International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228621

Fundraising Tracking System Using Blockchain

Prof. Sumit Shevtekar, Ajay Raut, Pranit Chaudhari
ME Computer Engineering, Department of Computer Engineering, Pune Institute of Computer Technology, Pune, Maharashtra, India

Article Info

Publication Issue :
Volume 8, Issue 6
November-December-2022

Page Number : 165-172
Article History
Accepted: 05 Nov 2022
Published: 18 Nov 2022

ABSTRACT

People no longer trust charities as a result of the lack of openness, which has caused social investment to stagnate. The donor is unaware of how his money is being used legally. Mistrust of the donor is increased by corruption. In this study, a decentralised network named Charity-Chain that is based on the Ethereum blockchain is proposed. By employing smart contract-based incentives to ensure that their impact is independently validated and available to everyone, it aids social organisations in managing initiatives transparently. For funders (philanthropic organisations, impact investors, and small donors), this makes it much simpler for them to monitor their transactions and, as a result, restore their trust in funding these types of social organisations.

Keywords : Blockchain, Ethereum, Gas, Donation System, Digital Charity, Blockchain, Smart-contracts, Ethereum, Track-ing Donation, Charitable Foundations, Transparency.

I. INTRODUCTION

The lack of openness in the transactions involving donations and monies provided by the government or other contrib-utors is the issue that the paper seeks to solve. Allowing contributors to trace their contributions is necessary to in-crease transparency in social funding. The goal is to maintain financial security and ensure the traceability of a donor's donation. This will pique donors' interest in learning more about the impact of their donations and assist reverse the public's declining trust in charity. Donations will primarily be processed through blockchain. A contributor might track their contribution throughout the way from the beneficiary through a charity and beyond. Charity chain records each transaction using a blockchain. With thanks using blockchain technology's inherent data immutability and it furthers project openness, is tamper-resistant, and accountability. For traditional donations and online crowdfunding to gain more respect, philanthropic information must be made more transparent. Technically, the transparency of charity can be improved by establishing a traceability system using Internet technologies[1]. This paper presented a new charity model system based on blockchain technology to achieve this.

II. LITERATURE SURVEY

With the use of the blockchain, a decentralised transaction ledger for generating, validating and transact with other nodes that are part of the same network achieved. The level of secu-rity required for financial transactions is additionally increased by various cryptographic hash algorithms of particular cryp-tocurrencies. Financial services, healthcare services, as well as business and industry, can all use the blockchain[2]. Today, a charity application needs a mechanism that can validate itself independently of other applications or systems. Blockchains are employed because they are not tied to any one system and can independently verify the consistency and integrity of transactions.Because it is a blockchain, Ethereum was selected as a due to improved scalability and is a public platform. Runs from 7 to 20 transactions per second[3].The charitable system won't be monopolised by a single authority thanks to blockchain. The general public will have simple access to the transactions and be able to check that their money is being used as intended.China's government provides an excellent illustration of how to use blockchain technology effectively. It is the first to employ blockchain technology for e-government. The relationship of trust between citizens, the government, and producers is improved.It is employed to ensure the perishable food's quality. The application securely communicates each stage's status of the produce. Manufacturing, transportation, and marketing are the steps[4].China has a vast population like India. Despite this, by making the production of food resources transparent, it has successfully employed Blockchain to boost public confidence in the government. Due to the fact that all transactions are recorded and visible in the event of discrepancy, this promotes equitable resource distribution to the population and raises government responsibility. India can apply similar use cases to manage its enormous population. Financial institutions are utilising blockchain to improve cyber security. The benefits of blockchain include its speed, affordability, decentralised registry, and ability to deliver secure payment information[5]. Each Indian resident receives an Aadhar number in India, which confirms their biometric information as well as their location and other in-formation. Blockchain technology can be used in conjunction with the Aadhar for a variety of purposes, including voting and healthcare[6]. Blockchain can eliminate data loss due to single point of failure and privacy disclosure[7]. The consensus protocol is very important since it determines the criteria used to validate a new node. When using the programme, an improper consensus methodology could produce unfavourable outcomes[8]. The difficulties a blockchain application faces are resource requirements and scalability[9].

III. BLOCKCHAIN OVERVIEW

Blockchain ensures decentralised and secure transactions by maintaining an immutable record of all transactions in a distributed ledger. A block containing the transactions is connected to the chain. We refer to the three technologies that make up blockchain technology as distributed ledger[10], consensus protocols, and cryptography[11]. Although these technologies are not new, blockchain is a novel technology because of the use of these technologies when combined. In digital partnerships, a Distributed Ledger is used to do away with the necessity for a reliable third party and lower the possibility of a single point of failure. In a peer-to-peer network like the one used by blockchain, each network node has a synced copy of the ledger. The original data can still be accessed from the other nodes even if one node malfunctions or behaves maliciously, which is not possible if the data is stored by a central administrative authority. Blockchain thus enhances fault tolerance. Blockchain users employ consensus protocols to settle on a single state for updating the ledger. The network is more secure the more nodes there are in the network validating a state change. A consensus protocol is used by blockchain to validate transactions, build new blocks, and add those blocks to the chain.Every participant in the blockchain network receives a secure digital identity and all transactions are verified using cryptography technology. Using a set of participant-owned public and private keys, this is accomplished.

An overview of blockchain technology is shown in figure

1. The infrastructure layer, platform layer and distributed computing layer make up the three levels that make up the blockchain architecture. The hardware needed to run the blockchain is included in the infrastructure layer. Nodes, the network's participants, are included.A node may carry out any of the subsequent actions: Initiate transactions, validate transactions and blocks, create blocks, and keep a copy of the ledger. The network infrastructure required for commu-nication within a blockchain or between blockchains is the other element of the infrastructure layer.For communication between the client and the blockchain network, the platform layer provides the means to invoke Remote Procedure Calls (RPCs)[12], web Application Programming Interface (API) [13], and Representational State Transfer (REST) APIs[14]. The blockchain architecture's distributed processing layer guarantees local data access, fault tolerance, immutability, privacy, authenticity, and security of the transaction data. The application layer deals with the business logic which varies from need of blockchain user. To ensure fault tolerance and immutability, the ledger of transaction records is duplicated among distributed nodes linked via a peer-to-peer network. The immutability of a blockchain prevents the change of transaction records once they have been updated in the ledger. The blockchain network employs a consensus method to decide on the next block to be formed, the sequence in which transactions should be processed, and how the ledger should be updated. Additionally, the distributed computing layer is in charge of user authentication through encryption[15] and data privacy through the use of hashing[16].

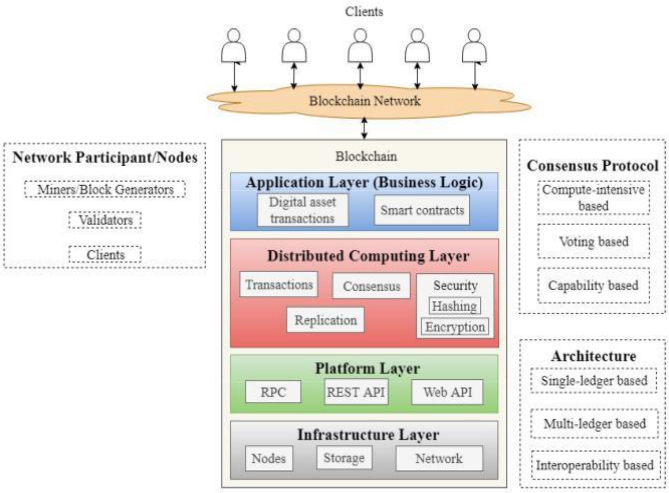

Fig. 1. Overview of blockchain.

The different layers that make up the blockchain architecture include the following features.

- Decentralization: Blockchain makes it possible to share a database directly within a distributed ledger without the use of a middleman. The network nodes process and store the transactions. Once a consensus has been obtained, the nodes update the ledger.

- Transparency: The transaction data replicated on the blockchain network's network nodes is kept as a chain of connected transactions, starting with the very first transaction. The network is highly transparent and secure since changes to the network are made public knowledge.

- Immutability: The blockchain stores transactions as blocks. A cryptographic hash function is used to connect each block in the chain to the one before it. Any effort to change the content of a block will have an impact on the blocks that follow it in the chain. In order to modify one block, a malicious attacker must computationally alter every block after it in the chain. Due to the replication of the chained blocks across numerous nodes, this becomes challenging.

- Traceability: Complex transaction events, including those in a supply chain, are easier to track thanks to the distributed, transparent nature of blockchain technology. It is possible to determine the source of each change in the asset's condition. As a result, the blockchain network is improved in terms of security, effectiveness, and transparency.
- Trustless: Blockchain permits the transfer of assets be-tween unidentified parties with a lack of mutual con-fidence. The legitimacy of transactions in an untrusted environment is ensured by dispersing the ledger among a number of network nodes and updating this ledger via consensus.

IV. PROPOSED SYSTEM

The system model has been presented in this section. The application's users are categorised according to their roles as Donors, Organizations(Beneficiaries) and General user.

- Organization (Beneficiary): These are organisations, NGOs or other social businesses that require resources (financial or otherwise). On the Charity-Chain system, they will be able to post their requirements in a predetermined format. They will be crucial in mining as well.
- Donor: They are the organisations that will view the requests made public by various groups and if their tender is accepted, decide to contribute to the cause in accordance with their abilities and preferences.
- General User: Anyone who visits the platform for the first time, they become general users as they have not decided to become donor or beneficiary.

On the platform the organization (beneficiary) will create the request for raising the funds. While creating the request it has to mention the target amount and the time period in which it has to complete the target amount. The donor then can see the request on the platform. The platform is general and anyone who is in need can create the request for funds. The donors who are willing to donate the funds can donate through their account. The amount is kept in the smart contract until the target amount is not reached or the time period is not finished. If the mentioned target amount by the beneficiary is reached within the specific time period then the amount is transferred to the beneficiary else the amount is given back to the donors.

As the Ethereum blockchain provides the transparency, scalability and security our application become robust. Using the Ethereum blockchain one can track the entire history of his account address. Making use of that functionality, we can track the funds of donor and give them complete transparency. Due to the lack of transparency in the centralized system many people do not donate their money to anyone. If we provides the functionality of tracking the funds many people will come forward and make donations for the needy organizations (beneficiaries). The centralized systems are not safe from the various type of attacks. These companies have their own data-center and faults in their data center will cause the loss of data of various users. From the other scenario also if the platform increased its users then for small organization it is not an easy task to scale up their business and taking help from the other end up with loosing their users. So avoid all these issues we have proposed system using Ethereum blockchain for raising the funds. It is complete transparent as the underlying infrastructure that we are using is Ethereum blockchain and it is public blockchain.

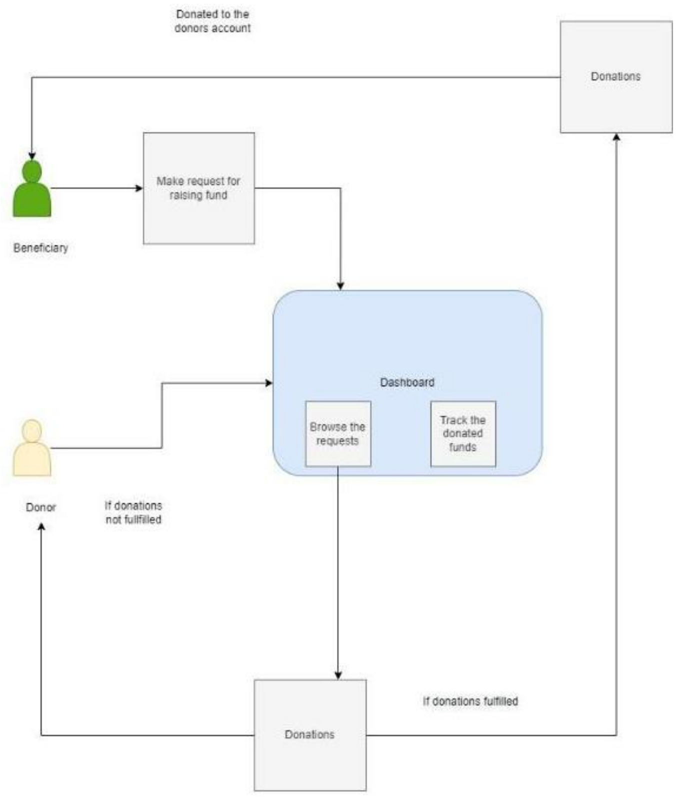

Fig. 2. Proposed system.

A. Data Flow

Data flow in the proposed system is show in the figure 3. The user who visits the platform is the General user because he yet not decided to donate or create a request for donation of funds.A General user can also track the donation by entering the address and can able to browse the requests that were created by the beneficiaries. If he decided to become the beneficiary, he first create the request for the raising the funds via the create the request functionality. While creating the request for raising the funds, the beneficiary has to mention the goal amount and the time period in which the goal amount should be reached. After filling all other required details, the beneficiary can raise the request for raising the funds for need. The platform will be general fundraising system, so anyone who is in need, can create the fund request. The beneficiary have to mention the reason for the raising the funds that could be single person or various organizations raising the funds for the startups. If he decided to become donor, he first can browse the requests that were created by the beneficiaries. Then he can donate the funds in the form of cryptocurrency eth. The amount is hold in the smart contract until the target amount is reached or the end date specified by the beneficiary reached. If the target amount is reached within the time the total donations made by the donors are transferred to the beneficiary else the amount send back to the donors. After donating to the beneficiary, the donor can track the funds whether it is reached to the specific organization.

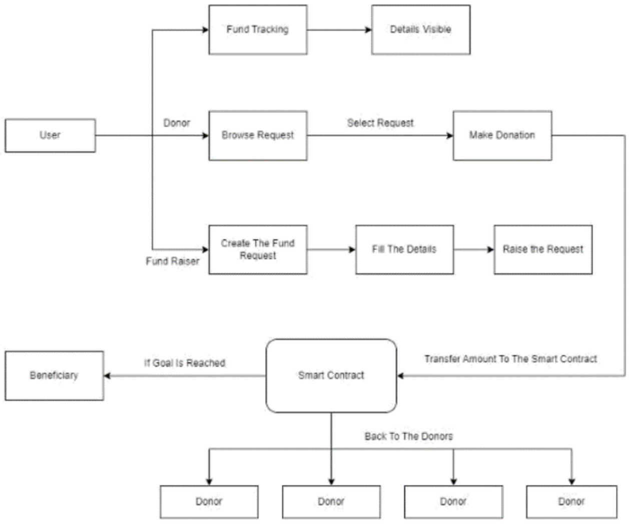

Fig. 3. Data flow

V. SYSTEM DEVELOPMENT

1)Ethereum Blockchain : Ethereum blockchain is the public blockchain meaning that anyone can take part and leave the blockchain network as per his wish. Another benefit of public blockchain is that every transaction can be tracked by anyone by simple making use of address. We are making use of that to develop the proposed architecture for raising the funds. The Ethereum's architecture is shown in the figure 4. The business logic is written in the Solidity programming language. Solidity is similar to the programming languages such as java, python, javascript etc. After the writing code, it is then compiled by the Ethereum compiler which checks any error in the code. Ethereum compiler then generate its Bytecode which is only understood by the Ethereum virtual machine. After that the contract is deployed on the Ethreum network. The miner then verifies the trasaction. The miners are the nodes that are intended to verify the transaction. Ethereum uses proof of work to select the miner.

2)Smart Contracts : The blockchain network's soul, which regulates all transactions occurring there, can be thought of as consisting of smart contracts. Decisions for all transactions are to be made via smart contracts. The rules created to process any transaction that occurs on the blockchain network are known as smart contracts. A smart contract is a set of lines of code that runs on top of a blockchain and specifies a set of rules that multiple parties must agree to in order for them to interact. The smart contract is automatically carried out in the event that certain predetermined conditions are satisfied. Between individuals, organisations and the assets they possess, a smart contract can establish a connection. A smart contract can significantly lower transaction costs. We can say that is an auto-enforceable code, means it standardizes transactions rules and it indirectly reduces transaction cost of: Reaching an agreement, Formalization, Enforcement. Using such smart contracts a Dapp is created. Dapp stands for Decentralized Application.

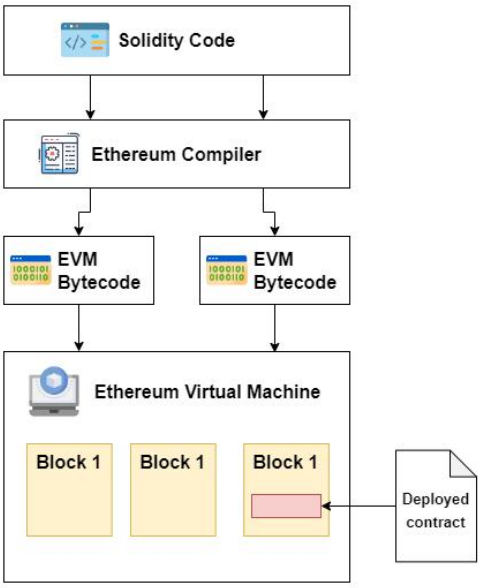

Fig. 4. Ethereum architecture

3)EVM : The Ethereum Virtual Machine serves as the environment in which smart contracts are carried out. Additionally to being sandboxed, it is also totally isolated, which means that any contracts operating inside an EVM have no access to the internet, file systems, or other processes. An object that links to accounts or users is a transaction. Every transaction that is created has a specific amount, known as Gas, added to it. This gas's main functions are to reduce the amount of effort required for the transaction and to pay for its execution. The gas is gradually reduced as the EVM is processing a transaction in accordance with some rules laid out in the smart contract. The author of the transaction determines the gas price and must pay gas price from the transmitting account.

4) Consensus Protocols: A consensus protocol is a crucial component of blockchain technology. It is necessary for dis-tributed and peer-to-peer processes and systems to agree on a single value of data. Every participant in the network is informed whenever a new transaction is ready to be added to the network. Either they can accept it and link it to the chain or they can reject it. Consensus is reached when a majority of parties agree to the transaction. Blockchains are decentralised, thus malicious players might introduce errors and thwart important

transactions. Due to the possibility of the bad peer to post flawed transactions in the absence of a robust, fully proven consensus method, blockchains' reliability promises are rendered meaningless. The lack of a central authority to take responsibility and correct the mistakes only serves to make matters worse. This guarantees consistency and stability in a network made up of numerous random and unreliable nodes. Consensus protocols are difficult to reproduce or duplicate because they need a lot of time and computational resources to execute. The mechanisms of consensus change depending on the blockchain they are validating the blocks in. The best and most efficient way to reach a consensus is a topic of constant and continuous discussion.There are many protocols that are being used by the Blockchain applications. Some of these are Proof of Stake (PoS), Proof of Work(PoW), Delegated Byzantine Fault Tolerance (dBFT), Delegated Proof of Stake (DPoS), Proof of Existence (PoE), Proof of Activity (PoA).

A. Modules in the proposed system

The modules in the proposed system are shown in the fig.

- Create Fund Request : This module is responsible for the creation of the fund request by the various organization(beneficiaries). While creating the fund request, beneficiary have to mention the target amount, last date and reasons for the requesting the fund.
- Browse The Requests : This module is responsible for the searching the fund requests that were created by the beneficiary.
- Donate The Funds : This module is responsible for the donating the funds to the requests that were created by the beneficiary. After browsing the specific requests, donor can donate the ethers. This is the heart of our proposed system.
- Tracking The Donations : This module is responsible for the tracking the donations that were made by the donor. This is the main feature of our system. Using the Ethereum blockchain we can track the transactions. Mak-ing use of that functionality we can track the donations.

VI. CONCLUSION

As a result, the suggested system will track donations and inform the donor when their money has successfully reached the beneficiary. Smart contracts are used by charity chains to handle and track donations. Because it is a public platform, the Ethereum platform is used. Transparency in the donations would ultimately encourage the donor to make larger contributions to such adaptable yet effective system.

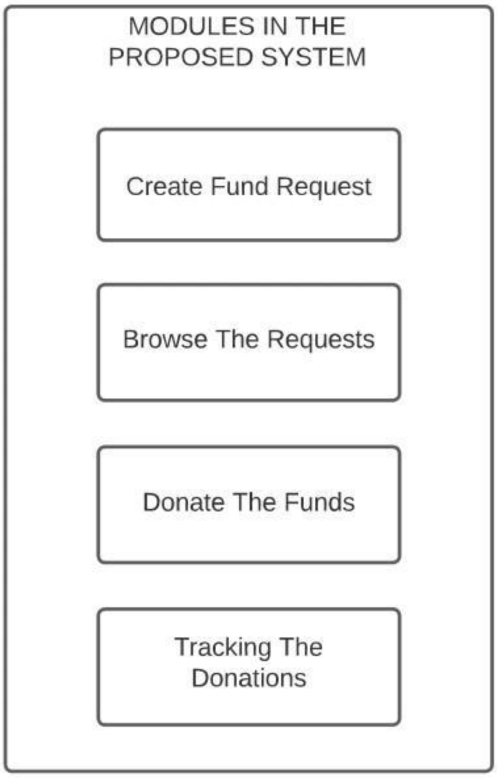

Fig. 5. Modular diagram.

VII. ACKNOWLEDGMENT

Without the extraordinary assistance of our supervisor, Prof. Sumit Shevtekar, ME COMP, Pune Institute of Computer Technology, neither this work nor the research that went into it would have been feasible. From the first time we encountered this subject to the final copy of this dissertation, his excitement, expertise, and meticulous attention to detail served as an inspiration and guided our work.

VIII. REFERENCES

1. Zhang Peng, Li Ping, Zhao Wenbo, Resolving the Dilemma of Charity and Credibility: The Theory and Evidence of the Application of Traceability System Principles, Social Sciences Research, 2016(03)40-46.
2. Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee, "A Critical Review of Blockchain and Its Current Applications", International Conference on Electrical Engineering and Computer Sci-ence (ICECOS) 2017 DOI:978-1-4799-7675-1/17/$31 .00 ©2017 IEEE.
3. Ashiq Anjum, Manu Sporny, Alan Sill, "Blockchain Standards for Compliance and Trust", 2325-6095/17/$33.00 © 2017 IEEE.
4. Heng Hou, "The Application of Blockchain Technology in E-government in China", 978-1-5090-2991-4/17/$31.00 ©2017 IEEE.
5. Sachchidanand Singh, Nirmala Singh, "Blockchain: Future of Financial and Cyber Security", 978-1-5090-5256-1/16/$31.00 c 2016 IEEE.
6. Kumaresan Mudliar, Harshal Parekh, Dr. Prasenjit Bhavathankar, "A Comprehensive Integration of National Identity with Blockchain Tech-nology", 978-1-5386-2051-9/18/$31.00 ©2018 IEEE.
7. 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".
8. Pinyaphat Tasatanattakool, Chian Techapanupreeda, "Blockchain: Chal-lenges and Applications", 978-1-5386-2290-2/18/1.00 ©2018 IEEE.
9. Nabil Rifi, 1Elie Rachkidi, Nazim Agoulmine, Nada Chendeb Taher, "Towards Using Blockchain Technology for eHealth Data Access Man-agement", published in 978-1-5386-1642-0/17/$31.00 ©2017 IEEE.
10. Financial Conduct Authority, "Discussion paper on distributed ledger technology," Financial Conduct Authority, London, U.K., Discuss. Paper DP17/3, 2017.
11. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.
12. Remote Procedure Call. Accessed: Jun. 12, 2019. Online]. Available: https://en.wikipedia.org/wiki/Remote procedure call
13. Web API. Accessed: Jun. 12, 2019. Online]. Available: https://en.wikipedia.org/wiki/Web API
14. Representational State Transfer. Accessed: Jun. 12, 2019. Online]. Available: https://en.wikipedia.org/wiki/Representational state transfer
15. R. C. Merkle, "A digital signature based on a conventional encryption function," in Proc. Conf. Theory Appl. Cryptograph. Techn. (CRYPTO), London, U.K.: Springer-Verlag, 1988, pp. 369–378.
16. M. Swan, Blockchain: Blueprint for a New Economy. Newton, MA, USA: O'Reilly Media, 2015.

Cite this article as :

Prof. Sumit Shevtekar, Ajay Raut, Pranit Chaudhari , "Fundraising Tracking System Using Blockchain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 6, pp. 165-172, November-December 2022. Available at doi : https://doi.org/10.32628/CSEIT228621

Journal URL : https://ijsrcseit.com/CSEIT228621