iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** I **Month of publication:** January 2022

DOI: https://doi.org/10.22214/ijraset.2022.39855

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 I Jan 2022- Available at www.ijraset.com

Blockchain: Medical Data System

Janak Damre[1], Abhishek Kharche[2], Siddhesh Jungade[3], Vikas Sanap[4], Prof. Sudesh A. Bachwani[5]

[1, 2, 3, 4, 5]*Department of Computer Engineering*
[1, 2, 3, 4]*Government College of Engineering Yavatmal, Maharashtra, India,*
[5]*Assistant Professor, Government College of Engineering Yavatmal, Maharashtra, India*
[1, 2, 3, 4]*Dr. Babasaheb Ambedkar Technological University Lonere, India*

Abstract: ***We've been hearing a lot about cryptocurrencies lately. With about 3,000 distinct cryptocurrencies on the market right now, it's evident that they're here to stay, despite their unpredictable nature. But did you realise that nearly all cryptocurrencies are based on the same idea? Blockchain technology underpins nearly all cryptocurrencies. Blockchain, also known as the shared ledger, is one of the most secure digital technologies due to its distributed nature.***
Keywords: Centralized & Decentralized, Blockchain, Solidity

I. INTRODUCTION

A. What Is a Blockchain?

A blockchain is a decentralised database that is shared among computer network nodes. A blockchain acts as a database, storing information in a digital format. Blockchains are well known for their critical role in keeping a secure and decentralised record of transactions in cryptocurrency systems like Bitcoin. The blockchain's novelty is that it ensures the fidelity and security of a data record while also generating trust without the requirement for a trusted third party.

The structure of data in a blockchain differs significantly from that of a traditional database. A blockchain is a digital ledger that accumulates data in the form of blocks, which contain sets of data. When a block is full, it is closed and linked to the preceding one, producing a data chain known as the blockchain. All additional data that comes after that newly added block is compiled into a new block, which is then added to the chain once it's full.

A database organises data into tables, whereas a blockchain organises data into chunks (blocks) that are strung together, as the name suggests. When implemented in a decentralised manner, this data structure creates an irreversible data chronology. When a block is filled, it becomes permanent and part of the chronology. When each block is added to the chain, it is given a specific time stamp.

B. How does a Blockchain Work?

Blockchain is a technology that combines three fundamental components: cryptographic keys, a peer-to-peer network, and a digital ledger. There are two sorts of cryptography keys: private and public. Both of these keys are held by each individual or node and are used to establish a digital signature. The most significant feature of blockchain technology is the digital signature, which is a unique and secure digital identification reference. Every transaction is validated by the owner's digital signature.

In a peer-to-peer network, a mathematical verification authorises a deal or transaction. This peer-to-peer network is made up of a huge number of people who function as authorities in order to reach a consensus on transactions and other matters.

The digital ledger is a system that stores all of these transactions. In layman's terms, the digital ledger is a spreadsheet that contains all of the nodes in a network as well as the history of all purchases done by each node. The digital ledger's information is highly secure, and the digital signature protects it from being tampered with. The most intriguing aspect of this ledger is that anybody may view the information, but no one can alter it.

C. History of Blockchain

In his dissertation, Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups, published in 1982, David Chaum suggested the first-ever blockchain-like protocol. Stuart Haber and W Scott Stornetta expanded on this concept in 1991, describing the method of creating a cryptographically protected chain of blocks with non-tamperable timestamps.

Satoshi Nakamoto, on the other hand, popularised blockchain in 2008. He modified the concept by timestamping each block utilising hashcash-like methods instead than relying on a central authority or "trusted parties." These enhancements were so groundbreaking that they have since become the foundation of today's cryptocurrencies.

D. Why Do Transactions Fail?

Why Do Deals Fall Through?

Consider a money transaction between two persons. Now, presuming the sender sent the money from his bank correctly, there's no way the transaction can go wrong, right?

There are a number of things that can go wrong, including the following:

1) At the bank, something may have gone wrong (such as a technical issue)
2) It's possible that the sender's account was compromised.
3) It's possible that the day's transfer limitations were surpassed.
4) Never credited on the other side of a debt from one account.
5) Data mismanagement

Cryptocurrencies, on the other hand, do not have any of these issues. Let's start with a definition of a cryptocurrency.

E. What is a Cryptocurrency?

A cryptocurrency is a type of digital currency that uses cryptography to authenticate asset transfers, control new unit additions, and secure financial transactions.

One of the most significant advantages of cryptocurrencies over traditional (fiat) currencies is that they are not governed by any central body. The funds cannot be hacked or stolen since there is no single point of failure or "vault."

Consider the ubiquitous Microsoft Excel spreadsheet programme as an example. You have the ability to make modifications to the data that may differ from previous versions of the spreadsheet that have been shared with others. When you make modifications to a Google Sheets document, however, the changes are reflected in all other shared copies. Similarly, cryptocurrencies' shared and dispersed nature keeps everyone on the same page.

As a result, cryptocurrencies (at least those that use the blockchain) are secure due to the transparency and distributed nature of blockchain technology.

F. What Are the Types of Cryptocurrencies?

Several cryptocurrencies are currently accessible on the market. The following are a some of the most well-known:

1) Bitcoin, Litecoin, Ethereum, Z Cash, and Dash are all digital currencies.
2) Ripple
3) NEM Stellar Monero

As previously said, there are approximately 3,000 cryptocurrencies on the market, which has nearly swamped the market with possibilities. According to most analysts, the great majority of these options will eventually fail as people gravitate toward a select handful.

II. FEATURES OF BLOCKCHAIN

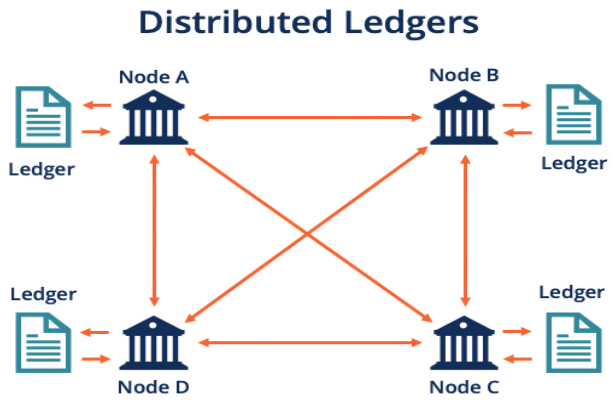
These are the four characteristics of Blockchain that we will discuss in depth:

1) We have a public distributed ledger that uses hashing encryption to work.
2) Every block has a hash value, which serves as the block's digital signature.
3) A proof-of-work consensus technique is used to approve and verify all transactions on the Blockchain network.
4) The Blockchain network makes use of the miners' resources, which are used to validate transactions in exchange for incentives.

III. PUBLIC DISTRIBUTED LEDGER

A public distributed ledger is a set of digital data that is shared, synchronised, and copied across various sites, countries, and institutions all over the world. Consider a blockchain that anyone in the network may access from anywhere in the world. Because everyone in the network has a copy of the ledger, if someone tries to change data in one of the blocks, everyone in the network can see the change. Data manipulation is prevented in this way.

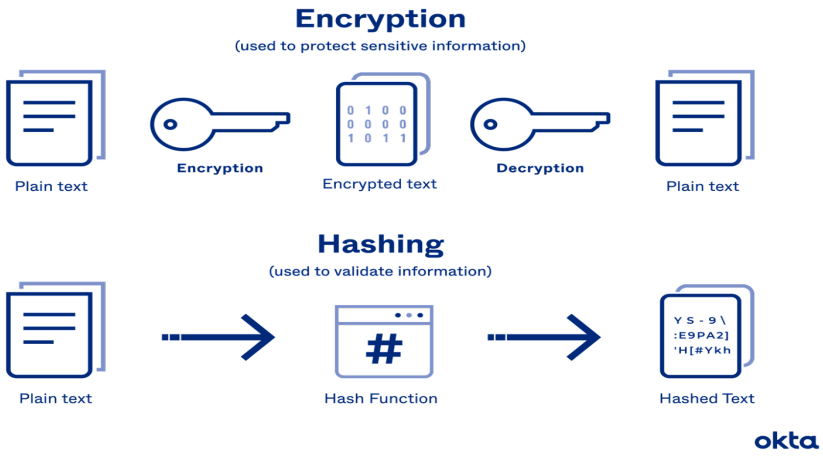
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue I Jan 2022- Available at www.ijraset.com



IV. HASH ENCRYPTION

To ensure that the data in the blocks is kept secure from unwanted access and is not altered, blockchain employs cryptography (see definition of "cryptography" above). The encryption algorithm used by Blockchain is SHA-256. One of the most powerful hash functions available is SHA-256. For a text, this cryptographic hash technique creates a nearly unique 256-bit signature. Digital signatures are also used to verify users on the blockchain.

A public and private key is assigned to each user. The public key is used to uniquely identify the user, while the private key grants access to all of the account's contents. From the sender's perspective, the message is hashed; the output is then processed through a signature algorithm with the user's private key, and finally, the user's digital signature is obtained. The user's message, digital signature, and public key are all sent during the transfer.



The message is transmitted through a cryptographic procedure on the receiver's side to generate a hash value. Through a verification function, that hash value is compared to the hash output received, bypassing the digital signature and public key.

As previously stated, SHA-256 is used to encrypt and safeguard the data in each block of a blockchain. There are four fields in each block:

1) Previous hash—in the Blockchain, this field records the hash of the previous block. Transaction details—in the Blockchain, this field maintains information on many transactions.
2) This field includes a random value (the nonce value) that is only used as a variate for the hash value.
3) This field includes the block's unique identity; it is a hex value of 64 characters, including letters and digits, produced using the SHA-256 method.

To obtain the fourth item, the hash address of that particular block, the first three values (previous hash, transaction data, and nonce) are sent through a hashing function.

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

V. PROOF OF WORK

Bitcoin is based on the proof-of-work algorithm. What is the definition of evidence of work? It's a piece of data that's difficult to produce (in the sense that it takes a long time or costs a lot of money) but that can be easily confirmed by others and meets particular criteria. Proof of work in bitcoin is a competition between miners who wish to add a block to the Blockchain, which requires them to solve a mathematical challenge to obtain the block's nonce value. When a miner discovers a nonce value, he or she informs the rest of the network, and if other miners confirm the claim, the miner is paid with 12.5 bitcoins or another form of payment. The block is also added to the Blockchain after a nonce value is found. The basic goal of miners is to choose a nonce value. They must identify a value that is less than or equal to the goal value. If they discover a value that is higher than the target, their mining attempt will be rejected. However, if they can successfully construct a hash value that is less than the goal value using the nonce, their work is accepted. To generate the hash value, the miner's complete processing capacity is put to use.

It takes a lot of time, money, and resources to find a nonce value. When a miner discovers the nonce value, he or she informs other miners about the discovery, and if the claim is verified, the miner receives a reward. As a result, a miner is rewarded for being the first to discover the nonce, and a block is added to the Blockchain. As previously stated, the award is 12.5 bitcoins as of today. The amount of bitcoin a miner can make is halved every four years. Mining is the only method new bitcoins can be created, and it ensures that the number of bitcoins in circulation is limited.

VI. USES OF BLOCKCHAIN

Blockchain is used for a lot more than just money and bitcoin. Here are some of the most common blockchain applications across various industries:

1) Tracking system for anti-money laundering
2) Markets for non-traditional products
3) development of unique content
4) IoT operating systems that operate in real time
5) Advertising perceptions
6) Tracking of music royalties
7) Payments made across international borders
8) Mechanism for voting
9) Monitoring the supply chain and logistics

VII. OTHER FIELDS THAT USE BLOCKCHAIN

The financial services industry is one of many that makes considerable use of blockchain technology, but it is far from the only one. In its article "Eight Ways Blockchain Will Impact the World Beyond Cryptocurrency," Forbes mentions healthcare, crowdfunding, and ride-sharing. Let's have a look at some additional areas.

A. Travel

Blockchain technology can be used for things like:

1) Tracking luggage, especially with several flights on one itinerary and foreign flights, is one application of blockchain technology.
2) Passengers are being identified, time is being saved, and lineups and wait times are being reduced.
3) Making and accepting service payments

B. Music

With the rise of digital music, issues such as piracy and artist recompense have arisen. Blockchain has the ability to:

1) Assist in the prevention of music piracy (illegal file sharing).
2) To be used to compensate artists for songs and albums that have been purchased

C. Cyber Security

Blockchain is being used by even large corporations like Lockheed Martin in their cybersecurity efforts. Blockchain has the ability to:

1) Because of its cryptography feature, it can help secure sensitive data.
2) Users and devices can be authenticated using the public and private keys, eliminating the need for passwords.

D. Human Resources

The use of blockchain technology to improve time-consuming and costly HR procedures is a logical fit. It can, for example:

1) Remove the need for individual background checks on prospective employees— Data about one's identification and employment history can be stored in blockchain transactions.
2) Employers and employees can keep track of payments and costs, making things like filing taxes considerably easier.

E. Blockchain as a Use Case in Banking

Banking is a great place to use blockchain. At the moment, a user must verify his identification at each bank he visits. Is there a way to make the process go more smoothly using Blockchain? Yes, it is correct. To make it work, we'll need truffle, ethereum, ganache, and smart contracts, all of which are part of the Blockchain technology ecosystem.

VIII. COMPARISON BETWEEN

A. Blockchain vs. Cloud Computing

Now that we're familiar with both words and their characteristics, let's look at the key differences:

A cloud is something to which we can connect via the internet. We can obtain data on the internet through cyberspace. Blockchain, on the other hand, is an encrypted system that stores data in secure databases using various types of encryption and hashes. The system distributes these data records across multiple nodes and establishes an agreement on the data's location.

In blockchain, data in the form of records is immutable, but data in the cloud is malleable. Blockchain is a spectacular technological achievement that is a decentralised, distributed ledger that retains a record of the origin of a digital asset. It does not provide any services. Cloud computing, on the other hand, is a type of computing that offers services in three different formats: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) (IaaS). Without relying on any third-party trusted centralised authority, blockchain ensures that data is not tampered with, but the cloud does not guarantee perfect integrity and tamper-free data. Cloud computing has the potential to speed up the execution of blockchain-based applications. However, data retrieval is centralised (since all data is housed in a company's centralised set of data centres). Blockchain, on the other hand, is based on the principle of decentralisation, which means it does not keep any of its data in a single location.

Data and its existence on the cloud can be public or private, which means it can be made visible to other users or kept hidden. Transparency of data is one of the most important features of blockchain technology

The majority of cloud computing is based on a typical database structure, with the data being kept on the devices of the participants. Blockchain, on the other hand, is an incorruptible and dependable online database record of various digital transactions in which users can update data with the consent of each party involved.

Cloud computing services are provided by companies such as Amazon Web Services (AWS), Alibaba Cloud, Google, IBM, and Microsoft, while blockchain technology is used by projects such as Ethereum, Bitcoin, Hyperledger Fabric, and Quorum.

- *Conclusion:* Both blockchain and cloud computing are having a significant impact on how businesses operate and how traditional computing is done. Their emergence has revolutionised the way the world of application development, storage, online transactions, and other services functions, as well as the existing business infrastructure. Despite the fact that cloud is a well-oiled model for speeding up blockchain projects, its merging and blockchain cloud services are still in their infancy.

B. Blockchain vs. DataBase

The table below summarises the key distinctions between blockchains and databases.

Database	Blockchain
Centralized	Decentralized
Permissioned	Permission-less
Requires administrator	No administrator

Blockchain vs relational database

1) *Decentralized Control:* Blockchains, in general, allow several parties to share information without the need for a central administrator. In the case of blockchains, the consensus process we outlined before plays a significant role in decision-making. Databases, on the other hand, have very different usability. In a database, a central administration is essential since there are times when you can't rely on agreement. Sometimes a single person's basic intelligence proves to be superior to the sum of a million other people's intellects.

2) *Its Own History:* Centralized databases only keep track of current information. They don't look up information that has already been recorded. The situation is different with blockchains. They can not only store up-to-date information, but also go back in time to look up information from previous transactions. Blockchains can be used to generate databases with histories of their own, growing like ever-expanding archives of their own history.
3) *Performance:* While blockchains are perfect as transaction platforms and are employed as systems of records, they are as slow as databases when it comes to digital transaction technology. There will undoubtedly be enhancements to the performance and nature of blockchain technology, but databases already provide similar services. They've been around for decades and have seen their performance increase by a factor of ten.

- *Confidentiality:* Like a centralised database, a permissioned blockchain can be managed both in terms of write and read operations. Blockchains, on the other hand, have no advantage over centralised databases if confidentiality is the main goal.

IX. CONCLUSION

Although blockchain is a strong technology, existing healthcare management systems have a number of shortcomings that create a lot of inconvenients, such as being sluggish, ineffective, insecure, and inefficient, as previously stated. Almost all of these flaws can be remedied with blockchain technology. When blockchain technology is used, it should be done after extensive testing and study. When used appropriately, blockchain may significantly increase effectiveness, efficiency, and security, all of which are important factors in data storage and transfer.

After all, the entire idea of a decentralised blockchain is to provide a hard-promise in the form of an immutable record with open, non-discriminatory participation. In certain sense, we accept decentralization's inefficiency since it is the only way for a network to attain these characteristics.

X. ACKNOWLEDGMENT

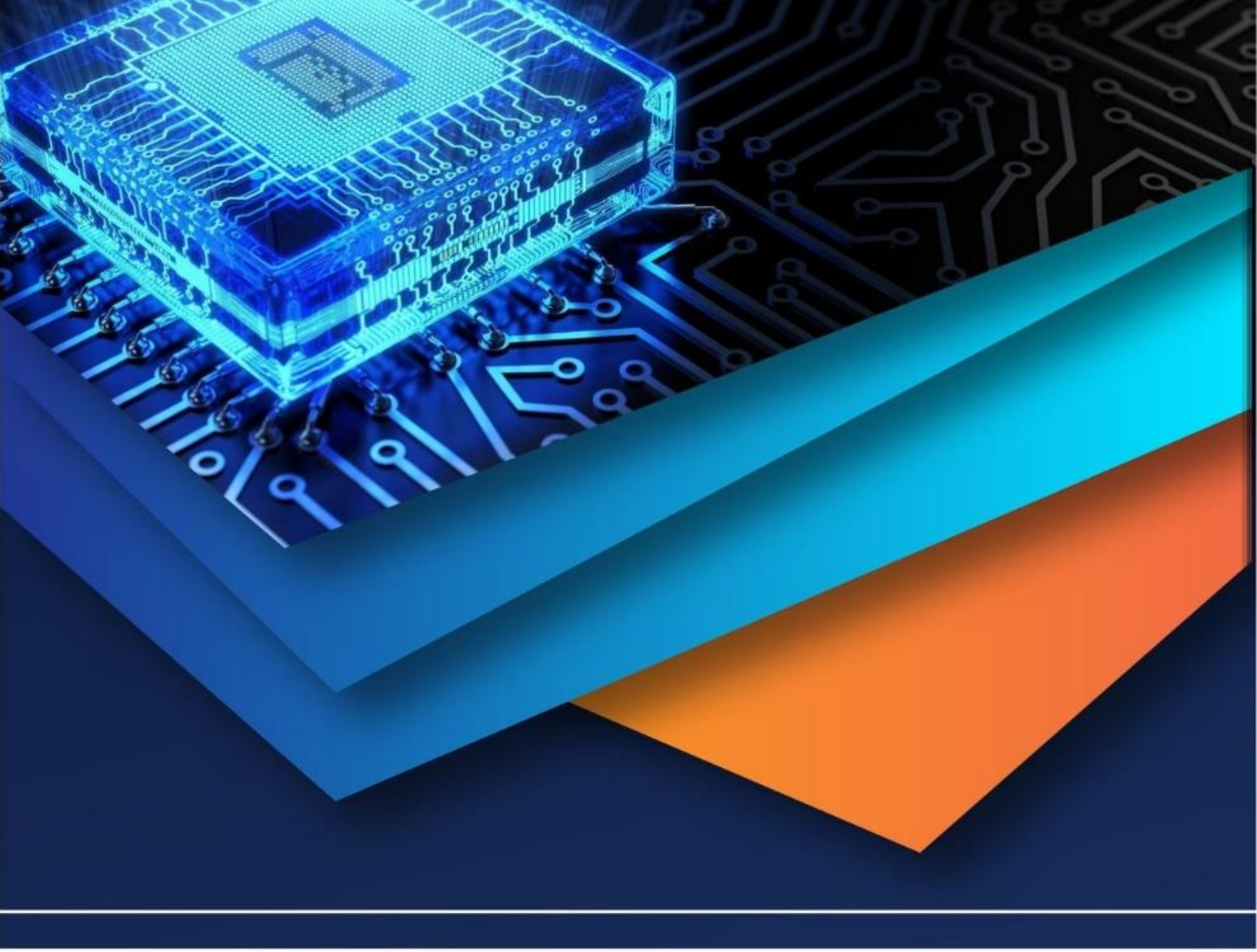
Without the involvement and assistance of many people who contributed to this work, it would not have been able to finish it. However, we would want to convey our gratitude and debt of gratitude to our guide for their unwavering support, generosity, and understanding during the period of the paper.

This paper has taken a lot of time and effort to complete. However, without the help and direction of many others, I would not have been able to finish my work. We would like to express our heartfelt gratitude to each and every one of them.

We owe Miss. Sonal Sawarkar a huge debt of gratitude for her advice and supervision. We'd like to express our gratitude to her for supplying the required data and resources for this work.

REFERENCES

[1] GFG : https://www.geeksforgeeks.org/
[2] Berty : https://berty.tech/blog/
[3] Blackdice : https://blackdice.io/
[4] Architecture of Blockchain: https://mlsdev.com/
[5] Solidity GitHub document : https://docs.soliditylang.org/
[6] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), 2018, pp. 1-6, doi: 10.1109/AIEEE.2018.8592253.
[7] "Blockchain Size". Archived from the original on 19 May 2020. Retrieved 25 February 2020.
[8] "Blockchains: The great chain of being sure about things". The Economist. 31 October 2015. Archived from the original on 3 July 2016. Retrieved 18 June 2016. The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the crypto currency.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY