TAEJAE FCI ISSUE BRIEF

영지식 증명 투표는 민주주의를 구원할 수 있을까?

2023.3.14

발제 | 김지혜 국민대학교 전자공학부 교수
정리 | 안솔비 연구원 (태재미래전략연구원)

올해 초 브라질에서는 폭도들이 의회와 대통령궁, 대법원을 점거하는 사태가 벌어졌다. 지난해 치러진 대선에서 루이스 이나시우 룰라 다시우바 대통령이 1.8%포인트의 표 차로 신승을 거두자 패배를 받아들이지 못한 자이르 보우소나루 전 대통령의 극성 지지자들이 벌인 폭력 시위다. 2년 전 미국 의사당 난입 사건의 복사판 같은 이번 폭동은 결국 선거 시스템에 대한 깊은 불신이 원인이었다.

민주적인 권력이양을 위해 선거 시스템에 대한 신뢰는 필수다. 그러나 정치가 극단적으로 분열되며 선거 부정에 대한 음모론이 민주주의를 위협하고 있다. 기술은 선거 시스템에 대한 신뢰를 끌어올리고 훼손된 법치의 기반을 세우는 역할을 할 수 있을까?

올 초 미국 라스베이거스에서 열린 세계 최대의 정보기술 전시회인 CES에서는 “인류가 당면한 문제를 해결할 수 있는 3대 기술 가운데 하나”로 한국 스타트업 ‘지크립토’의 투표 시스템을 꼽았다. 지크립토는 오현옥 한양대 정보시스템학과 교수와 김지혜 국민대 전자공학부 교수가 공동 창업한 블록체인 스타트업으로 영지식 증명(zero Knowledge)에 기반한 블록체인을 투표 시스템 ‘지케이보팅(zkVoting)’’을 개발해 CES 2023에서 최고 혁신상을 수상했다.

태재미래전략연구원에서는 김지혜 교수를 초청해 영지식 증명을 이용한 투표 시스템이 해결할 수 있는 문제와 적용 가능성을 살펴봤다. 영지식 증명은 블록체인을 활용해 자신이 가진 정보의 내용은 공개하지 않지만 자신이 그 정보를 가지고 있다는 사실을 증명할 수 있는 기술이다.

김 교수는 이 기술로 완전한 비밀 투표가 보장되며 투표의 전 과정을 누구나 투명하게 검증할 수 있어 기존 온라인 투표의 한계를 극복할 수 있다고 설명했다. 특히 불필요한 사회적 비용을 줄이는 동시에 다양한 민주적 실험을 용이하게 할 것이라며 새로운 기술에 대한 사회적 신뢰를 확보하는 것을 새로운 투표 시스템의 성패를 가를 중요한 요인으로 꼽았다.

세미나 발제 주요 내용

■ 2023 CES에서는 인류가 당면한 문제를 해결할 수 있는 3대 기술 중 하나로 '블록체인 투표시스템'을 꼽음

○ 투/개표에 대한 불신이 커지며 사회적 혼란이 가중되고 있는 상황에서 불신을 줄일 수 있는 기술적 혁신의 중요성이 대두됨. 2021년 미국, 2023년 브라질에서의 의회 난입 사건을 통해서만 보더라도 사회적 불신의 비용이 감당하기 어려운 수준으로 증가했음을 알 수 있음.

○ 일반 전자투표의 해킹 위험성이나 관리자에 의한 조작을 효과적으로 방지할 수 있는 시스템으로 비용 면에서도 훨씬 더 효율적.

■ 영지식 증명 투표는 '누구나 검증 가능한 블록체인 온라인 비밀 투표 시스템'

○ '영지식 증명(zero knowledge)'이란 정보 공개 없이 '상대가 필요한 정보를 가지고 있다'는 것만 확인하는 기술.

- 투표를 하기 위해 집 주소, 나이, 성별, 주민등록번호 등 신상을 다 공개해야 하는 지금과 달리 '투표할 권리가 있는 유권자'라는 것만 확인하는 셈.

○ 영지식 기술을 도입하면 개인의 프라이버시 보호와 표의 유효성 증명 둘 다 가능

- 현재까지 여러 블록체인 투표시스템이 나왔지만, 공개 블록체인 상에서 투표가 기록되면 비밀 투표가 불가능하고 암호화해서 투표를 저장하면 투표의 정당성을 검증할 수 없다는 문제가 있었음.

○ 'zkVoting'의 특징 : 무결성, 비밀성, 검증성, 부인방지를 모두 지원하는 블록체인 온라인 투표 시스템

〈표 1.〉 기존 블록체인 투표 시스템과 zkVoting 시스템 비교

	기존 블록체인 투표 시스템	지크립토 ZKVOTING 시스템
무결성 (INTEGRITY)	● 폐쇄 블록체인 기반 ● 블록체인 구축, 관리에 대한 위험성, 시간, 유지 비용 증가	● 공개 블록체인 기반 (DAPP 지원 모든 블록체인 가능) ● 클레이튼, 이더리움 등 공개 블록체인 활용 ● 보안성, 유지관리 경제성, 안정성 증대
비밀성 (PRIVACY)	● 제한된 비밀 투표 ● 개표자는 투표자를 알 수 없음 ● 이해관계자만 투·개표 검증 가능	● 비밀 투표: 본인 제외 누구도 투표자 및 투표 내용 모름 ● 매표 금지: 투표 회유 등 투표 내용을 제 3자에게 보여주는 것을 금지 ● 강압 저항: 유권자의 투표 비밀키가 탈취되어도 안전한 투표 가능
검증성 (VERIFIABILITY)	● 투·개표 검증을 위해서 투표 복호화가 필요 ● 제한된 사람만 개표 검증 ● 이해관계자만 투·개표 검증 가능	● 종단간 투표 검증: 전 과정 검증 가능 ● 투표자 검증: 유권자는 본인의 표가 반영되었는지 확인 ● 투표 적합성 검증: 유권자의 유효투표, 이중투표, 복수후보 투표 등 적합성을 모든 사람이 검증 가능
부인방지 (NON-REPUDIATION)	● 대부분의 투표 시스템에서 선관위가 투표(비밀)키를 유권자에게 나눠줌 ● 유권자는 투표 비밀키로 투표 ● 투표 비밀키를 유권자가 만든 것이 아니기 때문에 부인 방지 달성 어려움	● 유권자가 투표 검증키, 투표 비밀키를 직접 생성 ● 투표 검증키를 선관위에 등록 ● 선관위조차 투표 비밀키를 모르기 때문에 대리 투표 불가 ● 부인 방지성 제공

■ **디지털 민주주의로의 전환은 빠르고, 저렴하고, 안전하며, 정확한 투표를 가능하게 함으로 직접민주주의를 실현함**

○ 영지식 기반의 전자투표로 기존 투표시스템을 대체하면 투표에 들어가는 비용이 절감되고, 다양한 투표 형태를 적용하기 용이해짐

○ 현재 DAO에서는 공개투표만 가능하나 영지식 기반 투표를 적용하면 비밀투표가 가능해짐. DAO의 가능성을 소셜DAO나 정치DAO로 확장시킬 수 있음

토론 주요 내용

■ **아무리 기술이 발달하더라도 투·개표 모두 사람이 하는 일이다. zkVoting으로 대리투표나 위임투표를 막을 수 있는 방법이 있는가? 전자투표 시스템은 항상 해킹의 위협이 있는데, 해킹이 진짜 불가능한가?**

○ zkVoting을 이용한 투표에서는 내가 투표한 것을 타인에게 증명할 수 없고, 가짜 키 생성이 가능하기 때문에 매표금지와 강압저항이 모두 가능하다. 가짜 키를 생성해서 투표를 하면 정상적인 표로 접수가 되지 않는데, 본인이 아니면 키의 진위 여부를 알 수가 없다. 즉, 타인이 강압적으로 투표를 하게 하더라도 본인이 가짜 키를 생성해서 투표를 한 '척'할 수 있기 때문에 매표, 강압, 위임 등이 무의미하다.

○ 현재 양자컴퓨팅에도 안전한 영지식 기술을 개발 중이며, zkVoting은 해킹의 위험이 0에 가깝다고 볼 수 있다.

■ **디지털 기술의 발달이 민주주의의 발전으로 이어질 것이라는 기대가 있었지만, 현실은 오히려 갈등을 심화시키는 것 같다. 디지털 기술로 심화된 갈등을 디지털 기술로 해결하는 것이 가능한가?**

○ 물론 그런 측면이 없다고 할 수는 없지만 기술과 사회는 같이 진화하며, 기술의 발전으로 분명히 국민의 관심이나 전반적인 사회의 투명도 측면에서 나아진 면이 있다. 새로운 것을 도입하는 데에는 늘 두려움이 따르고 기술이 주는 유익을 경험하기 전에는 저항이 있기 마련이다. 사람들을 기술로 설득하는 것은 쉽지 않다. '이 시스템은 신뢰할 만하다'고 사람들을 설득하여 사회적 신뢰를 확보하는 것이 성패를 가를 관건이라고 본다.

■ **직접민주주의는 포퓰리즘으로 흐를 위험이 있는데, 전자투표 시스템 도입으로 무조건 직접민주주의를 확대하는 것이 바람직한가?**

○ 꼭 정치적 영역이 아니더라도 전자투표 시스템이 활용될 수 있는 영역은 다양하다. TV 오디션 투표부터 지역 단위의 간단한 행정적 결정은 오히려 직접민주주의가 긍정적인 영향을 끼칠 수 있는 부분이다. 물론 직접민주주의가 내포하는 포퓰리즘의 위험성을 줄이고, 신속한 '민의(民意)' 반영의 긍정적 측면을 극대화하기 위해서는 정교한 설계와 논의가 필요하다.