iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.43742

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Implementation and Analysis of Cryptocurrency

Sowmiya L[1], Keerthana D[2], Mahalakshimi L[3], Ramya A[4]
[1, 2, 3, 4]*Info Institute of Engineering*

Abstract: A crypto currency is a digital currency mainly based on blockchain technology. The use of virtual currency has become widespread in many different systems in recent years. Virtual money is not fully controlled and regulated hence most of the countries have not admitted this currency in their economic activities. The project aims to understand the basic concepts of cryptocurrency, how they works , analyze the different type of crypto at market and the hardship they face . We will be also trying to use this knowledge to create a small prototype of a crypto system.

I. INTRODUCTION

Cryptocurrency is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it.They are , an encrypted, peer-to-peer network for facilitating digital barter, is a technology developed nine years ago. Bitcoin, the first and most popular cryptocurrency, is paving the way as a disruptive technology to long standing and unchanged financial payment systems that have been in place for many decades. Lets see the original idea and motivation, the mode of operation and possible applications of cryptocurrencies, and blockchain technology.

II. EXISTING SYSTEM

1) Bitcoin
2) Ethereum
3) XRP
4) LiteCoin
5) Lkadot
6) Stellar
7) Monero

III. DISADVANTAGES OF EXISTING SYSTEM

1) Scalability
2) Cybersecurity Issues
3) Price Volatility
4) Lack of Inherent Value
5) No Regulations

IV. PROPOSED SYSTEM

1) In the proposed system, centralized intermediaries, such as banks and monetary institutions, are not necessary to enforce trust and police transactions between two parties.
2) Because they do not use third-party intermediaries, cryptocurrency transfers between two transacting parties are faster as compared to standard money transfers.
3) Flash loans in decentralized finance are a good example of such decentralized transfers. These loans, which are processed without backing collateral, can be executed within seconds and are used in trading.

V. ADVANTAGES OF PROPOSED SYSTEM

1) Transaction Cost
2) Private Transactions
3) Scalability and Performance
4) Interoperability and Open Source

©IJRASET: All Rights are Reserved

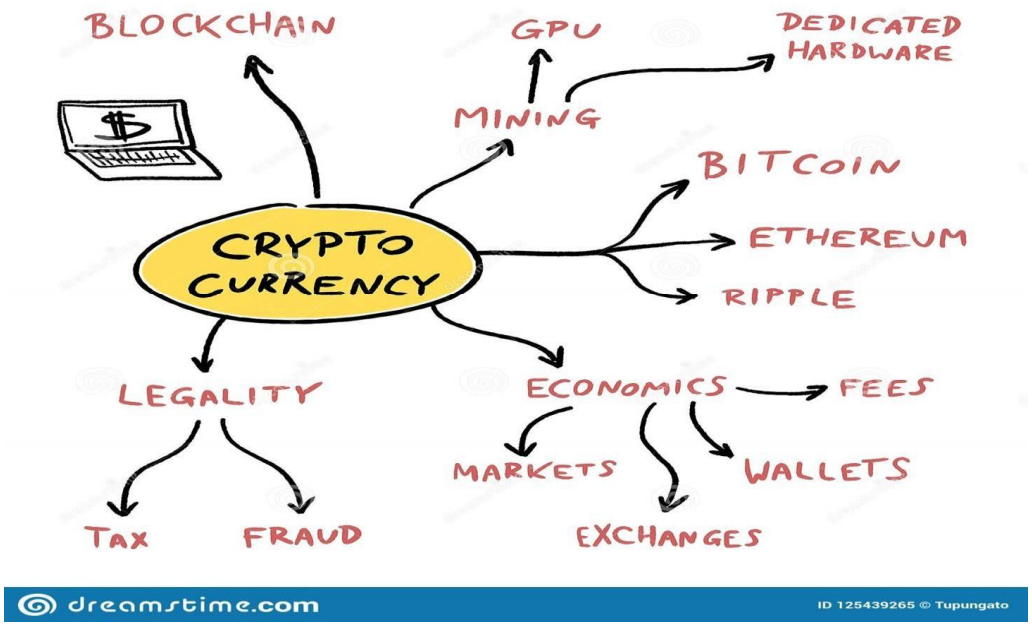
VI. LITERATURE REVIEW

After the global economic disaster of 2008, public agree with in traditional banking structures turned into a concern. maximum in particular, the first signs of financial turmoil seemed on March 16, 2008, while undergo Stearns and Lehman Brothers declared financial disaster (Wilson, 2019). The shock's ramification did now not prevent at these establishments; as an alternative, the debt contagion persevered to unfold and hit different economic powerhouses such AIG, the financial institution of america, Citigroup, JPMorgan Chase, Goldman Sachs, and Morgan Stanley. past the usa, the global economic crisis additionally spread to Europe and Asia. for instance, following the disaster, Finland pronounced decreases in business manufacturing, personal investments, and exports (Söderlund & Kestilä-Kekkonen, 2014). In China, maximum economic institutions and foreign banks were suspended and then stopped recruiting staff (Marquez-Velazquez, 2010). Banks mentioned a sizeable scarcity of liquidity after shadow banks had financed themselves the use of quick term unsecured or collateralized marketplace borrowing (Milne, 2018). At a global level, the recognition of banks and different financial establishments (e.g., insurance organizations) become tarnished in the public eye. inside the aftermath of the 2008 global economic crisis, an unknown man or woman, group, or business enterprise operating beneath the pseudonym 'Satoshi Nakamoto' added an electronic peer-to-peer system primarily based on the cryptocurrency bitcoin (Nakamoto, 2008). Bitcoin is a decentralized digital currency delivered in 2008 and deployed at the beginning of 2009. It got here as a response to the financial institutions that often privatize profits and socialized losses (Lerer & McGarrigle, 2018). A giant impetus in the back of the introduction of cryptocurrencies became the need to create a machine that allowed quick and cheap transactions without the intermediation of any trusted 1/3 events (e.g., banks) (Bação et al., 2018; Chapron, 2017; Kfir, 2020; Kolber, 2018; Sudzina, 2018). similarly, many scholars, fans, and futurists do not forget bitcoin a future alternative for kingdom-issued foreign money (Bouri et al., 2018; Bouri et al., 2017; Hong, 2017). because the bitcoin release, greater than 1,600 cryptocurrencies have entered into movement (Wilson, 2019). past the hype, cryptocurrencies are currently used to shop for real goods and actual offerings within the actual world (Dostov & Shust, 2014; Guadamuz & Marsden, 2015). Cryptocurrencies present a full-size shift faraway from the traditional layout, control, and law of financial systems (Shahzad et al., 2018). The technology at the back of the proliferation of cryptocurrencies is blockchain (Hashemi Joo et al., 2019; Lu et al., 2019; Searing & MacLeod, 2019). Blockchain era is described with the aid of Treiblmaier (2018) as "a virtual, decentralized and dispensed ledger wherein transactions are logged and delivered in chronological order to create everlasting and tamper-proof records." Blockchain generation is based on peer-to-peer connectivity and cryptographic safety, permitting a decentralized approach with better transparency and accept as true with as opposed to the centralized and opaque nature of traditional economic systems. Briere et al. (2013) opined that cryptocurrencies, especially bitcoin, are new financial devices and opportunity investments with diversification benefits. Many cryptocurrencies are used as a medium of change for daily payments, and they inherently have similar traits to other financial markets, in particular valuable metals (Omane-Adjepong et al., 2019). Blockchain generation has attracted massive interest from important banks and international retail banks (Dashkevich et al., 2020; Polasik et al., 2015). Many monetary establishments capitalise on blockchain to set up economic technology (often called FinTech) startups to leverage blockchain in handing over financial services and underpin cryptocurrencies (Milne, 2018). This paper strives to investigate the function and significance of cryptocurrencies in contemporary-day transactions and economic systems. a narrative literature assessment is conducted to synthesize earlier research on cryptocurrencies from the finance angle. no matter recent tries to apprehend the phenomenon of cryptocurrencies, there is nevertheless a loss of scholarly insights that examine cryptocurrencies' opportunities and challenges in contemporary economic systems. for instance, Flori (2019) makes a comprehensive assessment of the economic programs of cryptocurrencies. despite the fact that, the scope of his examine is narrowly focused on bitcoin. Chohan (2017) performed a thematic overview on cryptocurrencies. however, numerous points in Chohan's research continue to be theoretically unexplored and conceptually unelaborated, inclusive of the challenges of cryptocurrencies within the economic ecosystem. additional opinions have been published currently, addressing the connection among privacy and cryptocurrencies (Harvey & Branco-Illodo, 2020; Herskind et al., 2020). however, they lack a complete analysis of different elements influencing the uptake of cryptocurrencies in the economic atmosphere. consequently, the study's novelty resides in imparting a more balanced and more in-intensity expertise of the possibilities and demanding situations delivered about by the use of cryptocurrencies in finance. This take a look at will fill inside the modern-day gap in the literature concerning the shortage of comprehensive evaluation of cryptocurrencies from the finance perspective. furthermore, enterprise and finance researchers are nevertheless unusual with the brand new possibilities these rising digital monetary contraptions can offer to individuals, businesses, and economic establishments (Charfeddine et al., 2020). The studies additionally identified a lack of reviews focusing at the opportunities and challenges of cryptocurrencies in present day finance. This take a look at is one of the first tries towards understanding the function of cryptocurrencies in reshaping and disrupting present day monetary structures.

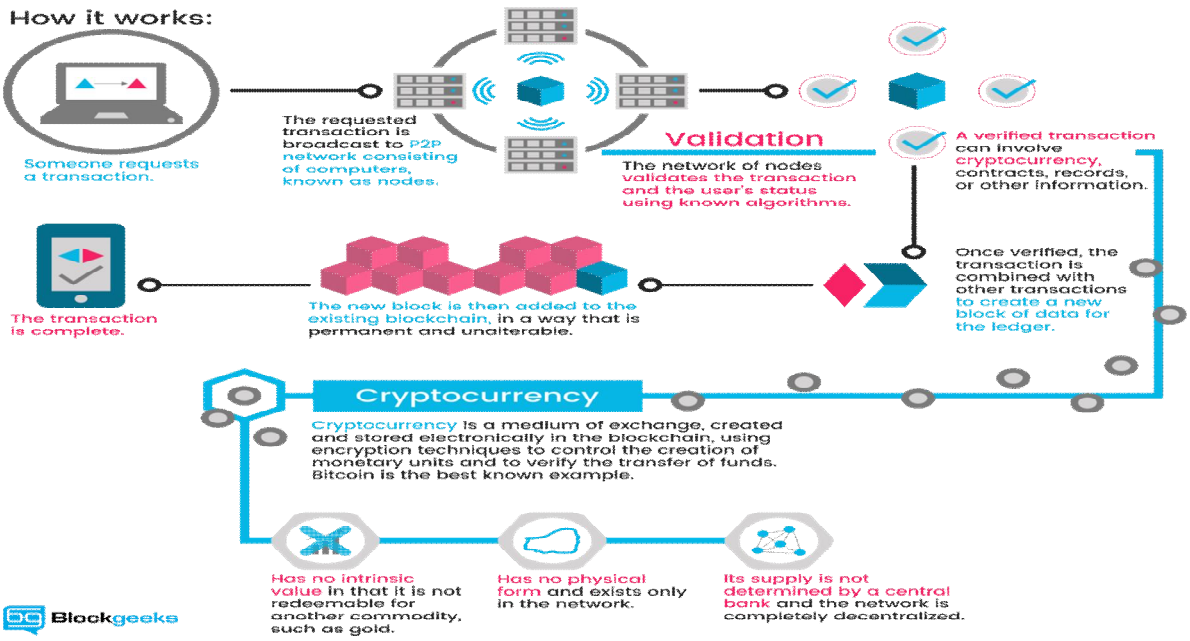
©IJRASET: All Rights are Reserved

We argue that by way of clarifying what cryptocurrencies are, how they paintings, and the way they can be used, we increase the modern literature, which remains significantly inconclusive and poor concerning the a long way-accomplishing opportunities of cryptocurrencies in contemporary financial systems. accordingly, our studies objectives will solution the subsequent studies query "what are the opportunities and challenges of cryptocurrencies in cutting-edge finance? This have a look at offers numerous contributions. Dorfleitner & Lung (2018) record that the popularity of cryptocurrencies in the monetary context has been marked with the aid of exponential marketplace extent growth. We also make contributions to this literature through a timely evaluation, and we upload to the controversy by way of scrutinizing the topics mentioned in the cryptocurrencies literature.

VII. FLOW CHART



VIII. SYSTEM ARCHITECTURE



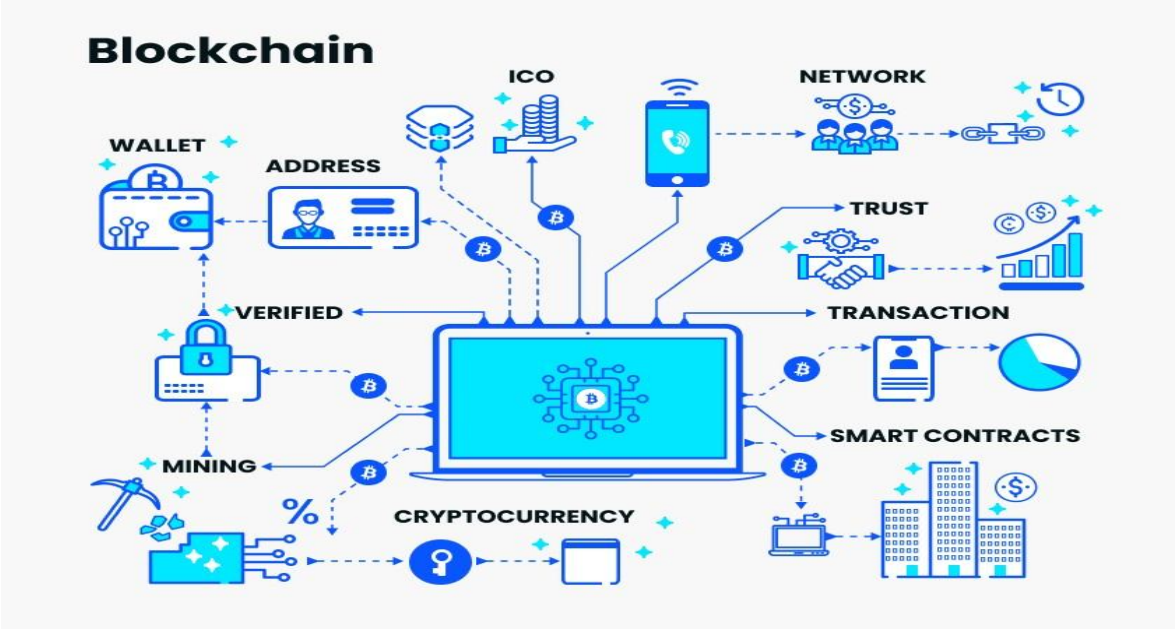
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

IX. REQUIREMENT

1) Front-end - HTML, Javascript, Ajax
2) Styles - css, Bootstrap
3) Language - php
4) Back-end - Mysql Softwares Used - WAMP/XAMPP/LAMP
5) Note:Currently suggested framework – Solidity

X. MODULES

- Hash
- HMAC
- Cipher
- Decipher
- Sign
- Verify



A. Blockchain

The validity of each cryptocurrency coins is supplied by way of a blockchain. A blockchain is a constantly developing listing of statistics, referred to as blocks, which can be related and secured using cryptography. every block normally includes a hash pointer as a hyperlink to a previous block, a timestamp and transaction information. by layout, blockchains are inherently proof against modification of the data. it is "an open, allotted ledger that may report transactions between two events successfully and in a verifiable and everlasting manner". for use as a dispensed ledger, a blockchain is commonly controlled by using a peer-to-peer community together adhering to a protocol for validating new blocks. as soon as recorded, the records in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the community majority.

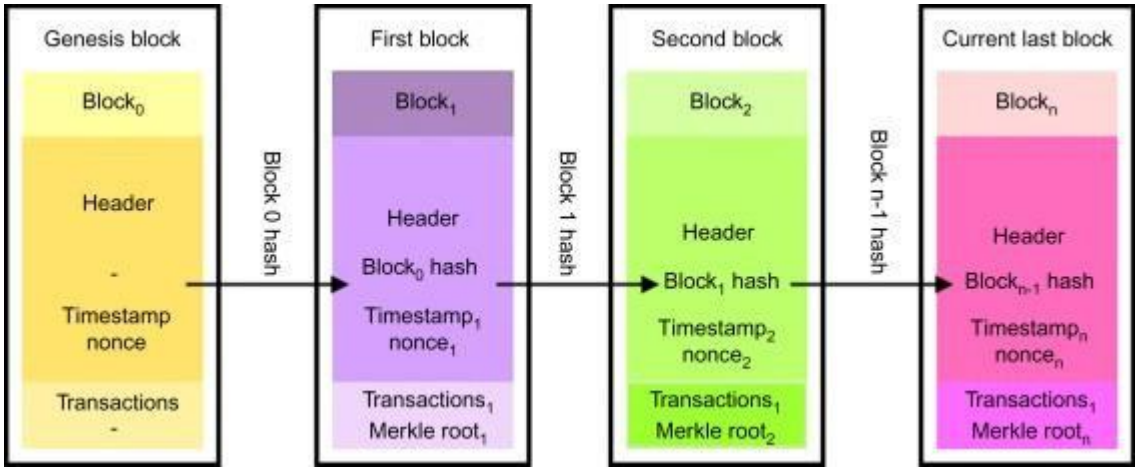
B. Nodes

within the international of cryptocurrency, a node is a computer that connects to a cryptocurrency network. The node supports the applicable cryptocurrency network thru either relaying transactions, validation or web hosting a replica of the blockchain. In terms of relaying transactions every network pc (node) has a replica of the blockchain of the cryptocurrency it supports, when a transaction is made the node growing the transaction broadcasts information of the transaction the use of encryption to other nodes all through the node community so that the transaction (and every other transaction) is understood.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Timestamping

Cryptocurrencies use various timestamping schemes to "show" the validity of transactions introduced to the blockchain ledger with out the want for a relied on third party. the primary timestamping scheme invented was the evidence-of-work scheme. The most broadly used proof-of-paintings schemes are based totally on SHA-256 and scrypt.



D. Mining

In cryptocurrency networks, mining is a validation of transactions. For this effort, successful miners reap new cryptocurrency as a reward. The praise decreases transaction costs through growing a complementary incentive to make contributions to the processing electricity of the network. The rate of producing hashes, which validate any transaction, has been expanded by using specialized machines together with FPGAs and ASICs walking complex hashing algorithms like SHA-256 and scrypt.

E. GPU fee rise

An boom in cryptocurrency mining increased the demand for photographs cards (GPU) in 2017.popular favorites of cryptocurrency miners such as Nvidia's GTX 1060 and GTX 1070 photos playing cards, in addition to AMD's RX 570 and RX 580.

F. Wallets

A cryptocurrency wallet stores the public and private "keys" (address) or seed which may be used to acquire or spend the cryptocurrency. With the private key, it's miles possible to write in the public ledger, efficiently spending the related cryptocurrency. With the public key, it is feasible for others to ship foreign money to the pockets.

G. Anonymity

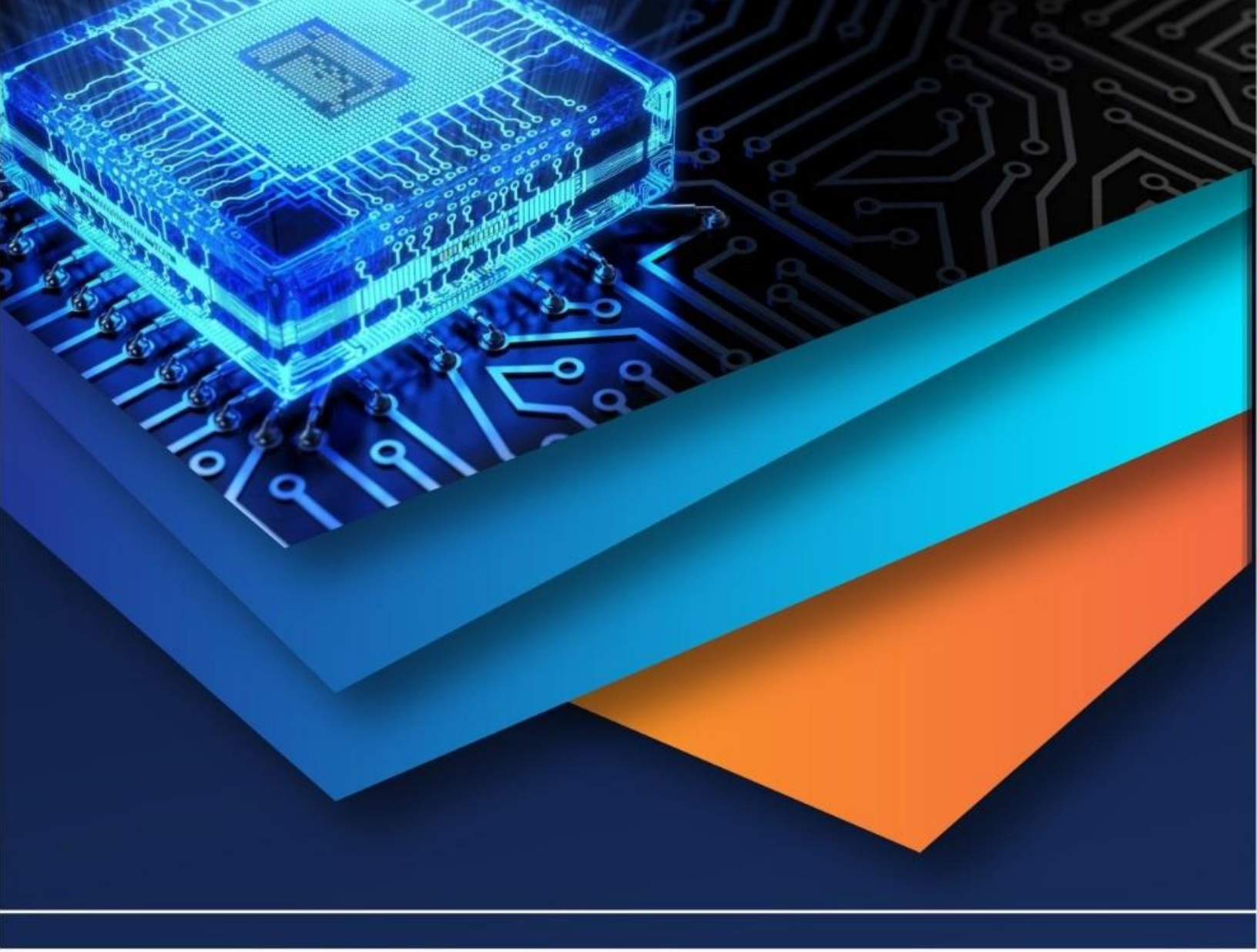
Bitcoin is pseudonymous rather than anonymous in that the cryptocurrency inside a pockets isn't always tied to people, however alternatively to one or more precise keys (or "addresses"). Thereby, bitcoin owners are not identifiable, but all transactions are publicly available inside the blockchain. nevertheless, cryptocurrency exchanges are often required via regulation to gather the non-public records of their users.

XI. CONCLUSION

On this paper, we aimed to create a very cozy and Decentralised system .The challenge might be evolved with Its pockets and this wallet may be integrated with different CryptoCurrencies like DeFi, NFT, software Tokens, shop cost Tokens which will be utilized by all form of traders and buyers.

REFERENCES

[1] https://www.researchgate.net/publication/353887034_A_STUDY_ON_CRYPTOCURRENCY_IN_INDIA
[2] https://ijirt.org/master/publishedpaper/IJIRT153630_PAPER.pdf
[3] https://docs.ie.edu/cgc/research/cryptocurrencies/CGC-Cryptocurrencies-and-the-Future-of-MoneyFull-Report.pdf
[4] https://www.ibm.com/docs/en/datapower-gateway/10.0.1?topic=apis-crypto-module



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)