the legality of any transaction which does not reveal any of the sender's or recipient information. It can be stored using the approved Zcash wallet that comes in both the mobile application and desktop forms.
7. **XRP:** It is the élite enterprise blockchain resolution in the domain for worldwide payments. Ripple is a policy for a universal system of payments, expenditures, and exchange which is normally acknowledged for the digital payment procedure[18]. Ripple transactions practice a smaller amount of energy when compared with Bitcoin and costs less.
8. **Ethereum Classic:** It was developed as a riven version of the Ethereum Blockchain that runs smart contracts. It mainly targets to resolve the similar issues as Ethereum such as transaction finality and solicitations which run precisely scheduled not having any chance of deception and also any intrusion of third party.
9. **Decred:** It is an open-focused cryptocurrency intended to provide a truthfully devolved, reasonable, and dominant substitute to customary currency. With Decred, the community associates control the structure, sort the rules, and regulate the course of the scheme. In this, cross-platform wallets are accessible. Both miners and users have the equivalent extent of power over the system. Based on the changes in the blockchain technology, it is easy to add or remove a feature.
10. **Tron:** It is a blockchain-built distributed policy that targets to build an open, universal digital structure with distributed storing expertise, and permits laidback and cost-effective distribution of digital content. It has no middle distributers. The creators can have profits right from their customers and clients. It enables involvement of content to foremost service benefactors like Facebook, YouTube and so on as the content initiator, which lets one have overall authority over one's specific data, wherein others will be recompensed for their specific content.

Even though some cryptocurrency are similar when compared with one another, there are various discrepancy about the way they designed, the technology they are using, the privacy included and many more. The below table aims to elucidate this miscellany[17]. The designated cryptocurrencies are related and compared on the base of numerous parameters: on what technology and algorithms they are associated with, their distributed nature, any mining rewards, and average block size, block time and transaction fee. The below table replicates our considerate information of the designated cryptocurrency. It should identify about the fact that analyzing strong and clear discrepancies amongst cryptocurrency is not an easy job.

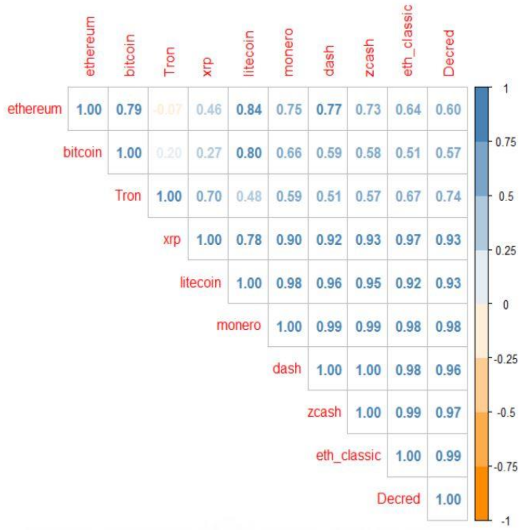
Additionally, these cryptocurrency are a moving objective. These cryptocurrencies are not an intermediate of exchange now and can be one tomorrow. As a result, the indication does not only aim at depicting or categorizing the designated cryptocurrency. Possibly, to get a categorically strong depiction of cryptocurrency and all their diverse features in observation of giving the preeminent advice, needs more work to be done and additional study is necessary. However, for the resolutions of this study, we are of the opinion that the table organized below is an effective instrument, consenting to draw approximately few best conclusions based on this supervisory analysis.

Name	Algorithm	Mining Reward	Average Block Size	Average Block Time	Average Transaction fee
Bitcoin	SHA-256 hash	Yes	1.316 MB	at least 10 minutes	$ 13.84USD
Ethereum	Keccak-256	Yes	57096.00KB	10s -15s	$5.70 USD
Litecoin	Scrypt	Yes	18KB	2.5 minutes	$0.067 USD
Monero	RandomX	Yes	74.677 KB	2 minutes	$0.094 USD
Dash	X11 algorithm	Yes	39.543 KB	2.5 minutes	$0.2 - $0.3
Zcash	SHA256 compression	Yes	8.482 KB	1m 15s	0 USD
XRP	Ripple Proof of Correctness Algori thm (RPCA)	Yes	doesn't use blockchain	NA	0.00001 XRP
Ethereum Classic	Keccak256	Yes	1.975 KB	13s	$0.021 USD
Decred	Blake-256 hashing algorithm	Yes	393KB	5 minutes	No Fee
TRON	Lamport algorithm	Yes	1MB	3s – 10s	No Fee

Table 2: Overview of various Cryptocurrency parameters (Up to May 2020)

5. Analysis

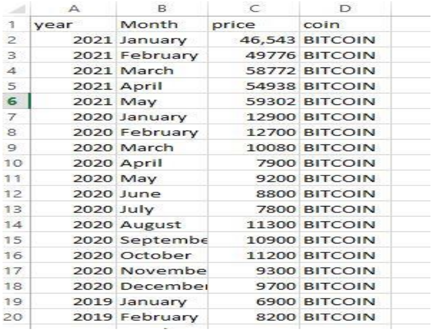
Correlation is a measure p between two quantitative variables. For this analysis, cryptocurrency from the last five years based on the info itinfocharts.



	ethereum	bitcoin	Tron	xrp	litecoin	monero	dash	zcash	eth_classic	Decred
ethereum	1.00	0.79	-0.07	0.46	0.84	0.75	0.77	0.73	0.64	0.60
bitcoin		1.00	0.20	0.27	0.80	0.66	0.59	0.58	0.51	0.57
Tron			1.00	0.70	0.48	0.59	0.51	0.57	0.67	0.74
xrp				1.00	0.78	0.90	0.92	0.93	0.97	0.93
litecoin					1.00	0.98	0.96	0.95	0.92	0.93
monero						1.00	0.99	0.99	0.98	0.98
dash							1.00	1.00	0.98	0.96
zcash								1.00	0.99	0.97
eth_classic									1.00	0.99
Decred										1.00

Figure 1: cryptocurrency dataset

Based on the above collected and organized dataset, we derived the correlation as follow:



	A	B	C	D
1	year	Month	price	coin
2	2021	January	46,543	BITCOIN
3	2021	February	49776	BITCOIN
4	2021	March	58772	BITCOIN
5	2021	April	54938	BITCOIN
6	2021	May	59302	BITCOIN
7	2020	January	12900	BITCOIN
8	2020	February	12700	BITCOIN
9	2020	March	10080	BITCOIN
10	2020	April	7900	BITCOIN
11	2020	May	9200	BITCOIN
12	2020	June	8800	BITCOIN
13	2020	July	7800	BITCOIN
14	2020	August	11300	BITCOIN
15	2020	Septembe	10900	BITCOIN
16	2020	October	11200	BITCOIN
17	2020	Novembe	9300	BITCOIN
18	2020	Decembei	9700	BITCOIN
19	2019	January	6900	BITCOIN
20	2019	February	8200	BITCOIN

Figure 2: Correlation table

From the above correlation table of various cryptocurrency we observe:

1. Litecoin is strongly correlated with Ethereum followed by bitcoin[15].

2. XRP and Tron are less likely correlated with bitcoin.

3. XRP is strongly correlated with Ethereum classic.

4. Litecoin is very strongly correlated with Monero.

5. Dash is very strongly correlated with ZCash and followed by Ethereum Classic.

6. Conclusion

Cryptocurrency definitely is the future for all the currencies. They runs on Block chain technology which makes them easy to monitor and also tamper proof with very fast transaction process. As trades, it is important to recognize and understand how fast this cryptocurrency is growing. All the laws and existing economic structure may change overnight. These cryptocurrencies are a very hot area in the worldwide business and economic system. Their advancement gained a massive attention of many opportunists. They are easily portable. If the cryptocurrency failed to attain the trust, then their future might drop. A various types of cryptocurrency gained the massive attention. Nearly many countries already started to issue national cryptocurrency. It is also very much possible that bitcoins might provide a better way for other various cryptocurrency to flourish in the future. Regardless of the blemishes, bitcoins are still considered as an accomplishment that has been achieved with abundant expertise in the digital currency. It has provided a substitute currency for the less advanced countries and has unlocked the accesses of economic revolution. The cryptocurrency are entering into the financial stage and varying the worldwide financial landscape.

References

1. BRATSPIES, R.M., "Cryptocurrencies and the Myth of the Trustless Transaction", March 2018, 49p.
2. BRITO, J., SHADAB, H., and CASTILLO, A., "Bitcoin financial regulation: securities, derivatives, prediction markets & gambling", 24 July 2014, 78p.
3. BUCHKO, S., “How Long do Bitcoin Transactions Take?”, December 2017, https://coincentral.com/how-long-do-bitcoin-transfers-take/
4. CPMI, “Digital currencies”, November 2015, https://www.bis.org/cpmi/publ/d137.pdf, 21p.
5. CPMI, “Distributed ledger technology in payment, clearing and settlement – An analytical framework”, February 2017, https://www.bis.org/cpmi/publ/d157.pdf, 23p
6. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf
7. Ramesh, A., “Features of various Blockchains: A Comparison”, February2018, https://www.xoken.org/blog/ features -of-various-blockchains-a-comparison/
8. https://bitinfocharts.com
9. https://bitcoin.org
10. https://bitcoin.org/bitcoin.pdf

11. https://coinmarketcap.com/charts/.
12. https://coinmarketcap.com/coins/views/all/.
13. https://cryptocoincharts.info/markets/info.
14. https://cryptocurrencyfacts.com/asic-mining-basics/.
15. https://litecoin.com.
16. https://ripple.com
17. Lokaiah Pullagura, P Ratnababu, A Complex Integrated Approach of Blockchain With Bigdata For Secure Scientific Data Sharing, Jul2020, Vol. 12 Issue 2, p33 -43. 11p.
18. Mandal, K., & Ghantasala, G. P. (2019). A complete survey on technological challenges of iot in security and privacy. *Int. J. Recent Technol. Eng.*, *7*(6S4), 332-334.
19. Kumari, N. V., Ghantasala, G. P., & Arvindhan, M. (2020). 4 Compulsion for Cyber. *Securing IoT and Big Data: Next Generation Intelligence*, 59.
20. G S Pradeep Ghantasala,Dr.N.Krishna Raj,Chaitali Bhowmik, Cryptocurrency miners - Major Cyber Threat of 2018, International Journal of Pure and Applied Mathematics, Volume 119 No. 18 2018, 1775-1788