International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 10 Issue 12, December, 2021, Impact Factor: 7.751

Cryptocurrency: A Future Scope

Mr. Divyaansh Kataria[1], Mr. Kavin Kataria[2]

Main Author: Mr. Divyaansh Kataria email : kdivyaansh21@gmail.com

ABSTRACT

Blockchain is a decentralised transaction and data management technology that was first designed for the cryptocurrency Bitcoin. Since the concept was first proposed in 2008, there has been a surge in interest in Blockchain technology. The core qualities of Blockchain that provide confidentiality, anonymity, and data integrity without a third-party organisation in charge of the transactions are driving interest in the technology, which opens up new research fields, particularly in terms of technological hurdles and constraints. This article aims to present a thorough mapping analysis with the purpose of gathering all relevant research on Cryptocurrency.

Keywords: Blockchain, Cryptocurrency, Decentralization, Distributed ledger technology.

INTRODUCTION

A cryptocurrency is a digital or virtual currency that is protected by encryption, making counterfeiting and double-spending practically impossible. Many cryptocurrencies are built on blockchain technology, which is a distributed ledger enforced by a distributed network of computers. Cryptocurrencies are distinguished by the fact that they are not issued by any central authority, making them potentially impervious to government intervention or manipulation.[1]
Blockchain is a subset of what is known as distributed ledger technology ("DLT"). DLT is a method of storing and sharing data across various data stores (also known as ledgers), each of which contains the same data records and are managed and controlled by a distributed network of computer servers known as nodes. Blockchain is a distributed ledger that uses an encryption method known as cryptography and specific mathematical algorithms to create and verify a continuously growing data structure – to which data can only be added and from which existing data cannot be removed – in the form of a chain of "transaction blocks". [2,3]

The primary goal of this article is to gain a thorough understanding regarding the current research subjects, difficulties, and future prospects in Cryptocurrency.

NEED FOR THE STUDY

As cryptocurrency has gotten a lot of attention and everyday more people are trading and purchasing Bitcoins. As a result, it is very likely that Bitcoin will survive in the long run. It is critical as a future study area, and it will draw both industry and academics to do additional study from both a business and technical standpoint.

RESEARCH GAPS

The applications of Blockchain technology is not just limited to cryptocurrency. Instead, the concept of a decentralisation and a public ledger can be extended to a variety of other applications in different industries, which adds to the intrigue of the Blockchain research. Therefore, the study of the various possibilities of using Blockchain in other environments is vital, as it can disclose and generate better models and options for conducting transactions in various industries.

LITERATURE SURVEY

The term "cryptocurrency" has become a buzzword to describe a wide range of technological advancements that make use of a method known as cryptography. In simple terms, cryptography is the process of encrypting data and then changing it into an unreadable format that can only be deciphered (or decrypted) by someone with a secret key. There are several methods to structure a consensus mechanism. The Proof of Work ("PoW") and Proof of Stake ("PoS") methods are the two most often utilised mechanisms in the context of cryptocurrencies.

a.Proof of Work ("PoW"): In a PoW system,network participants must solve so-called "cryptographic puzzles" to add new "blocks" to the blockchain. Mining is a term used to describe the process of solving puzzles. Simply put, these cryptographic puzzles are made up of all previously recorded information on the blockchain, as well as a new set of transactions to be included to the next "block." The PoW process necessitates a tremendous amount of computational resources, which use a significant amount of electricity, because the input of each puzzle grows greater over time (resulting in a more difficult calculation).[4]

When a network participant (also known as a node) solves a cryptographic puzzle, it verifies that he has finished the task and is paid with a digital form of value (or in the case of a cryptocurrency, with a newly mined coin). This payment serves as a motivator to maintain the network. Litecoin, Bitcoin Cash, Monero, and other cryptocurrencies are examples.

b. Proof of Stake (PoS): In a PoS system, a transaction validator (i.e. a network node) must verify ownership of a specifc asset (or in the case of cryptocurrencies, a certain amount of coins) in order to participate in the validation of transactions. Instead of "mining," this process of authenticating transactions is referred to as "forging." In order to validate a transaction in the case of cryptocurrencies, a transaction validator will have to prove his "stake" (i.e., his share) of all coins in existence. He will have a better chance of validating the following block depending on how many bitcoin he owns (i.e. this all has to do with the fact that he has greater seniority within the network earning him a more trusted position). Cryptocurrencies such as Neo and Ada (Cardano) utilize a PoS consensus mechanism.[5]

Various players in cryptocurrency[6,7]

The cryptocurrency market is a new stage on which many players take on different roles. These are the important players in the market to give some further insight on how it operates:

a) Cryptocurrency users
b) Miners
c) Cryptocurrency exchanges
d) Trading platforms
e) Wallet providers
f) Coin inventors
g) Coin offerors

A Blockchain application was originally characterised as a solution created using Blockchain technology. Some prototype applications for implementing Blockchain in different settings are smart contracts, smart property, digital content distribution, Botnet, and P2P broadcast protocols. [8] This demonstrates that Blockchain technology isn't just for currency. Instead, the concept of a public ledger and a decentralised environment may be used to a variety of additional applications in many industries, making Blockchain research even more intriguing.

However, rather than applying Blockchain technology in another context, a set of diverse applications were designed for the Bitcoin environment. Some of the apps were created with Bitcoin analysis in mind. BitConeView[9] and BitIodine[10] are two applications that use a visual presentation to enable people investigate the Bitcoin network and study how Bitcoin transactions are executed. These kinds of apps can assist people grasp what Blockchain is all about and how a decentralised transaction works. By following transaction flows, analysis programmes can also aid in the detection of fraud and related security risks. Security is another important area for applications. CoinParty[12] and CoinShuffle [11] are two Bitcoin mixing programmes that can help the Bitcoin network become more safe by giving an extra layer of privacy for users. Because security and privacy are the most important features in a decentralised transaction environment, these types of applications and solutions are anticipated to become more prevalent in the future.

Advantages

- Cryptocurrencies are a new, decentralised money paradigm. To enforce trust and police transactions between two parties, centralised intermediaries such as banks and monetary organisations are not required in this system.
- Cryptocurrencies promise to make it easier to move funds between two parties without the use of a trusted third party such as a bank or credit card firm. Public and private keys, as well as various incentive schemes such as proof of work and proof of stake, are used to secure such decentralised transfers.[13]
- Compared to traditional money transfers, bitcoin transfers between two transacting parties are faster since they do not employ third-party intermediaries. Flash loans are a nice illustration of decentralised transfers in decentralised finance. These loans, which are not backed by security, can be completed in seconds and are employed in trading.
- Investing in cryptocurrencies can be profitable. Over the last decade, the value of cryptocurrency markets has surged to billions.

- One of cryptocurrency's most notable use cases is the remittance industry. Currently, cryptocurrencies such as Bitcoin are used as intermediary currencies to facilitate cross-border money transfers. As a result, a fiat currency is changed to Bitcoin (or another cryptocurrency), then sent across borders and converted back to the target fiat currency. This method simplifies and reduces the cost of money transfers.[14]

Disadvantages

- Despite the fact that they pretend to be anonymous, cryptocurrencies are essentially pseudonymous. They create a digital trail that can be deciphered by entities like the Federal Bureau of Investigation (FBI). This gives governments and federal agencies the ability to trace the financial transactions of regular persons.[15]
- Criminals are increasingly using cryptocurrency for undesirable operations such as money laundering and unlawful transactions. Cryptocurrencies have also grown popular among hackers who use them to spread ransomware.[16]
- Cryptocurrencies are supposed to be decentralised, with their wealth spread between multiple parties on a blockchain. In actuality, there is a lot of power in the hands of a few people. [17]
- One of the conceits of cryptocurrencies is that anyone with a computer and an Internet connection may mine them. Mining popular cryptocurrencies, on the other hand, needs a lot of energy, often as much as entire countries. Mining has become concentrated among huge corporations with revenues in the billions of dollars due to high energy prices and the unpredictability of the industry. According to an MIT research, 10% of miners are responsible for 90% of the country's mining capacity.[18]
- While cryptocurrency blockchains are extremely secure, other crypto repositories such as exchanges and wallets are vulnerable to hacking. Over the years, many cryptocurrency exchanges and wallets have been hacked, resulting in the theft of millions of dollars' worth of "coins."[19]
- Price volatility affects cryptocurrencies traded on public exchanges. Some economists regard cryptocurrencies as a passing fad or speculative bubble.[20]

CONCLUSION

Cryptocurrency is based on a decentralised transaction environment in which all transactions are recorded in a public ledger that is accessible to everybody. Blockchain's purpose is to give all of its users with anonymity, security, privacy, and transparency. These characteristics, on the other hand, present a slew of technological issues and constraints that must be addressed.More work and research, in order to get a complete picture of cryptocurrencies and all of its various aspects in order to provide the best possible policy guidance, is arguably required.

REFERENCES

[1]. Narayanan, A., Bonneau, J., Felten, E., Miller, A. &Goldfeder, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction (Princeton Univ. Press, 2016).
[2]. Yli-huumo J, Ko D, Choi S, Park S, Smolander K. Where Is Current Research on Blockchain Technology ?—A Systematic Review.PLos ONE. 2016;11(10):1–27.
[3]. Swan M. Blockchain: Blueprint for a New Economy. ª O'Reilly Media, Inc.º; 2015.
[4]. R. HOUBEN, "Bitcoin: there two sides to every coin", ICCLR, Vol. 26, Issue 5, 2015, 195.
[5]. World Bank Group (H. NATARAJAN, S. KRAUSE and H. GRADSTEIN), "Distributed Ledger Technology (DLT) and blockchain", 2017, FinTech note, no. 1. Washington, D.C.,
[6]. "Virtual Currency Schemes – a further analysis", February 2015.
[7]. "Virtual Currencies – Key Definitions and Potential AML/CFT Risks", June 2014.
[8]. Kishigami J, Fujimura S, Watanabe H, Nakadaira A, Akutsu A. The Blockchain-Based Digital Content.
[9]. Distribution System. In: Big Data and Cloud Computing (BDCloud), 2015 IEEE Fifth International Conferenceon; 2015. p. 187±190.
[10]. Di Battista G, Di Donato V, Patrignani M, Pizzonia M, Roselli V, Tamassia R. Bitconeview: visualizationof flows in the bitcoin transaction graph. In: Visualization for Cyber Security (VizSec), 2015 IEEE Symposiumon; 2015. p. 1±8.
[11]. Spagnuolo M, Maggi F, Zanero S. BitIodine: Extracting Intelligence from the Bitcoin Network. In: Christin.N, Safavi-Naini R, editors. Financial Cryptography and Data Security. vol. 8437 of Lecture Notes inComputer Science. Springer Berlin Heidelberg; 2014. p. 457±468.
[12]. Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In.Kutyowski M, Vaidya J, editors. Computer SecurityÐESORICS 2014. vol. 8713 of Lecture Notes inComputer Science. Springer International Publishing; 2014. p. 345±364.
[13]. Ziegeldorf, JH, Grossmann, F, Henze, M, Inden, N, Wehrle, K. CoinParty: Secure Multi-Party Mixing ofBitcoins. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy.CODASPY'15. New York, NY, USA: ACM; 2015. p. 75±86.
[14]. "Bitcoin: A Peer-to-Peer Electronic Cash System," Pages 1-3. Accessed Dec. 20, 2021.
[15]. Decrypt. "What Are Flash Loans?" Accessed Dec. 20, 2021.

[16]. Coinmarketcap. "Bitcoin Price." Accessed Dec. 20, 2021.
[17]. New York Times. "Pipeline Investigation Upends Idea That Bitcoin is Untraceable." Accessed Dec. 20, 2021.
[18]. National Public Radio. "How Bitcoin Has Fueled Ransomware Attacks." Accessed Dec. 20, 2021.
[19]. NBER. "Blockchain Analysis of the Bitcoin Market." Accessed Dec. 20, 2021.
[20]. Bitcoin.com. "Hackers Have Looted More Bitcoin Than Satoshi's Entire Stash." Accessed Dec. 20, 2021.