

# Blockchain-Based Charitable Donation Privacy Protection Scheme

Le Deng\*, Shuxian Liu, Huan Xu, Wei Wang, Wenzhong Yang

*School of Information Science and Engineering of Xinjiang University, Urumqi, China*

## Abstract

Blockchain has the characteristics of decentralization, tamper-proof, information traceability, openness and transparency, and has a good fit with charitable donations. Aiming at the problems of data center management, poor transparency and tampering in the existing charity traceability process, a secure sharing scheme of charity donation data based on blockchain is proposed. The scheme uses the blockchain to store the hash value, key and access policy of the encrypted data, and the original data is stored in IPFS(InterPlanetary File System), which ensures the privacy of users. A trust model based on reward and punishment mechanism is proposed to evaluate the trust value according to the behavior of nodes. Ciphertext policy attribute encryption technology combining trust and time attribute is used in smart contract to design data security sharing method. After evaluation and analysis, the scheme has the characteristics of openness and transparency, decentralization, and difficulty in tampering, which provides a new reference for solving the long-standing corruption problem in the charity field.

## Keywords

blockchain,charity,access control

## 1 Introduction

In modern society, various charitable forces represented by charitable organizations have grown rapidly, and social charitable awareness has been significantly enhanced. Charitable donations through charitable organizations play an important role in national and regional responses to emergencies, such as the Novel Coronavirus (Covid-19) epidemic, earthquakes, typhoons, floods and other disasters, as well as social and public issues such as poverty alleviation, pensions, and diseases. With the disclosure of various charitable scandals, problems in the process of charitable donations have been exposed to the public one by one, such as the lack of credibility of charitable organizations, corruption of charitable organizations, low transparency of information disclosure, and the inability to trace the use of donations, which has led to scandals in the charitable industry. The public gradually lost trust in the charity industry.

The emergence of blockchain brings hope to solve problems in the field of charity, everyone turns their attention to promoting the transformation of public welfare into blockchain, hoping to use blockchain to realize on-chain donations and information traceability. The features of blockchain, such as decentralization, openness and transparency, information that cannot be tampered with and traceable, and smart contracts, can perfectly solve the problems in philanthropy. Combining blockchain technology with the public welfare system can effectively monitor the whereabouts of each donation, forming a closed loop from fundraising to donation. Due to the characteristics of blockchain technology, it is difficult to modify the data once recorded, which can greatly improve the public's trust in non-profit organizations, so that non-profit organizations can self-certify their fairness and fairness, improve transparency, and build credibility.

In recent years, academics from around the world have performed substantial research on how to address the problem of public distrust in philanthropic organizations. Basil D Z summary how might

---

AIoTC2022@International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology

EMAIL: \*sc\_dengle@stu.xju.edu.cn (Le Deng)



© 2022 Copyright for this paper by its authors.

Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings (CEUR-WS.org)

cause-related marketing affect attitudes toward the charity involved[1]; MD Diarmuid Analyzed the characteristics of charities in charities to drive charitable accountability [2]; Inger Lyngdrup explores when and why charity vanished from public relief in Copenhagen and thereby differentiates itself from the traditional research field on welfare that focuses on studying the growth of taxation and social spending in the 19th century[3]; Davidson S points to potential fraud by middlemen who oversee and manage money[4]; A. Farsya Kirana aims to examine the institutional mechanism and information systems success factors that influence trust and distrust in the online donation platform and how it influences attitude and online donation intention[5]. Some scholars tries to propose a charitable donation system combined with Internet technology,Hai-ying YU proposes a model of trust formation in online charity information, rooted in the information processing theory [6]; Lanerolle proposes a system that manages donations after investigating current disaster management system in Sri Lanka and in several other countries which get affected by natural disasters frequently [7]. D.Chhibber Virtualizing Food Donation Distribution through Mobile Application and Cloud-Based Supply Chain Management[8]. Although the above methods have certain improvement effects, they have not changed the problems existing in the traditional charitable donation process, and the credibility of charitable undertakings is still low. With the development of blockchain technology, a type of solution has emerged, namely blockchain + charity: Mohd Nor R proposed a decentralized, authentic and transparent donation system to solve the problems of additional fees, information opacity and processing delays in online donation platforms[9]. Wu H developing a reliable service system of charity donation loaded on the blockchain to cope with the complex service needs of charities due to the COVID-19 epidemic[10];Farooq M S designed a blockchain-based charity management platform aiming to provide a transparent, secure, auditable and efficient system[11].

These methods make some improvements in the donation method, but they do not consider the privacy information involved in the donation process, and the privacy information of participants is not protected. We think attribute encryption can be used to protect privacy.Zhang X proposed a novel blockchain-based architecture for data sharing with attribute-based cryptosystem (BaDS), the architecture can achieve privacy-preserving,user-self-controlled data sharing, and decentralization by using blockchain and several attribute-based cryptosystems[12]. Axin Wu In view of the efficiency of ABE, the privacy protection of the attribute and the abuse of the secret key, the efficient and privacy-preserving traceable attribute-based encryption in blockchain is proposed[13]. Zhang X propose a privacy-preserving and user-controlled architecture for data sharing based on blockchain system and Ciphertext-Policy Attribute-Based Encryption (CP-ABE), called ThemisABE[14].

In this paper,we proposes a charity foundation scheme based on blockchain,Our main contributions are as follow:

- We propose a blockchain-based charity donation privacy protection scheme that aims to provide a transparent, secure, auditable, and efficient system. At the same time,we established a trust model for nodes, and a trust evaluation framework is proposed.
- Combining symmetric encryption with attribute encryption, we not only protect the confidentiality of data, but also provide fine-grained access to data according to user roles and attributes.
- We use the time attribute to automatically revoke the user's attribute key, which solves the key management problem existing in the ABE solution.

## 2 Preliminaries

### 2.1 Blockchain

On October 31, 2008, Satoshi Nakamoto posted an article on the Cypherpunk mailing list entitled "Bitcoin: A peer-to-peer Electronic Cash System, this paper points out the disadvantages of traditional Electronic payment System and proposes an Electronic payment System based on cryptography instead of credit. With the success of Bitcoin, blockchain, the underlying technology of bitcoin, has received wide attention around the world. Blockchain is a new application mode of distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and other computer technologies. Its essence is a decentralized database, which is a string of data blocks associated with cryptography. Each data block contains a certain amount of transaction information, which is used to

verify the validity of its information and generate the next block. In a narrow sense, blockchain is a distributed ledger that combines blocks of data in a sequential manner in chronological order, and is cryptographically immutable and unforged. Broadly speaking, the block chain technology is to use the piece of chain to verify the data structure and data storage and use of distributed node consensus mechanism to generate and update the data, use cryptography ways to ensure the safety of data transmission and access, use of intelligent automation scripts code contracts to programming and operating data of a new kind of distributed infrastructure and calculation.

## **2.2 Smart contract**

A smart contract is a computer protocol that runs programmatically on a blockchain and is automatically validated, irreversible, and performed. The cryptographer Nick Szabo made the initial suggestion in 1994. The goal is to reduce the reliance of traders on reliable third parties by converting traditional contract terms into code and embedding them in hardware or software that can be implemented autonomously. The development of practical smart contracts is now possible because to the advent of blockchain technology and the availability of platforms for developing smart contracts built on high-level languages like C++ and Solidity. A set of executable functions, state variables, and identifying addresses make up a smart contract, which is essentially a state machine. Other users can start a transaction to the specified contract by identifying the address, which activates the relevant execution function in the specified contract, returns the execution result, and updates the status of the contract. This happens after the contract deployer has specified the pertinent permission confirmation logic and uploaded the compiled contract to the blockchain. As a result, smart contracts increase the computing power of blockchains and enable developers to govern and control data on the chain using logical operations.

## **2.3 Attribute-based encryption**

In order to enable one-to-many data sharing, the attribute encryption mechanism uses a number of user attributes as identity identifiers and defines an access policy that corresponds to a set of attributes. The ciphertext corresponds to an access control structure, and the key corresponds to a set of attributes. The decryption succeeds only when the attributes of the access user meet the corresponding access control structure.

# **3 Proposed scheme**

## **3.1 System model**

The charity foundation system model proposed in this paper is mainly composed of users, non-profit organizations (NPO), regulatory organizations, logistics enterprises, consortium blockchain and IPFS, as shown in Figure 1.

### **1) User**

Users can be divided into donor and beneficiary, and users can choose their identity after registering. Donor can donate according to their personal wishes and set up access policies for personal privacy information. The beneficiary submits help information in the system.

### **2) Non-Profit Organizations**

The subject trusted by users will generate donation projects according to the information submitted by the beneficiary, formulate use plans for the donations and materials received by the project, and collect feedback information.

### **3) Regulatory organization**

Responsible for the distribution of relevant certificates to users who apply for registration, and as the supervision department of donation process, to supervise and manage non-profit organizations.

### **4) Logistics enterprises**

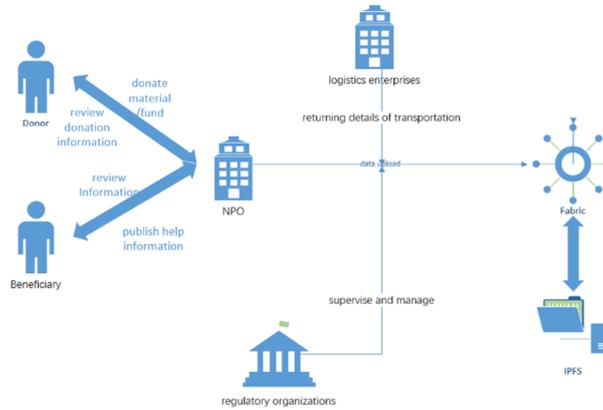
Provide material transportation services for the NPOs, returning details of transportation.

### **5) Consortium Blockchain**

The consortium blockchain consists of a number of non-profit organizations and regulatory organizations that jointly maintain the blockchain. Donation metadata is stored in the consortium blockchain to prevent data from being maliciously tampered with or corrupted.

#### 6) IPFS

Store the original data of the donation information and generate the hash address of the original data.



**Figure 1** System Network Architecture Diagram

### 3.2 Trust model based on reward and punishment mechanism

Blockchain generally uses peer-to-peer network(P2P) as a network mode, in P2P network, users can share information freely, but the characteristics of openness and anonymity provide convenience for malicious nodes lacking sense of responsibility to abuse the network. Aiming at the problem of malicious nodes in the network, a trust model for nodes is established, and a trust evaluation framework is proposed by taking reputation, scale and transparency of nodes as trust factors. We introduces reward and punishment mechanism, transparency report index and Zhongji transparency index FTI(China Foundation Transparency index) as an intuitive evaluation system to optimize the existing charity model and improve the trust model.

In the scheme, the nodes are divided into user nodes and organization nodes. The user node is a network node used by user, and only one trust factors, namely the reputation of the node, need to be considered for personal use. Institutional nodes are used by NPO, supervisory agencies and logistics enterprises respectively. The credit factors of supervisory agencies and logistics enterprises Only consider reputation a trust factor, while NPO also consider scale and transparency on the basis of reputation. An initial reputation value will be assigned to each node during initialization, both users and organizations have the function of reporting. When users or organizations have malicious behavior, they can expose malicious behavior through the reporting function. When the malicious behavior is verified successfully, the whistleblower will gain reputation, and the reputation of the malicious user will be reduced by 10 points, Minimum trust value is 0. The reputation of the user will be increased by 1 point for every normal donation or assistance completed; the reputation of the institution will be increased by 1 point for every 10 normal projects completed, Trust value up to 100.

The network provides a new channel for the development of philanthropy, provides a platform for NPO, establishes and enhances the relationship between NPO and donors, volunteers and beneficiary.

- reputation is one of the important factors affecting the charity industry. Whether individuals or organizations, good reputation has a positive effect on them and can establish trust relationships. This scheme is evaluated according to the behavior of nodes in the network, and the reputation value is always in the range of 0-100. Initialization assigns an initial reputation value to each node, according to the behavior of the node in the system to enhance or reduce the reputation value  $r$ , the trust value  $Tr$  based on reputation can be expressed as :

$$Tr = 10 \times \frac{r}{100}, r \in [0,100] \quad (1)$$

- scale is a trust factor that NPO need to consider. The size of the NPO will affect users' judgment. Users who lack donation experience will be easy to choose larger NPO, and believe that their

services and processes are more standardized. This scheme determines the size of the organization according to the information submitted by the NPO when it is registered. The determination of the size is mainly based on the two factors of organizational assets A and the number of employees S. Classification of assets, every ten times a score, 100000 level is 0-2, million level is 2-4, 10 million level is 4-6, billion level is 6-8, billion and above is 8-10 ; the classification of the number of employees is similar, with 0 – 2 in individual level, 2 – 4 in 10 level, 4 – 6 in 100 level, 6 – 8 in thousand level and 8 – 10 in thousand level. The trust value Ts based on scale can be expressed as :

$$T_s = A \times 50\% + S \times 50\% \quad (2)$$

- Donor tend to trust NPO with high transparency. After entering the era of online philanthropy, it is easy for the public to obtain donation information, but the information disclosure is not good. Information disclosure includes basic information disclosure, fundraising information disclosure, project implementation information disclosure, financial information disclosure, daily disclosure, and disclosure channels / frequencies. This scheme calculates the trust value Tp based on transparency according to the China Charity Transparency Report Index issued by the China Charity Donation Information Center under the Ministry of Civil Affairs, the ranking index of China ' s most transparent charitable foundation, the development of the foundation center network, and the ' Central Fund Transparency Index ' FTI provided by the Center for Integrity and Governance Research of Tsinghua University. For fair selection of data in recent three years, the average values are calculated to be i1, i2 and i3, which can be expressed as :

$$T_p = i_1 \times 20\% + i_2 \times 30\% + i_3 \times 50\% \quad (3)$$

- The trust value calculation of node: based on the four trust factors of network capability, reputation, scale and transparency, the trust value of any node k in the network is defined as Tk, and the user node does not consider the scale Ts and transparency Tp, which can be expressed as:

$$T_k = \begin{cases} T_r \times 0.4 + T_s \times 0.2 + T_p \times 0.4, & T_r \geq 6 \\ -T_r \times 0.4 + T_s \times 0.2 + T_p \times 0.4, & T_r < 6 \end{cases} \quad (4)$$

The weight coefficient in this scheme is set according to the network and the actual situation. Nodes with reputation value greater than or equal to 6 can receive the gain from reputation, and the trust evaluation score is higher. Nodes with reputation value less than 6 are punished, which reduces their trust value.

### 3.3 Donation data access control

It is composed of four stages of system initialization, data encryption, data storage, and data access. In this process, in order to improve encryption efficiency, the symmetric encryption algorithm SM4 and CP-ABE are combined, and the original data is encrypted using the symmetric encryption algorithm, and then the symmetric key is encrypted with the CP-ABE algorithm, which realizes fine-grained access control while ensuring data confidentiality.

#### 3.3.1 System initialization

Execute the initialization algorithm of the property-based encryption to initialize the system's parameters and produce the system's master key MK and common parameter PK. The user initiates a registration request to the regulator and submits the identity information Infouser (nickname, ID number, name, contact information, etc.), and after the regulator verifies the identity information, a public-private key pair (Pub<sub>user</sub>, Pri<sub>user</sub>) and a certificate Cert<sub>user</sub> representing his identity are generated. The collection of attributes A<sub>user</sub> is determined based on the identification data that the user has provided, and the regulator then provides the user the public-private key pair, identity certificate, and attribute collection through a secure channel.

---

Procedure init:

---

- 1 .  $PK, MK \leftarrow CPABE_{setup}(1^\lambda)$
- 2 . User send  $info_{user}$  to institution
- 3 . If institution pass user's request Then  
     generate  $(Pub_{user}, Pri_{user}), Cert_{user}$
- 4 .  $A_{user} \leftarrow Extract Info_{user}$
- 5 . Send  $(Pub_{user}, Pri_{user}), Cert_{user}, A_{user}$  to user

---

### 3.3.2 Data encryption

The random key  $K(K=k_1 \otimes k_2)$  for symmetric encryption is calculated when the data owner uploads the donated material after first generating two random keys,  $k_1$  and  $k_2$ . To ensure the safe keeping of the original data file, the SM4 symmetric encryption technique uses  $K$  as the encryption key.  $File_{enc}$  is used to represent the encrypted file. The original data file is computed using the SHA256 technique to get the file hash value, which is represented by  $file_{hash}$ , before the original data is encrypted. The final access control policy is composed of attributes, a trust value interval, and a time interval, and is created by the data owner. The final access control policy' and the generated public parameter  $PK$  are used as the input of the encryption algorithm of CP-ABE scheme. Attribute encryption is performed on  $k_2$  to obtain the encrypted ciphertext  $C_{enc}(k_2)$ , only when the user's attribute set meets the access control policy,  $k_2$  can be obtained.

---

Procedure encrypt:

---

- 1 .  $k_1, k_2 \leftarrow generate\ two\ random\ key$
- 2 . Compute  $K= k_1 \otimes k_2$
- 3 .  $file_{hash} \leftarrow SHA-256(file)$
- 4 .  $file_{enc} \leftarrow SM4_{enc}(file, K)$
- 5 .  $C_{enc}(k_2) \leftarrow CPABE_{enc}(PK, k_2, policy')$

Policy' =  $policy \cap [T_{k1}, T_{k2}] \cap [t_s, t_e]$

---

### 3.3.3 Data storage

The IPFS contains the original data file that has been symmetrically encrypted by the data owner. The IPFS returns a distinct storage address  $Addr$ , which is then symmetrically encrypted to produce  $Enc(Addr)$ . The client creates a transaction record using the Fabric SDK and stores it in a new blockchain block along with the original data hash  $file_{hash}$ , the key  $C_{enc}(k_2)$  encrypted by the attribute base, the encrypted IPFS file system storage address  $Enc(Addr)$ , and the description  $M$  taken from the donated data, then broadcast to other nodes on the chain to reach a consensus to complete the information on the chain, description information including project name, project number, donor, donation information.

---

Procedure storage:

---

- 1 .  $Addr \leftarrow store\ file_{enc}\ to\ IPFS$
- 2 .  $Enc(Addr) \leftarrow SM4_{enc}(Addr, k)$
- 3 .  $M \leftarrow Extract(file)$
- 4 .  $Contract \leftarrow fabricSDK(M, Enc(Addr), file_{hash}, C_{enc}(k_2))$

---

### 3.3.4 Data access

The data owner encrypts the data in accordance with the attributes, trust values, and access duration of the access request if a data accessor wishes to know specific details about donated data. Data accessor can access the blockchain records and retrieve the encrypted file storage address  $Enc(Addr)$ , original data hash value  $file_{hash}$ , and key encrypted by characteristics  $C_{enc}(k_2)$ . The contributed data ciphertext

can only be obtained by data accessor when their attributes align with the access policy and access window established by the data owner.

In this scheme, smart contract and CPABE are combined to realize access control with time dimension, and three functions are designed to realize access control with time dimension. The steps to access the data are as follows:

- The data accessor sends a request to the data owner that contains the public key  $Pub_{user}$ , the duration  $[t_s, t_e]$ , and the digital certificate  $Cert_{user}$ .
- After receiving the access request, the data owner first verifies the identity of the data accessor, and then sends  $k_1$  encrypted with the public key of the data accessor to the data accessor.
- The data accessor uses the attribute KeyGeneration algorithm  $KeyGeneration(MK, S)$  to generate the user's attribute private key  $SK_{user}$ ,  $S$  includes the user attribute set  $A_{user}$ , the trust value, and the timestamp of sending the request.

$$S = A_{user} \cup T_k \cup Time_{request} \quad (5)$$

- After obtaining the encrypted ciphertext data, the data accessor uses the public parameter  $PK$ , the attribute private key  $SK_{user}$ , and the ciphertext  $C_{enc}(k_2)$  as the input of decrypt algorithm  $Decrypt(PK, SK_{user}, C_{enc}(k_2))$ . If the data accessor attributes meet the access policy, the key  $k_2$  in plaintext is output. The key  $K = k_1 \otimes k_2$  can be calculated. The user can decrypt the encrypted file according to the obtained storage address  $Enc(Addr)$  to obtain  $Addr$ , then obtain the original ciphertext file  $file_{enc}$  from IPFS according to the address, and call SM4 decryption algorithm, the symmetric key  $K$  and the original ciphertext  $file_{enc}$  are used as input to decrypt the ciphertext  $file_{enc}$  for get the original data file. SHA256 algorithm is used to hash the decrypted file, and the hash value of the file is obtained, which is compared with the hash value saved in the block-chain. If the hash values are the same, the files are not tampered with and the data query succeeds. Otherwise, the file is tampered with or damaged, and the data query fails.
- In order to prevent a data accessor that does not comply with the access policy from still using the previous attribute private key to access the data, if the trust value of the data accessor is reduced and is not within the trust value range set by the data owner, when the attributes of a user are found to be changed, the attribute set will be regenerated, and the attribute key will be regenerated when applying to access data.

---

Procedure access:

---

- 1 . User send  $quest(Pub_{user}, [t_s, t_e], Cert_{user})$  to owner
  - 2 . Owner verify user's identity :  
If verify  $signature_{user} = true$   
Owner send  $enc(k_1)$  with  $Pub_{user}$  to User
  - 3 .  $SK_{user} \leftarrow KeyGeneration(MK, S)$
  - 4 .  $k_2 \leftarrow CPABE_{Dec}(PK, SK_{user}, C_{enc}(k_2))$   
compute  $K = k_1 \otimes k_2$   
 $Addr \leftarrow SM4_{Dec}(Enc(Addr), K)$   
 $file \leftarrow SM4_{Dec}(file_{enc}, K)$   
 $Hash_{file} \leftarrow SHA256(file)$   
If  $file_{hash} = Hash_{file}$  then  
query success  
else  
return false
  - 5 . If user's attr exchange then  
User send  $info_{user}$  to institution  
 $A_{user} \leftarrow Extract Info_{user}$
-

## 4 Scheme analysis

In this scheme, combined with a variety of Internet technologies such as blockchain, SM4, CPABE, IPFS, a charity donation model based on blockchain is constructed, the upstream and downstream information involved in the donation process is incorporated into the consortium blockchain. The transaction data are uploaded to the blockchain, which makes the transaction data open and transparent by using the characteristics of untamperable and traceable blockchain, and effectively solves the problems of easy data tampering and poor transparency in the process of traditional charitable donations.

### 4.1 Safety analysis

1) data confidentiality: Most of the data stored in the chain are encrypted ciphertext data, such as original file ciphertext, storage address, symmetric key of attribute encryption, file hash value, etc. Even if a malicious user gets the  $k_2$  stored on the blockchain,  $k_1$  is only available to data accessor and cannot calculate the file encryption key  $K$ . Moreover, even if the accessor has a key  $k_1$  without access to the data, he cannot get the key  $K_2$ . Therefore, data confidentiality is protected.

2) data integrity: In this scheme, the data integrity is reflected in two aspects. One is the untamperability of blockchain. The Merkle tree and block connection of blockchain make it impossible for malicious users to modify the data stored in blockchain at will, unless more than 51 % of the nodes in the whole network are tampered with, it is almost impossible in a large blockchain. Second, the original data integrity verification. The hash value is calculated before the encryption of the original data. Due to the uniqueness of the hash value, when the user finally gets the ciphertext and decrypts it, the comparison of the hash value can verify whether the original file is tampered with and ensure the integrity of the data.

3) privacy protection: The donation metadata is stored on the chain, and the original data is stored on the IPFS to ensure the scalability and security of data storage. NPO encrypt donation data according to the access strategy set by data owners. When data are accessed, the owner sets the access period for the accessor. Only the accessor who satisfies the access strategy can view the complete donation data within the set time range, which fully guarantees the privacy of the donation data.

### 4.2 Performance analysis

In order to accurately evaluate the actual performance of the scheme, the operating system of this paper is the virtual machine Ubuntu 18.04.5 installed on VMware Workstation Pro. The experimental hardware environment is AMD Ryzen 54600H CPU @ 3.00 GHz, and the memory is 16 GB. Using python language, based on openssl, gmssl, PBC library simulation test, test performance of scheme.

The scheme proposed in this paper is characterized by the combination of symmetric encryption and attribute encryption, encryption overhead is mainly reflected in the two encryption process. Therefore, the performance test in this paper is mainly to test the performance of the two encryption methods, and the final total encryption and decryption overhead is the time superposition of the two encryption methods. As shown in Figure 2, this paper tests AES, DES, SM4 three symmetric encryption algorithms, and selects different sizes of files for encryption. It can be seen that the encryption performance of the three algorithms is determined by the size of the original data. The larger the original data, the longer the encryption time. After considering the two factors of efficiency and security, SM4 is selected as the symmetric encryption method in this paper.

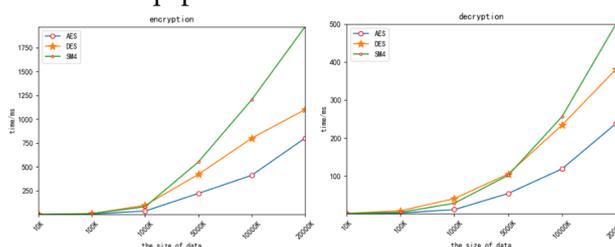


Figure 2 time cost of symmetric encryption algorithm

Figure 3 shows the encryption and decryption time under different number of attributes. The size of encrypted files is determined, which does not affect the encryption and decryption time. The number of attributes is taken as a variable, and the number of attributes used for encryption and decryption is increased from 5 to 50, with an increment of 5 for each time. It is observed that the encryption and decryption time increases with the increase of the number of attributes, but the time used is not more than the second level, indicating that the data can be secured and the data can be obtained in time.

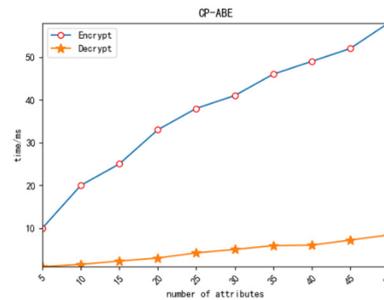


Figure 3 time cost of CPABE

## 5 Conclusion

This paper proposes a scheme for charitable donations, with the help of the characteristics of traceability and untamperability of blockchain, the whole process of donation is guaranteed to be open, transparent and traceable. IPFS is used to expand the storage capacity of blockchain, and the basic architecture of storing metadata on the chain and storing original data under the chain are designed. In view of the problem of data information leakage, combined with symmetric encryption and attribute encryption technology, an access control scheme based on block chain with time attribute is constructed to realize the fine-grained access control of data by data owners. The time attribute is introduced to make the access authorization without additional revocation cost. In the future, algorithm efficiency and consensus protocol will be our research direction. This work was supported in part by the National Nature Science Foundation of China under Grant 61762085, in part by the Autonomous Region Science and Technology Program of Xinjiang Grant 2020A02001-1.

## 6 References

- [1] Basil D Z , Herr P M . Dangerous Donations? The Effects of Cause-Related Marketing on Charity Attitude[J]. Journal of Nonprofit & Public Sector Marketing, 2003
- [2] MD Diarmuid, Rutherford A C . Promoting charity accountability: understanding disclosure of serious incidents[J]. Accounting Forum, 2018:S0155998217301977-
- [3] Inger Lyngdrup, Nørgård . The role of charity in public relief, 1708–1871: Copenhagen as case[J]. Scandinavian Journal of History, 2018:1-24
- [4] Davidson S, Filippi P D, Potts J . Disrupting Governance: The New Institutional Economics of Distributed Ledger Technology[J]. SSRN Electronic Journal
- [5] A. Farsya Kirana, F. Azzahro, P. Wuri Handayani and W. Resti Fitriani, "Trust and Distrust: The Antecedents of Intention to Donate in Digital Donation Platform," 2020 Fifth International Conference on Informatics and Computing (ICIC), 2020, pp. 1-6, doi: 10.1109/ICIC50835.2020.9288548
- [6] H.-y.YU, P.-w. DONG and T. MA, "Exploring Donors' Online Charity Adoption Base on Trust on Information Adoption Process," 2018 International Conference on Management Science and Engineering (ICMSE), 2018, pp. 110-118, doi: 10.1109/ICMSE.2018.8745097
- [7] P.Lanerolle, S.Rathnayaka, H.Rupasinghe, S.Madhushanka, U.Samarakoon and D. Kasthurirathne, "Donate.lk: A Smart Donation Handling System," 2018 National Information Technology Conference (NITC), 2018, pp. 1-6, doi: 10.1109/NITC.2018.8550078
- [8] D.Chhibber, A.Tripathi and S.Ray, "Do VIR: Virtualizing Food Donation Distribution through Mobile Application and Cloud-Based Supply Chain Management," 2021 IEEE International

- Conference on Consumer Electronics (ICCE), 2021, pp. 1-5, doi: 10.1109/ICCE50685.2021.9427641
- [9] Mohd Nor R , Rahman M M H , Rahman T , et al. Blockchain sadaqa mechanism for disaster aid crowd funding. 2017
- [10] Wu H , Zhu X . Developing a Reliable Service System of Charity Donation during the Covid-19 Outbreak[J]. IEEE Access, 2020, PP(99):1-1
- [11] Farooq M S , Khan M , Abid A . A framework to make charity collection transparent and auditable using blockchain technology[J]. Computers & Electrical Engineering, 83
- [12] Zhang Y , He D , Choo K . BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT[J]. Wireless Communications and Mobile Computing, 2018, 2018:1-9
- [13] Wu, A., Zhang, Y., Zheng, X. et al. Efficient and privacy-preserving traceable attribute-based encryption in blockchain. *Ann. Telecommun.* 74, 401–411 (2019). <https://doi.org/10.1007/s12243-018-00699-y>
- [14] Zhang X, Chen T, Feng Y, et al. A Data Sharing Scheme Based on Blockchain System and AttributeBased Encryption[C]//2021 The 3rd International Conference on Blockchain Technology. 2021: 195-202