HOW DO CRYPTOCURRENCIES AND BLOCKCHAIN TECHNOLOGY WORK?

Abstract

Cryptocurrencies are a recent trend when it comes to transactions, though its introduction dates far back to 2009. They are rising to the standards of efficient transaction medium and offer advancements that could potentially revolutionize the whole economic system. While the reason for the sudden hype that emerged for these in the field of marketing, business etc. continues to remain uncertain, Blockchain technology which is the technological algorithm under which these cryptocurrencies function, with its exceptional and unusual approach towards logical structuring of secure layouts contributes in the attempt of finding the answer. It has provided with an algorithm that no present technology can practically hack into! But how far is the scope of the word ‘present’ from the prior sentence? Especially with the galloping advancements in technology, will it still beat the odds and attain what it was able to achieve only to the current extent? The answers to these questions have the potential to determine the scope of cryptocurrencies in future. This paper attempts to find these answers.

Objective

This paper intends to help understand the working of blockchain technology in employing cryptocurrencies as a medium of exchange and in turn gaining knowledge on the emerging concept of cryptocurrency itself. It starts with the circumstances which led to the development of cryptocurrencies and the sense of security it attempts to attain. It seeks to do so by taking into account various facts and speculations made by investors in this field.

Keywords: Cryptocurrency, Blockchain, ledger, Cryptocurrency mining, Hash, Nonce.

Author

Nivethitha M
BCA LLB (Hons.) – 1st year
School Of Excellence in Law
The Tamil Nadu Dr. Ambedkar Law University
Chennai, India.

I. INTRODUCTION

It has been hundreds of thousands of years since human beings stepped foot on this planet. It is an undeniable fact that evolution in humans has taken hold of all aspects of life right from food habits to clothing, from language to labour and what not. But if there is one thing that retained its essence in spite of these transformations, it is trade and commerce. It underwent its share of changes but they were mere reflection of advancements in the domain but the core concept, that is, people in need of something exchanges it with someone who has and is willing to sell the thing in return for something else, remains unaltered.

Initially, there was a barter system being followed. In this concept, a person in need of a commodity exchanges it with a person possessing the commodity and is willing to exchange it for another commodity that the other person is offering. This posed difficulties as the ration of good that needs to be exchanged for a given quantity of another good was very uncertain and often led to confusion. It is also worthy to mention that the person who has the commodity that the potential buyer is willing to purchase is often not willing to sell it in exchange for the thing that the buyer is offering and so barter system requires you to find a person who is willing to do both which is practically a tiring hunt.

This setting was slowly replaced by Coin system, where commodities were exchanged for coins made of precious metals. These were accepted, as metals hold value in itself and so people need not go around searching for a person in need of coins in exchange for the good they need, since these coins can be used as medium to initiate a second trade and so on. This made people to accept coin as a medium of exchange. But people can still deny to accept coins since there is no necessity or obligation for the seller to accept it. Also, precious metals have more valuable uses than being a symbol of assurance and so the need for substitutes arose.

The next is an interesting form of exchange medium (money) that arose where people established a trade in return for currencies made, not of precious gold or platinum, but paper! There is a surplus supply of paper in economy and what quality of it made it a reliable, reassuring, acceptable source of money? Well, it was not all the paper that held this position, but paper currencies printed and issued by government recognized authority like Reserve Bank of India for India and The Bank of England for UK were accepted as a medium of exchange, in fact, an Undeniable medium of exchange in the respective countries. People accept it because the government says it can be accepted and assures of its worth. A centrally organized system of bank was introduced, which is still widely in use which stores the currencies of each individual customer of the bank in structures called accounts and a centralized record of all the details of balance and transactions is maintained. Banks offer handful of advantages as they are answerable to their customers and so taking in charge of one’s money is reduced is just one among the merits.

The practical utility of paper currencies for hand-to-hand transaction involving a large sum of money seemed to impose physical difficulties at times and so is being over taken by online media like card transactions through which transactions are virtually moneyless. The system which recently gained popularity are transactions through apps highly called as mobile wallets of Unified Payments Interface.

Most of the systems have one or the other disadvantage. Introduction of net banking and other online transactions as an extension of bank has also been proven hackable as fraud reports and cybercrimes are filed in this regard frequently and a centralized system such as bank led to demand for accessibility. This is where Cryptocurrency comes into play.

II. WHAT ARE CRYPTOCURRENCIES?

In this transaction setting, transactions are carried out through digital currencies called cryptocurrencies like Bitcoins, Ethereum, Dogecoin, Litecoin, etc. A transaction is said to have been taken place when cryptocurrencies from an user is transferred to another. Blockchain technology is used for the functioning of cryptocurrency-based transactions and in this technology, transaction is recorded in the transaction list called 'ledger' where each user gets a copy of it.

There are people who dedicate their system's power for the purpose of cryptocurrency transactions who receive rewards in the form of digital money for the service they render for the benefit of the arrangement. This is called cryptocurrency mining. The miners aid the structure by validating legitimate transactions which serves as a key element in holding the structural integrity of this technology.

III. WHAT HAPPENS IN THIS TECHNOLOGY?

Every time a new legitimate transaction takes place, this is noted in the ledger and updated and reflected in every single copy of the ledger belonging to all the systems involved in the network, or simply, all miners. The decentralized nature of this technology where every system maintains its own ledger offers accessibility that a centralized system does not. Many such cryptocurrencies are employed through blockchains.

Blockchains are not a transaction medium, it is rather the encrypting technology which provides security to the transactions being made through cryptocurrencies.
In this form of transactional arrangement, transactions are recorded in the ledger, while the ledgers are in turn arranged into blocks (cubicle structures). A number of blocks are connected together which brings the name blockchain.

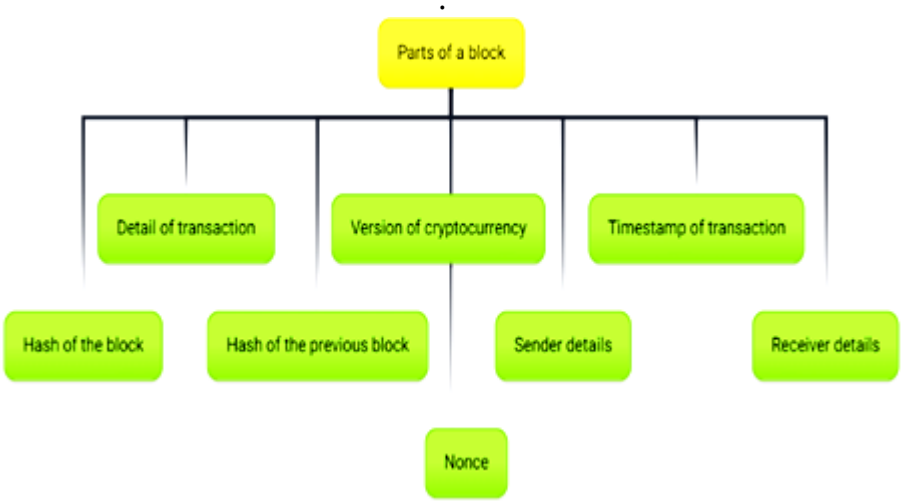
When a transaction takes place, its details are entered into a block. The blocks are established only if all or majority of miners validate the details of the transaction given in the block in their copy of the ledger. In case of legitimate transactions, the blocks are validated.

The most interesting part of blockchain technology comes out when a new transaction takes place. In this case, when the facts of the transaction that needs to be carried out has to be checked, the computer not only checks the computer's copy of the ledger, but the checking is carried out with every single copy of the ledger belonging to every single computer involved in the network. Only if majority of the computers give a green signal for the conduction of the transaction, the process is carried on, else, the transaction request is considered invalid and stands rejected.

IV. CONTENTS IN A BLOCK

Each block contains various details about the transaction it holds and the common ones are:

- Details of Initiator of transaction (sender)
- Details of recipient (receiver)
- A unique identifying code for each block called ‘Hash’
- The hash of the preceding block in the blockchain
- Version of cryptocurrency used for the transaction
- A special encrypted code that the miner has to solve in order to authorize and validate the transaction of the block, called Nonce.
- A timestamp indicating the position of the particular block in the chain.
- Details of transaction



V. UNHACKABLE?

Contents of a block varies from one layout to another and the listed ones are the commonly found details engraved in a block.
If we were to pick one among the listed which plays a crucial role in any blockchain for that matter, it is the part where each block contains the hash of the preceding block in the chain. As we know hashes are unique codes and so no two blocks can have the same hash and a given block cannot have two hashes. Once the transaction request is authorized by majority of miners and the block is closed, the hash remains constant.

This very detail is what makes the blockchain practically ‘Unhackable’. If a person tries to tamper with the details of transaction in their copy of the ledger, all the other ledgers show a different set of facts regarding the same transaction and so the transaction does not get approval from majority of miners and so remains invalid indicating intentional or unintentional tampering. Hacking into majority miner computers which are of different configurations at the same time to display the tampered data to seek approval for the fraudulently modified transaction is not practically possible, at least not with the current level of technology, considering there are almost a million miners for bitcoin alone.

Another way to see it is that, the moment a modification is made by a hacker in the transaction contained in a block, the hash of the block no longer remains the same. This means the succeeding block has the initial, that is, the hash of the block before tampering, as the hash for previous block and with the change in hash, the succeeding block turns invalid and this affects the validity of every other consecutive block and so the entire chain collapses indicating efforts made to illegitimately modify data. This is a major improvement when it comes to attaining an unhackable transaction platform.

It is worthy to mention that, when we say blockchains are 'practically' unhackable, we only speak with reference to the existing level of technology. It would be a safe bet to say that with the rate at which advancement in technology is taking place, this may not be the case in future.

Investments in Cryptocurrencies can be understood as a combination of money exchange and share marketing, where money is invested upon, not different shares, but in different cryptocurrencies which are widely speculated among the users to be the future of currencies.

Cryptocurrency is not a currency by itself. It is a general term used to represent a number of sub classifications. Not to mention, there are over 22,000 cryptocurrencies at the beginning of 2023 and among them, only around 8000 are active ones. All of the different cryptocurrencies differ in their characteristic features and one may seem to offer an upper hand over the others when segregated on the basis of a particular quality. Bitcoin, Litecoin, Ethereum, Doge etc. are just some of which are popularly invested in.

Just like in stock marketing, the value of the cryptocurrencies keeps fluctuating and upon change in their value, it is the investor's choice to either spend it, leave it or increase the investment. But it is necessary to keep in mind that the fluctuations do not display a predictable pattern and any such attempt at predicting are mere expectations and may not be right.

If the investments made are devoid of statistical influence, then what guarantee do we have on the money invested? The thing is, we do not. Then what is that about cryptocurrencies that account to all the investments? A detailed discussion on the merits and demerits of this technology may help throw some light on this.

1. **Merits:** Though cryptocurrencies may not seem flattering with only the sole understanding of risks involved, there are two sides even to this coin. It is basically understood with the high enthusiasm among various business groups that volunteer to invest in cryptocurrencies that, negatives are not all that this technology has to offer. Some of their merits are:

    - Decentralized nature of such transactions makes room for accessibility: The major demand for accessibility and secure transparency is the main cause for the development of this technology. So, it aids in fulfilling this requirement.
    - Their organization aims at providing Highly secure transactions Blockchain technology, as mentioned in the previous sections, is almost practically unhackable with the current technology which urges users to promote it.

- Only hash of the sender and receiver is visible which makes the users 'pseudo-anonymous '.

  The transparency offered by this system ensures security by providing each user an unique hash and carrying forward transactions under the hash rather than revealing the name of the people involved in the transaction.

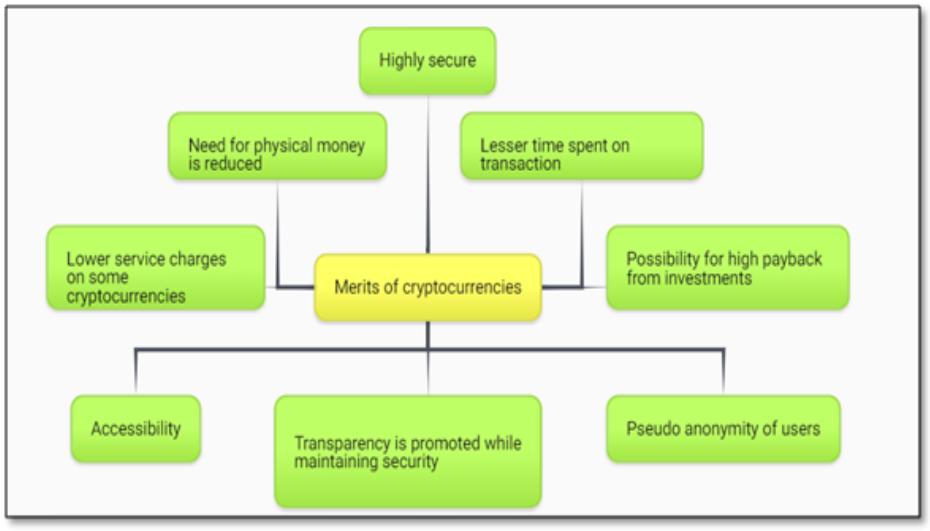
- International transactions can be carried out in a matter of minutes while traditional transactions take a longer time.

  The procedure followed for the transaction to take place is the same regardless of the users. So comparatively International transactions can take place in a matter of minutes.

- For some cryptocurrencies, the service charge on transactions are very low and even zero at places. Many cryptocurrencies have charges demanded for transaction near zero which attracts many users to invest more in cryptocurrencies and prefer to make transactions through it.

- It reduces the need for physical money Yet another reason why cryptocurrencies emerged is due to the difficulties that arise when hand to hand transactions involving large sum of money is required and the concept of digital currency and digital assets makes it easier.

- Possibility for high returns from the investment.The value of cryptocurrencies keep fluctuating and there is high possibility that it yields good returns to the investment.



2. **Demerits:** Any technology though possessing major merits inevitably has some demerits. Blockchain using cryptocurrency is no exception. Here are some of the disadvantages that accompanies this technology:

   - Fluctuating value of cryptocurrency is a risk in itself. The value of Cryptocurrencies keep fluctuating and there is a possibility that its value drops and the investors in

that currency can face a loss. This is a major risk factor of cryptocurrencies that limits the expansion of investors in cryptocurrencies.

- It is not an authorized form of transaction in many countries
  Transactions through cryptocurrencies are not authorized by any legal bodies in many of the countries. Especially in India, it is not regulated by an government authority. This is also a factor which limits the expansion of these methods.

Parameters	Bitcoin	Ethereum	Dogecoin	Citation
Crypto representation	BTC	ETH	DOGE	https://www.bankrate.com/investing/bitcoin-vs-dogecoin-vs-ethereum-crypto-comparison/
Profitability (as per data from April 2023 and speculations)	Highly profitable	Most profitable out of the three	Highly profitable	https://tradersofcrypto.com/guides/crypto-mining-returns/
Investment 2023 (Speculated)	Very high among the three	High among the three	High among the three	https://www.forbes.com/advisor/in/investing/cryptocurrency/top-10-cryptocurrencies/
Value (On 21st September 2023)	Bitcoin : Rs.2245414.00	Ethereum: Rs.2244800347.68	Dogecoin: Rs.5.15	https://www.binance.com/en/feed/post/1182360?ref=568213964
Mining comfort	Hardest to mine among the three	Easier to mine than bitcoin and Doge	Easier to mine than Bitcoin	https://www.simplilearn.com

- Scams and intrusion attempts.

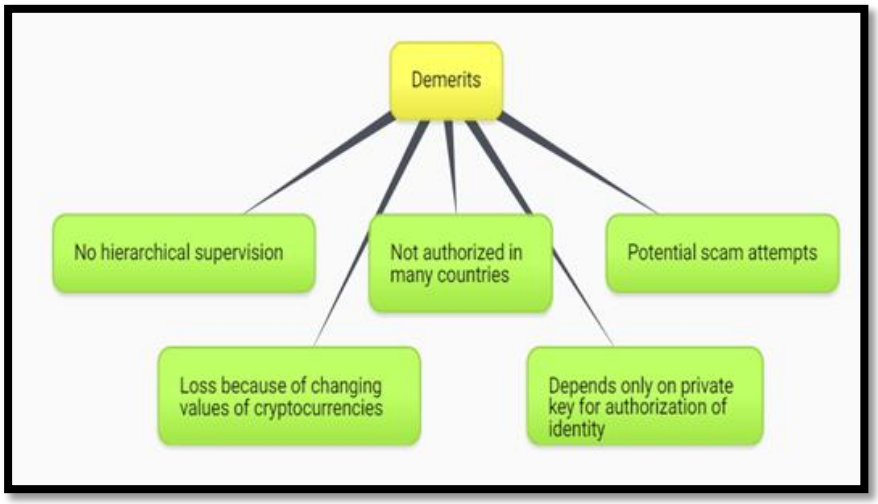
  Though blockchains provide great security for the transaction process, there are several attempts made by scammers to trick the users into falling for the trap they set.

- Relies on private key for identity

  The sole proof for identity of the user is the private key owned by them and if that is lost, there are no alternatives to rely on.

- No supervision

  As there is no Government authority that deals with the management of cryptocurrencies, supervision of transactions are not done higher than the miner verification stage and lack of supervision often comes out as a scary factor of technologies with respect to monetary transactions.



3. **Comparison between some popular Cryptocurrencies** There are a great number of cryptocurrencies that are popularly and widely investedupon. Some of them are Bitcoins, Ethereum, Dogecoins etc. The following table compares and contrasts between these on the basis of a few parameters:

   The tabular column depicts the overall view and recent trends exhibited by the three cryptocurrencies which necessarily includes speculations and perspectives of investors.

VI. TYPES OF BLOCKCHAINS

Blockchains can be broadly classified into the following types:

- Public blockchains
- Private blockchains

- Hybrid blockchains
- Consortium blockchains

1. **Public Blockchains:** As the name suggests, public blockchains are open blockchains that provide access to users without any constraints. It does not restrict its users from indulging in the network based on any criteria and is basically a largely decentralized network with highly replicated copies of ledgers. It works similar to the working of blockchains discussed in prior sections as a network of systems where transactions are authorized by miner computers and details of transactions are provided to the users constraint-less. Validation of any transaction in the network is done for currently made transactions as well as previously made ones. Some of the prominent features of public blockchains are:

    - Highly flexible as the number of conditions are lessened.
    - Higher level of verification takes place as due to lack of constraints, more users join and so more miners are created which results in copies of ledgers being made which implies more number of systems have to validate the transaction for its occurrence.
    - Highly decentralized
    - High accessibility
    - Open environment for carrying out the transaction.
    - Lower transaction speed due to increased number of approval needed for proceeding with the transaction.
    - Higher amount of system power is required as more number of systems are involved

2. **Private Blockchains:** As the name suggests, private blockchains are constrained blockchains which restricts the access and involvement of users based on some conditions. They are usually employed in cases where only some of the users' involvement is required in the transaction process for reasons of confidentiality, security, privacy etc. Organizations, institutions, enterprises and various other groups of individuals use private blockchains to confine the circulation or access of sensitive details within themselves. Some of the features of private blockchains are as follows:

    - Less flexible due to regulatory restrictions
    - Less decentralized due to limited involvement of systems
    - Less verified transactions take place
    - Highly private as data security is given preference to
    - Rate at which transactions are performed is higher due to limited nodes
    - Lower energy consumption
    - Lower security of transactions than public blockchains due to reduction in the number of systems that need to verify the transactions because of the reduction in overall number of computers involved in the blockchain.

3. **Hybrid Blockchains:** Hybrid blockchains are a combination of features of both public and private blockchains. In this type of blockchains, accessibility is maintained by letting some sections of transactions as completely accessible as in public blockchains while some set of transactions are given limited access to, like that of a private blockchain. This is a mixture of properties of both the blockchains which allows customizing the access granted to a particular section of the blockchain. Some of the prominent features of hybrid blockchains are:

    - Flexibility can be given as per the requirements
    - Not very decentralized
    - Customizable access
    - Transparency is given as per requirement
    - Security is provided to different parts of blockchain as per the requirement
    - It is not a completely open structure

4. **Consortium Blockchains:** Consortium blockchains is a group of private blockchains owned by different organizations from same or related field. Consortium blockchains can be imagined as a blockchain network where all the individual blockchains are accessed and controlled. In this layout some systems involved in the network are chosen to carry out the overview of access and approval of transactions and its details. Some features of consortium blockchains are as follows:

    - Efficient management of blockchains
    - Necessary level of decentralization can be done
    - Not an open structure

VII. FUTURE OF CRYPTOCURRENCIES AND BLOCKCHAINS:

Cryptocurrency is a very recent advancement in technology that managed to gain popularity and users within a short period of time. It is very reasonable to expect them to be the future of transactions and with growing improvements in transaction methodologies, it is a safe bet to say that more people are and will be inclined towards moneyless transactions. So, Cryptocurrencies and blockchains are of high potential and possess the potential to become a unified.

VIII. CONCLUSION

Today's world is a place that craves innovation and improvements and Cryptocurrencies and blockchains are not any less of it. The high potentiated technology is no doubt an important landmark in the history of financial transactions. It possesses a number of advantage and has managed to achieve a decentralized, transparent yet highly secure transaction forum that no other previous forums for transaction were able to offer. This in itself is a huge achievement. But there are a number of downsides to blockchain technology too that needs to be taken into consideration. But that is the case for any existing system of transaction where, there is no room for ideal theories in the practical utility of technology. The most likely conclusion that can be drawn in this regard is that this technology can be expected to grow along with growth in technology as a whole. The continuation of current rate of growth in technology can reap huge returns from

cryptocurrencies and blockchains and this can further aid in creating an absolutely unshakable system of transaction.

Blockchains, though seems to offer a lot of advantages over many other existing systems of transaction, it would take humanity its own time to accept and accommodate it as a common day to day system of transaction. The idea of digital assets and currencies like bitcoin, altcoins etc. with the idea of fluctuating value automatically lets people relate it to stockmarket and the limitations of it like loss upon investment etc., the advantages that this technology offers seems to outweigh it all and provide an even more transparent system of trade and commerce.

REFERENCES

[1] Arun Rupesh Maini)Mrwhosetheboss. "How Cryptocurrency ACTUALLY Works." Www.youtube.com, 6 June 2021, www.youtube.com/watch?v=rYQgy8QDEBI
[2] Bitcoin vs. Ethereum vs. Dogecoin: Top cryptocurrencies compared. (2022, August 30). Bankrate. https://www.bankrate.com/investing/bitcoin-vs-dogecoin-vs-ethereum-crypto-comparison/
[3] Crypto Mining Returns. (n.d.). https://tradersofcrypto.com/guides/crypto-mining-returns/
[4] Discover the latest Crypto News & Feed from Influencers. Binance Feed. (n.d.). https://www.binance.com/en/feed/ https://www.binance.com/en/feed/post/1182360?ref=568213964
[5] Gadekallu, T. R. (2022, March 18). Blockchain for the Metaverse: A Review. arXiv.org. https://arxiv.org/abs/2203.09738
[6] IBM. "What Is Blockchain Technology - IBM Blockchain | IBM." Www.ibm.com, 2023, www.ibm.com/topics/blockchain.
[7] Paul, P and Aithal, P. S. and Saavedra, R. and Ghosh, Surajit, Blockchain Technology and Its Types—A Short Review (December 26, 2021). International Journal of Applied Science and Engineering (IJASE), 9(2), 189-200. (2021). ISSN: 2321-0745. , Available at SSRN: https://ssrn.com/abstract=4050933
[8] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 2018, pp. 473-475, doi: 10.1109/ICOIN.2018.8343163.
[9] Tretina, K. (2023, March 24). 10 Best Cryptocurrencies To Invest In September 2023. Forbes Advisor INDIA. https://www.forbes.com/advisor/in/investing/cryptocurrency/top-10-cryptocurrencies
[10] Yasar, K. (2023, July 7). Pros and cons of cryptocurrency. WhatIs.com. https://www.techtarget.com/whatis/feature/Pros-and-cons-of-cryptocurrency
[11] Yukun Liu, Aleh Tsyvinski, Risks and Returns of Cryptocurrency, *The Review of Financial Studies*, Volume 34, Issue 6, June 2021, Pages 2689–2727, https://doi.org/10.1093/rfs/hhaa113 https://academic.oup.com/rfs/article/34/6/2689/5912024

