Secure Message Passing Using Consortium Blockchain in Government Organization

Rudransh Gupta[1], Neerav Jain[1], Nikita Choudhary[1], Sakshi Rai [1], and Swasti Singhal [2]

[1] Computer Science and Information Technology, KIET Group Of Institutions, Dr. A.P.J. Abdul Kalam University, Ghaziabad, India [2]Faculty of Computer Science and Information Technology, KIET Group Of Institutions, Dr. A.P.J. Abdul Kalam University, Ghaziabad,

Email: rudransh9119@gmail.com, neerav.galaxy@gmail.com, nikita31choudhary@gmail.com, sakshi.2024ec1205@kiet.edu, swasti.singhal@kiet.edu

***Abstract*—Blockchain is a digitally distributed, decentralized ,public ledger that exists over a network .This research paper present a consortium blockchain-based distributed system designed for secure and transparent message passing. Consortium blockchains, with their restricted access to trusted participants, ensure enhanced security and control. This system provides a secure, tamper-resistant platform for governmental and organizational communication. By harnessing the potential of blockchain technology, this paper offers a transformative solution for secure data exchange in the digital age. This paper details the technical aspects, real-world applications, and the far-reaching implications of adopting this innovative system, heralding a new era of trust and reliability in secure communication.**

Keywords—Secure Message Passing, Consortium Blockchain, Government Organizations, Decentralized Communication, Ethereum, Smart Contracts

I. INTRODUCTION

In an era defined by the ever-expanding digital landscape, secure and confidential communication is paramount, particularly for governmental bodies and organizations handling sensitive information. The conventional methods of safeguarding government data have proven inadequate in the face of evolving cyber threats. To address this pressing concern, we propose a solution that leverages the power of consortium blockchain technology to construct a secure communications network designed exclusively for governmental and organizational use. Blockchain technology, has already demonstrated its versatility by underpinning an array of applications. From facilitating smart contracts to managing digital rights, wagers, escrow services, and digital currencies, blockchain's potential is undeniable. Moreover, its utility extends to maintaining critical records in healthcare, title management, voting systems, and safeguarding intellectual property This blockchain-based infrastructure serves as the foundation for our proposed secure communications network. confidentiality, ensuring that sensitive information is not compromised. This envisioned system seeks to create secure communication channels for government personnel, echoing the familiar format of channels on platforms like Discord. What sets this solution apart is the implementation of a consortium blockchain, designed to admit only vetted and approved organizations, thereby ensuring a higher degree of transparency and security. The network's nodes will be interconnected using the robust" yarn" mechanism, and it will employ Meta Mask as the authentication mechanism, guaranteeing the integrity and identity of participants. These secure channels are meticulously tailored to the unique needs of governmental entities, offering access exclusively to authorized individuals. In addition to channel-based interactions, the platform will feature a direct messaging capability to enable secure one-to-one communication among government representatives. Security is further bolstered by the implementation of end- to-end encryption and message confidentiality, safeguarding sensitive information from potential breaches. Blockchain technology has seen widespread adoption across various sectors, including banking and finance ,government services, energy and utilities, manufacturing, and technology services . While the application of blockchain in these domains is progressing, there remains ample room for further innovation and development. This paper's anticipated contribution is to provide a comprehensive overview for researchers seeking to integrate blockchain technology as a foundational component of their applications. By examining the possibilities and challenges associated with blockchain integration, we aim to inspire further research and development in this promising domain.

In the following sections, it will delve deeper into the intricacies of blockchain technology, the benefits of consortium blockchains, the technical aspects of our proposed communication network, and its potential impact on secure governmental and organizational communication. This paper aims to be a guide and reference for future research in this forward-looking field.

Additionally, to visualize the working standards of a consortium blockchain Figure.1 , we will discuss the specific standards and processes integral to our proposal, ensuring the security and effectiveness of the network.

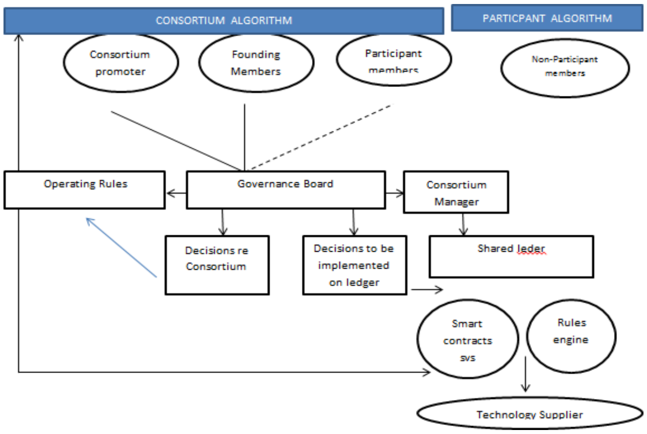

Figure. 1. WORKING STANDARDS OF CONSORTIUM BLOCKCHAIN

A comprehensive comprehension of blockchain characteristics and an overview of current blockchain-enabled applications across industries. Based on a content analysis methodology, we highlight the growing academic community's interest and identify important research streams which are the classification of blockchain-based applications across a multitude of industries, guiding researchers by providing a roadmap of prospective research avenues, challenges, and opportunities for which additional research is required; and assessing the suitability of blockchain technology to create value in these sectors in light of the various limitations this technology presents. It is important to note that this review cannot in any way be deemed exhaustive due to the rapid development of blockchain technology.

II. RELATED WORK

Blockchain is a new type of database which is quite useful and versatile. It has many challenges but the results are even greater in value because it prevents us from all kinds of frauds and deception as it is quite transparent and immutable. [1]

Blockchain allows payments to be finished without any bank or intermediary hence it can be used in different services including public services. Therefore, businesses that require high reliability and honesty can rely on blockchain. Though there could be a problem of scalability with blockchain as the amount of transactions are increasing exponentially which makes the blockchain bulky.[2]

Through blockchain, storing degree and achievement certificates securely is possible by adding this information to the blockchain through the college or university. Students can then access or share their credentials with employers through their online CV, providing a secure method that eliminates concerns about institutional changes or data loss.[3]

Blockchain applications span a diverse range of sectors, including cryptocurrency, financial services, risk management, and the internet of things (IoT).

Moreover, they extend to public and social services, showcasing the versatility of blockchain technology in revolutionizing various industries. The spectrum of blockchain applications encompasses not only the realm of digital currencies and financial solutions but also extends its transformative impact to fields such as risk management and the integration of IoT.[4]

As of its involvement in the financial and official sector, the integration of central bank money on the blockchain involves incorporating traditional central bank-issued currencies onto a blockchain platform. This allows for the digitization and secure tracking of central bank money transactions. [5]

The exponential growth of blockchain technology in the financial sector is evident in its widespread applications, encompassing money transfers, cross-border payments, identity verification, contractual agreements, trade finance, insurance, smart contracts, auctions, and currency trading. Western nations, such as the USA, Australia, Canada, South Korea, Russia, and Israel, have actively embraced and invested in blockchain-oriented applications, recognizing the transformative impact it can have on financial processes. This global momentum underscores the drive to integrate blockchain solutions into traditional financial systems, emphasizing their potential to enhance efficiency, transparency, and security across various financial operations.[6]

In addition to presenting Blockchain platforms like Ethereum and Hyperledger, along with relevant case studies, the exploration of future directions in Know Your Customer (KYC) practices further enriches the understanding of this evolving landscape. The continuous evolution of KYC processes in the context of Blockchain involves exploring innovative solutions, such as decentralized identity verification and self-sovereign identity models. These approaches aim to enhance user privacy and control over personal information, while simultaneously streamlining and securing KYC procedures for various industries, including finance and healthcare.

Moreover, the integration of artificial intelligence and machine learning within Blockchain-based KYC systems is gaining prominence. These technologies contribute to more efficient identity verification processes, reducing the risk of fraud and enhancing overall compliance. As the synergy between Blockchain and KYC continues to unfold, there is a growing emphasis on creating interoperable and standardized frameworks, fostering collaboration between industry stakeholders, and addressing regulatory challenges to ensure widespread adoption and seamless integration into existing systems. This forward-looking perspective underscores the dynamic nature of KYC in the context of Blockchain technology, paving the way for more secure, efficient, and globally accessible identity verification processes. [7]

Blockchain is also gaining popularity in the financial sector. A subdomain of blockchain 'Cryptography' assumes a pivotal role in fortifying the security and integrity of payment services within the financial domain. In the sphere of digital transactions, cryptographic methodologies are systematically employed to encrypt confidential financial data, thereby ensuring its confidentiality and mitigating the risk of unauthorized access. This meticulous approach to secure communication is particularly imperative in online payment services, where the protection of financial information during transmission is of paramount concern.[8]

The exponential growth of blockchain technology in the financial sector is evident in its widespread applications, encompassing money transfers, cross-border payments, identity verification, contractual agreements, trade finance, insurance, smart contracts, auctions, and currency trading. Western nations, such as the USA, Australia, Canada, South Korea, Russia, and Israel, have actively embraced and invested in blockchain-oriented applications, recognizing the transformative impact it can have on financial processes. This global momentum underscores the drive to integrate blockchain solutions into traditional financial systems, emphasizing their potential to enhance efficiency, transparency, and security across various financial operations.[9]

Payment systems rooted in blockchain technology, such as cryptocurrencies, extensively leverage cryptographic algorithms. These algorithms are instrumental in securing transactions, governing the creation of new units, and verifying the transfer of assets. Widely adopted cryptographic techniques, including public and private key cryptography, contribute to the establishment of secure wallets and facilitate reliable peer-to-peer transactions.

The employment of cryptography in finance, particularly within payment services, functions as an indispensable layer of defense. It fortifies the confidentiality, integrity, and authenticity of financial transactions in the contemporary digital landscape.[10]

Blockchain also presents remedies to the growing challenges of security, verifiability, and transparency. Its objective is to foster a collaborative and dependable digital ecosystem. By eliminating the vulnerability associated with a single point of failure, this technology becomes applicable in sectors prioritizing direct information flow and robust network security.[11]

III. METHODOLOGY EMPLOYED

The objective of employing a consortium blockchain for secure message passing within government organizations is to elucidate the practical steps and considerations entailed in the deployment and operation of a secure messaging system. This section revolves around the transformation of theoretical design and conceptual frameworks into a fully operational system, guaranteeing secure and trusted communication within the government body.

In figure. 2, various facets such as infrastructure setup,network configuration, smart contract development, security protocols, access control, integration, testing, and deployment, all contributing to the establishment of a secure and efficient messaging system for government use

A. <u>Setting Up Blockchain Nodes and Token Initialization</u>:

The foundation of the Secure Message-passing system lies in the creation and management of blockchain nodes. To ensure the security and transparency of communications, we use a consortium blockchain approach, where access is restricted to vetted members. The blockchain nodes are strategically set up to form a network that underpins the entire system.

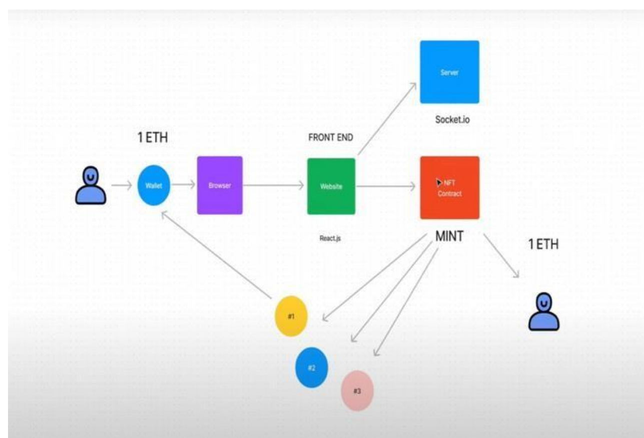

Figure. 2. Architectural Diagram of Application

The initialization of tokens plays a pivotal role in facilitating secure communication and data management. Ethereum, a well-established blockchain platform, is harnessed to create these tokens. Smart contracts, coded in Solidity, provide the backbone for this process. These contracts validate nodes within both public and private blockchains, fostering the creation ofa robust consortium blockchain network.

B. <u>Frontend Development:</u>

The user interface (UI) and overall user experience are paramount in the Secure Message Passing System. A dynamic and user-centric platform is essential for smooth government communication and data management. The front-end development integrates various tools and technologies to create an elaborate orchestration that caters to the intricate needs of the project.

React.js, a popular JavaScript library for building interactive and dynamic web applications, is the cornerstone of our frontend development. It provides the necessary foundation for all government organizations to securely interact and exchange data over the platform.

C. Deploying Smart Contracts and Tokenization:

The deployment of smart contracts and tokenization is a critical component of the system's functionality. Hardhat, an intricately designed development environment for Ethereum software development, is employed in conjunction with Ether.js for the efficient deployment of smart contracts. These contracts, written in Solidity, not only create tokens but also handle transactions and maintain token holder balances. Users acquire tokens by sending Ethereum (ETH)

```
node_modules > @openzeppelin > contracts > token > ERC721 > ERC721.sol
pragma solidity ^0.8.0;
import "../../ introspection/IERC165. sol";
/**
* @title ERC721 Non-Fungible Token Standard basic interface
* @dev see https :// eips . ethereum . org/EIPS/eip -721 */
contract IERC721 is Context, ERC165, IERC721, IERC721Metadata {
event Transfer ( address indexed from , address indexed to , uint256 indexed tokenId ) ;
event Approval ( address indexed owner , address indexed approved , uint256 indexed token
event ApprovalForAll ( address indexed owner , address indexed operator , bool approved )
function balanceOf(address owner) public view returns (uint256 balance);
function ownerOf(uint256 tokenId) public view returns (address owner);
function approve(address to , uint256 tokenId) public ;
function getApproved(uint256 tokenId) public view returns (address operator);
function setApprovalForAll(address operator , bool approved) public ;
function isApprovedForAll(address owner, address operator) public view returns (bool);
function transferFrom(address from , address to , uint256 tokenId) public ;
function safeTransferFrom(address from , address to , uint256 tokenId) public ;
function safeTransferFrom ( address from , address to , uint256 tokenId , bytes memory da
public ; }
```

the token's contract, which allocates tokens in return. We follow the widely recognized ERC-721 standard within the Ethereum blockchain ecosystem for token creation. ERC refers to Ethereum Request for Comments, which are technical standards for tokens on the Ethereum platform, accessible online as EIPs - Ethereum Improvement Proposals [10]. EIPs consist of core protocol specifications that cover those already implemented and released, or those planned to be, along with client APIs and contract standards. ERCs encompass application-level standards and conventions for Ethereum, such as smart contract and token standards. Furthermore, ERC20 outlines the standard token interface and offers a model implementation for a smart contract token API, while ERC721 does the same for non-fungible tokens [8]. Two primary standards exist for tokens: ERC-20 for fungible tokens (FTs), and ERC-721 for non-fungible tokens (NFTs). FTs are used to represent various amounts of identical assets and are frequently utilized for integrating crypto-currencies on the Ethereum platform. NFTs can symbolize ownership of various types of unique assets, including physical property like houses or artwork, as well as collectibles such as virtual pets or game cards.

The ERC-721 standard offers fundamental features for monitoring and transferring NFTs through its smart contract API, considering transactions made by both the original owners and third parties. In this context, these authorized mediators can be brokers, wallets, or auctioneers, and are referred to as operators.

```
pragma solidity ^0.8.9;
import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
contract Dappcord is ERC721{
    address public owner;
    uint256 public totalChannels;
    uint256 public totalSupply;
    struct Channel {
        uint256 id;
        string name;
        uint256 cost;
    }
    mapping(uint256 => Channel) public channels;
    mapping(uint256 => mapping(address => bool)) public hasJoined;

    modifier onlyOwner() {
        require(msg.sender == owner);
        _;
    }

    constructor(string memory _name, string memory _symbol)
        ERC721(_name, _symbol)
    {
        owner = msg.sender;
    }

    function createChannel(string memory _name, uint256 _cost)
        public
        onlyOwner
    {
        totalChannels++;
        channels[totalChannels] = Channel(totalChannels, _name, _cost);
    }
    function mint(uint256 _id) public payable {
        require(_id != 0);
        require(_id <= totalChannels);
        require(hasJoined[_id][msg.sender] == false);
        require(msg.value >= channels[_id].cost);

        hasJoined[_id][msg.sender] = true;
        totalSupply++;

        _safeMint(msg.sender, totalSupply);
    }
    function getChannel(uint256 _id) public view returns (Channel memory) {
        return channels[_id];
    }
   function withdraw() public onlyOwner {
        (bool success, ) = owner.call{value: address(this).balance}("");
        require(success);
    }
}
```

This feature enables broker/wallet/auction applications to interact with any NFT on Ethereum, supporting both basic and complex smart contracts that monitor numerous NFTs. Allow me to demonstrate the functionality of ERC-721 contracts by referencing the code from a popular implementation, Open Zeppelin. Here is the code for the Solidity interface of ERC-721 tokens in Listing 1, and Listing 2 shows a snippet of the corresponding implementation. As illustrated in Listing 1, the interface of a contract is defined through events and functions. Events are related to data that is recorded on the blockchain transaction logs through the smart contract's code. Events enable quick searches and offer cost-effective data storage for information that doesn't need to be accessed on chain. Functions are linked to code that can be executed during a transaction. Next, we will outline the events and functions established by the ERC-721 standard.

D. Real time Communication:

To enable real-time communication within the system, we leverage Socket.io, a JavaScript library. This library facilitates bidirectional communication between web browsers and the server. This feature enhances the overall user experience and ensures that communications occur promptly and seamlessly.
In Figure. 3, the Use Case Diagram, we provide a visual representation of the various use cases and interactions within the Secure Message Passing System, illustrating how the implemented components function together to achieve secure and efficient communication and data management.

The implementation of these technical components and tools ensures that the Secure Message Passing System meets its goals of secure, efficient, and user-centric government communication and data management.

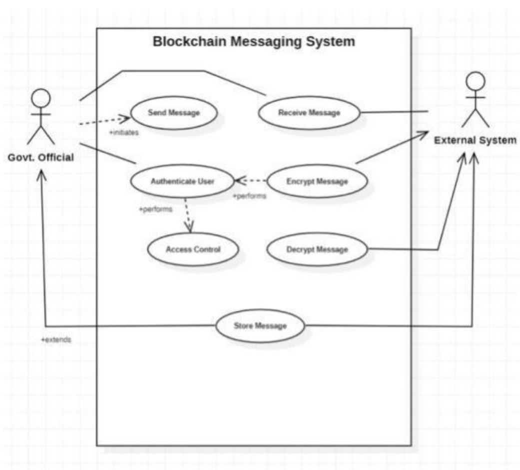

Figure.3 Use-Case Diagram

IV. RESULT

Consortium Blockchain provides a safe and effective platform for exchanging data for Government organizations (intra-communication or inter-communication). Data confidentiality is computed based on steps A–D in the proposed section (i.e., initialization, identity authentication, signature and verification, and data transfer) to accomplish a safe and efficient data exchange. The blockchain client allows users to access shared analytics and collaborate on shared data. The suggested framework has been shown to provide significant performance improvements over existing methods in terms of time cost and throughput, as were measured in experimental settings. In addition, the efficiency of information exchange was significantly increased in experimental simulations of the suggested approach. Fig. 4 illustrates the data confidentiality ratio of the proposed Access control enabled (ACE-BC) framework.

Access control systems are crucial in regulating system utilization within a consortium by effectively limiting access to authorized members. This not only guarantees compliance with applicable rules but also provides other benefits, such as increased efficiency, scalability, and stability. Users gain advantages from the system's user-friendly interface, secure file attachment features, extensive audit trails, and immediate notifications.

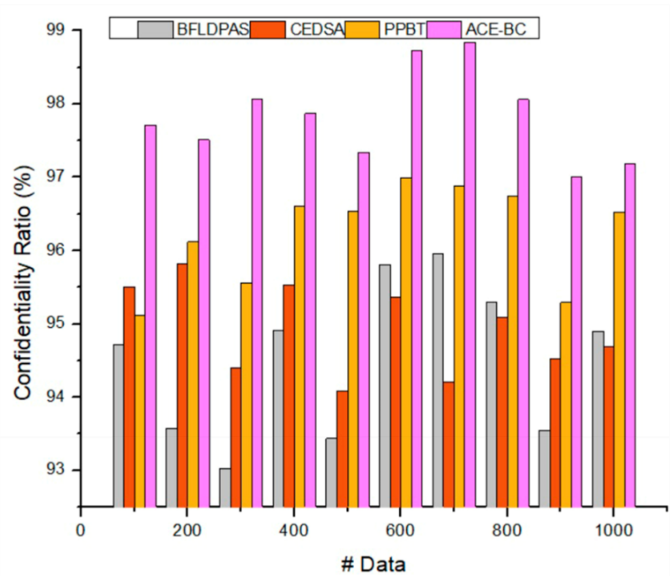

Figure. 4. Data Confidentiality Ratio

Figure 4 shows that the introduced ACE-BC framework attained a higher **confidentiality ratio (97.54%)** than the other methods. This is because successful public and private key generation helps encrypt the original data. In addition, access control mechanisms were utilized to maintain the data access restriction. Therefore, the ACE-BC approach improved the overall confidentiality rate compared to the BFLDPAS, CEDSA, and PPBT.

V. FUTURE WORK

The development and implementation of the Secure Message Passing System (SMPS) using consortium blockchain technology within government organizations marks a significant stride toward enhancing secure and trusted communication. However, several areas warrant further exploration and development to refine and expand upon the system's capabilities.

Scalability: The SMPS has demonstrated its potential with in government organizations. Future work could focus on optimizing and enhancing the system's scalability to accommodate larger consortiums and more extensive communication networks. This would require addressing potential performance bottlenecks and ensuring seamless operation as the user base expands.

Interoperability: As government organizations increasingly collaborate and share information, the SMPS could be extended to facilitate interoperability with other secure communication platforms. Developing standardized protocols for communication between different consortiums and systems would promote seamless information exchange.

Enhanced Security Measures: Continual efforts should be made to fortify the security measures of the SMPS. This includes ongoing research into emerging threats and vulnerabilities, as well as the development of advanced encryption techniques to further safeguard communication. Enhancements in identity verification methods and access control could bolster security. User Experience: To ensure the SMPS remains user centric, future work could focus on refining the user interface and incorporating user feedback for continuous improvement. Implementing features that cater to specific user needs and preferences would enhance the overall experience.

Regulatory Compliance: Given the dynamic nature of regulations and compliance requirements, ongoing work will be essential to ensure that the SMPS remains compliant with evolving legal and regulatory standards.This includes adapting to changes in data protection and privacy regulations.

VI . REFERENCES

[1] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in Proc. 2017 IEEE Int. Congr. Big Data, Jun. 2017, pp. 557-564, doi:
[2] D. Xiang et al., "Decoupling Consensus and Storage in Consortium Blockchains by Erasure Codes," in Proc. 2022 4th Int. Conf. Data Intell. Secur. (ICDIS), Shenzhen, China, 2022, pp. 194-199, doi: 10.1109/ICDIS55630.2022.00037.

[3] B. Pan et al., "Secure Data Access and Consensus Algorithm based on Consortium Blockchain in LVC," in Proc. 2021 Int. Conf. Comput. Blockchain Financial Development (CBFD), Nanjing, China, 2021, pp. 185-189, doi: 10.1109/CBFD52659.2021.00043.

[4] X. Zeng, N. Hao, J. Zheng, and X. Xu, "A consortium blockchain paradigm on hyperledger-based peer-to-peer lending system," China Communications, vol. 16, no. 8, pp. 38-50, Aug. 2019, doi: 10.23919/JCC.2019.08.004.

[5] X. Wang, Q. Feng, and J. Chai, "The Research of Consortium Blockchain Dynamic Consensus Based on Data Transaction Evaluation," in Proc. 2018 11th Int. Symp. Comput. Intell. Design (ISCID), Hangzhou, China, 2018, pp. 214-217, doi: 10.1109/ISCID.2018.10150.

[6] L. Ni, S. Zhang, G. Li, K. Han, and H. Sun, "A Design of Extensible Architecture Based on Consortium Blockchain," in Proc. 2022 IEEE 14th Int. Conf. Advanced Infocomm Technology (ICAIT), Chongqing, China, 2022, pp. 320-324, doi: 10.1109/ICAIT56197.2022.9862749.

[7] Y. Zhang, S. Lin, and J. Zhao, "SV-DEMR: An Electronic Medical Record Data Sharing Scheme Based on Searchable and Verifiable Encryption via Consortium Blockchain," in Proc. 2022 Int. Conf. Blockchain Technology Information Security (ICBCTIS), Huaihua City, China, 2022, pp. 123-126, doi: 10.1109/ICBCTIS55569.2022.00038.

[8] H. Zhu, Y. Su, Y. Qiu, J. Li, H. Xu, and X. Liao, "Civil Aviation Data Monitoring System Based on Encryptable Consortium Blockchain," in Proc. 2021 2nd Int. Conf. Electronics, Communications Information Technology (CECIT), Sanya, China, 2021, pp. 378-382, doi: 10.1109/CECIT53797.2021.00074.

[9] A. Roy, M. A. Habib, S. Hasan, and A. T. M. Shifat, "A Scalable Cross-Border Payment System based on Consortium Blockchain Ensuring Auditability," in Proc. 2023 6th Int. Conf. Electrical Information Communication Technology

10.1109/BigDataCongress.2017.85.

[10] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Journal of Parallel and Distributed Computing, vol. 11, no. 2, pp. 145-157, 2017,

[11] D. Malhotra, P. Saini, and A. K. Singh, "How blockchain can automate KYC: Systematic review," Wireless Pers. Commun., vol. 122, pp. 1987-2021, Jan. 2021.

[12] A. I. Piotrowska, "Fields of potential use of cryptocurrencies in the payment services market in Poland - results of an empirical study," Copernican J. Finance Account., vol. 5, no. 2, p. 201, 2016.

[13] R. Weerawarna, S. Miah, and X. Shao, "Emerging advances of blockchain technology in finance: a content analysis," Personal Ubiquitous Comput., vol. 27, pp. 1-14, Jan. 2023, doi: 10.1007/s00779-023-01712-5.

[14] B. Jia et al., "Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT," IEEE Trans. Ind. Inform., vol. 18, pp. 4049-4058, Jul. 2021, doi: 10.1109/TII.2021.3070862.

[15] I. Kremenova and M. Gajdos, "Decentralized networks: the future Internet," Mob. Networks Appl., vol. 24, no. 6, pp. 2016-2023, Dec. 2019.

[16] D. W. Chadwick et al., "A cloud-edge based data security architecture for sharing and analysing cyber threat information," Future Gener. Comput. Syst., vol. 102, pp. 710-722, Feb. 2020, doi: 10.1016/j.future.2019.09.042.

[17] B. Le Nguyen et al., "Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data," Comput. Mater. Contin., vol. 65, pp. 87-107, Oct. 2020, doi: 10.32604/cmc.2020.011905.

[18] S. Singhal and M. Jena, "A study on WEKA tool for data preprocessing classification and clustering," presented at the 2nd Int. Conf. Adv. Comput. Commun. Control Networking (ICACCCN), 2020, pp. 197-202,

[19] S. Singhal, N. Pathak, and B. Singh, "Parameter Boosted Approach to Collaborative Filtering Based Recommender System," V. V. S., 2022.

(EICT).Khulna, Bangladesh, 2023, pp. 1-6, doi: 10.1109/EICT61409.2023.10427617.

[20] J. Hong, E. Oh, Y. Yang, K. Roh, M. Oh, and J. Kim, "Consortium Blockchain-based V2G Energy Trading System Using Tokens," in Proc. 2020 Int. Conf. Information Communication Technology Convergence (ICTC), Jeju, Korea (South), 2020, pp. 677-682, doi: 10.1109/ICTC49870.2020.9289330