A Survey on Use of Blockchain Technology in Introducing Transparency in Charity

Parth Mangalkar[1], Assistant Prof. Sonal Fatangare[2], Piyusha Patil[3] , Manjusha Katkhede[4]

[2]Assistant Professor, Computer Engineering, RMD Sinhgad School of Engineering, Warje, India
[1,3,4]UG Student, Dept. of Computer Engineering, RMD Sinhgad School of Engineering, Warje, India

---***---

Abstract - *The current online charity system that works on a client-server architecture has many cons to it. One of the main disadvantages of the charity system in India is corruption. Many charitable organizations in India are not transparent about their funding, and there are often cases of embezzlement of funds meant for charitable purposes. There is also lack of accountability as many organizations are not audited regularly. To address these problems we are building a decentralized blockchain based system that will provide full transparency to the donors and increase their trust in the system. The system is based on a decentralized distributed ledger that enables tamper-proof record-keeping and automates processes through smart contracts. This ensures greater accountability and transparency, reducing the risk of fraud or misuse of funds.*

***Key Words*: Blockchain, Distributed Ledger Technology, Cryptocurrency, Transparent, Smart Contracts.**

1. INTRODUCTION

Blockchain technology can be used in a variety of ways to enhance charity tracking and ensure the authenticity of content. Here are some functionalities that our blockchain based DApp will be providing :

1.1 Transparent donation tracking: Blockchain can provide a transparent and secure way of tracking donations made to a charity. Each transaction can be recorded on the blockchain, making it easy to track the flow of funds and ensure that they are being used for their intended purpose.

1.2 Immutable records: One of the key features of blockchain is that once a transaction is recorded, it cannot be altered or deleted. This can help ensure that charity records are accurate and trustworthy, reducing the risk of fraud or corruption.

1.3 Decentralized storage: Blockchain can be used to store content in a decentralized manner, ensuring that it is not controlled by any single organization or entity. This can help reduce the risk of censorship or manipulation of content. Here everyone in the network will be having a copy of transaction i.e a distributed ledger and hence the data won't be tampered easily.

2. RELEVANT TERMINOLOGIES

2.1 Distributed Ledger Technology (DLT):

A ledger refers to an orderly and systematically stored set of information, often electronic, that is intended for purposes such as bookkeeping, data retrieval, processing, and management. On the other hand, a distributed ledger is a type of data structure that can be used to transform a collection of uncommitted copies into a final uniform state, typically through the use of a consensus mechanism that ensures eventual consistency.

2.2 Smart Contracts:

Smart contracts are designed to be tamper-proof and irreversible, and they are executed automatically once the conditions encoded within them are met. They can be used to automate a wide range of transactions, from simple payment transfers to more complex arrangements like the exchange of goods or services.

2.3 Ethereum Virtual Machine(EVM):

The EVM is a Turing-complete virtual machine, meaning that it can execute any arbitrary code, as long as it does not exceed the gas limit (a unit of computational effort required to execute operations on the Ethereum network). This makes it highly versatile and flexible, enabling developers to create complex dApps that can run autonomously without the need for intermediaries.

2.4. Proof of Stake (PoS)

Proof of Stake (PoS) is a consensus mechanism used in blockchain networks to secure the network and validate transactions. Unlike Proof of Work (PoW), which requires miners to solve complex mathematical problems to validate transactions and earn rewards, PoS relies on validators who hold a certain amount of cryptocurrency as a stake to validate transactions and earn rewards.

Validators must hold a certain amount of cryptocurrency and lock it up as collateral in order to participate in the network. The probability of being chosen to validate a new block is proportional to the amount of cryptocurrency they have staked. Validators are incentivized to act honestly, as they stand to lose their staked cryptocurrency if they are found to be engaging in malicious behavior.

3. LITERATURE SURVEY

Sr no.	Name of Journal/Year of Publication	Paper Title	Author Name	Research Gap	Algorithms Used
1.	INT-JECSE - 2022	CrowdFunding Fraud Prevention using Blockchain.	Dheeraj Kumar S, Subash I, ShanthaKumari A, Deepa R	The authors have used the Proof of Work algorithm which is less time efficient as compared to its rival consensus algorithms such as Proof of Stake(PoS) and Delegated Proof of Stake(DPoS).	Proof of Work
2.	IRJET - 2022	Charity System using Blockchain Technology	Rhythm Negi Blessy Thomas, Prajkta Ghorpade Ammu Attiyilya	The authors use the PoW consensus algorithm and make use of Bitcoin blockchain which can only undergo 7 transactions per second.	Proof of Work & ECDSA
3.	IRJET - 2022	Blockchain Based Charity System Using PHP/MySQL	Varsha Kamble, Sapna Mandavkar, Hrishikesh Ramane	The authors have used Laravel for backend and PHP which is not suitable for modern Web applications which are based on the Blockchain technology.	Proof of Work
4.	Elsevier	Blockchain-based donations traceability framework	Abeer Almaghrabi, Areej Alhogail	The authors make use of the Bitcoin Blockchain which is comparatively slower as compared to the Ethereum Blockchain when it comes to the rate at which transactions are processed.	SHA-256 Bitcoin-P2P protocol

5.	IJRASET	Transparent Charity System using Smart Contracts on Ethereum using Blockchain	Purva Deepak Patil1 , Dikshita Jaiprakash Mhatre, Nidhi Hemant Gharat3 , Jisha Tinsu4	Future Work - MySQL will be used for centralized storage. In the paper authors haven't mentioned which algorithm they have used.	-
6.	International Journal of Research Publication and Reviews	Charity Donation System Based On Blockchain Technology	PROF.Dhanashri Patil, Abhishek Kadam , Gargi Sheytey , Tanmay Budage and Ashutosh Sonar	Not well chosen technology for building the application.	SHA-256.
7.	Elsevier B.V	DT-DPoS: A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust	Yuanyuan Suna, Biwei Yanb, Yan Yaoc , Jiguo Yuc	The paper have told about the difference between DPoS and DT-DPoS , So there is no research gap.	Delegated Proof of Stake(Dpos) DT-DPoS
8.	Springer - 2021	A donation tracing blockchain model using improved DPoS consensus algorithm.	Xiujun Wang, Yufei Peng, Wei She	The authors have not given out a detailed layout of how to implement the proposed algorithm and make use of it in Decentralized Apps (DApps).	Delegated Proof of Stake and K-means algorithm
9.	Elsevier - 2020	A Blockchain-based CrowdFunding Platform for Future Smart and Connected Nation.	Vikas Hassija, Vinay Chamola, Sherali Zeadally	The authors have proposed the use of the PoVV algorithm. But the issue with this algorithm is that the energy consumption and other associated costs increase exponentially as the number of competing nodes (developers) increases.	Proof of Virtual Voting for showing relevant NGO suggestions to the donor. ECDSA for public key cryptography.

4. ALGORITHMIC SURVEY

Sr no.	Publication :	Algorithm Used :	Space/Time Complexity :	Remark :
1.	INT-JECSE - 2022	Proof of Work	Keccak-256 is used in a hash function which returns a 256 bits string or 32 bytes array. Time taken to add a new block - 12s.	Keccak-256 is stronger than usually used SHA-256.

2.	IRJET 2022	Proof of Work & ECDSA	ECC is significantly faster than the other counterparts like RSA which are used for public key cryptography. Time taken by ECDSA in signature generation and verification is 93ms & 125ms	Efficient algorithms like ECDSA and Keccak-256 are used making the overall process of encryption and exchange of keys very fast.
3.	IRJET 2022	Proof of Work	Keccak-256 is used in a hash function which returns a 256 bits string or 32 bytes array. Time taken to add a new block - 12s.	Keccak-256 is stronger than usually used SHA-256.
4.	Elsevier https://doi.org/10.1016/j.jksuci.2022.09.021	SHA-256,	Time complexity for 41 steps : 2253.5, (O(N)) Memory requirement is 216 × 10 words O(1)	The time and space complexities depends on the number of steps the algorithm has used, used widely by technology leaders.
5.	International Journal of Research Publication and Reviews	SHA-256.	Time complexity for 41 steps : 2253.5, (O(N)) Memory requirement is 216 × 10 words O(1)	The time and space complexities depends on the number of steps the algorithm has used, Used widely by technology leaders.
6.	Elsevier B.V	Delegated Proof of Stake(Dpos) DT-DPoS	Block generating time < 1 second Block generating time < 1 second	Improves the throughput of the transaction and verification speed. The number of witness node present in consensus are less so, Algorithms are more scalable. They are using ring signatures for more security.
7.	Springer 2021	Delegated Proof of Stake K-means algorithm	Block generating time < 1 second Time Complexity : O(N^2) (n is the input data size)	Improves the throughput of the transaction and verification speed. K-Means is slow when it comes to bigger datasets

5. LIVE SURVEY

Sr no.	Existing Work	Website link	Technology/algorithm used	Remark
1.	Binance Charity	https://www.binance.charity/binance-charity-wallet	Binance Blockchain (BNB) Proof of Staked Authority (PoSA) Tech used - ReactJS for the frontend MySQL for backend.	Makes the use of their own blockchain and PoSA consensus algorithm which is faster and consumes less energy as compared to the blockchains using Proof of Work (PoW) consensus. It supports various Cryptocurrencies like ETH, BTC, etc.
2.	Giveth	https://trace.giveth.io/communities	Proof of Work consensus algorithm, Keccak-256 hash algorithm. Tech used - React js , node js , docker	Good user experience, easy to understand and donate using Metamask. Has various campaigns, funds and communities to which users can donate.
3.	GiveCrypto	https://givecrypto.org/	Ethereum Blockchain PoW consensus algorithm ReactJS for frontend MySQL for backend.	It uses coinbase as the crypto wallet through which people can donate real money which is converted to cryptocurrency and vice-versa.
4.	TrackMyCharity	https://trackmycharity.org/	Proof of Work (PoW) consensus algorithm.	The website is not active currently and donations cannot be made.

6. PROPOSED WORK

After going through a lot of relevant research papers and also studying the currently existing systems, we have decided to propose a charity application using blockchain for which the basic algorithm will be as follows.

Step 1: New Donors and NGOs can register to the application.

Step 2: The Government body will approve the NGO if the registration record of the NGO is found in the Government registration records.

Step 3: The approved NGOs can make requests for donations and start new campaigns for raising funds.

Step 4: The signed in users will search for the causes to which they want to make donations to and select the relevant campaigns and NGOs to make donations to.

Step 5: The donors will make the donations by simply selecting the amount to donate and click on the donate button. Once the donate button is clicked, a smart contract will be executed which will automatically transfer the donated sum to the crypto-wallet of the respective NGO.

Step 6: The transaction is verified using the Proof of Stake (PoS) consensus algorithm and then only, a new block is added to the blockchain and the donation sum is transferred to the NGO.

Step 7: Once the sum is received by the NGO, a thank you message will be sent to the donor automatically with the help of smart contract.

7. CONCLUSIONS

In India, the current charity framework is plagued with issues such as low transparency, concerns around data security, lack of trust among individuals, and fake foundations. To tackle these problems, this paper proposes a novel approach that utilizes blockchain technology to revolutionize the charity framework. Our blockchain-based charity applications will also ensure that there is transparency in the transactions process and also that the process is not controlled by any one authority.

REFERENCES

[1] S. Pandey, S. Goel, S. Bansla and D. Pandey, "Crowdfunding Fraud Prevention using Blockchain," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2019, pp. 1028-1034.

[2] Rhythm Negi1, Blessy Thomas2, Prajkta Ghorpade3, Ammu Attiyil4, Prof. Y. I. Jinesh Melvin5 “Charity System using Blockchain Technology”2022 International Research Journal of Engineering and Technology (IRJET)

[3] 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.

[4] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19(1).

[5] YILDIRIM, İ., & Şahin, E. E. (2018). Insurance Technologies (Insurtech): Blockchain and Its Possible Impact on the Turkish Insurance Sector. Journal of International Management Educational and Economics Perspectives, 6(3), 13-22.

[6] Hu, B., & Li, H. (2020). Research on Charity Systems Based on Blockchain. Research on Charity System Based on Blockchain, 768(072020), https://iopscience.iop.org/article/10.1088/1757- 899X/768/7/072020.

[7] Nixon, R. (2009). Learning PHP, MySQL, JavaScript, CSS & HTML5: A Step-by-Step Guide to Creating Dynamic Websites. Shroff Publishers & Distributors Private Limited- Mumbai. 4.

[8] Rangone, A., & Busoli, L. (2021, March). Managing charity 4.0 with Blockchain: a case study at the time of Covid-19. Managing charity 4.0 with Blockchain: a case study at the time of Covid-19, 18(01), 31. https://doi.org/10.1007/s12208-021-00281-8.

[9] Ming Li, Jian Weng, Anjia Yang, Wei Lu,Yue Zhang, Lin Hou, Jia-Nan Liu, Yang Xiang, Robert H.Deng, “ CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourcing”

[10] 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.

[11] Aashutosh Singh, Rohan Rajak, Harsh Mistry, Prachi Raut “ Aid, Charity andDonation Tracking System Using Blockchain “ ISBN: 978-1-7281- 5518

[12] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee, “A Critical Review ofBlockchain and Its Current Applications”, International Conference on Electrical Engineering and Computer Science (ICECOS) 2017 DOI:978-1-4799-7675-1/17