ISSN 2277-2685
IJESR/Sep. 2023/ Vol-13/Issue-3/1-10
Mr.E. Suresh Babu *et. al.*, / International Journal of Engineering & Science Research

Block chain Based Management for Organ Donation and Transplantation

Mr.E. Suresh Babu[1],Gangadhari Pranay[2], Sruthika Sharma[2], Paladugu Nagarjuna[2],Gurram Ravi Chandra[2]
[1.]Assoc.Professor,Computer Science and Engineering, CMR Engineering College, medchal, T.S, India,
[2]B.Tech,Computer Science and Engineering,CMR Engineering College,medchal, T.S,India

Abstract: With regards to registration, donor-recipient matching, organ removal, organ delivery, and transplantation, today's systems for organ donation and transplantation provide a variety of needs and obstacles as well as technological, clinical, ethical, and legal limitations. Therefore, a complete system for organ donation and transplantation is necessary to ensure a just and effective procedure and to improve patient experience and trust. In this work, we present a completely decentralised, secure, trackable, auditable, private, and reliable private Ethereum blockchain-based system for managing organ donation and transplantation. We create smart contracts and outline six algorithms with information on how they were implemented, tested, and validated. By conducting studies of privacy, security, and confidentiality as well as by contrasting our solution with the alternatives already available, we assess the performance of the suggested solution. On Github, we make the smart contract code accessible to everyone.

1. INTRODUCTION

As an alternative payment mechanism, crypto currencies are becoming more and more popular. These currencies' foundation is blockchain, which provides security and anonymity. It guarantees the immutability of data and permits pseudonymous behaviour from the parties involved in transactions. Block chain records are openly verifiable. To maintain a Sybil-resistant network, Bit coin mining depends on Proof-ofWork (PoW) [1]PoW reduces transaction throughput since it requires a lot of time and resources [2], .Protocols at layer two provide a solution to the scalability issue. It allows users to conduct transactions off-chain and significantly reduces the amount of data processing required on the blockchain.

The literature review [3] lists many solutions, including payment channels, channel factories, payment channel hubs, side chains, and commit chains. Payment Channels are often used in several applications. It is modular and does not call for significant modifications to the protocol layer. By locking their cash for a certain amount of time, two parties may mutually decide to establish a payment channel. Payments are routed via an existing network of channels by nodes that are not directly linked by a payment channel[4]. This network of linked payment channels is known as a PCN, or payment channel network. The two most well-known networks are Raiden Network for Ethereum [5] and Lightning Network for Bit coin . It is difficult to create payment and routing mechanisms for these networks that protect user privacy. The majority of routing algorithms concentrate on determining a single route for a transaction. Finding a single route for a high-value transaction is a difficult challenge, however. Channels along a route could not have enough balance after a number of payments have been completed in the network for them to transmit the cash. High-value payments should instead be divided along many pathways in these situations to improve the success rate of transactions. However, designing a protocol for multi-path payment is not simple, and we go over the difficulties encountered.

A Description Of The Project: We propose CryptoMaze, an efficient, privacy-preserving, atomic multi-path payment protocol. Our protocol optimizes the setup cost by avoiding the formation of multiple off-chain contracts on a channel shared by partial payments. To date, no other protocol has been able to achieve this optimization.

- Our protocol ensures balance security, i.e., honest intermediaries do not lose coins while forwarding the payment.
- Our protocol description ensures unlinkability between partial payments.
- We have modeled Crypto Maze and defined its security and privacy notions in the Universal Compos ability or UC framework.
- Experimental Analysis on several instances of Lightning Network and simulated networks show that our proposed payment is as fast as Atomic Multi-path Payment [6]. The run time is around 11s for routing a payment of 0.04 BTC in a network instance of 25600 nodes. The communication overhead is within feasible bounds, being less than 1MB.

2. LITERATURE SURVEY

2.1 Existing System To reflect the information pipeline model among donor hospitals, regulators, and receiver hospitals, the authors of [7] created a multi-agent software platform. The pre-transplantation duties are optimised using this platform, which may increase process effectiveness. Additionally, it enables the storage of information about potential donors and enhances direct communication between all parties involved in the organ transplantation process. The platform was used to mimic an information process, and it was determined that three to five hours may be saved.

The TransNet in [8] is a system that uses barcode scanning technology to help label, package, and monitor organs and other biological products for transplantation at the site of organ recovery. It entails enhancing the labelling system with a customised application and a transportable barcode printer that is compatible with DonorNet. The device in the operating room will be used by procurement coordinators during organ recovery to print labels and scan each organ that will be transferred. Similar to this, a lot of supply chain management systems have depended on barcodes, RFID tags, and Electronic Product Codes (EPC) to identify and share product information and make it easier to monitor products through different stages [9].Finally, to increase the effectiveness and fairness of patient selection within the current system in Australia, the authors in [10] proposed MIN, a manageable mechanism for the online matching of deceased organs to donors. The MIN process just assigns an incoming organ to a patient, minimising |KDPI-EPTS|, tie-breaking by waiting list length, and then arbitrarily after that. The Kidney Donor Patient Index (KDPI) determines the organ's quality. The Expected Post-Transplant Survival Score (EPTS), on the other hand, gauges the recipient's quality of life following the transplant. The MIN mechanism functions better than the one that the Australian Organ and Tissue Authority is now considering, according to testing data.The authors of [12] suggested a blockchain-based decentralised app for organ donation. Patients register their information, such as their medical ID, organ type, blood type, and state, via an online application. Except when a patient is in a critical condition, the system would run on a first-in, first-out (FIFO) basis. It provided speedier service, more transparency, and improved security. However, it should be adjusted when used in various regions in accordance with their laws and requirements. Similar to this, the authors in [13] created a web-based programme employing FIFO to choose an organ donor for each genuine patient in need of a transplant. This patient is given precedence in the event of an emergency. The registered hospital accepts the registered donors and registers the receivers to match them with a suitable donor based on the request. Additionally, an organ donation and transplantation application using blockchain has been presented in [14].Additionally, a blockchain use case for organ donation has been developed. Simply put, the procedure starts when the patient submits a transplant request and the donor signs a smart contract for organ donation. A licenced physician or registered nurse verifies and hashes both documents, makes a confirmed mismatching pair, and broadcasts the result across the network. A doctor must approve the match before it can be sent via the network. In the event that a match is discovered, the doctor approves and generates a hash as the following step. The confirmed matched pair is added to the blockchain if the doctor creates a hash. Finally, all the information required for medical experts to be ready for the logistics of the procedure is sent to them.

2.2 Proposed System

We describe our blockchain-based organ donation and transplantation solution in full in this section. An overview of the system architecture of our suggested solution is shown in Figure 2. It demonstrates how our approach, which involves both organ donation and organ transplantation, makes use of two smart contracts (SCs). An application programme interface (API) connects a front-end decentralised application (DApp) to the functionalities and events of these smart contracts, allowing participants to use them.Every smart contract has distinct functionalities that can only be used by participants who have received prior authorization. These individuals will have access to data kept on the chain and be able to inspect transactions, logs, and events. Doctors, hospital transplant team members, procurement organisers, organ matching organisers, a transporter, and a transplant surgeon are among the participants. The creation of a waiting list, acceptance of donors upon approval of medical tests, and automatic matching of the donor and recipient are all tasks carried out by the organ donation smart contract. The majority of the transplant procedure is managed by the organ transplantation smart contract. It consists of three steps: taking an organ from a donor, transporting the organ to the recipient, and implanting the recipient with the organ. For the sake of review and verification, all prior stages are recorded and kept on the ledger. Using a private permissioned Ethereum blockchain also ensures authorisation, confidentiality, and privacy.

2.3 Private Ethereum Network with Permission

Private blockchains, where the transactions and data are not available to the general public and are only accessed by authorised organisations, provide increased security and privacy. To enhance privacy, security, and secrecy, businesses may utilise the Ethereum blockchain to create their own private-permissioned blockchain. Details of donor organ transplants are often kept in tight confidence. This information includes the patients' medical histories and

ISSN 2277-2685
IJESR/Sep. 2023/ Vol-13/Issue-3/1-10
Mr.E. Suresh Babu *et. al.*, / International Journal of Engineering & Science Research

family backgrounds; as a result, a private permissioned Ethereurm blockchain is the best choice for this kind of deployment.

Blockchain integration

The foundation of our suggested solution is the blockchain network. The foundation for documenting transactions is provided by it events permanently to ensure accountability and data provenance.

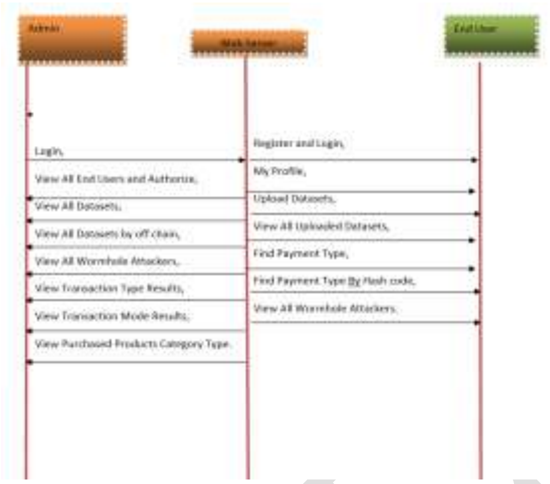


Fig 1: System Flow

3. SYSTEM ANALYSIS & DESIGN

We outline the technical details and algorithms for our suggested blockchain-based system for organ donation and transplantation in this section. The suggested solution is based on a private Ethereum blockchain, to which only authorised players and validation nodes are added.The Remix IDE, an open source website that allows creating and managing smart contracts, is used to test the Solidity-written smart contracts. Our suggested approach is mostly implemented via organ donation and organ transplantation. Each one's specifics are shown below.

3.1 Organist donation

The patient's physician, a member of the hospital transplant team, a procurement organiser, and a matching organiser are the four parties that take part in the organ donation smart contract. Each participant may participate by invoking the smart contract's operations since they all have an Ethereum address[14]. There are many distinct sorts of variables in this smart contract. One of the variables is the Ethereum address, which is used to provide certain entities, such the procurement organiser and the matching organiser, a special address. The second kind is mapping, which in our approach connects an entity's Ethereum address to a Boolean to indicate that the address must meet specific requirements. For the approved transplant surgeon and physicians, mapping is utilised as an example. Additionally, mapping is utilised for patient validity to guarantee that patient selection is unique. Additionally, there is an enumerating variable called "Bloodtype" that contains the various blood types, including "A,""B,""AB," and "O." The blood kinds are represented as "0", "1", "2", and "3" in this variable's accepts uint8 input. The enumeration variable "OrganType" also takes uint8 input, where "0" denotes "Heart," and so on. "Lung" is represented by "1. "2" stands for the liver, while "3" stands for the kidney.

3.2 Organizing Transformation

The major partners in the organ transplantation smart contract are the transplant surgeon, transporter, and donor surgeon. By using the smart contract's functions, any participant may take part. It has several different kinds of variables. For instance, the donor and transplant surgeons' addresses are stored on public Ethereum addresses. In addition, it includes a mapping system for the licenced transporters who are permitted to convey the removed donated organ from the donor hospital to the receiving hospital. The "OrganStatus" variable, which is an enumerated list of all the states the donor organ will experience, is another feature.

3.3 System Architecture: The Organ Transplantation smart contract has a set of attributes used to describe the details of the transplantation process. There is only one surgeon to take the responsibility from the donor side and only one surgeon to do the transplantation for the recipient; therefore, they are declared as Ethererum addresses. Furthermore, more than one transporter can exist in the system; thus, it is declared as mapping[15]. In addition, the smart contract has five primary functions; namely, Removing Donated Organ, Start Delivery, End Delivery, Receive Donated Organ, and Organ_Transplantation. Finally, the organ donation smart contract will have a 1:n relationship with the transplantation smart contract since only one organ donation smart contract can include all patients, whereas several transplantation smart contracts can exist for the various possible donation processes. We present six algorithms to explain the details of the various functions involved in our smart contracts.

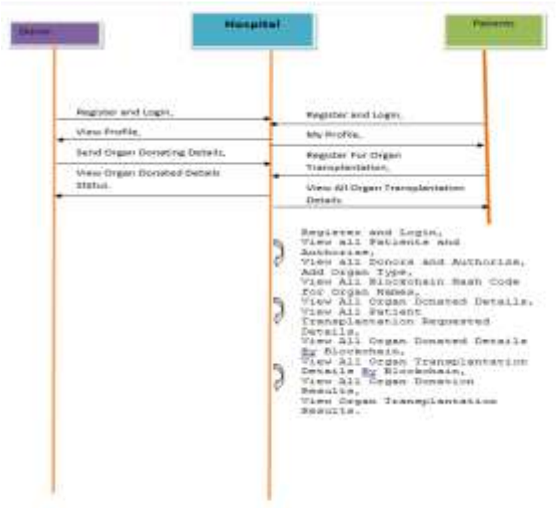
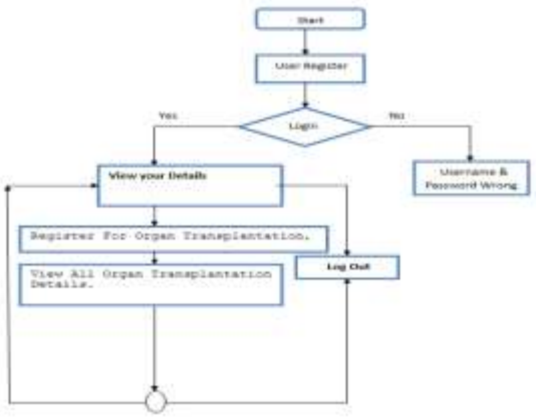
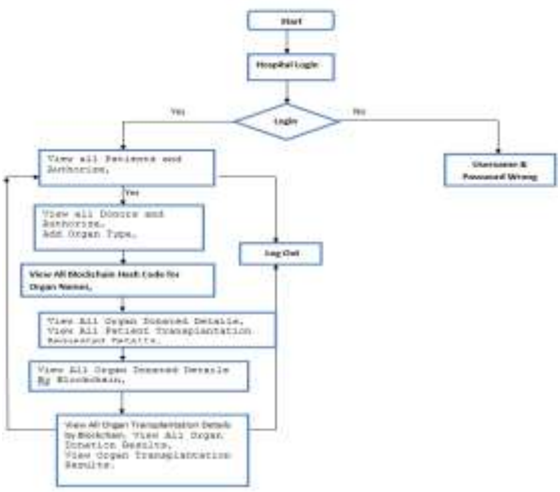


Fig 2 : System Architecture

3.4 Data Flow Diagram : Whenever a new system is developed, user training is required to educate them about the working of the system so that it can be put to efficient use by those for whom the system has been primarily designed. For this purpose the normal working of the project was demonstrated to the prospective users. Its working is easily understandable and since the expected users are people who have good knowledge of computers, the use of this system is very easy.



Patients



Hospitals

Fig 3: Flow Diagram

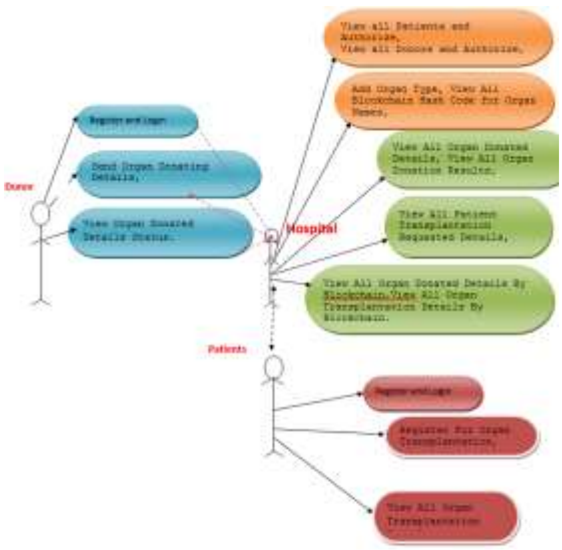


Fig 4 Use Case UML Diagrams

4. CONCLUSION

This article presents a private Ethereum blockchain-based system for managing organ donation and transplantation in a decentralised, responsible, auditable, traceable, secure, and reliable way. We created smart contracts that automatically record occurrences to guarantee the data's authenticity. We include six algorithms together with information on how they were implemented, tested, and validated. To ensure that smart contracts are secured against frequent assaults and vulnerabilities, we examine the solution's security. We contrast our approach with other already accessible blockchain-based alternatives. We go through how other systems dealing with similar issues may easily adapt our approach to match their requirements. By creating an end-to-end DApp, our solution may be enhanced in the future. Furthermore, a genuine private Ethereum network can be used to deploy and test the smart contracts. Finally, the Quorum platform can offer better confidentiality since transactions between entities can only be viewed by specific participants and no one else, in contrast to our solution where transactions between participants can be viewed by other actors authorised in the private blockchain.

5. FUTURE SCOPE

The observations of all the thirty-two sub-experiments conducted in this research leads to the conclusion that for the given set of experiment environments, Scheme A of executing the chaincode is superior because it generated fewer blocks for a write-operation as compared to a write-operation in Scheme B. Therefore, this study endorses leaving the “match run” process in the chaincode. Additionally, the read-operations seem unaffected by any of the parameters under the scope of this study. However, the write-operations performed best when the “batch time out” period was close to the transaction rate. It is safe to assume that medical institutions, especially government-backed, would be extremely circumspect in using any new technology. This empirical study concludes in favor of continued research in using blockchains for this purpose. Nevertheless, there are significant unanswered questions on issues such as data privacy and performance, requiring more investigation.

6. REFERENCES

[1] L. A. Dajim, S. A. Al-Farras, B. S. Al-Shahrani, A. A. Al-Zuraib, and R. Merlin Mathew, ‘‘Organ donation decentralized application using blockchain technology,’’ in Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS), May 2019, pp. 1–4, doi: 10.1109/cais.2019.8769459.

[2] Srihari Rao Nidamanuru, Rajesh Tiwari, Bhaskar Koriginja, Jincy Denny, J Ramesh Babu, “Identifying the Websites that Maintain Operational Standards through Obligation Links to Website-Standards Approval Body”, Turkish Journal of Computer and Mathematics Education, Vol. 12, Issue 10, 2021, pp 4456-4461, e-ISSN: 1309-4653.

[3] MD Rafeeq, VH Shastri, B Anandh, V Shanmugasundaram, PR Kumar, ... , An intelligent road traffic data management for upgrading real time performance
AIP Conference Proceedings 2426 (1) [4] Facts and Myths About Transplant. Accessed: Apr. 21, 2021.

[5] Organ Procurement and Transplantation Network. Accessed: Apr. 18, 2021.

[6] . Mrs.G.Sumalatha, B.Shiva Teja , B.Kranthi , K.Vijay Kumar, Financial Fraud Detection Anomaly Feature detection, , International Journal of Research, ISSN NO: 2236-6124, Volume VIII , Issue I, January/2019.

[7Sheo Kumar, Mrutyunjaya S Yalawar, K-NN SEMANTIC Inquiry on Scrambled Social Information BASE, ICDSMLA 2019: Proceedings of the 1st International Conference on Data Science, Machine Learning and Applications,982-991, 2020,Springer Singapore

[8] Harvard Business Review. (Dec. 13, 2021). Electronic Health Records Can Improve the Organ Donation Process. Accessed: Apr. 8, 2022.

[9] U. Jain, ‘‘Using blockchain technology for the organ procurement and transplant network,’’ San Jose State Univ., San Jose, CA, USA, Tech. Rep., 2020, doi: 10.31979/etd.g45p-jtuy.

[10] M. He, A. Corson, J. Russo, and T. Trey, ‘‘Use of forensic DNA testing to trace unethical organ procurement and organ trafficking practices in regions that block transparent access to their transplant data,’’ SSRN Electron. J., 2020, doi: 10.2139/ ssrn.3659428.

[11] P Chatterjee, SR Dutta, M Rafeeq
2022 8th International Conference on Smart Structures and Systems (ICSSS), 01-05, Comparison of segmentation of CU-Net, DRU-Net and DU-Net on Cervical Cancer Data Set.

[12] D. P. Nair. (2016). Organ is Free, Transplant Cost is Problem.

[13] P. Ranjan, S. Srivastava, V. Gupta, S. Tapaswi, and N. Kumar, ‘‘Decentralised and distributed system for organ/tissue donation and transplantation,’’ in Proc. IEEE Conf. Inf. Commun. Technol., Dec. 2019, pp. 1–6, doi: 10.1109/cict48419. 2019.9066225

[14] A Review on Various Cloud-Based Electronic Health Record Maintenance System for COVID-19 Patients.

[15]. Kumar, A., Mozar, S ‘An Overview of Various Security Issues and Application Challenges of the Attacks in Field of Blockchain Technology’. In:. (eds) ICCCE 2021. Lecture Notes in Electrical Engineering, vol 828. Springer, Singapore