

Charity System using Blockchain Technology

Rhythm Negi¹, Blessy Thomas², Prajka Ghorpade³, Ammu Attiyil⁴, Prof. Y. I. Jinesh Melvin⁵

^{1,2,3,4} UG Student, Dept. of Computer Engineering, Pillai College of Engineering, New Panvel, India

⁵ Assisstant Professor, Dept. of Computer Engineering, Pillai College of Engineering, New Panvel, India

Abstract - Charities in our nation are opaque and difficult to oversee, which has a detrimental influence on people's desire to give. When determining whether or not to donate money to charity organizations, many people question if their gift will make a difference. Many nonprofit organizations have shattered people's faith in generosity and called into doubt the authenticity of charitable projects by participating in shady practices to increase cash. Transparency is a major concern in today's charity industry. Blockchain [1] and smart contracts [2] create new prospects for charity by converting aid into digital assets and increasing confidence in nonprofit organizations. Donors can now track the effect of their gifts, and organizations can utilize crypto tokens [4] to motivate donation.

Key Words: Ethereum, Smart contract, Blockchain, charity, digital ledger, transparency.

1. INTRODUCTION

Charity is a critical part of a democratic society. It is well known that numerous situations occur in this world that result in catastrophic loss. The archaic system had a number of flaws, including a lack of transparency, donor distrust, and corruption.

We aimed to tackle the following main issues with current charity platforms:

Security: As the funds become larger, they must be more secure. Although strict procedures such as symmetric encryption are in place to keep e-payments safe and secure, they are still subject to hackers. Blockchain [1] can give that degree of security since it has never been hacked. Transparency and anti-fraud measures: We have witnessed and continue to witness many crowdfunding frauds. There is no method to track how the monies are spent. We intended to make the whole flow of cash visible at every level so that no money could be misappropriated.

Global contribution: Because certain platforms are country-specific, it might be difficult for people from different nations to participate to various initiatives. Anyone in the globe may contribute to the campaign via blockchain. Transactions are quick and easy.

We were exceptionally motivated by the CryptoRelief drive, which raised ~1 billion dollars for Covid Relief in

India from the whole worldwide society in a profoundly straightforward way.

2. LITERATURE SURVEY

A. Blockchain: A ledger is an organized and stored collection of data, particularly electronic data, for the purposes of accounting, retrieval, processing, and control. A distributed ledger is a data structure that may be used to bring an uncommitted collection of copies to a final consistent state (eventual consistency) via a consensus mechanism.

A distributed ledger is implemented using blockchain technology. Blockchain is a network of complete nodes (participants) that individually carry data. After reaching an agreement among network participants, fresh data is inserted. Data is immutable, transparent, and secure with blockchain.[1]

B. Smart Contract: A smart contract is a contract between two or more parties. Smart contracts allow business logic to be implemented on a blockchain that can be monitored. Smart contracts are value streams that are bound by certain terms and conditions. Smart contracts, unlike traditional contracts, are entirely digital, consisting of pre-programmed code recorded on the blockchain. A smart contract can do computations, store data, and move money to other accounts automatically. A new smart contract can be hosted on the blockchain by using a transaction in which the sender becomes the smart contract owner. The self-destruct function is another function that can be defined in a smart contract. In most circumstances, the smart contract owner is the only one who may use this function to delete the contract.[2]

C. Ethereum: Rizal Mohd Nor proposed to use blockchain technology to manage the assistance funds in disaster areas and establish the entire platform on Ethereum. The method is software-based, and it establishes transparency and trust through smart contracts with pre-programmed milestones for each philanthropic cause.[3]

D. Cryptocurrency-tokens: Cryptocurrency is a sort of digital currency that uses cryptographic technologies to issue and govern its units. We obtained virtual Ethereum tokens for donation and expenditure using Ethereum's Ropsten test network. The Ropsten network has a simple access point in Infura. With the MetaMask wallet, we can store Ethereum tokens and conduct transactions with them.[4]

2.1 Summary of Literature Survey

SN	Paper	Advantages and Disadvantages
1.	Hadi Saleh, Sergey Avdoshin, Azamat Dzhonov[1]	Advantages: Verifiable: Everyone will be able to track the donations. Disadvantages: i) Costly ii) Unsustainable.
2.	P. Agarwal, S. Jalan, A. Mustafi [2]	Advantages: i) In its decentralized system, a third party is not required. (Organization, Group, Individual) ii) No risk of hacking and fraud. Disadvantages: i) Expensive
3.	A. Mehra, A. Jain, S. Singanamalla, S. Lokam, M. Sivathanu, J. O'Neill [3]	Advantages: i) Transparency ii) Secure Disadvantages: i) unsustainable

3. PROPOSED WORK

Any web-based application is a centralized application which means that anything we do on the platform is managed by a server that is owned by a single company.

In our project we are proposing a Decentralized Application for charity funding in which there are two main categories- the campaign creators and donors. With the help of Ethereum Blockchain the information about all the transactions is secured on a blockchain network. Blockchain has a series of blocks which holds funds and transactions and as a result, it does not permit the money to end up in the hands of anyone and minimizes all potentials of it being mishandled.

3.1 Proposed Architecture

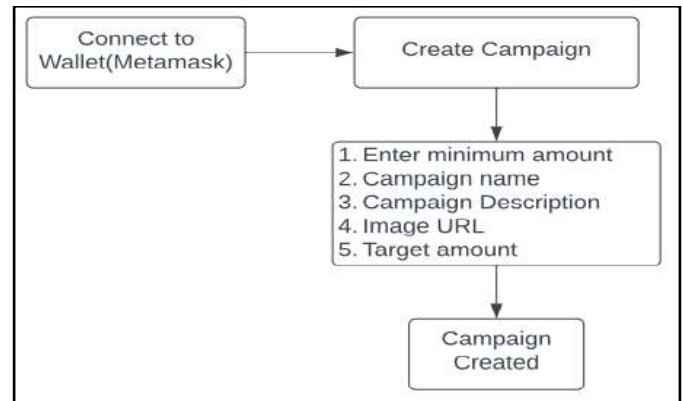


Fig 3.1(a) Creating a Campaign



Fig 3.1(b) Donating to a Campaign

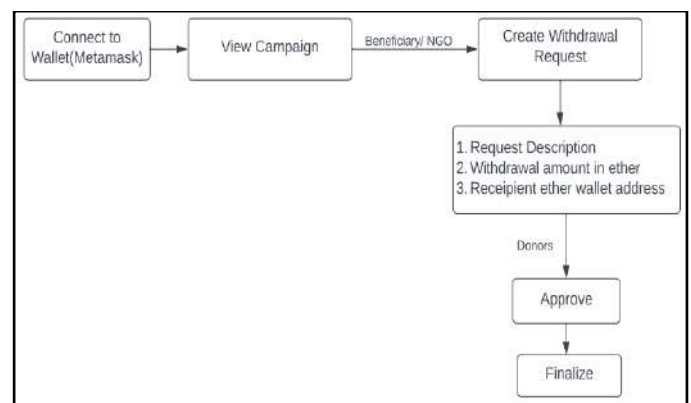


Fig 3.1(c) Withdrawal of Funds

(a) Creating a Campaign

For initiating a charity funding or to donate in an existing campaign, to perform these transfers, a client is first required to associate to the site their Ethereum wallet. Metamask, a browser extension, is used to integrate the wallet, which can be utilized to approve exchanges for digital currency. Any client whose wallet has been associated with the application can add to a mission. The client is just required to choose the mission, enter the contribution sum they want to donate, and afterward approve the exchange (for this situation, allowing it via Metamask). The mission data will be overseen by the smart contract which is Ethereum-based and as a result cannot be accessed maliciously.

(b) Donating to a Campaign

Clients with successful integration of wallet to the charity can donate the funds. The steps are easy with detailed instructions in the diagram given. The client needs to input the donation sum in their choice of campaign. Next step is to give consent for the transaction using Metamask. After the approval, assets will go directly to the campaign's wallet address. The creator of the campaign will not receive the funds in their wallet, This safeguard makes this process more streamlined and keeps it safe from unauthorized access.

(c) Withdrawal of Funds

The Maker of a Campaign can propose involving the assets as a Withdrawal Solicitation. Anyone who offers over a specific sum is called an approver and will have a choice to support or deny the solicitation.

Assuming you are the Campaign maker, you could have to pull out from the accessible funds for different reasons. You can make a Withdrawal Solicitation, as shown in the diagram given. More than half of the Approvers must endorse the request to approve it.

Taking into consideration, if you are a Donor who has offered more than the base donation amount specified, then, at that point, you are an approver. You can decide on the withdrawal demands made by the Maker and either support or deny the solicitation.

Neither the Donor nor the Maker can remove the funds without the endorsement of the majority of the approvers.

There is complete clarity in the flow of withdrawal of funds. Approvers will be able to track the status of their contributions. Any responsibility thereafter will not fall on the Maker as they are not the arbitrator in transferring funds.

3.2. Requirement Analysis

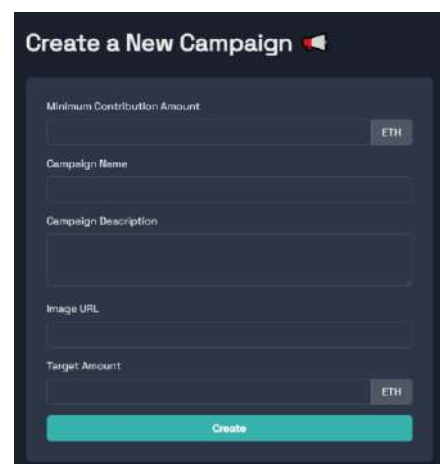
A. Software

- 1. NextJS:** Next.js is an open-source React front-end development web framework that allows React-based web apps to perform server-side rendering and generate static websites.
- 2. Chakra UI:** Chakra UI is a component toolkit that provides the building blocks needed to create React apps in a straightforward, modular, and accessible way.
- 3. Solidity:** It is the programming language for implementing Ethereum based Smart Contracts.
- 4. Web3:** web3.js is a bunch of libraries that enables one to use HTTP, IPC, or WebSocket to intercommunicate with a nearby or far off Ethereum node.

- 5. Ethereum Smart Contract:** It's a collection of functions and data stored at a specific Ethereum Blockchain address.

B. Hardware

Operating system	Windows / Linux / macOS
Processor	i3 or Higher
RAM	4GB(Minimum)
HDD	80GB



4. IMPLEMENTATION

Fig 4 (a) Creating Campaign

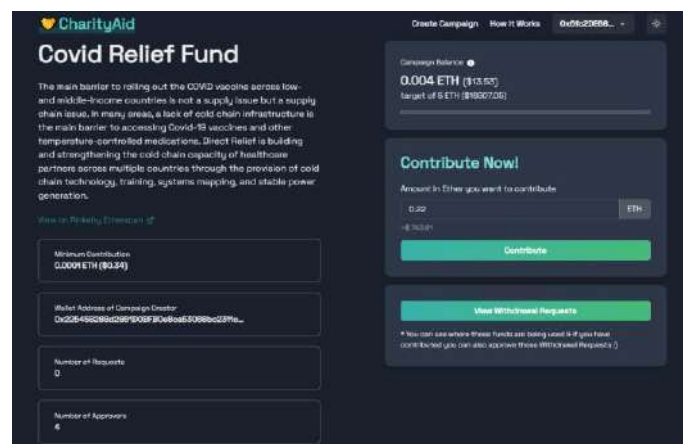


Fig 4 (b) Campaign description

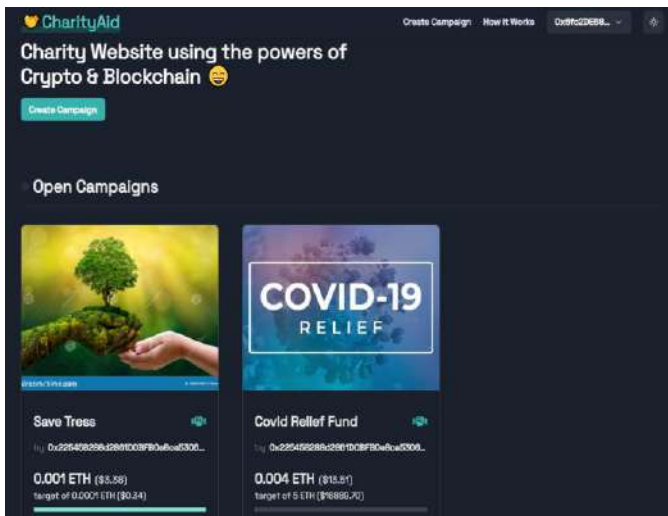


Fig 4 (c) HomePage

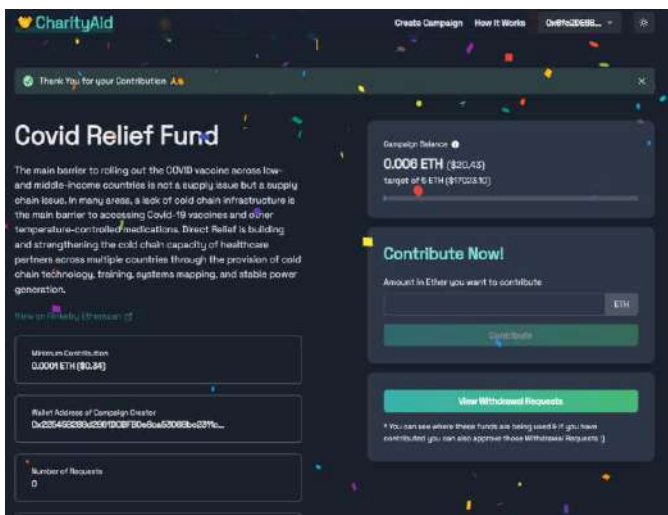


Fig 4 (d) Successful Donation

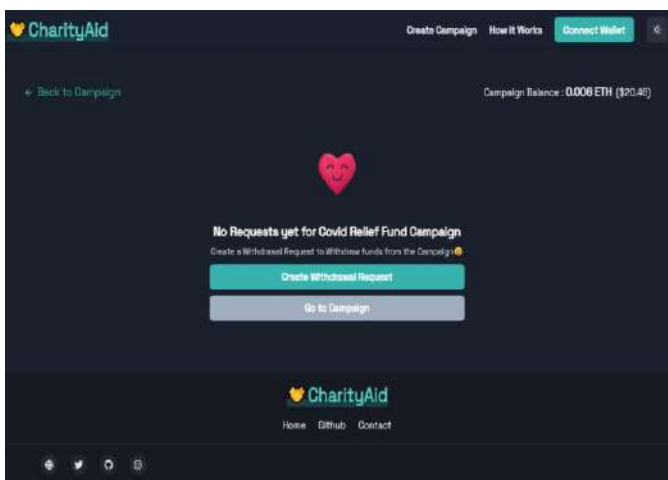


Fig 4 (e) Creating Withdrawal Request

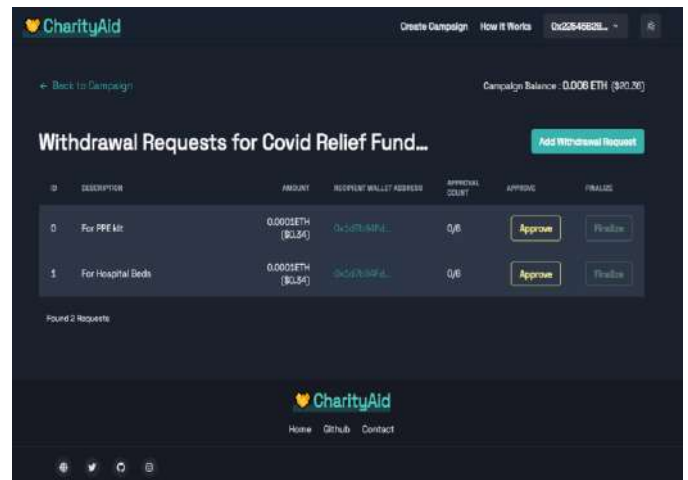


Fig 4 (f) Withdrawal Requests

5. CONCLUSIONS

Considering India's present charity framework, low straightforwardness, data security, trust issues among individuals, and issues related to the fake foundation have become problem areas that should be tended to right away. This paper offered a novel approach to utilizing blockchain innovation to revolutionize this Charity framework. Our proposed resolution was set in motion to make a start-to-finish vigorous and a platform for decentralized foundations.

ACKNOWLEDGEMENT

It is our pleasure to offer our heartfelt gratitude to our guide, Prof. Y. I. Jinesh Melvin, for his excellent contribution, capable leadership, encouragement, wholehearted collaboration, and constructive criticism during the period of this endeavor. We would like to express our heartfelt gratitude to Dr. Sharvari Govilkar, Head of Department, and Dr. Sandeep M. Joshi, Principal, for encouraging us and enabling us to share our work.

REFERENCES

- [1] Saleh, H., Avdoshin, S., & Dzhonov, A. (2019, November). Platform for tracking donations of charitable foundations based on blockchain technology. In 2019 Actual Problems of Systems and Software Engineering (APSSE) (pp. 182-187). IEEE.
- [2] Agarwal, P., Jalan, S., & Mustafi, A. (2018, February). Decentralized and financial approach to effective charity. In 2018 International Conference on Soft-computing and Network Security (ICSNS) (pp. 1-3). IEEE.

- [3] Mehra, A., Lokam, S., Jain, A., Sivathanu, M., Singanamalla, S., & O'Neill, J. (2018, April). Vishrambh: Trusted philanthropy with end-to-end transparency. In *HCI for Blockchain: a CHI 2018 Workshop on Studying, Critiquing, Designing and Envisioning Distributed Ledger Technologies*, Montreal, QC, Canada.
- [4] YILDIRIM, İ., & Şahin, E. E. (2018). Insurance Technologies (Insurtech): Blockchain and Its Possible Impact on Turkish Insurance Sector. *Journal of International Management Educational and Economics Perspectives*, 6(3), 13-22.
- [5] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE.
- [6] Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3), 2084-2123.
- [7] Peters, G., Panayi, E., & Chapelle, A. (2015). Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective. *Journal of Financial Perspectives*, 3(3).
- [8] Foroglou, G., & Tsilidou, A. L. (2015, May). Further applications of the blockchain. In *12th student conference on managerial science and technology* (Vol. 9).
- [9] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE.
- [10] Zhang, Y., & Wen, J. (2015, February). An IoT electric business model based on the protocol of bitcoin. In *2015 18th international conference on intelligence in next generation networks* (pp. 184-191). IEEE.
- [11] Eyal, I., & Sirer, E. G. (2014, March). Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security* (pp. 436-454). Springer, Berlin, Heidelberg.
- [12] Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014, November). Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 15-29).
- [13] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37).
- [14] Schwartz, D., Youngs, N., & Britto, A. (2014). The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, 5(8), 151.
- [15] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014), 1-32.
- [16] Vasin, P. (2014). Blackcoin's proof-of-stake protocol v2. URL:<https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf>, 71.
- [17] Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014, November). Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 15-29).
- [18] Akins, B. W., Chapman, J. L., & Gordon, J. M. (2014). A whole new world: Income tax considerations of the Bitcoin economy. *Pitt. Tax Rev.*, 12, 25.
- [19] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19(1).
- [20] Jayasinghe, D., Cobourne, S., Markantonakis, K., Akram, R. N., & Mayes, K. (2017, September). Philanthropy on the blockchain. In *IFIP International Conference on Information Security Theory and Practice* (pp. 25-38). Springer, Cham.