International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Blockchain Technology for Secure and Trustworthy Decentralized Applications

Elangovan Muniyandy[1], V.S. Radhika[2], Salar Mohammad[3], Sirigiri Joyice[4], Dr. Twinkle Dasari[5], Amit Verma[6], Dr. Ajmeera Kiran[7]

Submitted: 05/02/2024 **Revised**: 13/03/2024 **Accepted**: 19/03/2024

Abstract: This study explores the complex world of blockchain-based decentralized applications (DApps), concentrating on security and trust mechanisms. The study detects and classifies security flaws in DApps, which include flaws in smart contracts, difficulties with consensus, including dangers of data manipulation. By contrasting reputation-based systems with token-based incentives, it investigates trust mechanisms and clarifies their effects on user behaviour. The study emphasizes the crucial part that blockchain integration plays in boosting DApp security by employing its built-in immutability, decentralization, and cryptographic characteristics. The benefits of blockchain are supported by empirical data and vivid case examples. The paper ends with advice for DApp creators that emphasizes secure development methods, thorough audits, as well as user education while also indicating potential directions for future research.

Keywords: *Decentralized Applications (DApps), Blockchain Technology, Security Vulnerabilities, Trust Mechanisms, Smart Contracts, Blockchain Integration*

1. Introduction

1.1. Research background

The decentralized storage, sharing, and security of data have all been redefined by blockchain technology, which is now recognized as a disruptive force. Decentralized apps (DApps), which are becoming common, have the potential to completely transform a variety of sectors, from supply chain management to banking [1]. Nevertheless, despite its potential, problems with security and dependability still exist. This study explores the fundamentals of blockchain technology to see whether it has the ability to offer reliable security and trust mechanisms for DApps. This study looks at the complex interactions between blockchain and DApps in an effort to find ways to make these cutting-edge technologies more trustworthy and secure.

[1]*Department of Biosciences, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India Email: muniyandy.e@gmail.com*
[2]*Assistant professor, Department of Mathematics, School of Advanced Sciences, Kalasalingam Academy of Research and Education, Krishnankovil, Tamilnadu, India*
[3]*Assistant Professor, Department of Data Science, Anurag University, Hyderabad, India Email: salarhtma@gmail.com*
[4]*Research Scholar, Department of English, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India Email: sirigirijoyice01@gmail.com*
[5]*Assistant Professor, Department of English, Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India Email: twinklelingala@gmail.com*
[6]*University Centre for Research and Development, Chandigarh University, Gharuan Mohali, Punjab, India Email: amit.e9679@cumail.in*
[7]*Assistant Professor, Department of Computer Science and Engineering, MLR Institute of Technology, Dundigal, Hyderabad, Telangana, 500043, India Email: kiranphd.jntuh@gmail.com*

1.2. Research Aim and Objectives

Aims: This research's main aim is to look at how decentralized apps (DApps) could be made safer and more trustworthy by using blockchain technology.

Objectives

- To thoroughly assess and evaluate the available research on DApps, and blockchain technology, including the security implications of both.
- To create a mechanism for assessing the security and reliability of blockchain-based DApps.
- To scientifically evaluate, through a series of case studies, how well the blockchain has enhanced DApp security.
- To offer developers and other stakeholder's useful advice and insights that will improve the security as well as dependability of DApps.

1.3. Research Rationale

The expanding relevance of blockchain technology and DApps in transforming economies and sectors provides the foundation for this research. It must be accomplished to solve the security and trust issues that can impede the mainstream adoption of DApps for a variety of vital applications. This research seeks to close the knowledge gaps and provide beneficial insights to developers, organizations, as well as policymakers by comprehending the complex operations of blockchain technology and its incorporation into DApps. In the end, this study aims to support the development of reliable and secure

decentralized apps that can fully exploit blockchain technology.

2. Literature Review

2.1. Understanding Blockchain Technology and Its Foundations

Decentralized apps (DApps) are built on the foundation of blockchain technology, which is essential to their operation. Comprehending the basic concepts of blockchain technology will be essential to understanding the possibilities and constraints of DApps.

Blockchain Basics and Architecture: A distributed and unchangeable ledger that stores transactions across a network of computers constitutes the essence of a blockchain. These transactions are organized into blocks and connected in a chronological chain by those blocks. The preceding block's cryptographic hash has been incorporated into each new block, resulting in a safe and impenetrable structure [2]. As a result of this architecture, updating any data in a block needs to involve modifying all following blocks, which would be computationally impossible.

Principles of Decentralization: Blockchain technology has its foundation on the core idea of decentralization. Traditional centralized systems depend on middlemen for authorization and record transactions, which include banks or governments [3]. Blockchain, in contrast, runs on a decentralized network of nodes, where transactions have been verified via a consensus method. Decentralization increases accountability, lowers the possibility of single points of failure, as well as builds participant trust.

Role of Cryptography in Blockchain: A key component in protecting blockchain networks includes cryptography. Participants have the ability to conduct secure transactions thanks to public and private keys. Cryptographic hashing preserves the integrity of the data within blocks while digital signatures guarantee the reliability of transactions [5]. Together, these cryptographic safeguards protect the blockchain from fraud, unauthorized access, including modification.

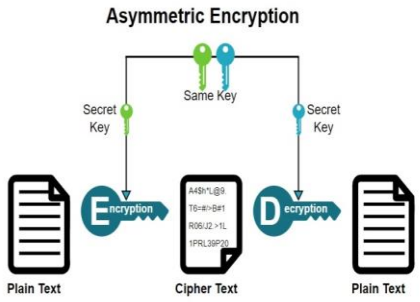

Fig. 1. Cryptography in Blockchain

2.2. Challenges and Security Concerns in Decentralized Applications (DApps)

Software application development and management have gone through a paradigm change thanks to decentralized apps (DApps). They provide new advantages as well as characteristics, but they also present a special set of difficulties in addition to security issues that need to be resolved to assure their viability and dependability.

Defining DApps and Their Characteristics: Software programs known as DApps function on decentralized networks, typically blockchain-based platforms. Open-source software, decentralized data storage, and consensus processes are just a few of its distinctive qualities [6]. DApps are distinguished from conventional centralized apps by these characteristics, which attempt to do away with middlemen, improve transparency, as well as empower users.

Common Challenges in Developing DApps: Developers have unique difficulties while creating DApps. Because blockchain networks could encounter performance problems while handling a huge amount of transactions, scalability is a constant worry [8]. In addition, the expense of carrying out smart contracts could seem exorbitant. DApps require to be improved in terms of user experience alongside accessibility in order to be more extensively used. In addition, maintaining backward compatibility alongside the DApp ecosystem's survival are continuous difficulties.

Security and Trust Issues Associated with DApps: The DApp landscape's primary concerns are security and trust. Sensitive information could be made available because of the immutable and transparent nature of blockchain data. The core component of DApps, smart contracts, is prone to vulnerabilities including reentrancy attacks and code mistakes [4]. Furthermore, DApps are susceptible to any flaws or consensus problems within the underlying blockchain network because the trust mechanisms strongly depend upon it.

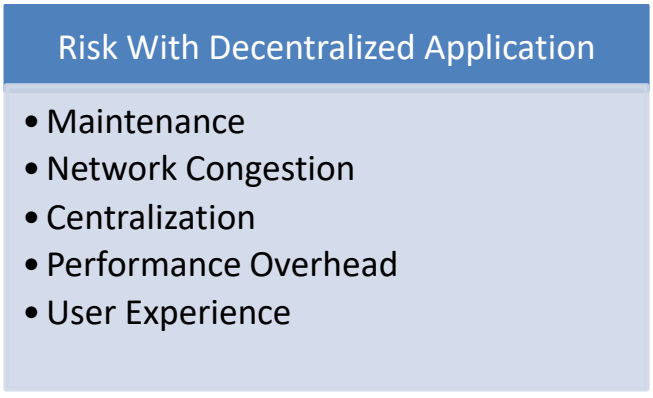

Fig. 2. Security Concerns in Decentralized Applications

2.3. Security Solutions and Frameworks for Blockchain and DApps

Blockchain technology and Decentralized Applications (DApps) have been constructed on security. A variety of security frameworks and solutions have been created to strengthen the reliability of these systems and precisely handle the special problems they represent.

Security Features Embedded in Blockchain: Blockchain platforms come with a number of built-in security mechanisms indicating a rise in their sturdiness. The decentralized and immutable ledger architecture a guarantees that data cannot be modified after it has been recorded. Data integrity is safeguarded by cryptographic hashing, as well as transactions are verified using digital signatures [7]. Together, these attributes provide the blockchain a high level of data security and trust.

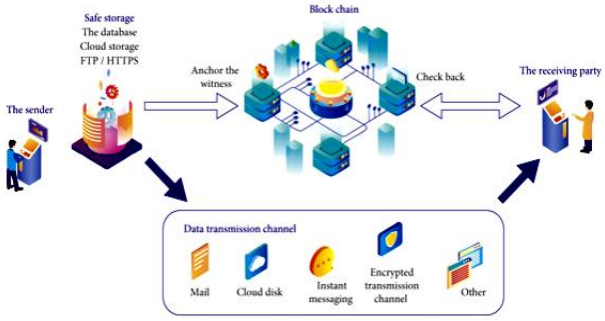

Fig. 3. Security Features Embedded in Blockchain

Vulnerabilities and Threats Mitigation in DApps: DApps, nevertheless, are subject to a unique set of risks and vulnerabilities. DApps are powered by self-executing scripts named smart contracts, which can incorporate code flaws or vulnerabilities that might be exploited by hostile parties. For example, reentrancy attacks have ended up resulting in serious security lapses [10]. Developers and security professionals have suggested a number of solutions to reduce these risks, including formal smart contract verification, rigorous code audits, and bug reward schemes.

Existing Security Frameworks and Best Practices: Numerous security frameworks and best practices have been established in the blockchain and DApp development communities as a result of the urgent requirement for security. These frameworks include procedures for risk assessment as well as mitigation and secure smart contract coding standards, including auditing procedures [12]. The significance of ongoing monitoring and updating to deal with new risks is further emphasized by best practices.

2.4. Trust Mechanisms in Blockchain and Their Adaptation to DApps

Although it is a fundamental component of both conventional and blockchain-based systems, the techniques by which trust is acquired and maintained are very different. It is essential to comprehend these trust mechanisms and the manners in which they apply to Decentralized Applications (DApps) in order to fully utilize blockchain technology.

Trust in Traditional Systems vs. Blockchain: In traditional systems, trust is frequently built between parties via the use of middlemen like banks. Blockchain, on the contrary, promotes trust through decentralization and transparency. The blockchain creates a transparent as well as immutable ledger by publicly recording every transaction and data entry [13]. This intrinsic openness lessens the need for middlemen and encourages participant confidence.

The Role of Smart Contracts in Trust Automation: By carrying out prescribed actions when certain criteria are satisfied, smart contracts, and self-executing code installed on blockchains, automate trust [14]. They do away with the requirement for middlemen and guarantee that written agreements are upheld [9]. By giving parties a tamper-resistant and transparent mechanism to communicate as well as trade assets without depending on a central authority, smart contracts encourage confidence.

Trust Models Tailored for Decentralized Applications: Trust models are changing in the context of DApps to accommodate the distinctive characteristics of blockchain technology. In order to preserve the integrity of transactions including data, these models make utilization of consensus methods, cryptographic techniques, as well as token-based incentives [11]. To build confidence among users who could utilize pseudonyms, they also include reputation systems and identity verification tools.

Fig.4. Trust Mechanisms in Blockchain

2.5. Literature Gap

Although there is a growing corpus of research on blockchain technology as well as Decentralized Applications (DApps), there is a glaring void in the literature when it comes to a thorough current synthesis of security and trust mechanisms specifically suited to the

dynamic environment of Dapps [15]. A lot of study has been done on the fundamentals of blockchain technology and its security, but less has been done on the specific problems, and fixes, including trust structures that apply to DApps. A focused investigation of the evolving security issues and cutting-edge trust mechanisms within the context of DApps is necessary to fill this knowledge gap and provide insightful information to researchers, developers, alongside stakeholders working to improve the security and reliability of these decentralized systems.

3. Methodology

The methodology used to examine the security and trust components of decentralized applications (DApps) based on blockchain technology is going to be discussed in this chapter. An interpretivism philosophy is implemented in an effort to obtain a better understanding of the complex interactions between confidence and safety in Dapps [16]. The study adopts a deductive methodology and starts with well-known ideas and frameworks before applying them to the setting of DApps.

The type of research methodology employed is descriptive. The current trust and security mechanisms in DApps are extensively documented, examined, as well as interpreted using a descriptive study approach. This design provides a thorough overview while allowing for the study of the present status of DApp security and trust. Secondary data are primarily employed in data acquisition. The primary source of data for this study is secondary data collecting [17]. A collection of existing books, articles, and reports, including documents on blockchain technology, DApps, security issues, including trust models is made. This secondary data is compiled from a wide range of sources such as technical documents, whitepapers, academic publications, alongside conference proceedings.

Data processing entails a thorough examination of the gathered secondary data. Researchers use content analysis techniques to locate and classify knowledge on security aspects, flaws, and trust frameworks, including recommended practices in Dapps [35]. The synthesis of current information and the detection of new trends and gaps are made easier by this method.

The researchers, who support the interpretivism concept, acknowledge the value of contextual knowledge and the importance of human interpretation in the study [18]. The analysis's conclusions are interpreted throughout in the context of DApps as well as blockchain, taking into account the particular difficulties and opportunities they provide.

A stringent source selection and data verification process is used to assure the dependability and accuracy of the study. Cross-referencing data from several sources improves to confirm conclusions and reduce bias [19]. Additionally, data analysis and interpretation continue to be performed in an open and organized manner.

In this study, ethics is of utmost importance. It is following ethical standards while using secondary data ensures accurate reference as well as crediting of the original sources. In addition, intellectual property rights are observed, and whenever required, permission is requested.

4. Results

4.1. Security Vulnerabilities in DApps

The trustworthiness and robustness of Decentralized Applications (DApps) are significantly hampered by security flaws. Multiple sorts of vulnerabilities, which includes smart contract vulnerabilities, consensus-related problems, as well as information manipulation vulnerabilities, have been discovered by the research and need to be carefully taken into account while developing and deploying DApps.

The self-executing scripts known as smart contracts, which control DApps, are prone to vulnerabilities including coding mistakes. Reentrancy attacks are one of the most notable instances, where hostile contracts take advantage of unexpected execution sequences to steal money [20]. Lack of input validation is another common problem that can enable attackers to modify contract parameters as well as cause unwanted behaviors.

For transaction validation, DApps frequently depend on certain consensus techniques. These mechanisms' vulnerabilities have the potential to jeopardize the network's integrity as a whole [21]. A concentration of stake among a small number of players, for example, could result in centralization issues including vulnerabilities in Proof of Stake (PoS) systems.

DApps regularly communicate with other data sources, which could possibly lead to security flaws if not managed appropriately. A major risk is Oracle-based attacks, in which rogue data sources give incorrect information to smart contracts [34]. These assaults can result in poor judgment as well as financial losses.

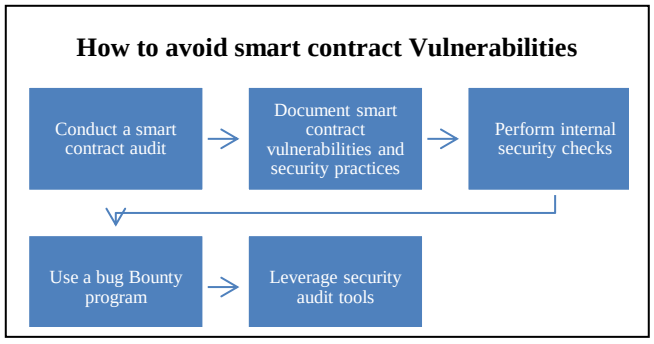

Fig. 5. Security Vulnerabilities

The effects of these vulnerabilities in the actual world are shown via illustrative case studies. For example, the infamous "DAO Hack" stole millions of dollars by using a smart contract vulnerability [22]. These instances highlight how important it is to implement preventative security steps in order to minimize such vulnerabilities while enhancing the overall security posture of DApps.

4.2. Trust Mechanisms and Their Efficacy

Determining how to trust mechanisms inside Decentralized Applications (DApps) affect user behavior as well as the overall trustworthiness of these decentralized systems depends on this evaluation. This investigation compares several trust models, which include reputation-based incentives and token-based systems.

Analyze Trust Mechanisms: DApps have several different trust mechanisms that work to build confidence in an untrustworthy world. User evaluations and comments are crucial for reputation-based systems since they contribute to building trust over time [23]. On the other hand, token-based incentives make use of financial incentives, including staking and rewards, to encourage desired behavior.

Assess the efficiency of trust mechanisms: It involves figuring out how well they can promote trust and reduce risk. In situations where user identities are known, reputation systems can turn out to be successful, but they could be less trustworthy in circumstances where users are using pseudonyms [24]. On the contrary, token-based incentives provide players with real economic incentives to behave in the network's best interests, but the success of these incentives depends on how the tokens are generated and distributed.

Impact on User Behaviour: The trust mechanism you choose has a big impact on how users behave and interact with DApps. Users could potentially be encouraged by reputation-based systems to act in a trustworthy manner in order to uphold their good reputation [25]. Due to users' economic incentives for participating in ways that improve the ecosystem, token-based incentives match user interests with the network's performance.

4.3. Impact of Blockchain Integration on DApp Security

The analysis of how blockchain technology is incorporated into decentralized applications (DApps) demonstrates an important impact on boosting security. The research delivers results that are supported by actual data as well as informative case studies that demonstrate the way the security mechanisms built into blockchains help make DApps trustworthy.

Blockchain Security Enhancement: The decentralization, immutability, as well as cryptographic properties of the blockchain platform naturally increase the security of DApps. Decentralization minimizes the possibility of malevolent control as well as lowers the risk of single points of failure [29]. Immutability guarantees that data cannot be changed after it has been captured, supporting data integrity. Digital signatures and cryptographic hashing offer strong protection against unauthorized access and data modification.

Empirical Data: The study uses empirical data in order to demonstrate the concrete advantages of integrating blockchain technology. Data shows that DApps utilizing blockchain technology significantly reduce security breaches and fraudulent activity [30]. Case studies of well-known DApps show a rise in user assurance as well as a fall in successful assaults.

Examples of Case Studies: Strong evidence of the good benefits of blockchain on DApp security may be found in real-world case studies [26]. The use of blockchain to protect financial transactions, and supply chain management, including identity verification within DApps are notable examples. These examples illustrate how integrating blockchains reduces vulnerabilities as well as improves overall security.

4.4. Best Practices and Recommendations for DApp Security

The thorough examination of the research yields a collection of best practices and suggestions for fortifying Decentralized Application (DApp) security. These technological tips and recommendations have the capacity to further enhance DApp security in an ever-changing environment by reducing vulnerabilities.

Implement stringent smart contract development procedures, which include code audits, formal verification, and exhaustive testing to spot and fix issues [27]. Encourage the usage of security libraries that are industry standards.

Effective Consensus procedures: To reduce the risks and vulnerabilities associated with centralization, carefully choose as well as modify consensus procedures. Systems implementing PoS (Proof of Stake) should take stake distribution and delegation techniques into account.

Oracle security and data validation: Put robust information validation measures in place to prevent outside data modification [28]. Make use of reliable oracles and data sources that have a track record of success.

Fig. 6. DApp Security

Regular Security Audits: To find and fix possible security flaws, conduct routine security audits and penetration tests. Use bug bounty schemes to encourage the public to find vulnerabilities.

Promoting user education on DApp security best practices, which include wallet security, private key management, as well as phishing awareness, is known as "user education and awareness."

5. Evaluation And Conclusion

5.1. Conclusion

The study has looked into the complex interactions between security and trust systems in blockchain-based decentralized applications (DApps). The research investigated security flaws, evaluated the efficacy of trust mechanisms, and emphasized the revolutionary nature of blockchain integration. The study emphasizes the significance it is to follow recommended DApp security best practices, such as safe smart contract creation as well as regular security audits. While user education and regulatory compliance remain crucial, a widely distributed consensus mechanism and reliable oracles are necessary. These insights are essential for the continued growth and security of DApps as they continue to transform many sectors.

5.2. Research recommendation

The findings lead to suggestions for DApp developers, including concentrating on secure smart contract creation, frequent security audits, including constant vigilance against new risks [31]. Data validation must put a strong emphasis on widely distributed consensus processes and reliable oracles. In addition, it's crucial to educate users about DApp security as well as to follow growing regulatory requirements. Interdisciplinary cooperation between blockchain professionals, security experts, alongside regulatory bodies is suggested to improve DApp security.

5.3. Future work

Future research needs to look at improved cryptographic algorithms and novel consensus mechanisms for tackling increasing security vulnerabilities in the developing DApp ecosystem [33]. Another crucial topic for further investigation is the difficulties with DApp scalability and interoperability across various blockchain networks [32]. Research should additionally investigate the effects of evolving rules on the security and compliance of DApps. For developers to develop more user-friendly and safe DApps, user-centric research to comprehend user behaviour and beliefs surrounding DApp security is also essential.

References

[1] Truong, N., Lee, G.M., Sun, K., Guitton, F. and Guo, Y., 2021. A blockchain-based trust system for decentralised applications: When trustless needs trust. Future Generation Computer Systems, 124, pp.68-79.

[2] Sodhro, A.H., Pirbhulal, S., Muzammal, M. and Zongwei, L., 2020. Towards blockchain-enabled security technique for industrial internet of things based decentralized applications. Journal of Grid Computing, 18, pp.615-628.

[3] Yue, K., Zhang, Y., Chen, Y., Li, Y., Zhao, L., Rong, C. and Chen, L., 2021. A survey of decentralizing applications via blockchain: The 5G and beyond perspective. IEEE Communications Surveys & Tutorials, 23(4), pp.2191-2217.

[4] Kh-Madhloom, J., 2022. Dynamic Cryptography Integrated Secured Decentralized Applications with Blockchain Programming. Wasit Journal of Computer and Mathematics Science, 1(2), pp.21-33.

[5] Cai, C., Duan, H. and Wang, C., 2018. Tutorial: building secure and trustworthy blockchain applications. 2018 IEEE Cybersecurity Development (SecDev), pp.120-121.

[6] Taş, R. and Tanrıöver, Ö.Ö., 2019, October. Building a decentralized application on the ethereum blockchain. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-4). IEEE.

[7] Tsolakis, A.C., Moschos, I., Votis, K., Ioannidis, D., Dimitrios, T., Pandey, P., Katsikas, S., Kotsakis, E. and García-Castro, R., 2018, July. A Secured and Trusted Demand Response system based on

Blockchain technologies. In 2018 Innovations in Intelligent Systems and Applications (INISTA) (pp. 1-6). IEEE.

[8] Zhang, J., Zhong, S., Wang, T., Chao, H.C. and Wang, J., 2020. Blockchain-based systems and applications: a survey. Journal of Internet Technology, 21(1), pp.1-14.

[9] Jena, A.K. and Dash, S.P., 2021. Blockchain technology: introduction, applications, challenges. In Blockchain Technology: Applications and Challenges (pp. 1-11). Cham: Springer International Publishing.

[10] B. Rawat, D., Chaudhary, V. and Doku, R., 2020. Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems. Journal of Cybersecurity and Privacy, 1(1), pp.4-18.

[11] Chaer, A., Salah, K., Lima, C., Ray, P.P. and Sheltami, T., 2019, December. Blockchain for 5G: Opportunities and challenges. In 2019 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[12] Badr, B., Horrocks, R. and Wu, X.B., 2018. Blockchain By Example: A developer's guide to creating decentralized applications using Bitcoin, Ethereum, and Hyperledger. Packt Publishing Ltd.

[13] Salah, K., Rehman, M.H.U., Nizamuddin, N. and Al-Fuqaha, A., 2019. Blockchain for AI: Review and open research challenges. IEEE Access, 7, pp.10127-10149.

[14] Al-Madani, A.M., Gaikwad, A.T., Mahale, V. and Ahmed, Z.A., 2020, October. Decentralized E-voting system based on Smart Contract by using Blockchain Technology. In 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC) (pp. 176-180). IEEE.

[15] Baset, S.A., Desrosiers, L., Gaur, N., Novotny, P., O'Dowd, A. and Ramakrishna, V., 2018. Hands-on blockchain with Hyperledger: building decentralized applications with Hyperledger Fabric and composer. Packt Publishing Ltd.

[16] Al-Breiki, H., Rehman, M.H.U., Salah, K. and Svetinovic, D., 2020. Trustworthy blockchain oracles: review, comparison, and open research challenges. IEEE access, 8, pp.85675-85685.

[17] Rosa, R.V. and Rothenberg, C.E., 2018. Blockchain-based decentralized applications for multiple administrative domain networking. IEEE Communications Standards Magazine, 2(3), pp.29-37.

[18] Aswathy, S.U., Tyagi, A.K. and Kumari, S., 2021. The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities, and Challenges. Recent Trends in Blockchain for Information Systems Security and Privacy, pp.261-292.

[19] Gururaj, H.L., Manoj Athreya, A., Kumar, A.A., Holla, A.M., Nagarajath, S.M. and Ravi Kumar, V., 2020. Blockchain: A new era of technology. Cryptocurrencies and blockchain technology applications, pp.1-24.

[20] Madine, M., Salah, K., Jayaraman, R., Al-Hammadi, Y., Arshad, J. and Yaqoob, I., 2021. appxchain: Application-level interoperability for blockchain networks. IEEE Access, 9, pp.87777-87791.

[21] Stephen, R. and Alex, A., 2018, August. A review on blockchain security. In IOP conference series: materials science and engineering (Vol. 396, No. 1, p. 012030). IOP Publishing.

[22] Antal, C., Cioara, T., Anghel, I., Antal, M. and Salomie, I., 2021. Distributed ledger technology review and decentralized applications development guidelines. Future Internet, 13(3), p.62.

[23] Siyal, A.A., Junejo, A.Z., Zawish, M., Ahmed, K., Khalil, A. and Soursou, G., 2019. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), p.3.

[24] Chang, Y.W., Lin, K.P. and Shen, C.Y., 2019, March. Blockchain technology for e-marketplace. In 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 429-430). IEEE.

[25] Palanivel, K., 2019. Blockchain architecture to higher education systems. Int. J. Latest Technol. Eng. Manag. Appl. Sci, 8, pp.124-138.

[26] Li, P., Nelson, S.D., Malin, B.A. and Chen, Y., 2019. DMMS: A decentralized blockchain ledger for the management of medication histories. Blockchain in healthcare today, 2.

[27] Gamage, H.T.M., Weerasinghe, H.D. and Dias, N.G.J., 2020. A survey on blockchain technology concepts, applications, and issues. SN Computer Science, 1, pp.1-15.

[28] Lim, S.Y., Fotsing, P.T., Almasri, A., Musa, O., Kiah, M.L.M., Ang, T.F. and Ismail, R., 2018. Blockchain technology the identity management and authentication service disruptor: a survey. International Journal on Advanced Science, Engineering and Information Technology, 8(4-2), pp.1735-1745.

[29] Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang,

H., 2018. Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), pp.352-375.

[30] Fauziah, Z., Latifah, H., Omar, X., Khoirunisa, A. and Millah, S., 2020. Application of blockchain technology in smart contracts: A systematic literature review. Aptisi Transactions on Technopreneurship (ATT), 2(2), pp.160-166.

[31] Raja Santhi, A. and Muthuswamy, P., 2022. Influence of blockchain technology in manufacturing supply chain and logistics. Logistics, 6(1), p.15.

[32] Rosa, R.V. and Rothenberg, C.E., 2018, August. Blockchain-based decentralized applications meet multi-administrative domain networking. In Proceedings of the ACM SIGCOMM 2018 Conference on Posters and Demos (pp. 114-116).

[33] Khan, S.N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E. and Bani-Hani, A., 2021. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications, 14, pp.2901-2925.

[34] Ma, L., Kaneko, K., Sharma, S. and Sakurai, K., 2019, November. Reliable decentralized oracle with mechanisms for verification and disputation. In 2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW) (pp. 346-352). IEEE.

[35] Hardjono, T. and Smith, N., 2019. Decentralized trusted computing base for blockchain infrastructure security. Frontiers in Blockchain, 2, p.24.

[36] Kalita, K., Ramesh, J. V. N., Cepova, L., Pandya, S. B., Jangir, P., & Abualigah, L. (2024). Multi-objective exponential distribution optimizer (MOEDO): a novel math-inspired multi-objective algorithm for global optimization and real-world engineering design problems. Scientific reports, 14(1), 1816.

[37] S. P. Praveen, P. Chaitanya, A. Mohan, V. Shariff, J. V. N. Ramesh and J. Sunkavalli, "Big Mart Sales using Hybrid Learning Framework with Data Analysis," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 471-477, doi: 10.1109/ICACRS58579.2023.10404941.

[38] P. Dedeepya, P. Chiranjeevi, V. Narasimha, V. Shariff, J. Ranjith and J. V. N. Ramesh, "Image Recognition and Similarity Retrieval with Convolutional Neural Networks," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 709-716, doi: 10.1109/ICACRS58579.2023.10404664.

[39] D. Gupta et al., "Optimizing Cluster Head Selection for E-Commerce-Enabled Wireless Sensor Networks," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2024.3360513.

[40] Singh, A., Rani, P., Ramesh, J. V. N., Athawale, S. V., Alkhayyat, A. H., Aledaily, A. N., ... & Sharma, R. (2024). Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication. IEEE Transactions on Consumer Electronics.

[41] Gupta A., et. al, (2020). An Analysis of Digital Image Compression Technique in Image Processing. International Journal of Advanced Science and Technology, 28(20), 1261 - 1265. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/3837

[42] Kaushik, K., Garg, M., Annu, Gupta, A. and Pramanik, S. (2021). Application of Machine Learning and Deep Learning in Cyber security: An Innovative Approach, in Cybersecurity and Digital Forensics: Challenges and Future Trends, M. Ghonge, S. Pramanik, R. Mangrulkar and D. N. Le, Eds, Wiley, 2021.

[43] Pandey, B.K. et al. (2022). Effective and Secure Transmission of Health Information Using Advanced Morphological Component Analysis and Image Hiding. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore.https://doi.org/10.1007/978-981-19-0151-5_19

[44] Pathania, V. et al. (2022). A Database Application of Monitoring COVID-19 in India. In: Gupta, M., Ghatak, S., Gupta, A., Mukherjee, A.L. (eds) Artificial Intelligence on Medical Data. Lecture Notes in Computational Vision and Biomechanics, vol 37. Springer, Singapore. https://doi.org/10.1007/978-981-19-0151-5_23

[45] Veeraiah, V., Khan, H., Kumar A., Ahamad S., Mahajan A. and Gupta A., (2022). Integration of PSO and Deep Learning for Trend Analysis of Meta-Verse. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 713-718.doi: 10.1109/ICACITE53722.2022.9823883.

[46] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Review on Comparative study of 4G, 5G and 6G Networks," 2022 5th International Conference on Contemporary

Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1830-1833, doi: 10.1109/IC3I56241.2022.10073385.

[47] V. Jain, S. M. Beram, V. Talukdar, T. Patil, D. Dhabliya and A. Gupta, "Accuracy Enhancement in Machine Learning During Blockchain Based Transaction Classification," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 536-540, doi: 10.1109/PDGC56933.2022.10053213.

[48] V. Talukdar, D. Dhabliya, B. Kumar, S. B. Talukdar, S. Ahamad and A. Gupta, "Suspicious Activity Detection and Classification in IoT Environment Using Machine Learning Approach," 2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, Himachal Pradesh, India, 2022, pp. 531-535, doi: 10.1109/PDGC56933.2022.10053312.

[49] P. R. Kshirsagar, D. H. Reddy, M. Dhingra, D. Dhabliya and A. Gupta, "A Scalable Platform to Collect, Store, Visualize and Analyze Big Data in Real- Time," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118183.

[50] V. V. Chellam, S. Praveenkumar, S. B. Talukdar, V. Talukdar, S. K. Jain and A. Gupta, "Development of a Blockchain-based Platform to Simplify the Sharing of Patient Data," 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM), Uttar Pradesh, India, 2023, pp. 1-6, doi: 10.1109/ICIPTM57143.2023.10118194.