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.2022.44931

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

Blockchain Difficulties and Valuable Open Doors: A Study

Pankaj Rajani[1], Prof. Divakar Jha[2]
[1]*LBHSSTICA-MCA, Mumbai, INDIA*
[2]*Mentor*

Abstract: ***Blockchain One of the hottest technologies in the market but what exactly the blockchain is . – A blockchain is a digital transaction of records that is organized in pieces of information called blocks. These blocks connect with each other through a cryptographic validation known as a hashing function. These blocks when are connected together form a structure of solid chain - a blockchain. As of now, the blockchain technology has touched many of the fields like financial services, Internet of things , Digital identities, social media etc However, as all things in the world have pros and cons blockchain is also having some cons which are not been addressed till date and since it is an emerging technology , there are some areas in which blockchain technology still needs to be discovered and how these can be used in those fields to have an outlast benefits of the technology. In this paper , our aim is to give the overall picture of the blockchain , how it works what are the challenges of the technology and what are the opportunities that can be explored in the blockchain field.***
Keywords: Blockchain, Cryptocurrencies, Bank Services, Centralized System, Decentralized System

I. INTRODUCTION

Blockchain is the technology which is been used widely in today's modern digital currency. With the help of blockchain a new currency was introduced in the market known as Bitcoin (The digital cryptocurrency) .

There is a myth circumventing that Bitcoin rises to Blockchain. Indeed, that is wrong. It is frequently reffered to as exactly the same thing. Bitcoin is cryptocurrency, digitized cash, that is permitted and held alive because of the technology called Blockchain . At the point when Blockchain technology started to exist, the primary application that was tried on the stage was Bitcoin. Bitcoin was first proposed in 2008 and executed in 2009 by Satoshi Nakamoto.

Till now bitcoin is having huge demands on the market. Many companies saw the boom in the market and have already started investing in blockchain technology. Recently,

Top big MNC's have started investing in blockchain technology. But exactly what is the blockchain technology?

Blockchain is essentially a sequence of blocks that save all committed transactions with the use of a public ledger . Blockchain works in a decentralized environment that consists of several core technologies, such as distributed consensus algorithms ,digital signatures, cryptographic hash. Each and every one of the transactions happen in a decentralized way that wipes out the necessity for any middle people to approve and confirm the transactions. Each transaction will be secured through cryptography and later all the transaction history will be grouped and stored as blocks of data. The great advantage of blockchain is that it can store any kind of asset, its ownership details, history of the ownership and location of assets in the network. Whether it is the digital currency bitcoin, or any other digital assets like a certificate, personal information, a contract, title of ownership of IP, even the real-world objects.

II. BLOCKCHAIN ARCHITECTURE

Before we understand how the blockchain works and how the transactions take place , we need to understand that how the block chain looks like and

What things are inside the block .

Below is brief explanation of about blockchain and how it looks like

A Block chain is the chain of the data which holds a complete list of transaction records like conventional public ledger.

Below is the figure of how the block chain looks like

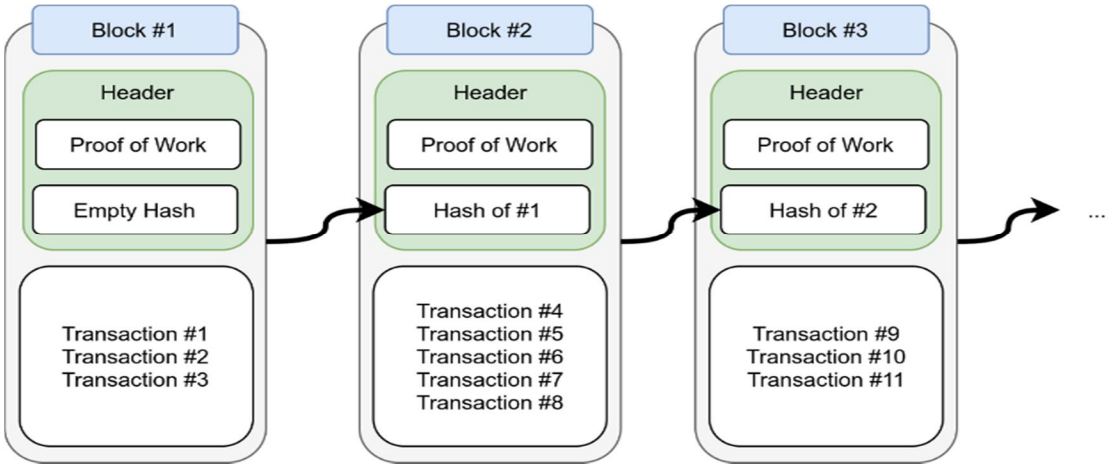


Figure 1 : An glimpse of the blockchain

A. Blockchain Explanation

Above figure depicts how a blockchain looks like

The first block is called the Genesis block because that block doesn't have any hash value of any previous block. The blockchain is extended by each additional block and hence represents a complete ledger of the transaction history .The blocks next added to the chain will have the hash value of the previous block so that chain can be made and if there is any discrepancy in the hash value . That block will not be added to the blockchain and chain will reject that block.

B. Block

Each block in the blockchain contains block header and the block body as shown in Figure 1. In particular, the block header includes:

1) Block version: shows which set of block validation rules to adhere to.
2) Parent block hash: a 256-bit hash value that points to the previous block.
3) Merkle tree root hash: the hash value of all the transactions in the block.
4) Timestamp: current timestamp as seconds since 1970-01-01T00:00 UTC.
5) nBits: current hashing target in a compact format.
6) Nonce: a 4-byte field, which usually starts with 0 and increases for every hash

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism to validate the authentication of transactions (NRI, 2015). A digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.

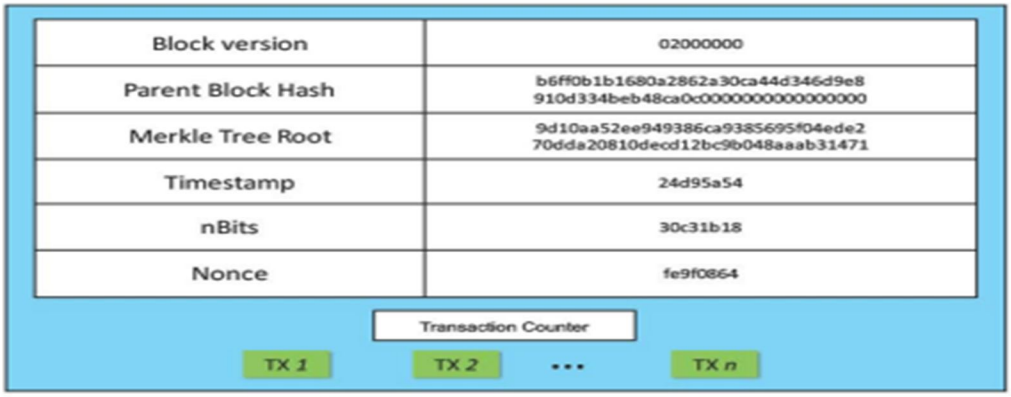


Figure 2: Block body

C. *Blockchain Transaction Process*

Blockchain technology is mostly about the transactions that we make digitally for ourselves. Eventually, these transactions make their way to the various blocks that become part of the Blockchain later on. So, it is important to understand the transaction life cycle in Blockchain technology.

This lifecycle follows the journey of a single transaction as it makes its way through each stage in the process of joining the blockchain. Transaction in simple words is the process of sending money by the sender and the receiver receiving it. The Blockchain transaction is also quite similar, but it is made digitally.

Let us understand the various stages in a blockchain transaction life cycle with the help of an example.

Sourav and Suraj are two Bitcoin users. Sourav wants to send 1 bitcoin to Suraj.

1) First, Sourav gets Suraj's wallet address (a wallet in the blockchain is a digital wallet that allows users to manage their transactions). Using this information, he creates a new transaction for 1 bitcoins from his wallet and includes a transaction fee of 0.003 bitcoin.

2) Next, he verifies the information and sends the transaction. Each transaction that is initiated is signed by a digital signature of the sender that is basically the private key of the sender. This is done in order to make the transaction more secure and to prevent any fraud.

3) Sourav's wallet then starts the transaction signing algorithm which signs his transaction using his private key.

4) The transaction is now broadcasted to the memory pool within the network.

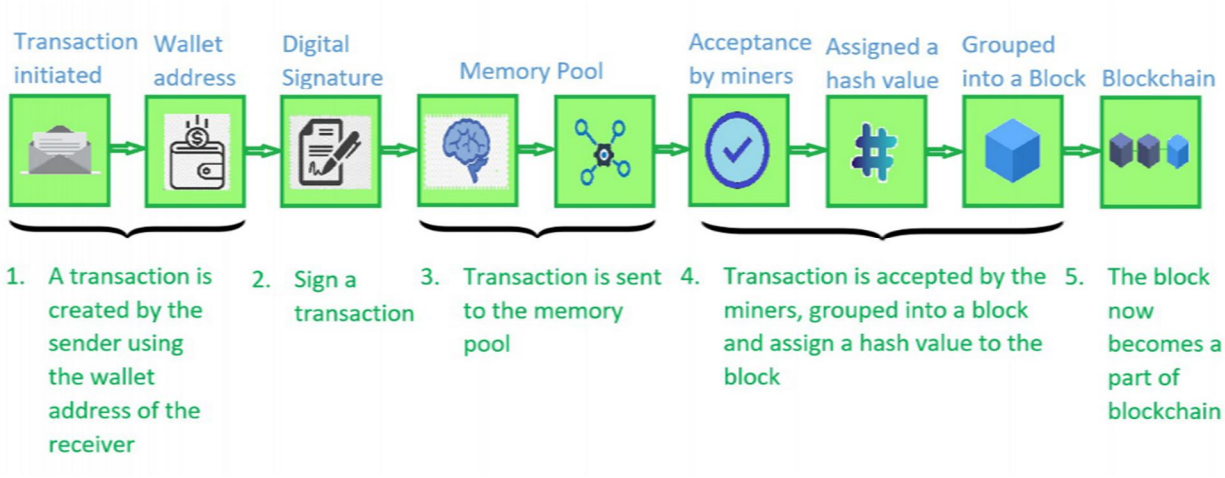
5) This transaction is eventually accepted by the miners. These miners, group this transaction into a block, find the Proof of Work, and assign this block a hash value to be mapped into the blockchain.

6) This block is now placed on the Blockchain.

7) As this block gains confirmation, it is accepted as a valid transaction in the network.

8) Once this transaction is accepted, Suraj finally gets his bitcoin.

The below diagram is a pictorial representation of the various stages in a transaction life cycle as discussed above.



III. KEY FEATURES OF BLOCKCHAIN

Many features make blockchain the superstar of security in keeping data without the need for trusted intermediaries and create a decentralized financial infrastructure. Blockchain has the following features:

1) *Decentralization:* A transaction in the decentralized network can be done between any two peers without a central authority. This reduces server costs and prevents the bottlenecks from the central server.

2) *Persistency:* Since the validation process is done on both transaction and block levels, it detects any tamper where each node of the network has a copy of the blockchain.

3) *Anonymity:* Blockchain is often described as anonymous, because the user is permitted to send and receive money without giving any personally identifying information, but only generation of one or more address.

4) *Auditability:* Since each block in the blockchain stores a list of transactions, a timestamp for validation and creation, and the hash of the previous block, users can easily verify and trace each transaction that is stored in the blockchain.

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

IV. POSSIBLE OPEN DOORS

The blockchain technology can be explored more in the fields but in the study it is defined to five fields Section 4.1 as Blockchain Testing ,
Section 4.2 as Stopping the tendency of the centralization Section 4.3 as Big Data analytics Section 4.4 as Artificial Intelligence

A. Blockchain Testing

As blockchain technology is still relatively new in the tech world, it has not seen widespread adoption among software developers and lacks of a more of the professional expertise. There are many blockchains in the market which can not be in upto mark in terms of the quality . Unlike the professional software development in which the software needs to be passed through all the phases of the lifecycle , blockchain lacks in terms of testing . The testing phase can be divided into 2 phases
Standardisation phase:In this phase, all criteria have to be made and agreed. When a blockchain is born, it could be tested with the agreed criteria to valid if the blockchain works fine as developers claim.
Testing phase: As for testing phase, blockchain testing needs to be performed with different criteria. For example, a user who is in charge of online retail business cares about the throughput of the blockchain, so the examination needs to test the average time from a user sending a transaction to the transaction being packed into the blockchain, capacity for a blockchain block and etc.

B. Stopping the Tendency of the Centralization

Blockchain networks are developing rapidly, however the range of nodes isn't preserving pace. This can lead to centralization, that could have terrible effects for the networks. This difficulty may be addressed through constructing a greater decentralized node infrastructure. One issue is node centralization.
A website called Are we decentralized yet highlights that many blockchains have low node counts, in addition to a small number of entities in control of the majority of voting/mining power.

C. Big Data Analytics

Blockchain and Big Data are two new technologies that are high on the agendas of many businesses. Both are projected to have a significant impact on how businesses and organizations operate in the future years. Big Data has been around for a long time, and blockchain technology is currently riding the crest of a wave of popularity. It can be used in 2 things or the combination of both :

1) *Data Management:* If we want to store important data that needs to be secured and distributed across network we can use blockchain. For eg: blockchain can be utilized to store patients, the data couldn't be altered and taking those private information is hard
2) *Data Analytics:* Blockchain can be used for the analyzing the data for which the data is been stored . For eg: The blockchain monetary transactions can be used to predict the potential customers which can be there for the long term of the business

D. Artificial Intelligence

Ongoing advancements in blockchain technology are setting out new open doors for AI applications. We can have AI-driven cryptocurrency exchanging stage that gives crypto brokers AI-based scoring frameworks, top notch information channels and high level determining so they can customize news and exchanging elements to boost their endeavours. AI can help to solve many problems of the blockchain technology. For eg: There is dependably an oracle who is liable for it is fulfilled to decide if the contract condition. By and large, this oracle is a trusted outsider. AI strategy might assist with building a clever oracle. It isn't constrained by any party, it simply gains from an external perspective and train itself. In like that, there would be no contends in the smart contract and the smart contract can become smarter

V. DIFFICULITES FACED IN BLOCKCHAIN:

The challenges faced in the blockchain technology are summarized below into 3 categories namely Section 5.1 as Privacy, Section 5.2 as Selfish Mining and Section 5.3 as Scalability

A. Privacy

Blockchain is considered to give security and privacy to the sensitive individual information as clients can make transactions with produced addresses as opposed to utilizing a genuine personality. Clients additionally could create many addresses if there should be an occurrence of information leakage.

However, a few specialists proposed that Blockchain may be weak as far as transactional security as the public key for starting an exchange is noticeable to the network peers. Despite the fact that , it is guaranteed that a friend can be unknown in the Blockchain network, a few late examinations on the Bitcoin have demonstrated the way that the transaction history would be able be connected to uncover member's true identity. Biryukov et al. proposed a method to connect peers pseudonyms to IP addresses while they are behind the firewalls or network address translation (NAT). The main reason behind blockchain's information leakage is on the grounds that the details and balances of all public keys are apparent to everybody in the network. Consequently, the protection and security necessities should be characterized at the initial phase of Blockchain applications.

B. Selfish Mining

Selfish mining is an underhanded cryptocurrency mining system in which one miner or a group tackles a hash, opens another block, and keeps it from the public blockchain. This activity makes a fork, which is then mined to get in front of the public blockchain. Assuming a group's blockchain gets in front of the genuine blockchain, it can acquaint its most up to date block with the network. The network is equipped to perceive the latest block, so the group's fork would overwrite the original blockchain. The miners could actually steal cryptocurrency from different clients by altering the blockchain.

C. Scalability

With transactions increasing day by day , the blockchain turns out to be weighty .Presently, Bitcoin blockchain has surpassed 100 GB storage. All transactions must be put away for validating the transaction. In addition, because of the original limitation of block size what's more, the time interval used to create another block, the Bitcoin blockchain can process almost 7 transactions each second, which can't satisfy the necessity of handling millions of transactions in a real-time design. In the mean time, as the limit of blocks is small, numerous small transactions may be deferred since miners incline toward those transactions with a high transaction expense. The size of the blocks are restricted, for instance, a Bitcoin block size is 1 MB .

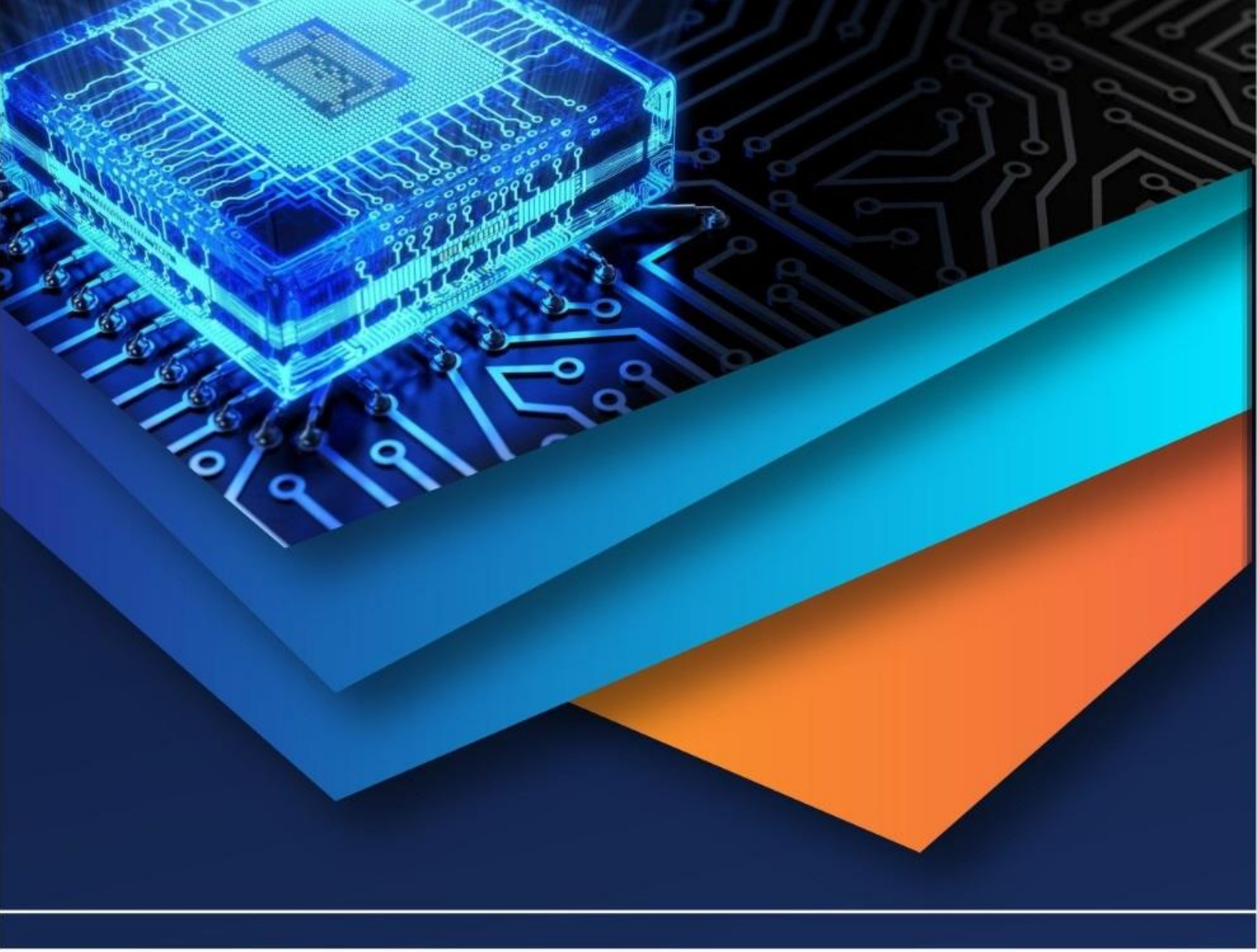
VI. CONCLUSION

The Blockchain technology is booming in the market and can help us to achieve more business and financial goals which will in turn increase the global economy. However, many explores about the blockchain are related to Bitcoin. Yet, blockchain could be applied to a variety of fields a long way past Bitcoin. Blockchain has shown its potential for changing the traditional business with its key attributes: decentralization, persistency, anonymity and auditability.

In this paper we had discussed overall understanding of the blockchain technology , Its overall creation , working , benefits , Challenges faced and opportunities where this technology can grow and explore . There are as yet many open issues that should be additionally explored and analyzed to create more useful and compelling industrial applications that can completely profit from the utilization of blockchain and accomplish the planned goals.

REFERENCES

[1] T. Aste, P. Tasca, and T. D. Matteo, ''Blockchain technologies: The foreseeable impact on society and industry,'' Computer, vol. 50, no. 9, pp. 18–28, Jan. 2017.
[2] M. Kouhizadeh and J. Sarkis, ''Blockchain practices, potentials, and perspectives in greening supply chains,'' Sustainability, vol. 10, no. 10, p. 3652, Oct. 2018. 117148 VOLUME 7, 2019 A. A. Monrat et al.: Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities
[3] A. Litke, D. Anagnostopoulos, and T. Varvarigou, ''Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment,'' Logistics, vol. 3, no. 1, p. 5, Jan. 2019.
[4] G. Peters, E. Panayi, and A. Chapelle, ''Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective,'' J. Financial Perspect., vol. 3, no. 3, pp. 1–25, Nov. 2015.
[5] S. Nakamoto et al., Bitcoin: A Peer-to-Peer Electronic Cash System. Citeseer, 2008. [Online]. Available: http://bitcoin.org/bitcoin.pdf
[6] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, ''Blockchain for AI: Review and open research challenges,'' IEEE Access, vol. 7, pp. 10127–10149, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY