

블록체인을 연계한 전자투표 시스템의 연구 동향

최승빈, 한동근, 김보성, 배성민, 신병철, 송성민, 장혁수, 박세진(교신저자)

계명대학교 컴퓨터공학전공

csb8226@naver.com, ehdrms001030@naver.com, kimbosung22@naver.com, smin9e@naver.com, sb5811c98@gmail.com, song47166@naver.com, hyeoksu459@naver.com, baksejin@kmu.ac.kr

A Study Trend of Electronic Voting System Linked to Blockchain

Choi Seung Bin, Han Dong Geun, Kim Bo Seung, Bae Seong min, Shin Byung Cheol,

Song Sung Min, Jang Hyeok Su, Park Se Jin

Department of Computer Engineering, Keimyung University

요 약

본 논문은 데이터의 조작을 방지하고 무결성 및 신뢰성을 보장하는 기술인 블록체인 기술을 사용하여 선거에 대해 다양한 제약으로 인한 선거 투표율의 저하 및 선거를 위해 필요한 다양한 비용들을 절감할 수 있는 방법인 전자투표 시스템을 실제 선거에 도입하게 된다면 어떤 효과를 기대할 수 있는지 조사하고, 블록체인을 이용한 전자투표에 관한 연구들이 어떤 방향으로 진행되고 있는지 그 동향을 알아보고 공통점과 차이점을 비교하고자 한다.

I. 서 론

선거의 방식은 현재까지 수기 투표로 진행되고 있었지만, 수기 투표는 여러 가지 제약이 존재한다. 또한 수작업으로 개표 및 집계를 함에 따라 개표 데이터 집계 오류 가능성이 있다는 문제점 또한 존재했다.

동유럽 국가 에스토니아에서는 2007년 세계 최초로 전자투표를 도입했고, 브라질과 파라과이의 대통령 선거도 전자투표 방식으로 치러졌다.[1] 선거방식을 블록체인 기반의 전자투표 방식으로 변경할 시 시간이 부족해 투표를 하지 못했던 사람들에게 대한 투표율 향상을 기대할 수 있고, 투표 개표과정의 간소화로 선거관리비용이 감소할 것으로 기대한다.

본 논문에서는 여러 논문과 자료를 참고, 인용해 블록체인을 연계한 전자투표 시스템 도입 시의 기대효과와 연구동향에 대해 알아보고자 한다.

II. 본론

현재뿐만 아니라 과거에도 투표 방식을 전자투표로 바꾸고자 하는 시도가 존재하였다.[2] 당시 전자투표를 도입했다면 데이터가 중앙 데이터베이스에 저장되는 전자투표를 수행해야 하는데, 이 경우 선거의 4원칙 중 비밀 선거 부분에서 문제가 발생할 수밖에 없는 구조가 만들어진다. 중앙 데이터베이스에 접근 권한이 있는 사람은 유권자가 어느 후보자에게 투표하였는지 데이터베이스에 접근하여 알 수 있고, 수정 권한까지 가지고 있다면 악의를 가지고 유권자의 투표 내용을 변경해 선거 조작이 가능하다는 문제가 발생한다. 이러한 사유로 선거에 전자투표 방식을 도입하기엔 큰 문제점이 존재했다.

그럼에도 불구하고 도입하고자 하는 시도가 존재한 이유는 투표를 제고에 관한 논문에서[3] 투표를 저하에 대한 사유를 알아보기 위해 미투표 유권자들에게 설문지를 진행한 결과 개인정보/출근으로 인해 미투표했다는 응답이 30.6%로 전체 사유 중 가장 높았다. 그리고 해당 연구에서 유권자 연령이 낮을수록 전자투표를 긍정하는 통계가 나왔다. 이를 바탕으로 향후에는 전자투표에 능숙한 인구가 증가할 것이고 투표를 저하 문제를 해결하기 위해 연

령층이 낮은 인구가 중요함에 따라 그들의 입장에서 기회비용을 낮추는데 효과적이라고 생각하는 전자투표 시스템을 도입하고자 한 것이다.

현재에는 블록체인 기술의 등장으로 하나의 데이터베이스에 모든 정보가 집중되는 현상을 막을 수 있기에 전자투표의 도입 가능성이 높아졌다.

블록체인은[4] Peer-to-Peer 네트워크 속에 존재하는 각 노드들이 블록체인의 사본을 가지고 있고, 새 블록이 추가될 때 체인의 무결성을 보장하고 변조를 방지하는 검증 과정을 거친 후 블록을 추가한다. 블록체인은 이 과정을 진행하기 위해 모두가 디지털 장부를 가지며, 모두가 장부를 가지기 때문에 무결성을 보장하며 변조를 막는 장치를 가지는 기술이다.

블록체인을 이용하면 유권자 중 투표에 참여한 인원내에 대해 각자 고유한 식별 번호를 가지는 블록이 생성되고 참여에 대한 데이터를 블록체인에 저장하게 된다. 블록체인은 데이터베이스와 달리 데이터를 중앙에서 임의로 수정할 수 없으므로 데이터베이스 방식의 문제점을 보완해 선거 내용의 변조 문제를 해결할 수 있을 것이다.

[그림 1]은 블록체인 기반 전자투표의 기본적인 구조[5]이다.

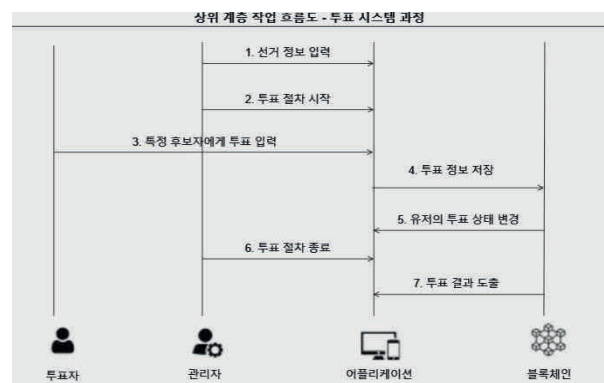


그림 1. 블록체인 기반 전자투표의 구조도

블록체인 기반의 전자투표는 관리자가 투표 정보를 입력한 후 투표를 시작하면 그 시점부터 유권자가 투표를 수행할 수 있다. 원하는 후보자에게 투표를 완

료하면 블록체인의 상에 그 정보를 기록하고, 이 정보를 바탕으로 중복투표를 막는다. 투표가 종료되면 블록체인 정보를 기반으로 집계해 결과를 공개한다.

기본 구조는 무결성을 보장하기 위해 개인정보를 활용한 본인인증을 기반으로 유권자가 투표를 수행해 중복투표를 방지한다. 완료된 투표는 관리자가 블록체인 정보 변경을 막고 재투표를 할 수 없도록 차단해 데이터 변조를 막는다. 최종적으로 본인인증 기반 투표결과를 공개하여 신뢰성을 높여 데이터에 대한 무결성을 보장하는 구조이다.

전자투표에는 보안 요구사항이 추가로 존재하며 요구사항에 대한 논문[6]에 따르면 요구사항에는 완전성(Completeness, 투표내용이 집계에 정확히 반영되어 누락되지 않아야 함), 비밀성(Privacy, 유권자의 투표내용을 제 3자가 알 수 없어야 함), 선거권(Eligibility, 선거하고자 하는 사람이 선거를 할 권리를 가지고 있는지), 이중투표방지(Unreusablilty, 정당한 유권자가 투표를 두 번 하여 1인 1표를 위배하지 않는지), 검증성(Verifiability, 유권자가 한 투표가 집계에 정확히 반영되었는지), 매표방지(Receipt-freeness, 유권자가 다른 사람에게 자신의 투표내용을 알려 팔 수 없게 함)를 지켜야 전자투표가 가능하다.

위 보안 요구사항을 충족시키는 전자투표 시스템을 블록체인 기반으로 구현이 가능한지 검증한 논문[7]에서는 보안 요구사항들을 충족하고 있음을 직접 구현을 통해 증명하고, 블록체인 기술의 사용 시 요구사항을 갖추는 전자투표 시스템의 구현이 가능하다는 점을 알 수 있다.

이에 따라 블록체인 기반 전자투표 시스템 설계 및 구현에 관한 논문에서는[8] 블록체인 기술 중 이더리움 플랫폼을 사용하여 블록체인 기술을 사용한 전자투표 시스템을 직접 구현한다. 이 연구에서는 블록체인 기술을 응용해 가상화폐 전송이 아닌 데이터 전송으로 전송내용물을 변형하여 데이터의 변조를 방지하도록 하는 방식을 기반으로 한다. 여기서 블록체인은 기본적으로 계좌 주소가 블록에 남아 투표자의 투표내용이 타인에게 공개된다는 문제점이 존재하는데, 이를 계좌정보의 암호화를 통해 해결하는 방안을 제시한다. 위 논문의 구현 결과에 따르면 투표의 4원칙을 위배하지 않는 전자투표 시스템을 구축한다.

유사한 방식을 사용한 다른 논문에서는[9] 이더리움을 기반으로 하여 스마트 컨트랙트를 사용하고 보안 요구사항을 충족시키기 위해서 우선 사용자의 정보를 최소화한 후 Firebase로 회원가입 내역 접근을 어렵게 만든다. 그리고 SHA 계열의 해시 알고리즘보다 강한 보안을 제공하는 SHA-3 Keccak 알고리즘을 활용해 사용자의 응답 및 기표내용을 예측하기 어렵게 만들어 입력값의 노출을 방지해 사용자의 익명성을 확보하는 투표시스템을 구현한다.

다른 연구에서는[10] 이전 논문과 동일하게 이더리움 블록체인 기술을 사용하되, 퍼블릭 블록체인과 프라이빗 블록체인을 묶은 하이브리드 블록체인 기술을 채택하여 투표내용의 익명성 문제를 해결하고 하이브리드 블록체인을 이용하기 위한 플랫폼을 제공하는 클라우드 서비스인 BaaS(Blockchain as a Service)를 사용해 투표시스템을 구현하였다. BaaS 시스템으로 사용자 인증 정보를 담는 블록체인과 투표내용을 담는 블록체인을 구분해 익명성과 검증성, 기밀성을 확보하는 투표시스템을 구현한다.

[표 1]은 세 가지 연구에서 제시된 시스템 구조 비교를 위한 표이다.

연구	플랫폼	세부 구현방식	보안방식
[8]	이더리움	Public	계좌정보 암호화
[9]	이더리움	Public	Firebase, SHA-3 Keccak
[10]	이더리움	Hybrid	BaaS

표 1. 연구별 시스템 구현 차이점 비교

연구들의 공통점 및 차이점을 비교 해 보았을 때, 세 연구 모두 이더리움 플랫폼을 채택하였다. 그 중 [8],[9]는 Public 블록체인을 사용하였고 [10]만 Hybrid 블록체인을 사용했다. 보안방식의 구현은 전부 다 다르나 공통

적으로 익명성을 중점적으로 확보하기 위해 각 보안방식을 채택하였다.

III. 결론

전자투표로 변경할 시 투, 개표의 간소화로 인해 선거관리비용 전반이 줄어드는 효과를 얻을 수 있다. 유권자는 전자투표로 변경 시 투표소에 가는 시간을 줄이고 원하는 장소에서 선거에 참여할 수 있어 시, 공간적 제약에서 자유로워질 수 있다. 그리고 블록체인의 기술적 특징을 통해 외부에서 위, 변조가 불가능하다는 특징 덕분에 자신의 투표 내용을 조작할 수 없다는 신뢰를 줄 수 있다.

본 논문에서는 선거의 방식으로 수기 투표를 대신해 블록체인을 연계한 전자투표 시스템 도입 시의 효과와 연구 동향을 알아보았다. 이를 알아보며 과거부터 전자투표를 도입하려 하는 시도와 그 이유 및 전자투표 도입 시 효과를 알 수 있다. 당시에는 중앙집중식 구조 외에는 구현이 불가능하다는 문제점이 존재하였으며, 중앙 데이터베이스에 투표 데이터가 저장될 시 이를 변조할 수 있는 문제가 있었다. 그럼에도 불구하고 연령층이 낮아수록 전자투표를 더 긍정하는 통계 결과가 나와 다양한 방법을 고려한 것으로 보인다.

블록체인 기술의 발달로 변조 문제는 해결할 수 있었으나, 단순히 블록체인의 기본적인 기술만 사용한다면 여전히 블록에 거래를 수행한 계좌 정보가 남기 때문에 비밀투표에 위배되는 문제를 해결할 수 없었다. 이를 해결하기 위해 계좌정보를 암호화하는 방식이나 하이브리드 블록체인 기술을 사용하여 전자투표의 보안 요구사항 보장이 가능함을 확인할 수 있었다.

향후 연구를 통해 선거의 4원칙이나 전자투표의 보안 요구사항을 위배할 수 있는 다양한 예외상황에 대한 방지책 및 대응법을 연구할 필요가 있을 것이다.

ACKNOWLEDGMENT

참 고 문 헌

- [1] 박은주, "전자투표 본격 도입 위한 선행과제는 바로 '보안'", 보안뉴스, 2023. 05. 10, <http://www.boannews.com/media/view.asp?idx=117909>
- [2] 정연정, "전자투표도입의 정치·사회적 쟁점과 발전방안," 한국정당학회보, vol. 4, no. 2, pp. 219-248, 2005.
- [3] 조지훈, "효율적인 투표율 제고방안의 모색 : 전자투표제를 중심으로", 서강대학교 정치학석사 학위논문, 2014
- [4] June Moon, "블록체인이란 무엇인가요? 어떤 원리로 작동하나요?", 2023, (<https://nordvpn.com/ko/blog/blockchain-technology-explained>)
- [5] 김도훈, "블록체인 기반 온라인 투표 시스템 개발," 한국정보과학회 학술발표논문집, pp. 2013-2015, 한국정보과학회, 2023.
- [6] 강서일 and 이임영, "전자 투표 시스템의 보안 기술 및 종이 영수증 동향," 정보보호학회지, vol. 15, no. 5, pp. 40-51, 2005.
- [7] 성기정, 정재린, 조은아, 이종호, 김희영, 김영우, and 이경현, "블록체인 기반 교내 전자투표 시스템," 정보보호학회논문지, vol. 28, no. 4, pp. 779-787, 2018.
- [8] 김세아, 원예중, 이지은, 최병주, "블록체인 기반 전자투표 시스템 설계 및 구현", 2018년 한국컴퓨터종합학술대회 논문집, pp.1931-1932, 2018
- [9] 김현아, 나연주, 이재윤, 정유리, 김형중, "효율성과 투명성을 확보한 블록체인 기반 전자투표 시스템", 한국시물레이션학회 논문지 vol. 30, no. 4, pp. 9-19, 2021.
- [10] 강명조, 김미희, "BaaS를 이용한 하이브리드 블록체인 기반 전자투표 시스템", 정보처리학회논문지. 컴퓨터 및 통신시스템, vol. 12, no. 8, pp. 253-262, 2023