UDC 004.75:004.056:364.04

Ya. I. SHEVCHUK, N. B. MELNYK, T. O. MUKHA
Lviv Polytechnic National University

OPTIMIZATION OF CHARITABLE DONATION TRANSPARENCY MECHANISMS USING SMART CONTRACT TECHNOLOGY

The article provides a comprehensive study of mechanisms for increasing the transparency of charitable activities using distributed ledger technologies. The relevance of the work is determined by the rapid growth of the charity sector in Ukraine and the need to overcome the trust crisis caused by cases of misappropriation of funds. Technical shortcomings of traditional centralized platforms were identified, specifically the vulnerability of relational databases to manipulation of transaction records. The transition to the «algorithmic trust» paradigm, where transparency is guaranteed by immutable program code, is justified.

A conceptual model of an information system built on a hybrid architecture is proposed. It combines traditional web technologies for managing non-critical data (interfaces, fund profiles) with a financial core on the Ethereum network. The choice of the Ethereum ecosystem is justified by its high reliability and the Solidity language's powerful capabilities for implementing complex financial algorithms. The conditional escrow mechanism implemented in the smart contract logic is the system's key instrument. A developed sequence diagram is described that models the donation lifecycle: from locking assets in the contract balance to the step-by-step release of funds after confirming the completion of specific project milestones.

The software structure of the smart contract, including the donate, verifyAndReleaseFunds, and refund functions, is analyzed in detail. The automatic refund function is considered a tool for protecting donor rights if the fund fails to meet its obligations. Significant attention is paid to cybersecurity issues: the use of access modifiers and the Checks-Effects-Interactions pattern to protect against Reentrancy attacks. To solve the problem of storing reporting documentation, integration with the decentralized IPFS system is proposed. The article describes the mechanism for recording unique file hashes (CIDs) on the blockchain, ensuring public accountability without overloading the network. The designed model allows each donor to track a donation's path from their wallet to the final beneficiary, based on mathematically proven facts.

Keywords: *charity, transparency, blockchain, smart contract, Ethereum, Solidity, escrow, IPFS.*

Я. І. ШЕВЧУК, Н. Б. МЕЛЬНИК, Т. О. МУХА
Національний університет «Львівська політехніка»

ОПТИМІЗАЦІЯ МЕХАНІЗМІВ ПРОЗОРОСТІ БЛАГОДІЙНИХ ВНЕСКІВ ІЗ ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ SMART CONTRACTS

У статті проведено комплексне дослідження механізмів підвищення прозорості благодійної діяльності за допомогою технологій розподіленого реєстру. Актуальність роботи зумовлена стрімким зростанням сектору благодійності в Україні та необхідністю подолання кризи довіри до фондів через випадки нецільового використання коштів. Виявлено технічні недоліки традиційних централізованих платформ, зокрема вразливість реляційних баз даних до маніпуляцій із записами транзакцій. Обґрунтовано перехід до парадигми «алгоритмічної довіри», де прозорість гарантується незмінним програмним кодом.

Запропоновано концептуальну модель інформаційної системи, побудовану на гібридній архітектурі. Вона поєднує традиційні вебтехнології для управління некритичними даними (інтерфейс, профілі фондів) та фінансове ядро на базі мережі Ethereum. Вибір екосистеми Ethereum обґрунтовано її високою надійністю та потужними можливостями мови Solidity для реалізації складних фінансових алгоритмів. Ключовим інструментом системи визначено механізм умовного депонування (escrow), реалізований у логіці смартконтрактів. Описано розроблену діаграму послідовності, яка моделює життєвий цикл пожертви: від блокування активів на балансі контракту до поетапного вивільнення коштів після підтвердження виконання конкретних етапів проєкту (milestones).

Детально проаналізовано програмну структуру смартконтракту, що включає функції donate, verifyAndReleaseFunds та refund. Функція автоматичного повернення коштів розглядається як інструмент захисту прав донорів у разі невиконання фондом своїх зобов'язань. Значну увагу приділено питанням кібербезпеки: застосуванню модифікаторів доступу та патерну Checks-Effects-Interactions для захисту від атак повторного входу (Reentrancy attacks). Для вирішення проблеми зберігання звітної документації запропоновано інтеграцію з децентралізованою системою IPFS. У статті описано механізм фіксації унікальних хеш-ідентифікаторів файлів (CID) у блокчейні, що забезпечує публічну підзвітність без надмірного навантаження на мережу. Спроєктована модель дозволяє кожному донору відстежувати шлях пожертви від власного гаманця до кінцевого бенефіціара на основі математично доведених фактів.

Ключові слова: *благодійність, прозорість, блокчейн, смартконтракт, Ethereum, Solidity, умовне депонування, IPFS.*

https://doi.org/10.32782/mathematical-modelling/2026-9-1-42 ISSN 2618-0332 (print), 2618-0340 (online)

Problem statement

Today, charitable and regular donations have become common practices among most Ukrainians. This enables the rapid collection of necessary funds and a timely response to any emerging challenges. According to the annual CAF World Giving Index [1], which is based on three indicators – the volume of donations, volunteering for non-profit organizations, and the willingness to help a stranger – Ukraine moved from 103rd to 7th place between 2014 and 2024 [2]. In 2023, the country even ranked second globally, and as of December, there were approximately 20,000 charitable organizations. Since the start of the full-scale war, their number has increased by 74 % [3].

Transparency is one of the primary obstacles charitable organizations face. While current legislation requires regular reporting to state authorities, many individuals also want to know exactly how their contributions are used. These concerns are not groundless, as numerous organizations have been accused of misappropriating funds. Furthermore, most donation platforms rely on relational databases to store transactions, which allows potential attackers to alter donation amounts or delete transaction records.

To verify the proper use of funds, charitable organizations may undergo audits; however, there is no legal requirement to conduct them regularly. This process can be delayed for weeks or even months due to the involvement of third-party personnel and the manual verification of bank statements.

The subject of this study is the tracking of charitable financial transactions using blockchain technology, which ensures an immutable record of all operations and enables real-time monitoring. If donors can see exactly how their money is spent, it will enhance trust in charitable activities, encouraging more people to donate without fear of misuse of funds [4]. Transparency must become the norm, not the exception.

Analysis of recent studies and publications

Active global research confirms that blockchain technology is the optimal response to the current crisis of trust in foundations caused by operational opacity, bridging the gap between scientific interest and practical implementation. The current stage of information systems development in the field of charity is characterized by a gradual transition away from traditional models built on «blind trust» in intermediaries. Instead, there is a shift toward an algorithmic trust paradigm. Under this approach, the security of each donation and the transparency of its use are guaranteed directly by the immutable smart contract code, which mathematically prevents any hidden manipulation of assets.

Study [5] explains that traditional financial reports of charitable foundations are often ineffective because they are submitted only once a year and contain only general figures that are difficult to verify. Instead, researchers suggest using blockchain to move toward a model in which the path of each individual donation can be tracked in real time. Smart contracts serve as a key tool here, enabling a «self-commitment» mechanism for the foundation: funds are effectively «frozen» in the system and transferred to the recipient only after the foundation provides digital evidence of having achieved a specific goal.

Another important aspect of blockchain implementation is discussed in the study [6], which focuses on protecting the personal data of donors and beneficiaries. They propose a combined architecture in which confidential information is stored in the distributed IPFS file system, while only its hash values and access rules are recorded on the blockchain. This approach addresses the problem of excessive network load and ensures that detailed information about contributions is available only to verified participants. This enables a system in which transaction transparency does not violate users' right to privacy, a mandatory requirement for modern charitable web platforms.

Study [7] directly addresses the loss of trust in charitable foundations due to opaque fund distribution and potential duplication of recipient records. The article proposes a decentralized system architecture based on the Ethereum platform, where smart contracts play a pivotal role in transaction management. These are viewed as a set of predefined rules that automatically initiate fund transfers

https://doi.org/10.32782/mathematical-modelling/2026-9-1-42 ISSN 2618-0332 (print), 2618-0340 (online)

upon fulfillment of specified conditions, completely eliminating the need for intermediaries and reducing transaction costs.

The scale of scientific interest in blockchain use in charitable activities from 2016 to 2024 is illustrated in [8]. Its authors confirm that ensuring transparency and implementing smart contracts have become dominant trends in modern research on charitable ecosystems. At the same time, this work identifies a significant issue: a massive gap between theoretical enthusiasm for blockchain and its practical application. It was found that scientists and developers still lack a clear understanding of the mechanisms for integrating smart contracts into daily donation management processes.

A practical approach to bridging the gap between theory and implementation is proposed in [9], which considers a hybrid architecture for a charitable web platform. Recognizing the technical limitations of fully decentralized systems, the researchers suggest combining smart contracts on the Ethereum network with traditional relational databases and REST APIs to enable convenient integration with existing foundation systems. This approach allows for optimizing network load and ensuring high processing speeds for client requests. Furthermore, the work implements a reliable transaction-tracking system: each payment is assigned a unique identifier, through which a donor can monitor the targeted use of their funds at every stage of their movement in real time.

The direct practical implementation of similar mechanisms is demonstrated in the study [10], where the authors developed a full-scale decentralized application for donation management. The main feature of this system is the implementation of a collective expense control algorithm. Logic was implemented programmatically so that the fundraiser does not gain direct access to the accumulated funds. To withdraw assets, they must submit a specific transaction request. The smart contract unlocks the funds and transfers them to the final recipient only after this request is approved by a majority of donors whose contributions exceed a system-defined minimum. This approach prevents the misappropriation of donations and ensures full accountability for foundations.

A new direction for the development of decentralized charitable platforms is explored in article [11], which proposes moving beyond purely cryptographic solutions and integrating blockchain with artificial intelligence algorithms. Such symbiosis would allow for deep analysis of donation usage patterns and the generation of real-time analytical reports, significantly increasing the efficiency of resource allocation.

The analysis of publications indicates that, despite active blockchain research in the charity sector, many solutions remain at the level of theoretical concepts or do not meet the needs of modern foundations. The task of creating a comprehensive system that effectively combines the security of decentralized smart contracts with the convenience of traditional web applications remains relevant.

Purpose of the research

The conceptual design of an information system for charitable foundation management and the modeling of smart contract execution logic that guarantees transparent donation distribution and protects them from abuse during collection and disbursement.

Presentation of the main research material

To address transparency issues in the charity sector, blockchain technology appears to be the most promising approach. Traditionally, databases are controlled by a single administrator, which creates risks of unauthorized interference or data loss. In contrast, blockchain is a distributed ledger stored simultaneously across numerous network nodes. Each new transaction, such as a charitable donation, is grouped with others into a block that is cryptographically linked to the previous one. This forms an unbreakable chain, making it impossible to change or delete information about past donations without altering all subsequent blocks, thereby making the system highly tamper-resistant. In the context of charity, this means every donor receives a guarantee that their payment history is immutable [12]. This decentralized structure eliminates any single point of failure, thereby significantly increasing the overall resilience of the charity platform's infrastructure against external attacks.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-42 ISSN 2618-0332 (print), 2618-0340 (online)

However, the mere recording of transactions does not solve the problem of the targeted distribution of accumulated funds. This is precisely what smart contracts are used for. A smart contract is a computer program that is hosted and executed directly on the blockchain. It operates on an "if-then" principle and automatically executes predefined conditions without third-party intermediaries. Consequently, the execution of financial agreements becomes entirely independent of human discretion, ensuring strict adherence to the initial terms of the donation. The code of such a contract is open for audit, allowing any user to verify its operational logic even before making a donation.

Currently, the Ethereum network is the most optimal environment for deploying such smart contracts. Unlike early blockchain systems designed solely to record cryptocurrency transfers, Ethereum was designed from the outset as a platform for building decentralized applications. Its primary advantage is the built-in virtual machine, which allows for the execution of program code of any complexity. To write smart contracts within this ecosystem, a specialized object-oriented programming language called Solidity is used [13]. The choice of this specific network for the conceptual design of a charity platform is justified by its high reliability, robust infrastructure, and established standards for creating secure financial algorithms, which are critical for processing donations.

Given the technical characteristics of blockchain, the conceptual design of a modern charitable platform requires a hybrid architecture. Fully decentralized applications often face scalability issues and the high cost of storing large volumes of data. Therefore, the proposed model involves distributing responsibilities between traditional web technologies and the blockchain. The client-side of the platform provides the user interface and integration with crypto wallets for direct donor interaction with the smart contract. The server-side is responsible for managing non-critical data, such as foundation profiles, text descriptions of charitable campaigns, and caching transaction history for rapid display. The financial core of the system – specifically the smart contracts written in Solidity – operates in isolation within the blockchain network and exclusively manages financial flows.

The primary tool for ensuring transparency in the proposed system is the escrow mechanism embedded in the smart contract logic. The use of a hybrid architecture enables effective segregation of the system's computational resources. While the web server handles the processing of user requests and the display of content, the blockchain serves as an unrivaled guarantor of the immutability of financial rules and the transparency of operations. This is particularly crucial for coordinating complex processes in a decentralized environment involving multiple parties with varying levels of data access. Modeling such interactions requires a clear definition of the information flows passing through all layers of the platform. To visualize the interaction among users, the web platform, and the blockchain, a sequence diagram was developed (Fig. 1).

The donation lifecycle is as follows: when creating a new fundraising campaign, the initiator specifies not only the target amount but also breaks the project down into specific milestones. When a donor makes a transfer, the funds do not go directly to the foundation's account; instead, they are locked in the balance of the smart contract associated with that specific campaign.

The foundation does not have the physical ability to withdraw accumulated funds immediately. To receive the first tranche, the organizer must fulfill the stated obligations and provide appropriate confirmations. The smart contract unlocks the next portion of funding only after the system records the successful completion of the previous stage. In the event that the collection does not reach the minimum required amount within the set timeframe, or if the foundation violates reporting conditions, the smart contract automatically initiates a refund function, transferring the donations back to the donors' wallets. This algorithmic approach completely eliminates the human factor from the financial control process, guaranteeing the targeted use of every donation.

The smart contract architecture provides for storing key fundraising parameters as data structures (structs). These include: the target fundraising amount, the address of the initiator's (foundation's) crypto wallet, time constraints (deadlines), and an array of stages indicating the required amount

https://doi.org/10.32782/mathematical-modelling/2026-9-1-42 ISSN 2618-0332 (print), 2618-0340 (online)

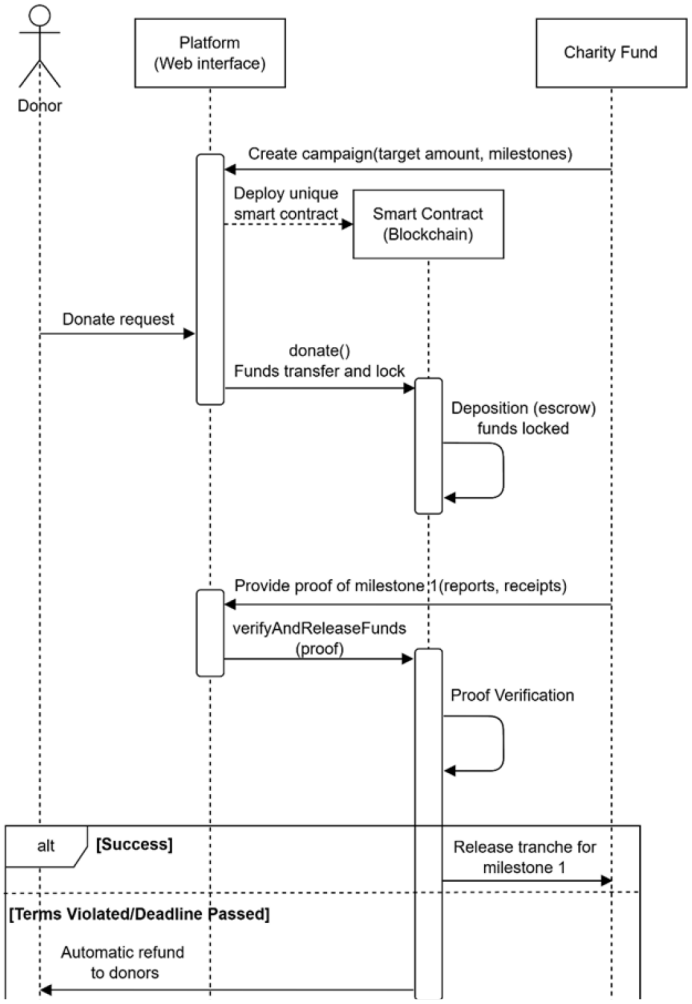

Fig. 1. Sequence diagram of the lifecycle using a smart contract

and execution status for each. Furthermore, the smart contract maintains an internal donor registry (mapping) that records each sender's address and donation amount, which is critical for enabling algorithmic refunds. The software implementation of the described structure in Solidity is as follows:

```
struct Milestone {
 uint256 targetAmount; // Milestone target amount
 bool isCompleted; // Execution status
 string reportCID; // IPFS report hash
}
struct Campaign {
 uint256 totalTarget; // Total target amount
 address initiator; // Foundation's wallet
 uint256 deadline; // Time constraint
 Milestone[] milestones; // Array of stages
}
mapping(address => uint256) public donorRegistry; // Donor registry
```

Financial flow management is carried out through three primary functions:

– Fund receiving function (donate): Allows for accepting transactions in cryptocurrency. When called, the contract verifies whether the fundraising deadline has passed and if the target amount has

https://doi.org/10.32782/mathematical-modelling/2026-9-1-42 ISSN 2618-0332 (print), 2618-0340 (online)

been exceeded. Funds are automatically credited to the smart contract's own balance, and a record of the contribution is added to the donor registry.

– Tranche unlocking function (verifyAndReleaseFunds): Responsible for transferring funds to the charitable foundation's wallet. It can only be invoked after verification that the current stage is complete. The function's logic checks for confirmation (e.g., a cryptographic signature from the platform administrator), then releases the amount corresponding to the cost of the completed stage.

– Guaranteed refund function (refund): Activated in case of a violation of fundraising conditions. For example, if the target amount is not collected by the specified date, or if the foundation fails to confirm the targeted use of the previous tranche. This function allows each donor to contact the smart contract and securely retrieve their initial contribution.

Such a software structure minimizes fraud risk because the rules for fund distribution are strictly enforced within the blockchain's state machine and cannot be arbitrarily changed or ignored by any party after the contract is deployed on the network.

Special attention is paid in the system's conceptual design to cybersecurity and the segregation of access rights. In the Solidity programming language, special modifiers are used to protect smart contract functions. For instance, the tranche unlocking function (verifyAndReleaseFunds) is protected by a modifier that allows its invocation exclusively by a verified platform administrator or a decentralized oracle after the verification of the reporting documentation. This technically precludes unauthorized withdrawal of funds by the fundraising initiator. On its part, the refund function is configured so that each donor can initiate a refund for only their own contribution recorded in the registry.

Furthermore, implementing protection for financial logic against common network vulnerabilities, particularly Reentrancy attacks, is critically important. To achieve this, the Checks-Effects-Interactions design pattern is applied in the smart contract architecture. When the refund function is called, the smart contract first checks the user's balance, then updates the balance to zero in the internal registry, and only then performs the actual cryptocurrency transfer. This eliminates the possibility of an attacker repeatedly calling the withdrawal function before the balance is updated.

An additional level of reliability is provided by the platform's hybrid nature. Since financial flow management is completely isolated within the decentralized Ethereum network, even in the event of a hypothetical compromise of the centralized web database server containing project descriptions, attackers will not have access to accumulated donations. The smart contract will continue to function autonomously according to the embedded immutable algorithm, maintaining 100 % integrity of donor assets.

Another important aspect of optimizing transparency mechanisms is the issue of storing reporting documentation (receipts, certificates of completion, photographs). Storing such voluminous files directly on the blockchain is technically unfeasible and economically impractical due to the high cost of transaction execution. At the same time, relying solely on traditional centralized servers to store reports creates the risk of report forgery or irreversible deletion after funds have already been unlocked.

To comprehensively address this issue, it is advisable to integrate the IPFS (InterPlanetary File System) decentralized file system into the proposed architecture. At each stage of verification, the charitable foundation uploads reporting documents to the IPFS network. The system generates a unique cryptographic file hash (CID) that is mathematically dependent on the file's content. Any change, even to a single pixel in a receipt photo, will result in a completely new hash. This unique identifier is passed to the smart contract upon invocation of the tranche-unlocking function and is permanently recorded on the blockchain [6].

This approach ensures absolute public accountability without overloading the Ethereum network. Any user or independent auditor, using public block explorers, can track the movement of funds from their wallet to the final beneficiary. Furthermore, using the hash stored in the transaction, anyone can retrieve the immutable original documents from IPFS on which the payment was based. Thus, algorithmic transparency is achieved not only at the level of financial transfers but also in documentary evidence of the targeted use of every donation.

https://doi.org/10.32782/mathematical-modelling/2026-9-1-42 ISSN 2618-0332 (print), 2618-0340 (online)

Conclusions

The article proposes a conceptual model of an information system for charitable foundation management that addresses issues of trust and transparency through blockchain technology. The feasibility of employing a hybrid architecture is justified, where traditional web technologies provide convenient user interaction and large-scale data storage, while smart contracts on the Ethereum network serve as an independent financial core.

The modeled smart contract execution logic is based on an escrow mechanism and phased project financing. The proposed algorithm eliminates the human factor from the donation distribution process, ensuring that funds are transferred to the charitable foundation only after evidence of the targeted use of the previous tranche is provided. The implementation of an automated refund function creates an unprecedented level of protection for donor rights.

The addressed cybersecurity issues, specifically the use of access modifiers and protection patterns against network attacks, confirm the high reliability of the proposed architecture. The conceptual model described serves as a solid foundation for the practical development and implementation of a decentralized web platform for managing charitable activities, facilitating the transition from a "blind trust" model to algorithmic transparency.

Bibliography

1. World Giving Index 2024: Global Trends in Generosity / Charities Aid Foundation. London : CAF, 2024. 20 p. URL: https://www.cafonline.org/docs/default-source/inside-giving/wgi/wgi_2024_report.pdf (дата звернення: 29.03.2026).
2. Прохода К. Запит на прозорість: як мають звітувати благодійні організації. *УНІАН*. 2026. URL: https://www.unian.ua/society/zapit-na-prozorist-yak-mayut-zvituvati-blagodiyni-organizaciji-13317063.html (дата звернення: 29.03.2026).
3. Благодійний бум: кількість благодійних організацій зросла майже удвічі від початку повномасштабної війни. Опендатабот. URL: https://opendatabot.ua/analytics/non-profit-2023 (дата звернення: 29.03.2026).
4. Як блокчейн допомагає у благодійності. Binance Square. URL: https://www.binance.com/uk-UA/square/post/624096 (дата звернення: 29.03.2026)
5. Ostern N., Furneaux C., Rosemann M. Blockchain for Charity: Trust-Related Affordances in the Charity Sector. *Proceedings of the Thirty-first European Conference on Information Systems* (*ECIS'2023*) : Kristiansand, 05 November 2023. Kristiansand, Norway. 2023. P. 268. https://aisel.aisnet.org/ecis2023_rp/268?utm_source=aisel.aisnet.org%2Fecis2023_rp%2F268&utm_medium=PDF&utm_campaign=PDFCoverPages (дата звернення: 29.03.2026).
6. Deng L., Liu S., Xu H., Wang W., Yang W. Blockchain-Based Charitable Donation Privacy Protection Scheme. *Proceedings of the 2022 International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology (AIoTC 2022)*: Virtual Event, Fuzhou, 21–23 October 2022. Fuzhou, China. 2022. P. 76–85. URL: https://ceur-ws.org/Vol-3351/paper11.pdf (дата звернення: 29.03.2026).
7. Naiknavare O. S., Patil M. P., Chawate R. C., Borana A. B., Sonawane S. Blockchain based Transparent and Genuine Charity Application. *International Journal for Research in Applied Science and Engineering Technology*. 2022. Vol. 10. № 3. P. 1909–1915. DOI: https://doi.org/10.22214/ijraset.2022.41021
8. Mohd Anim N. A. H. B., Rahim N., Tajuddin N. I. I., Ahmad A., Ismail A. Smart Contracts, Cryptocurrencies, and Donation Systems: A Bibliometric Analysis of Blockchain in Charity. *Selangor Business Review*. 2025. Vol. 10. № 1. P. 16–38. URL: https://sbr.journals.unisel.edu.my/index.php/sbr/article/view/190/116 (дата звернення: 29.03.2026).

9. Hu Baokun, Li He. Research on Charity System Based on Blockchain. *IOP Conference Series: Materials Science and Engineering*. 2020. Vol. 768, № 7. 072020. DOI: https://doi.org/10.1088/1757-899X/768/7/072020
10. Negi R., Thomas B., Ghorpade P., Attiyil A., Melvin Y. I. J. Charity System using Blockchain Technology. *International Research Journal of Engineering and Technology* (*IRJET*). 2022. Vol. 09. № 04. P. 563. URL: https://www.irjet.net/archives/V9/i4/IRJET-V9I4100.pdf (дата звернення: 29.03.2026).
11. Sahithi M., Varsha R., Dhanya L., Nambiar P. V. M. A Blockchain Based Solution for Transparent Charity Donations. *International Journal of Engineering Research & Technology (IJERT)*. 2025. Vol. 14. № 05. DOI: https://doi.org/10.5281/zenodo.18106587
12. Yasir Mr., Ingale D. G. Blockchain for Transparent Charity Donations. *International Journal of Ingenious Research, Invention and Development* (*IJIRID*). 2024. Vol. 3. № 5. P. 445–448. DOI: https://doi.org/10.5281/zenodo.14137474
13. Patil P. D., Mhatre D. J., Gharat N. H., Tinsu J. Transparent Charity System using Smart Contracts on Ethereum using Blockchain. *International Journal for Research in Applied Science and Engineering Technology*. 2022. Vol. 10. № 4. P. 743–748. DOI: https://doi.org/10.22214/ijraset.2022.41339

References

1. Charities Aid Foundation. (2024). *World Giving Index 2024: Global trends in generosity*. Charities Aid Foundation. Retrieved from https://www.cafonline.org/docs/default-source/inside-giving/wgi/wgi_2024_report.pdf [in English].
2. Prokhoda, K. (2026, March 16). Zapyt na prozorist: yak maiut zvituvaty blahodiini orhanizatsii [Request for transparency: how charitable organizations should report]. *UNIAN*. Retrieved from https://www.unian.ua/society/zapit-na-prozorist-yak-mayut-zvituvati-blagodiyni-organizaciji-13317063.html [in Ukrainian].
3. Opendatabot. (2023). Blahodiinyi bum: kilkist blahodiinykh orhanizatsii zrosla maizhe udvichi vid pochatku povnomasshtabnoi viiny [Charity boom: the number of charitable organizations has almost doubled since the start of the full-scale war]. Retrieved from https://opendatabot.ua/analytics/non-profit-2023 [in Ukrainian].
4. Binance Square. (2023). Yak blokchein dopomahaie u blahodiinosti [How blockchain helps in charity]. Retrieved from https://www.binance.com/uk-UA/square/post/624096 [in Ukrainian].
5. Ostern, N., Furneaux, C., & Rosemann, M. (2023). Blockchain for charity: Trust-related affordances in the charity sector. *Proceedings of the Thirty-first European Conference on Information Systems* (*ECIS'2023*). Kristiansand, Norway. https://aisel.aisnet.org/ecis2023_rp/268?utm_source=aisel.aisnet.org%2Fecis2023_rp%2F268&utm_medium=PDF&utm_campaign=PDFCoverPages [in English].
6. Deng, L., Liu, S., Xu, H., Wang, W., & Yang, W. (2022). Blockchain-based charitable donation privacy protection scheme. *Proceedings of the 2022 International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology (AIoTC 2022*. Fuzhou, China. https://ceur-ws.org/Vol-3351/paper11.pdf [in English].
7. Naiknavare, O. S., Patil, M. P., Chawate, R. C., Borana, A. B., & Sonawane, S. (2022). Blockchain based Transparent and Genuine Charity Application. *International Journal for Research in Applied Science and Engineering Technology*, 10 (3), 1909-1915. DOI: https://doi.org/10.22214/ijraset.2022.41021 [in English].
8. Mohd Anim, N. A. H., Rahim, N., Tajuddin, N. I. I., Ahmad, A., & Ismail, A. (2025). Smart contracts, cryptocurrencies, and donation systems: A bibliometric analysis of blockchain in charity. *Selangor Business Review*, 10 (1), 16–38. Retrieved from https://sbr.journals.unisel.edu.my/index.php/sbr/article/view/190/116 [in English].

9. Hu, B., & Li, H. (2020). Research on charity system based on blockchain. *IOP Conference Series: Materials Science and Engineering*, 768 (7), 072020. DOI: https://doi.org/10.1088/1757-899X/768/7/072020 [in English].
10. Negi, R., Thomas, B., Ghorpade, P., Attiyil, A., & Melvin, Y. I. J. (2022). Charity System using Blockchain Technology. *International Research Journal of Engineering and Technology* (*IRJET*), 9 (4), 563–567. Retrieved from https://www.irjet.net/archives/V9/i4/IRJET-V9I4100.pdf [in English].
11. Sahithi, M., Varsha, R., Dhanya, L., & Nambiar, P. V. M. (2025). A blockchain based solution for transparent charity donations. *International Journal of Engineering Research & Technology* (*IJERT*), 14 (05). DOI: https://doi.org/10.5281/zenodo.18106587 [in English].
12. Yasir, Mr., & Ingale, D. G. (2024). Blockchain for transparent charity donations. *International Journal of Ingenious Research, Invention and Development* (*IJIRID*), 3 (5), 445–448. DOI: https://doi.org/10.5281/zenodo.14137474 [in English].
13. Patil, P. D., Mhatre, D. J., Gharat, N. H., & Tinsu, J. (2022). Transparent Charity System using Smart Contracts on Ethereum using Blockchain. *International Journal for Research in Applied Science and Engineering Technology*, 10 (4), 743–748. DOI: https://doi.org/10.22214/ijraset.2022.41339 [in English].

Shevchuk Yana Ivanivna – Undergraduate Student (Bachelor's level) at the Department of Software Engineering of the Lviv Polytechnic National University. E-mail: yana.shevchuk.pz.2022@lpnu.ua, ORCID: 0009-0003-5471-472X.

Melnyk Nataliia Bohdanivna – Candidate of Physical and Mathematical Sciences, Associate Professor at the Department of Software Engineering of the Lviv Polytechnic National University. E-mail: nataliia.b.melnyk@lpnu.ua, ORCID: 0000-0003-2337-2395.

Mukha Taras Orestovych – Candidate of Technical Sciences, Senior Lecturer at the Department of Software Engineering of the Lviv Polytechnic National University. E-mail: Taras.O.Mukha@lpnu.ua, ORCID: 0009-0000-1188-3580.

Шевчук Яна Іванівна – здобувач вищої освіти на першому (бакалаврському) рівні кафедри програмного забезпечення Національного університету «Львівська політехніка». E-mail: yana.shevchuk.pz.2022@lpnu.ua, ORCID: 0009-0003-5471-472X.

Мельник Наталія Богданівна – к.ф.-м.н., доцент кафедри програмного забезпечення Національного університету «Львівська політехніка». E-mail: nataliia.b.melnyk@lpnu.ua, ORCID: 0000-0003-2337-2395.

Муха Тарас Орестович – к.т.н., старший викладач кафедри програмного забезпечення Національного університету «Львівська політехніка». E-mail: taras.o.mukha@lpnu.ua, ORCID: 0009-0000-1188-3580.

Дата першого надходження статті до видання: 31.03.2026
Дата прийняття статті до друку після рецензування: 12.05.2026
Дата публікації (оприлюднення) статті: 01.07.2026