Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 5 pp. 394-402, 2021

https://doi.org/10.5762/KAIS.2021.22.5.394
ISSN 1975-4701 / eISSN 2288-4688

# 마스터 노드 네트워크를 사용한 블록체인 익명 투표 모델

조재한[1], 이이섭[1], 최창훈[2*]
[1]금오공과대학교 컴퓨터공학과, [2]경북대학교 소프트웨어학과

# Anonymous Blockchain Voting Model using the Master Node Network

Jae-Han Cho[1], Lee-Sub Lee[1], Chang-Hoon Choi[2*]
[1]Department of Computer Engineering, Kumoh National Institute of Technology
[2]Department of Software, Kyungpook National University

**요 약** 전자 투표 시스템은 90년대 중반부터 세계 많은 국가들에서 널리 활용되고 있다. 최근에는 유권자들에게 신뢰성, 공정성, 그리고 투명성을 제공하기 위해 기존의 전자 투표 시스템에 블록체인을 적용하는 연구가 진행되어 왔다. 이 방식은 분산형 시민 참여를 촉진하는 기술로 유용성이 높다. 그러나 기존의 블록체인을 이용한 전자 투표 시스템들이 익명성을 충분하게 제공하지 못하고 있다. 익명성 부족은 분산형 시민 참여에서 많이 요구되는 중소규모의 투표의 경우에 중요한 제약 조건으로 작용하고 있다. 본 연구에서는 대시코인의 마스터 노드의 개념을 응용하여 블록체인을 사용한 투표시스템에 익명성을 제공하는 모델을 제안하였다. 먼저 블록체인에서의 송금과 투표 시스템의 요구사항에 대한 차이점들을 정의하였다. 블록체인 즉 탈중앙화 개발 환경에서 익명성을 제공하기 위한 병행적이고 자율적인 모델과 알고리즘을 제안하였다. 또한 제안된 모델에 대한 보안성과 운영 환경에 대한 논의를 기술하였다.

**Abstract** Electronic voting systems have been widely used in many countries around the world since the mid-1990s. In recent years, studies have applied blockchain to existing electronic voting systems in order to provide reliability, fairness, and transparency for voters. This approach is highly useful as a technology that promotes decentralized citizen participation. However, the existing electronic voting systems using blockchain have not sufficiently considered anonymity. Lack of anonymity acts as an important constraint in cases of small- and medium-sized voting, which is often required in decentralized citizen participation. In this study, we propose a model that provides anonymity to a voting system using blockchain by applying the concept of the master node in Dash cryptocurrency. First, we define the differences in the requirements of the transfer and voting systems in blockchain. We propose a parallel and autonomous model and algorithm to provide anonymity in the blockchain-that is, a decentralized development environment. In addition, a discussion of security and the environment for the proposed model is described.

**Keywords :** Blockchain, Electronic Voting, BEV, Decentralized, Master Node, Dark Coin

본 논문은 금오공과대학교 연구과제로 수행되었음.(2018104084)
*Corresponding Author : Chang-Hoon Choi(Kyungpook National University )
email: hoon@knu.ac.kr
Received March 23, 2021 Revised April 20, 2021
Accepted May 7, 2021 Published May 31, 2021

# 1. 서론

## 1.1 블록체인을 이용한 투표에서의 익명성

민주주의에서 투표는 중요한 요소로 작용하고 있으며 디지털 기술을 통해 시민참여를 활성화시키려는 노력들이 진행되어 왔다[1]. 시민 참여를 활성화하기 위해 IT 기술을 응용한 전자투표 방식이 널리 활용되고 있다. 전자투표는 90년대 중반부터 세계 주요 국가들이 도입하였고, 현재는 약 50여 개국이 공직선거에 전자투표를 도입하여 활용하고 있다[2]. 이러한 전자 투표 시스템은 유권자의 신뢰를 얻을 수 있으며 분산형 시민 참여를 촉진시키는 기술로 유용하다[3].

최근에는 공정성과 투명성을 강조하기 위해 블록체인을 도입하여 전자투표에 이용하고 있다. 블록체인은 가상화폐인 비트코인의 안전한 유통을 위한 기술로 본격적으로 주목을 받아왔다. 최근에는 일종의 분산장부기술로서 그 응용 분야가 금융 분야뿐만 아니라 다양한 분야로도 확대되고 있다[4].

전자투표는 블록체인의 주요 응용 분야 중 하나이며 블록체인을 접목한 전자투표 시스템을 (BEV : blockchain-enabled e-voting, 이하 BEV)라고 한다. BEV는 블록체인의 특성상 큰 규모의 투표에는 활용되기 어려우며, 당내 의사결정이나 내부 투표 등 중소규모에 적합하다. NIA에서 발표한 연구결과[5]도 국가적인 대규모 투표보다는 당내 의사결정, 청원, 주민 의견 수렴 등 중·소규모 투표 방식에 먼저 적용 가능하다고 하였다. 중·소규모 투표의 경우에 투표인들 간의 밀접한 이해관계로 익명성이 더욱 중요하게 부각된다.

## 1.2 탈중앙 시민 참여 기술과 익명성

EU에서는 블록체인을 기반으로 시민들의 자발적 참여를 유도하기 위해 탈중앙 시민 참여 기술(D-CENT : Decentralized Citizens Engagement Technology, 이하 D-CENT)[7]이라는 프로젝트를 수행하였다.

Fig. 1에서와 같이 블록체인 생태계 구축의 필수 요소인 보상 시스템을 제공하기 위해 Freecoin이라는 가상화폐를 구축하였다. 이를 기반으로 정책 결정, 조달, 전자투표와 같은 도구들을 블록체인을 직접 사용하지 않고 중앙 집중식 방식으로 개발하여 오픈소스 형태로 제공하였다. 이 도구들을 사용하여 시범 사업들을 추진하였다. 스페인의 바르셀로나와 마드리드에서 정책의 결정 및 우선순위 지정 등 시정 참여가 가능한 서비스인 Decided Barcelona[8]와 Decide Madrid[9]를 운영하였다. 아이슬란드 레이캬비크에서는 시민 참여 예산 시스템인 Better Reykjavik[10]를 핀란드 헬싱키는 지자체 정책 결정을 위한 알림 시스템으로 Decisions Helsinki[11]를 도입하여 운영 중이다.

Fig. 2와 같이 이더리움에서 스마트계약의 개발 기능이 제공됨에 따라, 투표 결과를 블록체인에 직접 기록하는 방법을 사용한 BEV들이 개발되었다[2,6,12,13]. 블록체인의 모든 정보는 누구에게나 공개되어 접근 가능하여 익명성이 요구되는 투표에는 적용이 불가능하다. 본 연구에서는 기존 가상 화폐의 송금에서 익명성을 제공하는 다크코인(Dark coin)의 익명성 제공 방법들을 분석하여 대시코인을 기반으로 투표에서의 익명성 제공하는 방법을 연구하였다.

논문의 구성은 다음과 같다. 2장에서는 이 연구에서 제안하는 코인조인을 응용하여 투표 시스템에 익명성을 제공하는 방법을 제시한다. 3장에서는 설계상의 문제점과 해결 방안에 대하여 정리한다. 4장에서 실제 적용에 있어서 필요한 논의를 수행한다. 마지막으로 5장에서는 결론 및 향후 연구에 대해서 정리하였다.

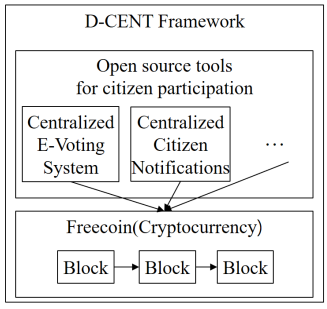



Fig. 1. D-CENT Framework

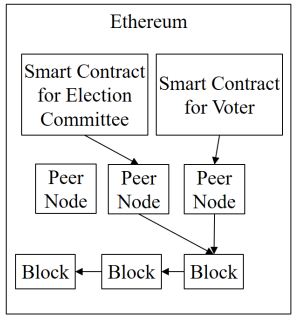



Fig. 2. Existing BEV Architecture

## 2. 블록체인을 사용한 익명 투표 모델

### 2.1 대시코인과 투표의 익명성

BEV에서는 대부분 후보자들을 대표하는 계정에 토큰을 전송하는 방법으로 투표를 진행한다[12,13]. 송금 트랜잭션은 〈송금자 계정, 송금액, 수신자 계정〉의 형태로 블록체인에 기록이 된다. 계정이 해시로 암호화되어 있으나, 비트코인 사용자들은 추적이 불가능한 것은 아니다. 따라서 투표에 적용하는 경우 충분한 익명성이 제공하기가 어렵다[14].

보다 완벽한 익명성을 제공해주는 암호 화폐들을 다크캐시(Dark Cash)라고 한다. 대표적인 다크캐시는 제트캐시(Zcash), 모네로(Monero), 그리고 대시코인(Dash Coin)이 있다[14]. 제트캐시는 송금자, 수신자, 그리고 송금액을 노출시키지 않고 영지식 증명(Zero-Knowledge Proof)으로 검증하는 방법이다. 영지식 증명은 일반적인 송금에는 적합할 수 있으나, 수신자의 수가 적고 송금액이 항상 1인 투표에는 적용하기가 어렵다. 모네로는 링서명(ring signature), 링 CT(ring confidential transactions), 스텔스 주소(stealth address) 기술을 사용하여 각각 송금자, 송금액, 수신자를 노출시키지 않는 방법이다. 투표의 경우 송금액이 일정하고 수신자도 쉽게 특정할 수 있으므로 적용이 어렵다. 송금자를 보호하는 방법인 링서명은 그룹 서명 방법의 일종으로 역시 투표에는 적용이 어렵다.

대시코인[15]은 비트코인의 하드포크로서 즉시 전송(Instant Send)과 비밀 전송(Private Send)을 제공하는 가상화폐로 이 서비스를 지원하기 위해 마스터 노드들로 이루어진 2차 네트워크를 구성한다. 마스터 노드들은 전체 블록 정보를 가지고 있는 풀노드(full nodes)들을 의미한다. 비트코인에서 풀노드들은 충분한 리워드(reward)를 받지 못하여 그 수가 점차적으로 감소하는 추세이다. 대시코인에서는 가상 화폐 생태계를 유지하기 위해 마스터 노드들에게 PoS(Proof of Stake) 방식으로 추가적인 리워드를 제공하여 해결하고 있다. 기존의 거래는 트랜잭션 단위로 블록체인에 저장되지만 코인조인에서는 믹싱 작업을 진행하여 익명성을 확보한다. 마스터 노드는 이러한 믹싱 작업을 여러 번 수행하여 자금 흐름의 추적을 더욱 어렵게 만들 수 있다.

마스터 노드들로 구성된 2차 네트워크는 투표에 서 요구되는 투표용지의 배포, 집계 등의 기능을 제공하기가 용이하여 다른 다크코인들보다 투표에 보다 적합하다.

### 2.2 BEV의 요구 사항과 개발 환경

송금과 투표는 데이터 처리에 대한 특성에 있어서 다음과 같은 차이점들이 있다. 첫 번째로 송금의 경우는 세션(session)이 단순하고, 세션 이전의 사전 작업이나 사후 작업이 거의 없다. 투표는 시작 단계에서 다양한 준비가 필요하고 완료 단계에서도 집계와 같은 사후처리가 요구된다. 두 번째로 송금은 최대 몇 분 이내에 처리해야 하지만, 투표는 최소 몇 시간에서 며칠이 소요된다. 따라서 알고리즘의 성능이나, 신속한 응답 시간이 요구되지 않는다. 세 번째로 송금과는 달리 투표는 도착지 즉, 후보자들이 소수이므로 익명성이 훼손될 가능성이 높다. 네 번째로 투표는 한 사람이 하나의 표를 행사하므로 잔금에 대한 개념이 없다. 이러한 특성은 잔금으로 인한 역추적 공격을 방어에 대한 용이성을 제공한다. 마지막으로 화폐는 사용 기한이 없으나 토큰으로 표현되는 투표용지는 사용 기한이 정해져 있으며, 투표 완료 이후에 다시 사용할 수 없다. 따라서 투표마다 ERC20(Ethereum Request for Comments 20)과 같은 토큰 생성 방법을 사용해야 한다.

이러한 투표의 특성을 반영하려면 기존의 송금 방법을 그대로 적용하기 힘들며, 세심하고 전면적인 재설계와 재개발이 필요하다.

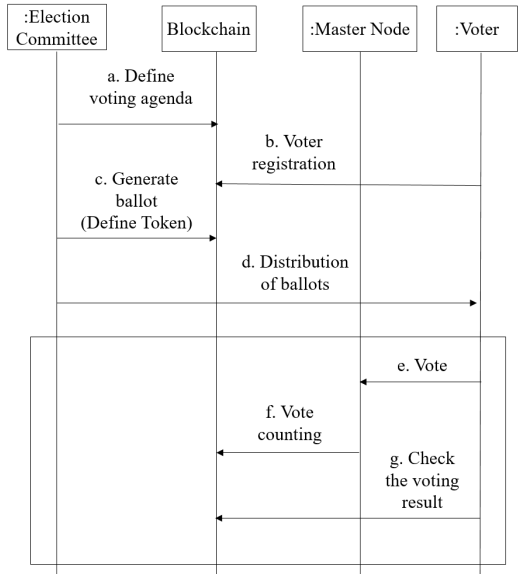



Fig. 3. Voting Process

Fig. 3은 전체 투표 프로세스를 순차도(sequence

diagram)로 정리한 것이다. a단계에서 선거관리위원회는 투표 안건에 대한 유권자 목록, 투표기간, 후보자 목록 등의 메타 정보를 정의하고 블록체인에 기록한다. b단계에서 투표자들은 자신이 적법한 투표자임을 블록체인에 등록한다. c단계에서 선거관리위원회는 투표용지를 대신할 토큰을 생성하고 d단계에서 투표자들에게 토큰을 배포한다. e단계에서 투표자들은 원하는 후보자 계정에 토큰을 전송하여 투표를 수행한다. 투표시간이 종료되면 f단계에서 집계가 수행된다. 집계가 완료되면 g단계에서 투표결과를 확인할 수 있다. e단계 이전 단계들은 투표의 환경에 따라 상이하므로 익명성을 다루는 e단계 이후를 연구 범위로 한정하였다.

Fig. 4는 일반적인 컴퓨팅 환경과는 다른 블록체인의 개발 환경을 보여준다. 블록체인은 전통적인 분산 시스템(distributed system)과는 다른 탈중앙화(decentralized) 시스템이다. 즉, 중앙 서버가 존재하지 않고 병행적(concurrent)이고 자율적(autonomous)인 알고리즘을 갖는 상호신뢰가 없는(Trustless) 노드들로 구성된 순수 P2P방식의 시스템이다. 따라서 기존 분산 시스템과는 운영 환경이 매우 상이하여 설계 및 개발 방법도 변경되어야 한다. 그림에서와 같이 각 노드는 스마트 계약(smart contract)으로 알고리즘이 구현된다. 이 계약들은 로컬 변수들을 포함할 수 있으나, 노드들 사이에는 블록체인에 저장된 정보만을 공유할 수 있는 제약점이 있다.

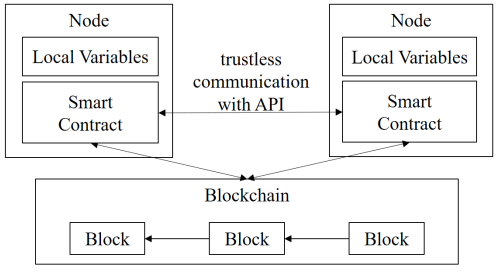



Fig. 4. Blockchain Architecture

Fig. 5는 투표 서비스의 구조를 보여준다. 각 사용자는 자신의 역할에 맞는 dAPP(decentralized Application)을 사용하여 피어 노드에 접근한다. 본 연구에서는 익명성 제공을 위해 각 피어 노드들이 직접 블록체인에 기록하지 않고 마스터 노드 네트워크를 통하여 익명화 과정을 거치고 마스터 노드들이 블록체인에 기록한다.

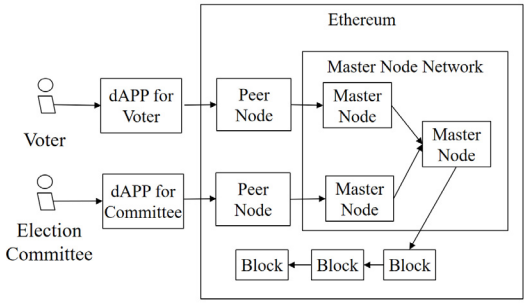



Fig. 5. Service Architecture

알고리즘들은 자율적으로 병행 수행되므로, 모든 노드들의 상태를 동기화시키는 방법이 필요하다. Fig. 6은 BEV 동기화에 필요한 상태 전이도를 보여준다. 이 상태는 블록체인에 기록되어 모든 참여 노드들이 공유할 수 있다. 시작 상태는 Fig. 3의 순차도에서 투표 준비가 완료된 상태를 의미한다. Fig. 6에서 투표 시작 시간이 되면 voting 상태가 되어 투표가 가능하며, 투표 기간이 종료되면 counting 상태로 전이된다. 모든 마스터 노드들의 집계가 완료되면 투표가 completed 상태가 되어 투표 결과를 블록체인을 통해 확인할 수 있다. 즉 모든 상태는 블록체인을 통해 동기화된다.

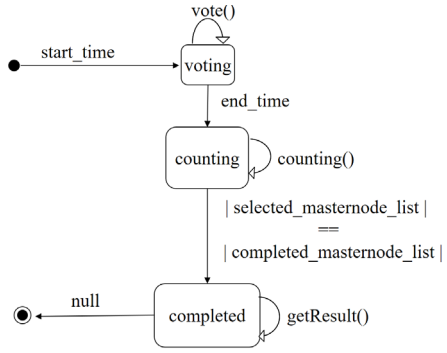


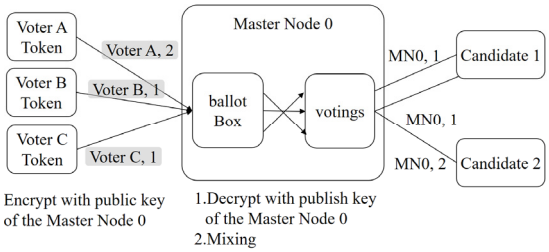

Fig. 6. State Transition Diagram

## 3. 핵심 설계 이슈와 해결 방안

BEV는 탈중앙화 투표 서비스로 다음과 같은 여러 가지 설계 문제들을 해결해야 한다. 해결 방안을 기술하기 위해 그림에서 표현되는 알고리즘들은 간결성을 위해 파이썬 스타일로 표현하였고, 개발 환경은 이더리움의 솔리더티[16]를 가정하였다.

### a. 트랜잭션 암호화와 믹싱

가장 기본적인 익명성 확보는 투표 정보에 대한 암호화다. Fig. 7과 같이 투표자가 마스터 노드만 알아 볼 수 있도록 마스터 노드의 공개키를 이용하여 암호화 하여 익명성을 향상시킨다. 마스터 노드는 투표 정보를 내부에서만 처리한다. 마스터 노드 내부의 투표함(ballot_box)에는 지금까지 도착한 투표용지들이 저장되어 있으며, 집계 상태가 되면 이를 믹싱하여 votings로 이동시키고 다음 처리를 수행한다.




```
1. contract Voter:
2.     def vote():
3.         transaction.receiver = getSelectedCandidateFromUI()
4.         transaction.amount = 1
5.         masternode = selectMasterNode(this)
6.         EnData = Encrypt(transaction, masternode.publicKey)
7.         masternode.ballot_box.append(EnData)
```

Fig. 7. Transaction Encryption

### b. 부하 균형

투표자가 믹싱을 위임할 마스터 노드를 선택해야 한다. 동기화 없이 마스터 노드를 자율적으로 선택하게 되면 특정 마스터 노드들이 집중적으로 선택되는 부하 균형(Load Balancing) 문제가 발생할 수 있다. 따라서 자신의 마스터 노드를 선택하는 selectMasterNode(voter) 함수에서 부하 균형을 고려해야 한다.

Fig. 8은 부하 균형을 위한 알고리즘을 보여준다. 대시코인에서는 마스터 노드들을 순서대로 나열해 주는 determisticOrdering()과 각 마스터 노드들의 가상의 결정적 랜덤 값(Pseudo deterministic random value)을 구하는 CalculateScore()를 제공한다. 이를 사용하면 각 노드들이 탈중앙화 시스템에서 특별한 동기화 작업이 없이 마스터 노드들의 순서를 공유할 수 있다.

마스터 노드들의 순서가 결정되면 부하 균형을 위해 각 투표자가 마스터 노드를 부하 균형을 이루면서 선택할 수 있다. 랜덤 함수의 특성상 확률적으로 충돌 문제가 일부 발생할 수 있으므로 length = |eligible voter list| / no_vote_slots * 1.2 와 같이 충분한 마스터 노드들을 확보해야 하며, 그래도 충돌이 발생하면 선택된 마스터 노드에 인접해 있는 믹싱에 대한 여유가 있는 마스터 노드를 선택한다.

```
1.  library BEV_library:
2.  def selectMasterNode(voter) {
3.    master_nodes = determisticOrdering()
4.    index = uniformRandom(voter.hash) mod | selected_masternode_list |
5.    selected = selected_master_node_list[index]
6.    if | selected.votings | == no_vote_slots + 1:
7.      selected = nearest of selected masternode with empty slot
8.    return selected
9.
10. def determisticOrdering():
11.   sorted_master_nodes = []
12.   scores = []
13.   for(masternode in selected_masternode_list):
14.   n = CalculateScore(masternode);
15.   if(n > best_score):
16.     best_score = n;
17.     sorted_master_nodes.append(masternode);
18.  return sorted_master_nodes
19.
20. def CalculateScore(masternode){
21.   n1 = GetHash(masternode+ current_mixing);
22.   n2 = Hash(n1); //hash the POW hash to increase the entropy
23.   return = abs(n2 - masternode_vin);
```

Fig. 8. Deterministic Ordering of Master nodes

### c. 편중된 투표

Fig. 9와 같이 한 단계의 마스터 노드만을 거치고, 투표의 결과가 편중되는 경우 익명성이 훼손될 수 있다. 이를 해결하기 위해 Fig. 10과 같이 여러 단계의 마스터 노드들을 통과하게 하여 보다 향상된 익명성을 확보할 수 있다. 이를 체인 믹싱(chain mixing)이라고 한다. 얼마나 많은 단계를 거쳐야 충분한 익명성을 확보할 수 있는가에 대해서는 논의단계에 설명한다. 체인 믹싱의 경우 다음 단계로 연결되는 과정에서도 부하 균형을 고려해야 하는데, 이 경우에도 Fig. 8에서 설명한 부하 균형 알고리즘을 다시 사용하여 해결한다. Fig. 8의 알고리즘의 라인 21처럼 +current_mixing을 추가하면 아발란체 효과(Avalanche effect)에 의하여 각 단계별로 랜덤하게 마스터 노드가 선택된다.

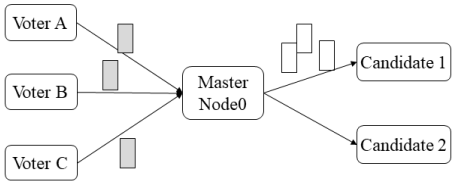



Fig. 9. Skewed Voting

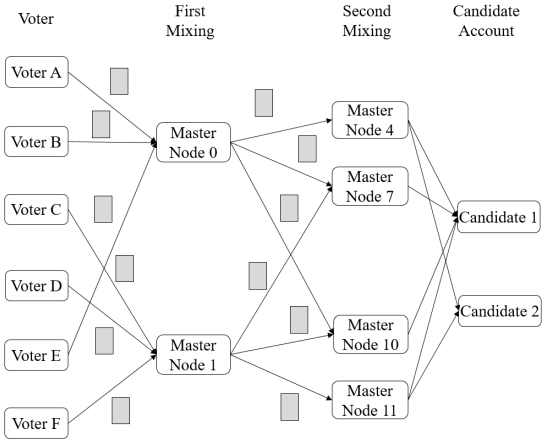



Fig. 10. Chain Mixing

### d. 집계 단계의 동기화

투표가 종료되면 집계 단계가 시작된다. 체인 믹싱에서 모든 마스터 노드들이 1차 믹싱을 완료했다는 정보가 공유되어야 다음 단계인 2차 믹싱을 수행할 수 있다. 따라서 각 단계가 완료되었다는 사실을 모든 선택된 마스터 노드들 사이에서 동기화할 필요가 있다. 이를 위해 Fig. 11의 알고리즘과 같이 각 마스터 노드들은 자신이 믹싱을 완료했다는 사실을 블록체인에 기록한다. 기록된 정보의 수가 확보된 마스터 노드들의 수가 되면 모든 노드들은 해당 단계를 완료했다고 판단할 수 있다. 라인 4-7은 집계 단계에서 부하 균형이 완벽할 수 없기 때문에 마스터 노드에 no_vote_slots 보다 투표용지가 적게 오는 경우가 발생될 수 있다. 이 경우 익명성 향상을 위해 0개의 토큰을 전송하는 트랜잭션을 추가한다.

Fig. 12는 블록체인에 저장되는 핵심 정보들의 구조를 보여준다. 블록체인에는 확보된 마스터 노드들의 목록을 유지하고 있으며, 하나의 선거에 대하여 하나의 ':Election'을 생성한다. :로 시작되는 식별자는 UML에서 익명의 객체를 의미한다. 따라서 여러 번의 선거가 진행되면 여러 개의 ':Election'들이 기록된다. 하나의 ':Election'은 해당 투표가 시작되기 전에 선거관리 위원회에서 필요한 값들을 결정하여 블록체인에 기록한다.

```
1. def counting():
2.   if cur_state != counting return
3.   for (i=0; i< |vote_slots |; i++):
4.     if i< | ballot_box |:
5.         votings.append(decrypt(ballot_box[i]))
6.     else:
7.         votings.append(generateFakeVote())
8.   votings.randomShuffling()
9.   master_node= selectMasterNode(this)
10.  EnData = Encrypt(transaction, master_node.publicKey)
11.  master_node.ballot_box.append(EnData)
```

Fig. 11. Counting Step Synchronization

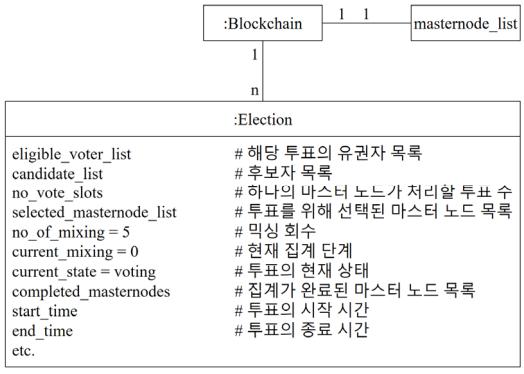



Fig. 12. Information Schema recorded in the Blockchain

## 4. 논의

신뢰가 없는 참여자들 사이에서 보상 시스템은 참여 동기를 유발시켜 생태계를 유지 발전시키는 블록체인의 본질적인 특성이다. 본 연구는 투표를 위한 것이므로 투표의 생태계 유지를 위해 각 참여자의 책임과 보상 요소를 고려해야 한다. 투표 시스템의 참여자는 투표자와 선거위원회 그리고 마스터 노드가 있다. 투표자는 권리를 행사하기 위해 투표권을 제공받고 세금 또는 회비를 선거위원회에 제공해야 하는 의무가 있다. 선거관리위원회는 투표 진행을 위한 대부분의 권한을 갖고 있으며 작업을 공정하고 안전하게 이루어지게 하도록 해야 하는 의무가 있다. 마스터 노드는 지속적인 금전적 보상을 받기 위해 컴퓨팅 자원을 제공한다. 선거관리위원회가 선거의 원활한 진행을 위해 마스터 노드들에게 비용을 지불하여 생태계가 유지될 수 있게 된다.

Eq. (1)은 체인 믹싱의 단계를 증가시킬 때 익명성이 어떻게 강화되는 가를 보여주고 있다. 믹싱 단계를 증가

시킬 때마다 익명성은 기하급수적으로 증가하므로 저렴한 비용으로 익명성을 충분히 증가시킬 수 있다.

$$n = S^m$$

where $n$ is the number of voters for backtracking, (1)
$s$ is the size of the voting slot,
$m$ is the number of mixing steps

Eq. (2)는 익명성을 추가로 제공하기 위해 필요한 체인 믹싱 수행 시간을 분석한 것이다. 수식에서 $s$와 $m$은 각 선거마다 결정되는 상수이므로 집계단계의 계산시간은 투표자 수에 선형적으로 증가하여 큰 문제가 없음을 보여준다.

$$O\left(\frac{v}{s} * m\right) = O(v) \quad (2)$$

where $v$ is the number of voters,
s is the size of voting slot,
$m$ is the number of mixing steps

블록체인 서비스를 개발하기 위해 사전에 공개형 블록체인(public blockchain)과 폐쇄형 블록체인(private blockchain) 중 하나를 선택해야 한다. 폐쇄형은 사용자 관리와 외부 공격 방어에 장점이 있으나 운영 규모가 작아 보상이 적으므로 블록체인 생태계의 구축하고 운영하기 위해 감당하기 어려운 비용이 요구될 수 있다. 또한 규모가 작아 내부 공격인 비잔틴결함허용 문제에서 취약하다. 따라서 이더리움과 같은 공개형 블록체인을 사용하는 것이 바람직하다고 판단된다.

대시 코인에서는 코인조인에서 발생하는 다음과 같은 다양한 익명성 공격들을 대비하여 몇 가지 기능을 개선시켰다. 첫 번째 문제는 합계 금액에 의한 코인 조인의 추적(Tracing Coinjoin By Amounts)이다. 특정 수신 금액의 조합으로 송금자와 수신자와의 관계를 유추할 수 있는 공격이다. 두 번째 문제는 순방향 연결 공격(Forward Linking attack)이다. 비트코인에서는 UXTO(Unspent Transaction Output)를 사용한다. 트랜잭션에서 송신자가 사용하고 남은 잔금을 트랜잭션 이후에 사용하는 순간 이전에 사용했던 트랜잭션들의 잔액을 확인하여 송신자를 특정할 수 있다. 세 번째는 잔금 연결 공격(Through Change Linking)이다. UXTO로 분리된 금액들을 결합하여 사용하는 경우에도 비익명화 공격이 발생한다. 위 세 가지 공격은 모두 잔금을 추적하는 방법이다. 투표는 잔금이 없으므로 위의 세 가지 역추적 공격을 모두 예방할 수 있다.

Table 1은 기존 방법들과의 특징에 대한 비교표이다. 기존의 BEV는 참여자의 보상에 대한 고려가 부족하다. 투표 정보의 저장은 D-CENT의 경우에만 데이터베이스에 저장된다. 블록체인에 저장되는 경우 선거관리위원회를 신뢰하지 않는 경우에도 사용될 수 있다. 기존 BEV의 경우 모든 정보가 노출되므로 익명성을 제공할 수 없다. 그러나 D-CENT의 경우에는 선거관리위원회를 신뢰하는 경우에만 익명성을 보장할 수 있는 제약점이 있다. 집계동기화와 부하 균형의 경우에는 익명성 제공을 위한 추가적인 작업으로 기존 방법들에서는 의미가 없다. 성능의 경우 D-CENT보다는 낮지만 투표의 경우 큰 문제가 되지 않는다.

Table 1. Feature Comparison among the Models

| Features | D-CENT | Existing BEV | BEV with Master Node |
|---|---|---|---|
| Rewards of the Participants | Strong | Weak | Strong |
| Voting Information Storage | Database | Blockchain | Blockchain |
| Trust for the Election Committee | Requires | Not Requires | Not Requires |
| Anonymity | Partially Provides | Not Provides | Provides |
| Counting Synchronization | N/A | N/A | Requires |
| Load balancing | | | |
| Transaction Encryption | Provides | Depends on Implementation | Provides |
| Performance | High | Low | Low |

## 5. 결론

투표에 블록체인의 적용은 시민 참여를 촉진시킬 수 있는 매우 중요한 연구 분야이다. 특히 블록체인을 이용한 중소 규모 투표에 있어서 익명성은 매우 중요하다. 따라서 본 연구에서는 투표 시스템을 블록체인으로 구현했던 기존 연구와는 달리 탈중앙화 환경인 블록체인에서 익명성을 어떻게 제공할 것인가에 대하여 연구하였다. 또한 이러한 기술들은 블록체인의 상호신뢰가 없는 환경에서 어떻게 적용한 것인가에 대하여 논의 하였다.

상호신뢰가 없는 탈중앙화 서비스에서 마스터 노드들 역시 리워드를 얻고자 하는 익명의 참여자들로 구성되어 서비스 안정성을 보장하기가 어렵다. 탈중앙화 서비스에서 분산시스템에 준하는 서비스의 안정성을 제공하는 2차 네트워크를 운영하는 방법에 대한 연구가 향후 필요하다.

블록체인 응용분야가 확대될수록 개방형 블록체인에서도 폐쇄형 블록체인의 특성인 허가형 (permissioned)과 같은 중앙화의 특성을 요구된다. 폐쇄형의 경우 규모가 작아 생태계 유지가 어렵기 때문에 개방형에서 폐쇄형 블록체인의 기능을 제공하는 방법도 향후 연구로 필요할 것으로 판단된다.

## References


[1] E. Brajaktari, Citizen engagement in public service delivery. The critical role of public officials, UNDP Global Centre for Public Service Excellence, United Nation, pp 1-20, 2016.

[2] E. Akbari, Q. We, W. Zhao, H. R. Arabnia, "From blockchain to internet-based Voting", *Proceeding of International Conference on Computational Science and Computational Intelligence*, IEEE, USA, Dec. 2017. DOI: https://doi.org/10.1109/CSCI.2017.34

[3] J. Gaber, "Building : A Ladder of Citizen Participation", *Journal of the American Planning Association*, Vol. 85, No. 3, pp.188-201, Jun. 2019. DOI:https://doi.org/10.1080/01944363.2019.1612267

[4] J. H. Jang, What if blockchain technology revolutionized voting, NIA Special Report, NIA(National Information Society Agency), Korea, pp.1-14. 2017.

[5] Y. R. Shu, S. H. Park, D. J. Choi, J. W. Lee, Blockchain security issues and the latest robust blockchain technology, Communications of the Korean Institute of Information Scientists and Engineers, pp.14-18, July 2020.

[6] N. Kshetri, J. Voas, "Blockchain-enabled e-voting," *IEEE Software*, IEEE, USA, Vol. 35, No. 4, pp.95-99, July/August 2018. DOI:https://doi.org/10.1109/MS.2018.2801546

[7] D. Roio, M. Sachy, D-CENT Decentralized Citizens ENgagement Technologies Specific Targeted Research Project Collective Awareness Platforms D5.5 Implementation of digital social currency infrastructure, European Union, pp.1-35, 2015.

[8] Ajuntament de Barcelona, "Decidim Barcelona", https://www.decidim.Barcelona/ (accessed Jan. 13, 2021)

[9] Madrid. "Decide Madrid" https://decide.madrid.es/ (accessed jan. 7, 2021)

[10] Betri "Reykjavik", https://betrireykjavik.is (accessed Fed. 10, 2021)

[11] Helsinki, "Open Knowledge Finland Blog Network". http://decisions.okf.fi/ (accessed Fed. 11. 2021)

[12] R. D. Lee, J. S. Lim, "Electronic Voting Systems Using the Blockchain", *Journal of the Korea Institute of Information and Communication Engineering*, Korea, Vol. 23, No. 1, pp.103-110, 2019.1. DOI:https://doi.org/10.6109/jkiice.2019.23.1.103

[13] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, G. Hjálmtýsson, "Blockchain-based e-voting system", *Proceedings of 11th IEEE International Conference on Cloud Computing*, IEEE, CA, USA, pp.983-986, July 2018. DOI:https://doi.org/10.1109/CLOUD.2018.00151

[14] J. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction", *IEEE Consumer Electronics Magazine*, IEEE, Korea, Vol. 8, No. 5, pp.20-25, September. 2019. DOI:https://doi.org/10.1109/MCE.2019.2923927

[15] E. Duffield, D. Diaz, "Dash: A privacy centric cryptocurrency", http://zioncoins.co.uk/wp-content/uploads/2015/06/Dash-Whitepaper.pdf (accessed Dec. 7, 2020)

[16] M. F. Victor, P. Ruppel, A. Kupper, "A Taxonomy for Distributed Ledger Analytics", *Proceeding of Computer,* IEEE. Vol. 54, No. 2, pp.30-38, Feb. 2021. DOI:https://doi.org/10.1109/MC.2020.3017466



조 재 한(Jae-Han Cho) [정회원]

- 2011년 8월 : 금오공과대학교 컴퓨터공학과 (공학사)
- 2014년 2월 : 금오공과대학교 컴퓨터공학과 (공학석사)
- 2016년 2월 ~ 현재 : 금오공과대학교 컴퓨터공학과 (박사수료)

〈관심분야〉
소프트웨어공학, 웹서비스, 블록체인, 딥러닝

이 이 섭(Lee-Sub Lee) [정회원]

- 1988년 2월 : 서강대학교 수학과 (이학사)
- 1990년 2월 : 서강대학교 전자계산학과 (공학석사)
- 2004년 9월 : 고려대학교 컴퓨터과 (이학박사)
- 2004년 9월 ~ 현재 : 금오공과대학교 컴퓨터공학과 교수

〈관심분야〉
소프트웨어공학, 클라우드 컴퓨팅, 인공지능, 블록체인

최 창 훈(Chang-Hoon Choi) [정회원]

- 1988년 2월 : 명지대학교 전자계산학과 (공학사)
- 1990년 2월 : 서강대학교 전자계산학과 (공학석사)
- 1997년 8월 : 서강대학교 대학원 전자계산학과 (공학박사)
- 1997년 9월 ~ 현재 : 경북대학교 과학기술대학 소프트웨어학과 교수

〈관심분야〉

컴퓨터 시뮬레이션, Data Science, 병렬처리, 블록체인