Blockchain Based Smart Contract Secure Charity System

Zhehao Fan
Department. of Computer Science
Virginia Tech
Falls Church, VA, US
zhfan@vt.edu

Tinghui Wu
Department of Computer Science
Virginia Tech
Falls Church, VA, US
tinghuiwu@vt.edu

Rundong Liang
Department of Computer Science
Virginia Tech
Falls Church, VA, US
rundong@vt.edu

Kaiyi Chen
Department of Computer Science
Virginia Tech
Blacksburg, VA, US
kennychen@vt.edu

***Abstract*—The emergence of blockchain technology, coupled with smart contracts, has presented a fresh opportunity to revolutionize traditional systems. This technology also provides a viable solution for addressing the declining social trust in various aspects of the conventional system, including charitable activities. [1] The proposed system in this paper leverages the decentralized nature of blockchain to create a more transparent information symmetry platform. Using such technology, we can provide a more transparent, publicly trusted, and efficient platform. And most importantly, diminishes human intervention and thus reduces the administrative overhead, which allows more resources to be directed to the people in need. As long as the system guarantees transparency, people will be more willing to donate the money because they know their donation making a positive effect on the people in need. This paper proposed a charity system that includes the system design, workflow chart, operation process, etc. Functions have been verified on Ethereum. And the user can use the frontend(Vue.js) to interact with the smart contract and donate to the donatee.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

A. Motivation and problem

As public charity grows, it needs more specialization to deal with the problems it poses. Traditional charities often suffer from a lack of trust and opaque information. [1] Some charities may use opaque fund management practices that lead to misuse and waste of funds, thus losing people's trust. On the other hand, there is a problem of information asymmetry in the process of how money is spent. For example, the most common donation process now is to give the money directly to a charity and entrust them to do charitable projects. However, after the donation is handed over to the charity, it is difficult for the donor to have a clear understanding of how the money is used, to whom it is used, how well it is used, etc. Some organizations that do a good job may give some feedback to the donor regularly, but they do not provide detailed information to the donor. Due to the non-transparency of the usage of the money process, many people lost their trust in the charity donation and thus stopping donate money. In the year 2000, approximately two-thirds of households in America made donations to charitable organizations. However, by 2018, this percentage decreased to just under half of American households. In other words, around 20 million Americans had ceased their charitable giving. Despite the total amount of money contributed to charity in the US continuing to increase (surpassing 480 billion last year), there has been a decline in the number of Americans actively participating in charitable giving. [2]

Establishing trust among participants who inherently distrust each other, without the involvement of

Identify applicable funding agency here. If none, delete this.

a trusted third party, has posed a significant challenge for many decades. [3]There may be a variety of reasons why people do not trust charitable organizations, including but not limited to the following. First, non-transparent financial management: The financial management of charitable organizations is not transparent and no financial statements are publicly available, making it difficult to prove the use and effectiveness of charitable organizations' funds. Second, corruption: Some managers or staff of charities may embezzle charity funds or use charity funds for illegal purposes, which can seriously damage people's trust in charities. Third, information asymmetry: charities may exaggerate the impact and effectiveness of their projects when promoting them, while donors do not know enough about the details of the projects, which can lead to information asymmetry and thus affect people's trust in charities.

The application of smart contracts in charitable organizations can help increase trust in charitable organizations because the core properties of smart contracts are programmability and tamper-evident. In the charity sector, smart contracts can be used to establish transparent, automated, and efficient donation and fund management mechanisms that avoid human interference and fraud in charitable organizations. Blockchain technology, combined with smart contracts, can enhance the transparency and openness of the charitable donation and distribution process. By leveraging blockchain, donors have the ability to track and verify the flow and utilization of funds associated with their donations in real-time. This increased visibility fosters trust in charitable organizations as donors can independently verify the integrity and proper allocation of funds, promoting accountability and minimizing the risk of misuse or mismanagement. In addition, smart contracts can also provide a more secure and efficient identity verification and authentication mechanism to ensure that donors' personal information will not be leaked or tampered with, thus further enhancing trust in charitable organizations.

B. Research goals and objectives

By using smart contracts, charitable organizations can have better fairness, credibility, and transparency. The use of smart contracts in charitable organizations can provide more transparent and secure donation and fund management solutions. It can be a good solution to the shortcomings of traditional charitable organizations. In a smart contract, all donation information is recorded on the blockchain, and donors can check the details of their donations at any time, along with the donation status; how the charity used it, when the donatee received the donation etc. Because of the tamper-evident feature of the blockchain, the use of smart contracts can enhance the credibility of charitable organizations. Smart contracts can reduce the cost and risk of fundraising for charitable organizations. Traditional charitable fundraising usually requires a certain amount of human, material, and financial resources to organize and promote, collect donations, and manage funds. Smart contracts can make the fundraising process more efficient and cost-effective by going digital.

II. Related work

The utilization of blockchain technology and smart contracts for charitable endeavors has garnered increasing interest.

First, GiveCrypto.org. This is a charitable organization that aims to alleviate poverty by distributing cryptocurrency to people in need. The organization leverages blockchain technology to enhance transparency in the distribution process and mitigate the risk of fraud.GiveCrypto.org does this by accepting cryptocurrency donations, converting them into local currency, and then distributing them to those in need. The organization uses blockchain technology to achieve transparency and security of funds and to ensure that donated funds are not misused. GiveCrypto.org's activities span the globe, especially in some economically challenged countries and regions. The organization works with local charities and NGOs to ensure that donated funds are actually reaching those in need.

Second, BitGive Foundation. BitGive is a non-profit organization that uses blockchain technology to facilitate donations to various charities. It uses a platform called GiveTrack to track the progress of donations and ensure that they are being used effectively. The BitGive Foundation uses data analytics to measure and evaluate the effectiveness of charitable programs. It uses Bitcoin blockchain data and other data to track the flow and use of donations, thus ensuring that donated funds are being used to their fullest extent.

Third, Alice.si. Alice is a blockchain-based platform that helps donors track the impact of their donations. Alice.si uses blockchain technology to enable the security and privacy protection of medical data. It uses blockchain technology to record and store medical data and protects the privacy and security of the data through distributed storage and encryption technology.The platform uses smart contracts to ensure that donations are used for their intended purpose and to provide transparency in the donation process.

III. Preliminaries

A. Brief background

1) Charity System: A charitable organization, or charity for short, is a nonprofit entity dedicated to philanthropy and social well-being. Activities conducted by charitable organizations typically serve the public interest or common good, such as educational or religious pursuits. The legal definition of a charitable organization (and the concept of charity itself) varies between countries and regions within those countries. As a result, regulations, tax treatments, and laws affecting charitable organizations also differ.Charitable organizations are prohibited from using their funds to benefit individual persons or entities. However, some have been criticized for allocating a disproportionate amount of their income to pay their leadership salaries. Businesses often provide donations to charitable organizations as a form of corporate philanthropy.Despite the good works accomplished by charitable organizations, their reputations are at risk, according to ICAEW Insights.

B. Building blocks being used

1) Blockchain: A blockchain refers to a decentralized ledger containing expanding collections of entries (blocks) that are interconnected securely using cryptographic hashes. [4]Every block in a blockchain consists of three essential elements: a cryptographic hash of the preceding block, transaction data that is organized in a Merkle tree structure with leaves representing data nodes, and a timestamp. The timestamp serves as a verifiable proof that the transaction data existed when the block was created.The blocks in a blockchain are linked together in a chain-like structure, similar to a linked list data structure. This linkage is established because every block contains information about its preceding block. As a result, once a block has been added to the chain, the transaction data stored within it becomes irrevocable, and any subsequent modification would require changing all subsequent blocks in the chain.This unique property of the blockchain structure ensures that the transactions recorded in the blockchain are irreversible, providing a secure and tamper-evident ledger of transaction data.

Blockchain is an innovative technology that allows individuals to communicate in a manner that doesn't rely on trust. It completely transforms the way businesses interact with each other, eliminating the requirement for a trusted intermediary... [5] Smart contracts ensure the security of transactions in a fully decentralized manner, providing a guarantee for their integrity and reliability. [6] In the majority of instances, P2P computer networks are in charge of administering blockchains, which function as communal decentralized ledgers. Within this network, nodes collaborate to uphold a consensus algorithm protocol, which encompasses the insertion and verification of fresh transaction blocks. [7]Blockchain records may not be immutable due to the possibility of forks, but they are still considered secure by design. Blockchains are an example of a distributed computing system with high Byzantine fault tolerance, meaning they remain operational even in the presence of potentially faulty nodes or components. Despite the potential for attack, blockchain technology has demonstrated its resilience as a robust solution for secure and transparent record-keeping.

2) Smart Contract: A smart contract is a self-executing contract that utilizes blockchain technology to automate its execution. It can eliminate the need for human involvement and enhance the security and dependability of the contract. Smart contracts operate based on the principles of decentralization and a distributed ledger utilizing blockchain technology. [8] It is a distributed network of multiple nodes, where the same contract code and data are stored on each node in the network, which makes smart contracts highly secure and reliable when executed. The result of smart contract execution is tamper-proof because the data structure of blockchain technology is based on a hash function, which guarantees the tamper-proofness and uniqueness of the data.

Smart contracts have several advantages. The first is efficiency. Smart contracts can automate the execution of transactions without waiting for human review, thus greatly improving the efficiency of transactions. In addition, smart contracts can automatically execute according to set logic and rules, such as the allocation of funds, and masking can reduce human error and fraud. The second is low cost. Smart contracts do not require the intervention of third-party trust institutions, and therefore can greatly reduce the cost of transactions. The third is security. Smart contracts are based on blockchain technology and therefore have a very high level of security. Every transaction is recorded on the blockchain and cannot be tampered with or lost. The fourth is flexibility. Smart contracts can be programmed to implement a variety of logic and rules that can be customized and modified to meet specific needs. This allows smart contracts to be adapted to various application scenarios and business needs. [9]

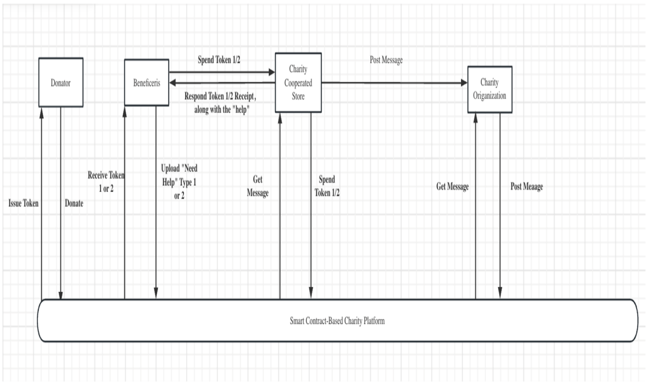
IV. Model

A. System model

The system model includes four parts: charity, donor, beneficiary, smart contract and charity cooperated store. The charity, as the initiator and administrator of the smart contract, can create the smart contract and set the donation rules, donation items, beneficiaries, and other information. The charity needs to be responsible for the operation and management of the smart contract and ensure that the contract is executed in compliance with the regulations. Donors can donate through the smart contract, select donation items and beneficiaries, and set donation amounts and donation methods. Donors need to provide certain identifying information and proof of donation to ensure the authenticity and traceability of the donation. The beneficiary is the beneficiary of the donation project designated by the charity and can receive the donation funds through a smart contract and provide a report on the use of the donation. Beneficiaries need to provide certain identification information and proof of qualification to ensure the legitimacy and transparency of the use of funds.

A smart contract is a program implemented based on blockchain technology and contains information on donation rules, donation items, beneficiaries, etc., as well as the execution process and logic of the smart contract. Smart contracts need to use secure programming languages and contract design patterns to avoid security vulnerabilities and attacks.A charity cooperated store is a model of cooperation between charities and merchants. Its role is to realize the organic combination of public welfare and business by selling goods or services to the public through the co-op merchants and donating part of the income to the charity. Through the operation of charity cooperative stores, charities can obtain more donation income, while merchants can enhance their brand image and social reputation by participating in charity activities.

When a donor logs in to the system, they can donate money or materials to the charity's online store. The system will exchange the donation with tokens, which are credited to the donor's account. If a beneficiary submits a help request to the system, the system will allocate tokens to the request. The beneficiary can then use the tokens to purchase items from the charity's online store. If the charity has the necessary resources and the transaction is validated, the items will be sent to the beneficiary. The beneficiary will then confirm receipt of the items to the system. Before the beneficiary confirms receipt, the charity store will be notified. The charity organization can assign additional points to the beneficiary's account, based on their documentation and eligibility. The charity organization must approve the transaction before the store can transfer the help to the beneficiary. The charity organization will update the beneficiary's credit score by posting a message to the system, and the system will automatically update the beneficiary's score.



B. Threat model

The first point of the threat model for smart contracts is algorithmic risk, where the algorithms in smart contracts can be flawed. The most common one is the random number attack. .A random number attack refers to the act of an attacker exploiting the weakness of the random number employed during the signing process, aiming to undermine the security of the digital signature. By tampering with the random number utilized in the signature, the attacker attempts to deduce the key and compromise the integrity of the digital signature. [10] In digital signatures, the signer needs to use the private key to sign the data and also needs to randomly select a number to calculate the signature to avoid signature duplication. However, if the process of generating random numbers is not secure, an attacker can damage the integrity and authenticity of a digital signature by calculating the random number used by the signer and then maliciously tampering with the signature.

The second threat model is the authentication risk of smart contracts. It refers to the security risk that exists when authentication is performed. Smart contracts usually involve interactions between multiple parties, at least one of which needs to be authenticated to participate in the execution of the contract. During the authentication process of a smart contract, it may be subject to man-in-the-middle attacks and brute force attacks.In a man-in-the-middle attack, an attacker inserts their own program or presence between two communicating parties, allowing them to intercept, modify, or forge the content of the communication. This unauthorized intervention enables the attacker to gain access to sensitive information or manipulate the communication for malicious purposes. [11]Man-in-the-middle attacks can result in the tampering of transaction data. An attacker can intercept transaction data and tamper with its contents, such as modifying the transaction amount, thereby allowing the attacker to gain an undue advantage. Man-in-the-middle attacks can also lead to contract code tampering. For example, in a contract, an attacker may change the contract's payee address to the attacker's address, thereby charging improper fees during contract execution. A brute force cracking attack is an attack in which an attacker tries to break the security measures of a contract by continuously trying different inputs. [12]The attacker may use some automated tools and algorithms to efficiently try a large number of combinations of inputs to try to find the contract's password to perform an illegal operation.

The third threat model is the environmental risk of smart contracts. The environmental risk of smart contracts refers to the vulnerabilities that may exist in the environment in which smart contracts run, and these vulnerabilities can be exploited by attackers to carry out attacks. Common attacks include smart contract vulnerability attacks and 51% attacks. A vulnerability attack on a smart contract can result in irreversible losses due to the immutability and auto-execution nature of the contracts. Common vulnerability attacks include re-entrancy attacks and overflow attack. A re-entrancy attack occurs when an attacker exploits the capability of a contract to pause its ongoing execution and enter the execution environment of another contract while performing an external call. By doing so, the attacker can repeatedly execute a specific method, taking advantage of the vulnerability to manipulate the contract's behavior and potentially gain unauthorized access or disrupt its intended functionality. [13] [14] The attacker invokes a contract with a specific attack code in the contract, and this invoked contract triggers the attacker's pre-implanted code and invokes a function of the original contract. If the called function contains a transfer operation, then the attacker can manipulate the execution state of the contract to transfer money to his address again and again until all the funds in the contract are stolen by the attacker. An overflow attack is when an attacker inputs data into a program that is outside of a predetermined range, thus causing unexpected results during program operation. In smart contracts, overflow attacks usually involve variables of integer type, and an attacker can alter the behavior of a program or stop it from running by constructing data out of the range of the variable. A 51% attack occurs when an adversary acquires dominance over a blockchain network by controlling over 51% of the total computational power. This level of control enables the attacker to manipulate transactions or obstruct the verification of specific transactions. [15]If an attacker controls more than 51% of the arithmetic power, then he can have control over the entire network and thus can tamper with transaction records and other malicious acts.

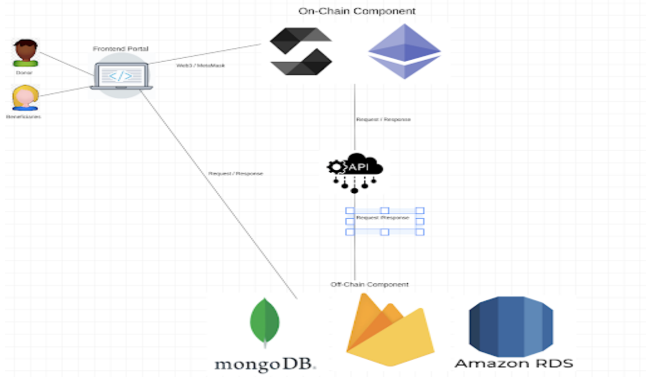
C. Security model

The security model for the random number attack is using a secure random number generator in a digital signature to prevent random number attacks. For a random number generator to be considered reliable, it must possess the ability to generate truly random numbers instead of pseudo-random numbers. This crucial characteristic ensures that the numbers generated are both unpredictable and impossible to reproduce accurately. [16]The entropy pool-based random number generator is a highly trusted and commonly used technique for generating random numbers. It operates by utilizing a combination of random events from a range of hardware and software sources as input. These random events are carefully mixed and filtered to produce truly random numbers that exhibit a high degree of unpredictability and cryptographic strength. [17]

The security model for authentication threats involves two primary components. The first component pertains to the prevention of man-in-the-middle attacks. To prevent unauthorized intervention by a third party, the integrity and authenticity of the message are verified through the use of digital signatures in this project. [18] but digital signatures do not guarantee the authenticity of the identity. Therefore it is also necessary to verify the identity of the user by using a password. The second part is the prevention of brute force attacks. Brute-force attacks can be prevented by using long and complex passwords, thus strengthening the security of passwords, or by limiting the number of access attempts and locking access to smart contracts after a certain number of password errors.

The security model for environmental risk encompasses two main components. The first aspect involves the prevention of vulnerability attacks. To avoid re-entry attacks, the smart contract must verify whether it is currently processing other function calls before executing a function. If a function call is being processed, the current call should be halted to prevent re-entry attacks. [19] During a transfer operation, it is crucial to update the recipient's balance before the sender's balance to prevent potential attackers from exploiting vulnerabilities in the contract. By doing so, the attacker is unable to call other functions in the contract prior to completion of the transfer. In addition, to guard against overflow attacks, developers should perform rigorous boundary checks to ensure input data falls within acceptable variable ranges.Another aspect to consider is the prevention of 51% attacks, which can be achieved by utilizing the PoW (Proof-of-Work) consensus mechanism. With PoW, attackers are required to invest considerable time and resources to solve mathematical puzzles before they are granted permission to add new transactions to the blockchain. This consensus mechanism requires participating nodes to verify their work before being granted permission to add new transactions. [20] [21]

D. Network model



By using a componentized structure to complete the network model, can reduce the workload, so that we don't need to implement our entire network architecture from scratch, and make the whole process simple. At the same time, using components to implement functions can make the project easier to adjust, reduce the workload of modification, and facilitate other learners to easily set up the overall data structure of the network model. Our main components are vue3, and solidity smart protocol. And we will store the off-chain computation in MongoDB in the future.

MongoDB®, developed by 10gen, Inc., is among the most commonly employed NoSQL databases in the industry. NoSQL stands for "not only SQL" and refers to databases that do not follow the traditional relational model with structured query language (SQL). [22]MongoDB is a data storage platform, which is used to store some of our data in the blockchain transaction, which is convenient for smart contracts to call. The main reason for using MongoDB for data storage is that it has the advantages of flexibility and scalability in terms of data, and can withstand a large amount of data and high traffic load. This makes a large amount of data in our agreement not to be lost, and at the same time, it has a flexible storage mode Data can be stored and managed without a predefined structure. And with the fast query mode in MongoDB, it can improve the efficiency of data calling when processing a large amount of data with smart contracts.

Vue, a progressive JavaScript framework, is commonly utilized in the development of user interfaces (UIs). [23]We make the client port of the web page into the Vue3 structure and use ts to control the smart protocol, making the front-end setup more flexible and efficient for front-end settings. And use a more modular way to build components, so that it is easier to manage complex logic and state. And we can reuse components in the future In this way, our front end is more flexible and lightweight. At the same time, through the combination of Vue3 and TS, a client application with clear structure, powerful types, improved maintainability and various tools and libraries available for you is developed. This results in efficient development, easier debugging, and a more robust end product.

Within this framework, when the front-end receives content requests from donors or beneficiaries, it invokes the smart contract system to execute the deployed smart contract on the blockchain. Upon completion of content processing, the smart contract content can be traced, and congestion issues within the smart contract during high-traffic scenarios can be alleviated. Modifications made to the state of the block trigger a broadcast to the linked nodes, thereby enabling data updates throughout the network. [24]

V. Research Methodology

A. Approaches

Ganache is a digital blockchain simulation that grants developers 100 units of test ether upon connection to Metamask, an internet-based wallet (i.e. a digital repository for cryptocurrency) employed by Truffle to execute smart contracts. [25] We first establish a virtual Ethereum currency system locally through ganache, associate this with metamask, and import multiple Ethereum currency accounts. Write the sol file and try to verify it on the remix platform to ensure that the sol smart protocol is correct. The ts file is generated through Redhat, and the ts file of vue3 is called to achieve the purpose of calling the protocol through the web page.

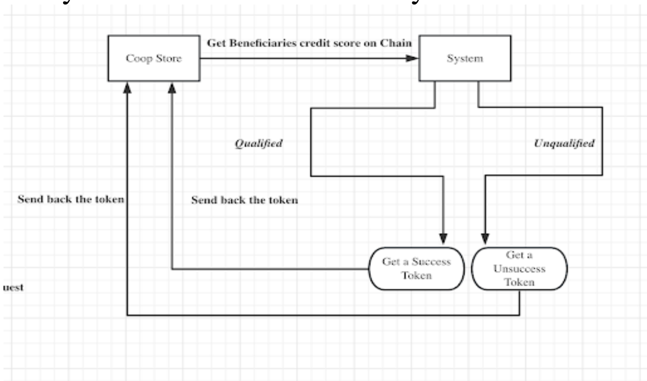
B. Protocol design

The protocol aspect of the charity has three components. First, participant identification. The smart contract needs to define the identity and authority of different participants involved in the charity activities, such as charities, donors, beneficiaries, etc. The contract needs to implement an identity verification mechanism to ensure that only authenticated participants can participate in the contract, thus ensuring the security and fairness of the contract.

Participant identification is implemented using a digital signature algorithm(DSA). The digital signature algorithm can be used to verify the identity of the participant and the authenticity of the transaction. In this algorithm, a participant can use his private key to sign the transaction information, and other participants can use that participant's public key to verify the signature, thus confirming the identity of the participant and the authenticity of the transaction. Specifically, using DSA is a digital signature algorithm. It is based on the discrete logarithm problem and uses a digital signature and verification algorithm to ensure the integrity and source reliability of the message.

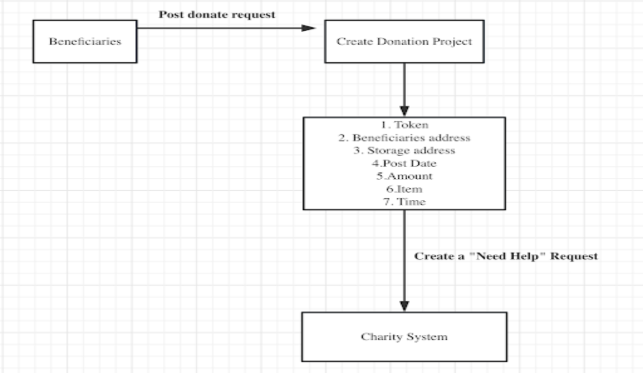
C. Donated Flow Chart

This chart is mainly used to illustrate how beneficiaries get donated. This is a very important part of our project. It describes how the store gives benefits to be donated and pass the verification process. By this method, the funds in the coop store are prevented from being forcibly acquired by malicious beneficiaries, and the purpose of clearing the balance of the coop store has been achieved. First, when the coop store receives a request from benefits, it will record the request itself and provide a spin lock to prevent the same benefit from calling the coop store multiple times to achieve the self-protection of the smart protocol. After receiving the request, the coop store will send it to the system to calculate the scores of benefits to see if the benefits meet the donation requirements. If the conditions are met, it will generate a qualified token through internal code, and if not, it will also generate an unqualified token. In order to prevent the token from being modified maliciously, all information will be calculated through the hash function, and a value of the hash function will be obtained to ensure that all content cannot be modified during transmission. When all the information is returned to the coop store, the coop store will accept all the messages and perform a hash function check on the information inside to ensure that the content has not changed. If the value of the hash function does not match, there may be an error in the data transmission, so the coop store will not accept the token and resend the original content to the system, check and return according to the benefits score again. This is the specific implementation of the entire model. At the same time, we perform multi-threaded processing while ensuring security to maximize the efficiency of smart contracts.



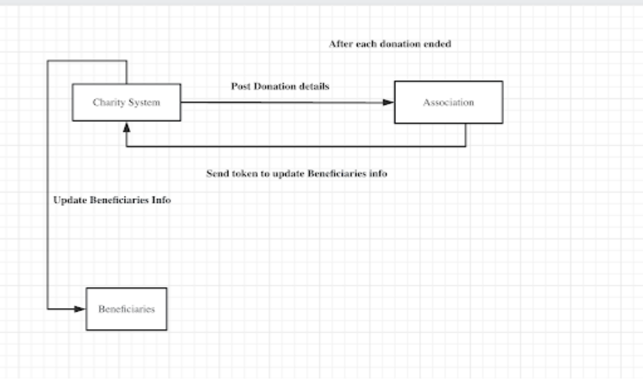
D. Beneficiaries Flow Chart

Here is how the beneficiaries post donate request work. It is mainly about the generation process of benefits post request and security protection. When benefits send a post donate request, it will be accepted by the smart agreement and create a donation project and generate 7 content segments for storage, which are token, benefits address, storage address, post date, amount, item, and time. and record it. After the donation project is stored, the content will be sent to the charity system and distribution and donation will begin. In order to ensure that the content during the transmission process is not intercepted, after the donation project is created, the encryption verification of the private key and the public key will be performed to ensure the correctness of the content, and the charity system will transmit its one-time public key to the beneficiaries for use by the beneficiaries The one-time public key encrypts the content, and when the charity system receives it, it will decrypt it with its own private key to keep the content confidential and prevent the information of beneficiaries from being maliciously intercepted and abused. In this way to ensure the security of the privacy of the beneficiaries, the platform of the charity system can be widely used by people.



E. Feedback Flow Chart

After the charity system receives the request from the user, we will send the donation detail to the association and wait for the association to complete the processing. After the association processing is completed, we will update the information of the benficiaries and send the latest token to the charity system. After the processing is completed Afterwards, the funds will be sent to the account of beneficiaries in the form of Ethereum to realize the whole process. After that the donation will end, waiting for new requests to be sent.


After each donation ended
Post Donation details
Charity System
Association
Send token to update Beneficiaries info
Update Beneficiaries Info
Beneficiaries

VI. Implementation and Experiments

A. Implementation Detail

To implement the proposed research, we developed a decentralized application (DApp) on the Ethereum blockchain using the Solidity programming language. The DApp comprises several smart contracts that handle the donation and fund management process. The smart contracts are designed to ensure transparent cy, immutability, and tamper-evidence of all transactions and data on the blockchain. In the DApp, donors can access a web interface to browse and select charitable projects to donate to. They can specify the amount of donations. The smart contracts manage the donated funds and ensure their transparent distribution to the intended beneficiaries. We integrated a decentralized identity management system to ensure secure and efficient identity verification and authentication. The system guarantees that donors' personal information remains confidential and cannot be tampered with.

In addition, we employed several security measures to protect the DApp from malicious attacks. For instance, we used role-based access control to restrict access to sensitive functions in the smart contracts. We also implemented a disaster recovery plan to ensure that the DApp remains operational in case of unexpected events. Overall, the implementation of the proposed research involved a careful selection of technologies and security measures to ensure the transparency, security, and efficiency of the donation and fund management process.

B. Evaluation Metrics

To evaluate the performance of the proposed research, we selected the following metrics:Transparency, Efficiency and Security. Transparency: This metric measures the level of transparency achieved in the donation and fund management process. We measure it by analyzing the number of transactions and the amount of funds transferred in each transaction. Efficiency: This metric measures the efficiency of the donation and fund management process. We measure it by analyzing the time required to process a donation, from the donor's submission to the successful distribution of funds. Security: This metric measures the level of security achieved in the donation and fund management process. We measure it by analyzing the number of attempted or successful attacks on the smart contracts and the identity management system.

C. Experimental Configurations

For our experiments, we used the Ropsten test network, a public Ethereum test network, to deploy and test our smart contracts and DApp. We selected a dataset of 100 charitable projects from different charitable organizations, including projects related to education, health, and poverty reduction. We compared our proposed system with traditional donation mechanisms, such as direct donations to charitable organizations or donations through third-party platforms.

D. Experimental Results

Our experimental results show that our proposed system achieved a high level of transparency, efficiency, and security in the donation and fund management process. Our system also provided donors with real-time feedback on the usage and impact of their donations, which increased their trust and engagement in charitable activities.

Account Address	Balance	Character
0x0DfeC1771aD013eF74c4B28F5533E3CB8A08067a	100.00	Donator
0x7D782dA1c52C6B5191f0e94f34489F1D8bC7ff71	100.00	Donator
0x9fc72186cabe96a404a5B679280065313A9063fd	100.00	Donator
0x1Fa92340A9edB10d51f4eE4666E771B9E5eCBe92	10.00	Donator
0x0De4751868a63A7C5fB1a8262e94634d01912B1E	5.00	Donator

Account Address	Balance	Character
0x810982b933aC773BEC0B0A3a8937b590a242Ae17	1.00	Beneficiary
0x2Af4C8AB1f247Dee258C8657cA97F91Af774c574	100.00	Beneficiary
0xeBb811DbCc67b98381a686748F6bD2185d81f07D	100.00	Beneficiary

Attribute	Value
Store Founder	Address
Donation End Date	2023/04/27
Status	Opening
Donation Amount	20ETH
Has Donated	Store
Capacity Status	0
Purpose of Establishment	Get Money

E. Insights and Analysis

The experimental results confirm the feasibility and effectiveness of using smart contracts and blockchain technology to enhance trust and transparency in the charity sector. Our proposed system provides a more efficient, secure, and transparent way of donating and managing funds, which can help address the problems of non-transparent financial management, corruption, and information asymmetry in traditional charity organizations. Our system can also help increase donor engagement and trust in charitable activities, which can lead to more sustainable and impactful social outcomes.

VII. Conclusions

In conclusion, the emergence of blockchain technology and smart contracts provides a opportunity to revolutionize charity systems. By leveraging the decentralized nature of blockchain, we can create a transparent platform that addresses the decline in social trust within the traditional charity system. This technology offers a solution that promotes transparency, public trust, and efficiency while reducing the need for human intervention and administrative overhead.

The proposed charity system provided in this paper offers a comprehensive framework including system design, workflow chart, and operational processes. The functions of the system have been successfully verified on the Ethereum blockchain, and users can easily interact with the smart contract and donate to the intended recipients through the frontend in Vue.js.By ensuring transparency in the donation process, individuals are more likely to contribute as they can witness the positive impact of their donations on those in need.

Overall, the application of blockchain technology and smart contracts in the charity sector holds tremendous potential to create a more equitable and efficient system. By embracing this innovative approach, we can foster trust, transparency, and direct resource allocation to benefit those who require assistance the most.

VIII. Statement of Work

Zhehao Fan

- In charge of writing Introduction, Related Work, half of the Preliminaries(Brief background on the selected topic)
- Write the Reference page while using the citation

Rundong Liang

- In charge of half of Preliminaries(Building blocks being used), Model, Conclusion, and Statement of Work
- Write the Reference page while using the citation

Tinghui Wu

- In charge of Research Methodology and Implementation detail under Implementation and Experiments
- Write the Reference page while using the citation

Kaiyi Chen

- In charge of Evaluation metrics, Experimental configurations, Experimental results under Implementation and Experiments
- Write the Reference page while using the citation

IX. Reference

References

[1] Morshed Mannan Primavera De Filippi. Blockchain as a confidence machine: The problem of trust challenges of governance. *Technology in Society*, 62(101284), August 2020.

[2] Whizy Kim. What happened to giving money to charity? *Vox*, 2022.

[3] Chao Li, Balaji Palanisamy, and Runhua Xu. Scalable and privacy-preserving design of on/off-chain smart contracts. pages 7–12, 2019.

[4] Ziyuan Wang, Lin Yang, Qin Wang, Donghai Liu, Zhiyu Xu, and Shigang Liu. Artchain: Blockchain-enabled platform for art marketplace. pages 447–454, 2019.

[5] Satpal Singh Kushwaha, Sandeep Joshi, Dilbag Singh, Manjit Kaur, and Heung-No Lee. Systematic review of security vulnerabilities in ethereum blockchain smart contract. *IEEE Access*, 10:6605–6621, 2022.

[6] Hangyu Tian, Kaiping Xue, Xinyi Luo, Shaohua Li, Jie Xu, Jianqing Liu, Jun Zhao, and David S. L. Wei. Enabling cross-chain transactions: A decentralized cryptocurrency exchange protocol. *IEEE Transactions on Information Forensics and Security*, 16:3928–3941, 2021.

[7] Xinle Yang, Yang Chen, and Xiaohu Chen. Effective scheme against 51history weighted information. pages 261–265, 2019.

[8] Alkhansaa Abuhashim and Chiu C. Tan. Smart contract designs on blockchain applications. pages 1–4, 2020.

[9] Mattei Maffei. Formal methods for the security analysis of smart contracts. pages 1–2, 2021.

[10] Sylvain Guilley and Youssef El Housni. 2018 workshop on fault diagnosis and tolerance in cryptography (fdtc). pages 49–54, 2018.

[11] Bhargav Pingle, Aakif Mairaj, and Ahmad Y. Javaid. Real-world man-in-the-middle (mitm) attack implementation using open source tools for instructional use. pages 0192–0197, 2018.

[12] Tanvi Gautam and Anurag Jain. Analysis of brute force attack using tg — dataset. pages 984–988, 2015.

[13] Muhammad Farman Andrijasa, Saiful Adli Ismail, and Norulhusna Ahmad. Towards automatic exploit generation for identifying re-entrancy attacks on cross-contract. pages 15–20, 2022.

[14] Yuchiro Chinen, Naoto Yanai, Jason Paul Cruz, and Shingo Okamura. Ra: Hunting for re-entrancy attacks in ethereum smart contracts via static analysis. pages 327–336, 2020.

[15] Yuechen Hao. Research of the 51 pages 278–283, 2022.

[16] Piotr Zbigniew Wieczorek and Krzysztof Gołofit. Dual-metastability time-competitive true random number generator. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(1):134–145, 2014.

[17] Mohammed Abutaha, Safwan El Assad, Ons Jallouli, Audrey Queudet, and Olivier Deforges. Design of a pseudo-chaotic number generator as a random number generator. pages 401–404, 2016.

[18] Junling Zhang. A study on application of digital signature technology. 1:498–501, 2010.

[19] Anjaneyulu Endurthi and Akhil Khare. Smart contracts resilient against malicious attacks in permission-less blockchain. pages 1201–1206, 2023.

[20] Alexander Hobbs, Andrew Kessler, and Richard De Moliner. Algorithmic balancing of hashrate in a proof-of-work (pow) consensus protocol. pages 45–48, 2022.

[21] Hamza Baniata and Attila Kertesz. Approaches to overpower proof-of-work blockchains despite minority. *IEEE Access*, 11:2952–2967, 2023.

[22] Gokul Prabagaren. Systematic approach for validating java-mongodb schema. pages 1–4, 2014.

[23] Jason Sianandar and Ida Bagus Kerthyayana Manuaba. Performance analysis of hooks functionality in react and vue frameworks. pages 139–143, 2022.

[24] Jinyoung Kim, Misoo Kim, and Eunseok Lee. Ecench: An energy bug benchmark of ethereum client software. pages 634–638, 2022.

[25] Samir Dani Abdul Jabbaraand. Investigating the link between transaction and computational costs in a blockchain environment. 58(11):3423–3436, 2020.