iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33791

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: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

Blockchain

Riya Singh[1], Riya Chauhan[2], Simple Sharma[3]
[1, 2]*Student,* [3]*Associate Professor, Dept. of Computer Science and Engineering, Faculty of Engineering and Technology, Manav Rachna International Institute of Research and Studies, Faridabad*

Abstract: Blockchain is a decentralized, computer-generated platform that fills in as a platform on which Bitcoin and other digital currencies operate. Blockchain uses a broad organization to monitor advanced exchanges, such as digital currency, referred to as a chain as options or changes are collected directly and linked to a single unit. This means that the blockchain cannot be secretly modified or modified. When an exchange is embedded in Blockchain and appears to be important to the organization, circles cannot change or modify it without shared understanding.
This paper discusses Blockchain, cryptocurrencies-Bitcoins, Ethereum.
Keywords: Component, format, style, styling, insert (key words)

I. INTRODUCTION

Cryptocurrency as a emerging topic has been the focus of engineers, investors and researchers over the past few years. Although the market is showing strong volatility, the total market value has reached hundreds of billions of US dollars with some experts predicting that it will reach USD 1 trillion this year. In addition, there are new cryptocurrensets, trading platforms, developers, banking and institutional partners that join the market regularly. Today, this multibillion-dollar market has a profound effect on people's investment and performance.

Digital development and technological advancement in today's world have encouraged the collection, analysis and implementation of Big Data analytics, which is integrated into all aspects of daily life and rapidly evolving. The Internet of Things (IoT) transforms network and communication infrastructure, cloud computing changes the way data is calculated and stored, while data mining techniques, machine learning, and Artificial Intelligence transform data extraction, problem solving, decision-making and performance . These Big Data analytic technologies are not only the focus of research and implementation, but also possible solutions and leading strategies for all aspects of human health, such as disease diagnosis, health care, etc. For example, the Map planning framework as a big data integration analytics process provided an important paradigm for both industry and academics.

Like encrypted digital currency, cryptocurrencies operate on a virtual system, and complete well-organized records of the largest network satisfy a 5 V aspect of Big Data (volume, variability, speed, authenticity and value). Therefore, it serves as a good tool for Big Data analytics, while Big Data analytics also holds the keys to the evolution and development of cryptocurrensets. For example, the global scale of digital production and IoT innovation has spurred the adoption of novel technology in general, making cryptocurrency another promising alternative. In addition, Big Data analytics can also help investors and developers make better decisions and overcome infrastructural barriers. On the other hand, technology based on cryptocurrensets has been shown to work in a variety of disciplines. This has fueled digital advancement and expanded the Big Data analytics network. In short, there are shared benefits of exploitation when it comes to the connection between Big Data and cryptocurrency and that potential remains immeasurable.

This academic paper focuses specifically on the interaction between Big Data and cryptocurrency, which are two key concepts that have been extensively investigated. We aim to present an in-depth investigation into their merger and a systematic review of the latest developments for all stakeholders. This paper is academically and industry-friendly to participants who want to gain a better understanding of the interaction between Big Data and cryptocurrency or aim to explore its future capabilities.

The rest of this paper is organized in such a way that cryptocurrency is fully introduced in Section 2. The Big Data and cryptocurrency collaborative research is summarized and reviewed by topics in Section 3. Finally, Section 4 concludes the findings and presents indications for future research.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

II. BLOCKCHAIN

Blockchain is a specific type of database. A blockchain collects information together in groups, also known as blocks, that hold set of information. Blocks have certain storage capacities, when filled connects to the previously filled block, forming a chain of data known as "blockchain".

When a block is filled it is set in stone and become a part of an irreversible timeline.

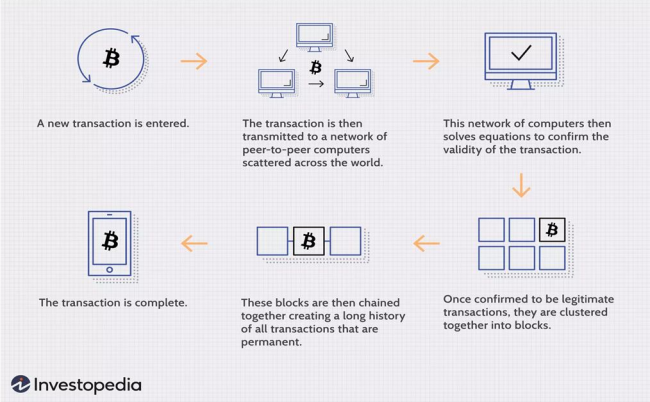


Figure1: Transaction process

A. History of Blockchain

Although blockchain is a relatively new technology, it already has a rich and interesting history. The following is a brief timeline of some of the most important and significant events in blockchain development.

1) *2008:* Satoshi Nakamoto, an impostor, publishes "Bitcoin: A Peer to Peer Electronic Cash System.
2) *2009:* The first successful Bitcoin (BTC) transaction took place between computer scientist Hal Finney and the mysterious Satoshi Nakamoto.
3) *2010:* Florida program designer Lazzlo Hanycez completed his first purchase using Bitcoin - two of John John's pizzas. Hanycez transferred 10,000 BTC's, which cost about $ 60 at the time. Today it costs $ 80 million. The market value of Bitcoin officially exceeds $ 1 million.
4) *2011:* 1 BTC = $ 1USD, providing cryptocurrency rate in US dollars. The Electronic Frontier Foundation, Wikileaks and other organizations are beginning to accept Bitcoin as donations.
5) *2012:* Blockchain and cryptocurrency are featured in popular television programs such as The Good Wife, injecting blockchain into pop culture. Bitcoin Magazine was introduced by the first Bitcoin engineer Vitalik Buterin.
6) *2013:* The BTC market fund has exceeded $ 1 billion. Bitcoin reached $ 100 / BTC for the first time. Buterin publishes a paper on the "Ethereum Project" suggesting that the blockchain has other opportunities besides Bitcoin (e.g., smart contracts).
7) *2014:* Sports companies Zynga, The D Las Vegas Hotel and Overstock.com are all starting to accept Bitcoin as payment. Butterin's Ethereum project is funded by Initial Coin Offering (ICO) which collects more than $ 18 million in BTC and opens new blockchain options. R3, a group of more than 200 blockchain firms, was formed to find new ways to use blockchain in technology. PayPal announces Bitcoin integration.
8) *2015:* The number of traders accepting BTC exceeds 100,000. NASDAQ and San-Francisco blockchain company Chain is a team to test stock trading technology in the private sector.
9) *2016:* Tech giant IBM announces blockchain strategy for cloud-based business solutions. The Japanese government recognizes the legitimacy of blockchain and cryptocurrensets.
10) *2017:* Bitcoin reaches $ 1,000 / BTC for the first time. The market value of Cryptocurrency reaches $ 150 billion. JP Morgan chief executive Jamie Dimon says he believes in the blockchain as a technology of the future, giving the ledger system a vote of confidence from Wall Street. Bitcoin always reaches the top at $ 19,783.21 / BTC. Dubai announces that its government will be provided with a blockchain by 2020.
11) *2018:* Facebook is committed to starting a blockchain group and is also showing the opportunity to build its own cryptocurrency. IBM is developing a blockchain-based banking platform with major banks such as Citi and Barclays logged in.

B. Blockchain Consists of Three Concepts: Blocks, Nodes and Miners

The whole series consists of many blocks and each block has three basic elements:

1) *Block Information:* A total of 32 called nonce. A nonce is generated randomly when a block is generated, and then generates a block title hash. The hash is a 256-bit number married to a nonce. It should start with a large number of eggs (e.g., very small). When the first block of the chain was created, the nonce formed a cryptographic hash. The information in the block is considered signed and merged indefinitely with nonce and hash unless opened.
2) *Miners:* Miners make new blocks in the chain through a process called mining. In a blockchain all blocks have a different nonce and hash, but also refer to the hash of the previous block in the chain, so blocking the block is not easy, especially on larger chains. Miners use special software to solve a surprisingly complex mathematical problem of finding a nonce that has adopted an accepted hash. Because the nonce has only 32 bits and the hash is 256, there are about four billion possible non-hash compounds that must be mined before the correct detection. When that happens the miners are said to have found a "gold nonce" and their block is added to the chain. When the block is successfully mined, the change is accepted by all nodes in the network and the miner is awarded financially.
3) *Nodes:* One of the most important ideas in blockchain technology is the distribution of power in certain areas. No single computer or organization can own a chain. Instead, a distributed ledge with locations connected to the series. Nodes can be any type of electronic device that stores copies of the blockchain and keeps the network running. Every node has its own copy of the blockchain and the network must agree algorithm to any newly excavated block in order for the chain to be renewed, trusted and validated. As blockchains are transparent, all actions in the ladder can be easily checked and viewed. Each participant is given a unique alphanumeric identification number that identifies their transaction.

C. Working of blockchain

Here are five basic principles that underpin technology.

1) *Distributed Database:* Each group in the blockchain has access to the entire database and its complete history. No single group controls data or data. All parties can verify the records of their direct transaction partners, without a consultant.
2) *Peer Transfer:* Communication occurs directly between peers instead of the central node. Each node stores and transmits data to all other nodes.
3) *Openness About Pseudonymity:* Everything that is done with the corresponding value is visible to anyone with access to the system. Each node, or user, in the blockchain has a unique alphanumeric 30-plus-character address that it identifies. Users can choose to remain anonymous or provide proof of identity to others. Transactions take place between blockchain addresses.
4) *Stability of Records:* Once the transaction has been entered into a database and the accounts have been updated, the records cannot be changed, as they are linked to all transactions that preceded them (hence the term "chain"). Algorithms and various methods are still being distributed to ensure that the recording in the database is permanent, tracked, and accessible to everyone else on the network.
5) *Computer Perspective:* The digital type of ledger means that blockchain transactions can be tied to the concept of calculation and actually planned. Users can therefore set algorithms and rules that trigger transactions between nodes.

D. Types of blockchain

There are four types of blockchain.

1) *Public Blockchain:* A public blockchain is a non-restrictive, permission-less distributed ledger system. Anyone who has access to the internet can sign in on a blockchain platform to become an authorized node and be a part of the blockchain network. A node or user which is a part of the public blockchain is authorized to access current and past records, verify transactions or do proof-of-work for an incoming block, and do mining. The most basic use of public blockchains is for mining and exchanging cryptocurrencies. Thus, the most common public blockchains are Bitcoin and Litecoin blockchains. Public blockchains are mostly secure if the users strictly follow security rules and methods. However, it is only risky when the participants don't follow the security protocols sincerely. Example: Bitcoin, Ethereum, Litecoin

a) Advantages

- *Trustable:* Unlike in private blockchain, two nodes or participants do not need to worry about the authenticity of the other. In other words, they don't need to personally know or trust the other nodes as the process of proof-of-work makes sure there can be no fraud in transactions. So, one can trust public blockchains blindly without feeling the needing to trust individual nodes.
- *Secure:* There can be as many participants or nodes in a public network which makes it a secure network. The larger the network, greater the distribution of records and harder it is for hackers to hack the entire network. In addition to this, every node will do verification of transactions and proof-of-work which makes every transaction and block legitimate. Due to these practices and thoughtful cryptogenic encrypting methods, a public blockchain is much safer than the private one.
- *Open and Transparent:* Public blockchain is open and the data is transparent to all the participant nodes. A copy of the blockchain records or digital ledger is available at every authorized node. This makes the entire blockchain system completely open and transparent. No one shows a fake transaction or hides an existing one as every node has an updated copy of the database at any given point of time.

b) Disadvantages

- *Lower TPS:* The rate of transactions per second in a public blockchain is very low. This is because it is a huge network with a lot of nodes and for every node to verify a transaction and do proof-of-work is time-consuming. This is why public blockchains like Bitcoin can process only 7 transactions per second or Ethereum network has a rate of 15 TPS. On the other hand, a private network such as Visa has a rate of 24,000 TPS indicating a huge difference in speed of transaction processing and execution.
- *Scalability Issues:* Like we just saw in the point above, that public blockchain have a slow rate of processing and completing transactions. This causes issues in scalability as well. Because the more we try to increase the size of the network, the slower it will get. However, solutions like Bitcoin's Lightning Network helps in overcoming this problem. It maintains a rate of the transaction as we increase the size of the network.
- *High Energy Consumption:* The process of proof-of-work is highly energy consuming as it needs specialized systems (hardware components) to run a special algorithm. It is a matter of concern from both an environmental and economical standpoint. The apparatus to do proof-of-work is costly and consumes as much energy as the country of Ireland! The technology definitely needs to come up with energy-efficient consensus mechanisms.

2) Private Blockchain: A private blockchain is a restrictive or permission blockchain operative only in a closed network. Private blockchains are usually used within an organization or enterprises where only selected members are participants of a blockchain network. The level of security, authorizations, permissions, accessibility is in the hands of the controlling organization. Thus, private blockchains are similar in use as a public blockchain but have a small and restrictive network. Private blockchain networks are deployed for voting, supply chain management, digital identity, asset ownership, etc. Examples of private blockchains are; Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, etc.

a) Advantages

- *Speed:* Private blockchains' transactions occur at greater speed as compared to public blockchains. That means the transactions per second (TPS) rate is higher in the case of private blockchains. This is because there is a limited number of nodes in a private network as opposed to a public network. This fastens the consensus or verification process of a transaction by all the nodes in a network. Also, the rate of adding new transactions in a block is fast. Private blockchains can facilitate the transactions at a rate of up to thousands or hundred thousand TPS at a time.
- *Scalability:* Private blockchains are pretty scalable. That is, you can choose the size of your private blockchain as per your needs. For instance, if there is an organization that needs a blockchain of only 20 nodes, they can easily deploy one. Then after expansion, if they need to add more nodes, they can easily do so. This makes private blockchains very scalable as it gives an organization the flexibility to increase or decrease the size of their network without much effort.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

b) Disadvantages

- *Needs Trust-building:* As far as a public blockchain is concerned, it is like an open book or as we call it, an open ledger. This ensures the security and legitimacy of every user. Whereas, in a private network, there are limited participants in a restricted network. Especially within an organization, where colleagues know each other. They need to build trust to transmit confidential information within a network.
- *Lower Security:* As a private blockchain network has lesser number of nodes or participants, it runs a higher risk of a security breach. If anyone of the nodes gains access to the central management system, it can gain access to all the nodes in the network. This makes it easier for a node to hack the entire private blockchain and misuse the information.
- *Centralization:* Private blockchains are restricted that is they need a central Identity and Access Management (IAM) system for functioning properly. This system has all the monitoring and administrative rights. It gives permissions to add a new node in the network or decide the level of access they get for the information stored in the blockchain. This whole system contradicts the idea of decentralization which is one of the pillars of blockchain technology.

III. CONSORTIUM BLOCKCHAIN

A consortium blockchain is a semi-decentralized type where more than one organization manages a blockchain network. This is contrary to what we saw in a private blockchain, which is managed by only a single organization. More than one organization can act as a node in this type of blockchain and exchange information or do mining. Consortium blockchains are typically used by banks, government organizations, etc.
Examples of consortium blockchain are; Energy Web Foundation, R3, etc.

A. Hybrid Blockchain

A hybrid blockchain is a combination of the private and public blockchain. It uses the features of both types of blockchains that is one can have a private permission-based system as well as a public permission-less system. With such a hybrid network, users can control who gets access to which data stored in the blockchain. Only a selected section of data or records from the blockchain can be allowed to go public keeping the rest as confidential in the private network. The hybrid system of blockchain is flexible so that users can easily join a private blockchain with multiple public blockchains. A transaction in a private network of a hybrid blockchain is usually verified within that network. But users can also release it in the public blockchain to get verified. The public blockchains increase the hashing and involve more nodes for verification. This enhances the security and transparency of the blockchain network.
Example of a hybrid blockchain is Dragonchain.

B. Understanding Bitcoin

Bitcoin needs a collection of computers to store its blockchain. For bitcoin, this blockchain is just a specific type of database that stores every bitcoin transaction ever made. In these cases, the computers are not all under one roof and are operated by unique individuals or group of individuals.

C. Decentralisation

Computers that make up the bitcoin network are called "nodes".
In a blockchain, each node has a complete record of data stored in the blockchain since its inception. In this case, the data is the entire history of all bitcoin transactions. If one node has an error in its data, it can use thousands of other nodes to retrieve it and correct it. If one user interferes with a bitcoin transaction record, all other nodes can identify and point to a node with incorrect information. This information is a transaction list, but it is also possible that the blockchain may hold a variety of information such as legal contracts, government indexes, or a company product list.
The purpose of the blockchain is to record digital information and distribute it but not to edit it. The Bitcoin protocol is built into the blockchain. In a research paper introducing digital currency, the fake creator of Bitcoin, Satoshi Nakamoto, called it "a new fully-fledged peer-to-peer electronic money system, with no reliable third party." Bitcoin simply uses blockchain to openly record payments book, but blockchain can be used to consistently record any amount of data points, this can be in the form of transactions, voting options, product lists and much more. A common blockchain analogy would be google doc. When a person makes a document and shares it with people it is distributed and not copied and transmitted.

This creates a ground-breaking distribution chain that gives access to everyone who uses that document at the same time. No one should wait for one party to make a change in a document, everyone can change it as they wish and as the change is recorded in real time, the changes made clear.

IV. CRYPTOCURRENCY

A cryptocurrency, crypto or crypto currency is a digital asset designed to serve as an exchange system where individual identifier records are stored in an existing database in the form of computerized data using robust cryptography to access transaction records, control additional currency transactions, and secure currency transfer.

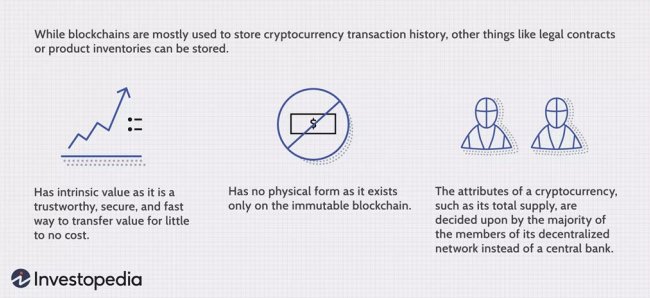


Figure 2: Attributes of cryptocurrency

A. *Understanding Cryptocurrencies*

Cryptocurrensets are programs that allow secure online payments displayed in accordance with real tokens, represented by the ledger in-app entries. "Crypto" refers to various encryption algorithms and cryptographic techniques that protect these entries, such as elliptical encryption, public and private key pairs, and hashing functions.

B. *Types of Cryptocurrency*

The first blockchain-based cryptocurrency was Bitcoin, which remains very popular and very important. Today, there are thousands of other cryptocurrencies with different functions and specifications. Some of them are clones or forks for Bitcoin, while others are new currencies built from scratch.

Some of the competing currencies resulting from the success of Bitcoin, known as “altcoins,” include Litecoin, Peercoin, and Namecoin, as well as Ethereum, Cardano, and EOS. Today, the combined value of all existing cryptocurrencies is approximately $ 1.5 trillion - Bitcoin currently represents more than 60% of its total value.

C. *Advantages and Disadvantages of Cryptocurrency*

1) *Advantages:* Cryptocurrencies hold the promise of making it easier to transfer money directly between two parties, without the need for a reliable external company such as a bank or credit card company. These transfers are instead protected by the use of public and private keys and various types of promotion programs, such as Proof of Work or Proof of Stake. In modern cryptocurrency systems, the user's "wallet", or account address, has a public key, and the private key is known only to the owner and is used to sign the transaction. Transfers are eliminated with minimal processing costs, which allows users to avoid excessive fees charged by banks and financial institutions for wire transfers. Cryptocurrencies hold the promise of making it easier to transfer money directly between two parties, without the need for a reliable external company such as a bank or credit card company. These transfers are instead protected by the use of public and private keys and various types of promotion programs, such as Proof of Work or Proof of Stake. In modern cryptocurrency systems, the user's "wallet", or account address, has a public key, and the private key is known only to the owner and is used to sign the transaction. Transfers are eliminated with minimal processing costs, which allows users to avoid excessive fees charged by banks and financial institutions for wire transfers.
2) *Disadvantages:* The anonymous nature of cryptocurrency transactions prepares them for a host of illegal activities, such as money laundering and tax evasion. However, cryptocurrency advocates often value their anonymity, citing privacy benefits such as the protection of hackers or activists living under oppressive governments. Some cryptocurrensets are more secretive than others. Bitcoin, for example, is a bad way to run an illegal online business, because forensic analysis of the Bitcoin blockchain has helped authorities arrest and prosecute criminals. Privacy coins exist, however, such as Dash, Monero, or ZCash, which are very difficult to track.

D. Special Considerations

Central to the appeal and functionality of Bitcoin and other cryptocurrencies is blockchain technology, which is used to keep an online ledger for all transactions ever made, thus providing the data structure of this secure and shared server agreed upon over a single local network, or computer storage. a copy of the ledger. All new blocks produced must be verified for each node before verification, making it difficult to create transaction history.

Many experts see blockchain technology as a major force in use such as online voting and refunds, and large financial institutions such as JPMorgan Chase (JPM) see the potential to reduce transaction costs by simplifying payment processing. However, because cryptocurrensets are visible and not stored in a central database, the digital balance can be erased by loss or damage to the hard drive if a backup copy of the private key is not available. At the same time, no central authority, government, or company can access your funds or personal information.

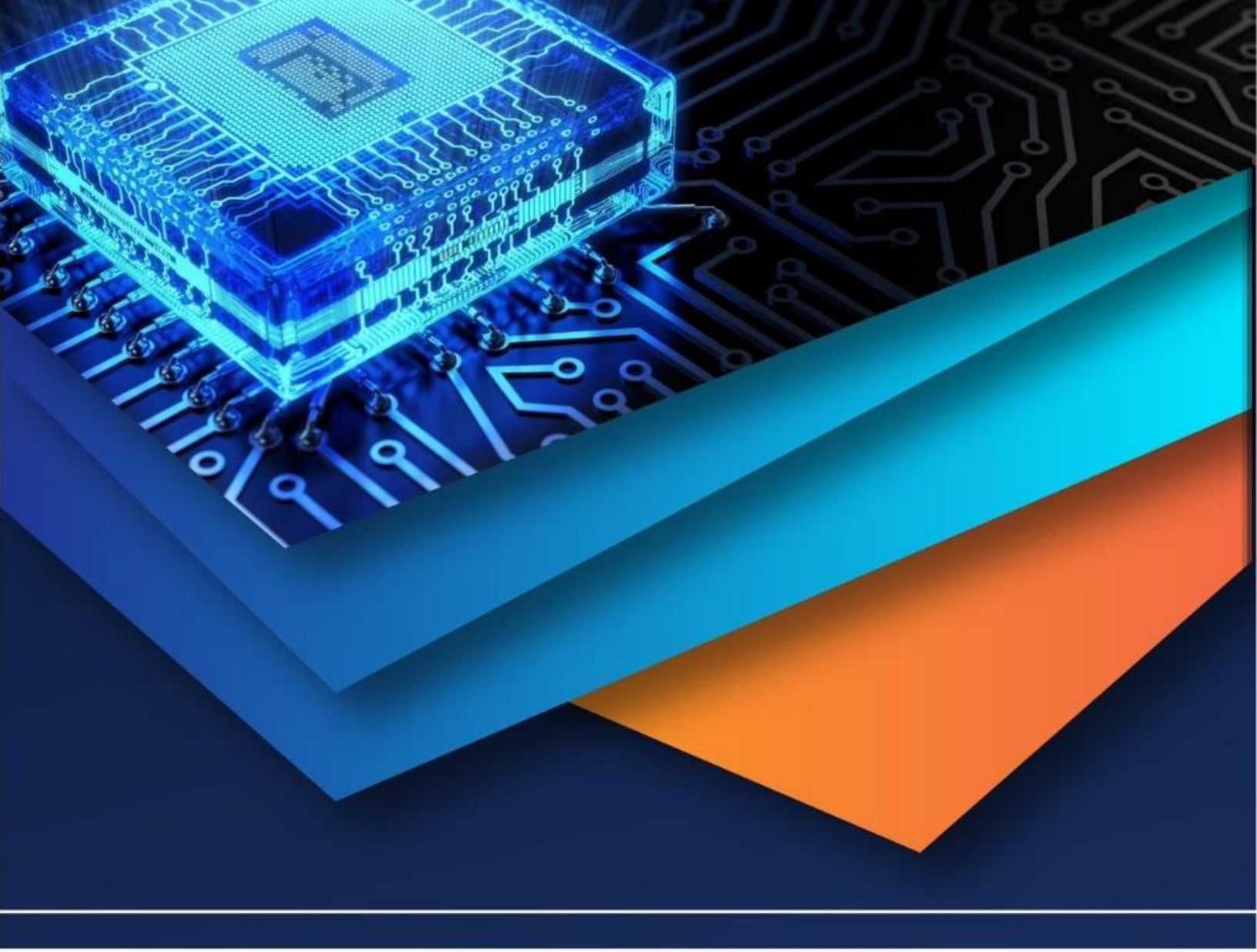
V. ACKNOWLEDGMENT

The common spelling of the word “confession” in America does not have an “e” after “g”. On the contrary, try to say “R. B. G. thank you ... ”. Provide customer approval for countless riches on the home page.

REFERENCES

[1] https://bitcoin.org/bitcoin.pdf
[2] https://github.com/ethereum/wiki/wiki/White-Paper
[3] https://hbr.org/2017/01/the-truth-about-blockchain
[4] https://www.mdpi.com/2504-2289/2/4/34/htm
[5] https://onlinelibrary.wiley.com/doi/book/10.1002/9781119019138

For pages exposed to translation journals, provide an English quote first corresponding to the original foreign language text
[1] “The king is dead. Long live the king! BERT rule may end. XLNet, a new model of people from CMU and Google surpasses BERT in 20 jobs. ”- Sebastian Ruder, researcher at Deepmind.
[2] "XLNet will probably be an important tool for any NLP consultant for a while… [is the latest NLP approach." - Keita Kurita, of Carnegie Mellon University.
[3] Luis von Ahn, Manuel Blum, Nicholas J. Hopper and John Langford. CAPTCHA Web Page: http://www.captcha.net. 2000.
[4] Mihir Bellare, Russell Impagliazzo, and Moni Naor. Does the equivalent duplicate reduce the error in the rating of Sound Protocols? At the 38th IEEE Conference on the Foundations of Computer Science (FOCS ’97), pages 374–383. IEEE Computer Society, 1997.Google Scholar
[5] "Artificial Intelligence: A Approach Approach" by Stuart Russell and Peter Norvig • Start reading "Java in brief"



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY