Journal of Knowledge Information Technology and Systems(JKITS), Vol. 15, No. 4, pp. 539-548, August 2020
https://doi.org/10.34163/jkits.2020.15.4.009

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Reliable Donation Service Using Ethereum Blockchain

Yonghu Kim, Ungki Baek, Yechan Jin, Ingyu Ham, Iksu Kim*

School of Computer Science and Engineering, Soongsil University

ABSTRACT

The existing donation system did not allow donors to know the donations used by donor organizations. As a solution, the method of storing donation details of donation organizations on the blockchain was introduced. This has the advantage of being unable to hide or modify the details, but there is no way to verify them if the donor organization intentionally manipulates them and stores them in the block chain. In this paper, we propose a reliable donation service using Ethereum Blockchain. Unlike the existing donation system, it helps to make reliable donations by storing immutable transaction details in the blockchain. Sellers selling goods, donors making donations, and social organizations using donations join one service to store all transactions in the blockchain. The transaction details associated with the donation are disclosed to all users and transaction ID is provided so that everyone can verify the transaction. The proposed service can prevent social organizations from the use of donations for their own interests because they have to purchase the goods using donations through the proposed service and provide them to the recipient. As a result, the proposed service can provide more transparency to donors and we can expect more donations from donors. We use the Ethereum platform and node.js server to implement the system.

KEYWORDS: Blockchain, Ethereum, Smart contract, DApp, Web service

ARTICLE INFO: Received 2 July 2020, Revised 26 July 2020, Accepted 10 August 2020.

*Corresponding author is with the School of Computer Science and Engineering, Soongsil University, 369, Sangdo-ro, Dongjak-gu, Seoul, 06978, KOREA.

E-mail address: iksuplorer@ssu.ac.kr

1. 서 론

기부금 횡령은 예전부터 계속 일어나던 문제이다. 국내 기부재단에서도 127억을 횡령하는 사건이 있었고 공신력 있는 국제기구인 유니세프 또한 사무총장이 2000만원 가량의 기부금을 개인적 용도로 사용한 사건도 있었다[1-2]. 또한, 2020년 6월 현재 위안부 기부금 횡령에 관한 의혹이 제기되는 등 기부문화에 불신을 낳고 있다[3]. <표 1>과 <표 2>는 2017년 한국보건사회연구원에서 발표한 기부를 하지 않는 이유에 대한 조사[4] 결과를 정리한 표이다. <표 1>을 보면 “기부단체를 신뢰할 수 없음”에 답한 비율이 28.1%이다.

표1. 기부를 하지 않는 이유
Table 1. The reason why people do not donate

구분		사례수	경제적 여유가 없어서	방법과 절차를 몰라서	시설 및 기관을 믿을 수 없어서	필요성을 느끼지 못해서	계
전체		916	51.7%	9.0%	28.1%	11.2%	100.0%
성별	남자	474	53.2%	8.9%	24.7%	13.2%	100.0%
	여자	442	50.1%	9.0%	31.8%	9.0%	100.0%

표2. 기부금 사용 내역 인지 조사
Table2. Survey on the recognition of donation usage history

구분		사례수	그렇다	아니다	기부 경험 없음	계
전체		2,000	29.3%	43.7%	27.0%	100.0%
성별	남자	1,017	25.8%	45.5%	28.8%	100.0%
	여자	983	32.9%	42.0%	25.2%	100.0%

또한, <표 2>에 명시된 기부 경험자의 기부금 사용처 인지율을 보면 사용처를 모르는 사람이 43.7%이며 기부를 경험한 사람 중 사용 내역 인지율을 계산하면 기부금의 사용 내역을 알지 못하는 기부자가 60%가 넘는 비율을 차지한다. 이처럼 자신이 기부한 금액이 어디에 사용되었는지에 대하여 알기 어렵고 기부 단체를 신뢰할 수 없다는 등의 이유에 의해 매년 기부 참여율 현황이 감소하고 있다.

현존하는 기부 서비스는 기부자가 기부금 사용 내역을 알 수 없다는 문제를 가지고 있다. 이러한 문제를 해결하기 위해 블록체인 기반의 기부 시스템들이 소개되어 왔다. 블록체인 기반의 기부 시스템들은 분산원장을 사용하여 모든 거래 내역을 저장하기 때문에 위조나 변조가 불가능하다는 장점이 있다. 하지만 여전히 기부금이 적절히 수급자에게 전달되고 있는지에 대해서는 보증할 수 없는 문제를 가지고 있다.

본 논문에서는 기부를 하는 기부자, 캠페인을 등록하여 관리하고 기부금을 사용하는 사회단체, 물품을 파는 판매자를 하나의 서비스에 가입시켜 모든 거래 내역을 블록체인에 저장하고 생성된 모든 거래 내역을 누구든 확인할 수 있는 투명한 기부 서비스를 제안한다. 제안된 서비스에서 사회단체는 기부금을 사용하여 물품을 구입하고 수급자에게 제공하기 때문에 부정한 목적으로 기부금을 사용하는 것을 예방할 수 있다. 따라서 기부자들에게는 기부 결과에 대한 투명성을 높여줄 수 있고, 결과적으로 사회단체는 더 많은 기부를 기대할 수 있다.

본 논문의 2장에서는 이더리움과 현존하는 기부 시스템을 소개하고, 3장에서는 신뢰성이 있고 투명성을 개선한 기부 시스템을 설계한다. 그리고 4장에서 제안된 기부 시스템을 구현하고, 마지막으로 5장에서 결론을 내린다.

2. 관련 연구

2.1 이더리움

이더리움(Ethereum)은 블록체인 기술을 여러 분야에 접목할 수 있도록 업그레이드한 기술이다[5]. 흔히 2세대 블록체인이라고 일컫는 이더리움은 이더(Ether)로 불리는 고유의 암호화폐를 사용한다. 이더의 공급은 어느 정부나 어떤 회사도 제어할

수 없도록 탈중앙화되어 있으며 이더를 결제 수단으로 사용하거나 가치 저장 수단 혹은 담보로 이용하고 있다. 이더리움 위에서 개발되는 탈중앙화 어플리케이션은 이더리움에 한 번 업로드되면 smart contract[6]를 통해 항상 프로그래밍 된 대로 동작하므로 완전히 신뢰할 수 있다.

2.2 Cherry

Cherry는 블록체인 기반 기부 서비스이다[7]. 기부금이 모금되고 전달되는 모든 정보를 실시간으로 블록체인에 기록해 투명하게 공개한다는 투명성과 소액결제로 기부를 쇼핑처럼 가볍게 할 수 있다는 장점이 있다. 하지만 기부 물품을 캠페인 주최 단체에서 구매하고 전달할 시에, 그 구매는 Cherry 외에서 이루어지므로 기부금이 어떻게 사용되는지에 대한 투명한 정보 공개를 기대할 수 없다는 단점이 있다. 또한, 기부자가 후원한 캠페인들에 대해서만 거래기록을 열람할 수 있다는 단점이 있다. 이러한 이유로 후원을 꺼리는 잠재적 기부자는 그 사회단체가 올바르게 기부금을 사용했는지 판단할 근거가 없어 후원 결정을 보류할 수 있다. 그리고 거래기록 열람의 정보 제공 측면에서 Cherry는 어떤 분야에 소비할 것인지 대략적으로 표시하므로, 구체적으로 어떤 물품에 어떤 금액을 소비하였는지는 알지 못한다는 단점이 있다.

2.3 블록체인 기반 기부 시스템

[8]에서는 블로거가 타인으로부터 기부를 받기 위해 자신의 블로그에 블록체인 기반의 비트코인 기부 시스템을 간단히 구축하는 방법을 소개하였다. 이 방법은 비트코인을 입금받을 전자 지갑을 생성하고 QR코드를 발급받는다. 기부자는 QR코드를 스캔하여 기부를 할 수 있다. [8]에서 제공하는 기부 시스템은 기부금에 대한 사용 내역이 중요하지 않은 경우에 편리하게 사용될 수 있다.

[9]에서는 기존 기부 시스템이 갖는 기부금의 투명성 문제를 지적하며 블록체인 기반의 기부 시스템을 제안하였다. 이 시스템은 데이터의 무결성을 검증하는데 규제 없이 참여할 수 있는 public 블록체인을 사용하였으며, 기부자와 수급자가 규제 없이 참여할 수 있게 하였다. 기부자들이 암호화폐로 기부를 하면 수급자는 그 암호화폐를 환전하여 사용하는 방식이며, 그 과정에 대한 기록은 블록체인 내에 남는다. 따라서 기부금에 대한 사용 흐름이 투명하게 확인될 수 있다. 하지만 수급자가 기부 서비스에 참여할 만큼의 경제적인 IT 환경을 갖추지 못하였거나, 노령의 수급자는 블록체인 기반의 기부 서비스에 직접 참여가 어려운 것이 현실이다. 또한, 서비스 운영자는 기부 서비스에 참여한 모든 수급자가 기부금을 받을 만한 자격이 있는지에 대한 판단을 어떻게 하느냐에 대한 기준의 모호함도 있다.

이러한 문제점들로 인해 기부금 수급자를 서비스에 직접 참여시키는 것보다 기부 물품 판매업체를 서비스에 참여시켜 거래 내역을 공개하고, 사회단체가 기부금을 더욱 투명하게 사용하도록 유도하는 것이 기부 서비스의 신뢰도를 높일 수 있다. 이를 위하여 사회단체는 캠페인에 모인 기부금을 환전하여 다른 목적으로 사용하지 못하도록 하고, 오로지 기부 서비스 내에서의 물품 거래를 통해 사회단체가 수급자에게 직접 전달하는 방식이 도입되어야 한다.

3. 시스템 설계

본 논문은 앞서 기술한 기부 서비스들의 문제점을 보완하기 위해 물품을 판매하는 판매자를 추가하고, 기부금의 사용도 기부 서비스 내에서 이루어

지게 함으로써 기부와 기부금의 사용 내역이 기부자는 물론, 아직 기부에 참여하지 않은 잠재적인 후원자들에게 모두 투명하게 제공된다. 이는 캠페인에 아직 참여하지 않은 잠재적인 후원자들이 사회단체를 신뢰하여 후원을 결정하는 데에 큰 도움을 줄 수 있을 것이다.

3.1 기부 서비스 이용자 관계 정의

본 논문에서 제안하는 서비스는 현존하는 기부 서비스에서 더 나아가 투명성과 접근성이 향상된 기부 서비스 모델이다. 기부금 사용에 대한 투명성을 제공하기 위해 블록체인을 사용하였고, 사회단체가 수급자에게 제공할 물품을 판매하는 판매자가 서비스에 참여한다. 서비스 이용자들의 관계는 <그림 1>과 같다.

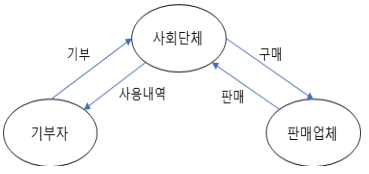

그림 1. 서비스 이용자 관계도
Figure 1. Service user relationship diagram

기부 서비스에서는 블록체인에 재화의 흐름을 기록하기 위해 포인트를 사용한다. 기부자는 현금으로 포인트를 충전하여 사회단체에 기부하고 사회단체는 기부받은 포인트로 판매업체를 통해 각종 물품을 구매한다. 그리고 판매업체는 수익 포인트를 현금으로 환전한다. 따라서 블록체인에 사회단체가 기부받은 금액이 저장될 뿐만 아니라 사회단체가 활동에 필요한 물품을 구매하는 기록도 저장된다. 따라서 기부자는 사회단체가 기부받은 포인트를 어디에 어떻게 사용하는지 투명하게 볼 수 있다.

3.2 전체 시스템 구조도

본 논문에서 제안하는 서비스는 <그림 2>와 같이 웹서비스의 api 서버가 DApp의 클라이언트가 되는 구조이다. 서버는 이용자와 통신하며 이용자에게 웹 서비스를 제공하고, 동시에 DApp의 클라이언트가 되어 서비스 내의 재화의 이동을 블록체인에 기록한다. 즉, 배포한 스마트 컨트랙트의 클라이언트가 웹서비스의 서버가 되는 것이다.

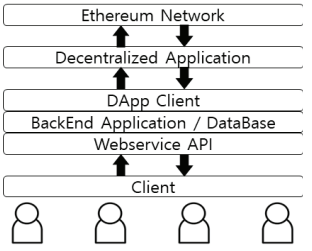

그림 2. 시스템 구조
Figure 2. System architecture

DApp(Decentralized Application)의 모델에는 사용자가 스마트 컨트랙트와 직접 상호작용하는 완전 탈중앙화된 모델과 서버가 스마트 컨트랙트와 통신하는 모델이 있다. 제안하는 서비스에서는 후자 모델을 적용하는데, 완전 탈중앙화된 모델로 서비스를 구현하면 실제 사용자가 어느 정도 이더리움에 대한 지식이 있어야 하고 MetaMask와 같은 플러그인을 설치해야 하기 때문이다. 강력한 투명성을 제공하더라도 결국 블록체인에 대한 지식이 없는 사용자가 이용하기에는 접근성이 부족하면 해당 기부 서비스는 오히려 기부 의욕을 떨어뜨릴 수 있다. 따라서 본 논문이 제안하는 서비스는 서버가 web3.js[10]와 Hdwallet[11]을 사용하여 사용자 대신 스마트 컨트랙트를 사용한다.

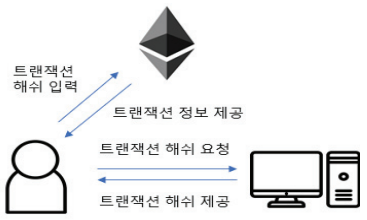

그림 3. 트랜잭션 조회
Figure 3. Transaction inquiry

<그림 3>과 같이 기부, 충전, 환전, 물품 구매 등 재화가 이동하는 트랜잭션이 일어날 때 해당 트랜잭션의 해쉬를 저장하고 사용자가 요구 시 트랜잭션에 대한 확인이 가능하다.

3.3 기부 서비스를 위한 웹 페이지 구성

웹페이지의 흐름은 <그림 4>와 같이 메인페이지를 통해 로그인, 회원가입, 마이페이지, 상점, 캠페인을 볼 수 있다. 마이페이지는 각 권한마다 볼 수 있는 내용들이 달라지는데, 기부자는 자신이 기부한 캠페인들의 정보를 볼 수 있고 사회단체의 경우에는 등록한 캠페인의 정보를 볼 수 있다. 또한, 판매자일 경우에는 자신이 등록한 상품정보 및 주문내역을 볼 수 있다. 캠페인의 상세 내역을 보여주는 페이지에서 기부자는 기부를 진행할 수 있으며, 사회단체는 상점 페이지에서 물품을 구매할 수 있다.

4. 시스템 구현

4.1 스마트 컨트랙트

신뢰할 수 있는 기부 내역을 보여주기 위해 캠페인 정보, 기부자의 잔액은 중앙화된 데이터베이스가 아닌 블록체인에 저장되어야 한다. 본 논문에서 제안하는 서비스는 PoS(Proof of Stake) 합의 알고리즘을 사용하는 이더리움에서 스마트 컨트랙트를 Solidity[12]로 작성하여 구현하고 Truffle[13] 프레임워크를 이용하여 Ganache에서 테스트한 후 테스트 넷에 배포하였다. 블록체인 네트워크 중 이더리움을 채택한 이유는 퍼블릭 블록체인이기 때문에 투명성이 높고 스마트 컨트랙트를 이용하여 Dapp을 운용하기 좋은 플랫폼이기 때문이다. <그림 5>는 제안 서비스에서 사용된 스마트 컨트랙트

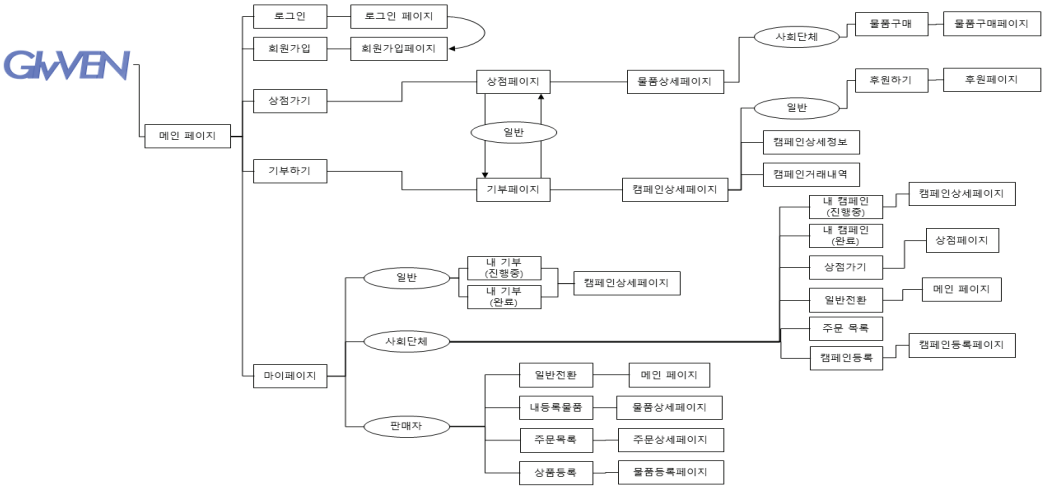

그림 4. 웹페이지 구조
Figure 4. Webpage structure

의 변수 선언부를 나타내며, 나머지 스마트 컨트랙트 코드는 [14]에서 Givven.sol 파일로 확인이 가능하다. 이 변수들을 통해 사용자 계정과 캠페인 정보를 저장할 수 있으며, 캠페인 정보에는 캠페인 단체명과 모금액이 포함된다. 또한, 유저와 기부금액을 매핑하고 상품과 수량을 매핑하는 mapping 자료형을 포함하고 있다.

```
contract Givven{

    address admin;
    mapping(string => uint) accounts;
    mapping(string => Campaign) campaigns;

    struct Campaign{
        string socialOrg;
        uint currentDonate;

        mapping(string => uint) donatevalue;
        mapping(string => uint) products;
    }
```

그림 5. 스마트 컨트랙트의 변수 선언과 정의
Figure 5. Declaration and definition of variables of smart contract

4.1.1 계정 등록


```
{ blockHash: '0x73457e253208a9561a194aa445a9b9f1f6a66b5f6b377597e03069bdf
8c5f3fe',
  blockNumber: 19129325,
  chainId: null,
  condition: null,
  creates: null,
  from: '0x021405Ba0D65147E494238436730fe6671e2da74',
  gas: 24697,
  gasPrice: '9000000000',
  hash: '0xb2f881db207438f8fce8fdbd2c61d23bea0a243089b8eaddd7873069a8983f
34',
  input: '0x18b8275a0000000000000000000000000000000000000000000000000000000
0000000002000000000000000000000000000000000000000000000000000000000000000
06756e6963656600000000000000000000000000000000000000000000000000000000',
  nonce: 50,
  publicKey: '0xdb4a97627dd6dcbd614ea3e35af5a21c0f0c709a073ed5081d08419d0
baac87ee4ae63f2777e04c290da66a5487b6cb3761594827fb4428246133851263899b2',
  r: '0x3961490e5365e7209eac6fd98c4fd25a40b0bfdec9e1758716559c78957bb259'
,
  raw: '0xf8c9328502187 11a0082607994fa7ea4a5632a4daa769eb9c34fecb4b6d431d
89480b86418b8275a0000000000000000000000000000000000000000000000000000000
0000002000000000000000000000000000000000000000000000000000000000000000067
56e6963656600000000000000000000000000000000000000000000000000000001ba0396149
0e5365e7209eac6fd98c4fd25a40b0bfdec9e1758716559c78957bb259a029aa9c6e8bef2
5140fa1af97cbf0da7104e29cded36aab4e32d3c460460aa9cf',
  s: '0x29aa9c6e8bef25140fa1af97cbf0da7104e29cded36aab4e32d3c460460aa9cf'
,
  standardV: '0x0',
  to: '0xFa7eA4A5632A4dAA769Eb9c34Fecb4B6D431d894',
  transactionIndex: 0,
  v: '0x1b',
  value: '0' }
{ name: 'addUser',
  params: [ { name: '_userEmail', value: 'unicef', type: 'string' } ] }
```


그림 6. 사용자 추가 트랜잭션
Figure 6. Transaction for adding user

사용자가 회원가입을 할 때 사용자의 고유한 id와 balance를 해쉬 mapping하여 등록한다. <그림 6>은 해당 트랜잭션에 대한 정보이다.

4.1.2 캠페인 등록

표 3. Campaign 구조체
Table 3. Campaign struct

자료형	변수명	설명
string	socialOrg	캠페인 소유 단체
uint	currentDonate	현재 모금액
Hashmap	donateValue	기부자와 기부금액 매핑

사회단체가 캠페인을 등록하면 블록체인에 <표 3>과 같은 구조체의 형태로 캠페인에 대한 정보를 저장한다. <그림 7>은 해당 트랜잭션을 abi로 디코딩하여 input 데이터를 추출한 모습이다.


```
{ name: 'createCampaign',
  params:
   [ { name: '_campaignId',
       value: 'tx test campaign',
       type: 'string' },
     { name: '_socialOrg', value: 'charity', type: 'string' } ] }
```


그림 7. 캠페인 생성 트랜잭션을 abi로 디코딩한 결과
Figure 7. Campaign creation transaction decoded in abi

4.1.3 기부

기부자가 사회단체에 기부를 진행하면 기부자, 기부 캠페인, 기부금액을 입력 받아 스마트 컨트랙트에서 트랜잭션을 요청한다.


```
{ name: 'donate',
  params:
   [ { name: '_userEmail', value: 'test_normal', type: 'string' },
     { name: '_campaignId', value: '테스트 캠페인1', type: 'string' },
     { name: '_value', value: '1000', type: 'uint256' } ] }
```


그림 8. 기부 트랜잭션을 abi로 디코딩한 결과
Figure 8. Donation transaction decoded in abi

<그림 8>은 기부를 성공적으로 마치고 블록체인에 저장된 트랜잭션에서 스마트 컨트랙트 함수를 실행할 때 주는 인자 값을 나타내는 부분이다. 이렇게 복호화된 데이터를 통해 사용자는 트랜잭션의 내용을 이해할 수 있다.

4.1.4. 거래

거래가 발생했을 경우 기부금을 사용하는 캠페인, 판매자, 거래 금액, 상품정보가 블록체인에 저장된다.

```
{ name: 'purchase',
  params:
   [ { name: '_campaignId', value: 'campaign1', type: 'string' },
     { name: '_seller', value: 'seller_test', type: 'string' },
     { name: '_product', value: '마스크', type: 'string' },
     { name: '_productNum', value: '10', type: 'uint256' },
     { name: '_value', value: '10000', type: 'uint256' } ] }
```

그림 9. 거래 트랜잭션을 abi로 디코딩한 결과
Figure 9. Trading transaction decoded in abi

<그림 9>는 구매가 성공적으로 이루어진 후 블록체인에 저장된 트랜잭션의 일부이다.

4.2 웹서비스

기부 서비스 이용자들은 <그림 10>과 같은 기능들을 사용할 수 있다.

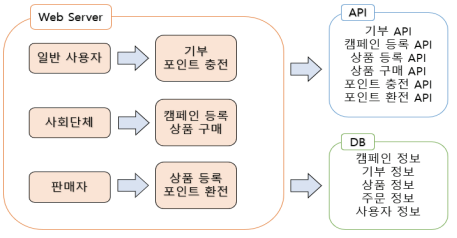

그림 10. 서비스 구조
Figure 10. Service structure

일반 사용자 권한을 갖는 기부자가 기부를 진행할 때 기부 API가 호출되며 DB에 있는 기부 정보에 새로운 기부 내역이 추가된다. <그림 11>은 기부를 실행하는 웹페이지이다.

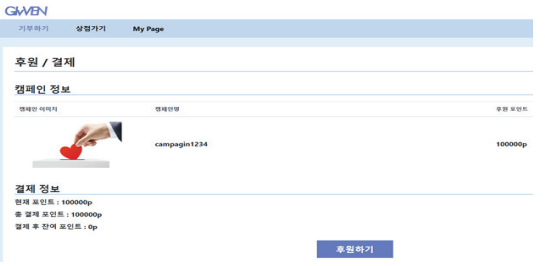

그림 11. 기부 웹페이지
Figure 11. Webpage for donation

사회단체는 <그림 12>와 같은 캠페인 등록 웹페이지에 캠페인을 추가할 수 있으며 등록이 진행되면 API 호출을 통해 DB에 새로운 캠페인 정보가 추가된다.

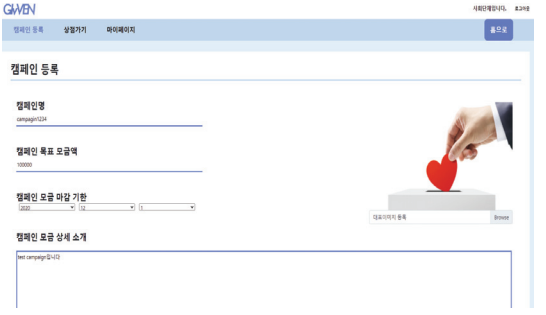

그림 12. 캠페인 등록 웹페이지
Figure 12. Webpage for campaign registration

상품판매자는 <그림 13>과 같은 웹페이지를 통해 판매 물품을 추가할 수 있으며, 사회단체는 모금이 완료된 캠페인이 있을 시 <그림 14>와 같은 웹페이지를 통해 물품을 구매할 수 있다. 상품 구매에 따라 상품 구매 API가 호출되면 DB의 상품 정보 내역에서 재고 수량이 감소하고 주문 내역에는 새로운 정보가 추가된다.

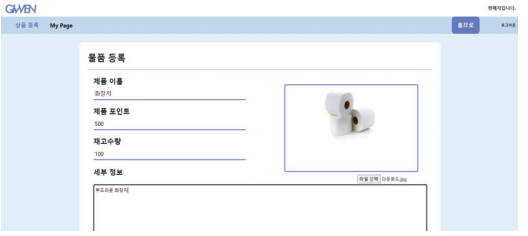

그림 13. 물품 등록 웹페이지
Figure 13. Webpage for goods registration

그림 14. 물품 구매 웹페이지
Figure 14. Webpage for purchasing goods

4.3 평 가

제안 서비스를 운영하여 etherscan[15]으로 조회한 결과 평균적으로 계정 등록은 약 2~3만 gas, 캠페인 등록은 약 4만 gas, 기부와 거래는 약 7만 gas가 소모되었다. 이는 2020년 6월 기준으로 약 500 ~ 2000원 상당의 수수료에 해당하며, 코드 최적화를 통해 수수료 비용을 개선할 수 있다.

<표 4>는 앞서 기술한 cherry와 제안 서비스를 비교한 결과이다. cherry와 달리 제안 서비스에서는 물품 판매자가 기부 서비스에 참여하여 사회단체와의 거래 내역이 블록체인에 곧바로 기록된다. 또한, 기부자뿐만 아니라 기부를 아직 결정하지 못한 잠재적인 기부자들도 캠페인의 지출 내역을 확인할 수 있어 사회단체의 신뢰도를 높일 수 있다는 장점을 가지고 있다.

표4. cherry와 제안 서비스의 비교
Table4. Comparison of Cherry and the proposed service

	Cherry	제안 서비스
참여자	기부자, 사회단체	기부자, 사회단체, 판매자
투명성	기부내역	기부내역, 물품거래
공개성	기부자가 기부한 캠페인만 지출 내역 확인 가능	기부자 제한 없이 캠페인의 지출 내역 확인 가능

5. 결 론

현존하는 기부 서비스는 기부자들에게 기부 내역의 무결성과 투명성을 보장할 수 없는 문제들을 가지고 있다. 그 결과 현재 여러 기관에서 기부금 횡령이 발생하고 있으며 기부금 사용에 대한 불투명성으로 기부에 대한 인식이 좋지 않다.

본 논문에서는 기존 기부 시스템이 갖는 가장 큰 문제인 불투명성을 보완하기 위해서 이더리움 기반의 기부 서비스를 구현하였다. 구현된 서비스는 이더리움에서 동작하는 스마트 컨트랙트와 웹 서버의 연결을 통해 판매업체가 기부 서비스에 참여하게 하고, 사회단체가 받은 기부금의 사용이 판매업체 간의 거래를 통해 투명하게 이루어진다.

제안된 기부 서비스에서 재화의 이동이 모두 블록체인 원장 안에 기록되기 때문에 네트워크에 참여한 모든 기부자와 기관은 물론, 기부에 참여하지 않은 일반인들도 거래 내역을 자유롭게 열람할 수 있다. 이 서비스를 통해 기부자들에게는 기부에 대한 투명성을 주어 기부에 대한 인식 개선과 성취를 느끼게 할 수 있고, 이를 토대로 사회단체는 기부자들로부터 더 많은 기부를 기대할 수 있다. 앞으로 오픈 소스로 제공되는 제안 서비스가 더 개선되고 널리 배포되어 수급자는 물론, 기부자, 사회단체, 판매업체 모두에게 이로운 서비스가 되기를 기대한다.

References

[1] An embezzlement by UNICEF Secretary General, https://www.donga.com/news/article/all/20130817/57067390/1, Jun. 2020.

[2] Six years in prison for embezzlement of donations worth 10 billion won, https://www.donga.com/news/Society/article/all/20190526/95697942/1, Jun. 2020.

[3] An embezzling donations to help the Japanese military sexual slavery victims, https://www.donga.com/news/Society/article/all/20200624/101665421/1, Jun. 2020.

[4] Ko Kyung-hwan, Domestic Donation Status, https://www.kihasa.re.kr/web/activity/research/view.do?menuId=38&tid=72&bid=93&division=002&ano=2730, Jun. 2020.

[5] Introduction of Ethereum, https://ethereum.org/en/, Jun. 2020.

[6] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, Hawk: *The blockchain model of cryptography and privacy-preserving smart contracts*, 2016 IEEE Symposium on Scurity and Privacy, pp. 839-858, 2016.

[7] cherry, https://cherry.charity/public/mainPage, Jun. 2020.

[8] Kinsta, How to Add a Bitcoin Donate Button to Your WordPress Site, https://kinsta.com/blog/bitcoin-donate-button/, Jun. 2020.

[9] K. H. An, and H. J. Seo, *Donate system development using Blockchain technology*, Journal of the Korea Institute of Information and Communication Engineering, vol. 22, pp. 812-817, 2018.

[10] Web3.js Javascript Api Document, https://web3js.readthedocs.io/en/v1.2.9, Jun. 2020.

[11] hdwallet provider github Repository, https://github.com/trufflesuite/truffle/tree/develop/packages/hdwallet-provider, Jun. 2020.

[12] Solidity Language Document, https://solidity.readthedocs.io/en/v0.6.10, Jun. 2020.

[13] Truffle and Ganache Api Document, https://www.trufflesuite.com/docs, Jun. 2020.

[14] Givven, https://github.com/who-is-hu/Givven, Jun. 2020.

[15] Etherscan, https://kovan.etherscan.io, Jun 2020.

이더리움 블록체인을 이용한 신뢰성 있는 기부 서비스

김용후[1], 백웅기[1], 진예찬[1], 함인규[1], 김익수[2]

[1] *숭실대학교 컴퓨터학부 학부생*

[2] *숭실대학교 컴퓨터학부 교수*

요 약

기존의 기부 시스템은 기부자가 기부금의 사용 내역에 대하여 알 수 없는 경우가 많았다. 해결법으로 기부 단체의 기부금 사용 내역을 블록체인에 저장하는 방법이 소개되었다. 이런 방법은 기부금 사용 내역을 숨기거나 수정할 수 없다는 장점을 가지고 있지만, 기부 단체가 의도적으로 기부금 사용 내역을 조작하여 블록체인에 저장했을 때 기부자가 기부 내역을 검증할 방법은 여전히 제공하지 않는다. 본 논문에서는 이더리움 블록체인을 이용한 기부 웹 서비스를 제안한다. 기존의 기부 시스템과 다르게 불변성을 가진 거래내용을 블록체인에 저장하여 믿고 기부를 할 수 있게 도와준다. 기부 물품을 판매하는 판매자와 기부자 그리고 기부금을 사용하는 사회단체를 하나의 서비스에 가입시켜 모든 거래의 내용을 블록체인에 저장한

다. 사회단체는 제안된 서비스를 통해 기부금을 사용하여 물품을 구입하고 수급자에게 제공해야 하기 때문에 자기 자신의 이익을 목적으로 기부금 사용하는 것을 예방할 수 있다. 결과적으로 기부자들에게는 기부 시스템의 투명성을 제공할 수 있고, 기부자들로부터 더 많은 기부를 기대할 수 있다. 시스템의 구현을 위해 Ethereum과 node.js 서버를 사용한다.

Yonghu Kim is currently a student in the School of Computer Science and Engineering at Soongsil University. His research interests include web service and blockchain.
E-mail address: dydgndlaek97@gmail.com

Ungki Baek is currently a student in the School of Computer Science and Engineering at Soongsil University. His research interests include web service and blockchain.
E-mail address: yachae85@gmail.com

Yechan Jin is currently a student in the School of Computer Science and Engineering at Soongsil University. His research interests include web service and blockchain.
E-mail address: roqhrryghl@gmail.com

Ingyu Ham is currently a student in the School of Computer Science and Engineering at Soongsil University. His research interests include web service and blockchain.
E-mail address: hfire1207@gmail.com

Iksu Kim received the B.S., M.S., and Ph.D. in Computer Science from Soongsil University, South Korea, in 2000, 2002, and 2008, respectively. He worked at SKYCOM as a manager until January 2009. He is currently an associate professor in the School of Computer Science and Engineering at Soongsil University since September 2009. His research interests include system security, network security, and blockchain.
E-mail address: iksuplorer@ssu.ac.kr