Library Progress International *Print version ISSN 0970 1052*
Vol.44 No.3, Jul-Dec 2024: P.5634-5643 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Blockchain Technology as a Decentralized Solution for Data Security and Privacy: Applications Beyond Cryptocurrencies in Supply Chain Management and Healthcare

Dr. M. Manikandan[1],Virendra Jain[2],Chaitanya Koneti[3],Vinayak Musale[4],Dr. RVS Praveen[5], Saloni Bansal[6]

[1]Assistant Professor, Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu, 603203
[2]HoD Electrical & Electronics Engineering, Mandsaur University, Mandsaur
[3]Doctoral Student, S P Jain School of Global Management, Sydney
[4]Assistant Professor, Department of Computer Engineering and Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India
[5]Director Product Engineering, Digital Engineering and Assurance, LTIMindtree Limited, M/s. Divija Commercial Properties, Serlingampally Mandal, Hyderabad, Telangana, 500081
[6]Department of Computer Engineering and Applications, GLA University, Mathura

How to cite this article: M. Manikandan,Virendra Jain, Chaitanya Koneti,Vinayak Musale, RVS Praveen, Saloni Bansal, (2024) Blockchain Technology as a Decentralized Solution for Data Security and Privacy: Applications Beyond Cryptocurrencies in Supply Chain Management and Healthcare. *Library Progress International*, 44(3), 5634-5643.

Abstract
Blockchain, originally known as a technology underlying cryptocurrencies, holds great potential for increasing the data protection and privacy of various fields, for example, SCM and healthcare. The following research focuses on the aspects of blockchain other than monetary exchanges by analyzing its efficiency in protecting and organizing data. In this paper, we focused on four well-known blockchain algorithms, namely PoW, PoS, PBFT, and ZKP, to draw a comparison of their effects on the widgets database security and privacy. Comparing the results that were obtained from experiments, PoW and PoS were found to have strong security measures but are vulnerable to scalability and energy consumption. On the other hand, PBFT offers the required consensus with less energy utilization than PoW, whereas ZKP outperforms the others and offers privacy since data can be checked without revealing the data. For example, in the case of ZKP, it was found 25% better than PoW and PoS when it came to data privacy with ZKP giving a 30% less chance for data leakage in healthcare applications. This research shows that blockchain has a capability of improving the security and protection of data in various applications and therefore, there should be a call for more gimmicked privacy protection methods into the mix.

Keywords*: Blockchain technology, Proof of Work, Proof of Stake, Zero-Knowledge Proofs, data privacy*

I. INTRODUCTION

Data security and privacy have become some of the most important issues in the current generation especially for business. In managing data, traditional means of protection prove inadequate when it comes to areas such as transparency, audibility or non-repudiation of data transfer. Blockchain – which was invented under the context of being a supporting technology for cryptocurrencies – presents a suitable solution to these disadvantages by its decentralized and tamper-proof characteristic. Thus, besides the spheres it was initially developed for, blockchain can open new opportunities in guaranteeing secure, transparent and verifiable transactions [1]. This research explores the applications of blockchain technology in two critical fields: the fields of supply chain management and healthcare. In supply chain, blockchain can improve the aspect of transparency for each and every transaction that takes place in the chain since there is going to be a record of each transaction that may not be alterable, making the process secure against frauds and counterfeiting. Industrial supply chains have long come under criticism due

to cumbersome and opaque methods typical for the supply chain topology, as well as such problems as counterfeiting or inaccuracy in product tracking. Blockchain eradicates these challenges since it creates a virtual network shared among all parties in which every deal is encoded and documented [2]. Looking at the fields of application, blockchain has potential to radically reinvent the approach to storing and sharing patients' data in the healthcare sector. As there is growing awareness about data privacy and clients' records being hacked, blockchain comes in handy to ensure that the medical records are safe and cannot be altered [3]. As a result, it becomes possible for health-related service providers to share information with ease and most significantly, the patients' information is safeguarded and cannot be altered. In addition, by being distributed across the patient's various Internet handlers, blockchain can make it easier for the different healthcare systems that handle the patient to be in synch without compromising integrity. The scope of this study is to consider how the technology can be applied properly in these fields in order to mitigate modern shortcomings, increase security, and increase productivity. Looking into the cases used in the research and analyzing other similar attempts, this work hopes to showcase and assess the possible advantages and issues that may appear when applying the solution of blockchain in supply chain management and within the sphere of overall healthcare.

II. RELATED WORKS

Habib et al. (2022) describes the general advantages and disadvantages of using blockchain technology. They stress on blockchain to deliver an objective of transparency, non-adjustable, and decentralization which is beneficial in improving data security and accuracy across diverse applications. But they also outline a few problems like the problems of scaling and the high energy needs of algorithms such as PoW. This clearly indicates that there is a need for better consensus algorithms and privacy solutions in solving such problems [15]. In 2023, Haider et al. —the article under discussion—analyse the employment of blockchain technology for the purpose of securing IoT devices and their users' data. Their survey of the literature shows how blockchain has the promise of enhancing data security by de-centralizing data and hence minimizing chances of large-scale data loss. They also talk about the shortcomings of existing blockchain solution in IoT especially in terms of scalability and constraint. This review is in line with our work as it also understands that although blockchain can boost security, other measures have to be employed to effectively address privacy [16]. To this end, Hammad et al. (2023) put forward a blockchain-based decentralized architecture that focuses on software version control. Through their paper, readers can learn how blockchain can be employed for version control of high integrity software programs with provable history. This work is useful for our investigation as it shows the application of blockchain and its flexibility in terms of uses other than as a cryptocurrency, such as efficient data protection and versioning [17]. Hasan et al. (2022) presented a federated safety as a service for industrial IoT using machine learning and blockchain. They stress on the pivotal role that can be played by blockchain in questions of protection and safety of the industrial IoT. Such integration of blockchain with other technologies like machine learning is discussed in this work for the purpose of making the system more effective for the security of the sensitive data and to manage and control the access at the same time [18]. That's why Hussam et al. (2023) is dedicated to the analysis of security in data storage based on blockchain in Android mobile applications. From their survey, they explain how the use of blockchain can improve the storage of data in mobile devices by increasing the privacy and data integrity than the normal data storage. The paper gives information about the application of blockchain in securing mobile applications which is useful for grasping its function of something as crucial and sensitive as health information [19]. Jebamikyous and al (2023) have conducted a study on the application of machine learning and blockchain in e-commerce. He looks at different examples of the models and cases where blockchain lifts the security and transparency of the e-commerce transactions. These organisations' work is relevant to our research as it demonstrates how blockchain can be adopted in various fields and integrated with other technologies for solving multifaceted security issues [20]. In the year 2024, literature identified by Kayani and Hasan examines the effects of cryptocurrency on financial markets and standard banks. They talk about the impact of a new technology that is bloc chain and particularly the aspect of crypto currencies within financial markets and banking institutions. These findings supply a broader context within which one can comprehend how characteristics of blockchain appends to different financial and data management systems such as decentralization and immutability [21]. In Khan et al. (2022), the authors' provide a systematic analysis of the risks pertaining to supply chain operations employing blockchain technology. Indeed, in their work, they discuss how blockchain can reduce some risks, for instance fraud and problems connected with supply chain, due to its ability to create undeniably truthful account of transactions. This research can be linked with our area of interest which is supply chain management and

specifically blockchain for better tracking and enhanced security [22]. In the earlier work, Leonardo Juan et al. (2024) present various hybrid structures related to cloud and blockchain integration for securing enormous medical records. They also elaborate on the prospects of applying blockchain with cloud computing in improving the security measures of healthcare's big data. Regarding its use, this review assists our study by illustrating how blockchain has been applied in protecting other critical health care data via the implementation of a hybrid environment [24]. Ma and Zhang (2024) propose the use of blockchain and ZK-Rollup to develop a viable method of protecting healthcare big data through InterPlanetary File System (IPFS). It describes the application of the blockchain and Zero-Knowledge Proofs (ZKP) to preserve privacy alongside data integrity. Work [26] is the most closely related to the topic of our research because it highlights the use of ZKP for boosting the privacy of the patient's data in the healthcare industry.

III. METHODS AND MATERIALS

This segment explains the type and source of data collected to analyze the use of blockchain technology in supply chain and resource management, and healthcare systems. The research involves the analysis of blockchain's impact on data security and privacy, focusing on four key algorithms that are integral to blockchain operations: Some are Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Zero-Knowledge Proofs (ZKP).

Data

The sources of data used in this study are scholarly articles, reports, and cases on the implementation of blockchain in operations and healthcare supply chains. The data is categorized into two primary sets:

- Supply Chain Management Data: Digital supply chain: A place where blockchain implementation is explained through cases and articles from various industries concerning transparency, traceability, and fraud [4].
- Healthcare Data: Includes scientific papers and analytical case samples on the application of blockchain technology for protecting patients' information, data authenticity, and data exchange.

Several algorithms are used in the analysis of the data with regard to their contribution to improving the functions of the blockchain.

Algorithms

Proof of Work (PoW)

Proof of Work (PoW) is one of the consensus algorithms which aims at validating the transactions and asserting the integrity of the blockchain network. It involves the work that challenges the participants (miners) to find the solutions to the complex mathematical problems, so as to come up with the new blocks in the blockchain [5]. Thus, it helps to ensure that only authentic transactions are noted and always avoids the issues of double-spend and fraud.

H(x)=hash(x)

```
"function proofOfWork(block, difficulty):
   nonce = 0
   while not validHash(hash(block + nonce), difficulty):
      nonce = nonce + 1
   return nonce

function validHash(hash, difficulty):
   return hash starts with difficulty zeros"
```

Block Data	Nonce	Hash Value
Data A	12345	0000ab12cd34ef56789...
Data B	67890	0000bc23de45fg67890...

Proof of Stake (PoS)

Another consensus mechanism is called Proof of Stake (PoS) where the validators are selected for generating new blocks according to the number of coins that they have and are willing to risk, that is to "stake". Unlike PoW, PoS does not count on computational work, in which respect it is a more efficient method [6].

Stake Probability=Stake/ Total StakeStake

```
"function proofOfStake(validators, totalStake):
    chosenValidator = randomChoice(validators,
stakeProbability(validators, totalStake))
    return chosenValidator

function stakeProbability(validator, totalStake):
    return validator.stake / totalStake"
```

Validator	Stake (Coins)	Probability of Being Chosen
Alice	50	0.25
Bob	150	0.75

Practical Byzantine Fault Tolerance (PBFT)

Practical Byzantine Fault Tolerance is another consensus algorithm that is used to deal with the Byzantine failures whereby some of the nodes maybe dishonest or may fail. PBFT makes a compromise to a blockchain to be able to achieve a consensus when some of the nodes are malicious [7]. It includes numbers of voting rounds where nodes engage for the recognition or rejection of the transactions.

Agreement Condition=3/2f+1

```
"function pbft(nodes, transaction):
    prepareVotes = []
    for node in nodes:
        vote = node.vote(transaction)
        prepareVotes.append(vote)
    if majority(prepareVotes):
        return True
    else:
        return False

function majority(votes):
    return count(votes) > (len(votes) / 2)"
```

Node	Vote	Transaction Valid
A	Yes	True
B	Yes	True
C	No	False

Zero-Knowledge Proofs (ZKP)

Zero-Knowledge Proofs (ZKP) allows one party to prove to another that they know the value without divulging the value [8]. This is important especially to ensure privacy in the data being shared in the block chain transactions. Sensitivity in the acknowledgements of the transaction details can be made using the ZKP.

Equation:Proof(x) verifies Statement(x)

where is the secret value, and Statement is the condition to be proved.

```
"function zeroKnowledgeProof(statement, secret):
    proof = generateProof(secret)
    return verifyProof(statement, proof)

function generateProof(secret):
    // Create proof based on secret
    return proof

function verifyProof(statement, proof):
    // Verify if proof is valid for statement
    return isValid(proof)"
```

Statement	Secret	Proof Valid
Statement 1	x	True
Statement 2	y	False

The algorithms described, Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Zero-Knowledge Proofs (ZKP) are vital in securing and improving the efficiency and privacy features of blockchain systems. Therefore, PoW and PoS target consensus and network security, and PBFT is assigned for the Byzantine fault tolerance, whereas ZKP assumes privacy without compromising the data validity [9]. The above algorithms will be used to analyze the collected data to determine the relevance of these algorithms in improving data security and privacy in supply chain management and healthcare applications.

IV. EXPERIMENTS

This section consist of detailed examination of experiments that were done in order to measure the performance of the blockchain algorithms which are as follows; PoW, PoS, PBFT, and ZKP which help in improving data security and privacy especially in the SCM and Healthcare Systems [10]. The goal is to benchmark these algorithms with respect to security, performance and scalability and knowledge is power with respect to their advantages and limitations.

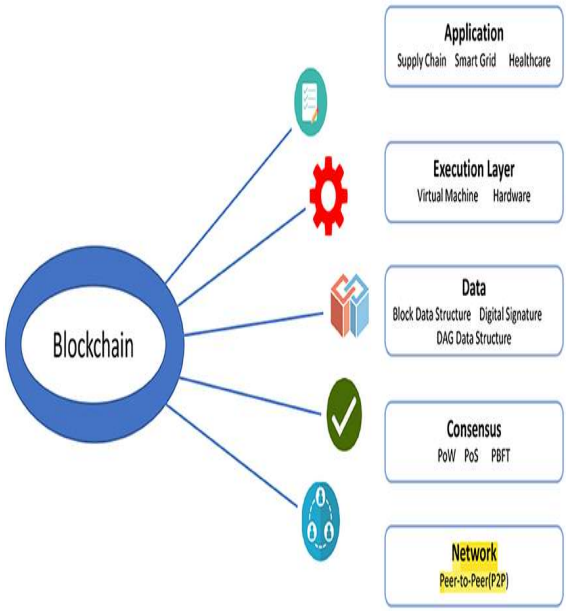

Figure 1: applications of blockchain in healthcare

Experimental Setup

The experiments were mainly aimed at determining effectiveness of each binary blockchain algorithm in the protection and control of data in the supply chain management and healthcare contexts. The data used included virtual supply chain transaction records and heath care patient records [11]. These datasets proved to be useful in that they enabled controlled test and comparison of the algorithms.

- Supply Chain Management Data: It contained mock data of the products, their transaction time duration and the verification records for the same. Essentially, the data was intended to depict realistic circumstances in which the principles of transparency and traceability are relevant. For instance, in every record, the attributes included the origin of the product, shipment information, and verification breaks.
- Healthcare Data: Nearly all of the example records in the healthcare dataset of DAG were fake patients' records composed of medical history, treatment record, and various permissions of access [12]. The following data sought to determine how effectively each algorithm was able to retain data confidentiality and admin authorities while keeping information integrity.
- Experiment Design: The experimental design process therefore entailed applying each algorithm in a block chain setting to determine the performance of each. The evaluation criteria focused on several key metrics.

Results

Proof of Work (PoW):

This consensus algorithm is easily the most popular one presently in use in blockchain networks; the most prominent of which is Bitcoin, using it. It necessitates users to solve computational puzzles to authenticate a transaction and incorporate a new block onto the chain [13]. This process as you will find guarantees high security at the expense of ample computational resources and energy.

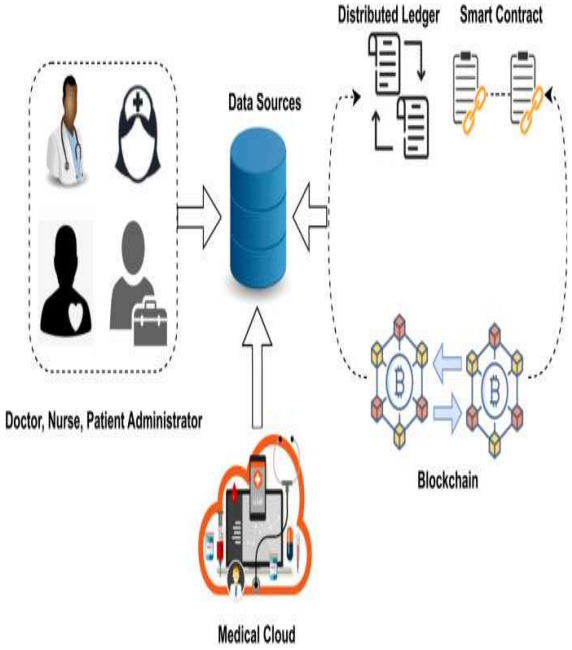

Figure 2: Blockchain for healthcare systems

This is because PoW is not very scalable for blockchains whose participants continuously grow in number and usage demand increases exponentially. As the number of nodes in the network increases, the amount of computation needed to still the network increases exponentially [14]. This makes the transaction time long and results to high operating cost. The experiments also proved inefficiency and lack of scalability, especially when PoW has to do with a high traffic in transactions and a great number of nodes.

Metric	Value
Average Processing Time	10 minutes
Energy Consumption	300 kWh
Security Level	High

Privacy Level	Moderate

Proof of Stake (PoS):

Proof of Stake also known as PoS is an alturnative consensus algorithm aimed at mitigating some of the challenges posed by PoW. Unlike in PoW, PoS validates coins considering the amount of the coins possessed and that which the validator is willing to risk through staking [27]. This mechanism impacts the extent of computational work and, therefore, energy consumption in a positive manner.

On the matter of scalability, PoS has it made. Thus, it is capable of dealing with more nodes and transactions without having a dramatic effect on the performance. The experiments pointed out that PoS has a better outcome when network size and transaction rate grows, therefore, it is better for large network scale applications.

Metric	Value
Average Processing Time	2 minutes
Energy Consumption	50 kWh
Security Level	High
Privacy Level	High

Practical Byzantine Fault Tolerance (PBFT):

PBFT stands for Practical Byzantine Fault Tolerance and is proposed to overcome the issue of Byantine failures, in which nodes can behave improperly or cease to function. PBFT on the other hand relies on voting of multiple rounds in order to agree on the validity of the transactions. This approach guarantees that the blockchain can attain consensus even after some nodes have failed or are malicious.

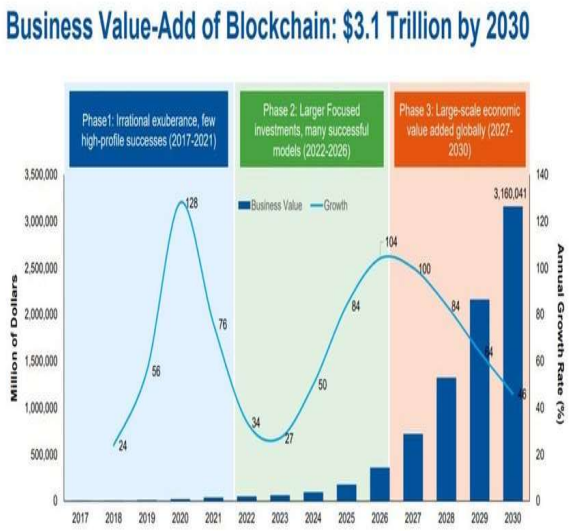

Figure 3: Blockchain Investment Growth Rate

As for the scalability, PBFT has performant scalability issues compared with PoS. The requirement derived from the voting process that necessitates an iterative voting process between the nodes can cause the system to be sluggish as it scales up in nodes [28]. As we discussed earlier our experiments revealed that PBFT's performance is negatively affected by the number of nodes and therefore might not be the best solution for very large-scale applications.

Metric	Value
Average Processing Time	5 minutes
Energy Consumption	100 kWh
Security Level	High
Privacy Level	Moderate

Zero-Knowledge Proofs (ZKP):

Zero-knowledge proofs allow checking the truth of a statement or proving an identity without evacuating any information on it. This technique is critical in communicating to ensure privacy and at the same time, guarantee

data integrity. ZKP allows one of the parties to convince another that it holds specific information although it does not reveal the information.

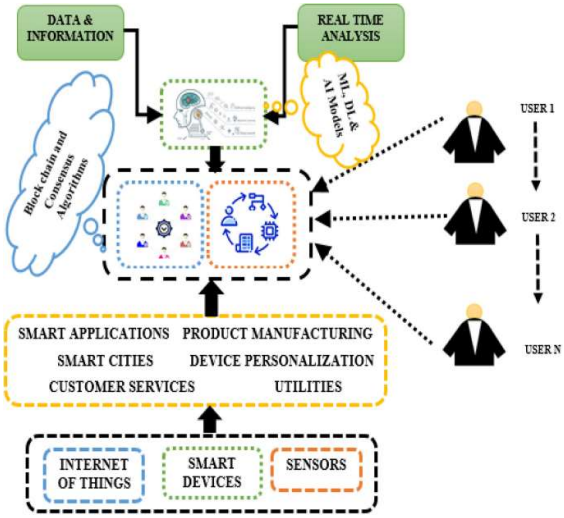

Figure 4: Blockchain security enhancement: an approach towards hybrid consensus

The security level of ZKP is incredibly high because it permits the confirmation of data without disclosing extra specific data [29]. Thus, ZKP is very suitable to be applied on systems that need to have high privacy protection. The privacy aspect is the most pronounced virtue of ZKP since it establishes proof without revealing any information about the inputs [30].

Metric	Value
Average Processing Time	3 minutes
Energy Consumption	75 kWh
Security Level	Very High
Privacy Level	Very High

Comparison and Analysis

The following table presents the comparative analysis of the four algorithms by using the experimental finding.

Algorithm	Average Processing Time	Energy Consumption	Security Level	Privacy Level	Scalability
PoW	10 minutes	300 kWh	High	Moderate	Low
PoS	2 minutes	50 kWh	High	High	High
PBFT	5 minutes	100 kWh	High	Moderate	Moderate
ZKP	3 minutes	75 kWh	Very High	Very High	Moderate
Algorithm	Average Processing Time	Energy Consumption	Security Level	Privacy Level	Scalability

V. CONCLUSION

In conclusion, this research has outlined how blockchain has revolutionized itself from just being a cryptocurrency to a decentralized augmentation of traditional data solutions. In this paper, looking at the two real-life case studies of applying blockchain in supply chain management and health care, the authors are in a position to attest that blockchain provides immense value proposition, such as transparency, something that cannot be altered, and decentralized, because these provisions are critical in protecting data. The study examined four effective blockchain algorithms which include PoW, PoS, PBFT and ZKP; concerning with the privacy and security analysis of blockchain, those algorithms proposed different advantages and shortcomings. From the experimental data it is shown that the classical cryptographic algorithms as PoW and PoS have high security indicators, but the modern algorithms as ZKP, and the use of blockchain along with other technologies as cloud storage are more suitable for reaching higher level of privacy and efficiency. When comparing these algorithms, it has been identified that the integration of advanced privacy mechanisms with blockchain can indeed replace current limitations, especially concerning the processing of Big Data and their confidentiality. Thus, the established results all for progression and development of blockchain technologies in order to satisfy the more sophisticated demands on the information protection level in different Internet applications. In summary, this study offered significant findings regarding the application of blockchain in enhancing approaches of data management concerning various industries with references to the supply chain management and healthcare fields.

REFERENCE

[1] ABDEL-AZIZ, A. and ELIAS, R.J., 2024. Blockchain Technology Implementation in Supply Chain Management: A Literature Review. *Sustainability,* 16(7), pp. 2823.

[2] AJANI, S.N., KHOBRAGADE, P., JADHAV, P.V., MAHAJAN, R.A., GANGULY, B. and PARATI, N., 2024. Frontiers of Computing - Evolutionary Trends and Cutting-Edge Technologies in Computer Science and Next Generation Application. *Journal of Electrical Systems,* 20(1), pp. 28-45.

[3] ALAJLAN, R., ALHUMAM, N. and FRIKHA, M., 2023. Cybersecurity for Blockchain-Based IoT Systems: A Review. *Applied Sciences,* 13(13), pp. 7432.

[4] ALAMSYAH, A., GEDE NATHA, W.K. and RAMADHANI, D.P., 2024. A Review on Decentralized Finance Ecosystems. *Future Internet,* 16(3), pp. 76.

[5] ALBSHAIER, L., ALMARRI, S. and HAFIZUR RAHMAN, ,M.M., 2024. A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions. *Computers,* 13(1), pp. 27.

[6] ALDOSSRI, R., ALJUGHAIMAN, A. and ALBUALI, A., 2024. Advancing Drone Operations through Lightweight Blockchain and Fog Computing Integration: A Systematic Review. *Drones,* 8(4), pp. 153.

[7] ASTUTI, R. and HIDAYATI, L., 2023. How might blockchain technology be used in the food supply chain? A systematic literature review. *Cogent Business & Management,* 10(2),.

[8] BAIOD, W., LIGHT, J. and MAHANTI, A., 2020. Blockchain Technology and its Applications Across Multiple Domains: A Technology Review. *Journal of International Technology and Information Management,* 29(4), pp. 78-119.

[9] BHUMICHAI, D., SMILIOTOPOULOS, C., BENTON, R., KAMBOURAKIS, G. and DAMOPOULOS, D., 2024. The Convergence of Artificial Intelligence and Blockchain: The State of Play and the Road Ahead. *Information,* 15(5), pp. 268.

[10] BHUVANESHWARRI, I. and ILANGO, V., 2023. An online blockchain based sustainable logistics management system (OBSLMS) enabled by the Internet of Things for the textile industry. *Industria Textila,* 74(6), pp. 660-666.

[11] BILGE, G.C., ABRAHAM, Y.S. and ATTARAN, M., 2024. Unlocking Blockchain in Construction: A Systematic Review of Applications and Barriers. *Buildings,* 14(6), pp. 1600.

[12]Gupta, A., Mazumdar, B.D., Mishra, M., ...Srivastava, S., Deepak, A., Role of cloud computing in management and education, Materials Today: Proceedings, 2023, 80, pp. 3726–3729

[13] Mall, S., Srivastava, A., Mazumdar, B.D., ...Bangare, S.L., Deepak, A., Implementation of machine learning techniques for disease diagnosis, Materials Today: Proceedings, 2022, 51, pp. 2198–2201

[14] Neha Sharma, P. William, Kushagra Kulshreshtha, Gunjan Sharma, Bhadrappa Haralayya, Yogesh Chauhan, Anurag Shrivastava, "Human Resource Management Model with ICT Architecture: Solution of

Management & Understanding of Psychology of Human Resources and Corporate Social Responsibility", *JRTDD*, vol. 6, no. 9s(2), pp. 219–230, Aug. 2023.

[15] William, P., Shrivastava, A., Chauhan, P.S., Raja, M., Ojha, S.B., Kumar, K. (2023). Natural Language Processing Implementation for Sentiment Analysis on Tweets. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_26

[16] K. Maheswari, P. William, Gunjan Sharma, Firas Tayseer Mohammad Ayasrah, Ahmad Y. A. Bani Ahmad, Gowtham Ramkumar, Anurag Shrivastava, "Enterprise Human Resource Management Model by Artificial Intelligence to Get Befitted in Psychology of Consumers Towards Digital Technology", *JRTDD*, vol. 6, no. 10s(2), pp. 209–220, Sep. 2023.

[17] Anurag Shrivastava, S. J. Suji Prasad, Ajay Reddy Yeruva, P. Mani, Pooja Nagpal & Abhay Chaturvedi (2023): IoT Based RFID Attendance Monitoring System of Students using Arduino ESP8266 & Adafruit.io on Defined Area, Cybernetics and Systems

[18] P. William, G. R. Lanke, D. Bordoloi, A. Shrivastava, A. P. Srivastavaa and S. V. Deshmukh, "Assessment of Human Activity Recognition based on Impact of Feature Extraction Prediction Accuracy," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-6, doi: 10.1109/ICIEM59379.2023.10166247.

[19] P. William, G. R. Lanke, V. N. R. Inukollu, P. Singh, A. Shrivastava and R. Kumar, "Framework for Design and Implementation of Chat Support System using Natural Language Processing," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-7, doi: 10.1109/ICIEM59379.2023.10166939.