iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XII **Month of publication:** December 2022

DOI: https://doi.org/10.22214/ijraset.2022.48008

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 XII Dec 2022- Available at www.ijraset.com

Blockchain Based Payment Method for Secure Transactions

Harshad Hakke[1], Abhishek Bharati[2], Akshay Ranit[3], S R Khonde[4]
Modern Education Society's College of Engineering, 19, Late Principal V. K. Joag Path, WadiaCollege Campus Pune-411001
Computer Department Savitribai Phule Pune University

Abstract: Blockchain is a type of distributed ledger that sits on the internet for recording transaction and maintaining a permanent and verifiable record-set of information. Token was created to reduce the government's control over cross-border transactions and to speed up the transaction process by removing the need for third-party intermediaries, Blockchain, on the other hand, provides a secure environment that token needs for peer-to-peer transactions. In other words, blockchain acts as bitcoin's ledger and maintains all the transactions of token. Token has a high degree of anonymity. Though the transactions are visible, it is close to impossible to identify the user.

It is the purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double spending or high security. We propose a solution to the double-spending problem

Keywords: Blockchain, Bitcoin, Consensus, Mining, Security.

I. INTRODUCTION

[5] As the energy sector develops and transitions, data and dataskills are becoming increasingly vital. Top energy firms are using Blockchain for various purposes, including commoditiestrading, peer-to-peer energy trading, eliminating middleman retailers, data management, and much more, due to Blockchain's potential to streamline existing processes andprovide new capabilities. To enable this future, whole new sectors, marketplaces, and resources, as well as unique types ofabilities, professions, and certificates, will be created.

These improvements will cost trillions of dollars in total. They want to combine Blockchain-based smart meters with real-time auctions to establish an automated energy market that will lower the cost of unbalancing present power systems and improve the system's overall performance.

As a result, the broad features of future solutions are frequently predicted and,in some cases, settled upon long before the technical competence to develop them is available.

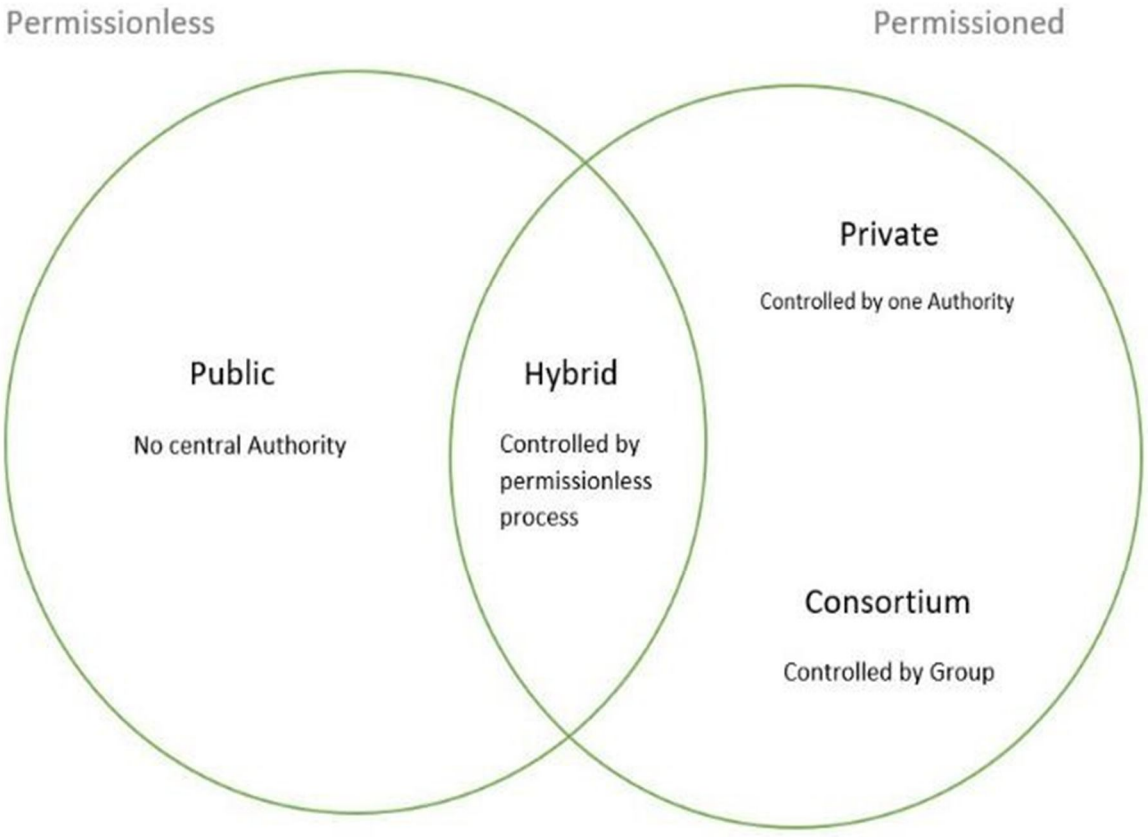
Open-source initiatives with a non-corporate approach will continue to playan essential role in the Metaverse, attracting some of the most talented creative minds. The 3Ds, known as: decentralization, decarbonization, and digitalization, all require a lot of data and automation to be successful. So, although AI and blockchain technologies are critical to that transformation, it's also essential that we have the right skills and technology in place to process that data and use it appropriately. Innovation and skill development in that area are critical.

The construction andoperation of immersive digital and frequently three- dimensional simulations, environments, and worlds where users and enterprises can explore, create, socialize, and participate in various experiences while still conducting business. Blockchain is open and still secure due to its distribution of its copies on various nodes and hashing algorithm. If attacker tries to change a block the hash value of entire block is changed which would be affect the next subsequent block which contains its hash value. In order to successfully attack, attacker needs to change all blocks after block he intends to change this will also take time due to consensus algorithm applied to validate the blocks. Further, a copy of blockchain is present on each and every node. Any malicious activity can be verified using local copies of the blockchain.

A. Classification of Blockchain Systems

There are three different sorts of blockchain systems: private, consortium, and public. The subsections below go overeach of these categories.

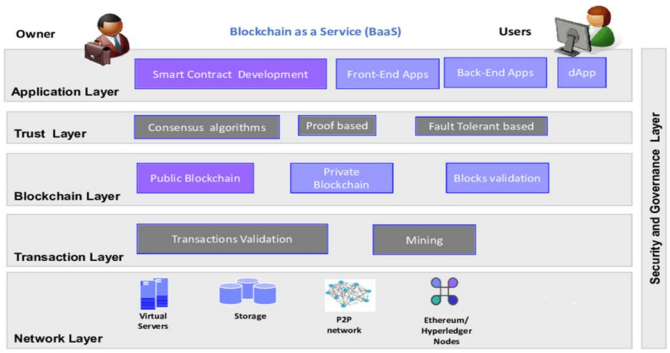
©IJRASET: All Rights are Reserved



1) *Public Blockchain:* A platform where people of various backgrounds and groups can transact, mine, and join the network. Permissionless blockchain is another name for them. Each member has complete authority to inspect any segment of the blockchain at any moment and to implement blockchain audits. Because it is transparent and open to all users, there are no definite validator nodes. Allmembers can collect transactions and begin the mining process to earn mining rewards. Because it is synchronisedon all nodes and can be validated by these local copies, blockchain is immutable. Every time a new block is added to the system, the hard work of cryptographic validation ofblockchain, paired with proof of work, provides security.
2) *Private Blockchain:* Private exchange and data sharing between multiple organizations or between a single organization (or groups of people) is a private blockchain system whose mining is controlled by selected people or organizations. Private blockchains are also known as authorized blockchains. This is because unknown members cannot access it without special permission. Theperson who controls the set of rules decides to join the node. This tends to centralize the network. When a node becomes part of the network of a private blockchain system, the node contributes to the execution of the distributed system, and each node imitates the law and works together to obtain upgrade approval. Unlike the public blockchain, it is reluctant to write operations. Compared to public blockchain, it is very cheap and fast because it does not require a huge amount of money, time and energy to get approval. Examples of private blockchains include Corda, Hyperledger, and Fabric. Corda allows businesses to build blockchain networks thatcan support inter-company contracts.
3) *Consortium Blockchain*: The blockchain which is considered partially permissioned and private blockchain is a Consortium Blockchain, where no individual organization is amenable for block validation and consentbut fairly a set of predefined nodes. The judgement of whocan mine and who can be the member of the network is decided by these nodes. Therefore, this is also known as partially centralized system, due to the command by few picked validator nodes, distinct from public blockchain that are fully decentralized, and the private blockchain that is fully centralized. Consortium decides whether write or read assent could be finite or public to the system participators. As well the barriers of the consent for a group of nodes do not assure irreversibility and volatility, as curbof the consortium by a bulk may advance to tinkering of the blockchain.

B. Architecture of a Blockchain System

The data layer, consensus layer, application layer, incentive layer, and network layer are the six levels that make up blockchain's architecture.



1) *DATA LAYER:* The data layer, which encompasses the entire blockchain, is the lowest tier. It keeps track of a connected network of blocks. Version, Time stamp, Merkle root, Difficulty target, Nonce, and Previous hash are all included in each block. The block architecture is split into two parts: the block head and the block body. The Merkle tree is calculated using the history of validated transactions in the block body. The block head contains the hash of the previous block, the time stamp, the software version, and the remaining entities, such as the difficulty goal, nonce, and the Merkle root, which are used to effectively and safely verify transactions.
2) *Network layer:* The network layer, which is the second lowest tier, has two primary goals: broadcasting and transaction verification. Blockchain networks are peer-to- peer networks with equal privileges for all nodes. Newly created transactions are broadcast to all network peers, who use a predetermined protocol to verify them. The transaction is transmitted to other nodes and a block is added to the data if verification is successful.
3) *Consensus layer:* the consensus layer consists of a number of protocols that are used to verify any changes made to the blockchain. Because all nodes in an open peer-to-peer network are masters, they agree on a standard mechanism for validating new transactions. Bitcoin utilises proof of work (PoW), whereas Binance and DASH use proof of stake (PoS), which reduces the amount of electricity used in PoW. DPoS is used by Tezos and EOS (Delegated Proof of Stake). PBFT is used by Zilliga. Proof of bandwidth, ripple, tendermint, stellar, Proof of Capacity, Proof of Importance, Proof of Ownership, and Proof of Activity are some of the less well- known algorithms. Section IV contains a full examination of some of these consensus algorithms. For public blockchain systems, PoW, DPoS, and PoA are commonly used.
4) *Incentive layer:* It is the magnet that pulls nodes into the verification mechanism. This layer is in charge of distributing a portion of the digital currency in exchange for the energy spent by nodes to validate transactions. This encourages additional nodes to participate, making blockchain more secure.
5) *Contract layer:* The contract layer is in charge of using programmable smart contracts to defend participant rights. Two or more participants sign these smart contracts cryptographically. Certain contract norms are agreed upon by both parties. It is kept on the blockchain system and is self-triggered for each node to verify the transaction. A high-level programming language is used to programme the rules. Non-Turing complete language is used to implement Bitcoin's contract. Ethereum, on the other hand, makes use of Turing complete language platforms. Solidity is a common choice for smart contract implementation in many blockchains. Solidity is Turing complete, which means it can handle loops and other complex features. Solidity is also used to programme Ethereum smart contracts, which are then translated to bytecode using EVM (Ethereum Virtual Machine). Bugs in smart contracts should not be introduced.
6) *Application layer:* It is the highest level. It saves the user interface for using the blockchain network. Any network change is visible at the application layer. Web-based applications are available for several blockchain platforms. Different applications, such as intellectual property, IoT, and so on, can be designed based on business logic.

II. LITERATURE SURVEY

[4] Nakamoto, Satoshi [1]. In this paper, the complete mechanism of blockchain technology for a electronic cash system that basically allows online payments to be sent directly from one party to another without going through a financial institution is presented.

It explains a network system which is distributed i.e. peer to peer network which resulted to be a solution for double spending and the Proof of Work algorithm for carrying out safe and secure transactions.

Judmayer, Aljosha et.al [2] presented an overview of blockchain technology in technical point of view also introduced the concepts of cryptographic currencies and the consensus ledgers. This paper mainly focused on the Bitcoin cryptographic currencies saying that the current scientific community is relatively slowly to this emerging and fast- moving field of blockchain technology reason as not sufficient resources available other than bitcoin. It explained deeply about bitcoin and why it has gained a huge market and interestin today's technology and also highlights the challenges in thearea of digital assets management and presents a discussion of Bitcoin usability, privacy, and security challenges from the user's perspective, the concept, characteristics, need of Blockchain and how Bitcoin works. It attempts to highlights role of Blockchain in shaping the future of banking, financial institutions.

Zibin Zheng et al. [3] provided an overview of blockchain architecture firstly and compared some typical consensus algorithms used in different blockchains. Also discussed various blockchain based applications that are covering numerous fields like financial services, reputation system, IOT so on. Furthermore, technical challenges of blockchain technology such as scalability of security problems waiting tobe overcome and recent advances are briefly listed and possible future trends for blockchain.

III. METHODOLOGY

Authentication: The original blockchain was designed to operate without a central authority (i.e. with no bank or regulator controlling who transacts), but transactions still haveto be authenticated. This is done using cryptographic keys, a string of data (like a password) that identifies a user and gives access to their "account" or "wallet" of value on the system. Each user has their own private key and a public key that everyone can see. Using them both creates a secure digital identity to authenticate the user via digital signatures and to 'unlock' the transaction they want to perform.

Authorisation: Once the transaction is agreed between the users, it needs to be approved, or authorised, before it is addedto a block in the chain. For a public blockchain, the decision to add a transaction to the chain is made by consensus. This means that the majority of "nodes" (or computers in the network) must agree that the transaction is valid.

The people who own the computers in the network are incentivised to verify transactions through rewards. This process is known as 'proof of work'. Understanding Libra Understand how Facebook leveraged specific aspects of blockchain technology to launch a new cryptocurrency calledLibra, and its potential impact on the banking and finance sector

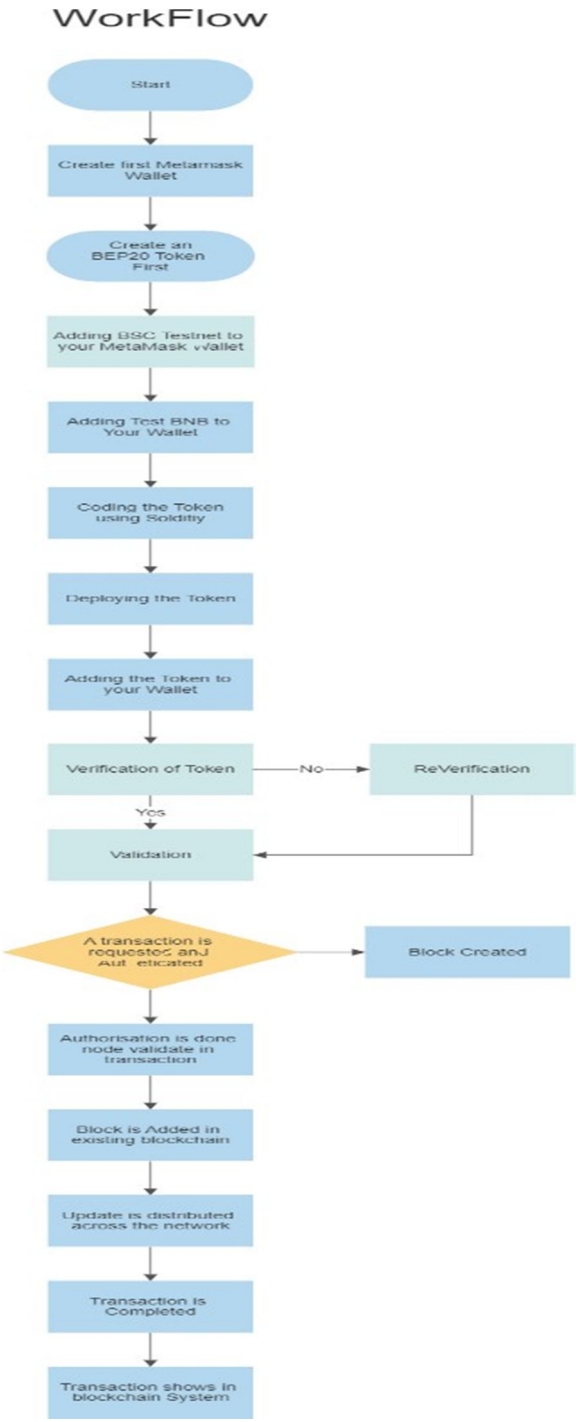
Proof of Work: requires the people who own the computers inthe network to solve a complex mathematical problem to be able to add a block to the chain. Solving the problem is known as mining, and 'miners' are usually rewarded for their work in cryptocurrency. But mining isn't easy. The mathematical problem can only be solved by trial and error and the odds of solving the problem are about 1 in 5.9 trillion. It requires substantial computing power which uses considerable amounts of energy. This means the rewards for undertaking the mining must outweigh the cost of the computers and the electricity cost of running them, as one computer alone would take years to find a solution to the mathematical problem.

The Power of Mining: The Cambridge Bitcoin Electricity Consumption Index estimates the bitcoin mining network consumes almost 70 terawatt-hours (TWh) of electricity per year, ranking it the 40th largest consumer of electricity by 'country'. By way of comparison, Ireland (ranked 68th) usesjust over a third of Bitcoin's consumption, or 25 TWh, and Austria at number 42 consumes 64.6 TWh of electricity per year, according to 2016 data compiled by the CIA.

The Problem with Proof of Work To create economies of scale, miners often pool their resources together through companies that aggregate a large group of miners. These miners then share the rewards and fees offered by the blockchain network. As a blockchain grows, more computers join to try and solve the problem, the problem gets harder and the network gets larger, theoretically distributing the chain further and making it ever more difficult to sabotage or hack. In practice though, mining power has become concentrated in the hands of a few mining pools. These large organizations have the vast computing and electrical power now needed to maintain and grow a blockchain network based around Proof of Work validation.

Proof of Stake: Later blockchain networks have adopted "Proof of Stake" validation consensus protocols, where participants must have a stake in the blockchain - usually by owning some of the cryptocurrency - to be in with a chance of selecting, verifying & validating transactions. This saves substantial computing power resources because no mining is required. In addition, blockchain technologies have evolved toinclude "Smart Contracts" which automatically execute transactions when certain conditions have been met.

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



IV. BACKGROUND AND RELATED WORK

[5] Software has evolved from a technology tool for solving specific problems to an industry that is omnipresent in most oftoday's corporate activities over the previous 60 years. Softwareengineering is defined as "the use of a systematic, disciplined, quantifiable methodology to the development, operation, and maintenance of software; that is, the application of engineering to software," according to IEEE Standard 610.12 . The Software Engineering Body of Knowledge (SWEBOK) provides a complete description of the core SE Knowledge Areas (KAs), which are also taken into account in this research.Software requirements, software process, software testing, software quality, software maintenance, software configuration management, and engineering management are examples of knowledge areas.

Property	Public	Private	Federated
Consensus	• Costly PoW	• Light PoW	• Light PoW
Mechanism	• All miners	• Centralised organisation	• Leadernode set
Identity	• (Pseudo) Anonymous	• Identifiedusers	• Identifiedusers
Anonymity	• Malicious?	• Trusted	• Trusted
Protocol & Efficiency	• Lowefficiency	• Highefficiency	• Highefficiency
Consumption	• High energy	• Low energy	• Lowenergy
Immutability	• Almostimpossible	• Collusionattacks	• Collusionattacks
Ownership&	• Public	• Centralised	• Semi-Centralised
Management	• Permissionless	• Permissioned whitelist	• Permissioned nodes
Transaction Approval	• Order ofminutes	• Order of milliseconds	• Order of milliseconds

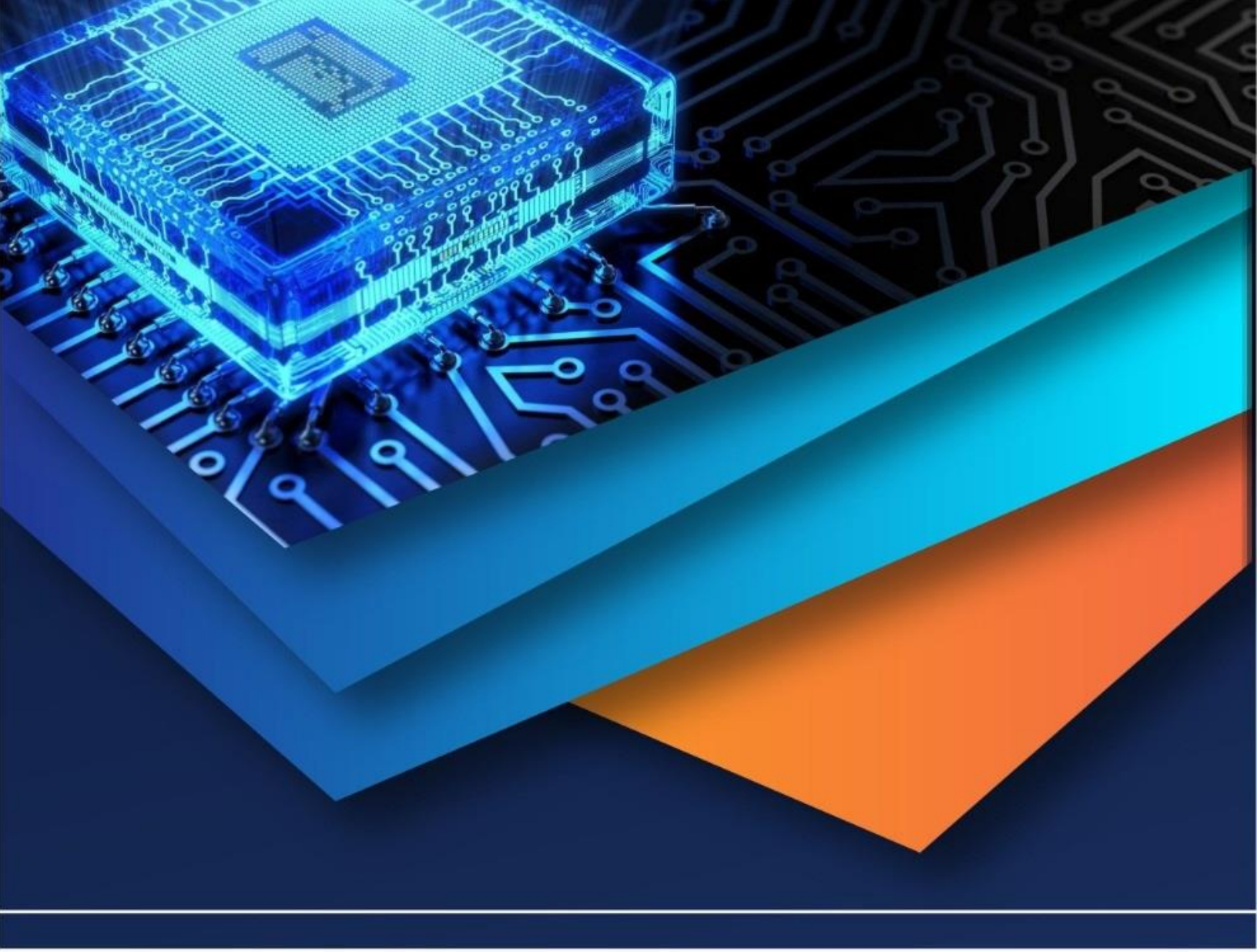
A few (optional) studies have audited the utilization ofblockchain, e.g., applications and shrewd agreement improvement. One of the latest orderly planning concentrates on blockchain innovations was performed. In this review, the creators mean to distinguish and plan different spaces of exploration connected with blockchain and perceive potential headings for future examination. Additionally, it led a methodical writing audit of blockchain and savvy contract advancement. Specifically, the creators identified strategies, methods, apparatuses and challenges looked during the creation and testing of blockchain-arranged programming. Their examination recommends future exploration on the best way to adjust standard testing procedures to blockchain-arranged programming and how to gauge code measurements for code improvement. Both past investigations answer questions connected with the more extensive utilization of blockchain innovation, yet they don't analyze specifically its use in further developing SE exercises. To be sure, they didn't investigate thecommitments that blockchain angles can bring to SE. Specifically, comparable to the use of blockchain to SE, to the best of our information, there give off an impression of being extremely restricted optional investigations. The more intently related study is a methodical planning study directed by Tariq and Colomo-Palacios. This concentrate on wrote about the purposes of blockchain in programming and illustrated the benefits that this new innovation can bring to theSE field. The consequences of this study demonstrate that savvycontacts can computerize the verification of undertakings that normally require human-in-the circle. Shrewd agreements execute tests, produce results and naturally reward programming engineers. Also, blockchain can improve the trustbetween parties in rethinking programming improvement.

V. CONCULISON

[5] Blockchain is a powerful tool for resolving complex issues quickly. Its ability to provide security in an open environment makes it attractive for usage in a variety of other fields, including health care, IoT applications, and finance. E-commerce retailers and delivery partners can use consortium blockchains to avoid fraud during transit by continuously updating package positions on the blockchain. One of the most innovative potential uses of blockchain could be to avoid fraud in chit funds, which are used to save money in Indian society. It can also serve as a ledger for disadvantaged farmers to share resources. We give a state-of-the-art survey of blockchain technology in this study. We began by discussing the background, classification, architecture, and several sorts of consensus.

REFERENCES

[1] Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System." March 2009.
[2] Judmayer, Aljosha, Nicholas Stifter, Katharina Krombholz, and Edgar Weippl. “Blocks and chains: introduction to bitcoin, cryptocurrencies, and their consensus mechanisms.” Synthesis Lectures on Information Security, Privacy, & Trust 9, no. 1 (2017)
[3] Zheng, Zibin, Shaoan Xie, Hongning Dai, Xiangping Chen, And Huaimin Wang. “An Overview Of Blockchain Technology: Architecture, Consensus, And Future Trends.” In 2017 IEEE International Congress On Big Data (Bigdata Congress) IEEE, 2017.
[4] Karthikeya Thanapal, Dhiraj Mehta, Karthik Mudaliar, and Bushra Shaikh “Online Payment Using Blockchain” Research Paper.
[5] Shantanu Gade, Mayur Manwar, Sidhharth Rasal,Vishal Kotkar,Shobha Raskar, Jaya Mane “blockchain: - an emerging digital technology” Research Paper.



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)