International Journal of Communication and Information Technology

E-ISSN: 2707-6628
P-ISSN: 2707-661X
Impact Factor (RJIF): 5.56
www.computersciencejournals.com/ijcit
IJCIT 2025; 6(2): 15-31
Received: 16-05-2025
Accepted: 19-06-2025

Chnar Mohammed Kareem
Computer Science Department, College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq

Ahmed Chalak Shakir
Information Technology Department, College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq

Corresponding Author:
Chnar Mohammed Kareem
Computer Science Department, College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq

DeFiDonate: Innovations in Decentralized Finance (DeFi) through blockchain technology

Chnar Mohammed Kareem and Ahmed Chalak Shakir

DOI: https://doi.org/10.33545/2707661X.2025.v6.i2a.138

Abstract
This paper proposes DeFiDonate, a web-based decentralized application that facilitates the transparency and privacy of donations to charities while also increasing trust through the use of blockchain and various Decentralized Finance (DeFi) solutions. The problem with traditional donation models is that they lack traceability and are centralized, with limitations and restrictions on donors. DeFiDonate proposed using Elliptic Curve Cryptography (ECC), Non-Fungible Tokens (NFTs), a form of smart contracts, and Elliptic Curve Digital Signature Algorithm (ECDSA).DeFiDonate provides flexibility for donors by making either a direct donation to beneficiaries or donating to a liquidity pool, then distributing funds through a decentralized voting system and encrypting sensitive data, like the wallet addresses, donation amounts, and donors' NFT identifiers with ECC, meaning it's recorded in both on-chain and off-chain safety, and confirming the transactions and validating the signature is unauthentic with ECDSA, the implementation of DeFiDonate composed on Django and Solidity for the creation of smart contracts; Truffle, Ganache, and MetaMask for local testing. These results indicate that the system is safe for use, as it provides transaction integrity and information security. Based on performance analysis carried out in Truffle Develop, the use of NFTs within contracts was found to be associated with a notable decrease in execution time. Another application blockchain developers can discuss is DeFiDonate, which exemplifies a trusted, decentralized, and transparent method of digital giving.

Keywords: Blockchain, smart contract, donation, DeFi, NFT, ECC, ECDSA

1. Introduction

Charity donations serve as a form of social solidarity that enhances collaboration, improves the social status and the economics of societies, and strengthens connections among all members of the population. However, the charitable donation methods include transferring large sums of funds via 70% of individual contributions, which requires boosting control and monitoring [1]. Existing strategies don't provide transparency in the areas of donation and charity. As transactions regarding contributions from multiple organizations lack suitable protection for record-keeping, the engagement of fraudulent individuals has negatively impacted public trust in this social cause. The donor is uncertain whether their assistance was employed accurately or not. Fraud is another cause that leads donors to lose faith in charities [2]. Alternately, another challenge is security, as centralized systems are vulnerable to fraud and breaches; these processes are slow to adjust, limiting quick responses to immediate needs. Another disadvantage of conventional donation systems is that they are costly to process, making them susceptible to single points of failure and, therefore, more likely to face security attacks and fraud [3]. The blockchain has gained popularity due to its potential applications in various sectors, including non-financial and financial associations, such as supply chains, healthcare, and insurance systems [1]. As a decentralized network of distributed nodes that eliminates the need for centralized authority and facilitates transaction management, these transactions are organized into blocks, with each block linked to the preceding blocks of transactions via a chain [4]. Key characteristics of blockchain technology are confidentiality, protection, transparency, autonomy, decentralization, and immutability [5]. Blockchain technology will help resolve such problems by providing an improved, more transparent, secure, and authentic system of tracking donations through smart contracts, enabling the immutability and transparency of transactions in a donation tracking system. That is, once stored in the blockchain, it is permanent and unerasable, which offers another sense of responsibility and protection. When saving something to the blockchain, it becomes immutable and cannot be altered or retrieved, providing a layer of sufficient accountability and security to all parties involved. It also allows all participants to confirm its execution and access transaction attributes. Moreover, blockchain decentralization eliminates the need for a mediator, which in turn reduces transaction costs and ensures that many donations can reach their intended recipients [3]. Conversely, Decentralized Finance (DeFi) is reinventing conventional, centralized finance by providing peer-to-peer and transparent, permissionless, and trustless solutions built on blockchain infrastructures. These types of solutions allow users to trade directly with each other, to access financial services without any intermediaries (e.g., exchanges, banks, brokers), and to integrate familiar functions into a single protocol, such as decentralized exchanges, token issuance, lending and borrowing protocols, governance, and automated marketplaces [6]. In this study, we propose DeFiDonate, a donation system on blockchain as a web application donation system, by merging DeFi capabilities, smart contracts, Non-Fungible Tokens (NFTs), serving as donor identity, trace the donation processes in a trusted way, utilizing Elliptic Curve Cryptography (ECC) for securely encrypting sensitive data, and with the Elliptic Curve Digital Signature Algorithm (ECDSA) to guarantee the legitimacy and reliability of donors' transactions and their signatures within the application.

Motivation

The charitable organization section is designed to increase the well-being of the poor people to eliminate economic, social and environmental challenges, this includes money giving to people experiencing poverty, donating in charity, organizing fundraisers, lobbying and awareness campaigns; the contribution of charitable organizations of the population and society is tremendous and this is the contribution of money and time to people experiencing poverty of the population [7]. Nevertheless, there is a lack of trust and openness in the way the funds are utilized; we must find a solution to tracking donations securely and transparently [8].

Combining blockchain technology and DeFi mechanisms can simplify the donation process by addressing those challenges and issues, enabling secure, transparent, and trackable donation systems, transforming traditional donation platforms, and encouraging users to donate by gaining their trust through smart contracts, NFTs, decentralized voting (including participants donors that deposit to the liquidity donation through the voting process), and ECC, aligning with the technological and revolutionary era, simplifying the monetary donation services that support beneficiaries, including individuals, institutions, or government organizations.

Contributions

We present the DeFiDonate web donation system that uses various DeFi mechanisms based on blockchain to ensure security, traceability, and fairness for every donation process, which includes:

- **NFT for identity and donation traceability:** Assigning an NFT to each registered donor in the application, which retains all contribution information, and assists in accountability without incurring additional blockchain gas fees.
- **Liquidity pool example for fund deposit:** An emulated Balancer Vault contract collates donations, and after a specified duration, the users cast their votes as to where the monies should be distributed towards selected groups.
- **Voting method based on contribution:** The stake of the donors' funds determines their contribution to the liquidity, as the voting and decision-making procedures are transparent and equitable, due to the use of smart contracts.
- **Peer-to-peer and liquidity donations:** These donations allow donors to choose how they want to donate their money and participate in deciding how that money will be utilized. This method is always present and consolidates people.
- **Securing distributed operation using ECC and ECDSA:** Apply ECC to encrypt valuable data when it registers on both on-chain and off-chain, as well as to confirm donations are authentic; ECDSA signs every transaction that takes place.
- **Integration of Web3 with Ethereum smart contracts:** An application was developed on Web3 using Django, which supervises the back end, and Web3.js interacts with the smart contracts on the blockchain. Due to the integration of the application with MetaMask, users have the opportunity to make confidential and safe donations on the Ethereum.
- **Smart contract deployment and local testing of blockchain:** An Ethereum environment with Truffle and Ganache installed to test and implement the system with their help. Before launching the system, the existence of smart contracts made it precise, reliable, and secure.

Problem statement

Transparency and openness have become the most desired concepts since faith in charities has declined in recent decades, as donations via mobile or bank applications decreased in the current systems due to adverse situations [9]. The use of social engineering methods by fraudsters to trick consumers into supporting fake organizations or charities has risen recently. As more individuals use social media to organize, communicate, and get involved in charitable projects, scammers have shifted to participating in multiple contribution fraud on these sites [10]; blockchain technology enhances humanitarian assistance operations by facilitating accountability, transparency, and real-time data, besides promoting effectiveness and efficiency by automating procedures, leveraging smart contracts, and assuring timely source delivery [11].

Related works

This section has selected several works in the field of charity and donation to make the donation process convenient, easy, transparent, effective, decentralized, and secure for the donor. J. Swati *et al.* [12] offer Crypto-GoCharity, a blockchain platform for charity that solves the trust and disregard in charities, incorporating MetaMask, Ganache, and hosting application data on a MongoDB cloud repository. The system transacts peer-to-peer, raises trustworthiness through a distributed ledger, and applies smart contracts to automate the process, which can help donors select organizations but is limited to map-based filtering and tracking of how their contribution is spent. I.

Segeda *et al.* [13]. Present a decentralized system with DeFi in charities based on blockchain with security and managing updates via smart contracts and a web for user interaction; to provide help and support during crises and wars, it also applies liquidity pools like UniSwap and mechanisms to record and control the donations and focusing on mathematical approaches for rewards to consumers. Yet, besides its efficiency in simplifying charities, it lacks identity management for participants and any encryption methods. B. He *et al.* [14] developed a proposal for a trackable system of charity donations based on Ethereum, which addresses security concerns in charity donation ecosystems while maintaining aspects of privacy through the use of privacy protection tools in encrypted algorithms. In addition, it utilizes Public Key Encryption with Keyword Search mechanisms (PEKS), a smart contract, a user interface, and a cloud server to ensure the privacy, verifiability, and traceability of storage; still, it does not handle security procedures, such as identity verification of donors or beneficiaries. Meeradevi *et al.* [15]. Presents a blockchain-based fundraising model for Non-Profit Organizations (NGO), assuring integrity and transparency by constructing a channel between the NGO and the donors using smart contracts and a decentralized distributed ledger, including traceability of real-time donation, and preventing the use of the funds, within hyper ledger fabric that deployed on Rinkeby, allowing them to made donations and contribute via the MetaMask, indicating the effectiveness in addressing transactions and powering donors' trust for making donations. But it lacks flexibility and consideration for the donors within the system. C. Nairi *et al.* [3]. Offer DonateBlocks for transparent, safe, and tamper-proof transactions to execute immutable records to track donations. It consists of blockchain platforms (Ethereum, Polygon), smart contracts, Web3.0, and a MetaMask wallet for following and controlling donations in a secure and decentralized manner, as well as the incorporation of the Interplanetary File System (IPFS) for saving files and Decentralized Identifiers (DIDs). The study itself provides a decentralized donation, which does not inform us about how it can be used or what security measures are taken to ensure its safety, e.g., encryption.

Backgrounds

The blockchain technology

Blockchain technology is regarded as the fundamental basis of cryptocurrencies, particularly the Bitcoin system. People speculate that Bitcoin was the first cryptocurrency structure to be developed, and it currently holds the highest value. Since then, many cryptocurrencies with more complex characteristics have appeared, such as Ethereum, which uses smart contracts. It is widely known in the blockchain world that it is a decentralized peer-to-peer network. The intention of using blockchain is to eliminate the intermediaries and administrators from the entire process, which is achieved by constructing an immutable and unalterable decentralized record accessible to everyone [16]. It is also a distributed system composed of growing collections of information, known as blocks, which are associated securely through encryption, where every block utilizes encrypted forms of the hashed details of the prior block in addition to the timestamp. Although blockchain data records are immutable, protected by their architecture and functioning as a decentralized computational network with exceptionally low failure rates [17]. There are two major security constructs used in the blockchain protocols (e.g., Proof of Work (PoW) and Proof of Stake (PoS)); under PoW, a piece of information known as a nonce is generated, which requires an extended period and consumes a notable portion of power due to the high computational requirements. Yet, others can determine if a block and nonce meet specific requirements.

Additionally, in PoW, miners within the network attempt to accomplish transactions, earning rewards. In PoS, miners maintain something as evidence at stake, and if they mine correctly, they will obtain a reward; otherwise, they will forfeit the fund that they have at stake [18]. Various applications and industries have been utilizing blockchain, as evidenced by current studies that focus on the implementation and application of blockchain technology across different business sectors, including digital IDs, supply chain management, healthcare, property, wills and inheritance, food traceability and security, digital voting, and money tracking [4].

Smart contract

Generally, a smart contract is considered a component of code that utilizes blockchain technology to execute and enforce a contract, thereby simplifying the terms of the agreement among parties who are unknown to each other. When meeting a specific requirement, the system transfers digital assets to all parties engaged. Compared to conventional contracts not involving third parties, this reduces transaction fees [19].

Ethereum is another public blockchain that was introduced in 2014 and offered an operational application within the smart contracts paradigm; mainly, through Ethereum, the primary objective transitioned from the innovation of the use of cryptocurrencies to developing decentralized applications, giving rise to the second release of the blockchain protocol, which was known as blockchain 2.0 [20].

Decentralized Finance (DeFi)

The phrase DeFi encompasses several types of financial projects built on blockchain platforms, such as Ethereum, Solana, Binance Smart Chain (BSC), Polygon, Aptos, and several others, that implement financial transactions, like investment, digital assets, and trading; DeFi has been one of the most interesting possibilities for investing in the previous years, mainly because of its decentralized, highly transparent, and open features. Hundreds of billions of bucks have joined the DeFi corporation. Ethereum holds more than 80 percent of DeFi locked-value accounts in various blockchain accounts [21]. Since 2021, DeFi has proven to be an exceptional application in derivative protocols, stablecoins, prediction markets, and payments [22]. Numerous DeFi protocols are now integral components of a broader environment that encompasses recognized applications and tokens; for example, Compound and AAVE are protocols used for lending and borrowing, while Balancer, SushiSwap, and UniSwap are Decentralized Exchange (DEX) protocols, and using dHEDGE and yEarn for asset management [23]; DApps protocols typically operate with a liquidity pool, depicted as a pool of assets that enable exchanges. Any pool may have restrictions limiting its membership to only specific types of property, and an exchange involves consumers exchanging pool assets for other pool assets [24].

Non-Fungible Tokens (NFTs)

NFTs are digital assets with unique attributes, differentiating them from other digital resources, including digital currencies and traditional financial assets; when compared to digital currencies, NFTs are incompatible, whereas fungible products are comparable, as their value is established by their uniqueness rather than any distinctive characteristics they may possess [25], by applying decentralized digital ledger technology the blockchain preserves NFTs to confirm ownership rights and public authenticity for every token. Like Ethereum, an NFT is a type of Ethereum token, specifically the ERC-721 token, which signifies the right to the underlying infrastructure asset; for instance, if an artist mints an NFT for their work, the NFT serves as the digital title deed of the work; the perpetual NFT contracts serve as a building block, primitively, which can take many different forms in DeFi, such as derivatives and lending, and make DeFi composable; it will find new service applications because of blockchain acceptance within developing metaverse platforms, as they will enable usage with metaverse NFT assets to manage the upcoming virtual economy [26]. The NFT possesses one of the most critical characteristics of security, ingrained in the blockchain's ideas, including cryptographic algorithms that make it impossible to tamper with or forge. Another essential property of an NFT is that it is traceable, meaning that the history of each of its transactions can thebe kept as a whole, another trait is transferability to transfer such NFTs securely via smart contracts, which are irreversible and transparent; programmable features on the side of developers allow the implementation of automatic royalty systems, which award content creators a percentage of future sales, while scarcity is preserved with smart contracts, which select and mint some of the NFTs, consequently increasing their value due to their uniqueness; interoperability enables the processing of NFTs across multiple platforms. Proprietorship verification is protected via the blockchain and private keys, ensuring the transaction is authentic and saved permanently, and indivisibility implies the inability of NFTs to be split into smaller units; smart contracts possess this feature, while the uniqueness of the NFT is ensured through cryptographic hashing. Conducting unique identifiers from the metadata with cryptographic algorithms and saving them on the blockchain, preventing alteration and duplication immediately [27].

Ganache

Ganache is a solid and effective private blockchain built on Ethereum, which was developed specifically for securing and establishing data storage, enabling organizations and developers a configurable and safe platform for constructing, testing, and implementing DApps and smart contracts on a secure blockchain; it interacts easily with the Ethereum Virtual Machine (EVM), helping programmers to take advantage of Ethereum platforms' capabilities and characteristics; this involves leveraging the programming language Solidity, also the Ethereum's essential currency, Ether, and a comprehensive variety of Ethereum-based DApps and smart contracts, offering multiple features, making it an ideal choice for constructing and protecting data records. It provides a local experimental network, allowing programmers to validate their applications and smart contracts for connecting with the global Ethereum network, thereby decreasing the risk of exposing private information throughout the construction process and enabling programmers to simulate various network conditions [28].

MetaMask

MetaMask is an Ethereum wallet that enables simplified management of cryptocurrencies, secure transactions, and a configurable transaction chain. MetaMask also allows for a highly mobile application and a compatible browser extension. Besides these characteristics, MetaMask is freely available, has an enormous community, and provides solid customer support [12].

Security procedures

Security breaches have become more frequent and are happening at all times these days [29].

Elliptic Curve Cryptography (ECC)

ECC is an effective type of cryptography that employs public keys, established on an elliptic curve, for encryption and decryption; as the elliptic curve is a smooth, curvilinear surface of genus one in the field, its mathematical definition is as follows [30]:

$$y^2 = x^3 + ax + b \tag{1}$$

It offers an excellent encryption method using fewer keys than other encryption approaches. ECC also delivers multiple benefits in the verification and identification techniques, including high efficiency, low bandwidth requirements, and quick speed [31]. Table 1 below corresponds to the key sizes with diverse security aspects among ECC and RSA/DSA. It is also critical to note that a 160-bit ECC key delivers equal security as a 1024-bit RSA key. Additionally, the overall number of mathematical instructions processed and the total number of multiply-accumulate instructions performed are shown for each technique [32].

Elliptic Curve Digital Signature Algorithm (ECDSA)

A gradual transition from RSA to DS and subsequently to ECC has been observed over the past decade, driven by the latest developments and an effort to achieve the best possible, where recent encryption ideas, such as ECDSA, have gained popularity because of their compact code and high security, as well as efficient execution and a manageable code size [33]. The source code of the ECDSA digital signature scheme is based on ECC, or elliptic curve cryptography, which utilizes mathematical concepts involving elliptic curves to generate both a secret and a public key. The sender generates a digital signature of a message through a private key and adds it to the message to validate it with ECDSA. The recipient can verify the accuracy and integrity of the information passed via the application of the sender's public key [34]. Due to the importance of the ECDSA technique in blockchain and other applications, developing a feasible distributed signature scheme based on ECDSA is a highly objective goal. Regarding the value of the ECDSA approach in blockchain applications and beyond, establishing a feasible distributed signature service based on ECDSA is an essential objective [35].

Materials and Methods

DeFiDonate, the proposed platform, is a decentralized web application designed for donations and built on Ethereum blockchain technology as one of the decentralized solutions addressing the issues of security, trust, transparency, and centralization in traditional donation systems. We have deployed it based on a Python framework, Django (between frontend and backend), Solidity smart contracts, and NFTs combined with ECC/ECDSA cryptography. Figure 1 presents the methodology approach and implementation procedure of the DeFiDonate system.

Wallet integration process and the registration of the user

Institutions and donors register through DeFiDonate's web interface, and to donate, they associate with the website and seal the donation (or purchase) in their MetaMask wallet. The institutions on the platform are added through the approval process by the admin panel. Beneficiaries, on the other hand, are added to the application by the institutions to which they belong.

The building design of smart contract

Executing five smart contracts, including DonorContract for handling donor registration with the application, NFTContract to mint a unique ID for each donor and view their donation history, DonationContract to facilitate the direct donation process from the donor to one or multiple beneficiaries, LiquidityDonationPool, and MockVault to manage deposit process that made by any donor to the liquidity pool, and the voting operation to determine the transmission of the funds.

Encryption for security with ECC and ECDSA

Encryption of sensitive information (wallet address, amount of the donation, NFT IDs, and amount of the deposit) in a donation with the help of ECC before putting on such information in the databases of Django and blockchain, and then the digital signature established according to the ECDSA algorithm gets verified on all the processes of donation demanded by the donor.

Mechanism of voting and allocation of funds

Voting will only be allowed after the initial deposit has been made within 30 days of the initial deposit. The donors shall have the right to justify their vote to an institution, which is equivalent to the number of votes accorded to every donor, depending on the level of donation they have made. The smart contract shall quantify the weight of each vote, as the funds will be liquidated according to the regulations mentioned earlier.

Results

The establishment and testing of the DeFiDonate application completed using Windows 11 Pro 64-bit, 13th Gen Intel® Core™ i7-13620H (16 CPUs), ~2.4 GHz, and Random Access Memory (RAM) of 16384 megabytes (MB); the backend of the system was done in the programming language Django for the database, while the frontend interface was based on HTML, JavaScript, and Bootstrap to make the interface responsive, as the construction of smart contracts in the Solidity programming language (version 0.8.19) and deployed locally using Truffle and Ganache for Ethereum blockchain simulation, along with MetaMask as the web wallet. In addition, the front end is based on Web2.js to communicate with published contracts in the blockchain space; Postman is used to examine the effectiveness of the smart contracts and Django backend, check the API endpoints, and observe their responses.

Wallet integration process and the registration of the user

DeFiDonate has two types of users: donors and institutions. The two types of users register differently, as illustrated by the differences in the processes shown in Figure 2. Figure 3 confirms that the donors accessed a special web interface, where they reported their data wallet address. They used MetaMask, an Ethereum wallet, on the website to sign transactions for their donation procedures, without exposing their private keys. Upon successful registration, performing encryption with ECC for their wallet address, a unique NFT will be minted for them.

Additionally, encrypt them before recording them. For institution registration, apply the procedures similar to those shown in the registration form in Figure 4. However, it required admin approval from the admin site before adding it to DeFiDonate, as illustrated in Figure 5. Each institution also has an encrypted MetaMask wallet address within the system, employing it to collect donations from liquidity following confirmation. Moreover, each institution is responsible for adding its beneficiaries to DeFiDonate to receive funds from donors through the direct donation process and encrypting their wallet addresses with ECC.

The implementation of smart contracts

As we have explained above, DeFiDonate is a combination of five core contracts, created in the blockchain programming language Solidity; each plays a vital role in making the application usable in a decentralized, secure, and transparent donation and voting process. They were deployed and tested locally using Truffle and Ganache as an Ethereum blockchain, utilizing the MetaMask plugin to sign transactions by the donors locally in the frontend. The five contracts are:

- **DonorContract:** Handles the donor registration procedure, whereby only registered donors are signed in. It validates the wallet address of donors and associates their identity with NFTs.
- **NFTContract:** Offers a distinct NFT to all donors registered with DeFiDonate, which acts as a secure and verifiable identifier in each donation transaction, and monitors donors' donation history made within the application**.**
- **DonationContract:** This contract eases and streamlines the entire procedure of informing the donor that the beneficiaries have received the money with the help of ECDSA to record transactions once the signatures of the donor are verified, details of the donation and those of the recipient will be hashed and retained on-chain.
- **LiquidityDonationPool:** It enables the donors to deposit their donations into the pool, and after thirty days from the first donor deposit to the liquidity, a voting process starts, and only the donors who contribute to the liquidity can cast a vote to select an institution that receives the funds, and all deposit information is encrypted, such as donor address, deposit amount, and vote weight.
- **MockVault:** Acts as a pool to store and distribute the deposit funds made by the donors through the use of the LiquidityDonationPool.

Every contract has been tested through multiple stages, first using the local environment of Truffle, then via Truffle combined with Ganache, which presents as a simulator of the Ethereum blockchain. Web3 has linked the ABI of the deployed contracts to the Django database; therefore, information transmission among the backend programs is smooth.

Security procedures with ECC and ECDSA

In DeFiDonate, we provide Integrity, privacy, and legality associated with the donor's donation approach. By employing two methods of encryption, ECC and ECDSA, for verification. The ECC applied to protect sensitive data such as the donor's wallet address, the donation and deposit amount, the NFT IDs, the beneficiaries' and institutions' wallet addresses, and using the vote weight for the voting process before saving it on both the Django database and on-chain and making sure that those fields are invisible even when they stored publicly. The ECDSA has been merged with both the DonationContract and the LiquidityDonationPool to verify the digital signature of each donor before processing any donation within DeFiDonate. This will prevent unauthorized access, and only a holder of the proper wallet will be allowed to donate, accomplishing the verification operation within the contracts. The system, as a combination of ECC and ECDSA, provides:

- **Confidentiality:** guaranteeing the privacy of data on blockchain and off-chain through encryption.
- **Authenticity:** The donations and votes are signed and can be verified only by valid donors.
- **Integrity:** Implying, and preventing any form of tampering since the attempt to decrypt or validate the signature has failed.

Such a security model significantly reduces threats to key usage, funding transfer abuse, and the exposure of sensitive data, and is also compliant with the best practices of blockchain-based financial applications.

Direct donation process

With DeFiDonate, donors can directly contribute (ETH) to registered beneficiaries via the DonationContract, enhancing it with the help of MetaMask, smart contracts, and cryptographic assets that track all the transactions safely, traceably, and authentically; to make a direct donation, donors connect their MetaMask wallet account to DeFiDonate, identify one or multiple beneficiaries, and enter the amount to be donated, here the system generates a structured data payload associated with the donation and signs it with the donor's key through MetaMask.

The signature, along with the donation, will be sent with a request to the backend, which will then pass it to the DonationContract. Figures 5 and 6 below show the direct donation process. The relatively new concept designed by DeFiDonate provides an easy-to-use interface compatible with the Iraqi audience, which has an in-built ETH IQD converter that allows converting the value of Ether to Iraqi Dinar in real-time, and providing links to reliable websites to buy and sell Ether, which increases its convenience to those who are not familiar with the world of cryptocurrency infrastructure.

Liquidity deposit and voting procedures

DeFiDonate features decentralized liquidity, allowing donors to contribute in the form of ETH by entering the smart contract LiquidityDonationPool, authenticating every deposit using ECDSA, and protecting sensitive information, including the donor wallet, deposit amount, and vote weight, with ECC, based on the number of contributions made by the donors, to calculate their vote weight. After 30 days from the first deposit, each contributor of the deposit votes once through their profile page in DeFiDonate, using their vote weight (which depends on the total deposit they made). If a single institution acquires a majority of votes, it withdraws the liquidity and deposits it into the account of the winning institution. Nevertheless, votes on the institutions are equal, the funds will be distributed equally among the different institutions, ensuring a safe and decentralized delivery of the donation pool of funds; Figures 7 and 8 depict the deposit mechanism, while the administration of voting methods for donors, administrators, and institutional site interfaces is shown in Figures 9 and 10, as well as in Figure 11.

NFT-based donor tracking

How NFT plays a crucial role in DeFiDonate in ensuring the transparency and verifiability of each donation activity. After concluding a successful donation, whether direct or liquidity-based, the donor's NFT is updated with the transaction details made by the donor, guaranteeing each donors have an immutable and verified history of their contributions; it does not only serve as a digital identity but also as a record of donation activity that can be viewed from the donor profile section of the system, as shown in Figure 12.

Discussion

In this section, DeFiDonate, we provide a comparison with other systems based on blockchain technology through a comparative analysis of the following system requirements, as listed in Table 2: governance, security, privacy, transparency, traceability, and flexibility.

Comparative analysis

Unlike previously established systems, such as DonateBlocks [3], Crypto-GoCharity [12], DeFi charity platform [13], charitable donation system [14], and charity integrity [15]. The characteristics of the proposed DeFiDonate system are that it addresses all six requirements mentioned above:

- **Governance:** Implemented with the help of the donor voting mechanism, preventing the use of the deposited money until decentralized voting.
- **Security**: It is secured through the integration of ECC, utilizing encryption of confidential on-chain and off-chain information, and ECDSA, to authenticate and authorize digital signatures through any transaction, enabling unauthorized individuals to donate or participate in voting.
- **Privacy:** Controlled by encrypting sensitive data such as wallet addresses, the amount of donations, and NFT IDs to be preserved on-chain and in the database.
- **Transparency:** Ensured since all logic of smart contracts and donations, plus distributions of funds, are installed on the blockchain and are seen on the blockchain transaction logs.
- **Traceability:** The NFTContract facilitates every donation entry; it writes a record into the NFT of the donor so that the history can be verified (traceability).

- **Flexibility:** Achieved through both direct donations and contributions to liquidity pools, which are present as mechanisms that enable a donor to give according to their wishes.

Security discussion

DeFiDonate has two cryptographic standards: Within ECC, by Encrypting sensitive data, including the data of the block from as shown in Figure 13, and wallet addresses (donor, beneficiary, institution), donors NFT as we illustrate them in Figure 14, beside the amounts of donation, and the weight of the donor's vote, providing data confidentiality and practices relating to blockchain privacy. On the other hand, with ECDSA, all donation and deposit transactions are validated using this algorithm in the smart contract, preventing unauthorized individuals from conducting blockchain transactions and creating authenticity, thereby destroying spoofing or unauthorized activities. Such security methods are more efficient than classical donation systems and even some existing blockchain-based systems that fail to provide end-to-end encryption and robust cryptographic validation systems; the Figures [15, 16] demonstrate that ECC can achieve similar security levels as those of RSA/DSA cryptosystems, but with a significantly smaller key size, thereby improving efficiency and scalability.

Impact of NFT integration

To determine the effectiveness of DeFiDonate smart contracts, we have compared two versions of the system (with and without NFT support) in the Truffle Develop environment. In the evaluation, the time factor to perform procedures such as donor registration, direct donation, liquidity deposit, and voting was measured, which reveals that contracts using the NFT performed slightly better in time, which is explained by the fact that the NFT structure and its incorporation with the contracts, as depicted in the charts that represent the performance of the decentralized donation process (Figures 16, 17, 18, and 19) for the time, it is possible to achieve faster and more efficient execution, which improves overall performance.

Table 1: Key size comparison of ECC, and RSA/DSA [32]

Symmetrical key size (length in bits)	80	112	128	192	256
RSA/DSA key size (length in bits)	1024	2048	3072	7680	15360
Elliptic Curve key size (length in bits)	160	224	256	384	521

Table 2: Comparison between DeFiDonate and other donation systems

Ref.	System Name	Publication year	Blockchain type	Framework	Methods & algorithms	Governance	Security	Privacy	Transparency	Traceability	Flexibility
[12]	Crypto-GoCharity	2022	Public	Ethereum	Smart Contract, Cryptography	×	✓	×	✓	✓	×
[3]	DonateBlocks	2023	Public	Ethereum (Polygon)	Smart Contracts, DID, IPFS	×	✓	×	✓	✓	✓
[15]	Charity integrity	2023	Public	Ethereum (Rinkeby)	Smart Contracts	×	✓	×	✓	✓	×
[14]	Charitable donation system	2024	Public	Ethereum	PEKS, IND-CKA, Mythril	×	✓	✓	✓	✓	×
[13]	DeFi charity platform	2024	Public	Ethereum	Liquidity Model, AMM, Staking	×	✓	×	✓	×	×
	The proposal web application: DeFiDonate	2025	Public	Ethereum	ECC, ECDSA, NFT, Voting, liquidity (simulated Vault contract)	✓	✓	✓	✓	✓	✓

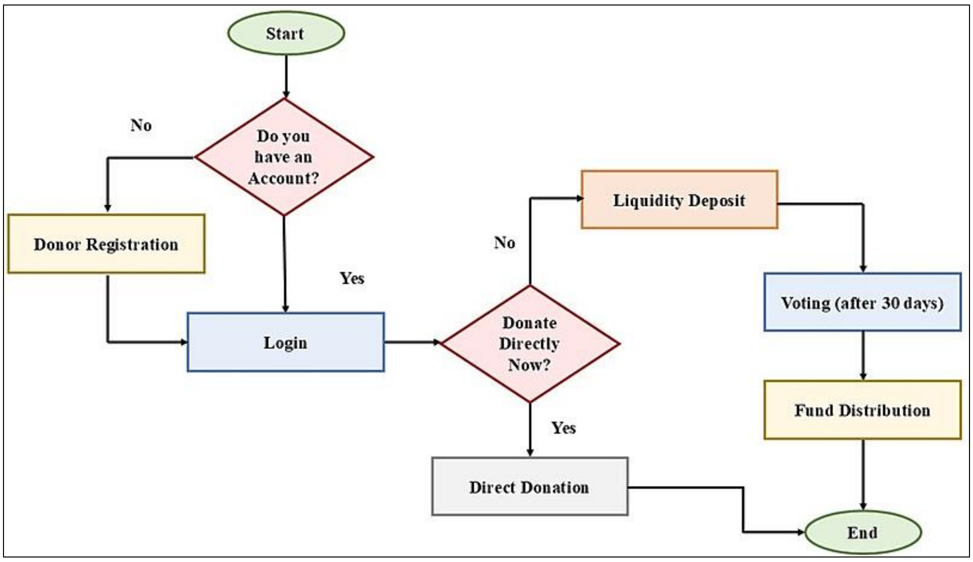
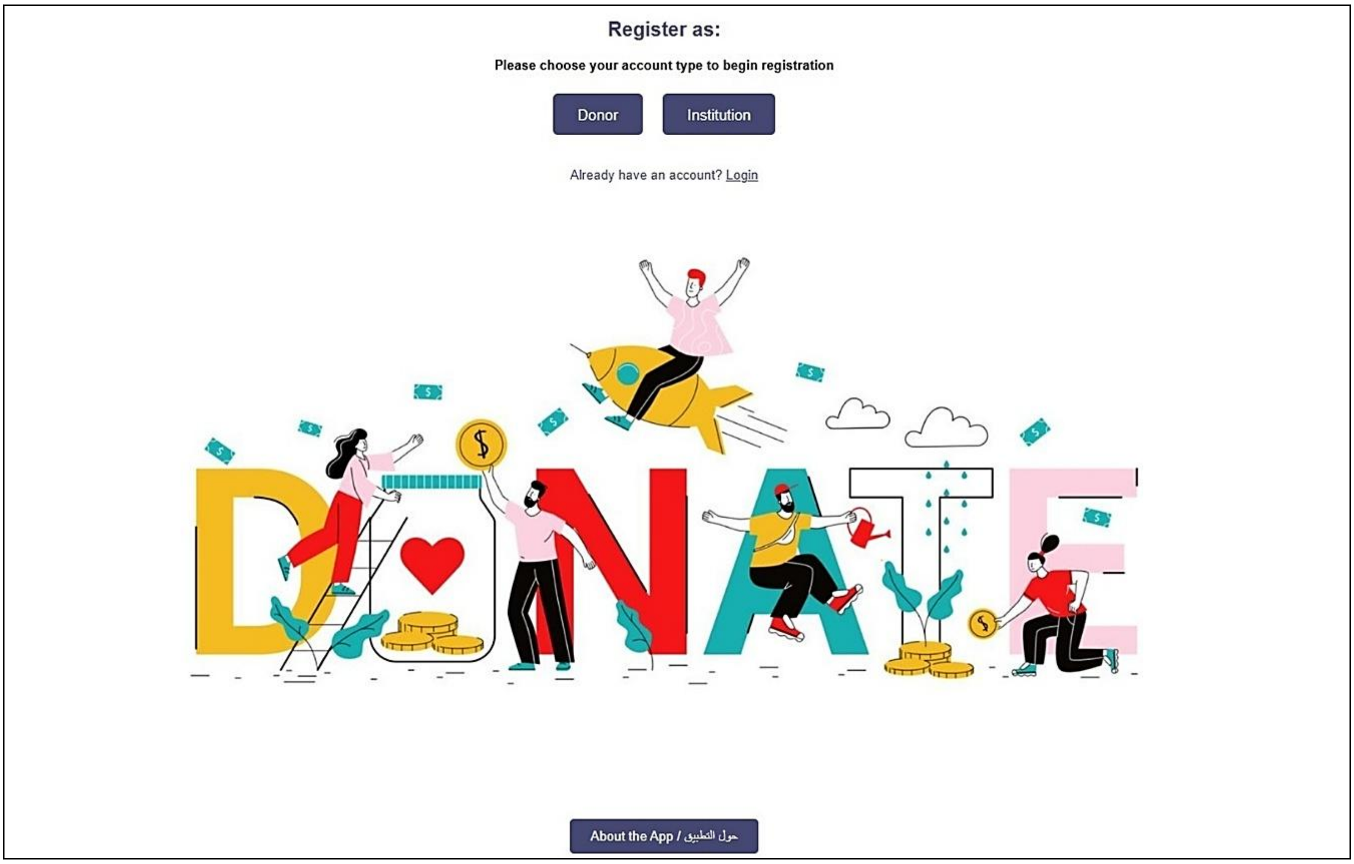


Fig 1: DeFiDonate methodology flowchart

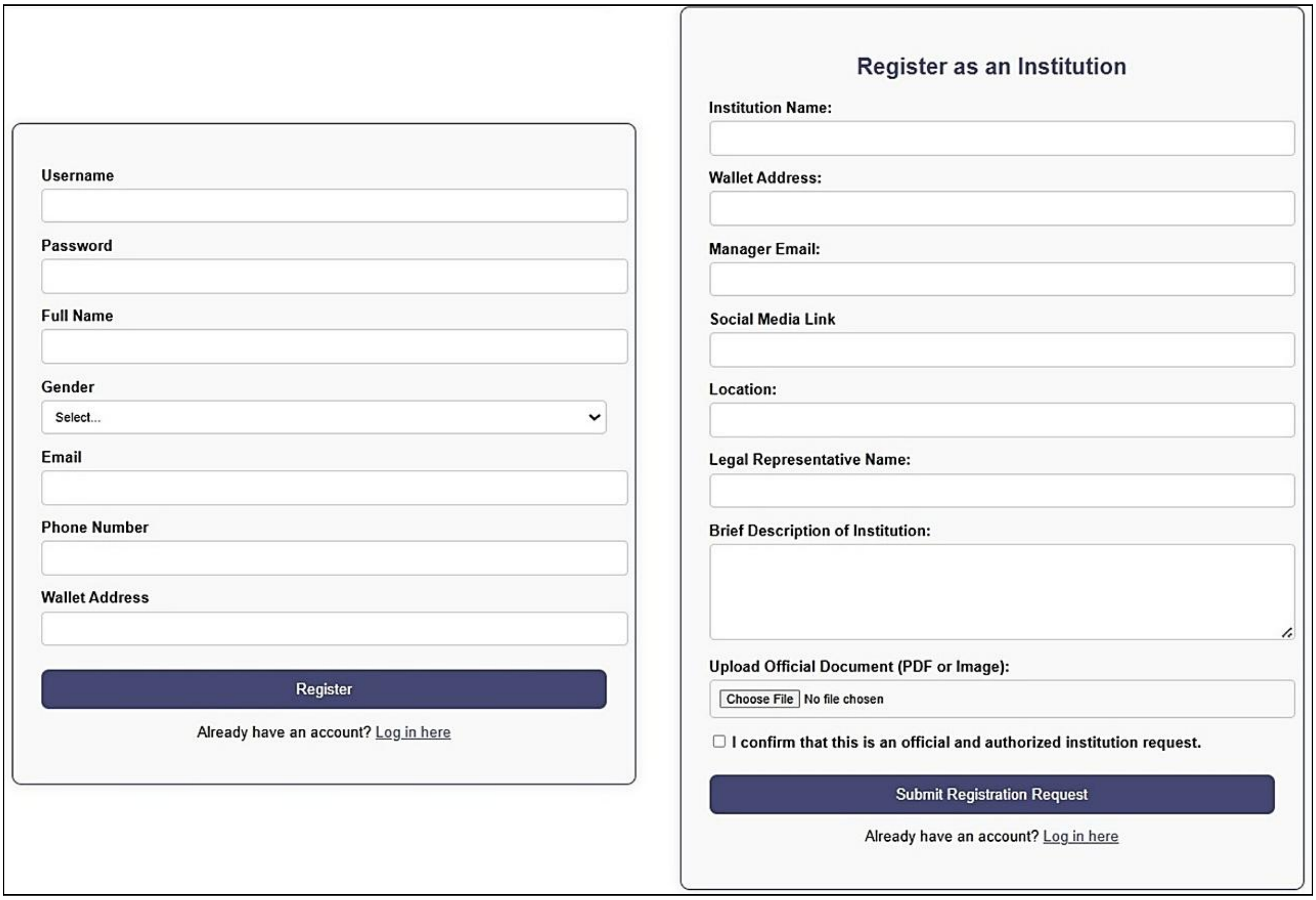


Register as:

Please choose your account type to begin registration

Already have an account? Login

Fig 2: DeFiDonate user registration interface



Username

Password

Full Name

Gender

Select...

Email

Phone Number

Wallet Address

Already have an account? Log in here

Register as an Institution

Institution Name:

Wallet Address:

Manager Email:

Social Media Link

Location:

Legal Representative Name:

Brief Description of Institution:

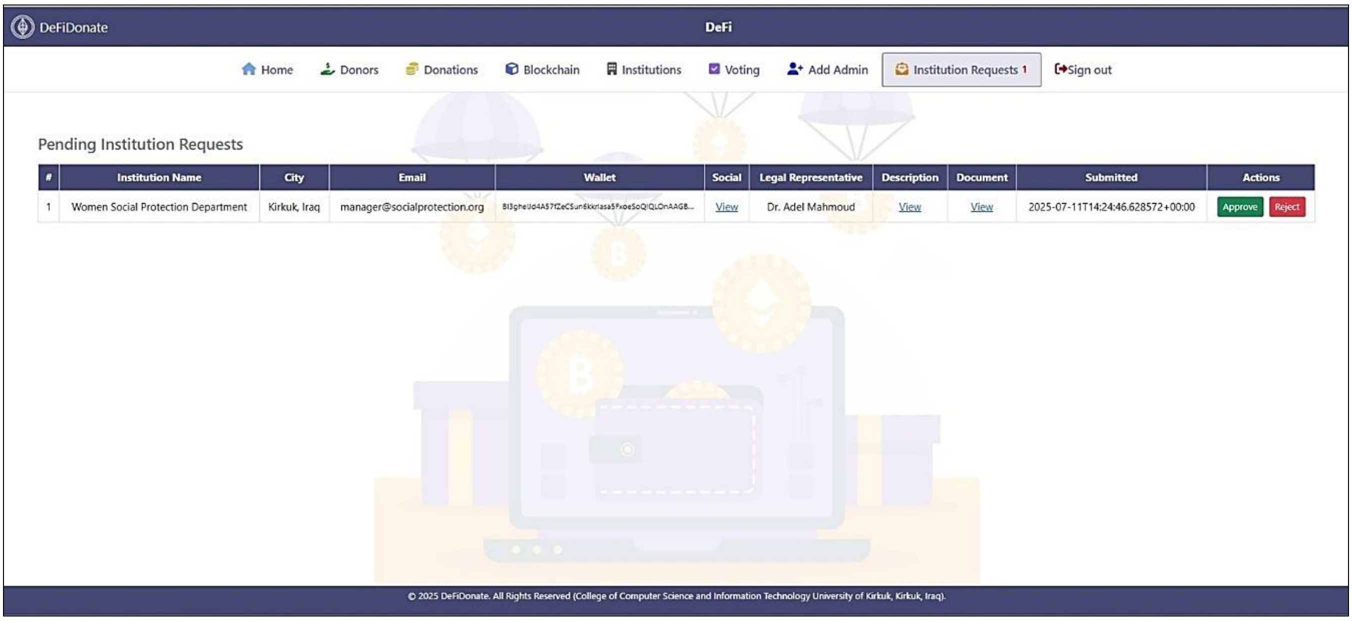
Upload Official Document (PDF or Image):

No file chosen

□ I confirm that this is an official and authorized institution request.

Already have an account? Log in here

Fig 3: Donor and institution registration form

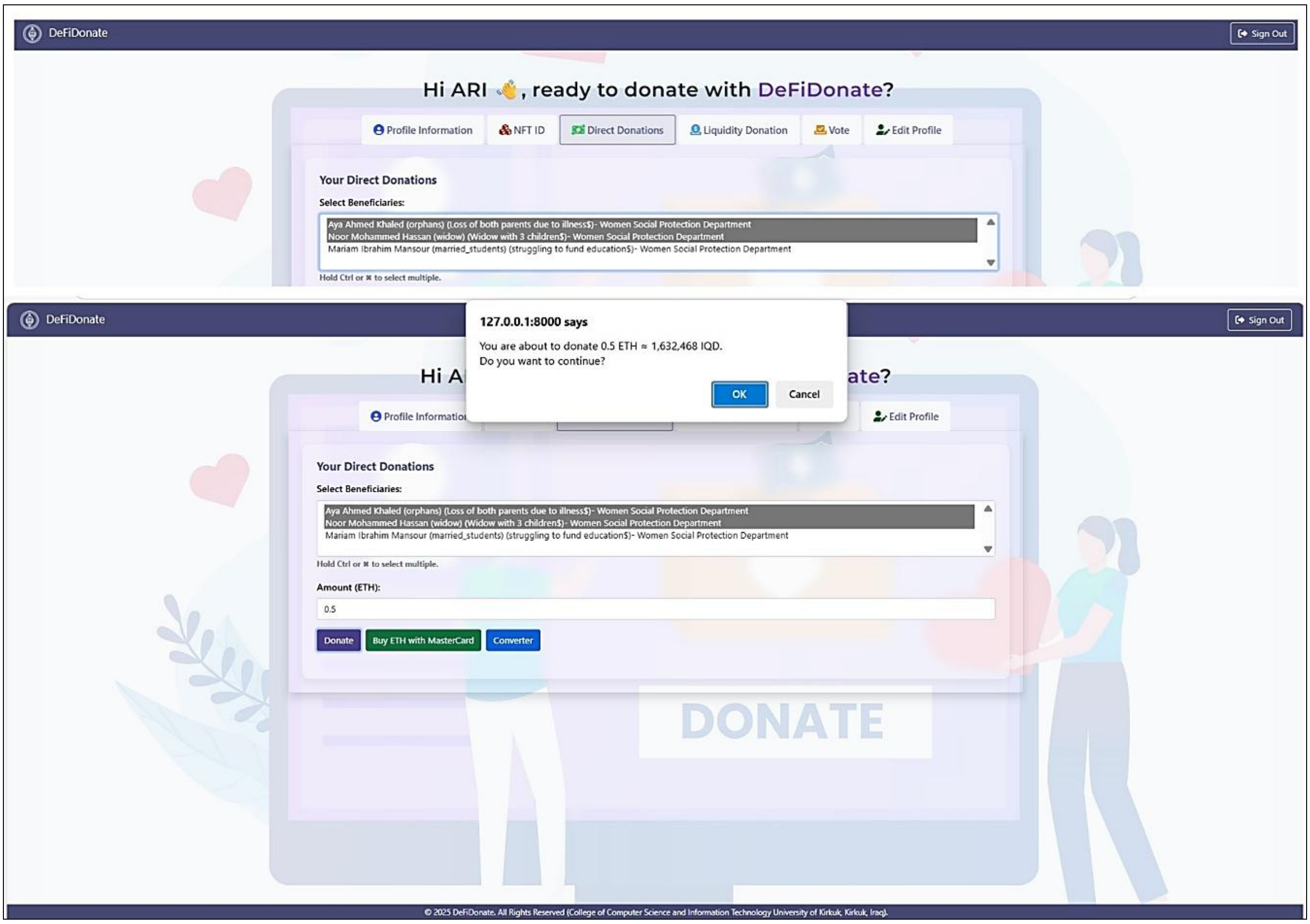


Pending Institution Requests

#	Institution Name	City	Email	Wallet	Social	Legal Representative	Description	Document	Submitted	Actions
1	Women Social Protection Department	Kirkuk, Iraq	manager@socialprotection.org	8I3gheUd4A57fZeCSun6kkrlasa5FxoeSoQIQLOnAAGB...	View	Dr. Adel Mahmoud	View	View	2025-07-11T14:24:46.628572+00:00	Approve Reject

© 2025 DeFiDonate. All Rights Reserved (College of Computer Science and Information Technology University of Kirkuk, Kirkuk, Iraq).

Fig 4: Admin site institution approval or reject



Hi ARI 👋, ready to donate with DeFiDonate?

Your Direct Donations

Select Beneficiaries:

Aya Ahmed Khaled (orphans) (Loss of both parents due to illness$)- Women Social Protection Department
Noor Mohammed Hassan (widow) (Widow with 3 children$)- Women Social Protection Department
Mariam Ibrahim Mansour (married_students) (struggling to fund education$)- Women Social Protection Department

Hold Ctrl or ⌘ to select multiple.

127.0.0.1:8000 says

You are about to donate 0.5 ETH ≈ 1,632,468 IQD.
Do you want to continue?

OK Cancel

Your Direct Donations

Select Beneficiaries:

Aya Ahmed Khaled (orphans) (Loss of both parents due to illness$)- Women Social Protection Department
Noor Mohammed Hassan (widow) (Widow with 3 children$)- Women Social Protection Department
Mariam Ibrahim Mansour (married_students) (struggling to fund education$)- Women Social Protection Department

Hold Ctrl or ⌘ to select multiple.

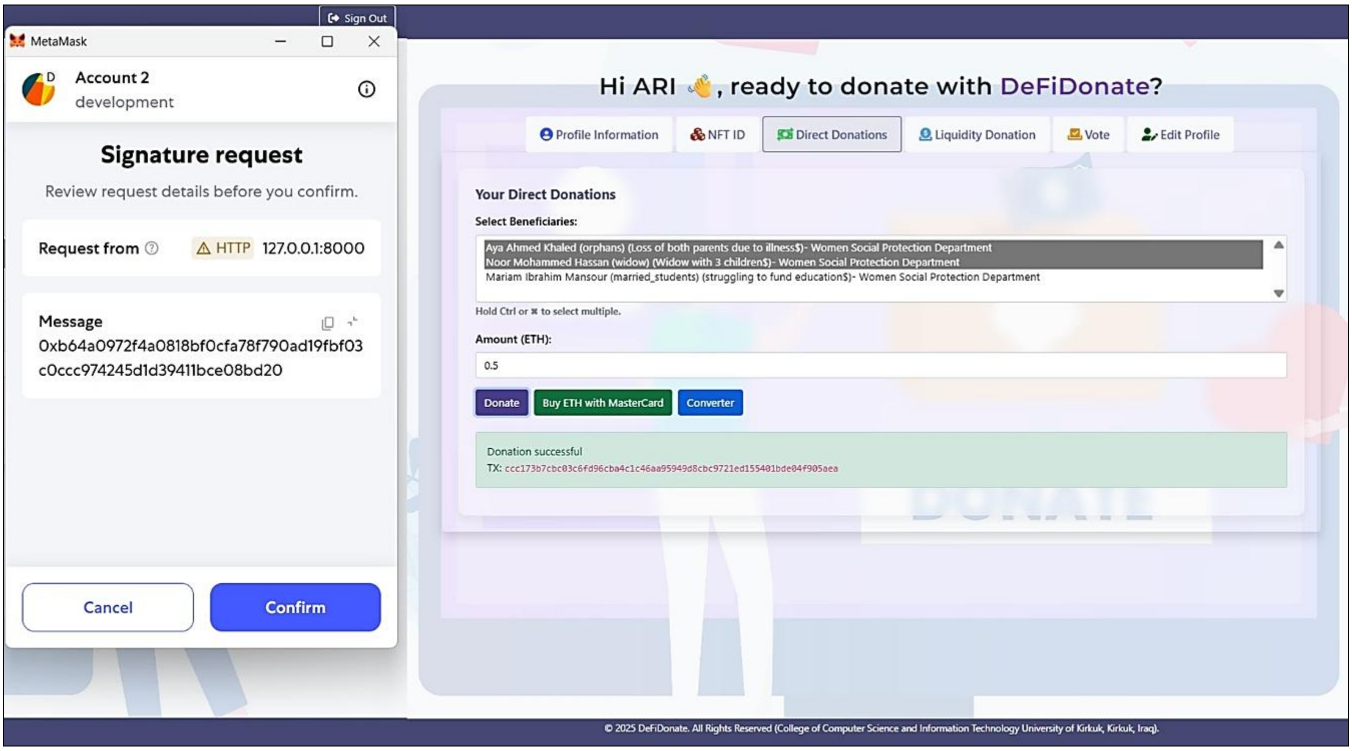
Amount (ETH):

0.5

Donate Buy ETH with MasterCard Converter

© 2025 DeFiDonate. All Rights Reserved (College of Computer Science and Information Technology University of Kirkuk, Kirkuk, Iraq).

Fig 5: Direct donation select beneficiary and confirmation



Account 2
development

Signature request

Review request details before you confirm.

Request from ⚠ HTTP 127.0.0.1:8000

Message
0xb64a0972f4a0818bf0cfa78f790ad19fbf03c0ccc974245d1d39411bce08bd20

Hi ARI 👋, ready to donate with DeFiDonate?

Your Direct Donations

Select Beneficiaries:

Aya Ahmed Khaled (orphans) (Loss of both parents due to illness$)- Women Social Protection Department
Noor Mohammed Hassan (widow) (Widow with 3 children$)- Women Social Protection Department
Mariam Ibrahim Mansour (married_students) (struggling to fund education$)- Women Social Protection Department

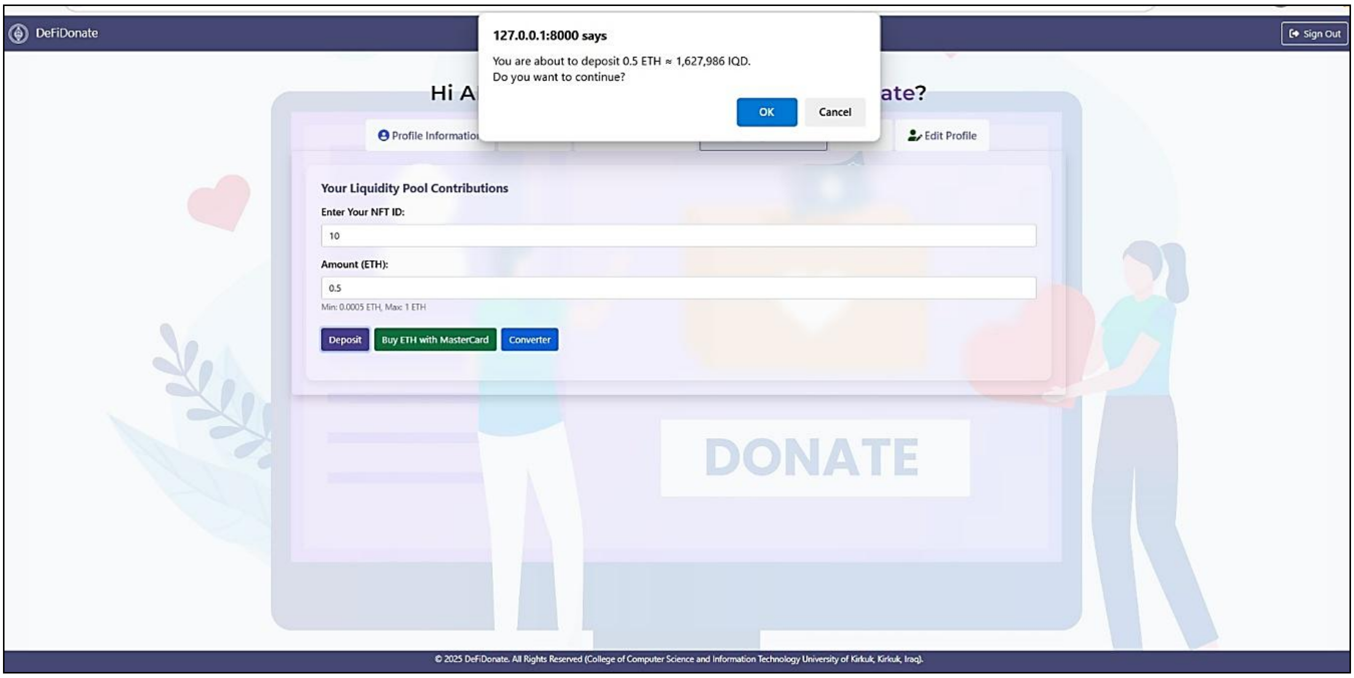
Hold Ctrl or ⌘ to select multiple.

Amount (ETH):
0.5

Donation successful
TX: ccc173b7cbc03c6fd96cba4c1c46aa95949d8cbc9721ed155401bde04f905aea

© 2025 DeFiDonate. All Rights Reserved (College of Computer Science and Information Technology University of Kirkuk, Kirkuk, Iraq).

Fig 6: Signature verification and success direct donation process



127.0.0.1:8000 says

You are about to deposit 0.5 ETH ≈ 1,627,986 IQD.
Do you want to continue?

Your Liquidity Pool Contributions

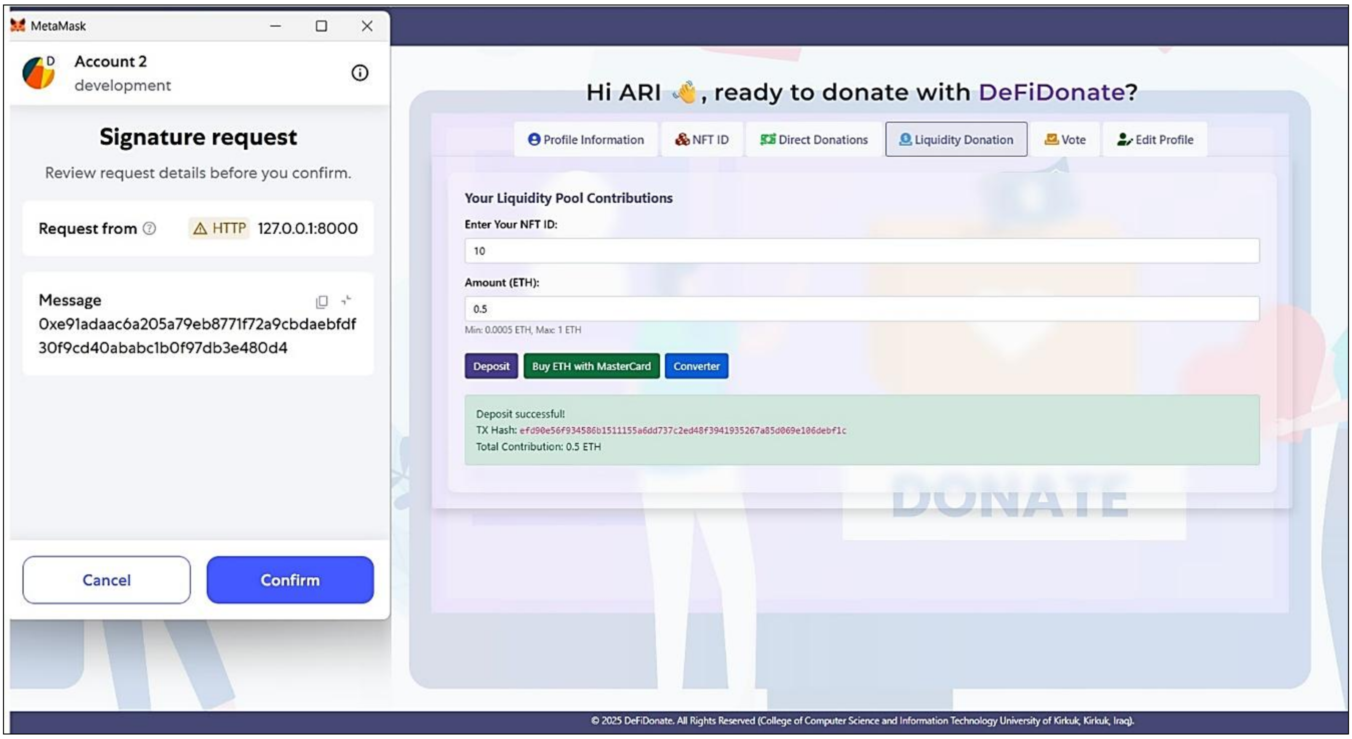
Enter Your NFT ID:
10

Amount (ETH):
0.5

Min: 0.0005 ETH, Max: 1 ETH

© 2025 DeFiDonate. All Rights Reserved (College of Computer Science and Information Technology University of Kirkuk, Kirkuk, Iraq).

Fig 7: Donor deposit funds in liquidity



MetaMask

Account 2
development

Signature request

Review request details before you confirm.

Request from ⚠ HTTP 127.0.0.1:8000

Message
0xe91adaac6a205a79eb8771f72a9cbdaebfdf30f9cd40ababc1b0f97db3e480d4

Hi ARI 👋, ready to donate with DeFiDonate?

Your Liquidity Pool Contributions

Enter Your NFT ID: 10

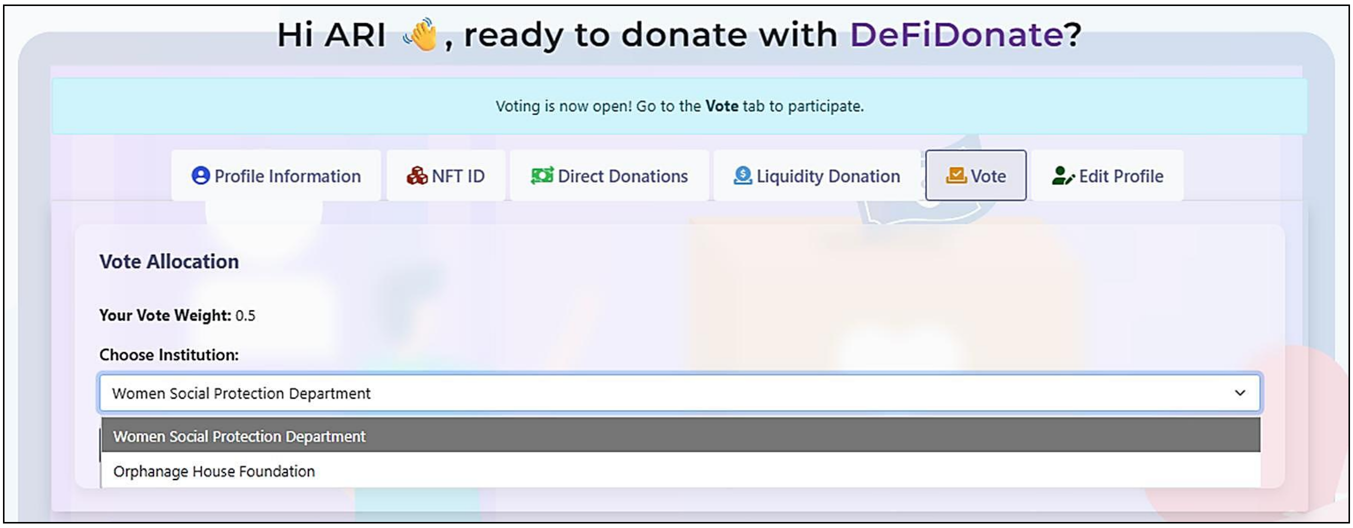
Amount (ETH): 0.5

Min: 0.0005 ETH, Max: 1 ETH

Deposit successful!
TX Hash: efd90e56f934586b1511155a6dd737c2ed48f3941935267a85d069e106debf1c
Total Contribution: 0.5 ETH

© 2025 DeFiDonate. All Rights Reserved (College of Computer Science and Information Technology University of Kirkuk, Kirkuk, Iraq).

Fig 8: Signature verification and success of the deposit operation



Hi ARI 👋, ready to donate with DeFiDonate?

Voting is now open! Go to the **Vote** tab to participate.

Vote Allocation

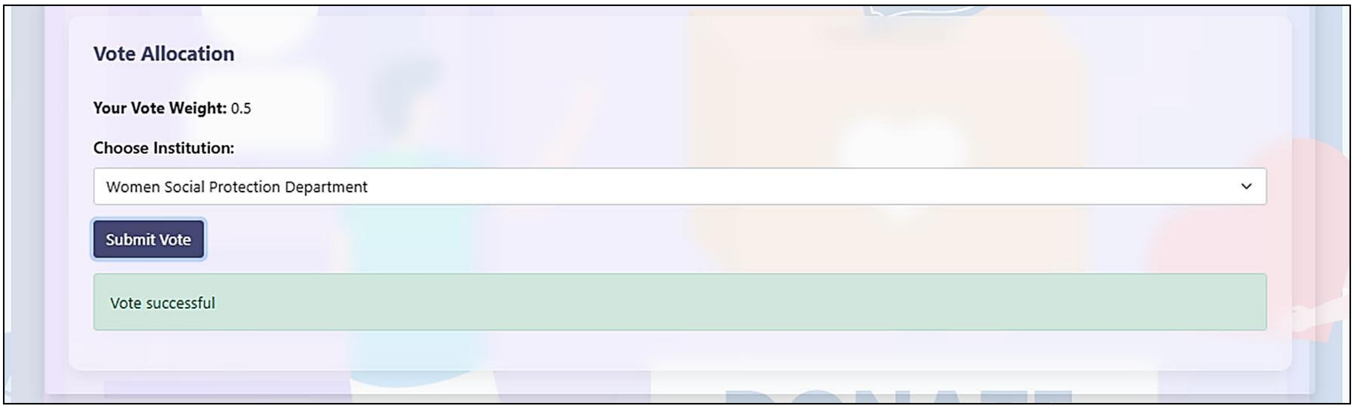
Your Vote Weight: 0.5

Choose Institution:

Women Social Protection Department

Women Social Protection Department
Orphanage House Foundation

A) Donor selecting vote option



Vote Allocation

Your Vote Weight: 0.5

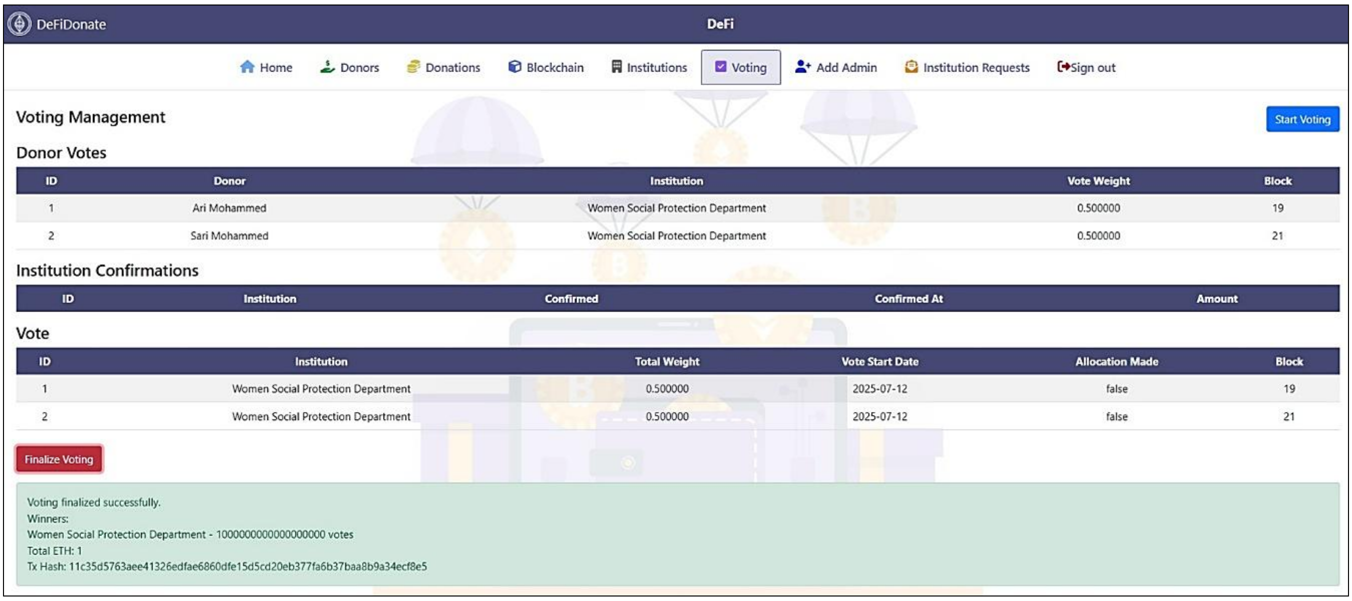
Choose Institution:

Women Social Protection Department

Vote successful

B) Donors vote confirmation and submit

Fig 1: Donor interface voting process



Voting Management

Donor Votes

ID	Donor	Institution	Vote Weight	Block
1	Ari Mohammed	Women Social Protection Department	0.500000	19
2	Sari Mohammed	Women Social Protection Department	0.500000	21

Institution Confirmations

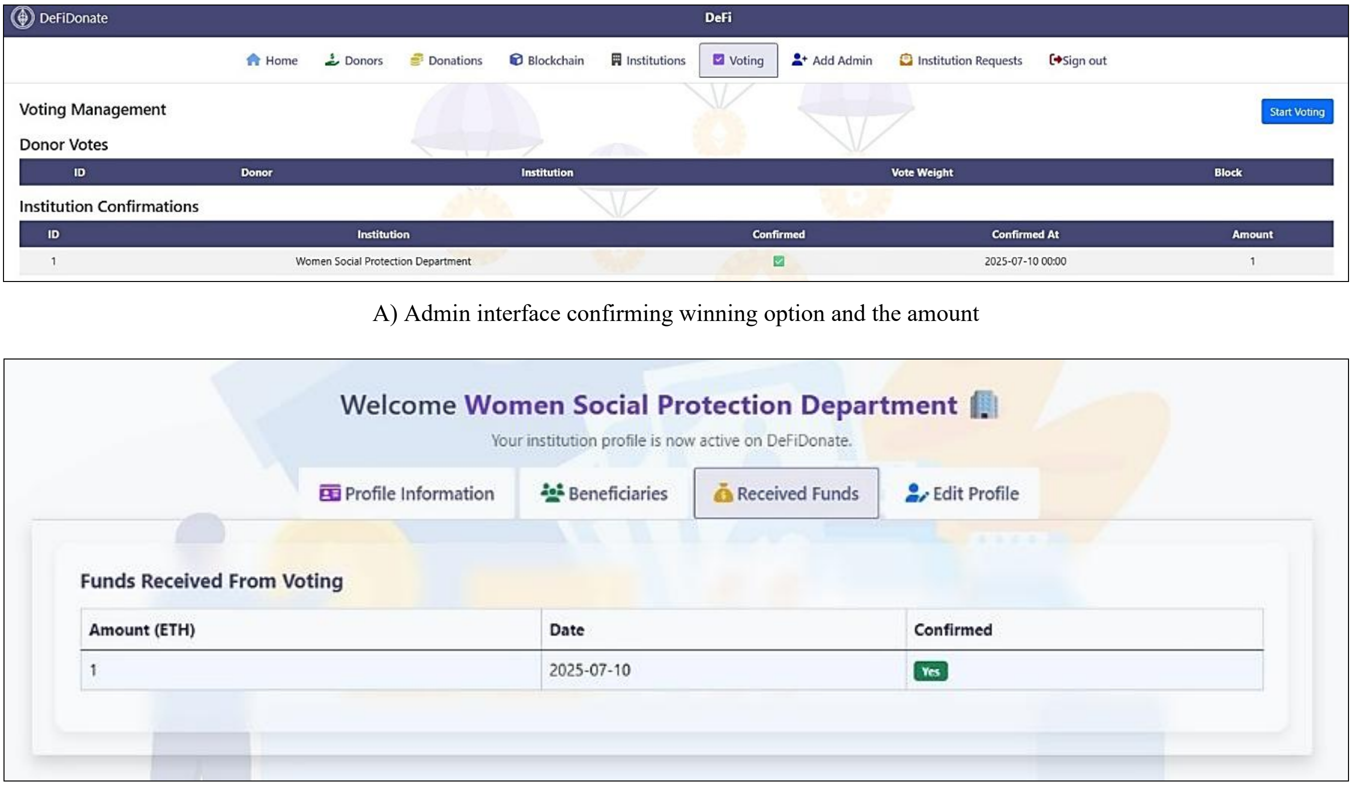
ID	Institution	Confirmed	Confirmed At	Amount

Vote

ID	Institution	Total Weight	Vote Start Date	Allocation Made	Block
1	Women Social Protection Department	0.500000	2025-07-12	false	19
2	Women Social Protection Department	0.500000	2025-07-12	false	21

```
Voting finalized successfully.
Winners:
Women Social Protection Department - 1000000000000000000 votes
Total ETH: 1
Tx Hash: 11c35d5763aee41326edfae6860dfe15d5cd20eb377fa6b37baa8b9a34ecf8e5
```

Fig 10: Admin interface finalize voting operation



Voting Management

Donor Votes

ID	Donor	Institution	Vote Weight	Block

Institution Confirmations

ID	Institution	Confirmed	Confirmed At	Amount
1	Women Social Protection Department	✓	2025-07-10 00:00	1

A) Admin interface confirming winning option and the amount

Welcome Women Social Protection Department

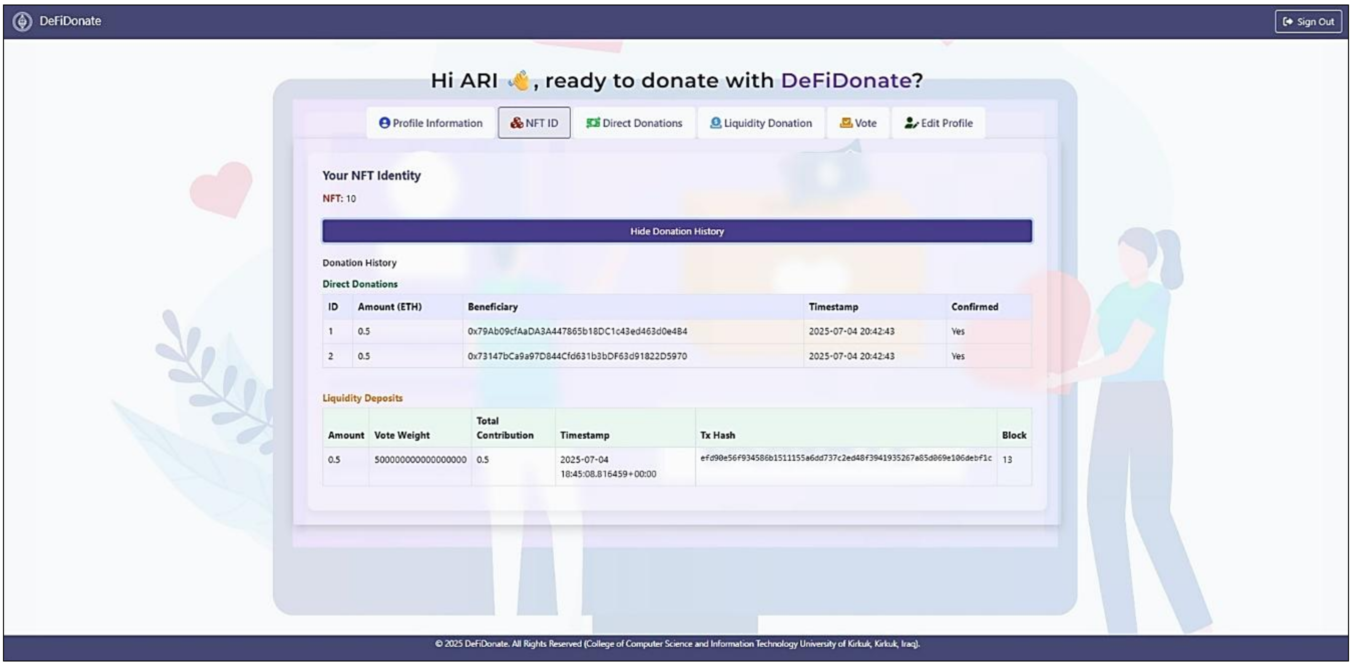
Your institution profile is now active on DeFiDonate.

Funds Received From Voting

Amount (ETH)	Date	Confirmed
1	2025-07-10	Yes

B) Institution profile interface confirming received funds

Fig 11: Confirmation of receipt of funds from both admin and institution interface



Hi ARI 👋, ready to donate with DeFiDonate?

Your NFT Identity

NFT: 10

Donation History

Direct Donations

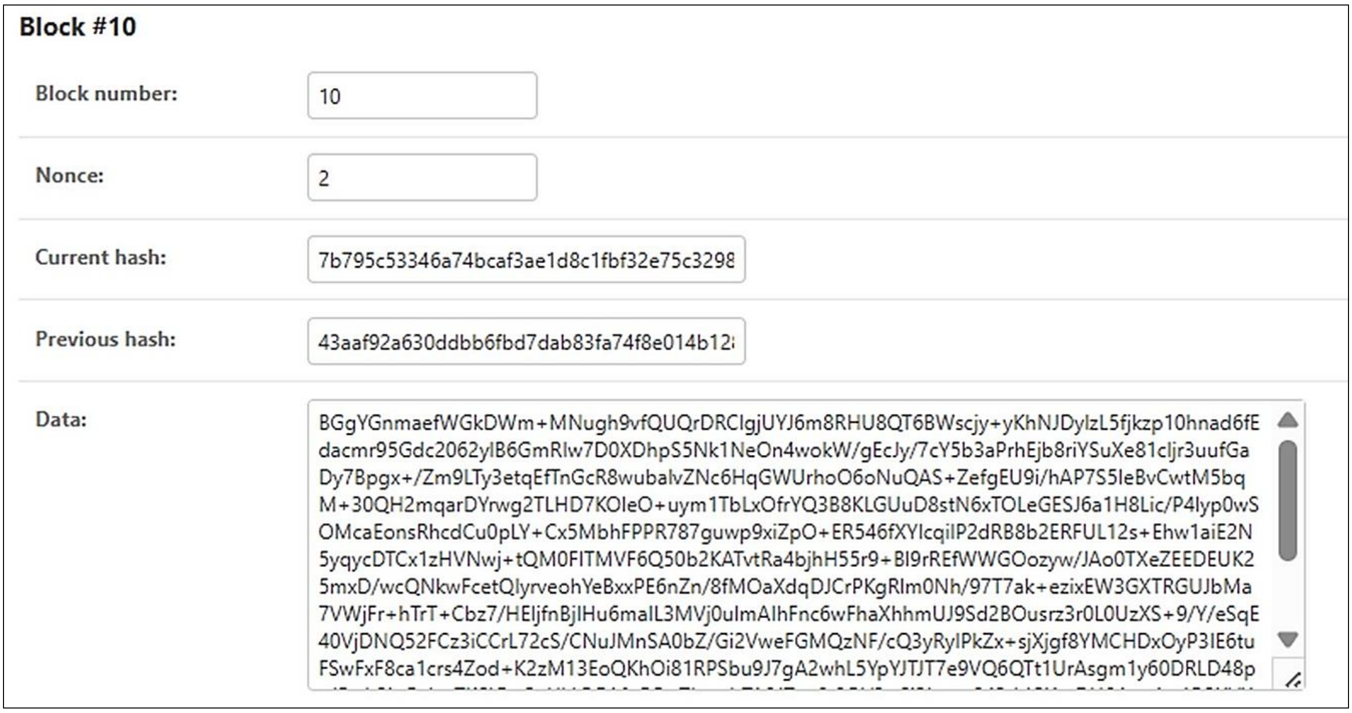
ID	Amount (ETH)	Beneficiary	Timestamp	Confirmed
1	0.5	0x79Ab09cfAaDA3A447865b18DC1c43ed463d0e4B4	2025-07-04 20:42:43	Yes
2	0.5	0x73147bCa9a97D844Cfd631b3bDF63d91822D5970	2025-07-04 20:42:43	Yes

Liquidity Deposits

Amount	Vote Weight	Total Contribution	Timestamp	Tx Hash	Block
0.5	500000000000000000	0.5	2025-07-04 18:45:08.816459+00:00	efd90e56f934586b1511155a6dd737c2ed48f3941935267a85d069e106debf1c	13

© 2025 DeFiDonate. All Rights Reserved (College of Computer Science and Information Technology University of Kirkuk, Kirkuk, Iraq).

Fig 12: NFT for editing donor history



Block #10

Block number: 10

Nonce: 2

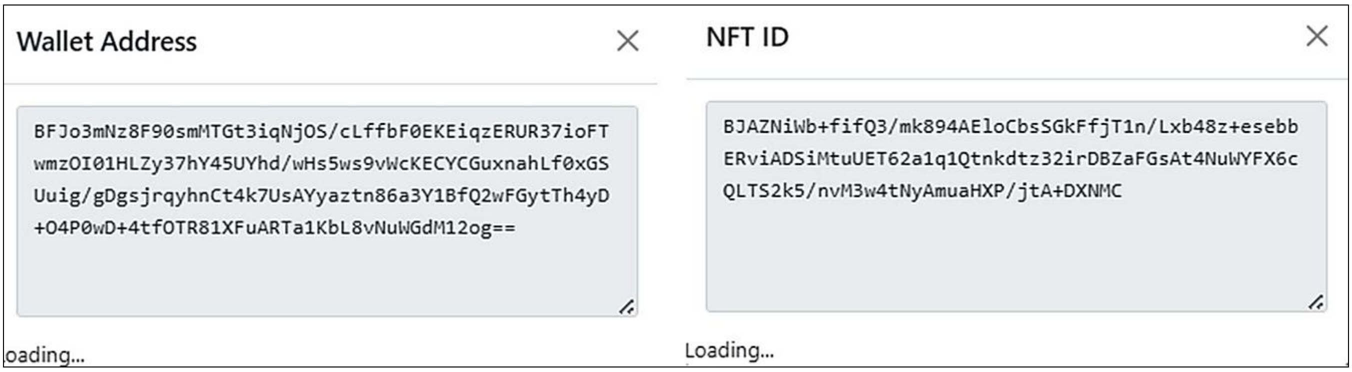
Current hash: 7b795c53346a74bcaf3ae1d8c1fbf32e75c3298

Previous hash: 43aaf92a630ddbb6fbd7dab83fa74f8e014b12

Data:

BGgYGnmaefWGkDWm+MNugh9vfQUQrDRCIgjUYJ6m8RHU8QT6BWscjy+yKhNJDylzL5fjkzp10hnad6fE
dacmr95Gdc2062ylB6GmRlw7D0XDhpS5Nk1NeOn4wokW/gEcJy/7cY5b3aPrhEjb8riYSuXe81cljr3uufGa
Dy7Bpgx+/Zm9LTy3etqEfTnGcR8wubalvZNc6HqGWUrhoO6oNuQAS+ZefgEU9i/hAP7S5leBvCwtM5bq
M+30QH2mqarDYrwg2TLHD7KOIeO+uym1TbLxOfrYQ3B8KLGUuD8stN6xTOLeGESJ6a1H8Lic/P4lyp0wS
OMcaEonsRhcdCu0pLY+Cx5MbhFPPR787guwp9xiZpO+ER546fXYIcqiIP2dRB8b2ERFUL12s+Ehw1aiE2N
5yqycDTCx1zHVNwj+tQM0FITMVF6Q50b2KATvtRa4bjhH55r9+BI9rREfWWGOozyw/JAo0TXeZEEDEUK2
5mxD/wcQNkwFcetQlyrveohYeBxxPE6nZn/8fMOaXdqDJCrPKgRIm0Nh/97T7ak+ezixEW3GXTRGUJbMa
7VWjFr+hTrT+Cbz7/HEljfnBjlHu6maIL3MVj0uImAIhFnc6wFhaXhhmUJ9Sd2BOusrz3r0L0UzXS+9/Y/eSqE
40VjDNQ52FCz3iCCrL72cS/CNuJMnSA0bZ/Gi2VweFGMQzNF/cQ3yRylPkZx+sjXjgf8YMCHDxOyP3IE6tu
FSwFxF8ca1crs4Zod+K2zM13EoQKhOi81RPSbu9J7gA2whL5YpYJTJT7e9VQ6QTt1UrAsgm1y60DRLD48p

Fig 13: Encrypted data in block



Wallet Address

BFJo3mNz8F90smMTGt3iqNjOS/cLffbF0EKEiqzERUR37ioFT
wmzOI01HLZy37hY45UYhd/wHs5ws9vWcKECYCGuxnahLf0xGS
Uuig/gDgsjrqyhnCt4k7UsAYyaztn86a3Y1BfQ2wFGytTh4yD
+O4P0wD+4tfOTR81XFuARTa1KbL8vNuWGdM12og==

oading...

NFT ID

BJAZNiWb+fifQ3/mk894AEloCbsSGkFfjT1n/Lxb48z+esebb
ERviADSiMtuUET62a1q1Qtnkdtz32irDBZaFGsAt4NuWYFX6c
QLTS2k5/nvM3w4tNyAmuaHXP/jtA+DXNMC

Loading...

Fig 14: Encrypted wallet address and NFT

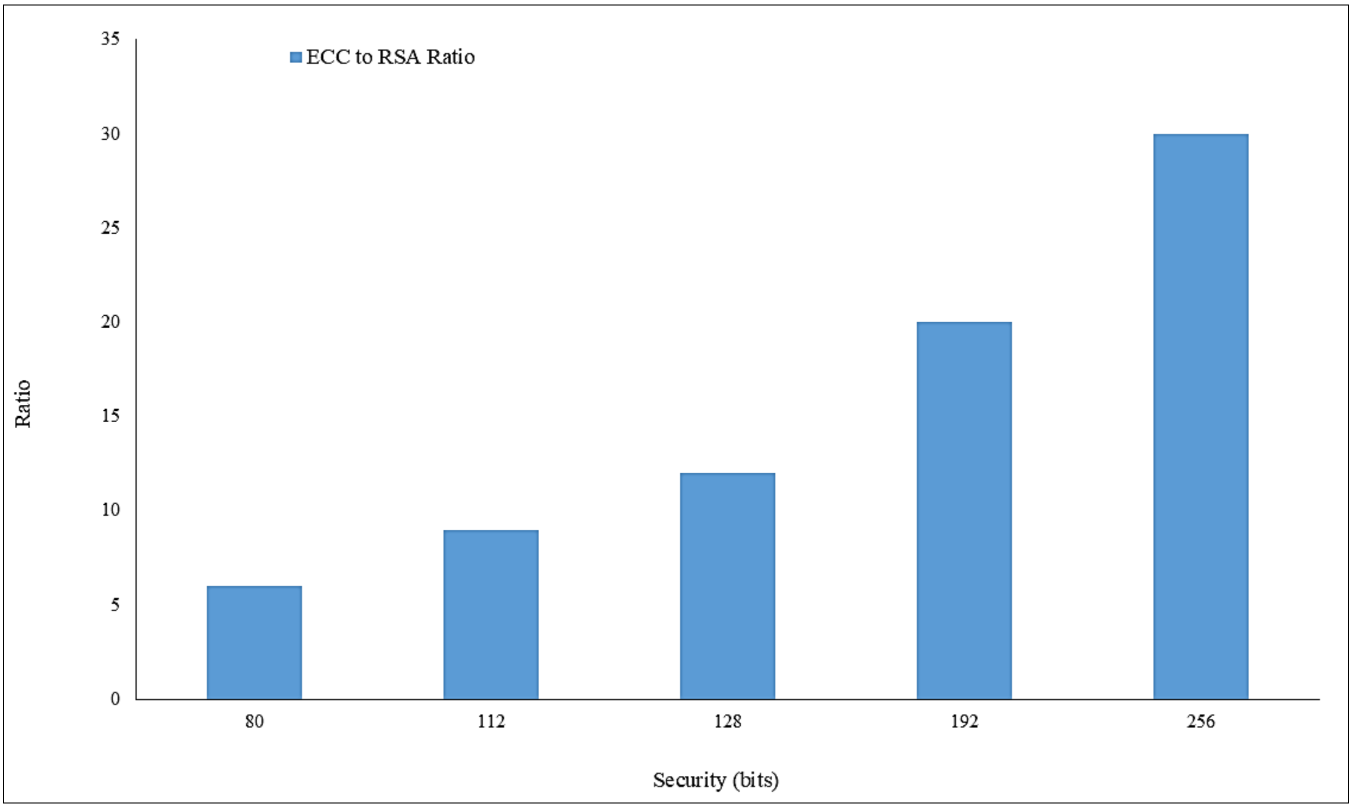


Fig 15: Key size vs security level [36]

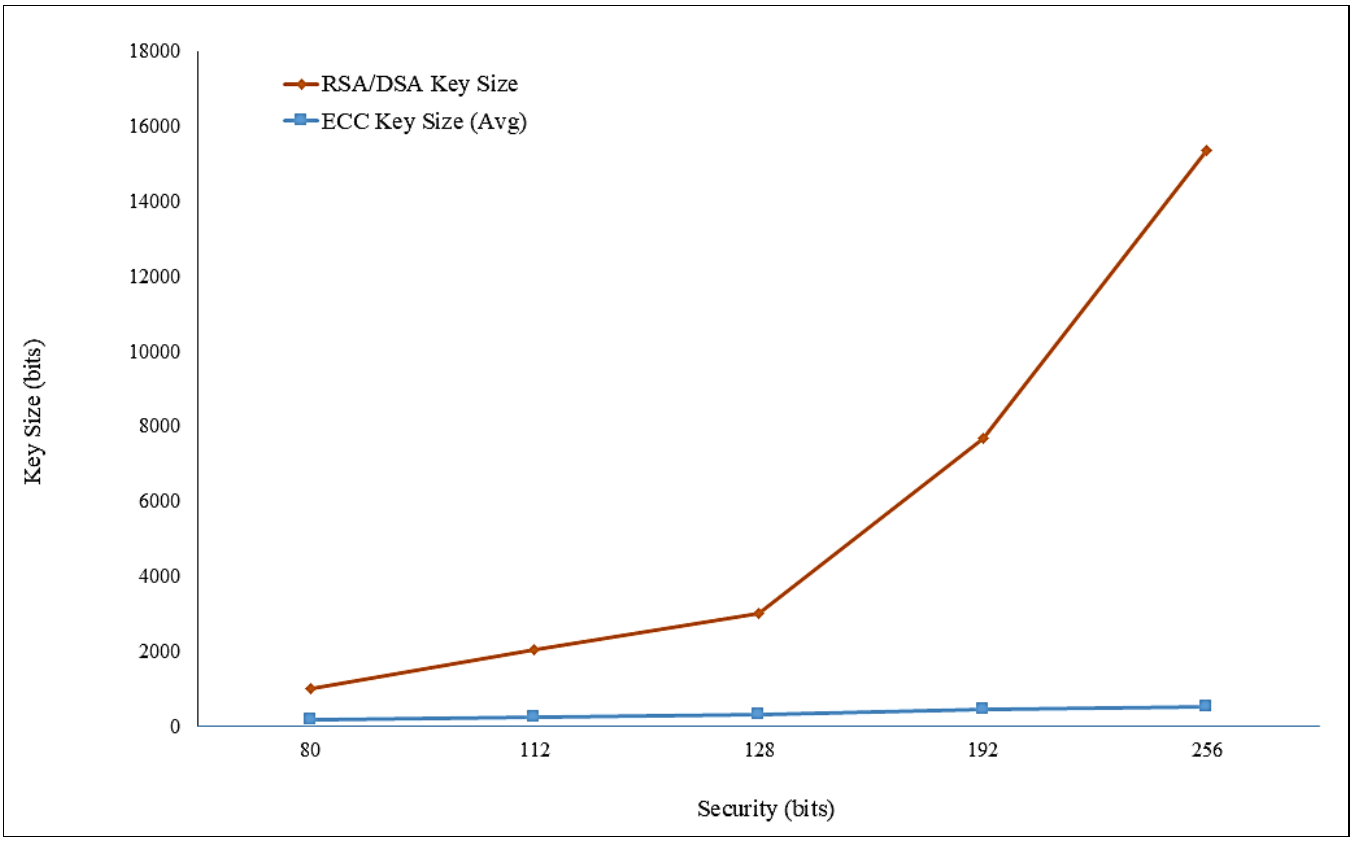


Fig 16: ECC to RSA Ratio vs Security [36]

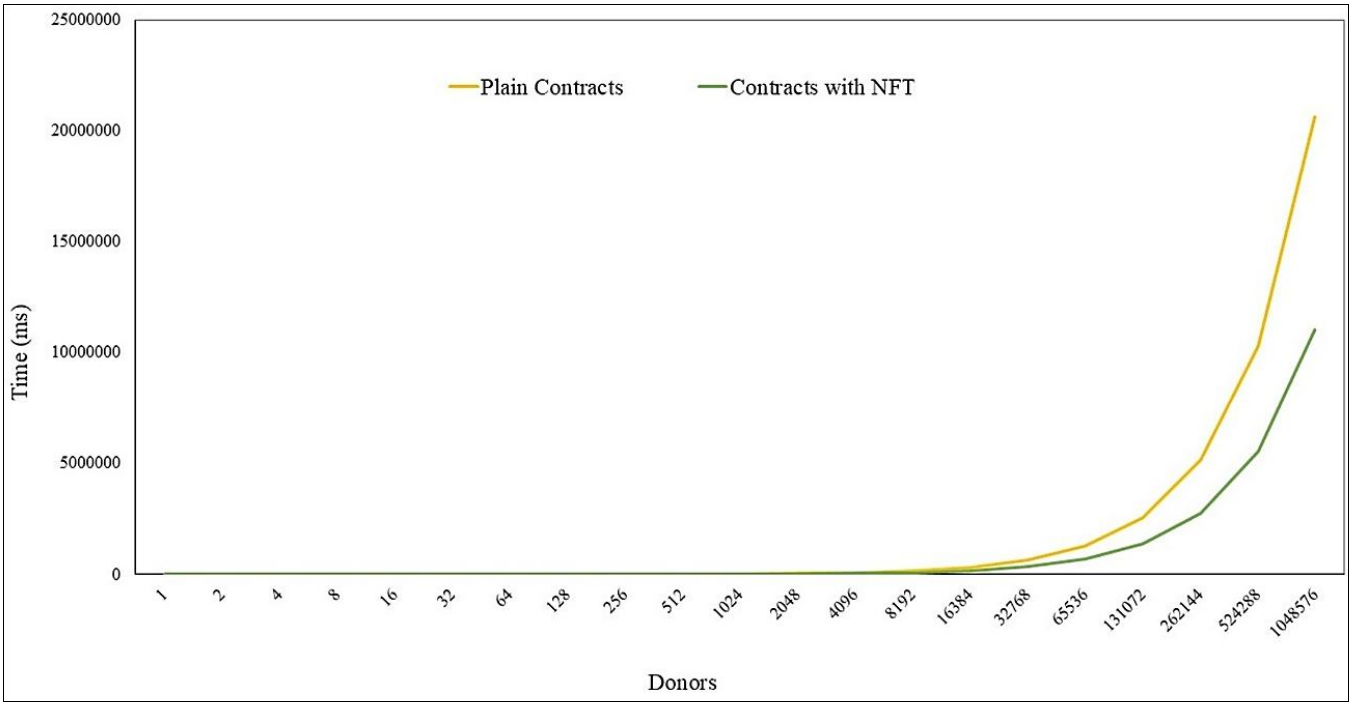


Fig 17: Time consumption for donor registration

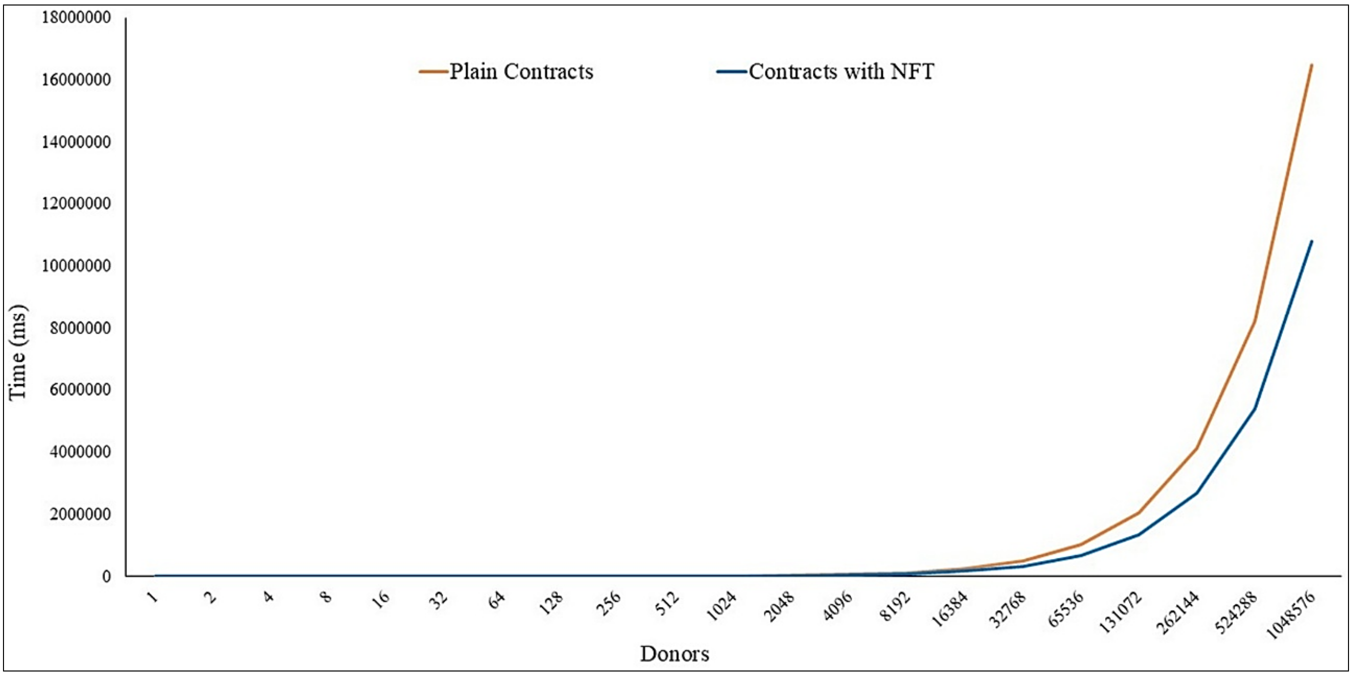


Fig 18: Time consumption of direct donation

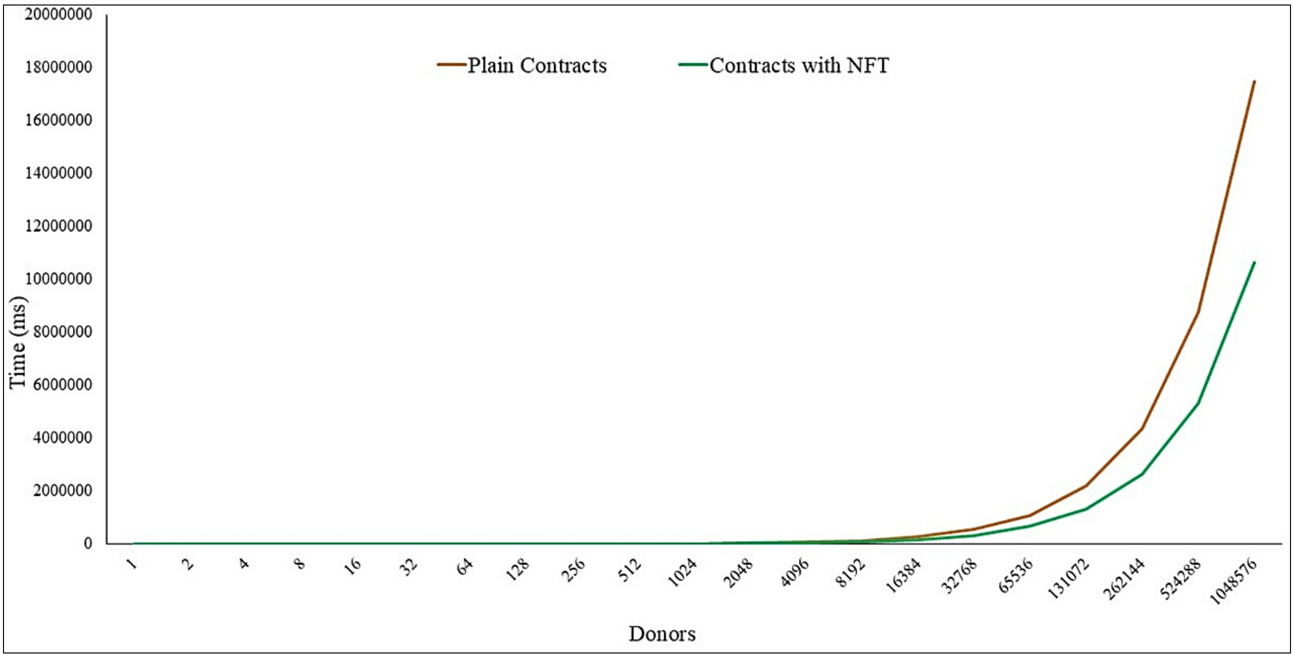


Fig 19: Liquidity deposit time consumption

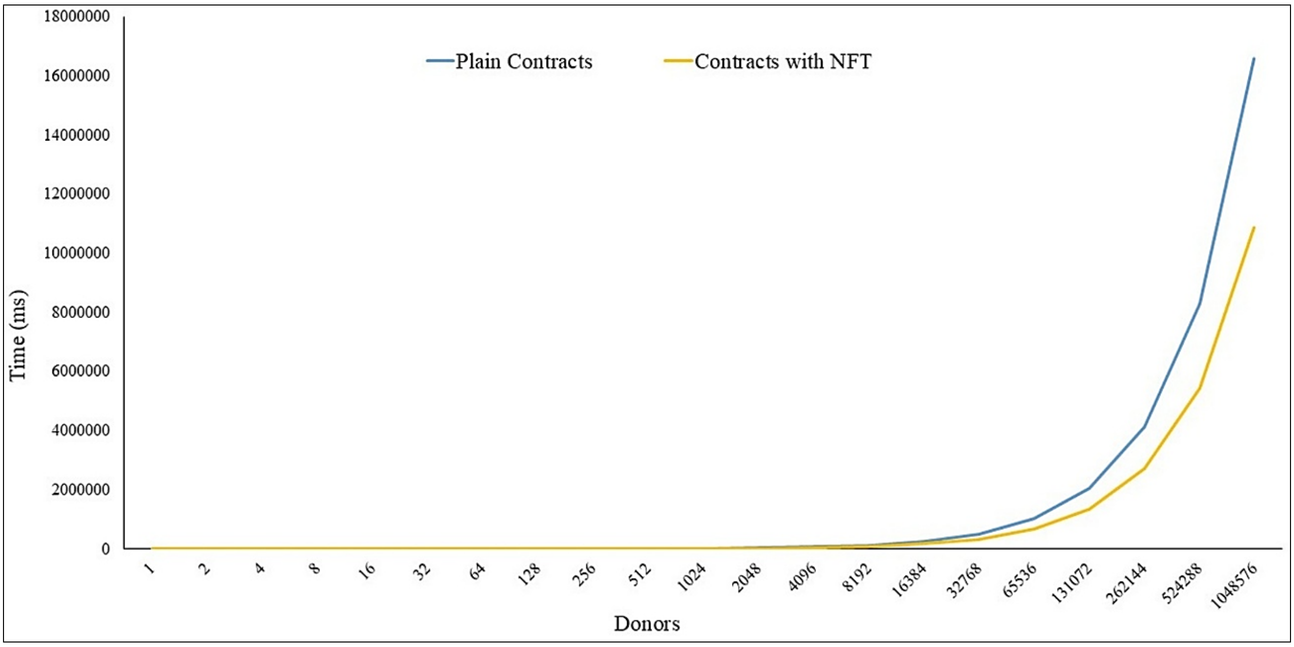


Fig 20: Voting time consumption

Conclusion

The study proposed a decentralized web application for donations via DeFiDonate, which securely and transparently processes donations on the Ethereum blockchain utilizing ECC, smart contracts, ECDSA, and NFTs by playing a significant role in addressing the problems associated with conventional donation sites, including untrustworthy environments, centralization, and data security concerns, where the donation process can be made directly or into a liquidity pool, then distributing the funds through a voting mechanism based on the contribution made by donors, which avoids bias and centralization; security procedures, such as privacy, are achieved by encrypting sensitive information and ensuring authenticity through the verification of a digital signature. Comparing it to other blockchain-based donation solutions, it offers a high degree of traceability and transparency, as well as flexibility in its operations, since its construction, development, and testing it using local Ethereum with Truffle, Ganache, and MetaMask; as the employing of NFTs showed that the processing time execution within is reduced when testing them locally in Truffle Develop. Finally, future development can proceed from this research by combining Layer-2 services to improve scalability, or by adding other fiat-to-crypto gateways and utilizing mobile application support to ensure greater access and reduce costs.

References

1. Almaghrabi A, Alhogail A. Blockchain-based donations traceability framework. J King Saud Univ Comput Inf Sci. 2022;34(10):9442-9454.
2. Proceedings of the 4th International Conference on Trends in Electronics and Informatics (ICOEI); 2020. IEEE; 2020.

3. Nairi C, Cicioğlu M, Çalhan A. Smart blockchain networks: revolutionizing donation tracking in Web 3.0.
4. Shaheen E, Hamed MA, Zaghloul W, Al Mostafa E, El Sharkawy A, Mahmoud A, *et al*. A track donation system using blockchain. In: 2nd IEEE International Conference on Electronic Engineering (ICEEM 2021). IEEE; 2021.
5. Kareem A, Shakir AC. Review: verification process of academic certificates using blockchain technology. Kirkuk Univ J Sci Stud. 2023;18(1):62-75.
6. Katya E, Rahman SR. Blockchain-based decentralized finance (DeFi) applications peer review information. Int J Adv Comput Eng Commun Technol.; 2024.
7. Ahmed I, Fumimoto K, Nakano T, Tran TH. Blockchain-empowered decentralized philanthropic charity for social good. Sustainability. 2024;16(1).
8. Meeradevi, Sowmya BJ, Nikisha K, Kushal S, Sadarangani VH, Vishal RK, *et al*. Blockchain-powered charity integrity system. In: International Conference on Emerging Technologies in Computer Science for Interdisciplinary Applications (ICETCS 2024). IEEE; 2024.
9. Tunçer S, Özdede A. Transparent donation management with smart contract-based blockchain. Available from: https://orcid.org/0000-0003-0569-098X
10. Acharya B, Lazzaro D, Cinà AE, Holz T. Pirates of charity: exploring donation-based abuses in social media platforms; 2024 Dec 20. Available from: http://arxiv.org/abs/2412.15621
11. Srivatsa A, Rai H, Kumar Srivastava A, Rai S, Pattanashetti D. Blockchain-powered transparency: tracking and disseminating donations for disaster-stricken regions.
12. Swati J, Nitin P, Saurabh P, Parikshit D, Gitesh P, Rahul S. Blockchain-based trusted secure philanthropy platform: Crypto-GoCharity. In: 6th International Conference on Computing, Communication, Control and Automation (ICCUBEA 2022). IEEE; 2022.
13. Segeda I, Kotsiuba V, Shushura O, Bokovets V, Koval N, Kalizhanova A. Decentralized platform for financing charity projects. Informatyka Automatyka Pomiary Gospod Ochr Srodowiska. 2024;14(3):129-134.
14. He B, Feng T, Fang J, Liu C, Su C. A secure and efficient charitable donation system based on Ethereum blockchain and searchable encryption. IEEE Trans Consum Electron. 2024;70(1):263-276.
15. Jumaa MH, Shakir AC. Review study of e-voting system based on smart contracts using blockchain technology. Iraqi J Sci. 2023;64(4):2001-2022.
16. Ahmed MM, Shakir AC. Review study: blockchain application in payroll system. Al-Kitab J Pure Sci. 2023;7(1):83-99.
17. Yadav N, Sarasvathi V. Venturing crowdfunding using smart contracts in blockchain. In: Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology (ICSSIT 2020). IEEE; c2020, p. 192-197.
18. Singh R, Gupta A, Mittal P. A systematic literature review on blockchain-based smart contracts: platforms, applications, and challenges. Distrib Ledger Technol Res Pract.; 2024 Nov 19. Available from: https://dl.acm.org/doi/10.1145/3704741
19. Migliorini S, Gambini M, Belussi A. A blockchain-based platform for ensuring provenance and traceability of donations for cultural heritage. Blockchain Res Appl.; 2025 Mar;100278. Available from: https://linkinghub.elsevier.com/retrieve/pii/S2096720925000053
20. Xue Y, Fan D, Su S, Fu J, Hu N, Liu W, *et al*. A review on the security of the Ethereum-based DeFi ecosystem. Comput Model Eng Sci. 2023;139:69-101.
21. Teng H, Tian W, Wang H, Yang Z. Applications of the decentralized finance (DeFi) on the Ethereum. In: IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC 2022). IEEE; c2022. p. 573-578.
22. Shah K, Lathiya D, Lukhi N, Parmar K, Sanghvi H. A systematic review of decentralized finance protocols. Int J Intell Netw. 2023;4:171-181.
23. Harvey CR, Hasbrouck J, Saleh F. The Wharton Initiative on Financial Policy and Regulation: the evolution of decentralized exchange: risks, benefits, and oversight.
24. Razi Q, Devrani A, Abhyankar H, Chalapathi GSS, Hassija V, Guizani M. Non-fungible tokens (NFTs): survey of current applications, evolution, and future directions. IEEE Open J Commun Soc. 2024;5:2765-2791.
25. Kim H, Kim HS, Park YS. Perpetual contract NFT as collateral for DeFi composability. IEEE Access. 2022;10:126802-126814.
26. Semnani A, Yang G. Non-Fungible Tokens (NFTs) beyond collectibles: a comprehensive review of applications.
27. Mathur G. GANACHE: a robust framework for efficient and secure storage of data on private Ethereum blockchains; 2023. Available from: https://www.researchsquare.com/article/rs-3495549/v1
28. Bansal K. Blockchain and IoMT-adopting SDN for patient-centric management and remote patient monitoring powered by 5G technology. Int J Commun Inf Technol. 2024;5(2):110-121.
29. Yan Y. The overview of elliptic curve cryptography (ECC). J Phys Conf Ser.; 2022.
30. Jumaa MH, Shakir AC. Iraqi e-voting system based on smart contract using private blockchain technology. Informatica (Slovenia). 2022;46(6):87-94.
31. Yang W. ECC, RSA, and DSA analogies in applied mathematics. Proc SPIE. 2022;138.
32. Guruprakash J, Koppu S. An empirical study to demonstrate that EdDSA can be used as a performance improvement alternative to ECDSA in blockchain and IoT. Informatica (Slovenia). 2022;46(2):277-290.
33. Alhaj AA, Alrabea A, Jawabreh OAA, Jawabreh O. Efficient and secure data transmission: Cryptography techniques using ECC. Indones J Electr Eng Comput Sci. 2024;36(1):1.
34. Groth J, Dfinity VS. Design and analysis of a distributed ECDSA signing service; 2023. Available from: https://eprint.iacr.org
35. Shayea GG, Mohammed DA, Abbas AH, Abdulsattar NF. Privacy-aware secure routing through elliptical curve cryptography with optimal RSU distribution in VANETs. Designs (Basel). 2022;6(6).