

User-independent blockchain donation system

Sang-Dong Sul*, Su-Jeong Lee**

*Professor, Dept. of Information & Communication Engineering, Dongyang Mirae University, Seoul, Korea

**CEO, E4NET Co., Ltd., Seoul, Korea

[Abstract]

This paper introduces the Cherry system, a user-independent blockchain donation system. This is a procedure that is delivered to the beneficiary's bank account through a virtual account when a donor makes a donation, so there is no difference from the existing donation delivery method from the user's point of view. However, within the blockchain, Cherry Points, a virtual currency based on the user ID, are issued and delivered to the beneficiary, while all transactions and the beneficiary's usage history are managed on the blockchain. By adopting this method, there was an improvement in blockchain performance, with transaction processing exceeding 1,000 TPS in typical transaction condition and service completion within 21.3 seconds. By applying the automatic influence control algorithm to this system, the influence according to stake, which is an individual donation, is greatly reduced to 0.3 after 2 months, thereby concentrating influence could be controlled automatically. In addition, it was designed to enable micro tracking by adding a tracking function by timestamp to the donation ledger for each individual ID, which greatly improved the transparency in the use of donations. From a service perspective, existing blockchain donation systems were handled as limited donation delivery methods. Since it is a direct service in a user-independent method, convenience has been greatly improved by delivering donations in various forms.

▶ **Key words:** Blockchain, POS, Smart contract, donation, hash, asymmetric encryption

[요 약]

본 논문은 사용자 독립방식의 블록체인 기부시스템인 Cherry system을 소개하고 있다. 이는 기부자가 기부를 하게 되면 가상계좌를 통해 수혜자의 통장으로 전달되는 절차라서 사용자 입장에서는 기존의 기부금 전달 방식과 차이가 없다. 다만 블록체인 내부에서는 사용자 ID에 따른 가상화폐인 체리 포인트를 매칭 방식으로 발행하여 수혜자에게 전달하면서, 모든 거래와 사용 내용을 블록체인에서 관리하는 방식이다. 이런 방법을 채택함으로써 Typical transaction 상황에서 1,000TPS 이상을 나타내고, 21.3초 이내에 서비스 완료되는 블록체인 성능의 개선이 있었다. 본 시스템에서는 권한 자동 제어 알고리즘을 적용함으로써 stake에 따른 권한은 2개월이 경과하면 0.3으로 크게 감소하여 권한 집중화를 자동으로 제어할 수 있었다. 또한 개인 ID 별로 기부금 장부에 타임 스탬프 추적기능을 추가함으로써 마이크로 트래킹이 가능하도록 설계되었고, 이를 통해 기부금 사용의 투명성을 개선하였다. 서비스 관점에서 기존의 블록체인 기부시스템들은 제한된 기부금 전달 방식으로 처리되었던 것을 사용자 독립방식을 적용함으로써 다양한 형태로 기부금을 전달하게 하여 사용자 편의성을 크게 개선하였다.

▶ **주제어:** 블록체인, 지분증명, 스마트 계약, 기부, 해시값, 비대칭 암호화

• First Author: Sang-Dong Sul, Corresponding Author: Sang-Dong Sul

*Sang-Dong Sul (sdsul@dongyang.ac.kr), Dept. of Information & Communication Engineering, Dongyang Mirae University

**Su-Jeong Lee (sjlee@e4net.net), E4NET Co., Ltd.

• Received: 2023. 09. 22, Revised: 2023. 10. 16, Accepted: 2023. 11. 06.

I. Introduction

우리나라의 경제 규모 대비 기부금은 정체되어 있다. 2020년 국세청 통계에 따르면 지난 10년간 기부금 비율이 GDP 대비 0.8% 수준이다.

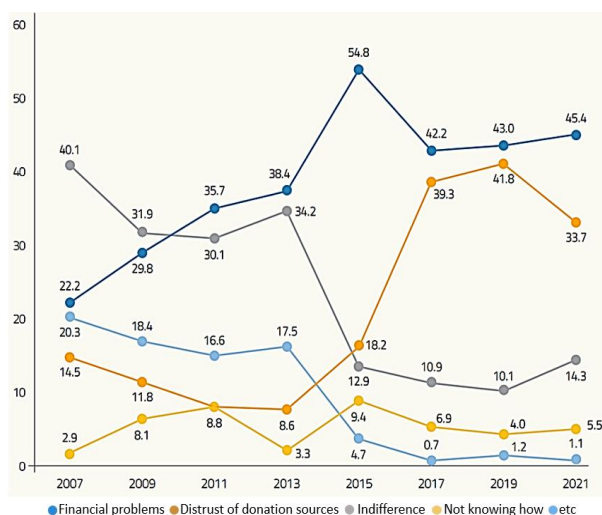


Fig. 1. Reasons not to donate (*source:Giving Korea)

이는 미국의 2.1%에 비교할 때 매우 저조한 수준이다. 이렇게 기부문화가 저조한 원인에는 “경제적인 여력 없음 > 기부처 불신 > 기부에 관심 없음 > 기부 방법, 단체 모름” 등으로 나타나고 있다.

특히 기부처에 대한 불신이 두 번째로 커다란 원인인 것을 Fig.1. 을 통해 알 수 있다. 이를 해결하기 위해서 기부 단체 모금 및 집행 정보에 대한 투명성, 구체성 등을 보증할 수 있는 시스템이 필요하다[1].

이러한 것을 개선하기 위해 오랫동안 정부와 단체에서 재정 상황을 정기적으로 보고하고, 제3기관을 통한 검증, 인증마크 부여, 기부자와 지속적인 오픈 커뮤니케이션 및 사례 공유 등의 여러 가지 시도를 하지만, 아직은 기부자들의 불신을 해소하기에는 부족한 점이 있다. 어떤 일이든지 사람이 개입하지 않고 시스템적으로 일이 처리되면 절차에 따라 진행되는 특성 때문에 불신의 여지가 없다. 이를 위해 가장 좋은 플랫폼이 블록체인 시스템이다. 블록체인은 P2P 형태로 탈중앙화하여 운영되는 것으로 투명성과 보안성이 우수하여, 기부금이 투명하게 운영되면서 안전하게 운영되기에 적합한 시스템이라고 할 수 있다.




II. Preliminaries

1. Local Donation Platform

국내에는 대기업이 주도하여 기부 플랫폼을 구축하고 있다. Table 1.에서 보듯이 대표적인 기부 플랫폼에는 네이버의 ‘해피빈’, 카카오의 ‘같이가치’ 그리고 한화의 ‘불꽃’ 등을 꼽을 수 있다. 이들은 인터넷상의 온라인 플랫폼으로 개인으로부터 다양한 형태로 기부금을 모을 수 있는 수단을 제공하는 강점이 있다. 그 한 예가 해피빈의 경우 가상화폐로 ‘콩’을 지급하는 방식을 도입하여, 클릭이나 온라인 활동 보상으로 화폐 대신 ‘콩’으로 지급하기도 한 대[2]. 다만 기부자들의 불만이 기부 금액의 투명성이나 자신이 기부한 금액이 어떻게 사용되는지 파악하는 데 미흡하다는 데 있다. 기부금의 투명성 확보를 위해 블록체인 기술을 활용하면 기부자나 기부단체, 기부 수혜자에 대한 기부금 흐름 및 내역 등을 투명하게 관리할 수 있다.

본 논문에서는 사용자 독립방식으로 기부 플랫폼을 구현한 Cherry system의 기술을 소개하려고 한다.

Table 1. Local Donation Platform

Platform	Description
 Happybean	<ul style="list-style-type: none"> Web Services, launched in July 2005 Accumulated donations: KRW 102.5 billion (December 2011) Naver Social Contribution: Platform operation, payment fee support, and donation 'bean' payment
 Together	<ul style="list-style-type: none"> Started December 2007, Web Services Annual donation: KRW 46 billion ('December 2011) Kakao Social Contribution: Platform operation, payment fee support, and donation per comment participation
 Bulggot	<ul style="list-style-type: none"> Web/App Service Launched September 2019 Annual contributions: undisclosed Hanwha Social Contribution: Platform operation, payment fee support, and donation per participation in posting photos

2. Blockchain Technologies

블록체인은 거래 장부를 hash 값으로 만들어서 블록 속에 기록하여 체인으로 서로 연결하여 보관하는 기술이다. 거래 장부가 은행같이 권위 있는 기관에서 중앙집중방식으로 관리되던 것을 네트워크상에 분산하여 P2P 방식으로 모두에게 공개하고 시스템적으로 합의에 의해 관리하는 탈중앙화된 거래기록 방법이다. 블록체인을 사용하면 아래와 같은 장점이 있다[6].

▶ 신뢰성 : 분산 네트워크에서 거래 장부를 관리하기 때문에 데이터 수정이나 위조가 어려워 거래의 신뢰성이 상승한다.

▶ 투명성 : 비록 거래 장부의 헤더는 암호화되었지만, 거래 내역을 네트워크에 참여한 모두가 공유하고 있어서 거래 과정이 투명하다.

▶ 보안성: 비대칭 암호화 기술을 사용하고 있고, 거래 내용을 hash 값으로 압축하여 블록에 체인으로 연결되어 관리하기 때문에 기록된 내용을 수정하려면 이전에 기록된 모든 hash 값도 수정해야 한다. 따라서 해킹해서 데이터를 위조하는 것이 무의미한 구조로, 보안성이 탁월하다.

▶ 탈중앙화 : 기존 은행의 거래 방식과 달리 블록체인 참가자가 직접 거래하면서 관리하기 때문에, 중앙에 의존하면서 지급해야 하는 거래 수수료를 절감하면서, 네트워크 참가자가 모두가 검증하는 구조로 안정성 높은 탈중앙화 시스템이다.

이와 같은 장점이 있어서 블록체인을 사용하여 기부시스템에 적용하면 기존의 기부 처리 방식을 파격적으로 개선할 수 있다.

3. Blockchain consensus

블록체인에서 블록의 생성과 거래를 할 때 유효성을 검증하는 것을 합의라고 한다. 이런 합의 과정에 대한으로 방식들로는 POW(Proof Of Work), POS(Proof Of Stake), DPOS (Delegated Proof of Stake), POA(Proof of Authority), Tendermint 그리고 PBFT (Practical Byzantine Fault Tolerance) 등 여러 가지가 있다. 그중에서 현재 기부 블록체인에 사용되고 있는 합의 방식인 작업증명(POW, proof of work)과 지분증명(POS, proof of stake)을 간단히 소개하면 Table 2.와 같다[12].

Table 2. Comparison for POS and POW

ITEMS	POS	POW
Validation	chosen validate	miners compete
Energe Consumption	less energy	significant energy
Security	cost-prohibitive	51% attack but Highly secure
Decentralization	possibility of centralization	higher level decentralization
Scalability	more efficient	restrictive
processing speed	more fast	relatively slow
Initial cost	cheap hardware	expensive system
Accessibility	easy	some difficulty

POW는 네트워크 참여자들에게 어떤 작업을 수행하도록 요구하여 블록을 경쟁적으로 검증하여 추가하는 과정을 수행한다. 이를 위해서 트랜잭션 검증, 작업증명 과정, 난이도 조절, 보상 등의 주요 과정이 필요하며, 네트워크의 분산성과 보안성을 높이지만, 많은 컴퓨터 자원을 이용하기 때문에 환경을 해치는 문제가 있다.

반면에 POS 방식은 보증금 스테이킹, 블록 검증, 보상 등의 간단한 과정으로 진행한다. 블록체인의 POS 방식은 일반적으로 다음과 같은 장점을 갖고 있다[3][8].

▶ 에너지 소모: POS는 POW와 비교하여 적은 에너지를 소비한다. POW는 컴퓨터의 계산력을 사용하여 블록 생성을 위해 수많은 채굴자가 경쟁적으로 작업을 수행하는 반면, POS는 Stake(보증금)를 가장 많이 지급한 사람이 블록 생성 작업을 수행한다. 이로 인해 POS는 에너지 측면에서 효율적인 구조라고 볼 수 있다.

▶ 확장성 증대: POS는 보증금이 많은 사용자가 새로운 블록을 생성하는 역할을 한다. 이는 많은 사용자가 참여할 수 있어 블록체인 네트워크의 확장성을 증대시킬 수 있다.

▶ 빠른 거래 속도: 블록 생성 권한이 특정 노드에 부여되기 때문에 여러 채굴자가 난이도에 맞게 채굴 경쟁을 하는 POW에 비해 빠르게 블록 생성할 수 있다[10].

블록체인에서 POS는 에너지 효율, 확장성, 속도 측면에서 강점이 있지만, 권한의 집중화 문제는 보완해야 할 점이다. POS 시스템은 많은 보증금을 보유한 사용자에게 더 많은 블록 생성 및 검증의 영향력을 부여하게 되어 있다. 이에 따라 보유량이 많은 사람에게 권한이 집중화되어 더 많은 결정 권한을 가지게 되는 부분 중앙 집중화가 발생할 수 있다. 그리고 블록 생성에 대한 대가로 더 많은 보상을 받을 가능성이 있어서, 권력의 불균형을 유발하고, 새로운 참여자들에게 블록 생성 권한을 가질 기회를 박탈할 수 있다[6].

본 논문에서는 POS 방식의 문제인 권한 집중을 근본적으로 막고 Stake에 따른 권한을 자동 분산시키는 권한 자동 분산 알고리즘 기술을 소개하고 있다[4].

4. Block structure

블록의 주요 구조는 헤더와 바디로 되어 있다. 바디에는 거래 정보가 기록되어 있고, 모든 거래 정보는 hash 값으로 압축되어 이진트리 구조로 연결되어 있고, Merkle hash 값으로 수렴되어 블록헤더에 저장된다. 또한 블록체인의 모든 거래 장부는 투명하게 관리한다. 그것은 블록헤더의 내용을 압축한 hash 값을 체인으로 연결하면 거래 장부의 관리가 안전하고 투명하게 관리된다. 모든 생성된

블록의 내용은 작업증명 시 채굴자들이 경쟁적으로 블록 검증을 한다.

Table 3. Block Header

Header	Byte	Description
Version	4	Software version
Previous Hash	32	Previous Block Hash
Merkle Hash	32	Hash for transaction information
Time	4	Block creation time
Bit	4	Difficulty of mining
Nonce	4	Arbitrary value for calculating hash values

Table 3.과 같이 구성된 블록헤더의 내용만을 이용해서 block hash를 생성한다. 그리고 새로 생성하는 block hash 내용에는 이전에 생성한 previous hash를 고려하기 때문에, 블록 데이터들은 체인처럼 상호 연관성을 유지한다[7].

채굴의 속도를 조절하기 위해서 채굴 난이도를 지정하면 채굴자는 nonce를 변화시키면서 hash를 생성한다. 채굴 난이도에 의해 발생한 기준이 되는 hash보다 작은 값이 나올 때까지 반복해서 채굴작업을 하여 빠르게 생성한 채굴자의 블록을 체인에 등록하고 보상하는 것이 전통적인 블록체인의 기술이다[9].

5. Blockchain encryption

블록체인에서 주로 사용되는 암호화 방식을 요약한 내용은 Fig.3.에 나타내듯이 데이터의 hash와 비대칭 암호화 방식이다.

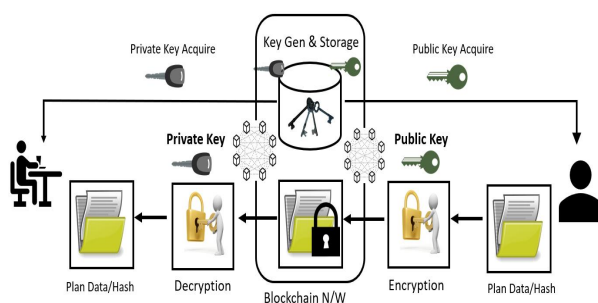


Fig. 3. Asymmetric Cryptography in Blockchain N/W

5.1 Hash

hash 함수는 블록체인에서 가장 핵심이 되는 장부 기술이다. hash 함수는 여러 가지가 있지만 보통 SHA-256으로 32바이트의 고정길이의 hash 값을 갖는 함수를 사용한다. hash 함수를 사용하면 유리한 장점은 3가지가 있다.

▶ 단방향성 : 어떤 데이터를 입력하든지 같은 입력값에는 동일한 결과의 hash를 나타내지만, 역으로 hash 값을 이용해서 원래의 입력값을 추출하기 힘든 단방향 구조이다.

▶ 충돌 저항성 : 데이터의 출력값이 동일한 값이 발생하는 것을 충돌이라고 하는데, 그 가능성은 2^{256} 으로 거의 불가능한 것으로 간주하여 충돌 저항성이 높다.

▶ 고정된 길이 : 입력 데이터가 몇 바이트인지 무관하게 hash 값은 SHA-256의 경우 256bit의 고정된 출력값을 갖는다.

이상의 3가지 특성 때문에 블록체인의 모든 장부는 hash 값으로 관리되어 저장된다. 그 hash 값을 사용해서 트랜잭션을 할 때마다 네트워크 참여자들은 무결성을 확인할 수 있다. 그리고 사용자가 특정 블록을 찾을 때 블록의 hash 값을 통해 찾기 편리하다. 추가해서 블록 내에 다양한 거래의 내용들을 이진 트리 형태인 머클트리 구조를 가진다. 머클트리의 최종값인 Merkle hash 값을 이용해서 블록 내의 거래 내용을 압축해서 보호 및 관리하게 된다[6].

5.2 Blockchain Asymmetric Encryption

일반적으로 블록체인은 비대칭 암호화 알고리즘을 이용하여 데이터를 보호한다. Fig. 3.에서 보듯이 블록체인 가입자가 최초에 등록하면 개인에게 설치된 블록체인 지갑에 개인키(private key)를 발생시키고, 블록체인 네트워크에서는 키 저장소에서 개인키에 쌍이 되는 공개키(public key)를 발행하여 관리한다. 데이터를 암호화할 때는 블록체인 네트워크에서 개인 ID에 부여된 공개키를 이용하고, 복호화할 때는 공개키에 쌍이 되는 개인키를 이용하여 사용자는 해독한다. 암호화할 때와 복호화할 때 키가 다른 것이어서 암호화된 데이터의 안정성이 보장되는 것이다.

블록체인에서 비대칭 암호화를 사용하는 중요한 이유는 2가지이다.

▶ 데이터 보호 : 블록체인 사용자가 자신의 장부 내용을 블록체인에 전송하거나 블록에 저장할 때 공개키로 암호화하여 보관하고, 이 장부를 열어 보려고 할 때는 공개키에 쌍이 되는 개인키로 복호화하여 데이터를 보게 된다. 이렇게 암호화할 때 키값과 복호화할 때 키값이 다르므로 데이터를 보호하게 된다.

▶ 전자서명 : 사용자 간 거래가 생성되는 것을 트랜잭션이라고 하는데, 이러한 거래를 할 때 개인키를 통해 소유자의 신원을 검증함으로써 거래의 무결성을 유지하게 된다. 일반적으로 송금, 수신, 계약 체결 등의 행위가 있을 때는 반드시 개인키로 거래 서명을 해야만 거래자의 신원

확인을 하게 되는 것이다. 이를 통해서 거래의 무결성이 보장되는 것이고 안전한 트랜잭션을 시작할 수 있게 된다.

“암호체계는 알고리즘이 아니라 키의 보안에 의해서 데이터가 보호되어야 한다.”라는 케르크호프스(Kerckhoffs's principle)의 주장과 같이, 해커가 어떻게 암호화했는지 암호 방법을 알고 있을지라도, 암호화된 내용은 보호되도록 설계되어야 한다. 블록체인 기술이 어느 정도 케르크호프스 주장에 근접한 기술로 장부를 블록체인에 넣을 때마다 hash 값을 만드는 것은 공개된 기술이지만 누구도 원본 데이터를 복원하는 것이 힘들다. 그리고 데이터를 블록체인에 올려서 저장할 때 비대칭 암호화하는 것도 어느 정도 공개되어 있다. 그렇지만 공개키와 개인키가 있어야 암호화된 데이터를 풀어볼 수 있기 때문에 일반 해커가 해독하기에 어려움이 있어서 데이터의 안정성을 보장할 수 있다.

6. Challenge for Current systems

블록체인을 이용한 기부시스템에 관한 연구가 POW 방식과 POS 방식 기반으로 제안되고 있다[11]-[15].

POW 방식을 적용한 기부시스템은 블록헤더에 bit와 nonce 대신에 wallet address와 money를 사용하여 블록헤더를 생성함으로 mining 기간을 단축하는 시스템이다. 이는 POW 방식으로 블록체인을 생성하는데 10분 이상 소요되는 시간을 축소하는 기법이지만, 전체 노드들의 합의 과정을 거쳐야 블록 생성되는 한계가 있어서 확장성에 문제가 있다[12][14].

POS 방식을 적용한 기부시스템의 경우 기부 관리 단계를 이용하지 않고 블록체인의 합의 과정을 통해 직접 수혜자에게 암호화폐(ETH)를 발행하여 투명성을 확보하는 방안이다[11]. 이는 수혜자가 적극적으로 사연을 게시판에 기록하여야 하고, 이더리움에 가입하여 지갑(wallet)을 가지고 암호화폐를 사용해야 하는 불편이 있다. 다른 연구로는 기부자가 기부 코인(DC)을 구매하고, 기부단체에 0원으로 기부 코인 매도하는 형태 수동식 기부 환전 시스템의 발전형이라고 할 수 있다[13]. 이는 블록체인을 통한 거래를 하기 때문에 투명성은 확보된다. 다만 이런 기부시스템을 이용할 경우 기부자가 지속적으로 관여해야 하는 복잡한 기부 시스템이다[15].

현재 제안되고 있는 블록체인 기부 시스템이 POW 방식과 POS 방식을 이용함으로 몇 가지 문제를 내포하고 있다.

- ▶ 확장되었을 때 TPS 속도의 문제

- ▶ 기부자가 가상화폐 및 wallet 사용 시 불편한 점
- ▶ POS 방식을 사용하는 경우 권한의 집중화
- ▶ 제한된 방식의 기부금 전달

본 논문에서는 기존의 블록체인 기부시스템의 문제들을 극복하기 위해 사용자 서비스와 블록체인 네트워크를 독립적으로 동작하게 함으로써 문제점을 개선하여 기부 서비스를 하는 Cherry system을 소개하려고 한다[4][5].

III. Cherry Blockchain System

기부시스템 대부분은 기부단체에서 기부받아 집행하기 때문에, 일반적으로 기부단체의 주관하에 모든 기부 대상이 선정되고, 기부금이 집행된다. 본 논문에서 소개하는 블록체인 기부시스템인 Cherry System은 기부자가 기부 이벤트, 기부 대상과 기부금의 사용 여부에 관한 결정에 참여할 수 있게 설계되었다. 그러므로 보다 투명하게 탈중앙화가 적용되는 기부시스템을 실현하게 된 것이다[16].

1. User-independent blockchain method

Cherry system에서 구현한 사용자 독립방식의 블록체인 기부시스템은 거래 관리는 블록체인 기반으로 진행되지만, 사용자는 블록체인에 연관이 없이 독립된 방식으로 서비스 받는 방식이다. 여기서 사용자는 기부공여자, 기부수혜자와 기부단체등 Cherry system을 사용하는 객체를 의미하며, 사용자는 블록체인의 지갑 관리나 가상화폐 거래 등 블록체인 관련된 프로세싱에 관여 없이 독립적으로 진행된다. 따라서 사용자의 앱은 블록체인의 wallet의 기능이 없고 단순히 기부 금액을 전달하거나 수신하는 것이고, 블록체인의 모든 기능은 Cherry System에서 관리하기 때문에 Cherry는 블록체인 게이트웨이 기능까지 전부 수행한다. Fig. 4.에서 기부자 지갑(Donor wallet)이나 스마트 계약, 기부단체 지갑(Donation group wallet)은 Cherry system 내부에서 블록체인에 의해서 관리되고, 사용자는 통상적인 방식으로 기부금 전달과 기부금 수혜를 받아서 사용하게 된다. 이렇게 하기 위해서 Cherry System은 사용자가 시스템에 등록하면 은행과 연동하여 가상계좌를 개설하고, 기금을 분리 보관하여 관리하면서 체리 시스템과 실시간으로 매칭하여 예치관리, 지급관리, 거래 내역조회 등을 하도록 한다. 시스템 내에는 블록체인의 포인트를 개인별로 관리하여 처리한다. 이렇게 함으로 기부자는 편리하게 기부하면서, 기부금의 사용처를 마이크

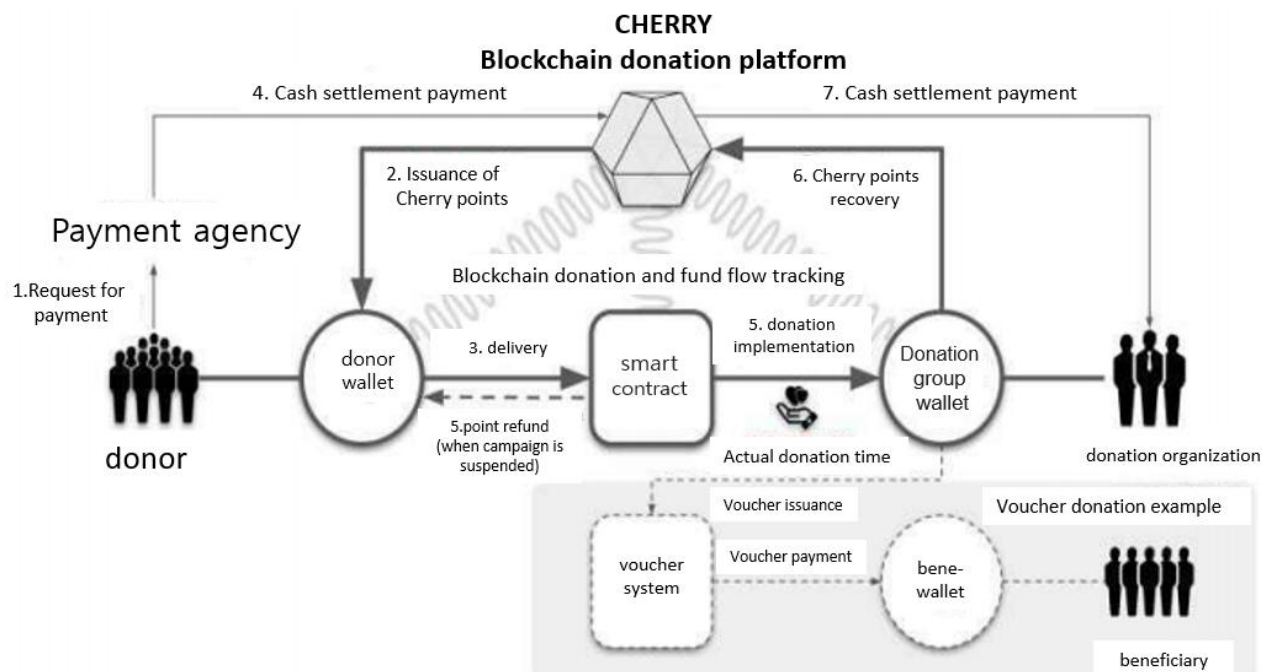


Fig. 4. Basic flow of CHERRY platform

로 레벨까지 트래킹이 가능하게 되었다. 기부금 수혜자는 카드시스템이나 바우처시스템 등의 다양한 형태의 서비스를 받을 수 있게 하였다.

2. Basic Donation Blockchain flow

본 논문에서 제안하는 블록체인 기반의 기부 플랫폼인 Cherry system의 기본 흐름은 Fig. 4.에서 보여주고 있다. 기부자가 블록체인 플랫폼인 Cherry system을 통해 기부를 이행하고자 할 때, 체리 앱을 통해서 지급 금액과 지급 대상을 선정해서 기부 의사를 표시한다. Cherry system의 블록체인 서버에서 해당 금액에 대응하는 체리 포인트(코인)를 발행해서 기부자의 지갑에 표시되면서 자동으로 선택한 기부 캠페인의 기부단체 지갑으로 체리 포인트를 전달함으로써 스마트 계약이 성립된 후에, 독립적으로 사용자에게 기부가 이행된다.

스마트 계약이 성립되어야 블록체인 서버는 원화 정산 지급을 진행하고, 체리 지갑에서 체리 포인트를 회수하게 된다. 이는 혹시라도 캠페인이 목표 기금이 완료되거나 다른 원인으로 캠페인이 중단되었을 때는 원화 정산이 되는 것을 방지하기 위해서 블록체인의 체리 포인트 전달의 과정이 완료되는 스마트 계약 후에 금융권을 통해 원화 절차가 진행되도록 하였다. 여기서 거래되는 지갑의 내용은 사용자 독립적으로 시스템에서 직접 관리하면서 거래 절차를 진행한다. 이런 일련의 과정이 실시간으로 이행된 후에

기부단체로 실제적인 법정화폐가 정산되어 전달된다. 체리 포인트에 매칭되는 기부금은 서버 내에 있는 분배 시스템에 의해서 다양한 형태로 수혜자에게 전달될 수 있도록 설계되었다. 분배 형태는 체리 카드, 체리 포인트, 체리 바우처 (상품권 / 금액 상품권) 혹은 쿠폰 등으로 사용하게 하고, 수혜자의 앱에서 확인하며 사용하게 한다. 이를 위해서 서버는 체리 포인트와 법정화폐를 매칭하여 분리함으로써 사용자 독립적인 관리를 할 수 있게 된다[16].

본 블록체인 시스템을 적용하기 위해서 기부단체의 공익사업 기금을 공신력 있는 금융 기관에 기부자 ID의 가상 계좌를 자동 생성하여, 분리 보관 예치하여 기금을 분배하도록 함으로써 블록체인 기록의 신뢰성을 극대화하였다. 또한 기부단체에 전달된 기부금이 분산되어 수혜자에게 전달되는 경우 기존 블록체인 기술을 사용하면 세부적인 추적이 불가능한 문제가 있는데, 본 시스템에서는 이포넷(주)이 보유한 특허 기술 "기부금의 자동 할당 분배 방식에 의한 능동적 블록체인 마이크로 트래킹 시스템 및 방법" 기술을 적용하여 기부자의 금액에 별도의 time stamp 추적 기능을 보강하여 기부자가 지급한 기부금의 정확한 사용처의 세부 내역까지 조회할 수 있도록 하였다[5].

3. Cherry System's Block Diagram

Fig. 5.의 블록다이어그램에서 보듯이 블록체인 내부에서 기부금 발생에 따른 체리 포인트의 전달과 계약 체결,

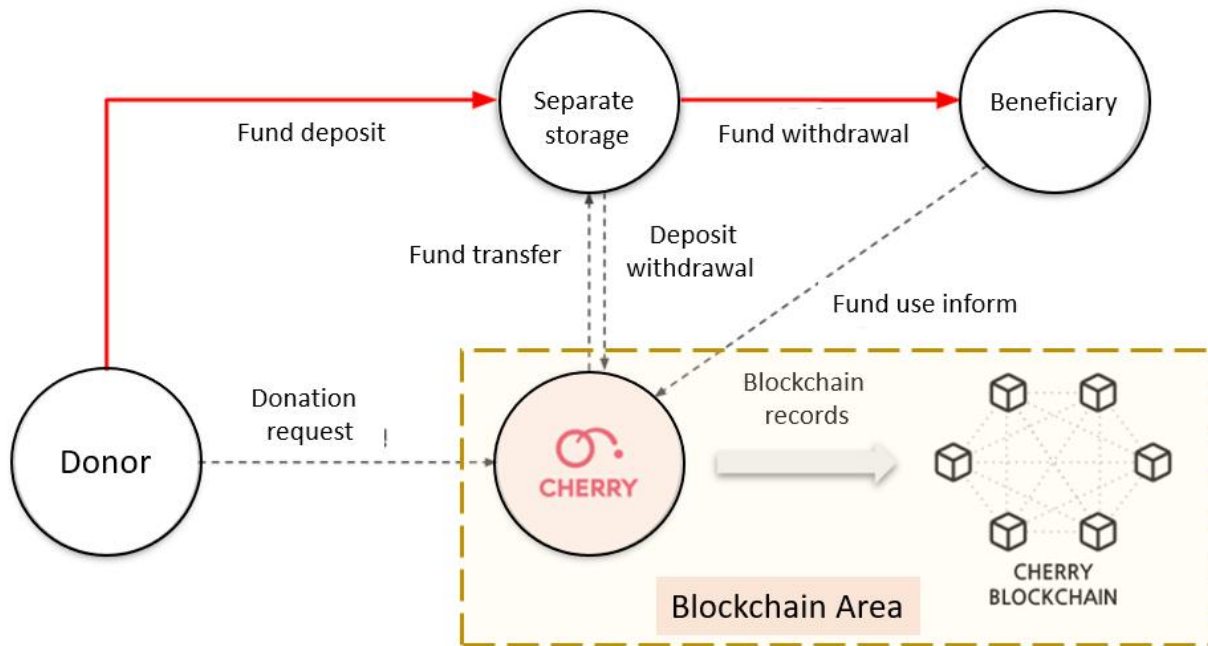


Fig. 5. Cherry System Block Diagram

기부 영향력 자동 결정 등을 블록체인 기반으로 동작하도록 구성하였다. 그리고 기부자 단말이나 기부단체 단말 등은 앱을 통해 개인 ID에 따라 블록체인 네트워크에 접근하여 기부금 결정과 기부금 전달 등의 행위가 사용자 독립적으로 이루어지도록 하였으며, 법정화폐는 가상계좌를 통해 외부 서버 시스템이 별도 관리하도록 하였으며, 블록체인에서 관리하는 포인트는 법정화폐와 매칭시켜 ID 단위로 블록체인 내부에서 관리하고 있다. 이를 통해 수혜자에게 다양한 형태의 기부금을 전달할 수 있게 되었다. 이런 시스템을 구현하기 위해서 사용자(기부자나 수혜자)를 블록체인과 법정화폐 시스템을 분리하여 처리하는 방식으로 운영하여야 하고, 본 시스템은 블록체인 게이트웨이의 전체 역할을 수행하는 모듈을 추가하여야 한다. 이렇게 함으로 POS로 운영되는 블록체인 자체의 성능을 상당히 개선할 수 있었다. 또한 가입자는 블록체인과 분리 방식으로 운영되기 때문에 별도의 wallet이나 거래비용 등을 지불할 필요가 없는 기부 플랫폼을 실현하였다. Fig.6.에서 보듯이 기부 수혜자의 체리 서비스 앱은 사용자 독립적으로 동작하기 때문에 일반적인 카드와 같이 결제하면 마이크로 트래킹 기술에 의해서 "체리 스크"에서 사용 내역이 구체적으로 추적가능하게 된다. 이는 단순 블록체인을 사용하는 경우 기부단체에 전달된 기부금액까지는 추적이 가능하지만, 수혜자의 구체적인 거래 내역까지 추적하는 것은 기부단체에 전달된 기금을 분리해서 추적할 수 있는 마

이크로 트래킹 기술을 적용하여 처리하기 때문에 가능한 것이다.

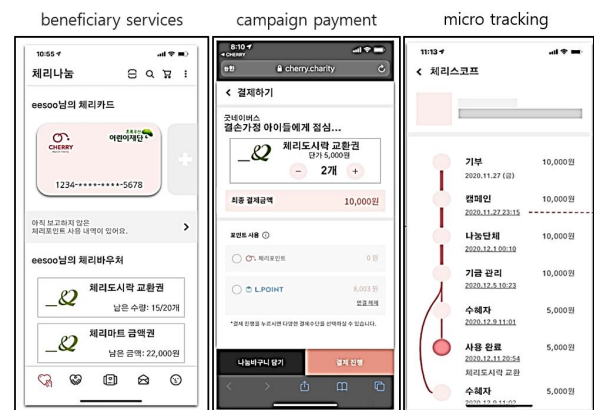


Fig. 6. Cherry Service App

4. Cherry cryptography method

본 논문에서 제시하는 블록체인 기부시스템은 Fig.7.과 같이 비대칭키 방식에 의해서 장부를 암호화하여 관리한다. 기부자가 최초에 가입하면 블록체인 체리 시스템에서는 개인 ID를 부여하면서 개인키와 공개키를 발생시켜서, 공개키는 체리 시스템이 관리하고, 개인키는 기부자 앱을 통해 개인이 관리하게 한다. 기부자가 앱을 통해 기부 금액을 전달하게 되면 기부 금액 관련 데이터를 블록체인에 저장하여 기록하고, 수혜단체에 기부 금액을 전달한다.

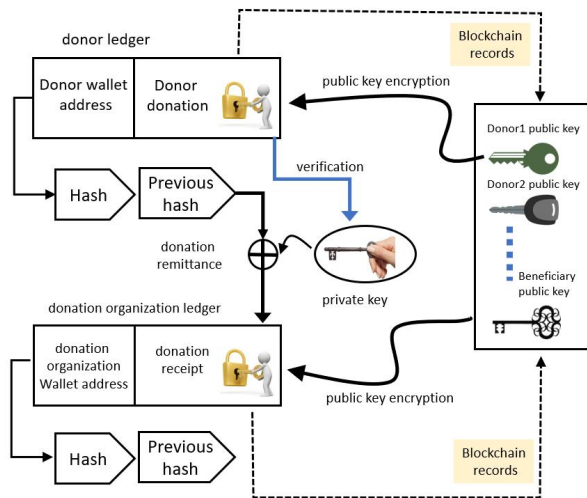


Fig. 7. Cherry Blockchain Encryption

▶ 기부데이터 암호화 : 기부자가 등록할 때 블록체인 시스템에서 개인 ID, 개인키와 공개키를 발행한다. 그리고 개인키는 앱을 통해 개인이 관리하게 하고, 공개키는 시스템에서 관리하며 블록 생성 및 데이터 암호화 시 사용된다. 그리고 개인이 암호화된 거래명세, 자신의 데이터나 장부를 해독할 때 개인키를 통해 복호화하여 볼 수 있게 된다.

▶ 기부금 전달 : 기부 금액을 기부단체에 전달하는 송금이 발생할 때 개인키를 사용하여 기부자는 디지털 서명한다. 디지털 서명이 완료되면, 거래의 유효성을 검증하고 블록체인 시스템을 통해 네트워크에서 검증 후에, 수혜단체 ID에 해당하는 공개키로 암호화하여 수혜단체에 전달한다. 수혜단체에서는 암호화된 거래금액을 전달받아서, 수혜단체의 개인키를 통해서 수신 금액을 수령하게 된다. 이것은 블록체인 네트워크에서 체리라는 포인트를 통해서 전달되는 과정이고, 체리를 받으면 동일한 금액의 법정화폐 통장에서 원화 정산 및 지급 처리가 완료된다. 이런 과정에서 중요 정보는 DB 저장 단계에서 암호화하였고, 닉네임과 지갑 주소 등의 서비스에 필요한 최소 부분만 노출하며, 기타 정보는 마스킹 처리하여 보호하였다. 모든 데이터 처리는 키 기반하여 코드성 메모리 적재방식에 의해 빠른 반응 속도를 제공하도록 설계하여 블록체인 서비스 응답속도를 개선하였다.

5. Automatic influence control POS method

POS는 이더리움과 같은 블록체인에서 사용하고 있는 합의 알고리즘이다. 일반적으로는 블록을 생성할 때 네트워크 참여자들의 기부 분량(stake)에 따라 합의하는 데 영향력을 미치게 된다. 이런 경우 기부 블록체인 시스템과

같은 private blockchain을 사용하는 경우 51% 공격의 위험이 있다[8]. 그리고 대량기부한 기부자의 stake가 커지고 결정 권한이 일부에 편중되는 우려가 잠재되어 있다.

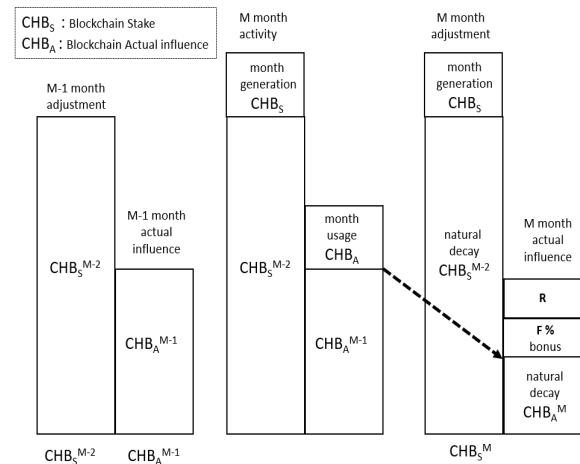


Fig. 8. Automatic Blockchain Influence control Algorithm

본 기부시스템에서는 권한의 집중화를 자동 제어하는 알고리즘을 적용하여 지분 합의 과정이 진행되도록 설계하였다. 기본 영향력인 기부자의 stake 분량은 시간에 따라 자동 감쇄하게 하였고, 추가로 영향력을 결정하는 요소로 기부자가 활동하여 발생하는 보너스(F)와 기부 결정 분량(R)의 요소를 고려하여 자동 산정한 후에, 실제 영향력이 자동 결정되도록 하였다. CHB_S 는 Cherry system에 기부하면 자동으로 생성되는 포인트로 영향력 분량이다. CHB_A 는 블록체인의 실제적인(Actual) 영향력으로 블록 생성과 이벤트 결정 등에서 부여된 CHB_A 만큼의 영향력을 행사하는 것이다. Fig.8.을 보면 자동 블록체인 영향력 제어 알고리즘의 월별 영향력을 상태를 나타내고 있다. M-1월의 실제 영향력(CHB_A^{M-1})은 이전 달에 기부한 CHB_S^{M-2} 에 의해 생성된 영향력이 한 달이 지난 M-1월에는 절반이 감소된 실제 영향력(CHB_A^{M-1})을 부여한다. M월에 기부 결정 분량(R)이 이벤트나 기부 정책 결정에 유효한 영향력 행사한 경우, 사용한 기부 결정 분량(R)이 남고, 기여도와 활동력에 기반한 일정 비율의 보너스(F)를 추가로 부여한다. 그리고 전월에 남아있던 실제 영향력(CHB_A^{M-1})은 자동으로 감쇄된 실제 영향력(CHB_A^M)만 남게 된다. 자동 감쇄 기부 영향력과 새로 생성된 영향력을 통해 신규로 결정되는 실제 영향력은 수식 (1)과 같다.

$$\begin{aligned} \text{당월 결산 기부 영향력} &= \text{전월 결산 기부 영향력} \times (1 - 2^{-1/N}) + \\ &\quad \text{신규 생성 기부 영향력} - \text{사용한 기부 영향력} \end{aligned} \quad (1)$$

자동 감쇄 알고리즘을 적용하여 전월 결산 기부 영향력을 계산하면 많이 기부한 경우에도 2개월이 경과되면, N이 2가 되어 영향력이 0.3이 되고, 36개월이 경과되면 0.02의 결산 영향력이 되므로 단순 기부를 많이 하여 stake가 큰 경우에도 일부 기부자에 편중되지 않고 기부 및 행사 참여자에게 자연 분산되는 효과가 있다.

6. Performance test

본 논문에서 제시한 Cherry System은 TTA에 의해서 성능 검증을 받았다. 테스트 환경은 Table 4.에서 보듯이 JMeter 방식을 이용해서 테스트하였고, 개별 블록에 부하는 4000 거래를 하며, GAS 용량을 64,000,000으로 제한하였으며, 1,000,000개의 트랜잭션을 30초간 전송하면서 성능 측정을 하였다.

Table 4. Test conditions

Main Items	Conditions
Method	JMeter
BatchTimeOut	1 second
One block load	4000 transaction
GAS	64,000,000
RDS	PostgreSQL
Authentication	OIDC / OAuth2

Cherry system의 성능테스트는 다양한 부하 조건에서 TPS 성능을 측정하였다. Fig. 9.에서 보듯이 데이터 처리 부분에서 산술연산이나 논리연산이 포함되는 Smart contract로 구현되는 경우에 해당하는 Complex data processing과 블록용량이 커지는 상황에서 블록의 확장 성능을 고려한 Large data size의 경우가 최악의 거래 상황인데, 139개의 TPS 성능을 보이고 있다. 또한 다수의 사용자가 동시에 데이터 조회를 요청하는 Query performance 상황에서는 TPS가 최대 2187.9를 나타내고 있다. 그리고 가장 일반적인 블록체인 트랜잭션으로 합의 및 데이터 등록 과정의 성능인 Typical transaction 조건에서 1032.5의 TPS 성능을 보이고 있다.

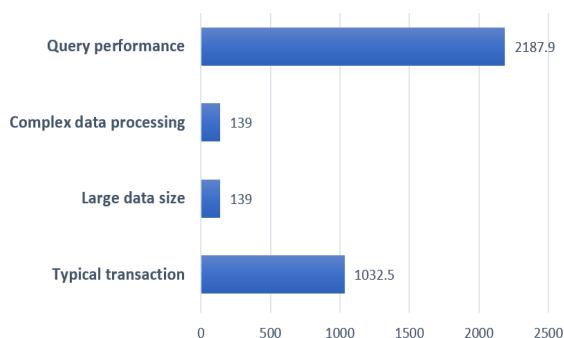


Fig. 9. TPS performance for Cherry system

Bitcoin을 사용하는 POW 방식의 기부시스템은 10 이하의 TPS를 보이고, 이더리움을 사용하는 POS 방식의 기부시스템을 적용하는 경우 15 정도의 TPS 성능을 보이고 있다[10]. 기존 기부시스템과 비교할 때, Cherry system의 개선된 정도는 Table 5.를 통해 알 수 있다.

Table 5. comparison between POW and POS

ITEMS	agreement	TPS
Bitcoin	POW	under 10
Ethereum	POS	14-15
Binance	POS	100-200
Cardano	POS	250-1000
Cherry	POS	Over 1000

서비스 응답시간은 가장 응답시간이 느린 거래 기능에 대해서 측정한 것으로, 데이터를 등록하여 처리 완료하는데 소요되는 시간을 10회 반복하여 측정한 평균 응답시간이 21.3 초를 나타내는 것을 Fig. 10.을 통해 알 수 있다.



Fig. 10. Service response time

전통적인 비트코인의 경우 블록 생성에 10분 이상 소요되고, 이더리움의 경우도 20초에서 수 분씩 소요되는 것으로 알려져 있어서, 서비스 불편에 대한 우려의 목소리도 있다[12]. 반면에 Cherry system은 기부시스템 속성상 near real time을 요구하는 서비스이다. 따라서 기존 시스템에 비교해서 21.3초의 평균 응답시간은 사용자가 자신의 기부 내용을 불편 없이 처리할 수 있을 정도로 개선된 것이다.

IV. Conclusions

본 논문에서 제안한 Cheery 블록체인 시스템은 블록체인과 법정화폐의 기부금 관리를 가입자별로 분리해서 관리하는 기법이다. 이를 위해 기부자가 기부금을 납부하면 가상계좌를 자동 생성하고 블록체인의 체리 포인트 관리를 별도 DB로 매칭하여 관리한다. 이렇게 함으로 기술적인 관점에서 POS/POW 방식을 사용하는 기존 기부시스템보다 TPS 성능이 상당히 개선되었고, 서비스 시간도 많이 단축되는 효과를 보았다. 그리고 POS의 권한 집중 문제를 해결하기 위해서, 본 시스템에서는 권한 자동 제어 알고리즘을 적용하여 단순 stake만으로 권한이 집중되는 것을 제어하고, 캠페인의 선정 및 행사 등의 결정에 선한 영향력 있는 참여자에게 권한을 추가로 부여함으로써, 권한 집중의 잠재적 문제를 크게 개선하였다.

또한 블록체인은 블록 단위로 추적하는 투명성의 한계가 있는데 본 논문에서는 블록 데이터에 타임스탬프 추적 기능을 추가함으로써 블록 단위보다 세분화된 마이크로 트래킹이 가능하게 하였다. 이를 통해 기부자의 수혜금의 용처를 실시간 앱을 통해서 최종 수혜자까지 추적 가능하게 하였다.

추가해서 서비스 관점에서는 사용자는 블록체인으로 관리되는 기부시스템이지만 기존의 금융거래와 동일한 서비스를 받게 하였다. 이렇게 함으로 기부자는 블록체인을 사용하는 불편함이나 거래비용 등의 문제를 해소할 수 있었다. 또한 수혜자에게 지급하는 수혜금은 체크카드, 선불카드, 현금, 상품권 등의 다양한 형태의 바우처를 지급함으로써 수혜자의 편의를 높이게 되었다.

REFERENCES

- [1] Beautiful Book, "Giving Korea 2022," The 21st Donation Culture Symposium, pp. 16-26, Dec. 2022.
- [2] Sjkim, Yjjang and Yrlee, "A Study on Changes in Donation Methods in Korea," The Beautiful Foundation, pp. 25-30, Mar. 2022.
- [3] Shhan, Dyhong, N.J. Choi. N.B. Lee and K.J. Kim, "Analysis of Consensus and Transaction of (D)PoS-based Blockchains", Korea Institute of Information Security & Cryptology, pp. 469-474, Jun. 2018. URI : <http://hdl.handle.net/10203/246821>
- [4] E4NET and Sjee , "AUTONOMOUS BLOCKCHAIN BASED DONATION SYSTEM AND METHOD," Patent, No. 1020200144715, Nov. 2020.
- [5] E4NET and Sjee , "ACTIVE BLOCKCHAIN MICRO-TRACKING SYSTEM AND METHOD BY AUTOMATIC ALLOCATION AND DISTRIBUTION OF DONATIONS," Patent, No. 1023363060000, Dec. 2020.
- [6] Sblee and Khkim, "Design of Enhanced Pos Mechanism for Scalability without Centralized Process ", The Journal of Korean Institute of Next Generation Computing, Vol. 16, No. 1, pp.75-85, Feb. 2020.
- [7] Zheng,Z., Xie,S., Dai,H.N., and Wang,H., "Blockchain Challenges and opportunities", International Journal of Web and Grid Services, Vol. 14, No. 4, pp. 352-375, 2018. DOI : 10.1504/IJWGS.2018.095647
- [8] Nguyen,C.T., Hoang,D.T., Nguyen,D.N., Niyato,D., Nguyen,H.T. and Dutkiewicz,E., "Proof of stake consensus mechanisms for future blockchain networks", Fundamentals, application and opportunities, IEEE Access, 7, pp. 85727-85745, 2019. DOI: 10.1109/ACCESS.2019.2925010
- [9] Hkkm, Smlee, Hwkwon and Emkim, "Design and Implementation of a Presonal Health Record Platform Based on Patient-consent Blockchain Technology", KSII Transactions on internet and information systems, Vol.15, No.12, Dec. 2021. DOI:10.3837/tiis.2021.12.008
- [10] Ksjang and Olee, " The Design and development of a Onchain Game for Scalability Verification of Blockchain Platform", Journal of Digital Convergence, Vol. 18, No. 10, pp.253-263, 2020. DOI:10.14400/JDC.2020.18.10.253
- [11] Cykim, Yhkim and Jhlee, " A Study about Blockchain Donation System using Ethereum", The KIPS fall conference 2019, Vol. 26, No. 2, pp. 453-455, Nov. 2019. UCI : 1410-ECN-0102-2022-500-000349274
- [12] Kwkwang and Hjyou, "A Study on the New Donation System Based on the Block Chain", The KIPS spring on-line conference 2020, Vol. 27, No. 1, pp. 358-360, May 2020. UCI : 1410-ECN-0102-2022-500-000360373
- [13] Yhkim, Ukbaek,Ycjin, Igham and Iskim, "Reliable Donation Service Using Ethereum Blockchain", Journal of Knowledge Information Technology and Systems(JKITS), Vol.15, No. 4, pp. 539-548, August 2020. DOI: 10. 34163/ jkits.2020. 15. 4.009
- [14] Khan and Hjseo, " Donate system development using Blockchain technology", Journal of the Korea Institute of Information and Communication Engineering (JKIICE), Vol. 22, No. 5, pp. 812-817, May 2018. DOI:10.6109/jkiice .2018.22.5.812
- [15] Sdyoo, " A Study on Consensus Algorithm based on Blockchain", The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), Vol. 19, No. 3, pp.25-32, Jun. 2019. DOI: 10.7236/JIIBC.2019.19.3.25
- [16] E4Net, Cherry donation platform product introduction, Retrieved from <https://cherry-manual.s3.ap-northeast-2.amazonaws.com>, 2020

Authors



Sang-Dong Sul received the B.S. and M.S. degrees in electrical engineering from the Korea Aerospace University in 1985 and 1988, respectively. Until 1993, he worked as a software developer at LG Information &

Communications and worked as a technical engineer at Agilent Technology until 2005 and worked as CEO of Borasys Co., Ltd. until 2017. He has been working as a professor in the Department of Information and Communication Engineering at Dongyang Mirae University since 2018. He is currently interested in sensor networks, blockchain, artificial intelligence and data analysis.



Su-Jeong Lee received her bachelor's and master's degrees in information processing from Sogang University in 1986 and 2001, respectively. She worked as an EDI system developer at Dongjin Information until 1994,

and as a card solution developer at BC Card in 1995. She founded E4NET Co., Ltd. in 1995 and currently serves as CEO. Her areas of interest are IT financial service, fintech solutions, blockchain platform and NFT application solutions.