Design and Implementation of Donation Information Traceability System Based on Blockchain

Jiawen Zhang[1a], Mengju Shen[2b], Yidan Tian[1c], Peng Nie[3,d*]

2012032@mail.nankai.edu.cn[a], 2535766246@qq.com[b], 2011767@mail.nankai.edu.cn[c],
*Corresponding author: niepeng@nankai.edu.cn[d]

School of Business, Nankai University, Tianjin 300350, China[1]
School of Cyber Science, Nankai University, Tianjin 300350, China[2]
School of Cyber Science & Tianjin Key Laboratory of Network and Data Security Technology, Nankai University, Tianjin 300350, China[3]

ABSTRACT. With the development of philanthropy and people's growing attention to charity activities, the role of online donation platforms is becoming increasingly prominent. To solve the problems of opaque information on the existing donation platform, maliciously tampered information on the flow of donations, we designed and implemented a donation information traceability system based on the blockchain. The system can be divided into two parts: the donation and the aided module, and has three major layers: a data storage layer, a functional module layer, and an application layer. The donation information traceability system not only enhances the transparency of the donations' information but also reduces the labor cost required for information disclosure. Moreover, the system expands the role of the charity sector in Chinese society.

Keywords: Ethereum, Smart contract, Traceability information query, Donation system

1 INTRODUCTION

In the past decades, the significance and importance of giving behavior have become more apparent than ever. Governments, policymakers and individuals have been paying considerable attention to charity events. According to World Giving Index[1] by Charities Aid Foundation (CAF), more than three billion people helped someone they didn't know in 2020 and donating money was up across the globe despite, or perhaps because of the pandemic. The promising trend leads to finding a solution for a better charity platform, which is transparent, secure, auditable, and efficient[2]. However, a large number of charity platforms are still struggling to gain donors' trust and interest because of scandals inside the philanthropy part. The inherent non-profit[2] characteristic of charitable donations and lack of supervision by intermediary agencies lead to difficulty in detailed audits. In this regard, there is an urgent need for charity platforms to improve transparency and social credibility.

We established a charity platform guaranteed by blockchain, which acts as a "middleman" between donors and beneficiaries. The decentralized nature of blockchain ensures data authenticity, and conditional publicity of donating information can hopefully help to eliminate asymmetry[3]. The smart contract, one of the most important features of blockchain, helps to build trust among various parties. As a disruptive new technology, blockchain technology is

naturally suitable for social welfare scenarios due to its decentralized network, distributed shared ledger, consensus and immutability.

2 SYSTEM DESIGN

2.1 Overall frame of the system

The donation information traceability system based on blockchain is designed and implemented from the perspectives of donors, charitable organizations and recipients, revolving around the entry of information by donors, the flow and distribution of donations and the receipt of donations by recipients.

The system can be divided into two parts[4]: the donor donates the charity and the recipient receives the charity (**Fig.1**). There are two nodes for this part: the donor and the charity organization.[10] Donors need to log in, browse the charity projects, select one and donate money to it. At this stage, donation information and project information will be packaged and uploaded to the blockchain. Charity organizations are responsible for providing and authenticating the public welfare project and uploading them onto the blockchain; they are also responsible for verifying the identity of donors. Considering citizens' privacy, we do not upload donor's personal information onto the blockchain but in the database.

In the part where recipients receive donations, there are still two nodes, the recipient and the charity organization. Recipients first uploads their request for help, and the charity verifies their identity and the authenticity of request, then uploads help information to the blockchain. Similarly, we stored the personal information of help seekers in the database. At the stage when platform receives the donations, it uploads the flow of funds to the blockchain. After information is posted, a transaction number is returned. Through this number, we can find the transaction information. Therefore, we store the number of each transaction in the corresponding table.
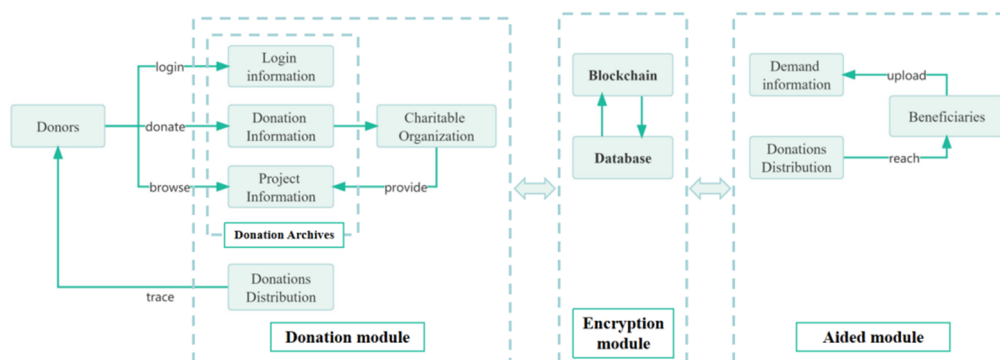

Fig. 1. System framework

For the platform information query function, donors can log in to check their historical donation information, but also to view the specific flow of funds and distribution information of each

donation. The charity has access to all donors' donation information. It is also possible to track 'problem' donations. For example, by inputting one person's donation information, the charity can find all the donors who have contributed to the same charity project.

2.2 Architecture of the system

The donation information traceability platform based on blockchain includes a data storage layer, a functional module layer and an application layer (**Fig.2**)[10]. In the data storage layer, data is stored in relational databases, which stores information such as basic user information and the "love token" IDs owned by users. The blockchain stores information on the creation, donation and use of "love tokens" to ensure that they cannot be tampered with, allowing the system to query the flow of "love tokens".

Functional layer includes the user registration and login, data collection query module. The data collection module collects information about "love tokens" and interacts with the data storage layer. The application layer provides interfaces for different objects, including token exchange interface, token donation interface, token usage interface, token flow query interface, user login and registration interface.
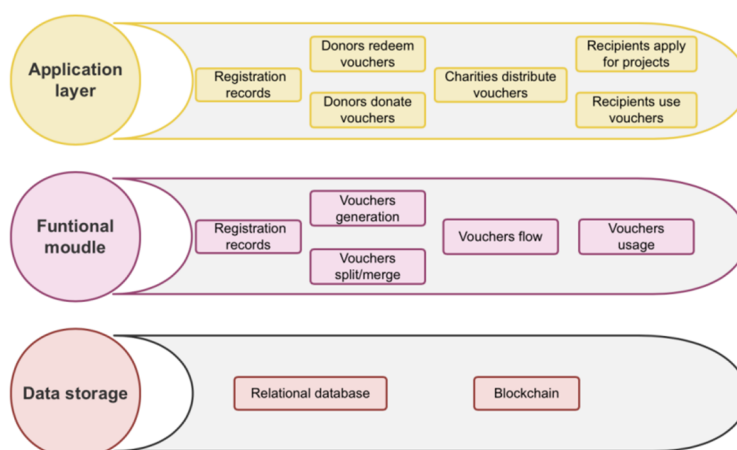

Fig. 2. System hierarchy diagram

3 IMPLEMENTATION OF THE SYSTEM

3.1 Design of the smart contract

The decentralization of blockchain has been applied in various fields, which has driven the rapid development and upgrading of blockchain technology[5]. The era of blockchain 2.0 represented by Ethereum has arrived, an important symbol of which is the application of smart contracts[6]. Therefore, this system uses Solidity smart contract to achieve practical functionality based on Ether. The platform uploads information about flow of charity funds on the blockchain through smart contracts. It is pre-compiled and deployed on the alliance chain. Donors and third-party charities can call the interface in the smart contract when they query information on the blockchain, which greatly improves the trustworthiness of the operation.

Firstly, we define three data structures to record information about the generation, flow and use of the funds[10]. We then define three mappings to record them and their corresponding automatic incremental numbers. In the information collection function, we add new information to the mapping and return the number corresponding to the event information, which is stored in the database. In the information query function, according to the number entered, we can find the specific information in the mapping and return it. If there is a write operation in the function of a smart contract, it will involve a transaction release. At this time, we cannot get the return value of the function. If we want to read that value during the transaction, we must use events and get the result via events with the back-end java code[7].

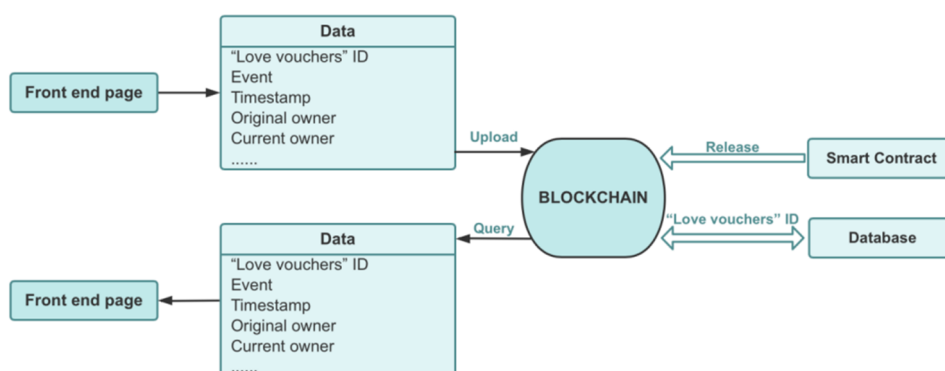## 3.2 Interaction between data and Ethereum

Fig. 3. Interaction between data and Ethereum.

First, we initialize a Private Blockchain via the genesis.json file. Then, we call the JSON_RPC interface provided by Ethereum through Ethereum's official lightweight SDK web3.js to realize the interaction with private chain. After the private chain is established, nodes need to be added first to provide accounts for each uploader to post transactions[8]. These nodes can be synchronized by the blockchain consensus mechanism. The next step is the process of data interaction (**Fig.3**).

Information entry. In the information entry module, the uploader enters detailed information that needs to be chained from front-end page. The data is then obtained by the back-end and encrypted using the SM3 secret algorithm. Next, the information is submitted by calling a function in the smart contract, published on the blockchain and the returned information number is stored in the database.

Information query. In the Flow Information Enquiry module, donor first logs in. When user sends a query request, the system will first find the specific location in the database. For historical donations, the system will search the database directly and return the results to the user. For donation traceability information, the system will first search the database for "love tokens" ids, and then find relevant transactions. These numbers are then used to find the corresponding information on the blockchain. Finally the returned information is consolidated and presented to the user.

Token splitting. Donors choose to donate a certain amount of their existing vouchers to a project, and the system uploads the voucher transfer or split information to the blockchain. For voucher donations, if the original voucher amount is equal to the donor's donation amount, then the vouchers do not need to be split and can be transferred directly. The voucher transfer information includes: voucher ID, voucher status, ownership before and after transfer, timestamp, and event description (*Transfer*). If the voucher amount is greater than their donation, the voucher will be split into two, one with an amount equal to the donation, which belonged to recipient; the other with the original voucher amount minus donation amount, and the owner remains the same. The status of the split token, instead of original one, will be valid, which will be uploaded onto blockchain. If the amount of a single voucher is less than the donation amount, the voucher will be transferred and the donation amount will be subtracted from the voucher amount, and next voucher will be selected in order of id.

The charity chooses to donate a certain amount of love tokens already in their account, and the system uploads the transfer or split information to the blockchain.

4   CONCLUSION

In order to control the scandals of "Internet + Philanthropy"[9], we use blockchain to create an charity traceability platform, enhancing the transparency. In this system, we build an Ethernet private chain and store the donor information, monetary flow information and recipient information on it. This ensures that the results obtained are not tampered with, which greatly enhances people's trust in Internet charity. Meanwhile, we have designed the "love tokens" , which can be split to create new entities each time they flow through the system. Finally, we provide a unified platform for donors and charities to check the history of donation flow.

Philanthropy empowered by blockchain is expanding the role in Chinese society. Blockchain is turning charity into a strategic convener, bringing multiple objects to work together in a more transparent and efficient manner.

REFERENCES

[1] Charities Aid Foundation, 2021.CAF WORLD GIVING INDEX 2021. www.cafonline.org

[2] Farooq, M. S., Khan, M., & Abid, A. (2020). A framework to make charity collection transparent and auditable using blockchain technology. Computers and Electrical Engineering, 83. https://doi.org/10.1016/j.compeleceng.2020.106588

[3] Wu, H., & Zhu, X. (2020). Developing a Reliable Service System of Charity Donation during the Covid-19 Outbreak. IEEE Access, 8, 154848–154860. https://doi.org/10.1109/ACCESS.2020.3017654

[4] Feki, E. et al. (2022) 'BELONG: Blockchain basEd pLatform fOr donation \& social project fuNdinG'. Available at: https://search.ebscohost.com/login.aspx?direct=true&db=edshal&AN=edshal.hal.03822576v1&lang= zh-cn&site=eds-live (Accessed: 8 March 2023).

[5] Ma Chunguang, An Jing, Bi Wei, Yuan Qi. Smart Contracts in Blockchain[J]. Information Network Security, 2018(11): 8-17.

[6] Li He. (2017).Blockchain 2.0 architecture and its application in insurance industry[J]. Golden Card Project   2017 (1) 45-29.
https://kns.cnki.net/kcms/detail/detail.aspx?FileName=ZGJN201706014&DbName=CJFQ2017

[7] Qian Weining, Shao Qifeng, Zhu Yanchao et al. Block chain and credible data management: problems and methods [J]. Journal of software, 2018, 29 (01) : 150-159. The DOI: 10.13328 / j.carol carroll nki jos. 005434.

[8] Ugaz-Burga, C., Espinoza-Grados, R. and Cardenas-Salas, D. (2021) 'Blockchain and smart contract for donation traceability', 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), Trends in Electronics and Informatics (ICOEI), 2021 5th International Conference on, pp. 510–517. doi:10.1109/ICOEI51242.2021.9453016.

[9] Xu Dukang. Research on blockchain-based trusted donation technology [D]. Nanjing University of Posts and Telecommunications, 2022.DOI:10.27251/d.cnki.gnjdc.2022.001407.

[10] Nie P, Zhou X, Wang C, Zheng H, Zeng Y. Design and Implementation of Coronavirus Vaccines Information Traceability System based on Blockchain. 2021 International Symposium on Artificial Intelligence and its Application on Media (ISAIAM), Artificial Intelligence and its Application on Media (ISAIAM), 2021 International Symposium on, ISAIAM. May 2021:121-124. doi:10.1109/ISAIAM53259.2021.00032