IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cipher Circle – A Decentralized Chat Application

[1]Vighnesh Sadvilkar, [2]Shraddha Chakraborty, [3]Vaishnavi Shitre, [4]Kanksha Tanksale, [5]Preeti Patil
[1,2,3,4]Student, [5]Professor
[1]Computer Engineering,
[1]Terna Engineering College, Nerul (W), India

Abstract: The growing imperative for secure and private communication within digital ecosystems has driven the emergence of decentralized architectures that safeguard sensitive information. This study outlines the architecture and deployment of a blockchain-based decentralized communication platform engineered for confidential messaging. By employing distributed ledger technology, the framework ensures data integrity and transaction transparency while maintaining participant anonymity through cryptographic methods. Advanced encryption methods are employed to protect the content of messages during transmission.

The system addresses the stringent security demands of corporate entities, legal institutions, and organizations managing privileged messages through automated protocol enforcement. Smart contracts operationalize governance parameters, ensuring adherence to regulatory frameworks and procedural standards. This research advances contemporary discourse on secure digital interaction models while establishing foundational principles for subsequent developments in decentralized information ecosystems.

Index Terms **- Blockchain, Decentralised Chat Application, Ethereum, Solidity, Web3.**

Introduction

In the modern digital era, developing a secure and confidential channel of communication is of top priority since the need for data security and privacy has become more prominent. Conventional centralized messaging applications expose user data to hacking, unauthorized access, and potential third-party intervention. Moreover, with rising significance associated with blockchain technology, decentralized applications (DApps) are rapidly becoming vital solutions to address these pressing security and privacy concerns.

This project presents a revolutionary Web3 Chat Application (DApp), a decentralized chat application built using Next.js, Hardhat, MetaMask, Solidity, and Ethereum blockchain technology. The application enables real-time, end-to-end encrypted communication among users on the Ethereum blockchain, thus ensuring unparalleled security and confidentiality. With the use of Solidity smart contracts for secure message handling and encryption, the platform enables seamless integration with MetaMask wallets for authentication and transaction signing. Next.js also provides a responsive and intuitive front-end interface that enhances the overall user experience significantly.

The primary motive behind this effort is to build a secure, decentralized messaging application that maintains user privacy and data protection by embracing blockchain technology. Through the deployment of decentralized technology and cryptographic practices in smart contracts, the below Web3 Chat Application guarantees communication to be in an encrypted mode and inaccessible to unauthorized users. The ultimate intention of this solution is to provide users with a secure, efficient, and transparent communication platform to meet the rising need for privacy-based digital communication.

I. REVIEW OF EXISTING TECHNOLOGIES

1. Storj

Overview:

Storj is a decentralized cloud storage platform allowing users to store files using blockchain technology securely. It operates on a peer-to-peer network and encrypts data before distributing it across multiple nodes.

Key Features:

- End-to-end encryption for files.
- Files are divided into smaller pieces and distributed across a decentralized network (sharding).
- Users can rent out their unused storage space in exchange for STORJ tokens.
- Redundancy and file availability are ensured through blockchain.

2. Filecoin

Overview:

Filecoin is a decentralized storage network built on the InterPlanetary File System (IPFS). It incentivizes users to provide storage by paying them in Filecoin tokens.

Key Features:

- Users rent out unused storage in exchange for Filecoin tokens.
- Data retrieval and storage deals are made through a decentralized marketplace.
- Built-in redundancy to prevent data loss.
- Works on the IPFS protocol, making content addressing efficient.

3. Sia

Overview:

Sia is another decentralized cloud storage platform that leverages blockchain technology to ensure data security and privacy. Users pay with Siacoin (SC) to store data across a decentralized network of hosts.

Key Features:

- Data is encrypted, divided into smaller chunks, and spread across multiple hosts.
- Users pay with Siacoin (SC) for storage, while hosts earn SC tokens.
- Redundant storage ensures data availability.
- Smart contract-based agreements between users and storage providers.

Key Gaps Identified in Existing Solutions:

In light of this analysis, the Cipher Circle seeks to fill the gaps identified in existing solutions with the help of these unique value propositions:

1. Enhanced User Experience and Interface Design:

-Simplified user-friendly step-by-step Onboarding interfaces guides, with tutorials, offer clear and pre-configured templates for everyday tasks. This will lower the barrier to entry for non-technical users, making it easier to adopt decentralized solutions.

2. Improved Scalability and Performance:

-Layer 2 Solutions: Use Layer 2 scaling technologies, such as off-chain processing or sidechains, to enhance transaction throughput and reduce latency. This helps address issues related to slow data retrieval and file uploads.

-EdgeNodesandCaching: Implement edge computing and caching mechanisms that store frequently accessed data closer to users, reducing retrieval times and improving user experience.

Challenges:

1. High traffic can slow down message processing on the blockchain.

-Solution: Use off-chain messaging with on-chain verification for improved efficiency.

2. User Authentication Without Centralized Control:

-Traditional login methods rely on centralized databases, contradicting decentralization principles.

-Solution: Implement wallet-based authentication (e.g., MetaMask, Wallet Connect) to enable decentralized identity management.

3. Regulatory and Compliance Challenges:

-Decentralized applications may face legal restrictions in different jurisdictions.

- Solution: Ensure compliance with evolving crypto regulations and provide optional identity verification mechanisms.

II. SCOPE

CipherCircle App aims to offer a secure and private messaging service by leveraging blockchain technology and cryptographic methods, thus encrypting all text messages and protecting them from unauthorized access. It leverages MetaMask to provide user authentication and transaction signing, thus allowing it to interact with the Ethereum blockchain securely. Chat data is saved in a decentralized fashion on Ethereum, thus eliminating centralized vulnerabilities and ensuring data integrity. The app informs users through resources and knowledge about blockchain privacy features, thus allowing best practices in secure communication. Additionally, it has an independent interface for companies to communicate confidentially with each other internally, thus protecting sensitive corporate information from disclosure. Automated smart contracts are used to securely execute intricate transactions, thus ensuring trustless and efficient functioning within the platform.

III. PROPOSED SYSTEM

The said system is a decentralized Cipher Circle Application (DApp) designed to facilitate secure, private text messaging over the Ethereum blockchain. With responsive front-end using Next.js, Hardhat for optimized smart contract deployment, MetaMask for seamless wallet integration, Solidity for safe, innovative contract development, and Ethereum for decentralized functionality, the app focuses heavily on user data privacy and security.

One of the most striking aspects of the DApp is the end-to-end encrypted messaging system. It facilitates users to send and receive text messages stored on the Ethereum blockchain, ensuring that conversations remain tamper-proof and confidential without the assistance of central servers. The Next.js-powered user-friendly interface offers a seamless user experience, and MetaMask enables wallet-based secure authentication for sending and receiving messages. Solidity-based smart contracts form the foundation of the system, deployed via Hardhat, which manages encryption, storage, and message retrieval. The contracts ensure security that only permits authorized users with legitimate wallet credentials to decrypt and view their messages, thereby avoiding unauthorized access and third-party interference. MetaMask's wallet integration enforces cryptographic authentication, requiring users to sign transactions for sending or accessing messages. Additionally, smart contracts implement access control mechanisms, ensuring that only the intended recipient's wallet address can decrypt and read each message. This decentralized approach eliminates single points of failure, offering unmatched privacy for users.

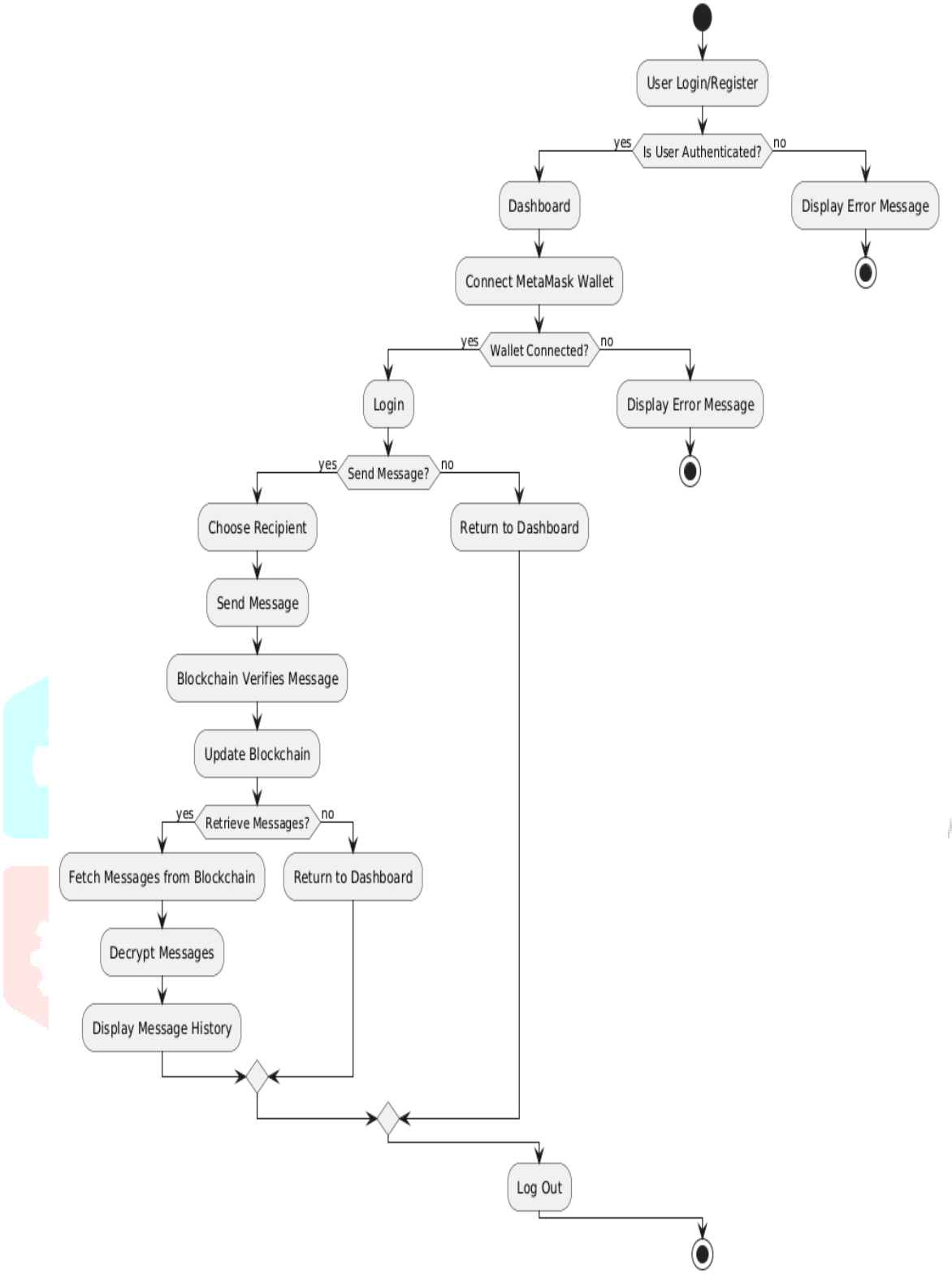

Figure 1: Flowchart of proposed system

System Flow:

Our Cipher Circle App is intended to offer a secure, decentralized messaging system to enable confidential communication. Our app is developed on Ethereum, with Next.js for smooth front-end, Hardhat for smart contract deployment, MetaMask for wallet support, and Solidity for secure smart contract code. The system offers end-to-end encryption and decentralization to protect confidential communications from unauthorized use.

The app is created to be straightforward and easily usable, with no long training process. The use of blockchain technology provides message security and confidentiality, the fundamental needs for sensitive use. The interface is intuitive, with an emphasis on usability while providing robust security through the use of MetaMask authentication and smart contract-based operations.

The dashboard is user-experience-oriented, and users can comfortably interact and communicate. It is only accessible to employees with MetaMask wallets linked to verified Ethereum addresses, thus guaranteeing operational security. The platform is made up of five major components that are meant to make the messaging process easy.

Central to the application is the Chat Window, which serves as the main workspace for users to observe and transmit messages. This section showcases live interactions, wherein messages are encrypted and preserved on the Ethereum blockchain, ensuring protection against tampering. The organized layout facilitates clear communication, particularly during critical discussions.

On the left, the Chat List Panel groups active conversations. Users can select from a library of active chats, each one linked to a unique smart contract address. This panel increases navigational ease, allowing users to switch between conversations with teams or collaborators in a simplified manner.

The right-hand-side Message Input Panel offers the users the convenience to write and send messages. Upon input, users authenticate transactions with MetaMask, which invokes the smart contract to add the message to the blockchain. This allows only the authorized parties to see the conversation.

The platform implements Message Encryption Rules in order to ensure security. Messages are encrypted via public-key cryptography prior to storage on-chain in a way that only the respective intended receivers with the respective private keys can decrypt and view them. This ensures confidentiality even on a public blockchain.

Lastly, the right-hand side has the Functional Buttons Panel that contains usability-enhancing features. Users can initiate new chats and update the chat list.

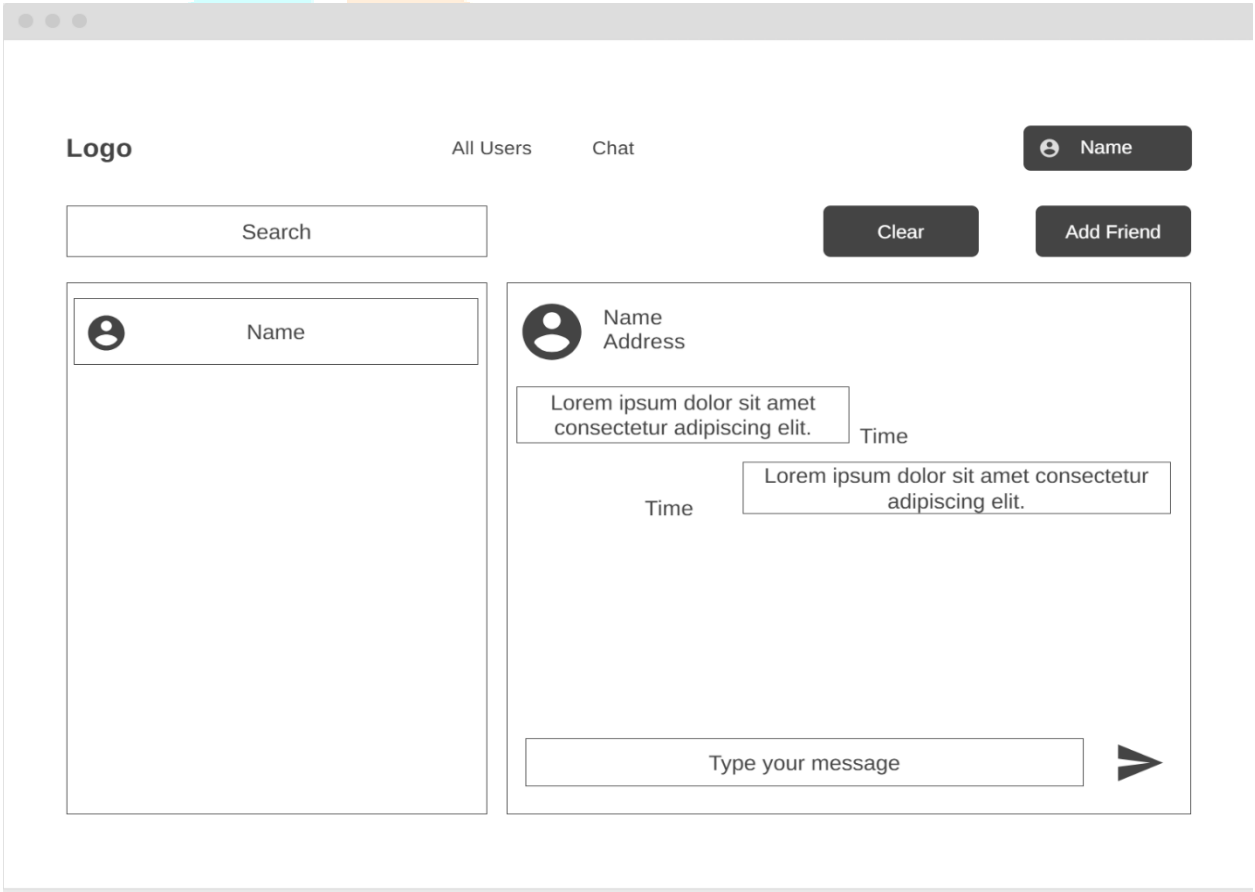

Figure 2: Wireframe of overall interface

Technology Used:

Next.js: Next.js is the front-end framework of the Cipher Circle Application, providing a responsive and fast user interface. Server-side rendering and static site generation using Next.js provide high-performance optimization, and API routes within provide smooth integration with the Ethereum blockchain. The React-based framework structure provides ease in component development with a smooth and scalable user experience.

Hardhat: Hardhat is the development environment used for smart contract building, testing, and deployment in the Cipher Circle Application. It has a comprehensive set of tools that support compilation and deployment of Solidity contracts to the Ethereum blockchain. Hardhat enables solid and efficient development of creative contracts through facilities like local blockchain simulation and advanced debugging capabilities.

MetaMask: MetaMask is the integration layer of the wallets, which provides secure interaction between users and the Cipher Circle Application. It enables users to connect their Ethereum wallets, sign transactions, and manage their identities in the blockchain world. The browser extension offered by MetaMask simplifies the user onboarding process and offers seamless interaction with the decentralized application.

Solidity: Solidity is the programming language of the smart contracts that power the Cipher Circle Application. It enables the creation of secure, decentralized logic to hold and encrypt chat messages in the Ethereum blockchain. Solidity's robust syntax ensures the application's fundamental functionality is tamper-proof and open.

Ethereum: Ethereum is the platform that enables the smart contracts and decentralized data storage of the Cipher Circle Application. Its decentralized network ensures that chat messages are encrypted and stored securely without relying on centralized servers. Ethereum's robust infrastructure enables the scalability and trustless functioning of the application, maintaining user privacy and security

IV. CONCLUSION

The blockchain-based Cipher Circle private messaging app brings forth a revolution for secure and private messaging; it is an app that changes the entire definition of digital messaging in this age of utmost data privacy. The offering melds together end-to-end encryption and decentralized user identity management to provide security, immutability, and efficiency for the communications of users so that sensitive information is naturally safeguarded against any threats from outside. Nonetheless, there are considerable barriers standing in the way of the app, particularly high transaction costs due to Ethereum gas fees, scalability restrictions in any blockchain network, and the challenges of navigating through constantly changing regulatory regimes across borders; the application directly implements pioneering solutions to counter these obstacles. For instance: zero-knowledge proofs provide maximum privacy by allowing secure verification without revealing any data; cross-chain communication protocols maximize scalability through interoperability with other chains; and decentralized moderation systems allow community Governance upon the platform to guarantee integrity without centralized interventions. Cipher Circle provides a truly Citadel for messaging services with unprecedented security, transparency, and user sovereignty because of its decentralized blockchain nature. It enables free conversations between people with little regard for the threat of surveillance, data breaches, or other forms of centralized control, drawing the roadmap for creating a trustless and resilient ecosystem that respects user sovereignty. Backing the application further with tried and tested scalable infrastructure and the latest cryptography along Ethereum lines reduces the vulnerabilities inherent in centralized systems while providing a near-perfect platform for privacy-focused user-centric communication. Thus, it ensures a seamless user experience for the nontechnical community, practically bridging the gap between cutting-edge blockchain technology and everyday use. This pioneering decentralized app has also paved the way toward a conceivable future of data security and digital sovereignty: where every user is the sovereign commander of his or her data, interactions, and digital history, until a fully secure, transparent, and fair DApps environment arrives, thus launching a re-imagination of the future of global communications in the Web3 era.

V. FUTURE SCOPE

1.Integration with Decentralized Storage:
Storing chat history on decentralized networks like IPFS or Arweave ensures persistence and censorship resistance.
2.Improved Privacy with Zero-Knowledge Messaging:
Implementing ZK-SNARKs or ZK-STARKs for encrypted message verification without revealing contents.
3.Cross-Chain Messaging Protocols:
Developing interoperability between Ethereum, Polkadot, and Cosmos for a broader user base.
4.AI-Powered Moderation and Spam Filtering:
Utilizing AI-driven smart contracts for automated content filtering while preserving decentralization.

5.Voice and Video Chat via Web3 Infrastructure:
Exploring decentralized communication frameworks like Livepeer for real-time multimedia messaging.
6.Decentralized Autonomous Organization (DAO) Governance:
Allowing the community to vote on platform upgrades, moderation policies, and feature enhancements.
7.Gasless Transactions with Meta Transactions:
Using relayer networks to enable gas-free transactions for a seamless user experience.
8.Enhanced User Experience with Progressive Web Apps (PWA):
Developing a mobile-friendly, lightweight chat interface with Web3 capabilities.

VI. REFERENCES

[1]. Johar, S., Ahmad, N., Asher, W., Cruickshank, H., & Durrani, A. "Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey" Applied Sciences, 11(14), 6252, July 2021.

[2]. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F.-Y. "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends" IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266-2277, November 2019.

[3]. Khan, F., Mantri, N., Rajput, S., Dhakane, D., & Padiya, P. "Anonymous De-Centralized Ephemeral Chat Application Using Interplanetary File System" International Journal of Advanced Computer Science and Applications, 11(5), 1-7, May 2020.

[4]. Kim, D., & Park, S. "Blockchain-Based Caching Architecture for DApp Data Security and Delivery" IEEE Access, 9, 123456-123467, August 2021.

[5]. Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. "Blockchain Smart Contracts: Applications, Challenges, and Future Trends" Blockchain: Research and Applications, 2(2), 100006, June 2021.

[6]. Hisseine, M. A., Chen, D., & Yang, X. "The Application of Blockchain in Social Media: A Systematic Literature Review" Journal of Information Security and Applications, 58, 102748, May 2021.

[7]. Sun, Z., Wang, Y., Cai, Z., Liu, T., Tong, X., & Jiang, N. "A Two-Stage Privacy Protection Mechanism Based on Blockchain in Mobile Crowdsourcing." International Journal of Intelligent Systems, 36(5), 2058–2080, May 2021. doi:10.1002/int.22374.
[8]. Lin, S. Y., Zhang, L., Li, J., Ji, L. L., & Sun, Y. "A Survey of Application Research Based on Blockchain Smart Contract." Wireless Networks, 28, 635–690, January 2022. doi:10.1007/s11276-021-02874-x.

[9]. Bhadoria, R. S., Das, A. P., Bashar, A., & Zikria, M. "Implementing Blockchain-Based Traceable Certificates as Sustainable Technology in Democratic Elections." Electronics, 11(20), 3359, October 2022. doi:10.3390/electronics11203359.

[10]. Taherdoost, H., & Madanchian, M. "Blockchain-Based New Business Models: A Systematic Review." Electronics, 12(7), 1479, March 2023. doi:10.3390/electronics12071479.

[11]. Sangeeta, N., & Nam, S. Y. "Blockchain and Interplanetary File System (IPFS)-Based Data Storage System for Vehicular Networks with Keyword Search Capability." Electronics, 12(4), 985, February 2023. doi:10.3390/electronics12040985.

[12]. Wang, X., Li, J., Zhang, X., & Chen, Y. "A Blockchain-Based Secure Data Sharing Framework for Internet of Things Using IPFS and Smart Contracts." Computer Communications, 194, 123–134, October 2022. doi:10.1016/j.comcom.2022.07.015.

[13]. Hussien, H. M., Yasin, S., Udzir, N. I., & Ninggal, M. I. H. "Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralized Storage." Sensors, 22(12), 4365, June 2022. doi:10.3390/s22124365.

[14]. Zhang, Y., Xu, C., Lin, J., & Ni, J. "Blockchain-Based Secure and Privacy-Preserving Data Trading in Social Media Platforms." IEEE Transactions on Network and Service Management, 20(1), 456–468, March 2023. doi:10.1109/TNSM.2022.3201234.

[15]. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. "Blockchain and IPFS-Based Secure Data Storage and Distribution for IoT Healthcare Systems." IEEE Internet of Things Journal, 10(5), 4235–4247, March 2023. doi:10.1109/JIOT.2022.3215678.

[16]. Li, M., Chen, Y., & Wang, J. "A Blockchain and IPFS-Based Decentralized Social Media Platform with Privacy-Preserving Smart Contracts." Journal of Parallel and Distributed Computing, 169, 245–256, November 2022. doi:10.1016/j.jpdc.2022.07.008.

[17]. Tariq, N., Khan, F. A., & Asif, M. "A Blockchain and IPFS-Based Framework for Secure Healthcare Data Sharing with Smart Contracts." Journal of Cloud Computing, 13(1), 98, September 2024. doi:10.1186/s13677-024-00512-3.

[18]. Baldauf, J., Obermeier, S., & Rannenberg, K. "Security Best Practices for Ethereum Smart Contract Development: A Comprehensive Guide." Electronics, 13(10), 1923, May 2024. doi:10.3390/electronics13101923.

[19]. Chatziamanetoglou, D., & Rantos, K. "A Permissioned Blockchain-Based Mechanism for Secure Configuration Management in Large-Scale ICT Systems." Electronics, 12(15), 3267, August 2023. doi:10.3390/electronics12153267.