A Study of Private Donation System Based on Blockchain for Transparency and Privacy

Junho Jeong
Dept. of Computer Science and Engineering
Kongju National University
Cheonan, Rep. of Korea
yanyenli@kongju.ac.kr

Donghyo Kim
Dept. of Computer Science and Engineering
Dongguk University
Seoul, Rep. of Korea
donghyo@dongguk.edu

Yangsun Lee
Dept. of Computer Engineering
Soekyeong University
Seoul, Rep. of Korea
yslee@skuniv.ac.kr

Jin-Woo Jung and Yunsik Son*
Dept. of Computer Science and Engineering
Dongguk University
Seoul, Rep. of Korea
{jwjung, sonbug}@dongguk.edu

***Abstract*—Nowadays, social inequality is an important social problem. Donations are one of the many ways to improve social inequality. Donation is largely divided into sponsorship by individuals such as corporations and public administration. In the individual sponsorship, it is common to donate to a donation organization and to support the aid recipients by donation organization. Many people are reluctant to support to this donation because of the lack of transparency. In addition, many donation organizations lack transparent and formal administration due to lack of working capital. Therefore, this paper proposes a method to enhance personal transparency by enhancing the transparency of donation organizations and protecting the privacy of sponsors using blockchain that is a Hyperledger fabric. And We implement a blockchain network for the proposed system.**

***Keywords*—blockchain; private donation; transparency; privacy preserving;hyperledger fabric;**

I. Introduction

Nowadays, social inequality is an important social problem [1]. Donations are one of the many ways to improve social inequality. Donation is largely divided into sponsorship by individuals such as corporations and public administration. In the individual sponsorship, it is common to donate to a donation organization and to support the aid recipients by donation organization.

Many people tend to avoid sponsorship because of the lack of transparency in the sponsoring organization. In addition, many sponsoring organizations lack transparent and formal administration due to lack of working capital. For this reason, many private sponsors are only sponsored by large donation bodies. As a result, small organizations are not well managed for their long-term sponsors, and have problems with their lack of information power, human resources, and opacity [2].

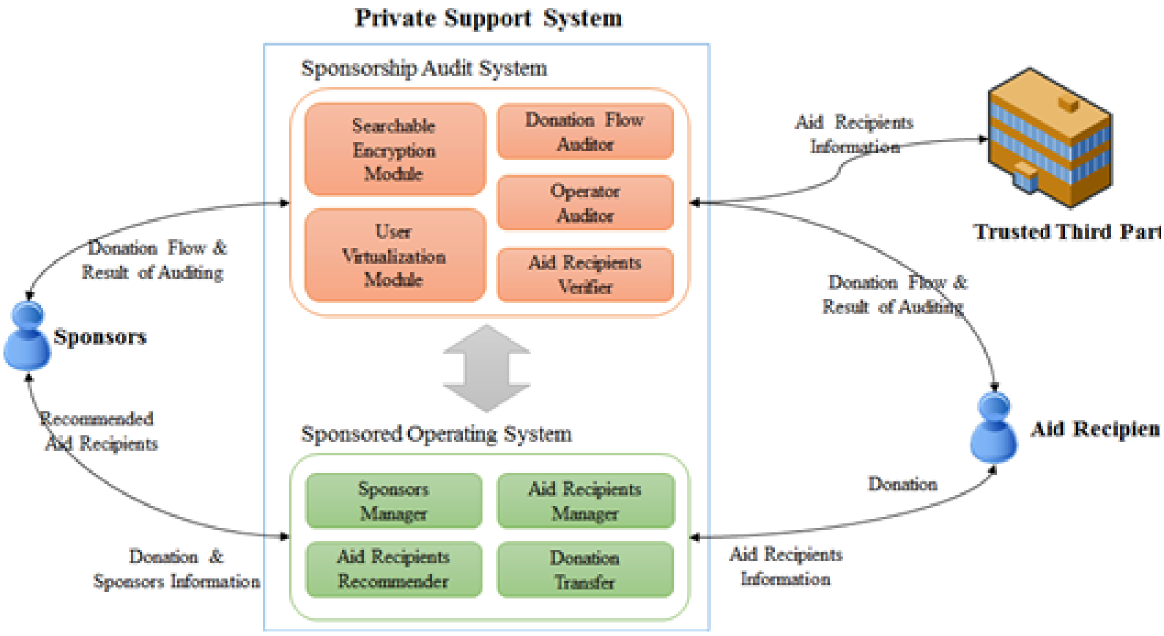

Private Support System
Sponsorship Audit System
Searchable Encryption Module
Donation Flow Auditor
Operator Auditor
User Virtualization Module
Aid Recipients Verifier
Sponsored Operating System
Sponsors Manager
Aid Recipients Manager
Aid Recipients Recommender
Donation Transfer
Donation Flow & Result of Auditing
Sponsors
Recommended Aid Recipients
Donation & Sponsors Information
Aid Recipients Information
Trusted Third Part
Donation Flow & Result of Auditing
Aid Recipien
Donation
Aid Recipients Information

Fig. 1. Private Support System Model [4]

*Corresponding Author: Yunsik Son (sonbug@dongguk.edu)

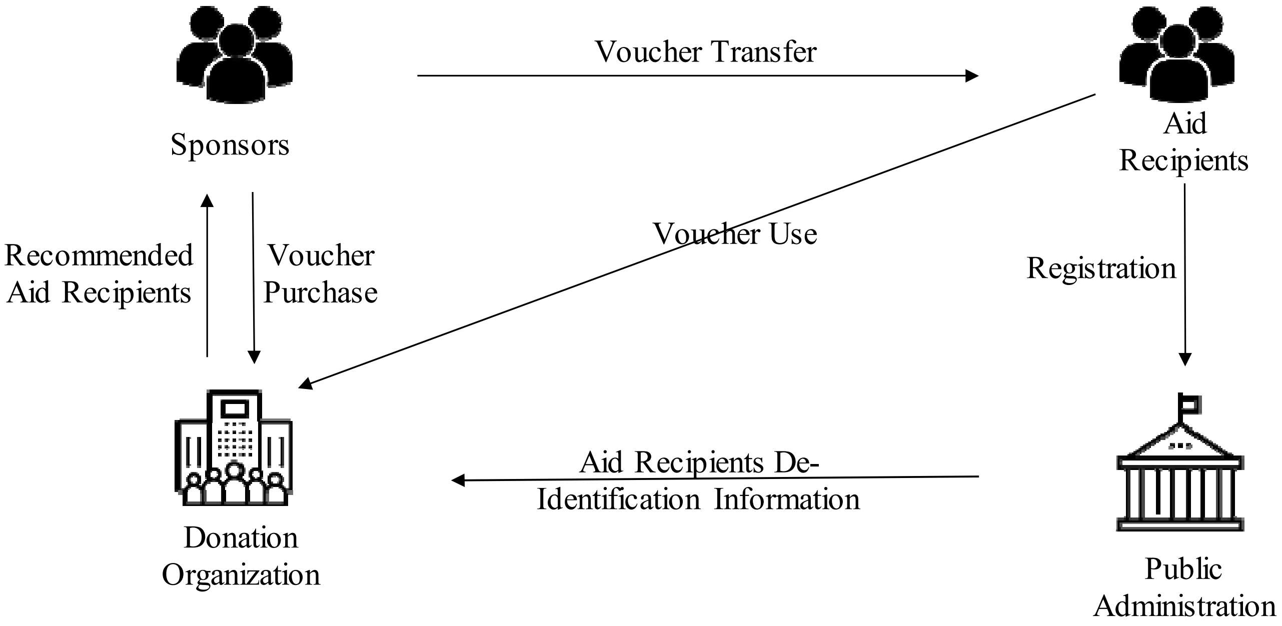


Fig. 2. Proposed System Workflow

Therefore, even small organizations need support for a system that can effectively manage aid recipients and sponsors and manage grants. The purpose of this study is to enhance the transparency of sponsoring organizations by using blockchain [3] and to activate individual donation by protecting the privacy of sponsor and aid recipients.

This paper is organized as follows. Section 2 analyzes the core functions required of small-size donation organizations and presents a support model using blockchain considering them in Section 3. Section 4 presents the results of building a blockchain network for this purpose. Finally, we conclude in Section 5.

II. Core Functions Required by Donation Organiztion

It is one of the main purposes of the donation organization to connect and support the aid recipients and the sponsors. Therefore, it is important for donation organizations to protect the privacy of their sponsors and their aid recipients.

Sponsors tend to want to know from their donation organization the details of how their donations are used. Satisfying this requirement is the most important function for managing Sponsors in donation organizations. Therefore, there should be regular notification of this information. In addition, it is necessary to inform sponsors regularly that information is needed. Ultimately, funding should be managed in such a way that it can be transparent and not opaque [4].

Therefore, core functions required for donation organizations are as follows. First, a function that regularly manages registered sponsors and recommends and connects the aid recipients in the desired condition. Second, a system in which most of the donations can be delivered to the sponsor. Third, an audit system that can audit all actions of such a system operator. Fig. 1 shows the structure of the personal sponsorship model to achieve this need [5].

In previous studies, such systems were considered for privacy when sponsors and sponsors were recommended [6]. The proposed study further proposed a system using a blockchain that can support the transparency of the model.

III. Private Donation System Based on Blockchain

In the past, the donation system using blockchain used a cryptocurrency to directly provide personal support. Such a system is at risk of being abused by malicious users for purposes such as laundering now, rather than sponsoring the correct aid recipients. The proposed system attempts to prevent this by providing the ability to audit operations and authenticate aid recipients in public administration. Fig. 2 shows the workflow of the proposed system.

The process of using the proposed system consists of three processes. The first process is system user registration and login. Every user is a regular user at the time of membership, and the email, password, and membership status are stored in the database. Sponsor is authorized as a sponsor through '*sponsor registration'* function, and when the sponsor is registered, personal information is stored in the blockchain as mappable encrypted data. The aid recipient can be authorized after verification of identity through '*aid recipient registration*' function that is a request to a public administration, and personal information is stored in the blockchain as encrypted data in the same form as the sponsor.

The second is the aid recipient verification process. When you register aid recipient information in the first step, the transaction is recorded in the aid recipient & public administration channel. The public administration will verify the information about the recorded aid recipients and update the information status. Thus, the information the aid recipient should store is the personal identification ID, address, reason for sponsorship, informed consent, and the range of information available to the sponsor.

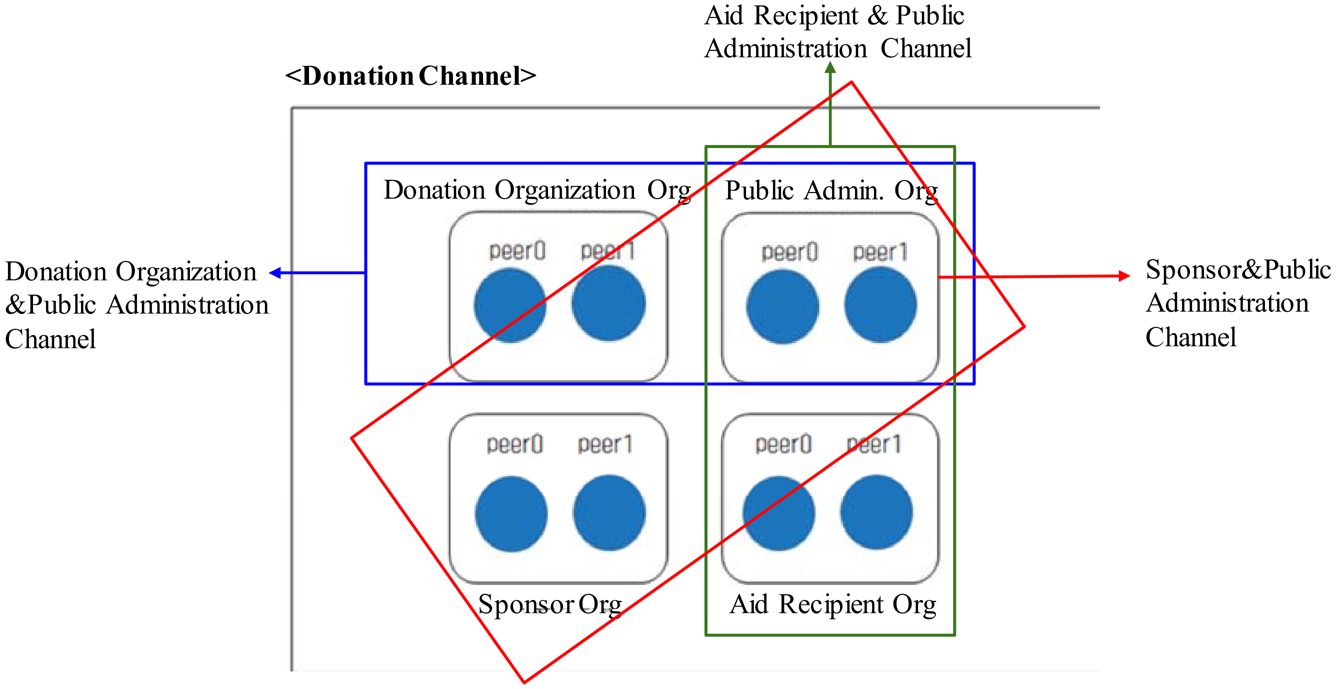

Aid Recipient & Public Administration Channel
<Donation Channel>
Donation Organization Org
Public Admin. Org
peer0
peer1
peer0
peer1
Donation Organization &Public Administration Channel
Sponsor&Public Administration Channel
peer0
peer1
peer0
peer1
Sponsor Org
Aid Recipient Org

Fig. 3. Blockchain Network for the Proposed System

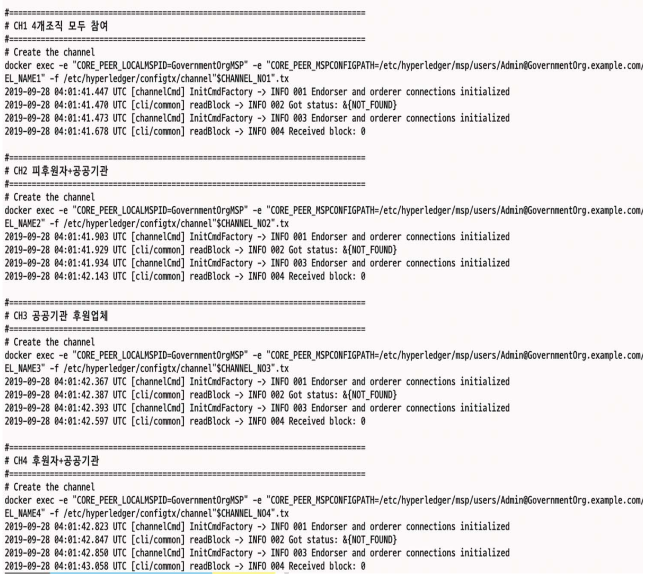
Third is the candidate recommendation process. The donation organization asks the public administration for a list of aid recipients. The public administration stores the relevant aid recipient information stored in the aid recipient & public administration channel in the public administration & donation organization channel. The donation organization then provides a list of persons using de-identification data to the sponsor who requested the aid recipient recommendation. The recommendation history is stored in all channels of the blockchain network. The history includes sponsor information, aid recipient attributes requested, donation organization information, and so on. There are five major chain codes for this flow, as shown in Table 1.

Table 1. Main Chaincode for proposed system

Chaincode	Permission	Channel
Aid Recipient Info. State Update (state: yes/no)	Public Admin.	Public Admin, Aid Recipient
Aid Recipient Info. Update	Aid Recipient	Public Admin, Aid Recipient
Sponsor Info. Update	Sponsor	Public Admin, Sponsor
Personal Info. Transfer	Public Admin.	Public Admin, Donation Org.
Recommend History	Sponsor	All

IV. EXPERMENATL ANALYSIS

The proposed system model implemented based on Hyperledger Fabric a blockchain network infrastructure framework and Docker that is an s/w virtualization platform in this paper. The environments for implementing Hyperledger Fabric blockchain network and certificate authority servers are Ubuntu v16.04 LTS, Hyperledger Fabric v1.2, Golang v11.4, Docker v18.06.1-ce, Docker-Compose v1.8.0, Nodejs v8. 11 and so on.



```
#==========================================================================
# CH1 4개조직 모두 참여
#==========================================================================
# Create the channel
docker exec -e "CORE_PEER_LOCALMSPID=GovernmentOrgMSP" -e "CORE_PEER_MSPCONFIGPATH=/etc/hyperledger/msp/users/Admin@GovernmentOrg.example.com/
EL_NAME1" -f /etc/hyperledger/configtx/channel"$CHANNEL_NO1".tx
2019-09-28 04:01:41.447 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2019-09-28 04:01:41.470 UTC [cli/common] readBlock -> INFO 002 Got status: &{NOT_FOUND}
2019-09-28 04:01:41.473 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and orderer connections initialized
2019-09-28 04:01:41.678 UTC [cli/common] readBlock -> INFO 004 Received block: 0

#==========================================================================
# CH2 피후원자+공공기관
#==========================================================================
# Create the channel
docker exec -e "CORE_PEER_LOCALMSPID=GovernmentOrgMSP" -e "CORE_PEER_MSPCONFIGPATH=/etc/hyperledger/msp/users/Admin@GovernmentOrg.example.com/
EL_NAME2" -f /etc/hyperledger/configtx/channel"$CHANNEL_NO2".tx
2019-09-28 04:01:41.903 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2019-09-28 04:01:41.929 UTC [cli/common] readBlock -> INFO 002 Got status: &{NOT_FOUND}
2019-09-28 04:01:41.934 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and orderer connections initialized
2019-09-28 04:01:42.143 UTC [cli/common] readBlock -> INFO 004 Received block: 0

#==========================================================================
# CH3 공공기관 후원업체
#==========================================================================
# Create the channel
docker exec -e "CORE_PEER_LOCALMSPID=GovernmentOrgMSP" -e "CORE_PEER_MSPCONFIGPATH=/etc/hyperledger/msp/users/Admin@GovernmentOrg.example.com/
EL_NAME3" -f /etc/hyperledger/configtx/channel"$CHANNEL_NO3".tx
2019-09-28 04:01:42.367 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2019-09-28 04:01:42.387 UTC [cli/common] readBlock -> INFO 002 Got status: &{NOT_FOUND}
2019-09-28 04:01:42.393 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and orderer connections initialized
2019-09-28 04:01:42.597 UTC [cli/common] readBlock -> INFO 004 Received block: 0

#==========================================================================
# CH4 후원자+공공기관
#==========================================================================
# Create the channel
docker exec -e "CORE_PEER_LOCALMSPID=GovernmentOrgMSP" -e "CORE_PEER_MSPCONFIGPATH=/etc/hyperledger/msp/users/Admin@GovernmentOrg.example.com/
EL_NAME4" -f /etc/hyperledger/configtx/channel"$CHANNEL_NO4".tx
2019-09-28 04:01:42.823 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2019-09-28 04:01:42.847 UTC [cli/common] readBlock -> INFO 002 Got status: &{NOT_FOUND}
2019-09-28 04:01:42.850 UTC [channelCmd] InitCmdFactory -> INFO 003 Endorser and orderer connections initialized
2019-09-28 04:01:43.058 UTC [cli/common] readBlock -> INFO 004 Received block: 0
```

Fig. 4. Channel Creation for Four Organizations

The system created various network entities and created all the certificates, keys, and genesis blocks for the entities to complete the creation of the channels. As shown in Fig. 4, the channels in which the four organizations participate, and the channels in which the groups participate, are created and initialized.

V. Conclusion and Futher Research

The proposed study verified the information on the candidates and built the basis for auditing the flow of funds and operators according to the support of the support fund of the sponsoring operation system using the blockchain. This will lead to a more transparent and privacy-supported system.

However, DApp using blockchain network was not implemented and performance analysis on the proposed chaincode was not done. Through the implementation of DApp that can be effectively used in the future, we will increase the utility of the proposed research and analyze its performance.

Acknowledgment

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(No. 2017R1D1A3B03029906), and this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT) (No. 2018R1A5A7023490) and this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT) (No. 2019R1F1A1045343) and this research was supported by the KIAT(Korea Institute for Advancement of Technology) grant funded by the Korea Government(MSS : Ministry of SMEs and Startups). (No.S2755615, HRD program for Enterprise linkages R&D)

References

[1] Hwang, C.□S.: Activation Policies of Giving Culture to Solve Cultural Disparities. The Journal of Cultural Policy, vol. 23, pp. 27-43. (2010)

[2] Lee, M.-Y., Yun, M.-H.: A qualitative study of fundraisers'ethical dilemma and conflict in the NGOs. Journal of Korean Social Welfare Administration, vol. 17, no. 2, pp. 247-275. (2015)

[3] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Weed Cocc, S., Yellick, J.: Hyperledger fabric: a distributed operating System for permissioned blockchains, Proceedings of the Thirteenth EuroSys Conference. (2018).

[4] Kang, C.-H., Park, T.-K, Oh, J.-Y.: A Study on Regular Donors' Giving Duration : Application of Survival Analysis Method. Journal of Korean Social Welfare Administration, vol. 18, no. 3, pp. 153-175. (2016)

[5] Jeong, J., Seo, A., Lee, J., Kim, Y.: A Study of Private Support System Model Design for Guarantee the Privacy of Sponsors and Aid Recipients, The 18th International Symposium on Advanced Intelligent Systems, pp. 544-550. (2017)

[6] Lee. J., Seo, A., Kim, Y., Jeong, J.: Blockchain-Based One-Off Address System to GuaranteeTransparencyandPrivacyforaSustainable Donation Environment, Sustainability, vol. 2018, no. 10, Article no. 4422, pp.1-14. (2018)