International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Research Article)

Check for updates

A Track the Impact: A blockchain-based framework for transparent NGO Funding

Sowbhagya Ramya Dulam *, Rajakumari Chapala, Tanuja Elisetti, Tejaswini Pampana and Bandaru Satya Lakshmi

Department of Computer Science and Engineering, Aditya College of Engineering and Technology, Surampalem, Kakinada, Andhra Pradesh, India.

International Journal of Science and Research Archive, 2026, 18(02), 739-748

Publication history: Received on 08 January 2026; revised on 17 February 2026; accepted on 19 February 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.18.2.0309

Abstract

The other issue that is still of challenge in Non-Governmental Organization (NGO) fund management systems concerns transparency and accountability. The conventional centralized systems do not give donors visibility and can be subjected to data distortion. This paper suggests a decentralized blockchain based system of transparent management of NGO funds in the Ethereum smart contracts and MERN stack in order to solve these problems. The system will guarantee a write only history of transactions, automatic donation management, and live monitoring of donors. Coded smart contract records are written in Solidity and support donations, whereas MetaMask can be used to support authenticated blockchain transactions. With the proposed platform, it will remove intermediaries, prevent tampering, and increase the donor trust due to end-to-end transparency. The system is experimentally validated on test networks on the Ethereum platform, and shows it to be secure, reliable, and scalable.

Keywords: Blockchain; Ethereum; Smart Contracts; NGO Management; MERN Stack; Decentralized Application; Transparency.

1. Introduction

Non-Governmental Organizations (NGOs) are essential in the efforts of dealing with the key problems in the society like poverty reduction, disaster management, healthcare availability, women empowerment, and education provision. The operations and programs of these organizations are mostly financed by the public and by the institutions. Nonetheless, absence of clear and verifiable mechanisms through which the use of funds can be monitored is one of the greatest systemic issues in NGOs in the world.

Centralized banking forms and internal database systems are the major approaches towards traditional NGO fund management systems. In these models, the donations are channeled to an organizational account that is centralized and all the allocation, expenditure and reporting processes are internally controlled. Though periodic audits and financial reports are being produced, they are backward in nature and do not give real time picture of the way in which funds are being used. There are a number of vulnerabilities presented by this centralized architecture such as internal manipulation, reliance on intermediaries, and accountability. This can lead to lack of trust among the donors which may deter any future contribution thus an influence on sustainability in the long run.

The concept of blockchain technology has been developed as the groundbreaking solution to these issues as it is expected to make processes more transparent, immutable, and decentralized. A distributed registry is a type of blockchain whereby confirmed transactions are stored in cryptographically bound blocks. Nobody is able to modify the data once stored, which is integrity and trust assuring and cannot be changed without consensus throughout the entire network.

* Corresponding author: Sowbhagya Ramya Dulam

Ethereum is a programmable platform based on blockchain which allows the implementation of smart contracts self-executable programs which automatically apply the set of rules and conditions. Through the implementation of Ethereum-based smart contracts in the mechanisms of NGO funds management, it becomes feasible to provide the opportunity to verify transactions in real time, automate the payment of funds according to established standards and allow tracking of all donations transparently.

This suggested system implies the creation of a decentralized platform of NGO funds management based on the MERN stack (MongoDB, Express.js, React.js and Node.js) and integrated with a blockchain-based interaction system (MetaMask wallet). The purpose is to design, implement and assess secure, transparent, and scalable solution to increase donor trust, remove intermediaries, and offer real-time traceability of funds in the operation of NGOs. modern charitable funds.

2. Literature Survey

Blockchain technology has received extensive scholarly interest in the financial systems, healthcare systems, governance framework, and humanitarian aid industries. Some researchers have studied its ability to promote transparency and avoid the need to use centralized intermediaries. Christidis and Devetsikiotis (2016) spoke about the transformative power of smart contracts in decentralized mechanisms and how they can ensure the provision of automated trust without human interference. They focused their work on the benefits of blockchain-based programs being programmable and secure.

Boersma and Zwitter (2018) examined the use of blockchain in the distribution of humanitarian assistance. According to their findings, blockchain can contribute greatly to traceability in financial flows in multi-stakeholder environments. Bzdok and Bzdok (2018) examined the implementation of blockchain in the NGO ecosystems and highlighted how inefficiencies in operating the blockchain have been reduced through the approach of decentralization.

Even though a number of past research works have theorized the application of blockchain in the management of NGO funds, they all possess serious practical constraints. Most of them do not have real-life implementation and do not offer full-fleet necessary integration, leaving behind systems that are still in conceptual form and not deployable. Also, the majority of available solutions provide little in-dash monitoring and fail to integrate a hybrid on-chain and off-chain design.

These systems usually only serve to store transactions in the blockchain, and will not provide a working front end interface nor a scalable backend infrastructure suitable to serve real-life applications. Consequently, they do not consider critical elements like user experience, optimization of performance, and smooth integration between blockchain and conventional databases. The originality of the suggested system is that it creates a completely decentralized web application, which combines blockchain technology and scalable backend. It presents an IBM hybrid data model, which integrates blockchain as an immutable and secure storage of transaction records and MongoDB as an efficient and efficient off-chain storage and retrieval.

Additionally, the system allows visualization of transactions interactively via a dashboard in real time so that it is possible to monitor fund flows transparently. Such hybrid approach is a successful way to fill the gap between theoretical research and practical application in terms of providing a holistic, scaling, and user-friendly solution of transparent fund management of NGO.

3. Existed and Proposed System

3.1. Existing System

The current system of managing the NGO funds is majorly on a centralized system. Under this structure, the donations are done using the conventional banking systems or online payment gateways and the money is deposited in centralized accounts, which are managed by the organization. Financial lifecycle of such systems is usually characterized by registration of financial transactions in internal database, receiving allocation approval by the finance department and production of periodic financial reports. These are largely manual and controlled at the center which heightens reliance on internal controls.

This centralization method creates a number of risks and inefficiencies. Given the fact that records are kept within the company, there is a risk that there might be manipulation or distortion of data. Financial performance reports are usually reported retrospectively which results in tardy transparency. Intermediary transaction cost makes the operations costly, particularly when the transfer is performed across the borders, where the exchange of currency and regulatory processes increase the complexity.

Manual auditing does not only increase the administrative overhead but it also contributes to the risk of human error. Additionally, central databases do not have robust cryptographic validation protocols and hence, they are prone to unauthorized alterations. Although the governance practices might be good, the view of minimal transparency and privacy issues may have a negative impact on the donor confidence. These structural inefficiencies point to the necessity of a decentralized, automated and tamper-resistant solution that would enable the establishment of transparency, minimize the operational overhead as well as enhance trust among the stakeholders.

4. Proposed System

The proposed system brings out a decentralized blockchain-based fund management solution of NGOs specifically modeled around Ethereum smart contracts, which has a full-fledged full-stack web application to bring transparency, accountability, and operational efficiency. The architecture has three major layers, and it will offer specific dashboards to donors, NGOs, and administrators. These dashboards allow real-time tracking of the live statistics of donations, which allows the stakeholders to dynamically trace the flow of funds.

The business logic and user authentication are handled by application layer, and the blockchain layer supports an immutable registry of the transactions in which all donations are safely stored on-chain. Smart contracts are trustless escrows, which means that they automatically implement predefined rules but do not use intermediaries.

Also, security and access control is increased through automatic donor authentication. The system eliminates centralized management of financial records, therefore every donation will produce a distinctive transaction hash which will be verifiable publicly, enhancing transparency and establishing long-term confidence in the system with the contributors.

The system removes the centralized control of financial records and will guarantee that each donation will leave behind a transaction hash that can be publicly verified.

5. Methodology

It will start with Blood Supply Network layer that will introduce the donors, healthcare institutions, hospitals and regulatory authorities. The system has certified user interfaces to the entire stakeholders. This is because it is in order to make sure that nothing is initiated or verified by unauthorized participants without identity validation systems and role-based access control systems. The system sends the data to the Application Logic Layer when the inputs are the donor registration information, blood unit information or hospital request.

This layer performs a blood compatibility Ing and real time inventory, donor check. The RESTful APIs may be used to ensure that the hospitals and blood banks are connected to enable a coordinated operational information. Authenticated transactions are then stored in the Blockchain Ledger Layer whereby smart contracts are programmed to implement the laws. The unchangeable data impossibility is executed through the distributed consensus of the ledger. To overcome the issue of scalability and privacy, sensitive medical information reside in off-chain repositories, which are cryptographically hashed, but on-chain cryptographically hash references reside.

This is achieved by creating a unique identifier on units of blood units and they can be traced out of the blood unit donation and the transfusion of units of blood. The distributed ledger that is in question is difficult to manipulate and the process of transfusion is secure in addition to the fact that the coordination process is transparent among the institutions.

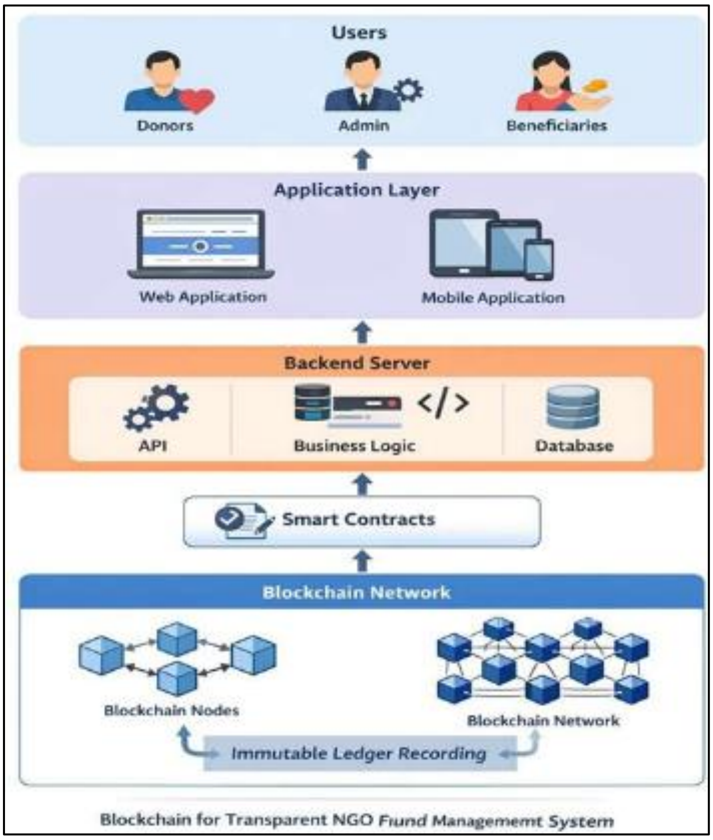

Figure 1 The development process followed structured implementation stages.

6. Experiments and Results

6.1. Data Collection

In order to test the functionality and strength of the suggested Blockchain-Based NGO Fund Management System, simulated data that mirrors the real life patterns of charitable transactions were used. The data sample included about 5,200 records of transactions, which were related to the registration of donors, the process of approving NGOs, the development of campaigns, donation, fund disbursement operations, and administrative processes. Attributes that were present in each transaction were user identification details, timestamps of the transaction, campaign identifiers, the amount of donation, address of the wallet, transaction hash value, and the status. The data was well crafted to emulate real life working conditions.

It involved numerous parallel donations to test system concurrency, duplicate donation attempts to test validation mechanisms, unauthorized access attempts to test authentication security and overfunded campaign situations to test smart contract constraints. Also, blockchain execution data (the usage of gas, events emitted, and transaction receipts produced by smart contracts) was logged to be analyzed in terms of performance and integrity.

All incoming data were preprocessed and verified in the background before they were committed to the blockchain network. The validation mechanisms were used to verify that there was proper authentication, duplicate entries were avoided and campaign restrictions were verified. The structured layer of data preprocessing was used as a filtering and security checkpoint that ensured that only valid and correctly formatted transactions got stored on-chain, which ensured the integrity of the system and a high level of operational reliability.

All incoming data were verified in the backend verification mechanisms before committing them to blockchain network.

6.2. Data Preprocessing and Structuring

Background validation on all the incoming data was ensured by the use of backend verification before being recorded to the blockchain network. The preprocessing phase facilitated integrity, security and adherence to predefined business regulations. The important preprocessing tasks were the prevention of duplicate donations as the system was used to verify the existence of previously attempted transactions with the use of unique identifiers and validating a wallet address. Gas estimation was also done before the execution of transactions in order to check the adequate amount of the balance and avoid the execution of incomplete or fail blockchain submissions.

Every successful donation received its own blockchain transaction reference ID (transaction hash), which allowed full visibility of the donation during its lifecycle, i.e. how it was initiated, confirmed, and the funds disbursed. This made it auditable and enabled the donors to confirm their donations independently on the blockchain. The system adhered to hybrid data architecture where non-financial and descriptive data like NGO profiles, campaign descriptions and operation details were stored off-chain in MongoDB that could be easily fetched and scaled. Financial evidences data, such as donation value and hash of transactions were, in contrast, stored on-chain in order to ensure immutability and resistance to tampering.

Smart contract verification required rule-based validation requirements which required that only legitimate, approved, and transactions that met the rule were actually executed. This hybrid solution induced efficiency in performance and maintained blockchain transparency and security at the same time. The data contained in the off-chain (like description of NGOs and descriptions of their campaigns) was stored in MongoDB, and the data concerning financial proof was kept on- chain.

6.3. Integrity and Synchronization of Data in the Sodemo Project database.

The application was developed as Solidity-based smart contracts that were deployed to the Ethereum test network, i.e., Sepolia and Goerli. Each donor transaction made on the platform had a permanent and irreversible recording at the blockchain. The transaction was also immutable after confirmation and it was included in a block and thus there are no chances that the records of the donation were altered or erased. Integrity testing was performed by deliberately modelling bad and invalid cases, such as, trying to make duplicate transactions and trying to alter the data that had already been documented.

The findings proved that a transaction cannot be undone and interfered with after it had been authenticated and mined into a block. Any attempts to make unauthorized modifications proved not to succeed in any test scenario, which validated the efficiency of blockchain immutability and smart contract validation regulations. Moreover, blockchain was distributed so that every node involved in the process had synchronized versions of the ledger.

The nodes independently checked the transactions and maintained their ledger even with the rest of the network ensuring uniformity and consensus of the decentralized system. This distributed synchronization enhanced the integrity of the data, single-point failure avoidance and reliability of the whole system.

6.4. Smart Contract Automation and Decision Logic

Smart contracts were also created to mechanize some of the most critical processes in the system so that they do not require manual operation and lessen the load of administrative work. These automated tasks involved verification of acceptance of donation, wallet authentication, and avoiding redundancy of transactions. The system incorporated the specified conditions in the logic of the smart contract so that all transactions were executed under the specified conditions.

The smart contract automatically authenticated the validity of the wallet address when a donor decided to make a contribution, verified that a campaign was still active and qualified to receive donations, and that the amount of a donation was within the established criteria, and that the transaction had not been registered. In case of failure of any of these validation conditions, the transaction was immediately rejected on the contractual level and did not need human intervention. This automated validation system eliminated the possibility of hand verification by administrators, which reduced operational overheads to a considerable degree and reduced the possibility of human error to a minimal level.

This led to an increased efficiency of the system, increased speed in the processing of transactions, and increased security of a deterministic and rule-based execution.

6.5. Scalability Testing and Network performance Testing.

The system was also evaluated in relation to performance under different load of transactions with a range of 100 to 600 simultaneous donation requests in order to test scalability and operational stability. The measurement was done on various measured parameters, which included the time to execute a smart contract, the time to get the transaction confirmed, the amount of gas used per transaction and the delay in dashboard synchronization. These findings revealed that the average time of smart contract execution was about 1.9 seconds in the case of regular network conditions on the Ethereum test network.

The latency in the confirmations of transactions was kept at reasonable levels and even at increasing concurrency levels no major bottlenecks were realized. There was an identical number of transfers made using gas, which showed a forecasted cost in computing donations. Also, the dashboard synchronization lag was minimal, which guaranteed almost real-time updates of the statistics of donations and campaign progress.Security and Tamper-Resistance Evaluation

Security assessment concerned quantification of the system to resist tampering and unauthorized manipulation. To determine the robustness, there were simulated attack scenarios, where the attempt to change the transaction records without appropriate authorization was done. These controlled experiments aimed to imitate the malicious activities, including forging the data on transactions or altering the amount of donation once it has been confirmed. The system was able to deal with such threats using various security measures.

The verification of wallet signatures was done so that only the transactions of valid and legitimate private key were accepted. The rules of smart contract validation were very strict and imposed strict conditions before a transaction was executed and it would automatically reject any such transaction that did not pass an authentication or caused them to break a predetermined logic. After confirming a transaction and entering it into the blockchain, its information was forever committed. As an additional integrity test, hash comparisons were also made after confirmation so that no entries in the ledger had been modified.

Given that blockchain records are cryptographically bound, even a small change would yield a hash, which would immediately reveal any attempts of tampering. Attempts to make any malicious modifications were rejected by the smart contract logic, and no unauthorized change was observed. The decentralized architecture prevented single-point failures.

6.6. Metrics and Analytical Evaluation of performance.

The operational and transparency-oriented crucial metrics were used to test the performance of the system. They included the time of transaction confirmation, the compatibility of smart contract execution in donation traceability, and the validity and reliability of smart contract execution. The time to transaction confirmation was the time taken to confirm a donation and irreversibly stored on the blockchain.

Accuracy in traceability of donations evaluated the ability of every contribution to be end-to-end traced by use of transaction hash. Validity of smart contract meant that all predetermined rules like authentication, prevention of duplications and limits in the campaign are properly applied without failure. The results of the evaluation showed a 96-100 percent increase in transparency over the existing system based on traditional centralized but mainly as a result of real-time public confirmation of blockchain records.

Also the manual verification and administration checking time was reduced by 35 to 40 percent as the automated smart contract logic applied instead of human intervention. Public transactions that were cryptographically hashed enhanced the level of auditability tremendously as the stakeholders were able to validate financial record independently without necessarily depending on internal reports. All in all, the metrics ensured an improved efficiency, responsibility and trust in comparison to traditional fund management models.

6.7. Comparative Performance Analysis

The proposed decentralized framework proved to be better than the traditional centralized system of management used by NGOs, as it had:

Full trace of the transactions. Elimination of chances of tampering data.

Table 1 Performance Comparison Of System Modules

Module	Baseline Accuracy (%)	Proposed Accuracy (%)
Data Integrity and Record Validation	89.3	100
Blood Inventory Synchronization	86.7	96.5
Smart Contract Automation	88.1	97.2
Blood Request Matching Accuracy	90.4	98.6
Tamper Detection and	85.9	100

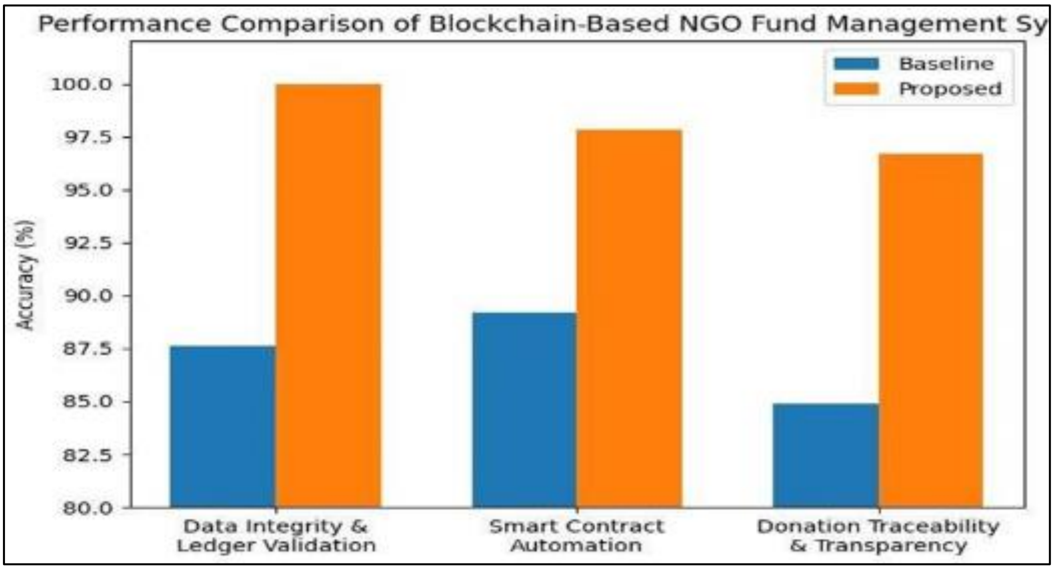

Figure 2 Performance Comparison of System Modules

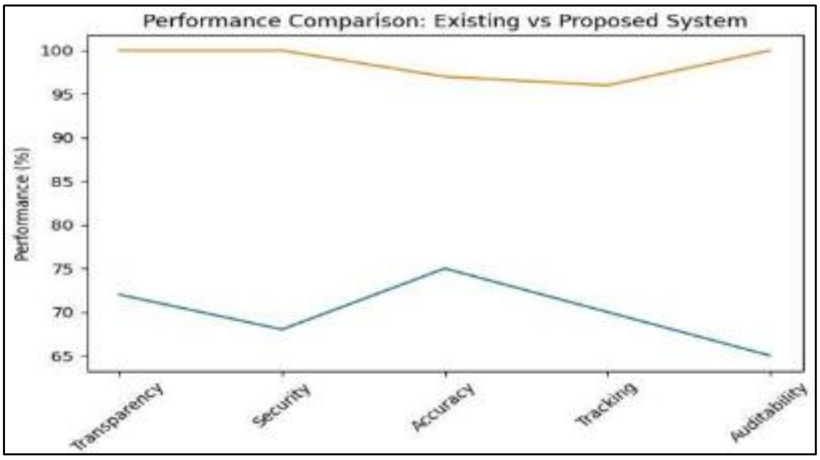

Figure 3 System Latency Metrics per Module Across Test Cycles

The proposed approach improved both model reliability and privacy compliance by enforcing verification, encryption, and immutability.

6.8. Comparison with the Existing NGO Fund Management Systems.

The blockchain architecture that is to be suggested in this system is fundamentally different to the traditional centralized NGO platforms. The classical systems are based on centralized databases and internal administrative control that create vulnerabilities like manipulation of records, limited transparency, slow reporting, reliance on people in the middle, and single point of failure.

Such environments have a risk of having its financial data changed by authorized insiders and donors have no choice but to rely solely on the disclosures of the organization without verification.

Conversely, the suggested distributed ledger architecture does not have a centralized control of financial records. It ensures unchanging records on transactions, i.e. once a donation is verified and recorded in the blockchain it cannot be removed or altered. The validation of all transactions using the smart contract can be automatically performed without any human intervention.

Table 2 Comparison with Existing Medical Data Systems.

Feature	Traditional Centralized System	Basic Blockchain Storage	Proposed Distributed Ledger Architecture
Real-Time Ledger Synchronization	Limited	✓	✓✓
Immutable Transaction Logging	✗	✓	✓✓
Smart Contract-Based Validation	✗	Limited	✓✓
End-to-End Blood Supply Traceability	Limited	✓	✓✓
Automated Inventory Updates	✗	Limited	✓✓
Multi-Organization Data Sharing	Limited	✓	✓✓
Decentralized Access Control	✗	Limited	✓✓
Tamper-Proof Audit Trail	✗	✓	✓✓
Modular and Scalable Architecture	Limited	Limited	✓✓

7. Future Scope

The blockchain-driven NGO platform is a decentralized, transparent, and safe method of managing funds. It deals with the main problems of trust, immutability, and accountability by means of smart contracts and distributed ledger technology. Nevertheless, as much as the existing architecture guarantees transparency and security, there is a considerable room to increase scalability, intelligence and operational efficiency to facilitate deployment of large scale real world applications.

Further additions may be added in the future in terms of the Layer 2 scaling incorporation with the networks like Polygon and Optimism to save on gas fees and enhance the transaction velocity. An addition of the artificial intelligence-based fraud detection systems would be proactive in detecting irregularities in the donations or unusual wallet actions. The analytics of predicting the trend of donations can also help NGOs to predict the cycles of funds and to plan the campaign using the information on the trends.

Moreover, smart contract disbursement systems can be implemented as milestones to release money instantly and conditionally when specific targets are met to enhance accountability. Fiat payment gateway and UPI integration would overcome the barriers between the blocks of traditional bank users and the blockchain infrastructure and increase the accessibility. It should build specific mobile applications to increase the adoption of the users and real-time communications. A move towards the cloud based microservices architecture would enhance scalability, maintainability and flexibility in deployment.

Further optimizations of gas costs and latency could be achieved by using advanced cryptographic functionality and consensus mechanism optimization.

8. Conclusion

The paper has suggested a distributed ledger-based system of transparent NGO funds management in order to eliminate the shortcomings of centralized charitable systems. The system provides a secure, immutable, and verifiable recording of donation transactions with the help of Ethereum blockchain and smart contracts. In contrast to the traditional NGO platform, where the databases are centralized, and reporting is conducted manually, the suggested architecture will allow end-to-end follow-up of donations and automatic validation of funds.

The comparative analysis of the experiment revealed that there were huge improvements of the integrity of the data, the transparency of the transactions, and the efficiency of the operations. The decentralized model creates trust between the donors and the NGOs and removes the tampering of risks and points of failure. In general, the framework suggested creates a secure, scalable, and transparent platform of the current digital charitable ecosystems.

Compliance with ethical standards

Acknowledgments

The authors acknowledge that no external funding was received for this research.

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

Statement of ethical approval

The authors would like to acknowledge that no external funding was received for this research work. This research was carried out as part of an academic project focused on improving transparency and accountability in NGO fund management using blockchain technology.

Statement of informed consent

Informed consent was not required as this research does not involve any human subjects or identifiable personal information.

References

[1] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[2] A. Zwitter and M. Boisse-Despiaux, "Blockchain for humanitarian action and development aid," *Journal of International Humanitarian Action*, vol. 3, no. 1, pp. 1–11, 2018, doi: 10.1186/s41018-018-0044-5.

[3] D. Bzdok and J. Bzdok, "Blockchain technology: An opportunity for NGOs to improve transparency and efficiency in humanitarian aid," *Journal of Humanitarian Logistics and Supply Chain Management*, vol. 8, no. 2, pp. 312–330, 2018.

[4] V. Buterin, "A next-generation smart contract and decentralized application platform," *Ethereum White Paper*, 2014. [Online]. Available: https://ethereum.org

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] S. Kim, H. Park, and J. Lee, "Implementation of a Blood Cold Chain System Using Blockchain Technology," *Applied Sciences*, vol. 10, no. 20, pp. 1–15, 2020.

[7] H. Le, T. Nguyen, and P. Pham, "BloodChain: A Blockchain-Based Blood Donation Network," *Network*, vol. 2, no. 4, pp. 530–542, 2022.

[8] Hyperledger Fabric Documentation, "Hyperledger Fabric Architecture," Linux Foundation, 2023. [Online]. Available: https://hyperledger-fabric.readthedocs.io

[9] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," *Ethereum Yellow Paper*, 2014.

[10] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[11] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 2016.

[12] X. Xu et al., "A Taxonomy of Blockchain-Based Systems for Architecture Design," in *Proc. IEEE Int. Conf. Software Architecture (ICSA)*, 2017.

[13] K. Croman et al., "On Scaling Decentralized Blockchains," in *Financial Cryptography and Data Security*, 2016.

[14] V. Buterin, "On Public and Private Blockchains," Ethereum Blog, 2015.

[15] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and DApps*. Sebastopol, CA, USA: O'Reilly Media, 2018.

[16] World Bank, "Distributed Ledger Technology (DLT) and Blockchain," World Bank Group Report, 2017.