Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 4-A, pp. 1069–1079
DOI : 10.47974/JIOS-1892

Recent trends and applications in blockchain technology : The concept of monitoring over cryptocurrency

Gajanand Sharma [#]
Ravi Shankar Sharma [†]
Jitendra Kumawat [§]
Shekhar Kumar Swarnkar [‡]
Gaurav Kumar Sharma [@]
Department of Computer Science & Engineering
JECRC University
Jaipur
Rajasthan
India

Geerija Lavania *
Department of Computer Science & Engineering
Jaipur Engineering College & Research Center
Jaipur
Rajasthan
India

Abstract

Blockchain Technology is eminent in the modern era which is digitalizing the development of provinces. Contribution of the exploration is to provide adequate pilot age about secured and decentralized data exchange. In this paper we have discussed about the few application of block chain with using Bitcoin. Cryptocurrency is the future currency and it is progressing at a fast pace. For the advantage of high growth of block chain, it is also subjected to various drawback of hacking and data leaks as it's also digital so we need proper security in every user. We are proposing the solution for the associating the each of the single cryptocurrency transaction as we as the cryptocurrency purchased with the digital

[#] *E-mail:* **gajanan.sharma@gmail.com**
[†] *E-mail:* **er.ravishankarsharma@gmail.com**
[§] *E-mail:* **drkumawatjitendra@gmail.com**
[‡] *E-mail:* **shekharsn19@gmail.com**
[@] *E-mail:* **sharmag84@gmail.com**
* *E-mail:* **girija47lavania@gmail.com (Corresponding Author)**

© Taru Publications

user identify, using the concept of the block chain and for the transparency purpose we work on hashing algorithm for every users.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Blockchain, Cryptograph, Bitcoin, Decentralization, MD5, SHA512, Transparency, Immutability, Applications.*

1. Introduction

The blockchain may be a ethically sound computerized record of financial trades that can be customized to confirmation financial trades as well as fundamentally everything of critical worth .Transaction process are continuously increasing around the world and it will certainly increase difficulties, vulnerabilities, incapacity, and the cost of current transaction systems due to lot of transaction rapidly. A solution that has been developed to reduced the complexities, difficulties, Incapacity, Inefficiencies, and Current Transaction Costs The system that is called bitcoin - A digital currency [1]. A Bit coin is like currency that is use for peer to peer transaction over network this is issue by central bank. Bit coin has no central monetary authority so no one can monitor it. Therefore network become panacea tool for crypto currency hence we have maintain the utilization of bandwidth [2,3,4].When the long time transaction Bitcoin is very useful for fulfill that purpose [5]. The process of transforming a common, plain text into a twisted substance and vice versa is related to cryptography, as seen in figure 1. In addition to protecting data from loss or alteration, cryptography can be used to obtain client consent for each exchange that is recorded in a decentralized manner, as seen in figure 2.

By allotting two key for both side In any case, the more common utilize of making one of these Two Key Open, which clarifies the wording of open key cryptography [6].

"Cryptocurrency acknowledged its name since it uses encryption to really take a look at trades. This suggests advanced coding is locked in with taking care of and imparting cryptocurrency data among wallets and to public ledgers. The mark of encryption is to give security and prosperity [8].

Cryptocurrencies are the computerized monetary forms intended to supplant the customary greenbacks while occurring in our regular routines particularly for the most recent few years. Mining Cryptocurrencies are one of the famous ways of having them and create a gain because of shaky qualities on the lookout. This extra gives security and proficiency to

the PC assets of the web clients. MiNo planned and created with twofold layer assurance which makes it in front of its rivals on the lookout [7].

It appears to be a little step toward a straightforward and equitable monetary framework that is immune to dishonest and exploitative methods and techniques at all levels [9]. The results indicate that fixed size clusters operate better in terms of precision, recall, and f measure for specific time stamps than variable size clusters. The choice of innovative clustering methods when performing social network analysis can also be determined via these types of indicators [10]. [11] The method for analyzing the movement of cold and deserted wallets on the Litecoin blockchain is presented in this article.

2. Blockchain

The basis of every corporate activity is information. It will be better accepted the sooner and more precisely. Blockchain is perfect for delivering such information because it provides instantaneous, shareable, and completely transparent data that is stored on an immutable ledger and can only be viewed by people with authorization to access the network. Because members have a single understanding of the truth, you can see all the details of a transaction from beginning to end, giving you more confidence and opening up new opportunities.

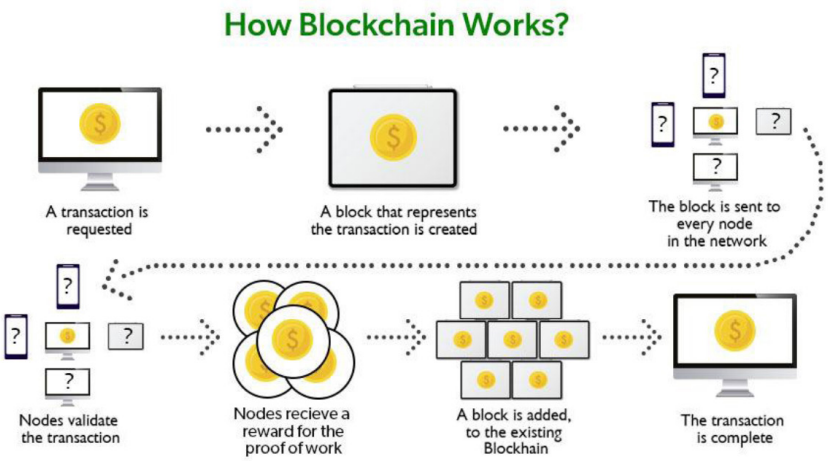


Figure 1

This Picture of Blockchain and its working process [16]

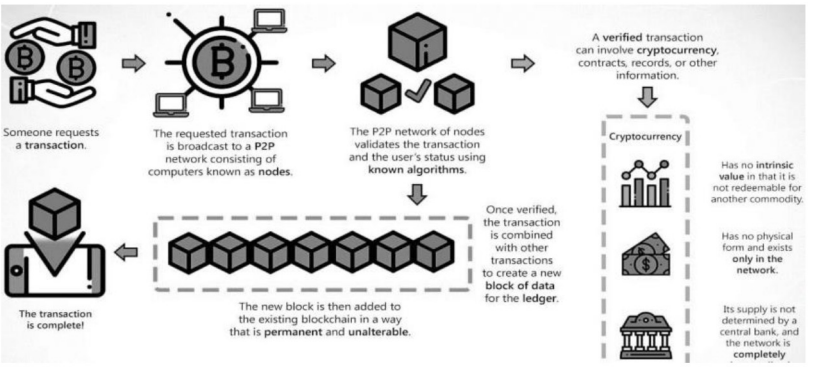


Figure 2

Working Process of Crypto Currency [17]

The verified square is added to a chain that is removed from the internet, creating an odd record with an interesting back-story. While blockchain technology maintains an open and secure ledger accessible to all participants via distributed organization, implementing adaptability across multiple mechanical divisions remains a significant difficulty. [18]. that is basically unimaginable. Bitcoin utilizes this model for financial exchanges, yet it tends to be sent from numerous points of view. The three main pillars of blockchain technology are (a) Decentralization (b) Transparency (c) Immutability

2.1 *Decentralization*

In blockchain technology different technical terminology use like Transparent, Decentralization, Miner, Consensus, Forks, Hash, Node, Timestamp [5]. In decentralization mean all participants in a Transaction have through to the same records, they can use real transactions, and after transaction it verifies identity without the need for third-party as shown in figure 3. It is like all source connected thorough network [19]. Nobody can manipulate with the information recorded on the Network even though it is unchangeable. The block chain is basic sufficient that everyone can follow the data when they need to Blockchain [12]. the comparison in between centralize and decentralize is given in figure 4.

2.2 Transparency

The identity of a person is hidden under strong cryptography and it is only reflected by the public speech [7]. If you try looking up a person's



Figure 3

Decentralize Network

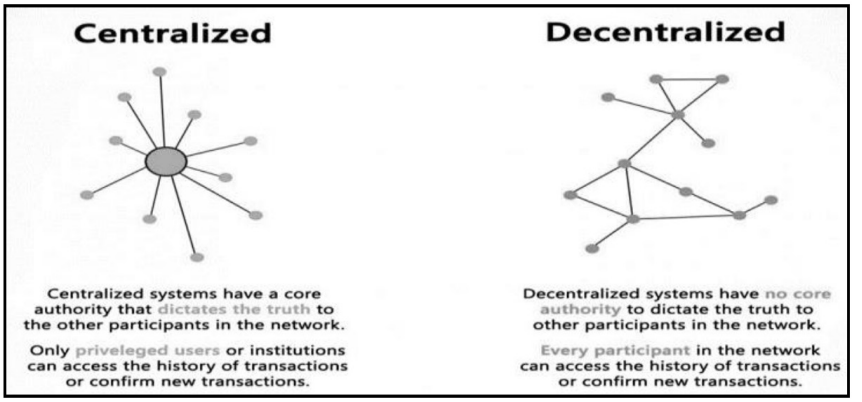


Figure 4

Comparison in between centralize and decentralize [20]

recent transactions, you would see "1MF1bhsFLkBzzz9vpFYEmvw T2TbyCt7NZJ gave 1 BTC" instead of "Bob sent 1 BTC."

2.3 *Immutability*

Unchanging nature, within the setting of the Blockchain, implies that once something has been entered into the Blockchain, not conceivable to evacuate .only can create new transaction for remove the error the both transaction will visible to everyone.

3. Agreement Calculation

It realized that Blockchain is a circulated decentralized organization that gives changelessness, protection, security, and straight forwardness. There is no focal position present to approve and confirm the exchanges, yet every exchange in the Blockchain is viewed as totally got and checked. This is conceivable simply because of the presence of the agreement convention which is a center piece of any Blockchain organization [12]

4. Applications of Blockchain Technology

There are various demanding and authentic applications of blockchain technology which are discussed below.

4.1 *Smart Contracts*

A smart framework is a contract of procedures that carry out a contract's terms. It's created in byte code and finished in a Blockchain environment. Smart Contracts can help solve problems like strategic default and drastically reduce verification and actuation costs. Smart Contracts have a variety of blockchain applications, including contract management, entertainment, and healthcare.

4.2 *Blockchain Internet-of-Things*

The Internet of Things (IoT) is a network of connected smart devices to the connectivity, engineering and internet machines, things, organisms, or citizens that also are given with provided with unique identifiers to exchange information without requiring human-to-human or human-to-computer communication using sensing devices, embedded software, and a shared language. The issues highlighted are addressed by blockchain technology, which improves the interconnection of IoT. Its network will allow devices to operate easily, safely, and autonomously by implementing 8 Smart Contracts that are only activated when particular prerequisites are achieved [5].

4.3 *Sharing Economy*

Sharing economy organization strategies have become extremely prevalent, resulting in some of the most successful firms in the previous 10 years. Blockchain is a technology to disrupt these organizations because it gives advanced capabilities for automating and giving consumers control back by democratizing the settlement process. Most previous studies have concentrated on blockchain technology or the collaborative economy. It's obvious that the sharing economy is a successful business idea. This trust in a sharing economy company's brand is critical because it increases the likelihood that customers will also trust the platform's providers.

4.4 *Governance*

All of a state's governing actions are considered to as administration. Many issues challenge present government, including such privacy

protection, food standards, and elections, to mention few of. Decentralization, blockchain based, and integrity, among many other Blockchain features, can help solve these problems. The government uses Blockchain technologies to ensure food security by the use of an intelligent farmer marketplace application. This program interconnected farmers to markets, kept accurate records of production, and grunted transport. This users can add that food is safe and of high value.

4.5 *Prediction Market*

The market's belief in the result of an uncertain event is reflected in the price of a prediction market contract. The contract is normally set up as a binary option, meaning it'll either terminate at a price or 0% or 100%. Participants trade contract whose payoffs are associated to the a future event in economic models, leading in prices which can be regarded as marketplace aggregate estimates. Predictions systems have previously been shown to provide accurate forecasts, even sometimes superior than advanced statistical techniques. Predictions marketplaces have indeed been widely employed inside the predictions of election, program management, product quality, and event impact due to its benefits. Prediction markets, on the other hand, have several drawbacks, such as poor anonymity and little market liquidity. Second, we show how to create smart contract-based prediction markets. After that, a contract implementation algorithm has been proposed. Finally, an interpersonal and inter prediction market based on a blockchain System is built to verify the algorithm's efficiency. The experimental results reveal that the market can accurately predict the certain event. Therefore, Blockchain's autonomy, self-sufficiency, and decentralized objective is to produce betting markets more effective and accurate There could be a deadly bug in the bit coin programmed. According to [15], a frequency-domain symmetric image encryption scheme using Karhunen-Loeve Transform and AES achieves lossless decryption and outperforms existing methods in quality and security based on statistical tests.

5. Bitcoin/Cryptocurrency

Block information, hashes, and data make up the three core components of the blockchain network's block architecture. Data communication is structured and directed differently for each type of node [13]. Since the programming language used in the inputs and outputs script is flexible, it can be used to create a variety of transaction types. One

way to use bitcoin to improve an already-existing financial and authentication service is through a bitcoin contract. A popular choice is to create the contract using a script that has a multiple-signature system called multiuser. Although the scripts are used to address a range of bitcoin problems, the chance of a transaction being set up wrongly has climbed as the sophistication of the scripts has increased. Since the unlocking script cannot be written when the locking script is specified improperly, no one can use a Bitcoin. The accuracy of a transaction's script can be checked using research that provides models of bitcoin contract-type transactions. The Bitcoin convention is based on the blockchain. Satoshi Nakamoto, the anonymous creator of Bitcoin, made reference to it as "another electronic money framework that is completely distributed, with no confided in outsider." Nobody has any restrictions on Bitcoin. When everything else is equal, a group of PCs verifies Bitcoin transfers. When someone pays for something using Bitcoin, PCs on the Bit coin network compete to check the transaction. The discussion of factors influencing visibility and their implications for the construction sector forms the paper's conclusion [14]. Bitcoins use a distributed conceptual model to document trades and issue new units, rather than relying on a central giving or coordinating power [7].

6. Conclusion

As forward-thinking as it may appear, Blockchain is tools that may help everyone reach the highest level of transparency. Missed trades, errors made by humans or machines, and trades that are executed without the parties' consent will all be eliminated. However, the most basic use of Blockchain technology is to verify the authenticity of an exchange by recording it on a primary register and a transmitted arrangement of registers that go along with it, all connected by a safe approval process. A blockchain has accelerated transactions by doing away with the need for a server and a central authority and allowing users to share transaction records and, in the end, authorize transactions using peer-to-peer network technology. The blockchain is a distributed system that makes use of peer networks and processing power. Technological techniques such as proof of work and proof of stack have been developed to bolster blockchain security. [13] Although blockchain security is continually getting better, flaws are still being found, and security research is continuing. An attacker makes many attempts to obtain a user's personal key stored on their computer or smartphone in order to hack bitcoin. A blockchain has

removed the need for a server and a central authority, sped up transactions, and allowed participants to share transaction records and, lastly, authorize transactions via peer-to-peer network technology. The blockchain is a distributed system that makes use of computer resources and peer networks. To improve the security of blockchain, technical techniques such as proof of work and proof of stack have been developed. The remaining data can be utilized to estimate the user information if the user data is not erased but rather left behind. In order to offer security, this research examined how to use a secure blockchain usage and removal mechanism. Efficiency studies seem to be necessary given the setting in which a significant amount of data is transferred. The goal of this research is to look into the issues and solutions that are needed in the field of cryptocurrency security. We can identify the issues with the current cryptocurrency framework, in which the user's identity is not linked to the cryptocurrency. To propose a cryptocurrency model that will associate each transaction's currency with the user's identity, allowing the digital identity code to uniquely trace the currency transaction. The Blockchain Market Engineering Framework serves as a roadmap for future IS research and aids practitioners and researchers in their efforts to recognize significant ideas in blockchain-based economic systems. However, these fundamental ideas should not be restricted to only a few components of our framework but should also take into account the interdependences, interactions, and reciprocal relationships between the many components.

Reference

[1] R. Vadapalli, *Blockchain Fundamentals*. UAE: Blockchain Prep, . ISBN: 301.345.908 (2020).

[2] V. Arya, "Multicast routing protocol for mobile ad hoc networks: A review," *La Pensée*, vol. 51, no. 2, pp. 116–126 (2021).

[3] V. Arya, *Image Compression Techniques Using MATLAB: Lossy, Lossless and Hybrid Image Compression Algorithms*. LAP LAMBERT Academic Publishing (2020).

[4] G. Sharma, A. Kumar, N. Gour, A. K. Saini, A. Upadhyay, and A. Kumar, "Cognitive framework and learning paradigms of plant leaf classification using artificial neural network and support vector machine," *J. Exp. Theor. Artif. Intell.*, vol. 36, no. 4, pp. 585–610 (2022), doi: 10.1080/0952813X.2022.2096698.

[5] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE PerCom Workshops on Security Privacy and Trust in the Internet of Things* (2017).

[6] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, pp. 473–478 (2018), doi: 10.1109/ICOIN.2018.8343163.

[7] G. Sharma, A. Kumar, N. Gour, A. K. Saini, A. Upadhyay, and A. Kumar, "Cognitive framework and learning paradigms of plant leaf classification using artificial neural network and support vector machine," *J. Exp. Theor. Artif. Intell.*, vol. 36, no. 4, pp. 585–610 (2022), doi: 10.1080/0952813X.2022.2096698.

[8] Mohammed Almukaynizi, Abhishek Dubey, Anupam Joshi, and Tim Finin, "Finding cryptocurrency attack indicators using temporal logic and darkweb data," in *Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI)*, pp. 91–93 (2018).

[9] M. Azman and K. Sharma, "HCH DEX: A secure cryptocurrency e-wallet & exchange system with two-way authentication," in *Proc. Int. Conf. Smart Syst. Invent. Technol. (ICSSIT)*, pp. 305–310 (2020).

[10] S. Sharma and A. Jain, "Dynamic social network analysis and performance evaluation," *Int. J. Intell. Eng. Inform.*, vol. 7, no. 2/3, pp. 180–202 (2019).

[11] A. S. Khadzhi, S. V. Zareshin, and O. V. Tarakanov, "A method for analyzing the activity of cold wallets and identifying abandoned cryptocurrency wallets," in *Proc. IEEE Conf. Russian Young Res. Electr. Electron. Eng. (EIConRus)*, pp. 1974–1977 (2020).

[12] A. Kumar, H. Sharma, S. Mathur, D. Sharma, G. Khandelwal, and G. Sharma, "Computer vision, machine learning based monocular biomechanical and security analysis," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 3, pp. 685–693 (2023), doi: 10.47974/JDMSC-1741.

[13] Y. M. Arif, H. Nurhayati, F. Kurniawan, S. M. S. Nugroho, and M. Hariadi, "Blockchain-based data sharing for decentralized tourism destinations recommendation system," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 6, pp. 472–486 (2020).

[14] S. Hamledari and M. Fischer, "Measuring the impact of blockchain and smart contracts on construction supply chain visibility," *Adv. Eng. Inform.*, vol. 50, 101444 (Oct. 2021).

[15] S. Rashaideh, A. Shaheen, and S. N. Al-Najdawi, "Real-time image encryption and decryption methods based on the Karhunen–Loève transform," *Int. J. Intell. Eng. Inform.* (2019).

[16] Y. Okazaki, "Unveiling the potential of blockchain for customs," *WCO Res. Paper*, no. 45, pp. 1–24 (2018).

[17] B. Sakız and A. H. Gencer, "Blockchain beyond cryptocurrency: non-fungible tokens," in *Int. Conf. Eurasian Econ.*, pp. 154–161 (Aug. 2021).

[18] W. Wang, F. Lumineau, and O. Schilke, *Blockchains: Strategic Implications for Contracting, Trust, and Organizational Design*. Cambridge University Press (2022).

[19] Sanjana Dubey, Rahul Biswas, Rachana Ghosh, Sudip Ghosh, Subham Chatterjee, Manish Jindal, and Shibu Sasidharan, "Psychosocial impact of COVID-19," *Diabetes Metab. Syndr. Clin. Res. Rev.*, vol. 14, no. 5, pp. 779–788 (2020).

[20] Y. Chen, J. I. Richter, and P. C. Patel, "Decentralized governance of digital platforms," *J. Manage.*, vol. 47, no. 5, pp. 1305–1337 (2021).

Received October, 2024