Comparative Analysis of Cryptocurrencies

by Aditi D Anchan

Submission date: 07-Dec-2021 04:07PM (UTC+0530)
Submission ID: 1723278655
File name: Cryptography.pdf (627.98K)
Word count: 3268
Character count: 17043

Comparative Analysis of Cryptocurrencies

By

Aditi D Anchan

PES1UG19CS030

Suhas RK

PES1UG19CS514

Ankith Rai

PES1UG19CS069

INTRODUCTION

Cryptocurrency is a form of digital currency it is a more secure way of transaction as it hides the identity of the user. Cryptocurrency is crypto - currency , where crypto is a short form for cryptography. Cryptography is the study of securing data by using technologies so that data won't be corrupted or misused . In cryptography various cryptographic algorithms are used to encrypt and decrypt messages . Cryptography is a subdivision of cryptology which has two types cryptography and cryptanalysis ,cryptanalysis is the study of breaking a given ciphertext . Cryptography is a growing field as threats to data and attacks on systems are increasing potentially .

The first cryptocurrency was developed in the year 2008. This was developed at the time when there was a huge financial crisis .The first ever cryptocurrency to be generated was bitcoin.
Cryptocurrencies are known to be more reliable than normal currencies today , as they are cheaper and faster for transactions . Cryptocurrencies are independent payment methods without third party interference . One of the good things about using cryptocurrency over a non digital currency is that every user who uses a cryptocurrency can verify and record their transaction , to avoid fraud and to maintain integrity . Cryptocurrencies have faced a lot of popularity and growth in recent years . Cryptocurrency follows a decentralized structure which means that each person's currency is not in the authority or bounds of the government . It has several advantages due to its decentralized nature , in normal bank transfer an additional transfer charge will be added , however in these digital currencies those charges are almost zero in fact people need not have a bank account for transferring these digital currencies.
Cryptocurrencies, unlike normal currency, are generated in a fixed amount and cannot be regenerated every time this however does not devalue the currency .

The decentralized nature of the cryptocurrency is handled by a system called blockchain.Blockchain is a public transaction database . It is a distributed database.It uses a supporting software and it does not need any intermediate party , it maintains a history of all transactions of the currency by using a set of blocks ,this is based on the concept of blockchain.
They are built in a very secure manner and they are immune to hacking activity. But still some aspects of cryptocurrency are immune to hacking.So every user can see all the transactions of the currency he has that has been made in the past. Database and blockchain are differentiated based on how they are structured . Databases are usually stored in the form of tables , whereas blockchain as the name suggests , stores the data in the form of a block . Once a block reaches its maximum capacity it is closed and linked to the previous blocks , so blockchain can also be defined as a set of blocks linked to each other , each containing some form of data.
Now if we talk about the disadvantages of cryptocurrency, The partial-anonymity of cryptocurrency makes it easier to conduct money laundering and transactions involved in terrorists activities.As mentioned earlier, the partial-anonymity of bitcoin may also help in seizure of criminals by conducting forensic-analysis of the coins involved in transactions.But some coins like ZCash, Dash takes anonymity to next level. Even the forensic analysis of these coins will maintain confidentiality.All the cryptocurrencies are virtual and balance related to these cryptocurrency that one has is only maintained in hard drives. If the backup of that hard drive is not maintained, then data related to cryptocurrency will be lost forever. Also no central government and private sectors have access to the personal information of cryptocurrency holders.

authenticated he/she can then be allowed to make public transactions.

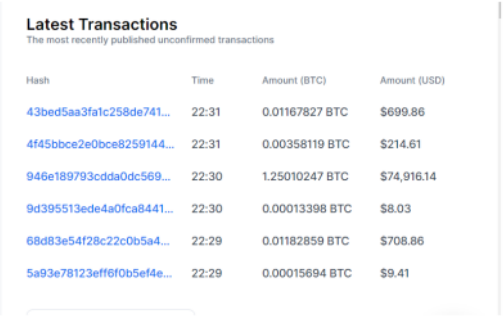
TYPES OF CRYPTOCURRENCIES

Bitcoin

Bitcoin was the first cryptocurrency to be invented in the year 2008,it is based on public key cryptography and began use in 2009 . It is a decentralized digital currency. .It follows a peer to peer transaction process , where there is no third party involvement . Bitcoins were created to reward the miners . Bitcoins do not have a central authority, they do not have a central server unlike normal currency .Bitcoin is ledger distributed,so it does not have a central storage . Bitcoin is the first digital currency to use blockchain. Bitcoin has made trading and transactions using cryptocurrency very popular . As bitcoin uses a blockchain platform it is very secure , it not only hides the identity of the user but also eliminates the slightest possibility of fraud .The bitcoin transactions are accessible to everyone ,so it is very difficult to reverse and fake.Bitcoin has gained popularity over the years , 12 years back when it was first created the value of bitcoin was around 11,170 rupees per coin as of now it's value is 46,15,807 rupees per coin . There are a total of 21 million bitcoins . Whenever there is an attack , the bitcoin users have the option of splitting to a new blockchain , so it requires a lot of effort for an attacker to achieve the attack , thus making it almost impossible to exploit bitcoins .

Bitcoins can be called as a balance of a bitcoin account , transactions of bitcoins happen through these accounts . Each bitcoin is identified by its bitcoin address . This address is generated by the public key. The bitcoin transactions that happen are using these bitcoin addresses ,the sender account or source address is known as input address and the receiver account or the destination address is known as output address . Transactions can have multiple input addresses as well as multiple output addresses.

Each sender must use a digital signature to authenticate his or her valid identity.Once the user is



Bitcoin transaction (source :blockchain.com)

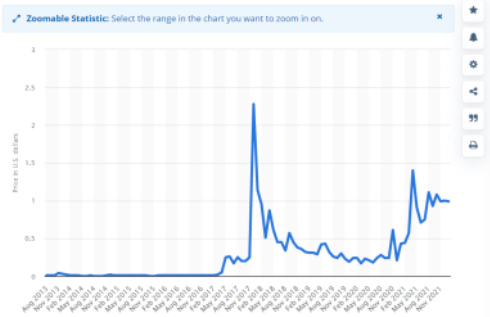
Ethereum

The concept of Etherium was developed by Vitalik Buterin. Ethereum has its own cryptocurrency known as ETH or Ether. This coin came out as an output because of his work and research on Bitcoin and the Bitcoin community. When Vitalik was working with Bitcoin,He found that Bitcoin was not solving the problems associated with cryptocurrency in the right way.The goal of any cryptocurrency is to replace the third parties for data storage and usage of third party services to keep track of complex financial transactions.The primary features of this coin is that they have programs which can execute themselves when some conditions are met.And they do not involve any third party assistance for this purpose and they are totally decentralized.And these functionality will be associated with this coin until they will be used for trading purposes.Ethereum now comes 2nd to bitcoin . The initial value of Ethereum when it was launched was 206 rupees , now it is

3,21,302 rupees . Like Bitcoins ,Ethereum has its corresponding account known as Ethereum account. Each account has a corresponding account address , which is used for transactions , this address is 20 byte long .

Ripple

Ripple was launched by Jed MC celeb , Christ Larsen and Aruthur Britto in 2012. This coin got its fame in recent years because of its growth in the first 6 years of its launch.The growth in its platform and its management has led them to be one of the biggest competitors of the crypto market. After having looked at the protocols used by Ripple , many companies, especially financial companies have adopted Ripple protocol.The ripple protool do not require any mining to verify the financial transaction it has done. Whereas Bitcoin uses mining for verifying its transactions. Since mining requires electricity and power for its working , as it requires computing power. We can reduce that in the case of Ripple transactions. Both bitcoin and ripple have similar characteristics . In this the currencies and transactions are verified by the members in the transaction network and not by the mining process unlike in bitcoin . XRP is the cryptocurrency token used by ripple networks for transactions . The nodes in ripple can be classified as gateway , Consensus Ledger and market makers . Gateway is the one which lets users take and put money into the ripple network . Ripple depends on a shared ledger which is distributed to everyone in the network . Market makers provide market liquidity . The current value of the XRP coin is around 71 rs



XRP coin value over the years (Source : statista.com)

Tether

This coin was launched by Bitcoin foundation director Brock Pierce with software engineer Criag kSellars and entrepreneur Reeve Collins.At first it was named as Real coin and later it was rebranded as Tether in 2014. Tether was initially launched to be stable having value of $1 that's why it is known as a stable cryptocurrency .

Litecoin

This coin is a peer to peer cryptocurrency created by charlie lee in 2011. It is also called LTC or silver to Bitcoin's gold. Technically it is very similar to bitcoin. Litecoin is not controlled by any central agency and it uses the 'scrypt' function as proof of work. Litecoin uses scrypt as its hashing function.It's transaction speed is high, transaction time is less , cost of transaction is not very expensive .The time taken to confirm the transaction of bitcoin is 4 times as that of litecoin. The number of litecoins produced will be more than bitcoins , as the limit of bitcoin is set to 21 million and limit of litecoin is set to around 84 million that is nearly 4 times the limit of litecoin , so litecoin will be cheaper compared to bitcoin . This makes it easy for access . Algorithms to create litecoins are very memory consuming . Litecoin value currently is 11,147.49 INR , back then when it was introduced the value was around 30 dollars cents .

Stellar

Stellar was founded by Jed McCaleb in 2014. It is an open blockchain network which provides connectivity between financial institutions for large transactions. Due to stellar now the transactions between the institutions happen instantaneously with no intermediaries. Stellar's native currency is LUMENS (XLM) and hence the network requires the users to have lumens in order to do transactions.The present value of stellar is coin is around 22 rs

COMPARATIVE STUDY OF CRYPTOCURRENCY

As we can see, the cryptocurrency family is becoming stronger and enriched with new cryptocurrency as days are passing. But if we have a close look at the market we can see that prominent coins have still managed to attract the attention of people and have established themselves in a very good manner. When we compare between the cryptocurrencies we can get to know that Bitcoin is the most established followed by etherium and others. Then if we look at the features of these coins we can see one common feature between them that is the fluctuations in their price.If we have a close look on the fluctuation on their price in last one and half years we can see that during March 2020, not only the crypto market but also all stock markets across world got crashed due to the attack of Deadly coronavirus and all coins took so long period to recover from the fall.

Variation in price of bitcoin from July-2021 to Nov-2021

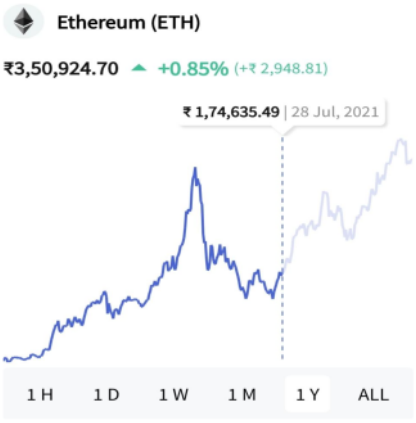
Month	July	Aug	Sept	Oct	Nov
Bitcoin	25,88,995	31,57,44	37,02,227	36,33,328	49,11,224

(source: www.coindcx.com)

As we can see from the price table there is no drastic change in price. But if we look at the price table from 2019, we can say that Bitcoin has gained a sharp spike in its price.And analysts also predict that both Bitcoin and Ethereum price will double at the end of the year. By the end of 2025 , analysts claim that Bitcoin will hit an all time high with price upto 280,00,000. And they claim that that year will also be called the Bitcoin year.

Variation of price of Ethereum from July-2021 to Nov-2021

Month	July	Aug	Sept	Oct	Nov
Ethereum	1,63,668	1,97,925	2,71,421	2,48,079	3,45,364



(source: www.coindcx.com)

Variation in price of Ripple from July-2021 to Nov-2021

Month	July	Aug	Sept	Oct	Nov
Ripple	50.41	75.08	106.28	92.14	98.15

(source: www.coindcx.com)

Variation in price of Tether from July-2021 to Nov-2021

Month	July	Aug	Sept	Oct	Nov
Tether	76.56	77.44	79.23	77.72	81.58

(source: www.coindcx.com)

Variation in price of Litecoin from July-2021 to Nov-2021

Month	July	Aug	Sept	Oct	Nov
Litecoin	10493.59	12928.69	17377.15	13630.50	21209.61

(source: www.coindcx.com)

Variation in price of Stellar from July-2021 to Nov-2021

Month	July	Aug	Sept	Oct	Nov
Stellar	17.21	21.09	31.74	26.25	30.80

(source: www.coindcx.com)

Characteristics comparisons of various Cryptocurrency

For comparison we will take four cryptocurrencies namely bitcoin,ethereum ,tether and ripple .

Transaction speed

Transaction speed tells how fast a crypto network can process a transaction . Many factors can affect the transaction speed for example if the number of transactions traffic is high then speed will be affected .The speed of bitcoin is around 10 mins per transaction . Bitcoin is one of the slowest cryptocurrency in the market .The reason for this is bitcoin has increased its block size , this in turn reduced its transaction speed . Also there are multiple attacks that can happen on bitcoins , congested traffic is one of the few reasons for slow transaction speed . Ethereum transaction speed is around 5 mins per transaction . Ethereum is faster compared to bitcoin but slower compared to other cryptocurrencies , the reasons behind this are similar to that of bitcoin's . Ripple's speed is 4 second per transaction , which is a very good speed . Tether transaction speed is around 6 mins per transaction.

Scalability

Scalability is the property of a coin to handle a large number of transactions in a limited amount of time . The scalability of bitcoin is around 7 transactions per second . The scalability of ethereum is more compared to , i.e it is capable of delivering two times the capacity of bitcoin , the scalability of ethereum is approximately 15 transactions per second . Ripple has a very high scalability around 1500 transactions per second , it beats both bitcoin and ethereum in terms of scalability and transaction speed .

Circulating supply

This tells the amount of cryptocurrencies that is generated and is getting circulated in the market . The amount of bitcoin around the world is currently around 17 million . There are a lot of ethereum coins present in the market right now , the number is nearly 102 million . Ripple's circulating supply count is greater than 40 billion beating ethereum , bitcoin and tether . Tether's is 7.8 billion

Block time

It is the time taken to produce new data or block .Each block stores the transaction details of the recent cryptocurrency . Block time of bitcoin is 10 minutes , ethereum is 15 seconds , for tether and ripple it is very less .

Maximum supply

This tells the approximation of the number of coins that will ever be created . Maximum supply of bitcoins is 21 million for ethereum there is no upper limit , for ripple it is 100 billion and it is 7.51 billion for tether .

Currency	Release Date	Founder	Symbol	Hash Function Used	Consensus Mechanism	Language Used For Implementation
Bitcoin	2009	Satoshi Nakamoto	BTC	SHA-256	POW(Proof Of Work)	C++
Ethereum	2015	Vitalik Buterin	ETH	Ethash	POW(Proof Of Work) , POS(Proof Of Stake)	C++ , Go
Ripple	2013	Chris Larsen & Jed McCaleb	XRP	ECDSA	Ripple Protocol Consensus Algorithm	C++
Tether	2015	Jan Ludovicus van der Velde	USDT	Omnicore	POW(Proof Of Work)	
Litecoin	2011	Charlie Lee	LTC	Scrypt	POW(Proof Of Work)	C++
Stellar	2014	Jed McCaleb	XLM	Stellar Consensus Model(SCP)	Stellar Consensus Model(SCP)	C , C++

Comparison table for various coins

REFERENCES :

[1]Vitalik Buterin https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[2] Jordi Herrera-Joancomartí https://www.researchgate.net/publication/281773799_Research_and_Challenges_on_Bitcoin_Anonymity

[3] Shainik Jani https://www.researchgate.net/publication/322436263_An_Overview_of_Ripple_Technology_its_Comparison_with_Bitcoin_Technology

[4] S. Nakamoto, ""“Bitcoin: A Peer-to-Peer Electronic Cash System”," www.bitcoin.org, 2008.

[5] S. Jani, "Scope for Bitcoins in India," December 2017. [Online]. Available: www.researchgate.net/publication/321780780_Scope_for_ Bitcoins_in_India.

[6] A. M. &. E. F. Joseph Bonneau, "Research Perspectives and Challenges for Bitcoins and Cryptocurrencies," IEEE Symposium on Security and Privacy, May, 2015

[7] N. Y. a. A. B. David Schwartz, "The Ripple Protocol Consensus Algorithm," 2014. [Online]. Available:www.ripple.com/files/ripple_consensus_whiteepaper.pdf

[8] . Reid, F., Harrigan, M.: An analysis of anonymity in the bitcoin system. In Altshuler, Y., Elovici, Y., Cremers, A.B., Aharony, N., Pentland, A., eds.: Security and Privacy in Social Networks. Springer New York (2013) 197–223

[9] Babaioff, M., Dobzinski, S., Oren, S., Zohar, A.: On bitcoin and red balloons. In: Proceedings of the 13th Association for Computing Machinery (ACM) Conference on Electronic Commerce. EC ’12, New York, NY, USA, ACM (2012) 56–73

[10] Donet, J.A., P´erez-Sola, C., Herrera-Joancomart´ı, J.: The bitcoin P2P network. In B¨ohme, R., Brenner, M., Moore, T., Smith, M., eds.: Financial Cryptography and Data Security. Volume 8438 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2014) 87–102

[11]Baumann, A., Fabian, B., and Lischke, M. (2014). “Exploring the Bitcoin Network,” in *WEBIST*, 369–374.

[12] Resta, M., Pagnottoni, P., and De Giuli, M. E. (2020). Technical Analysis on the Bitcoin Market: Trading Opportunities or Investors' Pitfall? Risks 8, 44. doi:10.3390/risks8020044

[13] Brugere, I (2013): Bitcoin Transaction Network Extraction. https://github.com/ivan-brugere/BitcoinTransaction-Network-Extraction. (Access Dec 2013).

[14] Dotson, K (2012): Paypal’s Abandonment of Major Cyberlockers May Become Bitcoin’s Big Win. http://siliconangle.com/blog/2012/07/11/paypalsabandonment-of-major-cyberlockers-may-becomebitcoins-big-win/. (Access Dec 2013)

[15] Drainville, D (2012): An Analysis of the Bitcoin Electronic Cash System. https://math.uwaterloo.ca/combinatorics-and-optimization/sites/ca.combinatorics-and-optimization/files/uploads/files/Drainville, Danielle.pdf. (Access Dec 2013).

[16] Reid, F; Harrigan, M (2013): An Analysis of Anonymity in the Bitcoin System. In: Security and Privacy in Social Networks, Springer: 197-223. arXiv:1107.4524v2 [physics.soc-ph]

[17] Ron, D; Shamir, A (2013): Quantitative Analysis of the Full Bitcoin Transaction Graph. Lecture Notes in Computer Science 7859: 6-24

[18] Evans, Jon (20 August 2018). "What the hell is the deal with Tether?". TechCrunch. Archived from the original on 19 August 2018. Retrieved 20 August 2018.

[19] Shaban, Hamza (14 June 2018). "Bitcoin's astronomical rise last year was buoyed by market manipulation, researchers say". *Washington Post*. Archived from the original on 15 June 2018. Retrieved 14 June 2018

[20] Samson, Adam (23 February 2021). "Tether and Bitfinex agree to pay $18.5m penalty after New York probe". *Financial Times*. Archived from the original on 23 February 2021. Retrieved 23 February 2021.

[21] Maxwell, G.: Coinjoin: Bitcoin privacy for the real world. post on bitcoin forum https://bitcointalk.org/index.php?topic=279249.

[22] Bissias, G., Ozisik, A.P., Levine, B.N., Liberatore, M.: Sybil-resistant mixing for bitcoin. In: Proceedings of the 13th ACM Workshop on Workshop on Privacy in the Electronic Society. WPES '14, New York, NY, USA, ACM (2014)

[23] Wallace, B.: The Rise and Fall of Bitcoin, Wired Magazine, 23 November 2011, http://www.wired.com/magazine/2011/11/mf_bitcoin/all/

[24] Brett, W.: Senators seek crackdown on "Bitcoin" currency,Reuters, 8 Jun 2011, http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608

[25] Reid, F., Harrigan M.: An Analysis of Anonymity in the Bitcoin System, arXiv:1107.4524v2 [physics.soc-ph] 7 May 2012.

[26] Bitcoin's block number 0, http://blockexplorer.com/b/0

[27] Bitcoin's block number 180,000, http://blockexplorer.com/b/180000

[28] Forbes: Top 10 Bitcoin Statistics, http://www.forbes.com/sites/jonmatonis/2012/07/31/top-10-bitcoin-statistics/

[29] Watts, D; Strogatz, S (1998): Collective Dynamics of Small-World Networks, Nature, Vol. 393, June 1998: 440-442.

[30] Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better - how to make bitcoin a better currency. In Keromytis, A., ed.: Financial Cryptography and Data Security. Volume 7397 of Lecture Notes in Computer Science. Springer Berlin Heidelberg (2012) 399–414

Comparative Analysis of Cryptocurrencies

ORIGINALITY REPORT

4%	3%	3%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.investopedia.com Internet Source	1%
2	inechain.com Internet Source	1%
3	"Blockchain and Trustworthy Systems", Springer Science and Business Media LLC, 2021 Publication	1%
4	crypsys.mmci.uni-saarland.de Internet Source	1%
5	Michael H. Tunick. "Minerals", Elsevier BV, 2022 Publication	<1%
6	www.mdpi.com Internet Source	<1%
7	scitepress.org Internet Source	<1%
8	Lecture Notes in Computer Science, 2015. Publication	<1%

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		