Donation Tracking System with Blockchain

Rana Dudu KABAK*, Taha UZ†, Prof. Dr. Ahmet SAYAR‡
Computer Engineering, Kocaeli University, Kocaeli, Turkey

***Abstract*—In this system, which we make with the smart contract on the blockchain, donors make their donations to a decentralized system, not to a person, and this system is transparently verified over the network and published publicly. The money collected in the contract is transferred to the people in need without being affected by the human factor through the receipt architecture created in the smart contract. The donation process is tracked in the system until the end user, thanks to the marking algorithm in the receipt. Users perform donation and donation tracking transactions by using the decentralized web application. The blockchain system has nodes such as donors, foundations, commercial companies, and needy people. To mention the information recorded in the distributed ledger in the blockchain network, such as the identity information of the donor, the amount of donation, the foundation/foundations he/she wants to donate, and donation rates are recorded. Regarding donations, information such as donation amounts and to which needy people these donations are sent are recorded. Detailed information on the subject is given in section I.**

***Keywords*—Blockchain, Ethereum, Binance Smart Chain, Donation Tracking, Smart Contract, DApp, Ethers, Contract ABI, BSCScan, EtherScan, Remix IDE, Wagmi, Donation**

I. Introduction

In large and small-scale donation events, it is generally planned to distribute the money collected in a foundation to those in need, and donors make their donations to the relevant aid organizations instead of transferring them directly to those in need. In this process, the transfer of money to the right people depends on the honesty and reliability of the foundation organizations. In this process, fraud and false documentation may result in donations not reaching the people in need. With this system on the blockchain, donors make their donations to a decentralized system, not to a person, and this system is transparently verified over the network (Ethereum, BSC) and published publicly.

Thanks to the money collected in the smart contract and the decentralized structure, donations are transferred directly to the people in need without being affected by the human factor with the receipt architecture created in the smart contract. Users follow the money transfer and follow-up transactions with the dApp on the web. They can follow the donation transaction carried out until the end user in the system, thanks to the marking algorithm in the receipt.

The components in the system, which we can call nodes, can be listed as donors, foundations, and commercial firms/needers. To explain the tasks of these nodes, donors are the nodes in the smart contract system on the blockchain and represent the donors. Individuals or organizations wishing to donate join the system through these nodes and make their donations. Foundation nodes are the nodes that collect, manage, and transfer donations to those in need. Foundation nodes direct donations according to the rules set in the smart contract and ensure the correct operation of the system. Finally, commercial firms/needy nodes represent the people who receive donations or need donations. The needy people register to the system on the blockchain to ensure that donations reach them and report their needs.

In this system, the necessary information is recorded in distributed ledgers by the blockchain logic. If we need to discuss the information recorded in distributed ledgers, we can first discuss donor information. Within the scope of donor information, information about the donor, such as the identity information of the donors, donation amounts, and the foundation to which the donation is made, is recorded. Regarding the donations, the amount of the donation and to which commercial organization/need holder the donation is directed are recorded in the distributed ledger.

In this study, basic information about blockchain and donation tracking systems is given in section II. In section III. similar studies, in section IV. open source technologies used in the study, in section V. detailed information about the architecture and infrastructure of the study is given, and the infrastructure of the related voucher system is explained in Figure 1. VI. and the last section presents the results obtained.

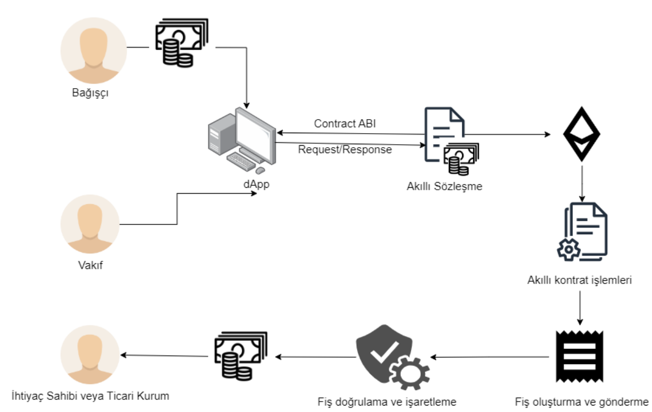

Fig. 1. Receipt System Infrastructure

II. Blockchain and Donation Tracking System

In this section of the article, blockchain technology, which is the primary technology used in the study, and the donation tracking system are mentioned.

A. Blockchain Technology

Blockchain technology is a system used as a distributed database that stores data transparently, immutably, and securely. It is a promising technology for solving many security-related problems and is becoming important in both the public and private sectors. This technology consists of groups of data, called blocks, linked together in a chained manner. Each block references the data of the previous block and is secured by cryptographic methods. Blockchain is decentralised, meaning data and transactions are shared and verified without central authority. Thanks to these features, blockchain is used in many areas, such as secure data sharing, resource tracking, and tracking systems.

Since the blockchain has a decentralized structure, it increases security and reliability. It offers a system where data is shared transparently and cryptographically verified in every transaction. This prevents data manipulation and ensures reliability. In addition, blockchain technology eliminates intermediaries and the execution of direct transactions, which reduces costs and speeds up transactions. Distributed data storage reduces the impact of failures or attacks that can occur at a single point [2]. Blockchain also provides traceability and transparency, improving the tracking of resources. All these advantages enable blockchain technology to provide effective and innovative solutions in many sectors.

B. Donation Tracking System

Within the smart contract, users interact to transfer funds from one electronic wallet to another. There are two functions that perform the transfer process. The first one is between the donor and the foundation/need holder, and the other one is between the foundation/need holder and the commercial firm. In the transfer function between the donor and the foundation, the nine-character code created for the transaction and the transaction information are kept in the receipt cutting logic, as well as the names of the users, identity information, wallet address, and donation amount. Between the foundation/need owners and commercial companies, if the amount in the additional receipt is spent by the foundation/need owner, variables that hold the wallet address and user names of the user from which user's money is spent are created.

The receipt of each transfer on the system is mutually stored on a variable that holds the users' receipts with a random code generated by the system. Here, foundations look at their receipts while transferring money to people in need, and the system creates a copy of these receipts. Here, if the foundations/needy people make any expenditure, it combines the amount in the receipts with the amount of money to be transferred. After the amount is equalized, the names of the donors are written on the receipt to be made by the foundation, the amount in the duplicate receipt is reset to zero, and the sign on the system that the money in this receipt has been donated is discarded. After this process passes through all condition states, the process is terminated by saving to the variable where the donors, foundation, and commercial company receipts are stored. In this way, all users affected by the transaction are notified, and donors can see to which institution or needy person how much money has been transferred by the foundation and how much money has reached the electronic wallets of the needy people.

TABLE I
User's Account Transfer History

Code	From	To	Donate Amount	Donaters
ASFN3N41G	RANA	AHBAP	0.20 BNB	-
DAS4454SW	AHBAP	MIGROS	0.25 BNB	TAHA[0.10] RANA[0.15]
LSY23Y4HS	AHBAP	MIGROS	0.05 BNB	TAHA[0.05]

III. Related Works

In this section, the relevant articles written as a result of the researches in the literature are analyzed, and the general frameworks of these articles are summarized.

When we examine the conference text published by Singh et al. [3] in this study, in the contract in this study, the wallet, approval, and ID information is obtained from the user, and the transfer transaction is carried out with the Ethereum network. The approach in this text is in token logic, and they use their tokens in exchange for currencies such as bnb and Ethereum. In this way, real money flow is provided by converting their currencies into currencies such as bnb or Ethereum. The user interface part of the transfer transactions on the back end was made using HTML, CSS, and React.js, and the user's wallet connection, mutual transfer confirmation, and transfer functions were connected to the web interface. With the help of the Web3 API in React.js, the user is informed about from whom to whom, when, and how much this transfer was made. The hash codes of these donation transactions are extracted from the table, and the transfer information is presented to the users. The difference between the study and the related study is that the token logic regarding the currency used is not followed. In the stock market style, the maths is turning, and it is not preferred due to the decrease and increase in the amount of the depreciation of the money in the hands of people in need.

In the paper published by Liu et al. [4], the Donation Tracing Blockchain model is proposed to make the donation process more open and transparent, and within this model, the Delegated Proof of Stake (DPoS) algorithm is proposed to prevent centralization and reduce the probability of malicious nodes being selected. This model uses the K-Means algorithm to pre-select the good nodes in the agent queue. Compared to Proof of Stake (PoS) and Proof of Work (PoW) algorithms, the DPoS consensus algorithm has the advantage of reducing the cost and time to reach consensus. The difference between this study and the related study is the consensus algorithm used.

The system in Ferwana's master's thesis [5] is designed for students to donate directly to students' wallets with the university's approval without a third-party organization. The donation to be made takes place within the framework of the rules provided by the university. These rules are included in the smart contract with the university's approval. The article recommends that the smart contract be optimized to get a large volume of data as a result of the project. The most crucial point of this article is that it eliminates the factors that create security vulnerabilities. To explain, indicating that the university accepts or rejects the donor request will prevent the possibility of a hacker or an unknown party entering this scope. In addition, possible delays in the donation delivery to the student may make the donor think that the donation has been lost. For this reason, the blockchain developed was reduced to private networks, the network traffic was reduced, and the transfer was made as fast as possible. The difference between the study and the related study is that the study provides a more general donation tracking system and a monitoring mechanism showing how charities spend donations.

The blood management system proposed in the conference paper published by Sadri et al. [6] is designed as a private and permissioned blockchain that only specific stakeholders can access. The main reason for choosing a private and permissioned blockchain in this study is to prevent public access to sensitive information such as donor and donation details. Blockchain brings more transparency to blood tracking, providing a reliable tracking mechanism. The basic design of the blockchain will also increase the system's security as it prevents unauthorized or illegal data modification. The proposed system uses Hyperledger Fabric as a private and authorized blockchain network. The difference between this and the related study is the type of blockchain network. Since the systems that need to be created for money transfer are already available in Ethereum, it was preferred.

The studies in the literature are generally based on donation tracking systems and blockchain integration and the use of this integration in different fields. However, one of the significant shortcomings of donation tracking systems is that there is no adequate explanation of how to provide information on where charities spend their donations. Unlike other studies, our work provides a tracking mechanism that shows how charities spend donations and transparently provides transfer information to donors. In the *I. Introduction*, we mention the proposed solutions that this paper contributes to the literature. These features are essential for increasing donor trust and enabling more effective management of donations.

IV. Utilized Technologies

In this section, a brief overview of the utilized technologies in the relevant study has been provided.

A. Blockchain Networks (Ethereum, Binance Smart Chain)

1) Ethereum: Ethereum, the primary technology used in the study, is the second most popular cryptocurrency after Bitcoin, with its unit Ether (ETH). Its market capitalization exceeds 210 billion American dollars. In the Ethereum network, snippets of code, called smart contracts, run decentralized on the blockchain. Thanks to this feature, Ethereum has become a programmable blockchain. These smart contracts enable the creation of decentralized applications and systems called Web 3.0. Thanks to smart contracts, it is also possible to create digital assets such as tokens and NFTs.

2) Binance Smart Chain: Binance Smart Chain, another blockchain network used in the study, uses Proof of Stake and Authority (PoSA) as a consensus algorithm. Like Ether on Ethereum, the BNB coin supports transactions on the BNB chain. Due to EVM compatibility, it is possible to create tokens on BSC. In this case, however, the tokens follow the BEP-20 standard instead of ERC-20.

3) Utilized Consensus Algorithm: In blockchain technology, reaching a consensus on the information to be recorded in the ledger is critical. In blockchains, which are distributed systems such as Ethereum, the network nodes must agree on a common point. At this point, the necessary agreement is provided by consensus algorithms. Blockchain technology should use a reliable and effective consensus algorithm [11]. The most important purpose of the existing consensus algorithms is to prevent malicious people in case of any attack on the system. In addition, it updates the registries of all nodes involved in the blockchain network in the same order of operation.

There are multiple consensus algorithms preferred in blockchains. The most commonly used of these algorithms are PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), and Practical Byzantine Fault Tolerance. Under this heading, the Proof of Stake consensus algorithm, which the Ethereum blockchain has adopted with Ethereum 2.0, will be discussed. The reason for this transition is that the PoS consensus algorithm contains easier puzzles than the PoW mechanism that was previously in use, and therefore, it takes much less time to create blocks [12]. However, it requires less hardware and electricity costs. For this reason, it can be said to be environmentally friendly.

As mentioned in the previous paragraph, the *Proof of Stake* algorithm was introduced in 2012 as a solution to the problem of high resource consumption of the PoW algorithm [13]. There are validators in this type of consensus algorithm instead of the miner concept. These validator nodes contribute to the system by depositing refundable amounts of their cryptocurrency. The primary purpose of such a system is to allow the validator nodes to prove their ownership and trust by betting redeemable stakes of their cryptocurrency. However, malicious attacks put these contributed stakes at risk, thus ensuring system security and consensus [14]. In the PoS algorithm, the individual node that forms the next block is selected based on how much it has bet against other competing nodes [15]. The wager is usually based on the number of coins the validator has in the network for a given blockchain network. In these systems, the transaction fee is usually the reward. Users who wish to be part of this verification process should lock their bets in the network, as mentioned.

However, in this case, the network will be dominated by a single node with the largest bet. To solve this problem, other methods have been added to the selection process. Two of these methods are called "Random Block Selection" and "Coin Age Selection" [16].

In the *Random Block Selection* method, the next forger is selected based on hash value and bet, and the node with the combination of the highest bet and the lowest hash value is determined. However, in this case, nodes can usually predict the next forger because the number of bets that the network nodes have is publicly available.

In the *Coin Age Selection* method, the next validator is selected based on how long the bet has been held and the stake. The coin age is calculated by multiplying the number of days the coins have been held in the wager by the number of coins wagered. After a node verifies a block, the coin age value is reset to zero. To prevent the blockchain from being dominated by nodes with enormous stakes, the node must wait a certain amount of time to verify the next block after a block is verified.

When a node is selected to validate the next block, it checks whether the transactions contained in the block are valid, and if the transactions are valid, they are signed by the node and ultimately recorded on the blockchain by the node. The node receives the transaction fees associated with these transactions in the block as a reward.

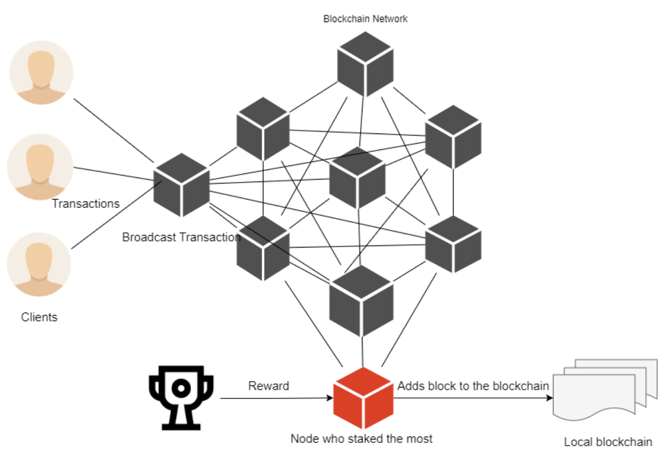

Fig. 2. PoS Algorithm

B. Remix IDE

Remix IDE is an integrated development environment for compiling and running smart contracts in the Solidity programming language. It can also be described as a suite of tools for interacting with the Ethereum blockchain. It compiles the written smart contract into bytecode, generates ABI (Application Binary Interface), and deploys contracts to various test networks of Ethereum (including the real Ethereum blockchain). All smart contracts created using Remix IDE are stored locally in the browser's cache [8].

In the study, the Remix tool provides an interface to ensure the system works correctly before the contract is transferred to the web interface during the development phase. Thus, it prevents any error arising from the functions in the smart contract in the web interface from being misunderstood by an error in the web interface. In addition, it is also used to publish the contract on the network and access the address or ABI information of the contract.

C. Etherscan ve BscScan

Etherscan [9] is an Ethereum blockchain browser used to track transactions, addresses, smart contracts, and other related data on the Ethereum blockchain. Thanks to the transparency of the Ethereum network, it provides its users with a publicly accessible database. Through this platform, users can search for Ethereum addresses, check transactions, examine smart contracts, and monitor other activities on the blockchain.

BscScan [10], just like Etherscan, is a blockchain scanner used to track transactions, addresses, smart contracts, and other related data on Binance Smart Chain. BscScan is a customized version of Etherscan for Binance Smart Chain. Thanks to the transparency of the BSC network, it provides its users with a publicly accessible database. Through BscScan, users can search for BSC addresses, check transactions, review smart contracts, and monitor other activities on the blockchain. In addition, BscScan provides APIs for many services that interact with BSC for developers to integrate their applications with BSC.

Etherscan and BscScan are important tools and resources for the ecosystem. They provide valuable information to users. Thanks to these scanners, anyone can read the contract's content, and they also provide an interface to display all transactions. In addition, as in Remix, it provides an interface to interact with the contract, and the ABI information can also be accessed. In this study, it is used to make the contract publicly readable and allow the person who publishes it on the network to verify it.

V. Recommended System Architecture

This section mentions the stages of the donation tracking system integration with blockchain and smart contracts in the donation system. The solution proposal of the article, the infrastructure and architecture of the work carried out, and the general operation are mentioned.

The system infrastructure is realized in a smart contract. In the contract, the transfer history of the users, the login code distributed by the contract owner to the users while registering to the system, and the user's identity information are stored. This part of the system functions like a database. The contract owner defines the registration code so the users can have full access to the system. To eliminate the anonymity of the users, user names and ID numbers are requested. After the user receives this information, the user-specific ID numbers are stored in a 'mapping' type variable converted to 'byte32' type. Apart from the registration code and identification information, the user's name, the total amount of money donated, and the amount spent by the foundation on the donation made by the user are stored.

Algorithm 1 Donation Transaction

```
procedure DONATION TRANSACTION
    Check if the sender is a foundation.
    if not a foundation then
        return
    Check if the sender is logged in with a citizen number.
    if has not logged in with a citizen number then
        return
    Check if the sender has a label for donating.
    if there is no label then
        return
    Create an array for usernames, amounts and addresses.
    Initialize the counter to 0.
    InvoiceNumber ← Length of the sender's staffInvoice array.
    for i=1 to InvoiceNumber do
        Element ← PersonnelInvoice[i]
        if Eleman.perAmount ≠ 0 then
            if Eleman.fromAddress ∈ transferCodestoAddressTrack as toAddress then
                Amount ← Element.perAmount
                Add UserName's and Amount's to the corresponding arrays.
                Add addresses to the address array.
                Increase the counter.
                Set the donationMade indicator to true.
            else
                if Eleman.quantity ≠ 0 then
                    Get username.
                    if Eleman.perAmount ≤ Amount then
                        Amount ← Amount - Element.perAmount
                        Add UserNames and Amounts to the corresponding arrays.
                        Add addresses to the address array.
                        Increase the counter.
                        Set the donationMade indicator to true.
                    else
                        Add UserName's and Element.perAmount to the corresponding arrays.
                        Add addresses to the address array.
                        Increase the counter.
                        Update donateBalance to Amount - Element.perAmount.
                        set Element.perAmount to 0.
    if Personnel.perAmount ≠ 0 then
        return "Transfer Failed!"
    Transfer
    amountDonate to _to.
    Create a transferCode using the transferCode ← codeCreator function.
    Call the function transferHistoryAndPersonnelInvoiceSavedFoundation with transferCode, sender, _to address, amountDonate, usernames, address array and amount array.
    Increase the totalSpending of the sender and _to with amountDonate.
```

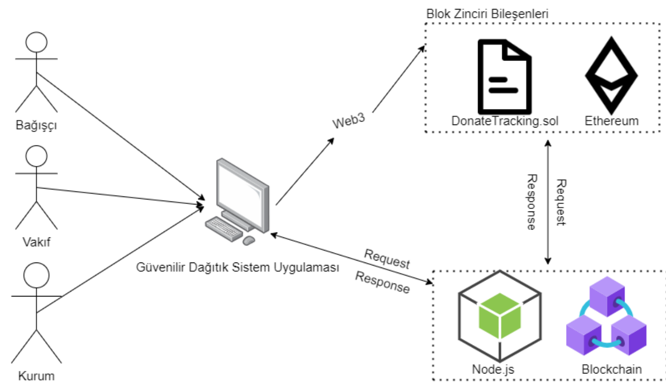

Fig. 3. General System Architecture

The data recorded in the distributed ledger ensures reliable and transparent operation of the system infrastructure. Users' transfer history, registration codes, and credentials are processed within the smart contract and stored in the distributed ledger. This data is subjected to a unique coding process with identification numbers to protect the anonymity of users. In addition, information such as users' names, donation amounts, and amounts spent by foundations are also stored. A unique transfer code identifies each transfer transaction, and these codes are associated with the user's identity information and recorded. This makes all transfers traceable and verifiable. Since the data in the distributed ledger is kept in a decentralized structure, reliability and transparency are ensured. As mentioned, users can view the data stored in the distributed ledger and track their transaction history through the web interface.

There are two types of transfer functions to transfer cryptocurrency from one wallet to another through the system. The first of these functions provides a transfer between the donor and the foundation. Here, foundation addresses are registered by the authorities (contract owners) on the system. When the user transfers money to the foundation addresses, they enter the percentage of how much they will donate to which foundation and perform the transfer process. Then, the system checks the user's specific identity information and registration code of the transfer transaction. After passing these conditions, the identity, user name, wallet address, and donation amount of the donor and the foundation are received. It is recorded in the variable called with a nine-character code randomly generated by the system. This structure can be considered as a receipt. This information recorded in the receipt is saved on a variable that stores the receipt codes created with the identity information of the users. In this way, a structure is built for each transfer in which only the receipts of the users who interact with this transfer are stored, and they can view them.

Secondly, a function performs the transfer between the foundation and the commercial company whose addresses are stored on the system. The general structure of the function is similar to the previous one, but there are some differences.

Donations made by donors are not transferred to the wallets of foundations. The human factor is eliminated, and thanks to the decentralized structure of the blockchain, it is stored in the contract to prevent fraud attempts by foundations. The structure within the transfer function is done through receipts. Here, the foundations transfer a certain amount from commercial companies to the donations made to them through receipts in the transfers for the goods to be purchased for aid to those in need. Here, the donation amounts in the receipts are traveled between them until they are equalized with the general amount to be spent. After this amount is equalized, in addition to the other receipt system, the names of the donors and the donation amounts are printed on the receipt and added to the receipt archives of all interacted users (donors, foundations, and commercial companies). The system creates a copy of the receipt to record the amount of money left in case foundations spend part of the amount in the receipts and do not spend the other part, and it is also used to mark that all the money in this receipt has been donated.

Within the contract, there are functions only the contract owner can call for the users to see the information more regularly. Adding and deleting the addresses of foundations and commercial companies/need owners on the system only by the authorized person is left to the contract holder. Thus, a more reliable donation is provided thanks to the controls.

The 'Ethers' and 'Wagmi' libraries in React are utilized for the smart contract, web interface, and electronic wallet to interact with each other. With Wagmi, blockchain networks such as Ethereum and Binance Smart Chain, where the contract can be uploaded, are defined in the system. The RPC address, network number, decimal number, network name, and symbol of these networks are defined. It must then be verified by the person who uploads the contract on the network. The ABI and address of the defined contract are obtained from the network and given as parameters in the 'Contract' function in Ethers. In this way, the interaction between the code in React and the contract uploaded to the blockchain network is realized. In addition to this information, the approval and authorization processes between the wallets and the contract within the transactions that users will perform with the contract are carried out through Ethers. Sometimes, the network information, signature authorization, and account information used in the interface must be accessed. In such cases, Wagmi is used.

The web interface provides users with account information, foundation transaction tracking, and code search sections. In the account information tab, users can access wallet information, ID number, total donation amount, registration code, user names, and the amount of money in the electronic wallet in a single place. In addition, the transfer information of the transfers with which he interacts in the smart contract section is also reflected in tabular form. In the foundation transaction tracking section, the receipts of total donations and expenditures made to foundations are presented to users in tables for everyone to follow. In the code search section, receipt numbers given to users, users can access transfer information they want to look at in case tables are too crowded.

TABLE II
TOTAL EXPENDITURES

AHBAP Total Expenditure	TEGV Total Expenditure
0.3000	0.3000

TABLE III
FOUNDATIONS' EXPENDITURE TRANSACTION TABLE

Code	From	To	Donate Amount	Donaters
HS83JDY57	AHBAP	MIGROS	0.25 BNB	TAHA[0.10] RANA[0.15]
AJDN29I3Y	AHBAP	MIGROS	0.05 BNB	RANA[0.05]
GDB3Y44PD	TEGV	MIGROS	0.30 BNB	TAHA[0.10] RANA[0.20]

VI. CONCLUTIONS

Within the scope of this study, an application is presented to the users with a suitable web infrastructure with the help of Wagmi and Ethers libraries with the help of contract ABIs of the data received from the smart contract by individuals (donor, foundation, and commercial company) in all transfers within the scope of donation. Within the voucher system used, foundations are only allowed to spend the donations defined in the system on the voucher, thus preventing the money from stagnating in a person's wallet and preventing fraud by spending within the contract. In these donations made by the donors, how much of the donation amount made by the foundations is spent by the foundations is then informed, and the money is tracked. The identity information, names, wallet address, and donation amount on the receipt are notified to all parties interacting with the transfer.

It should be noted here that a reliable donation tracking system structure targeted by eliminating the human factor has been achieved, ensuring that the donation transactions are carried out in a way that the rules of the money in the smart contract are predetermined and published in an environment where everyone can look at these rules safely reach the people in need.

REFERENCES

[1] A. Singh, R. Rajak, H. Mistry and P. Raut, "Aid, Charity and Donation Tracking System Using Blockchain," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 2020, pp. 457-462, doi: 10.1109/ICOEI48184.2020.9143001.

[2] Niranjanamurthy, M., Nithya, B. N., Jagannatha, S. (2018). Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing. doi:10.1007/s10586-018-2387-5

[3] A. Singh, R. Rajak, H. Mistry and P. Raut, "Aid, Charity and Donation Tracking System Using Blockchain," 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), Tirunelveli, India, 2020, pp. 457-462, doi: 10.1109/ICOEI48184.2020.9143001.

[4] Liu, W., Li, Y., Wang, X. et al. A donation tracing blockchain model using improved DPoS consensus algorithm. Peer-to-Peer Netw. Appl. 14, 2789–2800 (2021). https://doi.org/10.1007/s12083-021-01102-9

[5] E. ŞAFAK, Ç. ARSLAN, M. GÖZÜTOK, and T. KÖPRÜLÜ, "Dağıtık Defter teknolojileri ve Uygulama alanları üzerine bir inceleme," European Journal of Science and Technology, 2021.

[6] Sadri, S., Shahzad, A., Zhang, K. (2021). Blockchain Traceability in Healthcare: Blood Donation Supply

[7] Chain. https://doi.org/10.23919/icact51234.2021.9370704 Tiwari, Varun, Singh, Santosh, Vadi, Vikas. (2023). Smart Contract Using Solidity (Remix -Ethereum IDE). 12. 243-249. 10.17148/IJARCCE.2023.12253.

[8] LEE, W.-M. (2023). Beginning Ethereum Smart Contracts Programming: With examples in python, solidity, and javascript. APRESS.

[9] https://etherscan https://etherscan.io/

[10] https://bscscan.com/ bscscan

[11] Moritz Wendl, My Hanh Doan, Remmer Sassen, The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review, Journal of Environmental Management, Volume 326, Part A, 2023, 116530, ISSN 0301-4797, https://doi.org/10.1016/j.jenvman.2022.116530.

[12] Buterin, Vitalik, Griffith, Virgil. (2017). Casper the Friendly Finality Gadget.

[13] Moritz Wendl, My Hanh Doan, Remmer Sassen, The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review, Journal of Environmental Management, Volume 326, Part A, 2023, 116530, ISSN 0301-4797, https://doi.org/10.1016/j.jenvman.2022.116530.

[14] S. M. Skh Saad and R. Z. Raja Mohd Radzi, "Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (POS) and Delegated Proof of Stake (DPOS)", Int J Innov Comp, vol. 10, no. 2, Nov. 2020.

[15] Shifferaw, Y., Lemma, S. (2022). Limitations of proof of stake algorithm in blockchain: A review. African Journals Online, 21(97), 216947.

[16] Tarek Frikha, Faten Chaabane, Nadhir Aouinti, Omar Cheikhrouhou, Nader Ben Amor, Abdelfateh Kerrouche, "Implementation of Blockchain Consensus Algorithm on Embedded Architecture", Security and Communication Networks, vol. 2021, Article ID 9918697, 11 pages, 2021. https://doi.org/10.1155/2021/9918697