Journal of Information Systems Engineering and Management
2025, 10(22s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Novel Approach to Secure Organ Donation and Transplantation using CORDA Platform

Poojitha Ruthala[1], Panthadeep Bhattacharjee[2], Someswara Rao Thoram[3], Meena Khushi Rajendra[4]
[1]*Department of Computer Science & Engineering, NIT Rourkela, Odisha, India*
poojitharuthala@gmail.com
[2]*Department of Computer Science & Engineering, NIT Rourkela, Odisha, India*
panthadeep.edu@gmail.com
[3]*Amdocs Pvt. Ltd, Pune, India*
somesh328@gmail.com
[4]*Department of Computer Science, NIT Rourkela, Odisha, India*
Khushikumarimeena32@gmail.com

ARTICLE INFO

Received: 10 Dec 2024

Revised: 28 Jan 2025

Accepted: 14 Feb 2025

ABSTRACT

Organ donation and transplantation (ODaT) are essential elements of modern healthcare. However, the systems that oversee these processes often face significant challenges, such as inefficiency, security vulnerabilities and the prospect of unethical practices like organ trafficking. The traditional centralized systems often break down while maintaining data integrity, transparency, and equitable distribution of organs. In this paper, we propose an approach that integrates the AES encryption with a blockchain platform known as Corda in order to preserve privacy for a robust and secure transaction. This would enable us to maintain data integrity and confidentiality for a seamless participant-to-participant collaboration in course of ODaT.

Keywords: Distributed Ledger, Organ Donation, Corda, Blockchain Technology, Encryption, Privacy, Organ Trafficking, Healthcare.

1. Introduction

Millions of patients who entered end-stage organ failure have a second lease of life through ODaT. This technique (ODaT) involves the removal of an organ from the donor, who may either be living or dead, and transplanting it into a recipient whose organ has failed to function. Such a lifesaving medical procedure stands as a beacon of hope for all the patients. Organ transplantation has been in higher demand in the last few decades due to an increase in the number of cases of chronic illnesses such as diabetes, hypertension, and liver disorders, as well as finer surgical techniques and immunosuppressive therapies.

Although there have been remarkable advances in organ transplantation, the field still encounters several challenges. A great challenge is the scarcity of available organs, which makes many patients untreated at the right time. Socio-cultural barriers and unawareness have widened it further, along with myths relating to organ donation. Some ethical issues related to donor consent, fairness in the allocation of organs, and equitable access to transplants form great challenges. Another urgent issue is the trafficking of organs. Organ trafficking is another growing issue with the world, especially because of the growing trend in organ donations and transplantation. Organ trafficking targets the disadvantaged through force, fraud, or economic pressure. It remains a threat to the ethics of healthcare and the healthcare system [1].

As the need for organ transplants grows, it is evident that novel solutions are required to address these pertinent challenges. Advanced technologies can redefine the world of organ donation and transplantation. With regard to blockchain, the following is one of the most transformative technologies that brings much-needed transparency and traceability into action and ensures accountability across the whole process. The blockchain ledger is immutable; thus, every transaction—from registration of the donor through to organ allocation—can be put on it and audited. This goes a long way in ensuring ethical treatment of organs and also eradicates malpractices such as double allocation or trafficking.

In our system, the Corda privacy-centric blockchain architecture is used together with AES (Advanced Encryption Standard) [2] encryption. This framework ensures the protection of information concerning donors and recipients. Our system establishes fair distribution according to predefined medical conditions by the use of smart contracts that execute matching of donors and recipients. Thus, blockchain will ensure stakeholders trust as it offers a transparent system [3]. The main contributions of our paper are:

***Privacy-Preserving Blockchain-Based Integration using AES Encryption*:** Combining the privacy-oriented distributed ledger, which is Corda, with AES encryption would hide all information regarding donors and recipients. The whole system thus prevents unauthorized access breaches while allowing minimum data exposure solely to the authorized entities.

***Smart Contract-based Automatic Donor-Recipient Matching*:** This framework has an auto-matching process based on a smart contract, which checks medical criteria for the donor and recipient. Such automation increases efficiency and fairness in the allocation, with traceability and transparency retained at all steps of decision making.

***Dynamic Role-Based Access Control*:** This ensures granular role-based access control, meaning only notaries and matching authorities will have access to the needed data. Information is also AES encrypted inside the network, so it is unintelligible to anyone else other than the authorized entities, thus keeping it private.

***Prevention of Double Allocation through the Corda Notary Service*:** The Corda Notary service is used for the prevention of double allocation of organs. By using the AES algorithm along with this mechanism, it provides integrity and confidence in the organ allocation process.

1.1 Components of Corda

Corda is a distributed ledger [4] and comprises several components that work together to enable a secure and efficient transaction process.

Node: A Corda node is the basic building block of the network, representing a single participant—whether that is a business or an individual—and holds the node's private data and its own vault with states relevant to the participant. Functionalities of the nodes are cryptographic signing, communication with other nodes, and execution of flows, automating the business process. Services, in turn, include identity resolution and schedulers for time-based workflows.

Notary: It is a special node used for the uniqueness and verification of the transactions. The main role of the notary is to prevent double spending. Notary is used for the validation of transactions without viewing them, thus preserving the privacy of the participants.

CorDapps: CorDapps are Corda applications, which are used to build business logic on the platform. The three main components of CorDapps are contracts, states, and flows.

- *Contracts*: These are the rules that are related to state transitions and are used for the verification of transaction inputs and outputs.
- *States*: States are the shared facts that are stored on the ledger as immutable objects.
- *flows*: They are used for the creation, verification, and sharing of transactions between the parties in a sequential manner.

Ledger: The ledger, a set of shared facts in Corda, is distributed only between the participants who are involved in that particular transaction. The data minimization is supported by this architecture and provides consistency across the network.

Identity Service: Mapping of cryptographic keys to real-world identities is done by the Identity Service of Corda. This service provides a unique address to each connected entity on the network, which ensures safe communication and authentication.

Network Map Service: It is a directory that is used to record all the information about the available services and connection addresses of the participants.

Remote Procedure Call (RPC()): Developers use RPC to interact with nodes programmatically through a command-line shell to perform operations such as managing and testing node functionality.

Transaction: Transactions in Corda have inputs (states being consumed), outputs (new states being created), commands, and signatures from all the required participants, which update the ledger. There are two types of transactions, namely notary change transactions, which are used to change the state's notary and general transactions.

Flow Framework: Corda's flow framework enables communication between the CordApp and all the other parties that are present in the network. Corda uses a point-to-point messaging system for secure communication. It enables privacy by only sharing necessary information between nodes.

Compatibility Zone: Compatibility Zone provides governance features and ensures the nodes within the network are compatible and follow the rules that are shared, which are governed by the zone operator.

Time Window Service: It ensures whether the transactions are valid within a specific time frame and the non-participating entities.

In summary, Corda provides privacy, security, and scalability, and its components, such as notaries, CorDapps, and services, work together to enable large-scale software systems to support complex needs.

1.2 Why Corda for ODaT?

Corda is a permissioned blockchain. In public blockchains, data is shared among all the entities. In the case of Corda, it allows sharing of data between the parties who are involved in the transaction. In Corda, a single entity should be associated with a valid entity for getting permission to enter the network. Using this platform (Corda) in ODaT enables us to handle the medically sensitive data securely.

- *Enhanced Privacy*: Corda's point-to-point communication ensures that sensitive patient information is only shared with authorized parties, protecting patient privacy throughout the process.
- *Data Integrity and Security*: The immutable ledger of Corda guarantees that medical history, consent records, and donor-recipient matching details are securely recorded and tamper-proof.
- *Efficient Coordination*: The use of smart contracts on Corda automates consent verification, donor-recipient matching, and notifications, reducing delays and efficiency.
- *Compliance and Auditability*: The detailed audit trails of Corda transactions help to meet the legal standards and facilitate audits, ensuring compliance with strict healthcare regulations.

2 Literature review

India's National Organ and Tissue Transplant Organization (NOTTO) serves as the apex body for ODaT in the country. A national registry is maintained for donors and recipients, which is used for organ allocation. It ensures adherence to ethical and legal frameworks. NOTTO raises awareness among the people about the importance of organ donation and transplantation, which resulted in an increase of donor transplant rates in India. For instance, India achieved a record 18,378 organ transplants in 2023, reflecting the growing impact of NOTTO's initiatives [5]. However, it faces challenges such as delays in allocation and the chance of human errors. To address these issues, technological enhancements are needed to strengthen the system.

Ethereum [6] [7], an existing platform based upon blockchain, was designed to provide solutions for ODaT. This Ethereum solves the issues of lack of transparency, security, and centralization with respect to ODaT. In another paper, the Ethereum blockchain-based system [3] also uses smart contracts for solving crucial tasks. Ethereum's wide acceptance and interoperability provide a scalable and approachable solution to stakeholders involved in the ODaT management, and its decentralized nature ensures integrity and security of data [8]. Furthermore, in donation management systems that require blockchain, the generation of hash values plays an important role in ensuring data integrity. The hash values are used for validation and verification of a transaction [9]. The cryptographic approaches are used to improve security for recording transactions and for automating donor recipient matching by using smart contracts. By doing this, the accuracy and efficiency of the system get increased.

3 Methodology

The proposed methodology for this work is developing a robust, secure, and privacy-focused system for ODaT using Corda blockchain technology (Figure 1). It is integrated with AES encryption for enhanced data protection.

System Overview: In our system, there are three key entities, namely donors, recipients, and a matching authority. All these are the nodes that are responsible for the creation of Corda blockchain network. This platform ensures privacy by allowing the transaction information to be accessed only by the participants who are involved in that particular transaction.

Data Handling and Security: For encryption purposes, the AES algorithm is used to protect sensitive personal and medical information. At the time of registering the details, the donor information as well as the recipient information, like blood group, organ type, and name, are encrypted. This encrypted data gets stored on Corda's ledger, providing integrity, and cannot be changed once it gets stored.

During the matching process, the authority decrypts data to perform compatibility criteria tests. The AES encryption is used for securing the data so that the system ensures that data remains confidential during its lifecycle. This prevents the unauthorized access of data. The decryption key is provided only to the matching authority, which provides security and protects the sensitive information.

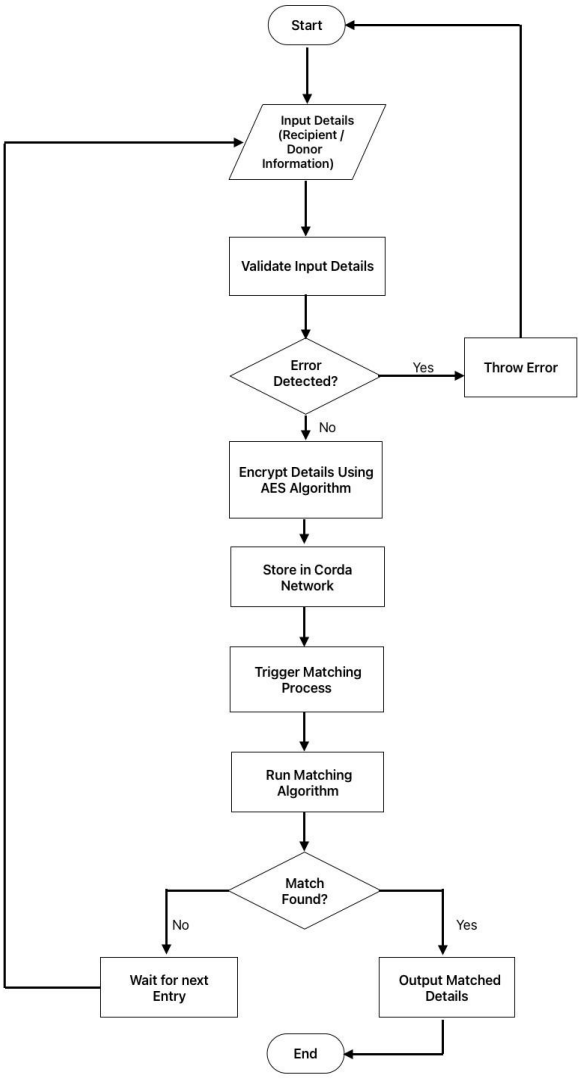

Figure 1: ODaT flow diagram

Registration Process: In this process, the donor and the recipient register details, which will get stored in the ledger. The input details are validated by the notary. In case of any error in the entry of input details, the system throws an error; otherwise, the details are encrypted by using the AES encryption algorithm. These details are transmitted to the Corda network for storage purposes (Figure 1).

Matching Algorithm: The matching authority has the critical role of finding compatible donors and recipients, and each new entry initiates the matching process, in which the system retrieves relevant encrypted data from the blockchain. Utilizing AES decryption, the matching authority will then assess the decrypted data against predefined compatibility standards, which involve blood type and organ type. The matching process is optimized to be real-time so that the potential matches are discovered as soon as possible. If a match is found, the details will be decrypted and securely passed on to the respective parties, thus offering the utmost confidentiality throughout the stages.

Privacy and Transparency: Corda's privacy model allows transactions and data to be visible only to the parties concerned. Along with AES encryption, this two-layer approach offers powerful protection of sensitive medical information. In addition, records in a blockchain are immutable, which provides an auditable trail and subsequently verifies the system's integrity while avoiding the breaching of confidentiality.

4 Results and Analysis

The result is the execution of a blockchain-based flow in the Corda system, which is specifically designed for organ donation and transplantation. In Figure 2, flow (ExampleFlow) is initiated by a participant known as ”QWER” with certain parameters: role as ”Recipient,” need for an organ transplant of ”eyes,” blood group ”A+,” and the interaction with the authority node with the label ”O=MatchingAuthority, L=London, C=GB.”. It then proceeds with creating a transaction, checking it against smart contract rules as constraints, signing it with the initiator's private key, and collection and verification of signatures of the matching authority (counterparty). The notary service proves the transaction valid for avoiding duplication and timestamps it for immutability. Once the system broadcasts this transaction to involved participants, it compares possible matches but fails to find any compatible donor for details applied. While no matching existence is detected, the flow ends up successfully logging a unique transaction ID, which in turn shows indeed that the transaction has been recorded on the blockchain. This will be a clear, secure, and traceable output of the process.

Figure 2: Recipient Registration

In Figure3 flow (ExampleFlow) is initiated by a participant known as ”JKL” with certain parameters: role as ”Donor,” need for an organ transplant of ”eyes,” blood group ”A+,” and the interaction with the authority node the label ”O=MatchingAuthority, L=London, C=GB.”. The transaction is then signed by the donor, and the signatures of the counterparty are gathered and confirmed. A notary service verifies and timestamps the transaction so no one can use them more than once. Upon broadcasting the transaction, it is matched with a recipient known as ”QWER” having akin requirements in being an eyes and blood group A+. The information is securely recorded, and the transaction yields a unique transaction ID that proves completion of the process. This system ensures that the matching is achieved efficiently, regardless of the registration sequence, whether the donor registers first or the recipient. In real time, the process between the matching parties proceeds smoothly.

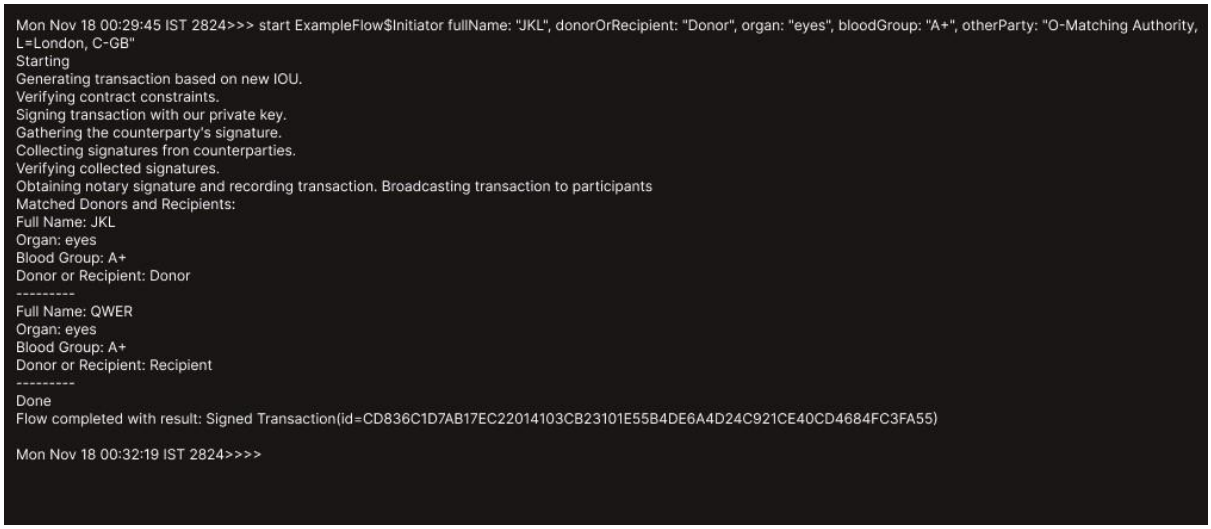

Figure 3: Donor Registration

Figure 4 illustrates the result of a vaultQuery command in a Corda blockchain network, which has been specifically designed to manage organ donation and transplantation. The list of states represents the details of participants—either donors or receivers—whose data is encrypted to maintain secrecy. These states include encrypted information of organ type, blood group, and participant name, as well as metadata such as whether the participant is a donor or recipient, and which country they are registered in and the authority who is responsible for this transaction. Every transaction would be verified by notary service and assigned a unique hash of that transaction, which would make it both immutable and traceable.

To safely store all the information, the AES symmetric encryption algorithm is used. AES operates on fixed block sizes and supports keys of 128, 192, or 256 bits. With this, the robust algorithm ensures that all sensitive details about the participants get encrypted prior to storage and decrypted when matching takes place.

Figure 4: Matching Authority

Table 1: Comparison of NOTTO, Ethereum, and Corda Systems

Metric	NOTTO (Centralized Database System)	Ethereum	Corda
Platform	Centralized database	Public blockchain	Permissioned blockchain
Participants	Donor, Recipient, Hospital, Matching Authority	Donor, Recipient, Hospital, Matching Authority	Donor, Recipient, Hospital, Matching Authority
Transaction Type	Registration, Matching, Transplantation	Registration, Matching, Transplantation	Registration, Matching, Transplantation
Data Privacy	Limited privacy, data stored in a central server	Public, all nodes can see transactions	Private, only relevant parties see transactions
Consensus Mechanism	Central authority decision making	Proof of Stake (PoS) / Proof of Work (PoW)	Notary-based
Smart Contracts	No smart contracts, traditional logic	Solidity/Vyper, flexible and general-purpose	Java/Kotlin, enforce legal agreements
Transaction Model	Relational database	Account-based model	UTXO model
Security	Susceptible to single point-of-failure and insider threats	Privacy enhancements needed for sensitive data	High privacy, encrypted data sharing
Interoperability	Difficult, often manual or custom integrations	Limited	Easy interoperability
Cost	Infrastructure costs, no per transaction fees	Variable gas fees based on network congestion	Predictable, no gas fees
Governance	Governed by a single authority	Decentralized governance via community consensus	Governed by a consortium
User Experience	Simple and centralized, no congestion issues	Seamless user experience, impacted by congestion	Consistent, though less seamless

5 Discussion

The following graph (Figure 5) depicts the comparison of NOTTO (Centralized database), Ethereum, and Corda on seven major features: privacy, consensus mechanism, scalability, smart contract model, transaction speed, energy efficiency, and use case focus. Database systems like NOTTO are noteworthy in terms of transaction speed and energy efficiency, making them ideal for high-performance, low-cost applications. Centralized systems, fall short in areas such as the consensus mechanism and smart contract model due to a lack of blockchain capabilities. Corda has been designed as it suits enterprise usage and has a high level of privacy as the transactions are only visible to the parties involved in the specific transaction, whereas the transactions carried out in the public blockchain of Ethereum are highly visible. Regarding the consensus mechanisms, Central authority makes the decisions in Centralized databases. Corda exploits notary-based validation, which is more suitable for private networks,

whereas Ethereum has moved from resource-intensive proof-of-work to proof-of-stake that improves scalability but is still less appropriate for enterprises (Refer Table 1). Scalability is one of the strongest points with Corda, using point-to-point communication, whereas Ethereum faces difficulties due to its global state synchronization, though layer-2 solutions aim to be able to improve this. Ethereum outshines Corda in smart contract functionality as it provides a robust platform for decentralized applications (dApps). On transaction speed, Corda processes faster in private networks, whereas Ethereum shows improvements with Ethereum 2.0. Corda leads in energy efficiency with lightweight mechanisms, while Ethereum has moved to proof-of-stake to mitigate its earlier energy-intensive proof-of-work. Finally, Corda's use case focus is tailored for enterprises like finance and healthcare.

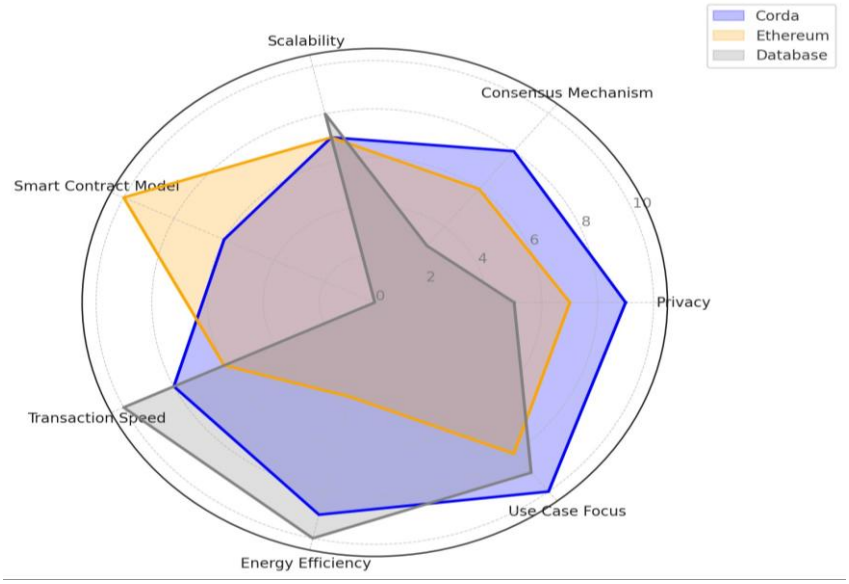

Figure 5: Comparison Graph

6 Conclusion

Through this work, we developed an ODaT system for improving the security, privacy, and efficiency in managing sensitive data. Corda's permissioned nature ensures that only authorized participants access specific information, safeguarding donor and recipient confidentiality. Healthcare professionals get efficient workflows without delay, which improves system efficiency. Based on the AES encryption integration, the system provides robust protection of data stored and transmitted in order to continue being data-compliant with privacy regulations such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act). This framework based on Corda therefore provides a safe, transparent, and ethical organ donation and transplantation process that builds trust and operational excellence.

References

[1] Juan Gonzalez, Ignacio Garijo, and Alfonso Sanchez. Organ trafficking and migration: A bibliometric analysis´ of an untold story. *International Journal of Environmental Research and Public Health*, 17, 05 2020.

[2] Shilin Liu, Yongzhen Li, and Zhexue Jin. Research on enhanced aes algorithm based on key operations. In *2023 IEEE 5th International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*, pages 318–322, 2023.

[3] Diana Hawashin, Raja Jayaraman, Khaled Salah, Ibrar Yaqoob, Mecit Can Emre Simsekler, and Samer Ellahham. Blockchain-based management for organ donation and transplantation. *IEEE Access*, 10:59013–59025, 2022.

[4] Chaehyeon Lee, Changhoon Kang, Wonseok Choi, Myunghun Cha, Jongsoo Woo, and James Won-Ki Hong. Code: Blockchain-based travel rule compliance system. In *2022 IEEE International Conference on Blockchain (Blockchain)*, pages 222–229, 2022.

[5] National Organ Tissue Transplant Organisation. About notto, 2024. Accessed: 2024-11-18.

[6] Navjeevan Chaudhary, SunilKumar S. Manvi, and Nimrita Koul. Organ bank based on blockchain. In *2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pages 1–5, 2022.

[7] Lama Abdulwahab Dajim, Sara Ahmed Al-Farras, Bushra Safar Al-Shahrani, Atheer Abdullah Al-Zuraib, and Rincy Merlin Mathew. Organ donation decentralized application using blockchain technology. In *2019 2nd International Conference on Computer Applications Information Security (ICCAIS)*, pages 1–4, 2019.

[8] Mr Shrihari, Gaurav Singh, Keerthi Reddy, and N Ajay. Organ donation and transplantation framework using blockchain. In *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, volume 1, pages 1–6, 2024.

[9] Rohit Baba, Vishvajit Gaikwad, Sanket Dhotre, Soumitra Chavan, and Rupali Waghmode. Platform for organ donation and transplantation using blockchain. *International Journal of Future Medicine Research (IJFMR)*, 6(3), 2024.