Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

Block Chain Based Financial Transactions Positive and Negative Aspects

Dr. Rakhi Mutha
Associate Professor, Dept. of Computer Engineering
Poornima Institute of Engineering & Technology

Abstract **: In the current era of Block Chain Based Financial Transactions, there is need to aware about positive and negative aspects. The crypto currencies have arisen as significant monetary frameworks. They depend on a protected ledger record information structure; mining is a vital piece of such frameworks. Mining adds records of past exchanges to the circulated record known as Blockchain, permitting clients to arrive at secure, powerful agreements for every exchange. This paper tries to take multiple major cryptocurrencies into consideration and also take multiple parameters into consideration that determine how beneficial a specific cryptocurrency is for a certain type of use. Comparing these major cryptocurrencies on these parameters provides us with a very clear and distinct idea of their individual pros and cons or merits and demerits while also allows us to gain clear knowledge of the major variables that determine how good a specific cryptocurrency is when it comes to certain kind of work and performance.**

Keywords: Cryptocurrency, Blockchain, Mining, Ledger.

I. INTRODUCTION

Bitcoin and blockchain technology are very much in today's world starting to shape and define new and different aspects in computer science and IT. The need for decentralized money has been exploited more as a theoretical concept, but in the past decade, it became viable, all is basically credited to the extremely well known paper of Satoshi Nakamoto that was first put out in the year of 2008, What this paper basically did was introduce or start bitcoin and blockchain as their distinct technologies. A Cryptocurrency is a peer to peer computerized trade framework in which cryptography is utilized to create and disseminate money units . This interaction requires dispersed confirmation of exchanges without a focal power.

Exchange confirmation affirms exchange sums, and regardless of whether the payer possesses the cash they are attempting to spend while guaranteeing that money units are not spent twice. This confirmation interaction is called mining . Cryptocurrencies utilize an assortment of mining advances, as indicated by their specific necessities. For occasion, certain Cryptocurrencies center around confining the number of exchanges approved per unit time, while others focus on accomplishing quick, lightweight administrations .

A few mining calculations are purposely memory escalated; others are computationally costly . In this paper, we look at multiple cryptocurrencies and their different aspects that will help us understand them better.

II. TERMINOLOGIES AND BASIC CONCEPTS

In order to look at different cryptocurrencies and determine which one is more feasible and which one is more reliable we need to know the basic components that make up these cryptocurrencies. So here is a brief explanation of the major concepts and terminologies that will be talked about and mentioned multiple times throughout this paper.

A. Block Chain

A blockchain in the simplest of terms is a distributed data set that is divided between the hubs of a PC organization. As a data set, a blockchain stores data electronically in advanced organizations. Blockchain is most popular for its important work in crypto currency frameworks such as Bitcoin to maintain a secure and decentralized record of exchanges.

The development of blockchain is that it ensures the consistently and security of information records and creates trust without the need to confide in outsiders. An important difference between a common data set and a block chain is the way information is organized.

Block chains collect data in collections, called blocks, which hold data sets. Blocks have specific storage limits, and when filled, they are closed and connected to the most recently filled square, forming a chain of information called a block chain.

All new data after the newly added block is arranged into a recently formed square, and then, at this point, once filled, the square is added to the chain as well.

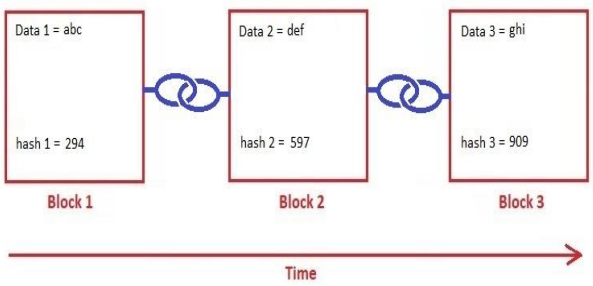

Figure 1 : Block chain

B. Mining

Mining, with regards to blockchain innovation, is the most common way of adding exchanges to the enormous dispersed public ledger of existing exchanges, known as the blockchain. The term is most popular for its relationship

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

with bitcoin, however different innovations utilizing the blockchain utilize mining. Bitcoin mining rewards individuals who run mining activities with more bitcoins.

Blockchain mining includes adding exchanges to the current blockchain ledger of exchanges disseminated among all clients of a blockchain. While mining is for the most part connected with bitcoin, different advances utilizing a blockchain utilize mining too. Mining includes making a hash of a block of exchanges that can't be effortlessly manufactured, ensuring the uprightness of the whole blockchain without the requirement for a focal framework.

Mining is regularly done on a committed PC, as it requires a quick CPU, just as higher power use and more hotness produced than average PC tasks. The fundamental motivator for mining is that clients who decide to utilize a PC for mining are compensated for doing as such. On account of bitcoin, it is 25 bitcoins per hash. For that reason a few programmers use machines they break into to mine bitcoins, getting an accidental casualty to pay for the expenses of mining while at the same time receiving none of the rewards.

C. Cryptocurrency

Cryptocurrency is a computerized installment framework that doesn't depend on banks to check exchanges. It's a distributed framework that can empower anybody anyplace to send and get installments. Rather than being actual cash hefted around and traded in reality, cryptocurrency installments exist absolutely as computerized passages to a web-based data set portraying explicit exchanges. At the point when you move cryptocurrency reserves, the exchanges are recorded in a public ledger. Cryptocurrency is put away in advanced wallets.

Cryptocurrency accepted its name since it utilizes encryption to check exchanges. This implies progressed coding is associated with putting away and communicating cryptocurrency information among wallets and to public ledgers. The point of encryption is to give security and wellbeing.

The principal crypto currency was Bitcoin, which was established in 2009 and stays the most popular today. A significant part of the interest in cryptocurrencies is to exchange for benefit, with examiners on occasion driving costs very much.

Cryptocurrencies run on a circulated public ledger called blockchain, a record of all exchanges updated and held by currency holders.

Units of cryptocurrency are made through a cycle called mining, which includes utilizing PC ability to take care of confounded numerical issues that create coins. Clients can likewise purchase the monetary standards from representatives, then, at that point, store and spend them utilizing cryptographic wallets.

III. BITCOIN:

Bitcoin is a decentralized premium money begat in January 2009. It follows the confounding thought proposed by the pen name Nakamoto in the white paper.12 It stays confidential to advance people or characters. Bitcoin offers an assurance of lower trade charges than conventional web based portion parts, and by any stretch of the imagination, not at all like authority money related guidelines, it works by decentralized powers.

Bitcoin is a decentralized current money made in January 2009. It follows the thinking about the befuddling nom de plume Nakamoto in the white paper. The individual or character of the person who makes the advancement stays confidential. Bitcoin offers an assurance of lower trade charges than conventional online portion installment instruments, and dissimilar to the authority type of money by any means, it works by decentralized powers.

Algorithm utilized - SHA 256

Bitcoin, though being the biggest and most popular cryptocurrency in the market does have some disadvantages or drawbacks that hold it back from being more efficient.

A. BITCOIN DRAWBACKS:

The Bitcoin scalability issue alludes to the restricted capacity of the Bitcoin organization to deal with a lot of exchange information on its foundation in a limited ability to focus time. It is identified with the way that records (known as blocks) in the Bitcoin blockchain are restricted in size and recurrence.

Bitcoin's blocks contain the exchanges on the bitcoin network. The on-chain exchange handling limit of the bitcoin network is restricted by the normal block creation season of 10 minutes and the first block size cutoff of 1 megabyte. These mutually oblige the organization's throughput. The exchange handling limit greatest assessed utilizing a normal or middle exchange size is somewhere in the range of 3.3 and 7 exchanges each second. There are different proposed and initiated answers to address this issue.

IV. ETHEREUM:

Ethereum is a blockchain stage that has its own crypto currency, called Ethereum (ETH) or Ethereum, as well as its own programming language, Solidity. As a blockchain network, Ethereum is a decentralized public record for confirming and recording transactions. The association's clients can make, appropriately, tweak and use applications on stage and use their Ethereum crypto currency as part of it.

Insiders refer to the association's decentralized app as "dApps." As a cryptocurrency, from 2021 onwards, Ethereum is second only to Bitcoin in the market. Ethereum aims to attract designers to collect and disseminate excellent scheduling and flow applications (dApps) that can be used without the risk of abandonment, distortion, or impedance. Ethereum describes itself as "the world's programmable blockchain." It isolates itself from Bitcoin as a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

programmable association that fills the commercial arena of money-related organizations, games, and applications that can all be paid for with the Ethereum crypto currency and protected from coercion, robbery, or control.

Ethereum's coordinators are eager to consider the ability of blockchain development for secure transactions of virtual currencies. Its ETH crypto currency was basically made as part of a method that relies on the applications it builds. It's protected from software engineers and various eavesdroppers, opening up a promising environment for restricting private information from clinical benefit records to projection voting form systems. Its reliance on crypto currencies opens up promising conditions for programmers to make and market games and commercial applications at the association. Unlike the Bitcoin blockchain, the Ethereum blockchain was not made to help crypto currencies. The Ethereum crypto currency is designed to provide internal funding for applications that rely on the Ethereum blockchain. With everything in mind, Ethereum has a broader desire. It should be a phase of broad employment where information can be securely stored.

Despite the differences, the two are producers of virtual financial norms that have become competitors in the contribution scenario. The more virtual financial criterion is simply:

they are coins that do not exist in real life, except that they are replaced by a series of codes that can be exchanged for a fee paid by buyers and merchants..

Algorithm used - Keccak-256

Again this one too has a set of problems that make it less useful and accessible than it could be.

and some of these drawbacks are -

A. Ethereum Drawbacks:

Low Scalability-Ethereum utilizes a Proof of Work (PoW) model, which empowers only 13 exchanges each second (TPS) contrasted with its huge interest of 1.355 million TPS consistently. This causes network blockage and requests high exchange charges

Unreasonable power utilization Its PoW model's calculation utilized for making exchanges utilizes gigantic computational power where an hour's power utilization goes up to 62.56KWh

V. RIPPLE(XRP):

Ripple is an innovation that goes about as both a cryptocurrency and a computerized installment network for monetary exchanges. It was first delivered in 2012 and was helped to establish by Chris Larsen and Jed McCaleb. Ripple's fundamental interaction is an installment repayment resource trade and settlement framework, like the SWIFT framework for global cash and security moves, which is utilized by banks and monetary mediators managing across monetary standards.

The one significant symbolic that is utilized by and large for the crypto currency is premined and it normally uses the ticker picture XRP. Ripple is the name of the association and the association, and XRP is the cryptocurrency token. The inspiration driving XRP is to fill in as a midway part of exchange between two money related guidelines or associations—as a sort of momentary reimbursement layer segment.

Ripple deals with an open-source and circulated decentralized stage that considers a predictable trade of money in any construction, regardless of whether it's dollars, yen, euros, or crypto currencies, as litecoin or bitcoin. Ripple is an overall portions association and counts huge banks and financial organizations among its customers. XRP is used in its things to work with quick change between different financial guidelines.

The high level cash, XRP, goes probably as a platform money to various financial structures. It doesn't separate between any fiat/cryptocurrency, which simplifies it for any cash to be exchanged for another. Each money on the climate has its own entryway—e.g., CADBluzelle, BTCbitstamp, and USDsnapswap. Accepting River required bitcoins as portion for the organizations conveyed to Lawrence, Lawrence doesn't actually should be in charge of any bitcoins. He can send the part to his entry in Canadian dollars (CAD), and River can get bitcoins from his entrance. One section isn't relied upon to begin an all out trade; different doorways can be used, molding a chain of trust undulating across the customers.

Algorithm used - Elliptic curve digital signature algorithm

A. RIPPLE *Drawbacks*:

The organization has focused on focusing on banks solely, and this is a mood killer for some early adopters of blockchain innovation. Truth be told, Jed McCaleb left Ripple in 2013 as referenced before, and forked out Stellar, which held the functionalities for day to day existence utilize like the first Ripple.

Ripple, the organization, has over 60% of XRP, and surprisingly however the probability of a huge auction is insignificant, they enjoy the supernatural 51% benefit and henceforth control the blockchain.

Since ripple is pre-mined, there exist practically zero impetuses for normal hubs to work in the organization, which then, at that point, leaves the corporate like banks to give the validator hubs. Since a couple of hubs are expected to run the organization, it's not actually appropriated.

VI. DOGECOIN:

Dogecoin (DOGE) is a distributed, open-source cryptocurrency. It is considered an alternative coin and a for all intents and purposes deriding picture coin. Dispatched in December 2013, Dogecoin has the image of a Shiba Inu canine as its logo.

While this is clearly a joke, Dogecoin's block chain still has its benefits. Its major advancement comes from Litecoin. The renowned part of Dogecoin, assessed utilizing Script, is its negligible charge and limitless offers. Dogecoin introduces itself as an "intriguing" variation of Bitcoin, with its logo being Shibu Inu (Japanese Dog).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

Dogecoin's easygoing exhibitions are with regards to the disposition of the flourishing crypto local area. Its secret advancement and limitless stock is a discussion about Bitcoin being quicker, more adaptable, and happily clarified by purchasers. Dogecoin is an "expansion coin," while crypto currencies like Bitcoin are deflationary in light of the fact that the quantity of coins that will be made has a rooftop.

Typically, the extent of Bitcoins that are imparted to the interaction through mining rewards is isolated, and its extension rate is parted around it until all coins are conveyed.

A. DOGECOIN *Drawbacks*:

Putting resources into Dogecoin isn't as old as in a more settled computerized money like Bitcoin. As a general rule, a couple of shops acknowledge cryptocurrencies. Those that do, in any case, are bound to take Bitcoin rather than Dogecoin. The ascent of Dogecoin will be hard to proceed without boundless acknowledgment.

While Dogecoin can possibly turn into a genuine member in the crypto domain, it is bound to fall and consume. To take a shot at contributing for no particular reason, it's anything but an ill-conceived notion to put resources into Dogecoin – all things considered, no one can tell what might occur. Notwithstanding, there are a plenty of elective speculations that are viewed as prevalent.

CONCLUSION

Crypto currency is a computerized installment framework that doesn't depend on banks to check exchanges. It's a distributed framework that can empower anybody anyplace to send and get installments. Rather than being actual cash hefted around and traded in reality, crypto currency installments exist absolutely as computerized passages to a web-based data set portraying explicit exchanges. At the point when you move crypto currency reserves, the exchanges are recorded in a public ledger. Crypto currency is put away in advanced wallets.

REFERENCES

[1] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, 2008. Available: https://bitcoin.org/bitcoin.pdf [Accessed Feb 15, 2019].

[2] B. Marr, “A very brief history of blockchain technology everyone should read”, Forbes, 16 Feb 2018. Available: https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-briefhistory-of-blockchain-technology-everyone-shouldread/#19c60b067bc4 [Accessed Feb 15, 2019].

[3] H. Dikariev, M. Miłosz, “Blockchain technology and its applications” (In Polish), Journal of Computer Sciences Institute (JCSI) no. 6 (2018), Lublin, 2018, p. 59-61.

[4] Cryptonite, “Is it too late to invest in Bitcoin? is it just a bubble?”, Hacker Noon, Sept 19, 2018. Available: https://hackernoon.com/is-ittoo-late-to-invest-in-bitcoin-is-it-just-a-bubble-704ba4f69d9d [Accessed Feb 17, 2019].

[5] “Bitcoin burglaries: the 5 biggest cryptocurrency heists in history” , Big Think, 23 Aug 2018. Available: https://bigthink.com/reubenjackson/bitcoin-burglaries-the-5-biggest-cryptocurrency-heists-inhistory [Accessed Feb 11, 2019].

[6] M. Paquet-Clouston, B. Haslhofer, B. Dupont, “Ransomware payments in the bitcoin ecosystem”, 2018.

[7] J. H. Mosakheil, "Security threats classification in blockchains", Culminating Projects in Information Assurance. 48, St. Cloud State University, 2018. Available: http://repository.stcloudstate.edu/msia_etds/48 [Accessed Feb 15, 2019].

[8] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, “The Blockchain as a Decentralized Security Framework”, 2018.

[9] L. Luu, Y. Velner, J. Teutsch, P. Saxena, “Smart pool: practical decentralized pooled mining”, USENIX Security Symposium, 2017.

[10] A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, S. Capkun, “On the security and performance of proof of work blockchains”, ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 3-16.

[11] L. Luu, D. Chu, H. Olickel, P. Saxena, A. Hobor, “Making Smart Contracts Smarter”, 2016. Available: https://loiluu.com/papers/oyente.pdf [Accessed Feb 19, 2019].

[12] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts”, IEEE Symposium on Security and Privacy, 2016, pp. 839- 858.

[13] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, “Town crier: An authenticated data feed for smart contracts”, Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 270-282.

[14] X. Lia, P. Jianga, T. Chenb, X. Luoa, Q Wenc., “A Survey on the Security of Blockchain Systems”, 2018