IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Comprehensive Review of Blockchain Technology

R.Saraswathi[1], Dr. S. Britto Ramesh Kumar[2]

Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous),

Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India[1]

Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous),

Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India[2]

Abstract

Blockchain technology has gained significant attention in recent years for its ability to enhance the security, reliability, and robustness of distributed systems. Research based on this technology has contributed to advancements in various domains such as finance, remote sensing, data analysis, and healthcare. This paper provides a comprehensive discussion on the role and fundamental concepts of blockchain technology, along with its different types and layer classifications. This research also reviews previous research studies, explores existing issues and challenges, examines key applications, identifies research gaps, and outlines promising future research directions in the field of blockchain technology. The decentralized and immutable nature of blockchain ensures transparent data exchange among untrusted parties without the need for intermediaries. Its growing adoption demonstrates the potential to revolutionize traditional systems by improving efficiency, accountability, and trust. As blockchain continues to evolve, understanding its architecture, limitations, and opportunities becomes crucial for researchers and practitioners aiming to build secure and scalable solutions for the future.

Keywords: *Blockchain Technology, hash, cryptography, Decentralization, Distributed*

1. Introduction

Blockchain technology serves as a ground breaking digital framework that allows for secure, transparent, and tamper-resistant data transferring across distributed networks. Fundamentally, blockchain acts as a decentralized ledger that chronicles transactions or data entries in a sequence of blocks, each connected to its predecessor through cryptographic hashes. This sequence of blocks is sustained by a network of nodes, which removes the necessity for a central authority and decreases the likelihood of data manipulation or fraud. Grasping the basic principles of blockchain is critical for its effective application in secure data management, mainly in vital sectors such as healthcare. The three fundamental principles—decentralization, immutability, and consensus shape the dependability, transparency, and security of blockchain systems[1].

In conventional systems, data storage and management are controlled by a central authority (such as a hospital database). In contrast, blockchain operates on a decentralized network, where numerous nodes (computers) contribute to the maintenance and validation of data. This eliminates a single point of failure, lowers the risk of attacks on central systems, and provides all participants with equal access to records. Within the healthcare sector, decentralization permits patients, providers, and insurers to securely share and access medical records without depending on a central authority.

2. Role of blockchain

Blockchain technology significantly changes the way secure and transparent data management is achieved, especially in sensitive areas such as medical [24]. Essentially, blockchain serves as a decentralized and unchangeable digital ledger that tracks transactions across a network of distributed nodes. This framework eliminates the necessity for a centralized authorization, thereby decreasing the likelihood of data manipulation and unauthorized access. In the healthcare sector, where maintaining the privacy, integrity, and accessibility of patient data is paramount, blockchain provides robust assurances by employing cryptographic methods to guarantee that once information is recorded, it cannot be modified or erased without being detected.

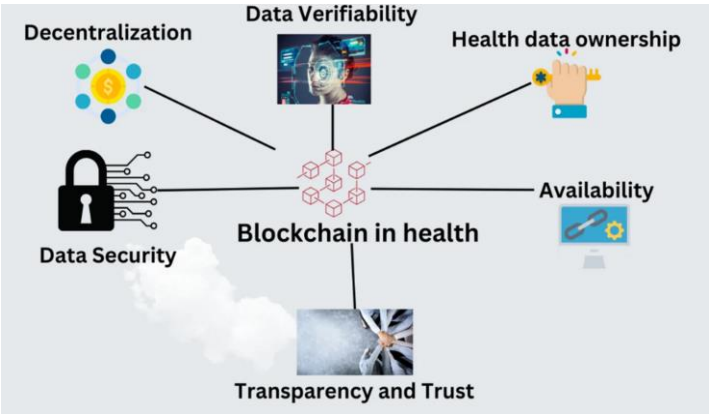

Figure 1. Role of blockchain

The main primary advantages of blockchain is its transparency in data management while allowing controlled access. Each transaction or data entry on the blockchain is time-stamped and connected to prior records, rendering the complete history of a medical record traceable and verifiable. At the same time, privacy is maintained through encryption and access control systems, such as smart contracts and permissioned blockchain, which limit data visibility to authorized users only[2]. This guarantees that patients, healthcare providers, and regulatory bodies can rely on the accuracy and origin of medical information without sacrificing confidentiality. Moreover, blockchain enables different healthcare systems to work together by serving as a central data layer for secure information exchange among various parties. For instance, a patient's medical records can be safely transmitted between hospitals, labs, and insurance companies without any duplication or inconsistency. By fostering accountability, improving security, and allowing for smooth data sharing. Figure 1 shows the role of Blockchain in secure for data security, transparency and trust, availability, health data ownership, decentralization and data verifiability.

3. Fundamental concepts of Blockchain Technology

3.1 Permanence

Once data is recorded on a blockchain, it becomes unchangeable and cannot be removed. Each block of information is cryptographically linked to the block before it, creating a secure and tamper-resistant chain. This guarantees a lasting audit trail, which is essential for monitoring medical transactions, prescriptions, and patient consent documentation. The feature of immutability boosts trust and accountability throughout the healthcare system[3].

3.2. Agreement

Consensus mechanisms function as protocols to reach a common agreement on the validity of data or transactions prior to their incorporation into the blockchain. Frequently used consensus algorithms include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). In the healthcare domain, consensus helps ensure that only confirmed and authorized information is recorded, thwarting fraud, duplication, or unauthorized access. It also facilitates secure collaboration among hospitals, laboratories, and pharmacies.

Main contributions of this paper includes role of blockchain technology, Fundamental of Blockchain technology, various types of blockchain technology, Blockchain layers, earlier works on blockchain, applications of blockchain, secure and privacy issues data management, challenges of Blockchain and future research directions[4].

4. Various types of blockchains (public, private, consortium)

Blockchain technology is not universally applicable to every situation. Based on how access and control are managed, blockchains can be categorized into three main types: **public**, **private**, and **consortium** (also known as federated) blockchains.

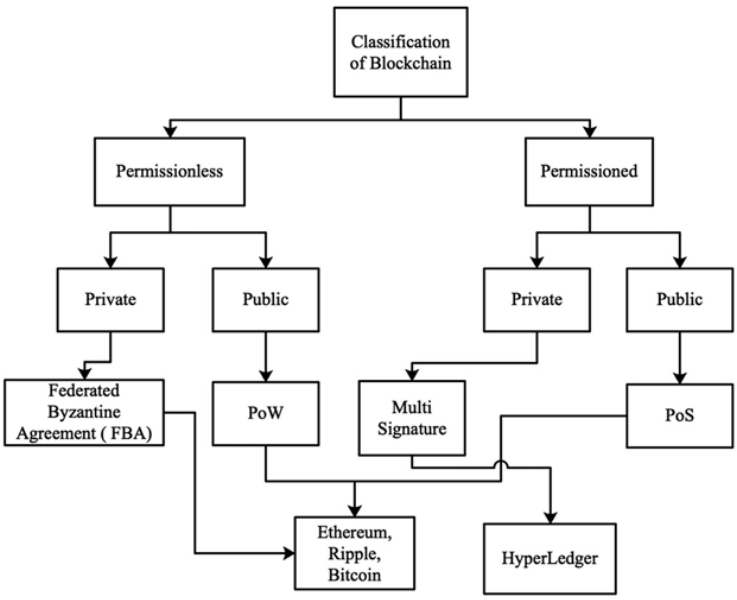

Figure 2. Classification of Blockchain

4.1. Public Blockchain

A public blockchain allows anyone to join, view, contribute, or take part in the agreement process. Examples include Bitcoin, Ethereum, and various other cryptocurrencies[5]. These networks are entirely decentralized and function without a central governing body. Security is upheld through consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS).

In the healthcare sector, public blockchains can facilitate open access to verified health certifications (like vaccine passports), though they should not be used for storing sensitive patient information due to privacy issues.

4.2. Private Blockchain

A private blockchain is limited to certain users or organizations. Only permitted participants can access, validate, or contribute to the blockchain. It is usually operated by a single organization, providing quicker transaction speeds and increased control. Private blockchains are ideal for internal business operations that demand confidentiality and efficiency. Hospitals or research organizations can utilize private blockchains to securely manage patient records, clinical trials, and administrative processes.

4.3. Consortium Blockchain

A consortium blockchain is overseen by a collective of organizations rather than a single organization. It merges the advantages of both public and private blockchains, allowing for partial decentralization with restricted access.

Only pre-approved nodes can engage in consensus, fostering trust among familiar participants.

A group of hospitals, insurance providers, and regulators can implement this type of blockchain for secure, interoperable sharing of patient data, while upholding privacy and compliance.ess, validate, or contribute to the blockchain[6].

Figure 2. shows the different types of blockchain each type serves different purposes and offers distinct advantages and trade-offs.

5. Classification of Blockchain Layers

The convergence of blockchain technology creates a robust framework that combines ultra-fast, low-latency data transmission with decentralized. This architecture ensures real-time e maintaining security, privacy, and interoperability across stakeholders. The system consists of several key components working in synergy. These devices, however, have limited computational power, necessitating efficient data offloading strategies. To minimize latency and reduce bandwidth strain, edge nodes process raw sensor data locally—performing anomaly detection, data filtering, and compression before transmission. This preprocessing ensures only relevant, high-priority data is forwarded, optimizing network efficiency. Ensuring seamless communication between IoT devices, edge servers, and cloud/blockchain layers.

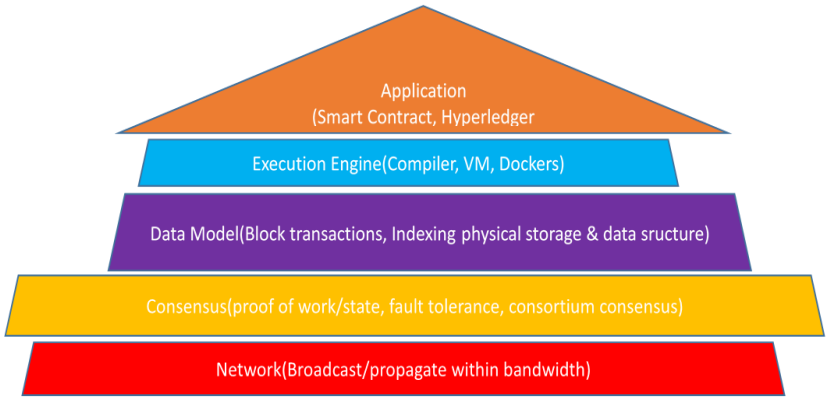

Figure 3. Classification Blockchain Layers

Blockchain layer processed medical data is hashed and stored on the blockchain**,** ensuring immutability and auditability. Smart contracts automate access control, consent management, and data-sharing agreements, while Decentralized Identifiers (DIDs) and zero-knowledge proofs (ZKPs) enhance patient privacy. Hybrid blockchain models (public for audit logs, private for sensitive records) can balance transparency and confidentiality [7].

6. Earlier works on blockchain technology

Table 1, provides a summary of the focused area, techniques and contribution research papers analyzed and reviewed.

Table 1. Comparative study of existing solutions

Author(s)	Year	Focus Area	Technique	Contribution
Guo et al.[1]	2025	Hybrid Blockchain	Linkable Ring Signature for Privacy Protection	To live processing Real-time data processing.
Teng et al.[2]	2025	Private and Enhanced Blockchain	Ring signature, Smart Contracts	To secure the Blockchain stored data.
Wijethilaka et al.[7]	2024	Consensus mechanism	Smart Contracts	To secure and protect the records.
Sun et al.[12]	2024	Hyperledger Fabric blockchain	Zero Trust Proof, Smart Contracts	To protect the records.
Prabha et al.[13]	2024	Data Security	Smart Contracts	It maintains the Immutable health records. Scalability issues; lacks real-time implementation results

Goa et al.[14]	2023	Public and private blockchain, consensus algorithms (PoW, PoS, PBFT)	Securing health records, enhancing data sharing	Detailed architectural framework; comparative analysis of attack-defense models; layered security
Priya et al.[15]	2022	Private blockchain	Homomorphic Encryption	More secure analytics of the data.

7. Issues and challenges of Blockchain Technology

7.1. Scalability and Latency in Blockchain Systems

Public blockchains like Ethereum or Bitcoin suffer from limited throughput and high transaction latency. This poses a critical limitation when handling real-time health data from IoT devices in 5G environments. Table 1 shows the existing solutions of the detailed explanations[8].

7.2. Interoperability among healthcare platforms

Healthcare data is fragmented across EHRs, hospitals, labs, and wearable devices, often using incompatible data formats and protocols**.** Lack of unified data exchange frameworks across blockchain and traditional systems.

Limited adoption of standards like FHIR (Fast Healthcare Interoperability Resources) and HL7 in blockchain-based implementations.

8. Applications of Blockchain Technology

A group of hospitals, insurance providers, and regulators can implement this type of blockchain for secure, interoperable sharing of patient data, while upholding privacy and compliance.ess, validate, or contribute to the blockchain. It is usually operated by a single organization, providing quicker transaction speeds and increased control. Private blockchains are ideal for internal business operations that demand confidentiality and efficiency.

8.1. Smart contracts and their healthcare relevance

Smart contracts are automated digital agreements coded to automatically implement the specified terms and conditions when certain criteria are fulfilled. These contracts operate on blockchain networks, providing transparency, immutability, and trust without requiring intermediaries. In the healthcare industry, smart contracts are crucial for optimizing processes, improving data security, and lowering administrative costs. A significant application is in the automation of patient consent management. For example, when a patient allows their medical information to be shared with a particular provider or research organization, a smart contract can automatically enforce access permissions and log the transaction on the blockchain for complete auditability. Smart contracts also enable automated processing of insurance claims. Instead of depending on manual assessment and approvals, claims can be processed and finalized automatically when specific conditions (such as completion of treatment, or a doctor's report) are confirmed through the blockchain. This enhances efficiency, mitigates fraud, and boosts patient satisfaction. In clinical research and drug supply lines, smart contracts help ensure compliance by automatically monitoring consent forms, watching study progress, and overseeing the handling of sensitive materials. They also help confirm the

authenticity and trackability of medicines, which lowers the chances of encountering counterfeit medications. In conclusion, smart contracts introduce automation, security, and reliability to healthcare operations. They decrease the likelihood of human error, guarantee adherence to regulations, and promote secure collaboration among patients, healthcare providers, insurers, and researchers, ultimately enhancing the quality and efficiency of healthcare delivery.

8.2. Compliance Requirements (HIPAA, GDPR)

Patient health records, diagnostic data, treatment history, and insurance information are just a few examples of the highly sensitive and private information handled by the healthcare industry. In addition to being a technological problem, protecting the privacy and security of this data is also required by law and ethics. The delicate nature of health information one of the most private categories of personal data is healthcare data. Serious repercussions, such as identity theft, insurance fraud, harm to one's reputation, and psychological suffering for patients, may result from a breach or abuse of such data. Furthermore, prejudice and societal stigma may result from the unapproved release of information about genetic disorders, mental health issues, or chronic illnesses. Maintaining rigorous confidentiality and integrity of patient information is therefore crucial at every level, including collection, storage, transfer, and dissemination.

8.3. Threats: Data Breaches, Tampering, Unauthorized Access

The huge value of medical records on the illicit market makes healthcare organizations an attractive target for hackers. Typical dangers include: Malware or phishing assaults that compromise data. Tampering with medical records, which can endanger patient lives by leading to incorrect diagnoses or treatments. Unauthorized access by internal staff or external attackers, especially in poorly secured or outdated systems. In order to safeguard the confidentiality, integrity, and availability of medical information, healthcare systems must adopt robust security and privacy measures, including strong encryption, access control, continuous monitoring, and secure data sharing frameworks. Technologies like blockchain and 5G, when properly implemented, can enhance these protections by providing decentralized, traceable, and secure data management environments[7].

8.4. Decision Making:

Sentiment analysis and Blockchain technology can work together to guarantee opinion mining [5,33]. Procedures are transparent, legitimate and trust worthy[8]. Data gathered online platforms or social media may be distorted or tampered within traditional sentiment analysis [21,24-26]. The dependability of sentiment analysis. The dependability of sentiment data is increased by storing validating user-generated material on a blockchain, which makes each record unchangeable and traceable[13,18]. Decentralised blockchain networks may also safely share sentiment datasets for machine learning models [25].

9. Research gaps in blockchain

9.1. Scalability and Latency in Blockchain Systems

Public blockchains like Ethereum or Bitcoin suffer from limited throughput and high transaction latency**.** Current consensus mechanisms (e.g., PoW, PoS) are not optimized for high-speed, low-latency environments like healthcare. There is a need for lightweight, energy-efficient, and scalable consensus protocols (e.g., PBFT variants, DAG-based systems) tailored to healthcare needs. Explore hybrid blockchain architectures

combining public and private chains. Integrate layer-2 solutions (e.g., rollups, state channels) to support high-frequency data without clogging the mainchain[13-15].

9.2. Interoperability among healthcare platforms

Healthcare data is fragmented across EHRs, hospitals, labs, and wearable devices, often using incompatible data formats and protocols. Lack of unified data exchange frameworks across blockchain and traditional systems. Limited adoption of standards like FHIR (Fast Healthcare Interoperability Resources) and HL7 in blockchain-based implementations. Develop blockchain-diagnostic middleware to connect heterogeneous systems. Design cross-chain communication protocols for healthcare blockchains to interact securely and seamlessly[16].

9.3. Regulatory and Ethical Considerations

Managing sensitive medical information on a decentralized ledger raises issues related to adherence to privacy laws such as HIPAA, GDPR, and DPA.

The unchangeable nature of blockchain may contradict the "Right to be Forgotten" provision outlined in GDPR. There are few existing frameworks that harmonize blockchains permanent storage with the requirements for data withdrawal, modification, or deletion. Explore off-chain storage solutions paired with on-chain hash references to facilitate controlled access and alterations to data. Investigate frameworks for privacy-preserving computation and data sovereignty that comply with ethical norms[17-20].

10. Conclusion

By offering a safe, open, and decentralized method of handling private data, blockchain technology data exchange, interoperability, and stakeholder confidence by leveraging the quick impenetrable characteristics of blockchain. Crucially, security and privacy protections are significantly enhanced by this integrated strategy. However, further research and interdisciplinary cooperation will be necessary to realize this objective. Researchers, engineers, healthcare professionals, and legislators must work together to address issues including scalability, interoperability, and regulatory compliance. It provides a strong basis for the future of all the sectors, to sum up and ongoing research will be necessary for its efficacy.

11. Future Research Directions

A number of exciting research avenues are opening up as blockchain technologies develop in order to address current issues and optimize the potential of safe, intelligent, and patient-centered healthcare systems. Blockchain consensus techniques like Proof of Work (PoW), which need significant processing power. Future studies should focus on developing consensus procedures that are lightweight and energy-efficient, such Delegated Proof of Stake (DPoS) and Proof of Authority (PoA). Variations of Practical Byzantine Fault Tolerance (PBFT)—that can function effectively on edge and fog nodes. However, achieving this necessitates thorough policy frameworks and governance models that outline data ownership, rights of access, management of consent, and legal responsibilities.

References

[1] Guo, F., Gao, Y., Jiang, J., Chen, X., Chen, X., & Jiang, Z. (2025). Linkable Ring Signature for Privacy Protection in Blockchain-Enabled IIoT. Sensors, 25(12), 3684.

[2] Teng, D., Yao, Y., & Huang, C. (2025). Optimizing signature space performance in privacy-enhanced blockchains: novel ring signature solutions. EURASIP Journal on Information Security, 2025(1), 6.

[3] Xue, L., Huang, H., Xiao, F., Li, Q., & Wang, Z. (2025). A Privacy-Enhanced Traceable Anonymous Transaction Scheme for Blockchain. IEEE Transactions on Information Forensics and Security.

[4] Aleisa, M. A. (2025). Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments. IEEE Access.

[5] Angelpreethi, A., & Britto Ramesh Kumar, S. (2018). Opinion mining using hybrid approach on big data: A perspective. *International Journal of Scientific Research in Computer Science and Management Studies*, 7(5). https://doi.org/10.5281/zenodo.17399553

[6] Shahzad, A., Chen, W., Zhang, Y., & Kumar, R. (2025). Zero-Trust Medical Image Sharing: A Secure and Decentralized Approach Using Blockchain and the IPFS. Symmetry (20738994), 17(4).

[7] Wijethilaka, S., Yadav, A. K., Braeken, A., & Liyanage, M. (2024). Blockchain-based secure authentication and authorization framework for robust 5g network slicing. IEEE transactions on network and service management, 21(4), 3988-4005.

[8] Angelpreethi, A. (2023). Fuzzy based sentiment classification using fuzzy linguistic hedges for decision making. *Mapana Journal of Sciences, 22*(Special Issue 2), 63–79. [Online]. Available: https://doi.org/10.12723/mjs.sp2.4

[9] Villarreal, E. R. D., García-Alonso, J., Moguel, E., & Alegría, J. A. H. (2023). Blockchain for healthcare management systems: A survey on interoperability and security. IEEE Access, 11, 5629-5652.

[10] Othman, S. B., & Getahun, M. (2025). Leveraging blockchain and IoMT for secure and interoperable electronic health records. Scientific Reports, 15(1), 12358.

[11] Prabha, P., & Chatterjee, K. (2024). RSHealth: A Ring Signature Scheme for Identity Anonymization and Transaction Privacy in Blockchain Based E-Healthcare Systems. IEEE Access.

[12] Sun, L., Liu, D., Li, Y., & Zhou, D. (2024). A blockchain-based E-healthcare system with provenance awareness. IEEE Access.

[13] Angelpreethi, A., & Britto Ramesh Kumar S (2016). Visualizing big data mining: Issues, challenges and opportunities. *International Journal of Control Theory and Applications, 9*(27), 455–460. [Online]. Available: https://serialsjournals.com/abstract/86429_61-182.pdf

[14] Gao, W., Yao, H., Qin, B., Dong, X., Zhao, Z., & Zeng, J. (2024). Post-Quantum Secure ID-Based (Threshold) Linkable Dual-Ring Signature and Its Application in Blockchain Transactions. Cryptography, 8(4), 48.

[15] Priya, J. C., Praveen, R., Nivitha, K., & Sudhakar, T. (2024). Improved blockchain-based user authentication protocol with ring signature for internet of medical things. Peer-to-Peer Networking and Applications, 17(4), 2415-2434.

[16] Velmurugan, S., Prakash, M., Neelakandan, S., & Martinson, E. O. (2024). An efficient secure sharing of electronic health records using IoT-based hyperledger blockchain. International Journal of Intelligent Systems, 2024.

[17] Andrew, J., Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, 215, 103633.

[18] Angelpreethi, A., & Britto Ramesh Kumar, S. (2019). Dom_Classi: An enhanced weighting mechanism for domain specific words using frequency-based probability. *International Journal of Applied Engineering Research, 14*(1), 140– 148, [Online]. Available: ijaerv14n1_21.pdf

[19] Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics, 12(3), 546.

[20] Devidas, S., Rekha, N. R., & Subba Rao, Y. V. (2023). Identity verifiable ring signature scheme for privacy protection in blockchain. International Journal of Information Technology, 15(5), 2559-2568.
[21] Angelpreethi A. Lexicon and Machine Learning Based Comparative Analysis to Classify the Students Opinions on Covid-19 Pandemic. IJIEMR Transactions. 2023;12(2):380–387. Available from: https://ijiemr.org/public/uploads/paper/590451676720775.pdf. 10.48047/IJIEMR/V12/ISSUE02/60.
[22]Frauenthaler, P., Sigwart, M., Spanring, C., Sober, M., & Schulte, S. (2020). ETH relay: A cost-efficient relay for ethereum-based blockchains. In *IEEE International Conference on Blockchain (Blockchain) 2020*, 204–213. https://doi.org/10.1109/Blockchain50366.2020.00032
[23]Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops*, 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634
[24] Angelpreethi, A., & Ramesh Kumar, S. B. (2019). NIC_LBA: Negations and intensifier classification of microblog data using lexicon based approach. *Journal of Emerging Technologies and Innovative Research, 6*(6),753– 759.[Online].Available: https://www.jetir.org/papers/JETIR1906R05.pdf
[25] Parimala, S., Kumutha, R., Iram, F., Sunena Rose, M. V., N. R., & Angelpreethi, A. (2024, July). Improved moth flame optimization with deep convolutional neural network for colorectal cancer classification using biomedical images. In *Proceedings of* 2024 Second International Conference on Advances in Information Technology (ICAIT), IEEE. .[Online].Available: 10.1109/ICAIT61638.2024.10690631
[26] Angelpreethi, A., & Ramesh Kumar, S. B. (2018). A dictionary-based approach to enhance the accuracy of opinion mining on big data. *International Journal of Research and Analytical Reviews, 5*(4), 1836–1844.
[27] Yang, S., Chen, Z., Cui, L., Xu, M., Ming, Z., & Xu, K. (2019a). CoDAG: An efficient and compacted DAGBased blockchain protocol. In *IEEE International Conference on Blockchain (Blockchain)*, 314–318. https://doi.org/10.1109/Blockchain.2019.00049
[Online]. Available:https://ijrar.com/upload_issue/ijrar_issue_20542657.pdf
[28] Xu, C., Qu, Y., Eklund, P. W., Xiang, Y., & Gao, L. (2021). Bafl: An efficient blockchain-based asynchronous federated learning framework. In *IEEE Symposium on Computers and Communications*, 1–6. https://doi.org/10.1109/ISCC53001.2021.9631405
[29] Garay, J. A., Kiayias, A., & Leonardos, N. (2015). The bitcoin backbone protocol: Analysis and applications. In *Annual International Conference on The Theory And Applications of Cryptographic Techniques*, 281- 310. https://doi.org/10.1007/978-3-662-46803-6_10
[30] Bae, J., & Lim, H. (2018). Random mining group selection to prevent 51% attacks on Bitcoin. In 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, 81–82. https://doi.org/10.1109/DSN-W.2018.00040
[31]Malik, S., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). TrustChain: Trust management in blockchain and IoT supported supply chains. In *IEEE International Conference on Blockchain (Blockchain),* 184–193.
[32]Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195. https://doi.org/10.1109/JIOT.2018.281223
[33] Angelpreethi, A. (2025). OPINE_NEG: An approach to detecting negations and intensifiers using social media data. *International Multidisciplinary Research Journal Reviews, 2*(8), 13–17. .[Online].Available: IMRJR.2025.020803.pdf
[34] Wang, K., & Kim, H. S. (2019). FastChain: Scaling blockchain system with informed neighbor selection. In *IEEE International Conference on Blockchain (Blockchain)*, 376–383. https://doi.org/10.1109/Blockchain.2019.00058
[35]Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2019). Analysis of blockchain technology: Pros, cons and SWOT. *Cluster Computing, 22*(6), 14743–14757. https://doi.org/10.1007/s10586-018-2387-5
[36]Manolache, M. A., Manolache, S., & Tapus, N. (2022). Decision making using the blockchain proof of authority consensus. *Procedia Computer Science, 199*, 580-588. https://doi.org/10.1016/j.procs.2022.01.071