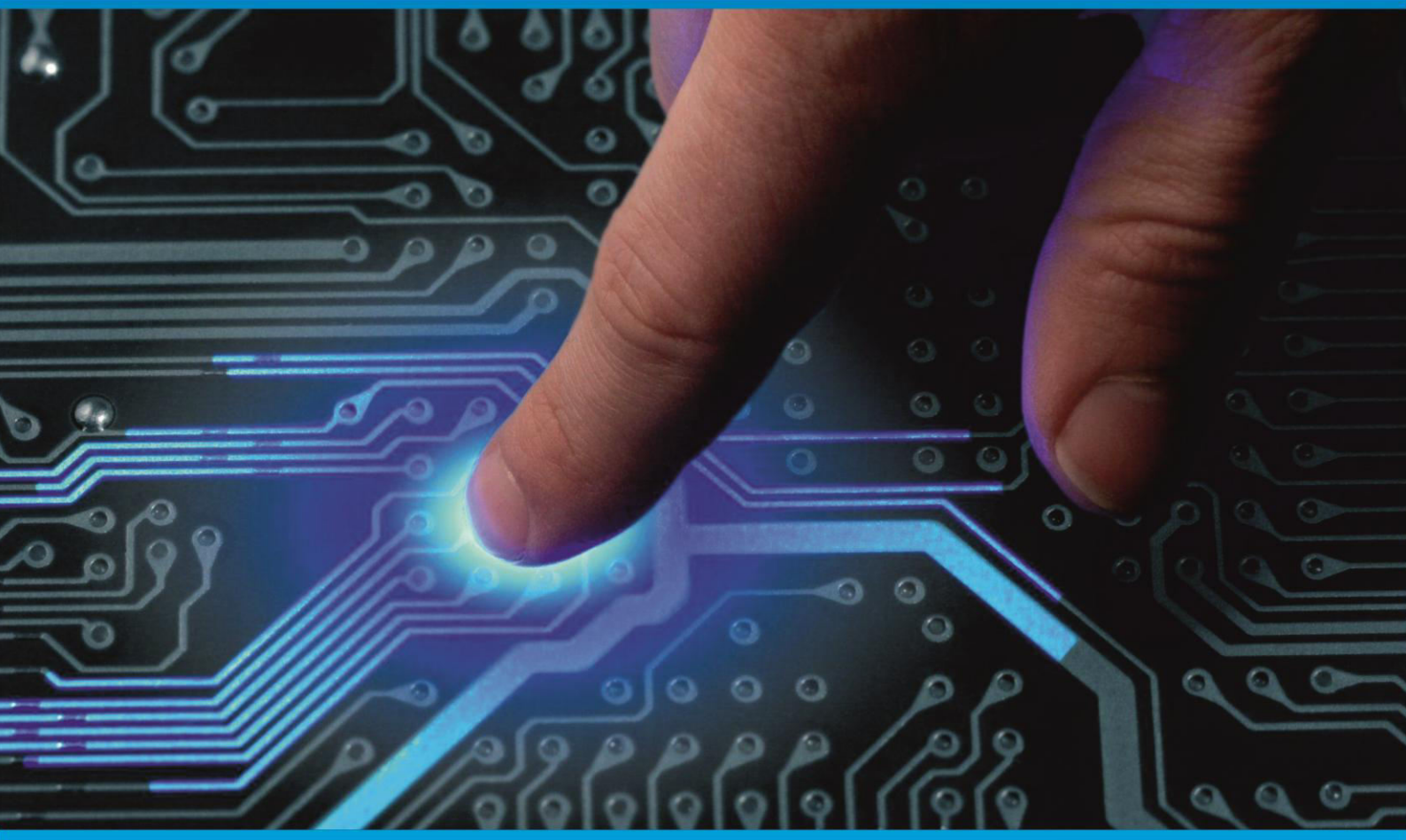
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 7, July 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007054 |

Medical Supply Chain Management using Blockchain

Gourav Jadhav, Abhishek Dhane

Analyst - Wipro Limited, India

PGD in UI/UX Student, Bhartiya Vidya Bhavan's Sardar Patel Institute of Technology, Mumbai, India

ABSTRACT: The blockchain technology has been developed over the course of the last decade in a variety of sectors, including finance, government, energy, health care, and many others, and it has achieved substantial acceptance. This article provides a comprehensive analysis of the blockchain technology used in the medical industry. In point of fact, the research that is still being conducted in this area is making remarkable strides. As a result, we have developed several contemporary applications for the blockchain technology, such as the sharing of electronic medical data, remote patient access, the medical supply chain, and other applications. Interoperability, security, authenticity, accountability, and seamlessness are essential qualities for stakeholders in the sectors of medical services. The blockchain network, which is hosted on the Internet, has the overarching goal of enabling peer-to-peer and interoperable usage of existing health data through a method that is patient-centric and does not involve third parties. This technology makes it possible to construct apps that can handle and communicate systemic fraud audit trails in a way that is protected, open to scrutiny, and unchangeable. This study does a literature review to determine the most significant obstacles that various health professionals are now experiencing and to evaluate the characteristics of blockchain technology that have the potential to address these concerns. At addition, we focused on identifying the shortcomings of the methodologies that were investigated, and in the conclusion, we discussed open-ended research as well as further research fields. On the other hand, future study has to concentrate on the difficulties and drawbacks of using this technology.

KEYWORDS: Supply chain management, blockchain technology, Smart contract, Distributed ledger, Business process re-engineering

I. INTRODUCTION

For the most part, the document certificate and privacy is extremely essential to give security for private information, and there have already been several platforms developed to store such a sort of massive data in a secure manner. In order to reach the maximum possible level of documentation dependability, several centralized cloud storage solutions include data encryption mechanisms. The real-time verification of huge documents is a highly laborious operation that requires a significant investment of both time and a significant amount of resources. For the purpose of verifying employees, students, and any other government documents by various entities, where manual processes have been followed by those organizations for a couple of years now. This includes employee verification, student document verification, and any other government document verification. The documentation that employees and students provide should be subject to random checks by both institutions and industrial organizations. This research significantly lowers the cost of traditional current systems by eliminating the need for such labor-intensive methods.

Blockchain: In its most fundamental form, blockchain technology is a decentralised data storage system that may be used to a variety of different transactional activities. Essentially, it is put into place so that the maximum possible level of data security can be attained during data transactions, and so that harmful requests from various networks, as well as data assaults, may be obliterated.

Decentralization: In order to eliminate many-to-one traffic sources, we need a decentralised system that can both ensure power and agility. By using such decentralised frameworks, we are also able to eliminate complications involving a single purpose of discontent or the delay of data. Within the context of our approach, a decentralised overlay structure is used.

Data authentication: Information that does not need to be kept and should be sent to blockchain networks is often stored in the user system or in the cloud administration. During the transfer, the specifics might get corrupted or be lost entirely. The stability of such information, which may have been changed off base, adds weight to the system, which may cause the patient to lose weight (demise). In order to assure that the information is not altered in any way, we use a lightweight advanced mark [2] layout along these lines. On the receiving end, information is validated by comparing it to the client's advanced mark; in the event that validation is successful, a receipt of information is sent to the patient.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007054 |

Adaptability: The problem of computationally increasing the proof of work (PoW) has been overcome; in any event, IoT devices have asset limits. In a similar vein, the Internet of Things (IoT) system is comprised of a number of hubs, and blockchain does not scale well as the number of hubs in the system increases. Our overlay system does away with the Proof-of-Work (PoW) principle and divides our overlay into many chains of squares rather than a single chain of squares. As a result, a single blockchain is not accountable for our overlay system when all aspects are taken into account. Instead, we dispersed the hubs among more than a few of different classes. Our model is dependent on the presence of the system in a distributed manner as well as various extra security aspects.

Data Storage: We utilise cloud servers to store encrypted data squares since it is not ethical to keep large amounts of information related to the internet of things (IoT) via blockchain. The data is safe when it is stored in the cloud because of additional layers of cryptographic security, such as the exclusive precondition encryptions and the sophisticated signature, both of which will be evaluated in the future. In any case, it can create a challenge in terms of trusting people from the outside. In order to accomplish this goal, we use Merkle Tree to record all of the transactions in separate squares. We then generate a consolidated hash of each square and send it on to the scattered scheme. Along similar lines, some of the changes that have occurred in the cloud's data may be readily examined. It is common for some degrees of decentralisation to be preserved when the capacity is done as such.

Consumer anonymity: The medical records of a patient may include sensitive information; thus, the information must be anonymized before being sent via the system. We supplement advanced markings with the lightweight ring structure[2] in order to increase the level of obscurity. An endorser has the ability to sign information namelessly by using the ring mark. This is because the mark is mixed in with several groupings known as the named ring, and no one is aware of which portion of the message is signed (apart from actual underwriter).

Data security: The information included in medical devices or databases must be precise, and their programmers are not permitted to make any changes. In order to protect the data from being accessed by programmers, we are using a scheme that involves double encryption. In this context, "double encryption" does not refer to the process of scrambling the same information with the use of two different keys; rather, it refers to the encoding of information as well as the encryption of key information. Next, we encrypt the key by utilising the beneficiary's open key to scramble the key, and then we encrypt the contents using the lightweight ARX computations. We also employ the key exchange method developed by Diffie Hellman to transmit open keys since it is almost unimaginable for an adversary to acquire the keys in this manner.

Digital Certificate: There is only one kind of document known as a digital certificate, and its specifics are much too complicated to be explained here. E-certificates have been utilised to facilitate both the sophisticated end uses of indication and the private movement of data in several areas of computer science in the modern age. Whoever worked here was the one who recommended utilising blockchain technology to generate electronic certifications for educational papers. This certificate was produced using a system that is based on automated approach. It was developed utilising a variety of different secure methods.

II. LITERATURE SURVEY

The A.G. Said to et. et. Al.[1] made a proposal for an authentication method for systems. Using Blockchain as a shorthand, the goal of the programme is to build an electronic credential at the request of the applicant. This will be accomplished by creating a legal electronic certificate registry. At the same time, the record of that student is kept by utilising hash values that are stored in blocks that are part of the blockchain. In addition, the buyer is given either a legible QR code or a serial number that complies with the requirements of the E-certificate. Instead, the demand unit (such as the organisation to which the applicant has applied for a job) is the one who is responsible for ensuring that the applicant's electronic file is legitimate by referring to the information that is stored in the blockchain and verifying it with either the QR code or the relevant serial number.

Cheng Jiin-Chiouet al.[2] proposed a digital certificate system that uses Blockchain and smart contracts. The next step would be to create an electronic paper record file that follows those pertinent pieces of information into the database, which would then determine the hash value of the electronic file. At the very end of the chain procedure, the hash value that is contained inside the ring is saved. The application will create a relevant QR code and query string information that will need to be fastened to the paper credential in order to function properly. Included in the package will be the demand gadget for verifying the authenticity of paper certificates by scanning them with mobile phones or inquiring about them online. Not only does the network increase the authenticity of paper-based certificates thanks to the immutable nature of the blockchain, but it also reduces the likelihood that electronic certificates of various kinds will be fraudulently used. There are many different kinds of certificates.

And Marco Baldi et. Al. [3] Certificate Validation Through the use of Shared Ledgers and Blockchains, the programme finds a solution to the issue by putting into action a process in which a number of CAs collaborate to share an open, shared, and secure database in which CRLs are stored. To this aim, we see the concept of decentralised

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007054 |

blockchain-based ledgers used for the usage of cryptocurrencies, which is becoming an increasingly popular option for meeting the high security and dependability criteria of a number of online services.

About Oliver et al.[4] highlights the application of blockchain as a monitoring and assessment method for government degrees. This study is a market comparison centred on two financial elements that contrast the price of the service as the major player that sits between the customer and the employer. Students want evidence of their competence that is both inexpensive and simple to verify, while businesses often require prompt and dependable verification of an applicant's degree before employing them. Each model is intended to uncover new avenues for developing this industry inside the European Union, with the end goal of growing regional markets and market shares.

Because of the arbitrary nature of hashing, there is never a guarantee that the process will produce an object that is adequate for its intended use. Mining for bitcoin is consequently a competitive enterprise in which miners are hashed and accepted into the network successfully by awarding fresh Bitcoin for each block [5]. Miners are a collective user network that validate and monitor transactions in addition to setting up specialised computer equipment known as "hashes." Voting using the processing power of their CPUs, they show their approval of genuine blocks by helping to expand them and by refusing to operate on fraudulent blocks [6]. These record strings, also known as hashes, are copied throughout the Bitcoin network on every computer so that a record may be kept of every Bitcoin transaction ever made.

Blockchain is a distributed ledger that may be used to safely trade digital currency, conduct transactions and business dealings [7], and it can also be used to regulate the peer-to-peer network. All of the nodes adhere to the same internode communication protocol, and any newly added artefacts are subjected to inspection. If the data in any block is verified, subsequent blocks will be unable to change it. In order to modify the data of an individual block, all relevant block data will need to be updated, which will result in the nodes of the network cooperating to reject the transaction. As the price of the cryptocurrency continues to rise, one important component is the amount of electricity that is needed to "farm" it. People all around the globe are spending more than 30 terawatt-hours of power to mine the cryptocurrency Bitcoin, according to the website Digiconomist that compiles information on Bitcoin. This is more than the population of at least 159 countries that make use of human resources, such as Hungary, Oman, Ireland, and Lebanon[8].

Mining for bitcoins is a relatively new technique for acquiring bitcoins, and it is produced by validating transactions on the Bitcoin Network. The transaction is saved in a public ledger, which is then examined and updated by all of the computers that are a part of the Bitcoin network. The "net" sum of all transactions is recorded in what is known as the ledger. A transaction is, in its most fundamental form, a timestamp for a database that could include some data [9]. According to Narayanan and his colleagues' definition [10], a block string is a data structure that is made up of a linked series of hash references. Any object in the list may be considered a block if it contains the data and hash of any previous block. It is now a tamper-evident file, which means that new data may only be added to the list; existing data cannot be changed without being discovered first.

The Hyperledger Sawtooth platform makes advantage of a flexible architecture that partitions the many different components of the system. This suggests that the blockchain level and the execution stage are no longer related to one another. Because of the adaptable nature of the design, various components of the network may be modified in response to changes in the requirements of the project. The transaction rules algorithm, the creating algorithm, and the consensus algorithm are all examples of modules that are subject to change. [11] Lamport et al. [12] propose methods that, under a variety of conditions, make it possible for the generals to come to an agreement with one another. The authors provide evidence that demonstrates how the issue may be resolved using any number of traitors and generals in a system in which the generals are able to send registered letters that cannot be forgiven. However, due to the extensive amount of communication that would be required, the cost of using this strategy will be rather high.

Proof of elapsed time, often known as PoET, is a built consensus solution that has shown to be more effective than proof of work (PoW). One interpretation of PoET is that it is a feature that arbitrarily causes a node to wait. The system is able to identify any users who are attempting to execute before their allotted random amount of time has passed because of the function that decides how much time a node may wait in what is known as a "trusted execution setting [13].

They either have a website, a globally dispersed library, or a worldwide environment. The global state consists of every piece of information that can be found in the ledger, including the most up-to-date status. There is a substantial amount of variety in the information that is applied to the global state depending on the blockchain sense [14].

The transactions are compiled as batches in Hyper ledger Sawtooth for use in other blockchain applications. Batches are used in situations when the sequence of the transactions is critical. It is important that transactions be carried out in the proper sequence, which may be accomplished by placing related transactions inside the same group of transactions. If a transaction does not depend on any other transactions other than those that have already been

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007054 |

validated and deposited in the blockchain, the sender is only permitted to generate a new batch for that transaction. This is the case if the transaction in question does not involve any other transactions. [15].

III. PROPOSED SYSTEM

From a functional point of view, this system illustrates the implementation of public using blockchain in both innovation and utilization contexts for such a proposal. A future roadmap for blockchain technology to be able to support complex applications is to complete this work. For a long time, creating an electronic payment system that meets legislators' legal requirements has been a challenge. In the digital world, distributed ledger systems are an exciting technical development. An endless number of applications benefiting from shared economies are provided by blockchain technologies. The purpose of this paper is to examine the use of blockchain as a service to incorporate electronic distributed transaction systems.

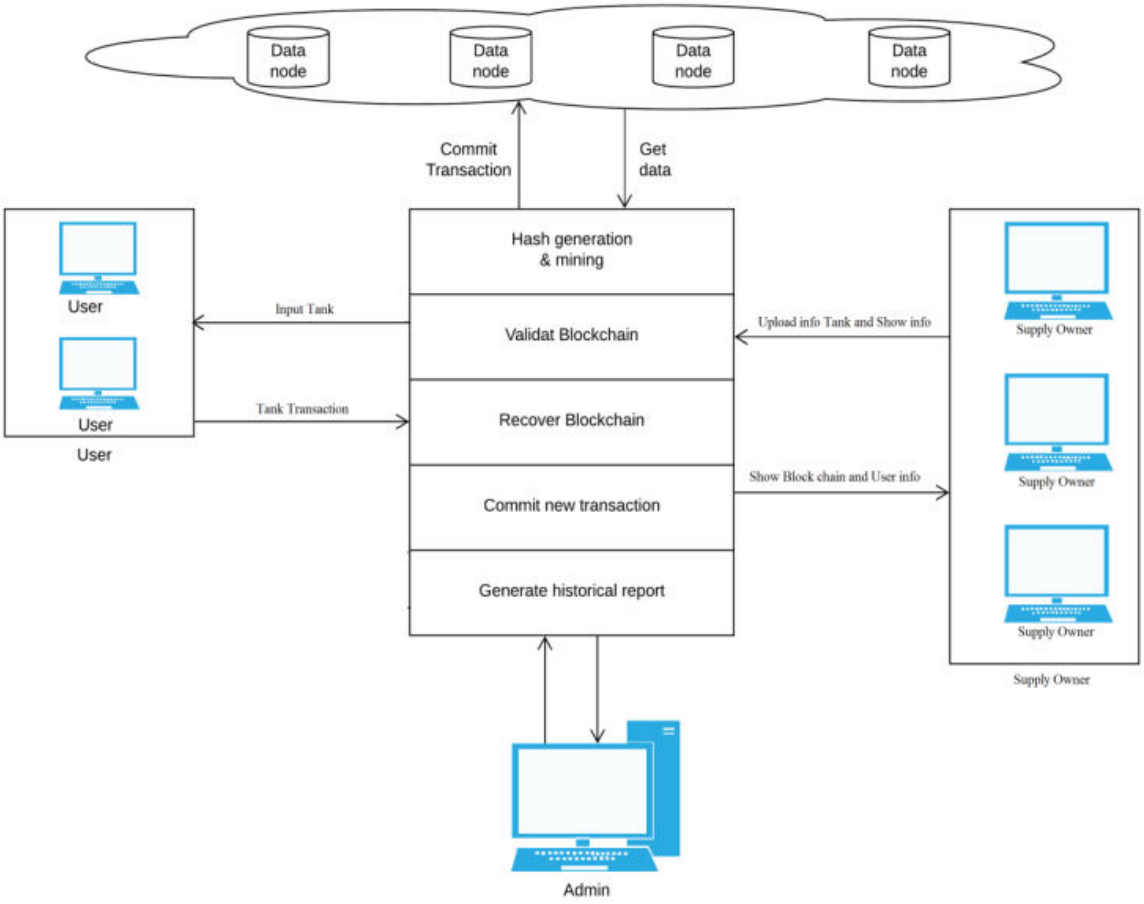


Figure 1 :Proposed System Architecture

Module Description

The system contains following modules:

1: Admin
2: Create transaction
3: Block Generation and blockchain validation
4: Consensus Algorithm validation and block chain recovery
5: Results Generation

- The management of operations management data delivery storage using the block chain is the core outline of the proposed algorithm.
- Without using any third party interface, the device creates trustworthy contact between different parties.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007054 |

- We use the algorithm of Hash generation and for the given string, the Hash will be generated.
- To validate the data, we use peer to peer verification before executing any transaction.
- If a chain is null, the current server blockchain will be restored or modified.
- This will be checked before the query is confirmed and committed to all nodes.
- The mining algorithm is used to verify the generated hash for the query until the current hash is generated..

Algorithm Design

1 : SHA 256 based Hash Generation
Input : initial transactional or input data Data[]
Output : Generation hash using SHA256 algorithm
Step 1 : Input data data[]
Step 2 : Perform SHA 256 from SHA suitable algorithms
Step 3 :New Hash= SHA256(data[])
Step 4 : Retrun String(**New**Hash)

Algorithm 2 : Protocol for peer to Peer node verification
Input : User input query, Current Node blockchain Current_Node[chain], Additional Outstanding Nodes blockchain NodesChain[Node_id] [Node_chain],
Output : Automatic recover blockchain if nodes fails
Step 1 : Transactional data or any event data for input to blockchain
Step 2 : Extract kth server's blockchain of time[t]
Current_chain←Current_node[Chain]
Step 3 : foreach

$$NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$$

End for
Step 4 :foreach (i into Node_Chain)
If (!.equalsNodeChain[i] to (Current_chain))
FlagVal 1
otherwise continue; commit query into the nodes
Step 5 :if (FlagVal == 1)
CCount = SimilarityyNodesBlockchian()
Step 6 : Determine majority of all server
Recover inacceptable blockchain from precise node
Step 7: end if; end for; end for
3. Transaction Mining Algorithm to generate valid hash
Input : Smart contract SC[], Transactions current hash CH[], Previous hash or genesis block PH[]
Output : Generate of valid hash and nonse
Step 1 : Generate the hash_Value for kth transaction consuming Algorithm no. 1
Step 2 :if (hash_Value.valid to smart_contract [])
Current hash is validate
FlagVal =1
Else
FlagVal=0
Continue; Mine the current hash again for next iteration
Step 3 : Return validated_hash[] till when flagVal = 1

IV. RESULTS AND DISCUSSIONS

In the part devoted to the results, we put the suggested classification method to the test by analyzing both sections with regard to performance assessment, blockchain execution, and the accuracy of false news identification. The system operates using a workstation with an Intel i3 processor running at 2.8 GHz and 4 gigabytes of random-access memory in a distributed way on a Java 3-tier analytics platform. This Liar dataset was used for the partial implementation of something that was collected from www.kaggle.com. Figure 2 demonstrates the amount of time necessary for a consensus to be reached using Proof of Work (PoW) in order to authenticate the blockchain across a minimum of 4 nodes. In order to validate the findings, we have shown our first experiment and study on the deployment of blockchain technology.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007054 |

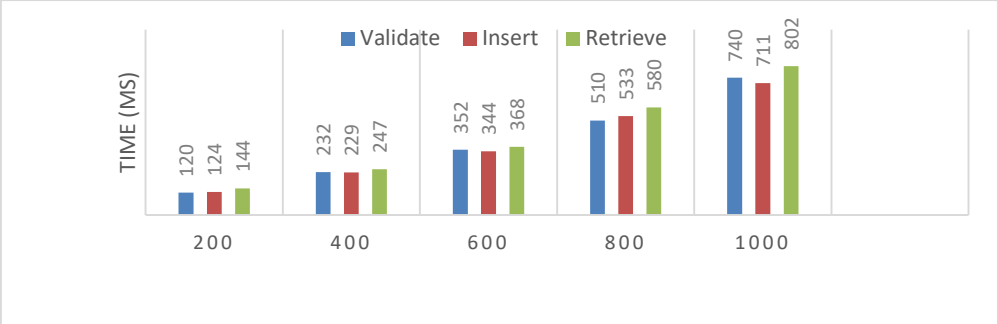


Figure 2: Time required for transaction with no. of transactions with blockchain

In the next experiment, we will assess a system that includes smart contract validation for a specific consensus mechanism in peer-to-peer environments with varying numbers of data nodes.

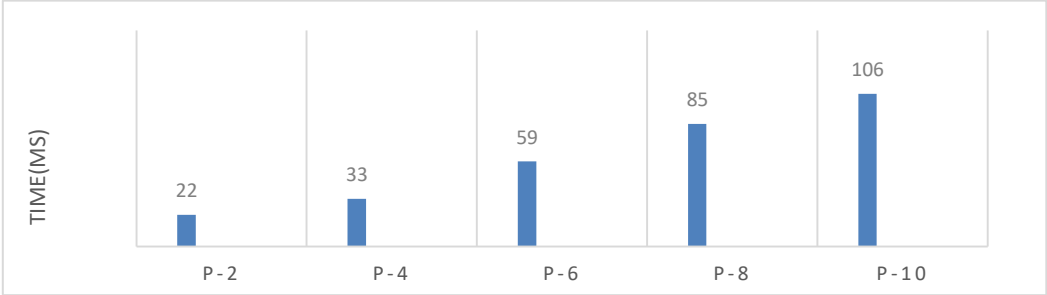


Figure 3: Time required for smart contract validation with different no. of P2P network in blockchain.

In the third test instance, an examination of the total variability that was derived from the SHA value that was suggested by the model is carried out. This was done with the intention of determining whether or not the suggested hash sequence is legitimate and in accordance with the mining policy that has been established. When the system creates SHA code for the specified transactional data, the computing policy is never fully satisfied, which is the case in many circumstances. In light of the mining circumstances, in order to adhere to the mineral extraction strategy, it is necessary to generate a number of distinct permutations on the text sequence. Figure 4 is an illustration of the amount of time required to construct the appropriate SHA string for a given transaction.

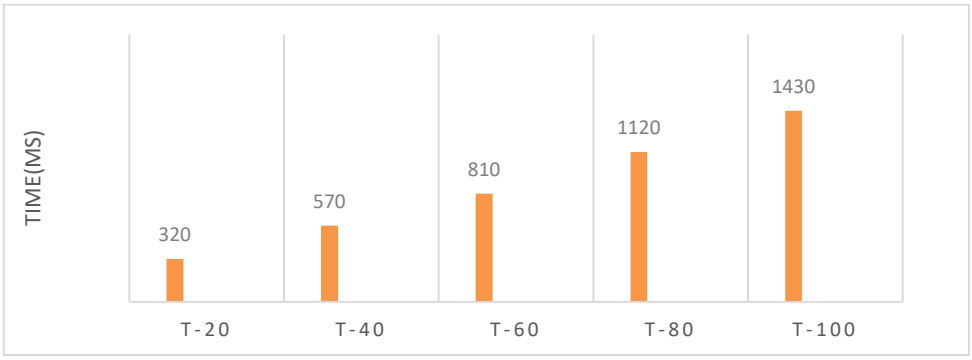


Figure 4: Time required for generation of valid hash for number of transactions

The data shown above illustrates the amount of time necessary to generate a valid hash for each kind of transaction, according to the definition of smart contracts. The production of a valid hash might at times be contingent on the complexity of the algorithm and the processing environment. When a smart contract specifies extra challenges for hash generation, the amount of time required for the development of a valid hash is increased to its maximum nonce.

V. CONCLUSIONS

Due of the particulars of this business and the need for more strong and effective information management frameworks, there are various research proposals to use Blockchain technology to the transaction industry. An interoperable

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007054 |

architecture has the potential to unquestionably play a big part in several applications of transaction usage that struggle with issues relating to the exchange of data and communication. In order to educate software engineers and domain experts on the potential as well as the limitations of this new technology, whether to create a decentralized application using an existing Blockchain, additional research on secure and efficient software practice for the use of Blockchain technology in transactions is also required. This is necessary in order to create a decentralized application using an existing Blockchain. The algorithm has made the proper decisions about the complexity, performance, and complexity of implementation so that the method may be executed. As a result of doing longitudinal research, we have a more refined comprehension of the rate at which new information is generated throughout the supply chain. There are a number of significant obstacles that must be overcome in order to realise the whole potential of the blockchain, the most important of which is the scalability of the technology and the data controls required to apply it to health care.

REFERENCES

[1] A.G. Said, R.P. Ashtaputre, B. Bisht, S.S. Bandal, P.N. Dhamale, "E-Certificate Authentication System Using Blockchain," International Journal of Computer Sciences and Engineering, Vol.7, Issue.4, pp.191-195, 2019.
[2] Cheng JC, Lee NY, Chi C, Chen YH. Blockchain and smart contract for digital certificate. In2018 IEEE international conference on applied system invention (ICASI) 2018 Apr 13 (pp. 1046-1051). IEEE.
[3] Baldi M, Chiaraluce F, Frontoni E, Gottardi G, Sciarroni D, Spalazzi L. Certificate Validation Through Public Ledgers and Blockchains. InITASEC 2017 (pp. 156-165).
[4] Oliver M, Moreno J, Prieto G, Benítez D. Using blockchain as a tool for tracking and verification of official degrees: business model.
[5] George F. Hurlburt and Irena Bojanova, "Bitcoin: Benefit or Curse?," in IEEE, 2014
[6] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, White Paper.
[7] Nirmala Singh and Sachchidanand Singh, "Blockchain: Future of financial and cyber security," in IEEE, Noida, 2016.
[8] Henrique Rocha ,MarcusDenker and Stephane Ducasse Santiago Bragagnolo, "SmartInspect: solidity smart contract inspector," in IEEE, Itly, p. 2018.
[9] GWYN D'MELLO. (2017, Dec.) https://www.indiatimes.com/technology/news. [Online]. https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more-electricity-than-irelandother-159-countries-no-kidding-335114.html
[10] Narayanan A., Bonneau J., Felten E., Miller A. & Goldfeder S. (2016) Bitcoin andCryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press
[11] Introduction to Hyper ledger Sawtooth (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/introduction.html) 49
[12] Lamport, L., Pease, M., &Shostak, R. (1982). The Byzantine generalsproblem. Menlo Park, CA: SRI International.
[13] PoET 1.0 Specification (2018) Retrieved January 4, 2019 fromhttps://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html
[14] Global State (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/global_state.ht ml
[15] Transaction and Bathces (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/transactions_and_batches.html

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details