IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12661

BLOCKCHAIN TECHNOLOGY

Mr. Rohan Anil Torankar[1], Mr. Neehal Jiwane[2], Mr. Ashish Deharkar[3]

Student Computer Science & Engineering, Shri Sai College Of Engineering and Technology Bhadrawati, Maharashtra, India[1]

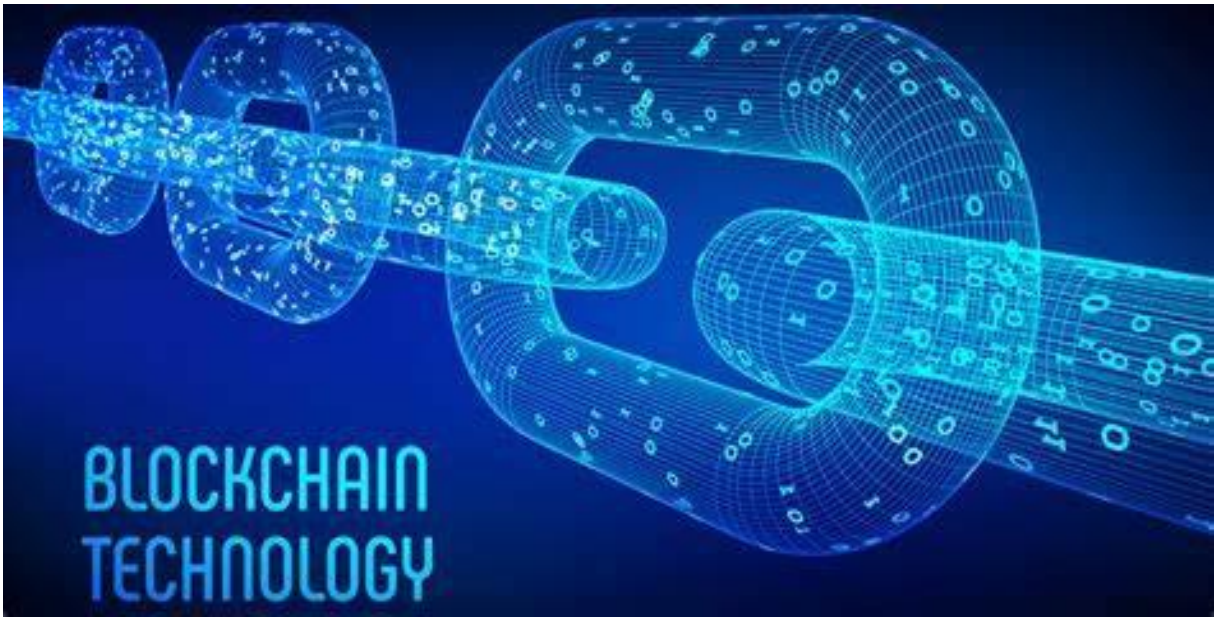
Assistant Professor, Computer Science and Engineering, Shri Sai College Of Engineering and Technology, Bhadrawati, India[2]

Assistant Professor, Computer Science and Engineering, Shri Sai College of Engineering and Technology, Bhadrawati, India[3]

Abstract: Blockchain is among the most pivotal technological inventions in recent times. Blockchain is a transparent plutocrat exchange system that has revolutionized the way a business was conducted preliminarily. Companies and crackers have started investing significantly in the blockchain request and it's anticipated to be a net worth of further than 3 trillion dollars in the forthcoming times. Its fashionability has increased exponentially because of its impeccable security and capability to give a complete result to digital identity issues. It's a digital tally on a peer-to-peer network. This paper gives sapience into Blockchain technology, its history, its armature, how it works, its advantages and disadvantages, and its operation in different diligence.

I. INTRODUCTION

Blockchain technology is typically associated with cryptocurrencies similar as Bitcoin. It's a database of records of deals which is distributed, and which is validated and maintained by a network of computers around the world. Rather of a single central authority similar as a bank, the records are supervised by a large community and no individual person has control over them and no one can go back and change or abolish a sale history. As compared to a conventional centralized database, the information cannot be manipulated due to the blockchain's erected-in distributed nature of structure and verified guarantees by the other peers. In other words, when a normal centralized database is located on an individual server, the blockchain is distributed among the druggies of a software. Blockchain allows anyone on the network to pierce everyone differently entries, which makes it insolvable for one central reality to gain control of the network. Whenever someone performs a sale, it goes to the network and computer algorithms determine the authenticity of the sale. Once the sale is vindicated, this new sale is linked with the former sale, forming a chain of deals. This chain is called the blockchain. Blockchain technology is grounded on a decentralized network, meaning it operates as a peer-to-peer network.



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12661

II. HISTORY OF BLOCKCHAIN

In the year 1976, a paper was released on “New Directions in Cryptography” bandied the conception of distributed tally. As Cryptography progresses, another paper entitled “Hot to Time-Stamp a Digital Document” by Stuart Haber and Scott Stornetta, which laid out the conception to timestamp the data rather of the medium.

Another important conception called “Electronic cash” or “Digital Currency” which came into actuality grounded on a model proposed by David Chaum also contributed towards the development of the conception of Blockchain, which was followed by protocols similar as e-cash schemes that introduced double spending detection. In 1997, Adam Back introduced another conception called. “Hash cash”, which offered a result to control spam emails. This led to the conception of creating money called as “b-plutocrat” by Wei Dai is grounded on a peer-to-peer network.

Satoshi Nakamoto was considered as the innovator of blockchain technology when he published a paper on bitcoin in 2008 as “Bitcoin: A Peer-to-Peer Electronic Cash System”. The epitome of the paper was on direct online payment from one source to another source without counting on a third-party source. The paper described an electronic payment system grounded on the conception of cryptography. Nakamoto’s paper handed a result to the double spending where a digital currency cannot be duplicated, and no one can spend it further than formerly. The paper stated the conception of public tally issues where an electronic coin sale history can be traced and verified if the coin has not been spent ahead and to prevent double spending issues. An open source program to apply the bitcoin system was released just a few months latterly and the first bitcoin network was begun in early 2009 when Satoshi Nakamoto created the first bitcoins. Although the innovator of the bitcoins remains amicable, bitcoins continued to be created and marketized and a large community was there to support and address colorful issues with the law. There are hundreds of different cryptocurrencies, such as Litecoin, Dogecoin etc., but bitcoins hold the captain's share of the request. It's cryptocurrency popularity exponentially increases cryptocurrency among the others. It was suitable to draw the attention of the druggies due to its ability to keep its druggies amicable, but it became really popular due to its translucency. Bitcoin has started to flourish since then and by the year 2013, investors started to pour finances into launch-ups related to Bitcoin. Bitcoins can be exchanged for regular currency, for any service or product. With the use of portmanteau software, druggies can electronically transfer bitcoins using a computer, mobile or a web operation. In 2015, the Ethereum platform was launched, which enabled blockchain to work with loans and contacts. It was grounded on an algorithm called smart contract icing the implementation of an action between the two parties. Due to Ethereum’s ability to offer a briskly, safer and more effective terrain, the technology became extensively popular.

III. BLOCKCHAIN ARCHITECTURE

Blockchain technology works on the conception of decentralized database where these databases live in multiple computers and every dupe of these databases is identical. Organizations keep their data in one place which is easy target for hackers, it has made the blockchain a temper-evidence technology. Blockchain can be considered as a peer-to-peer network that runs on the top of the internet. Blockchain armature can be substantially divided into three layers, which are operations, Applications, Decentralized Ledger and Peer-to-Peer Network. Applications are the top subcaste of the network, which is followed by the Decentralized Ledger, and the nethermost subcaste is the Peer-to-Peer Network. The operation subcaste contains the operation software of the Blockchain. For illustration, Bitcoin portmanteau software creates and stores private and public keys, enabling druggies to keep control over the unspent bitcoins. The operation subcaste provides a mortal readable interface where druggies can keep track of their deals.

The Decentralized Ledger is the middle subcaste in a blockchain armature that confirms a harmonious and temper-evidence global tally. In this subcaste, deals can be grouped into blocks which are cryptographically linked to one another. Deals can be defined as the exchange of commemoratives between two actors and every sale goes through a confirmation process before it's considered as a licit sale. Mining is the process of grouping deals into a block that is added to the end of the current blockchain. Blockchain uses a evidence-of-work algorithm to decide the chain that has needed the most accretive trouble to make and to determine a licit blockchain's legality. The nethermost subcaste in the blockchain armature is the Peer-to-Peer Network where Node types play different places and colorful dispatches are exchanged to lead the Decentralized Ledger.

3.1. operations It provides operation interfaces on top of the blockchain and is used for keeping the cryptocurrencies secure. This software can be installed on any platform.

3.2. Decentralized Ledger A decentralized tally is a participated and replicated database which is accompanied among the members of the network. It maintains the records of deals among the actors in the network. The tally is responsible

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

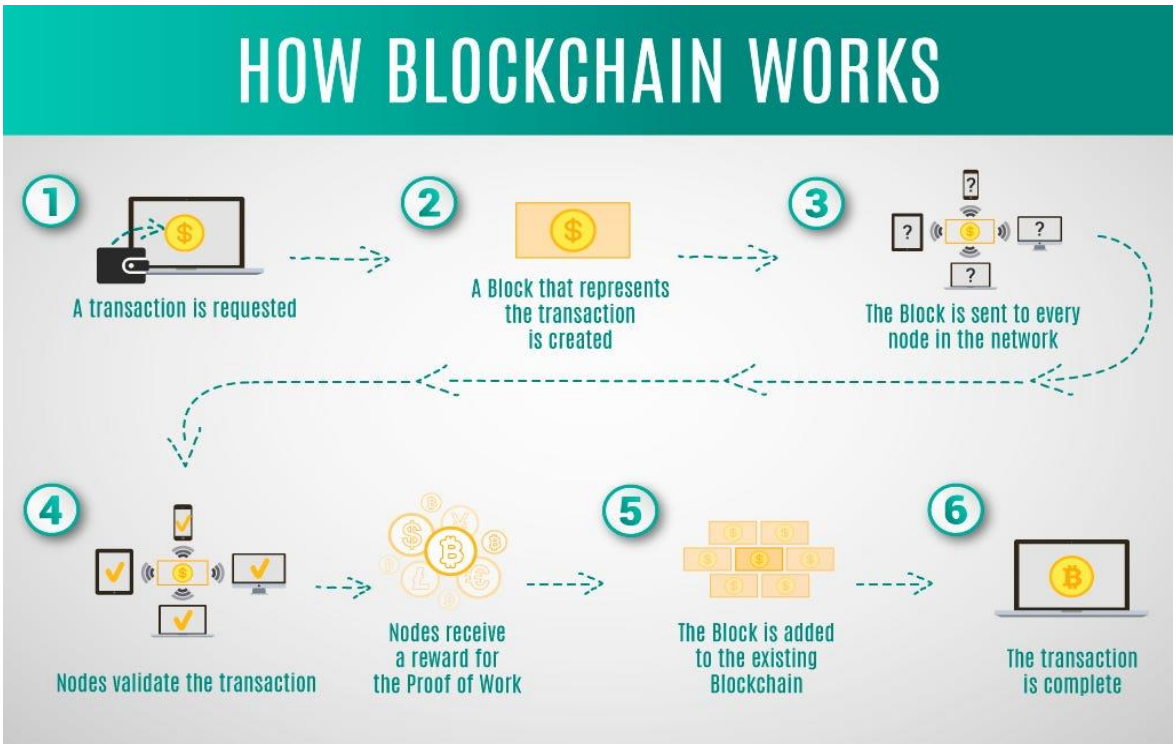
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12661

for keeping records of deals among the actors. Blockchain has the parcels of a database except the fact that it stores the information in the title and data is stored in the form of a commemorative or a cryptocurrency. It's needed to group the recently validated deals into blocks as the first step of recording deals in the tally. Any party in the blockchain can gather new deals and produce blocks that can be added to the blockchain. A block substantially consists of deals, and it has a pointer, time prints and a formerly.

Bumps perform colorful functions depending on their part in the blockchain network. A knot can be called a miner when it proposes and validates deals and performs mining to give agreement to secure the blockchain. It can perform functions similar as simple payment verification etc., and functions depending on the blockchain used. Evidence of work is defined as a agreement algorithm that verifies the delicacy of data. For illustration, Bitcoin uses hash cash as evidence of work for bitcoin deals. Miners are needed to complete evidence of work to corroborate the deals in the block so that it can be accepted by the network.

Evidence of work ensures security and agreement in the blockchain network. To corroborate the coming block, this hash is added to the current block of deals. In the coming step, add a nonce-which is defined as a arbitrary number that can be used only formerly, to the end of the coming block. A hash function is used to change this arbitrary number to induce a string that contains the number of bottoms in front of it. Evidence of work is expensive to maintain, and it can have unborn scalability and security issues as it always relies on the miners' impulses. There's an advanced solution called "evidence-of-stake," which is economic to apply, and it identifies who gets to modernize the agreement and defers unwanted forking of the underpinning blockchain. No non-public information is transferred on a blockchain network and all the deals are visible to every knot in the network. This peer-to-peer network doesn't bear any fresh protection and can be erected on any physical structure.



IV. CATEGORIES OF BLOCKCHAIN

Following three categories of blockchain technology were firstly described in the book 'Blockchain, Blueprint for a new Frugality' by Melaine Swan grounded on the operations in each category.

4.1. Blockchain 1.0 This Blockchain is principally used for cryptocurrencies and it was introduced with the invention of bitcoin.

DOI: 10.17148/IJARCCE.2023.12661

4.2. Blockchain 2.0 Blockchain 2.0 is used in financial services and industries, which includes financial assets, options, swamps and bonds etc. Smart Contracts were first introduced in Blockchain 2.0, which can be defined as the way to verify if the products and services are sent by the supplier during a transaction process between two parties.

4.3. Blockchain 3.0 Blockchain 3.0 offers more security and is more superior to Blockchain 1.0 and 2.0 and it is highly scalable and adaptable and provides sustainability. It is used in various industries, such as the arts, health, justice, the media and in many government institutions.

4.4. Generation X This vision is the concept of a singularity where this blockchain service will be available to anyone. This blockchain will be open to all and will be operated by autonomous agents.

V. TYPES OF BLOCKCHAIN

Blockchain have evolved greatly in the last few years and, based on its different attributes, they can be divided into multiple types.

5.1. Public Blockchains Public blockchains are open to the public and any existent can be involved in the decision-making process by getting a knot, but druggies may or may not be served by their involvement in the decision-making process. No one in the network has power of the checks and is intimately open to anyone sharing in the network. The druggies of the blockchain use a distributed agreement medium to reach a decision and maintain a dupe of the tally on their original bumps.

5.2. Private Blockchains These types of blockchains are not open to the public and are open to only a group of people or organizations and the ledger is shared with its participating members only.

5.3. Sidechains These blockchains are also known as pegged sidechains, where coins can be moved from one blockchain to another blockchain.
One-way pegged sidechain and a two-way pegged sidechain.
The one-way pegged sidechain allows movement from one sidechain to another whereas the two-way pegged sidechain allows movement on both sides of two sidelines.

5.4. Permissioned Ledger In this type of blockchain, the participants are known and already trusted. In permissioned loggers, an agreement protocol is used to maintain a shared version of the truth rather than a consensus mechanism.

5.5. Distributed Ledger In a distributed tally blockchain, the tally is distributed among all the actors in the blockchain and it can spread across multiple associations. In a distributed tally, records are stored continuously instead of sorted blocks and they can be both private or public.

5.6. Shared Ledger Shared ledger can be an application or a database that is shared by the public or an organization.

5.7. Fully Private Proprietary Blockchains. These types of blockchain are not a part of any mainstream applications and applications differ from the idea of decentralization. These types of blockchains come in handy when it is required to share data within an organization and provide authenticity of the data. Government organizations use private or proprietary blockchains to share data between various departments.

5.8. Tokenized Blockchains These are standard blockchains which generate cryptocurrencies through a consensus process using mining or initial distribution.

5.9. Tokenless Blockchains These blockchains aren't real blockchains as they don't have the capability to transfer values, but they can be useful when it isn't needed to transfer value between bumps and there's only the need to transfer data among formerly trusted parties.

VI. ADVANTAGES OF BLOCKCHAIN

a. One of the biggest advantages of Blockchain is Dispersion, which allows a database to be participated without a central body or reality. Because of the decentralized nature of the blockchain, it's nearly insolvable to temper the data as compared to conventional databases.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12661

b. Druggies are empowered to control their information and transactions.

c. Blockchains give complete, harmonious and over-to-date data without delicacy.

d. Since blockchain doesn't have any central point of failure due to its decentralized network, it can repel any security attack.

e. As no central authority is required, druggies can be assured that a sale will be executed as protocol commands.

f. Blockchains give translucency and invariability to the deals cannot be altered or deleted.

g. Blockchain's peer-to-peer connections help to identify fraudulent conditioning in the network and distributed agreement. It's nearly insolvable to foray a network as bushwhackers can impact the network only when they get control of 51 of the bumps.

h. By using blockchain, sensitive business data can be defended using end to end encryption.

VII. DISADVANTAGES OF BLOCKCHAIN

a. Blockchains are precious and resource ferocious as every knot in the blockchain repeats a task to reach agreement.

b. In the blockchain, users verify a transaction based on certificate authentication, land titles, cryptocurrencies, etc. But there is no way to reverse a transaction even if both the parties involved in the transaction are ready to do so or if the transaction goes sour due to some reason.

c. A sale on the blockchain is settled only when all the bumps in the blockchain successfully corroborate the sale. This could be a veritably slow process as the block fitted needs to be vindicated to mark the sale as authentic by all the bumps. A new conception called a lightening network where deals can be vindicated incontinently could be a good result to this issue.

d. The size of blockchain grows with the addition of a block. A knot needs to store the entire history of the blockchain to be a party in validating deals, causing the blockchain to grow continuously. Blockchain will grow briskly if it has large blocks and the result would separate the miners, and this would impact the health of the blockchain as Health is dependent on the number of bumps in the network.

e. On the blockchain, all the sale affiliated information is available intimately, which can become a great liability when distributed ledgers are used in sensitive surroundings similar as dealing with government data or cases' medical data. The checks need to be altered and access should be limited with proper concurrence only.

VIII. BLOCKCHAIN'S INDUSTRIAL USE

Blockchain's transparent and decentralized platform has attracted various industries and organizations are inclining more and more towards using blockchain for various business purposes. Banks and payment systems have started using blocks of the blockchain to make their operations smoother, more efficient and secure. Funds can be efficiently and safely transferred with decentralization technology. Blockchain has become increasingly popular among providers as it is able to restore the lost trust between the customers and healthcare providers. With the help of the blockchain, authorization and identification of people have become easier and fraud and record loss can be avoided. Due to the blockchain's ability to store and verify documents efficiently, the legal industries have started using the blockchain to verify records and documents securely.

Blockchain can significantly reduce court cases and battles by providing an authentic medium to verify and confirm the truthfulness of legal documents. Rigging of election results can be avoided with the effective use of blockchain. Voter enrollment and confirmation can be done using blockchain and ensure the legality of votes by creating a intimately available tally of recorded votes. Diligence similar as insurance, education, private transport and lift sharing, government and public benefits, retail, real estate etc. have started enforcing blockchain to reduce costs, to increase translucency and to make trust. Top market analysts predict that industries such as Banking and Capital Markets, Government, Insurance, Consumers will grow rapidly by 2020 and various other industries such as retail, health, pharmaceuticals, travel and transport will also start to use blockchains heavily in their respective domains. will be effective.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12661

IX. PRACTICAL IMPLEMENTATION OF BLOCKCHAIN IN ORGANIZATIONS

For an association, the stylish area to start enforcing the Blockchain is a single-use independent operation where no collaboration is needed among different operations and third parties. An easy approach to apply blockchain would be to introduce bitcoin as a payment system since bitcoin formerly has a solid and proven armature and it also has a growing request. Another safe and effective approach would be introducing the blockchain as a database technology for managing and maintaining digital transaction records.

Testing out these single-use independent applications would give an organization the idea of implementing the blockchain as scaled projects. As the next step, organizations can focus on localized applications such as Financial Service companies, where setting up private networks for transactions among their counterparts would help the organizations to save huge transaction costs. It's always a challenge to change the being results and apply a new and better solution which requires thorough planning and prosecution.

A good approach would be without affecting the end users but by providing cost-effective and efficient solutions which should be easily adaptive. Though transformative applications are still futuristic, it's important to evaluate their possibilities and start developing them which can unlock a new future for companies. Public identity systems or algorithm-driven decision-making systems can be benefited by transformative applications and new ecosystems will be governed efficiently with the support of these applications.

X. CONCLUSIONS

Blockchain is a revolutionary concept as it has been successfully able to bring transparency among the users and has become a game changer for many industries. Blockchain encourages entrepreneurship by destroying corruption and breaking down the walls of bureaucracy and establish the power of common millions.

This peer-to-peer technology has opened the door to new possibilities and has handed a particular ground for profitable commission. It's too early to say what lies ahead, but the future of blockchain looks promising and it can be concluded that blockchain technology is then to stay.

REFERENCES

[1] Pilkington, Marc. "11 Blockchain Technol-Ogy: Principles and Applications." Re-Search Handbook On Digital Transfor-Mations (2016): 225.
[2] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Tech-Nology: Beyond Bitcoin. Applied Innova-Tion, 2, 6-10.
[3] Atzori, Marcella. "Blockchain Technology And Decentralized Governance: Is The State Still Necessary?" (2015).
[4] Zheng, Zibin, Et Al. "An Overview of Block-Chain Technology: Architecture, Consen-Sus, And Future Trends." Big Data (Bigdata Congress), 2017 Ieee International Congress On. Ieee, 2017.
[5] Malinova, Katya, and Andreas Park. "Market Design with Blockchain Technology." (2017).
[6] Nguyen, Quoc Khanh. "Blockchain-a financial technology for future sustainable development." Green Technology and Sustainable Development (GTSD), International Conference on. IEEE, 2016.
[7] Ammous, Saifedean. "Blockchain Technology: What is it good for?." (2016).
[8] Cachin, Christian. "Architecture of the hyperledger blockchain fabric." Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Vol. 310. 2016.
[9] Condos, James, William H. Sorrell, and Susan L. Donegan. "Blockchain technology: Opportunities and risks." Vermont, January 15 (2016).
[10] Pilkington, Marc. "Blockchain technology: principles and applications. Research handbook on digital transformations, edited by f. xavier olleros and majlinda zhegu." (2016).
[11] Subash Thota, 2017. Analytics – Life Cycle. International Journal of Multidisciplinary Research and Development, pp. 117-126. http://www.allsubjectjournal.com/archives/2017/vol4/issue1 2/4-12-33.
[12] Nofer, Michael, et al. "Blockchain." Business & Information Systems Engineering 59.3 (2017): 183-187.
[13] De Filippi, Primavera, and Samer Hassan. "Blockchain technology as a regulatory technology: From code is law to law is code." arXiv preprint arXiv:1801.02507 (2018).
[14] Ahram, Tareq, et al. "Blockchain technology innovations." Technology & Engineering Management Conference (TEMSCON), 2017 IEEE. IEEE, 2017. Computer Science and Engineering 2018, 8(2): 23-29 29
[15] Boucher, Philip. "What if blockchain technology revolutionised voting." Unpublished manuscript, European Parliament (2016).

DOI: 10.17148/IJARCCE.2023.12661

[16] Iansiti, Marco, and Karim R. Lakhani. "The truth about blockchain." Harvard Business Review 95.1 (2017): 118-127.
[17] Sarmah, Simanta Shekhar. "Data Migration." Science and Technology 8.1 (2018): 1-10.
[18] Foroglou, George, and Anna-Lali Tsilidou. "Further applications of the blockchain." Columbia University PhD in Sustainable Development 10 (2015).
[19] Mougayar, William. The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons, 2016. [20] Bashir, Imran. Mastering Blockchain. Packt Publishing Ltd, 2017. [21] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127

BIOGRAPHY

Mr. Rohan Anil Torankar, UG Candidate of Computer Science and Engineering, Shri Sai College of Engineering and Technology, Bhadrawati

Area of Interest : - Cloud computing , Blockchain Technology, Data Science

