Charity System Based on Blockchain

Problem Statement

The charity organizations lack transparency and the supervision to them is difficult to achieve, which has a negative impact on the willingness of the people to donate.

Blockchain as a underlying technology of Bitcoin system provides a new solution for the charity system in terms of technology. This project aims to increase the transparency of charities to enhance the public's trust in charities and promote the development of philanthropy by blockchain-based charity system.

Introduction

With the development of Internet technology, there are more and more information access channels for people, philanthropy has become more open and transparent. Many problems in the process of philanthropy has been exposed. According to media reports, some people sold relief supplies and tents for money in the " 5.12 Wenchuan Earthquake", which showed the confusing daily management of charitable funds and materials. These caused a decline in willingness to donate and a reduction in donations between 2009 and 2012. At the same time, online crowdfunding has become a new way for the public to participate in public welfare undertakings. The crowdfunding platform has established a database for the project, a proper monitoring of the project is also an important part of the risk automatic control mechanism of the public welfare crowdfunding platform.

Improving the transparency of philanthropic information is an important way to improve credibility for traditional donation and internet crowdfunding. Using Internet technology, a traceability system can be established to increase the transparency of charities technically. For this purpose, this project idea is proposed.

Literature Review

Blockchain Technology

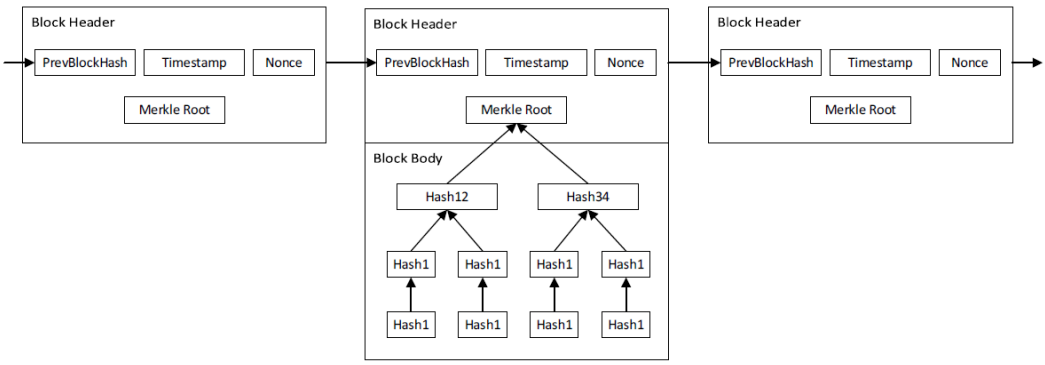
As the basic technology of Bitcoin, blockchain is decentralized, non-temperable, anonymous and traceable, that has great potential in

transforming traditional industries. A blockchain is a distributed database system involving multiple independent nodes. The entire database is maintained by nodes throughout the network. The blockchain can record all transaction information, whose process is efficient and transparent and the data is highly secure.

A blockchain is a series of blocks, each block consists of a block header and a block body. The block header contains metadata and the transaction data is encapsulated in the block body. The hash value (PrevBlockHash), timestamp (Timestamp), random number (Nonce), and Merkle Root of the previous block is contained in the header. The block body stores multiple transactions from the previous block in the form of a Merkle Tree. The leaf node of the Merkle Tree stores the hash value of the transaction information, and the non-leaf node stores the combined hash value of all the leaf nodes below it. The blockchain system is built on a P2P network, does not require a centralized organization as a credit endorsement. After the transaction, every node competes for accounting rights through a consensus mechanism. The node that wins the competition will package all transactions that occurred

within a certain period of time. The block will be broadcast to the whole network and all nodes will verify the block. After most nodes have authenticated successfully, the block will be added to the chain. From the beginning of the transaction to the end, each transaction is open and transparent, and there is no way to deceive each other between nodes. Asymmetric encryption enables anonymous transactions, and the chain structure ensures transaction traceability.

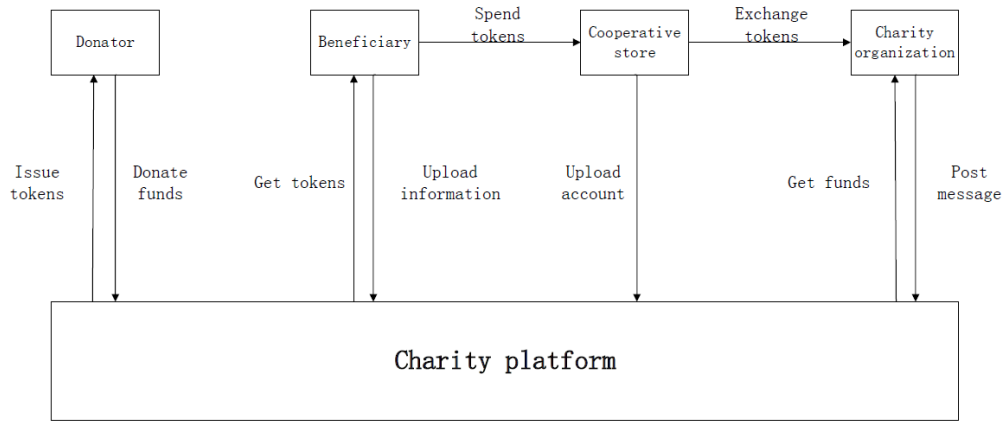
The data structure of the blockchain is shown below.



▼ Design

1. Charity System Mode

The charity system mode proposed is shown below.



There are four roles: donors, beneficiaries, charity organizations and cooperative stores.

The charity organizations get information of seek help and create charity projects through the platform.

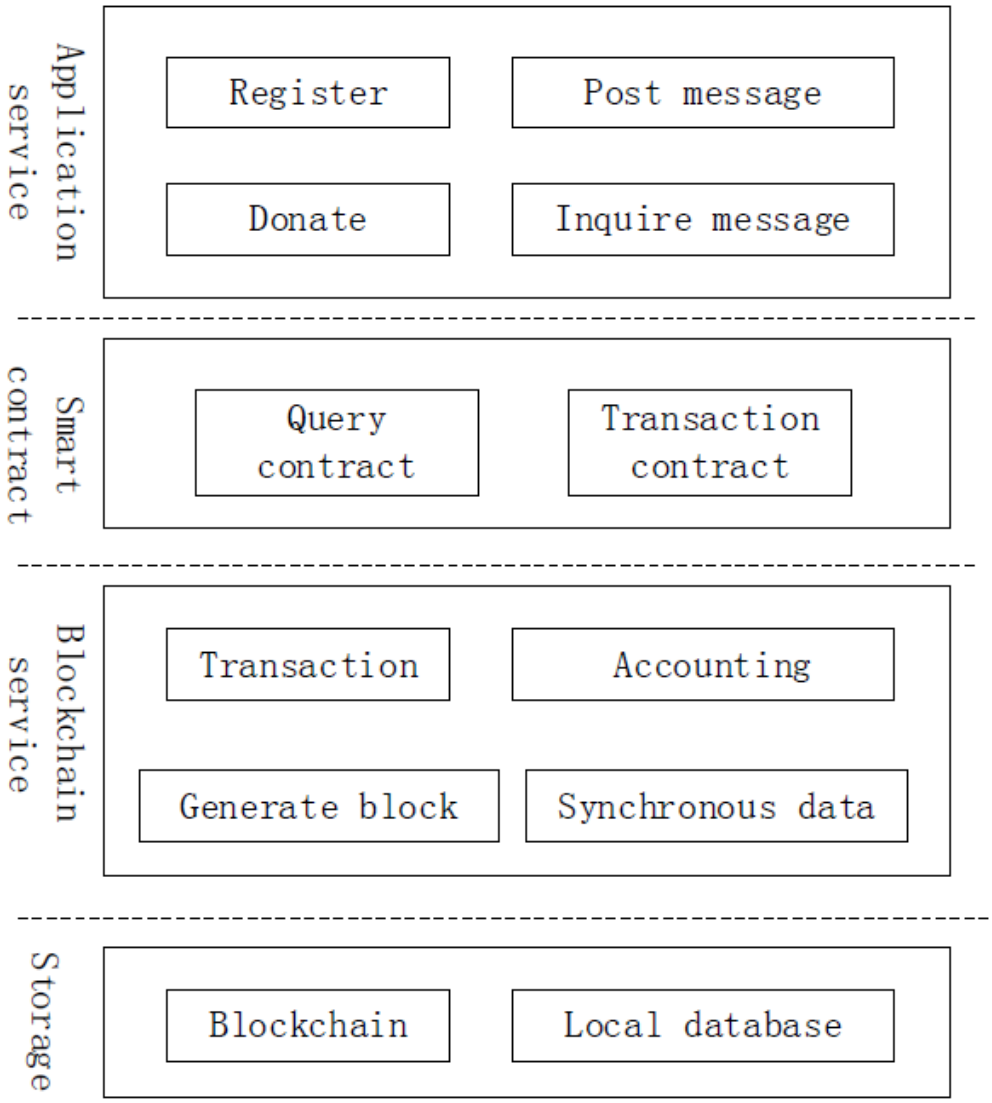
Donors learn about charity projects on the platform, then donate to beneficiaries or the charity organizations.

Beneficiaries upload their information to the platform for help, they can get and spend tokens in cooperative stores. The transactions occurred in the stores will be uploaded to the charity platform.
The cooperative stores supply services or goods to the beneficiaries to obtain tokens. The tokens can be exchanged for real money by charity organizations.

The flow of funds has been fully recorded on the blockchain, which allows transactions to be tracked and funds prevented from being abused.

2. Proposed Platform Architecture

We divide the platform into four layers, as shown below.



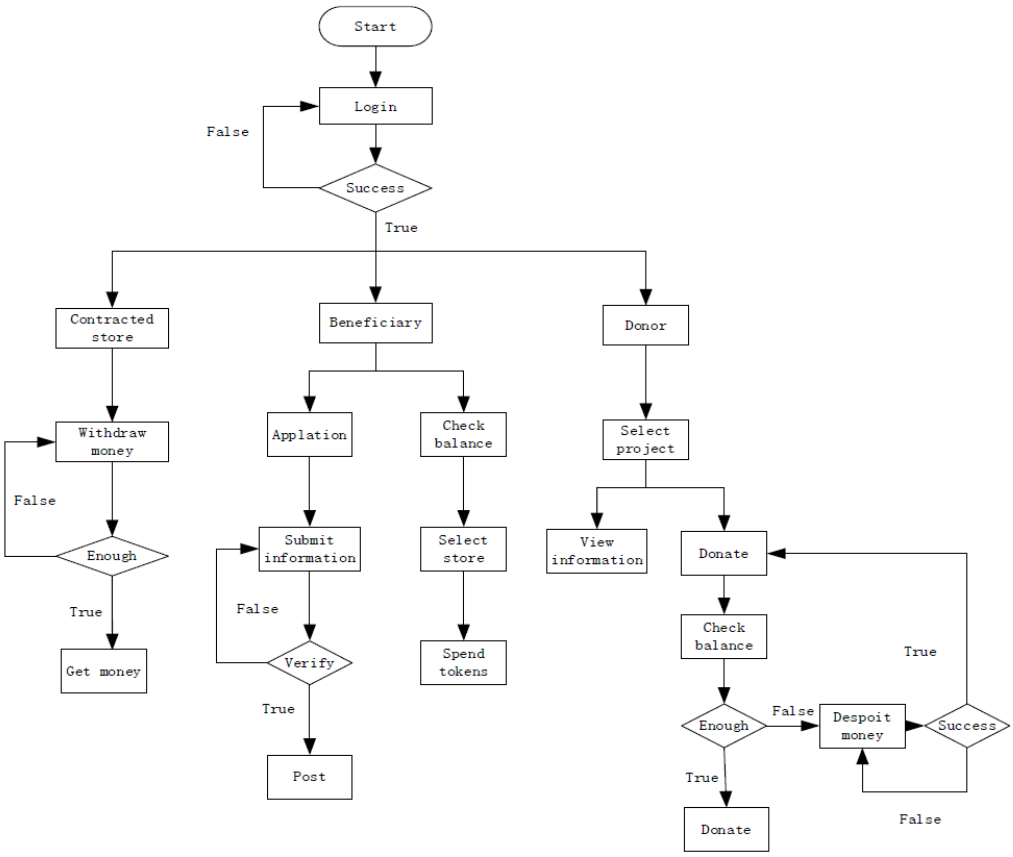
The application service layer encapsulates a variety of applications, including account registration, post charity information, donate funds, and inquire message, provides users with the functions of the platform directly.

The smart contract layer includes various scripts and smart contracts. It encapsulates query methods, transactions process and other details.

The blockchain service layer implements the functions of distributed accounting of the charity platform, including package block, get consensus on transaction, broadcast block, and synchronize data to a local database.

The storage layer is used to store data, including blockchain storage and local storage.

3. **Platform Usage Process**



1. Donor

After successful login, the donor browses the charity projects and select one project to be donated.

The system will check the balance of donor account. If the balance is insufficient, the user will be reminded to deposit. Donation can be completed only the balance is sufficient.

2.People in need

The people who need help should fill in the rescue information which will be uploaded to the charity organization for review, and the approved projects will be posted on the charity platform. The beneficiary can check the account balance to know the project status, and then use the tokens in cooperative shops to obtain services or products.

3.Cooperative shops

The shops provides the corresponding services or goods such as medicines or books to the

beneficiaries to obtain tokens. They can exchange tokens for real money by charity organizations.

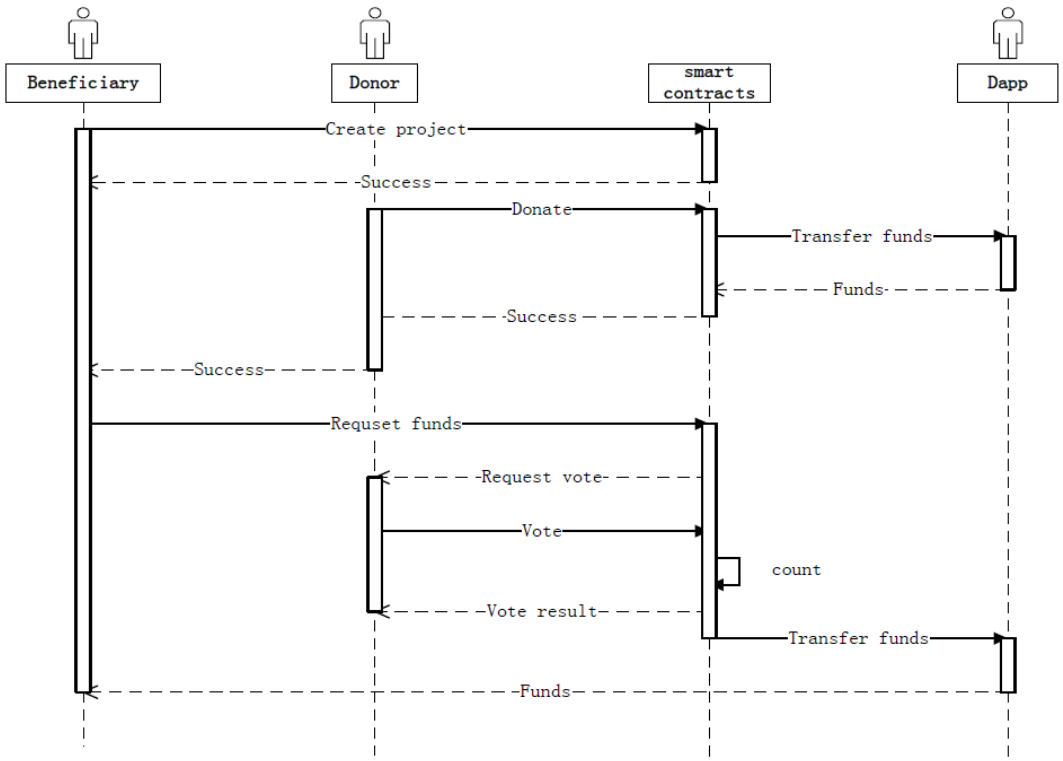
4.Charity organization

The organization can get donation from the platform to help other people and apply money to the cooperative shops for token exchanging.

▼ Development of System

1. **Dapp Model:**

   We will develope a charity fundraiser Dapp which is based on Ethereum to verify our system and demonstrate some core functions of the charity platform. MetaMask Browser Extension will be used to test our system and Solidity will be used to built smart contracts. The functions of creating project, donating, approving funds and transferring funds have been verified by us with the Dapp.



A beneficiary initiates a charity project through a smart contract, then the project will be deployed on the blockchain. Donors view the charity project in browser and select a appropriate project to make donation. The funds will be transferred to the Dapp administrator account. When the beneficiary needs

funds, the capital expenditure request is initiated with the smart contract, If most people who participate in the project agree to the request by voting, the donation funds of the project will be transferred from the Dapp administrator account to the beneficiary account.

2. **Build Smart Contracts**

   Smart contracts are value streams based on specific terms and conditions. Different from real contracts, smart contracts are completely digital, they are pre-programmed code stored on the blockchain. As the expansion of the blockchain, the smart contracts adapt well to the decentralization of the blockchain which can run in the whole network node. The transactions using the smart contract will be recorded on the blockchain without the need of managers. Once conditions are met, the smart contract will be executed automatically. Smart contracts can be used to define transaction logic for charity platform.
   In the Dapp, we have built smart contract to meet the functions described in the previous section, smart contracts structure is shown in Figure 6. Users can create a charity project using The ProjectList Contract which also supplies the view of all projects recorded on the blockchain. The Project contract is used to describe and store specific charity project, which provides an interface to operate the charity project and its funds. The structure of tokens expenditures is designed separately.

3. **Dapp smart contract structure**

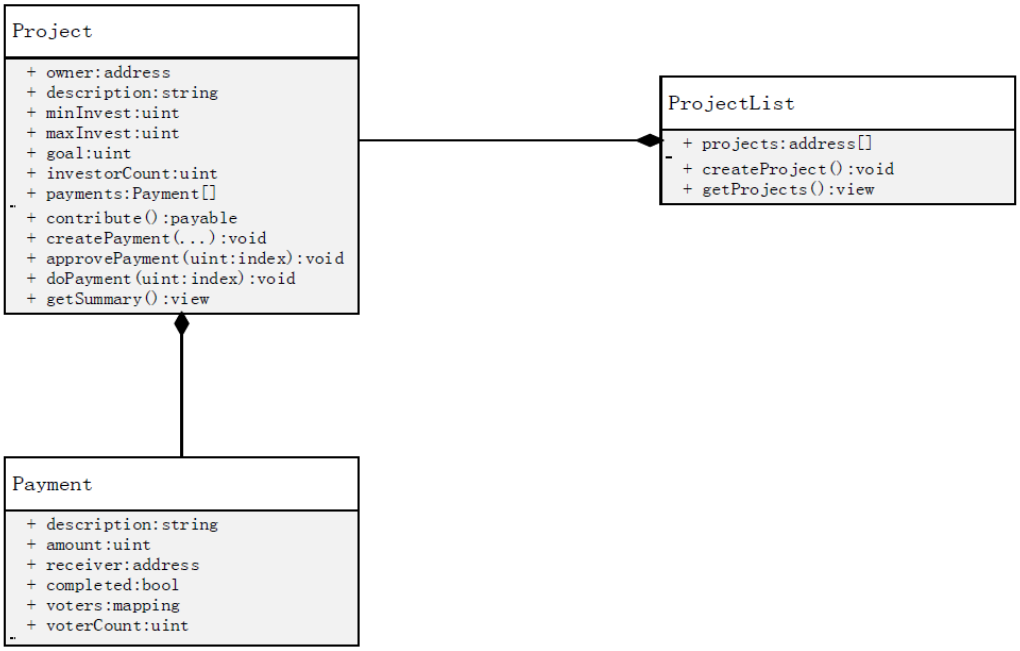


Figure 6. Dapp smart contract structure