분산원장기술 기반의 온라인투표에 관한 보안 위협, 국제 표준화 시작

박근덕 서울외대 AI블록체인연구소 부소장(jacepark926@gmail.com)

본고에서는 분산원장기술(DLT, Distributed Ledger Technology)을 활용한 온라인투표에 관한 보안 위협(ITU-T X.stov)에 대한 국제 표준안[1] 내용을 기반으로 정보통신 인프라 환경에서 운영되는 온라인 투표시스템의 보안 위협과 대응 방안을 소개하고자 한다.

DLT를 활용한 온라인투표는 많은 국가에서 DLT를 활용한 비금융 서비스 분야의 성공적인 사례 중 하나이지만, 정보통신 인프라를 기반으로 하고 있는 온라인 투표 과정에서 발생할 수 있는 잠재적인 보안 위협에 대한 분석은 매우 미흡한 실정이다. 최근 몇 년 동안 정보통신 인프라 기반의 다양한 애플리케이션과 서비스는 개인정보 등 중요 정보 유출 및 서비스 중단 등의 보안사고로 인해 사회적·경제적으로 막대한 비용을 치룬 경험이 있다. 특히 최근에는 가상 화폐 거래소의 보안사고(가상 화폐 탈취, 개인정보 유출 등)가 끊임없이 발생하고 있다. 또한 기업 내 중요한 정보를 볼모로 금전적 보상을 요구하는 랜섬웨어(예: 워너크라이, 페트야 등)가 기승을 부리고 있어 최신 기술과 관련된 보안 사고에 대한 대응 방안이 절실히 필요하다. 따라서 본 ITU-T 국제 표준안에서는 전 세계 주요 국가의 DLT를 활용한 온라인투표 이용 사례를 설명하고 DLT를 활용한 온라인투표 시스템의 모델을 제시한다. 그리고 온라인투표 모델에 근거한 투표 과정에서 발생할 수 있는 보안 위협을 식별하고 대응 방안에 관한 표준을 개발한다.

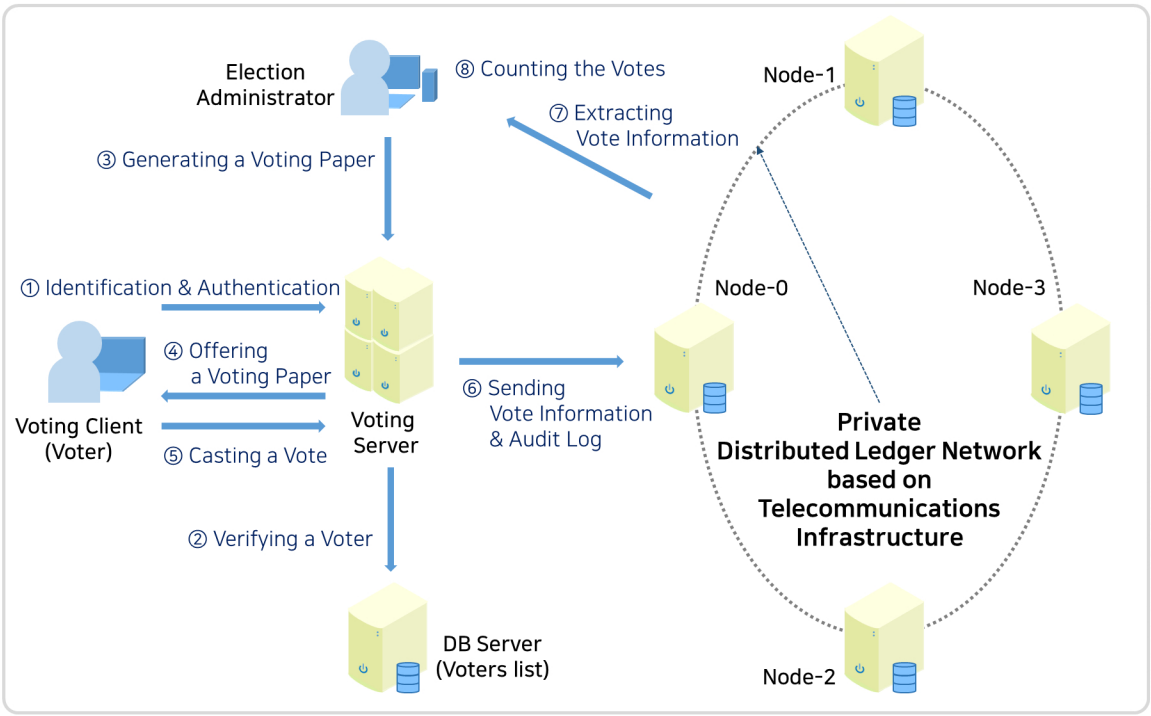
최근 전 세계 주요 국가(덴마크, 에스토니아, 한국, 스페인, 우크라이나, 미국 등)에서는 DLT를 활용한 온라인투표를 정치적인 정당 내 의사 결정, 지방자치단체 주민에 의한 사업 결정, 주식 시장에서 대리자 투표, 대통령 후보 선출 등에 적극적으로 이용하고 있다.(<표 1> 참조)

<표 1> 분산원장기술을 활용한 온라인투표 해외 사례

번호	국가	날짜	설명
1	덴마크	2014년 4월	덴마크 자유당(Danish Liberal Alliance) 정당은 코펜하겐 교외비도우레(Hvidovre)에서 열린 연례회의에서 내부 투표를 위해 블록체인기술을 사용함
2	에스토니아	2017년 1월	나스닥은 에스토니아 탈린 증권 거래소에서 프록시 투표를 실행하기 위해 블록체인기술을 사용하여 테스트를 성공적으로 마쳤고, 이 기술을 통해 투자자는 투자자 회의 중 온라인 투표를 하거나 투표권을 대리인에게 이전 할 수 있음
3	대한민국	2017년 2월	경기도는 블록체인기술을 기반으로 한 투표 시스템을 사용하여 주민들의 지역 사회 사업에 대한 투표를 실시함. 투표가 성공적으로 완료되었으며 9,000여 명의 주민들이 온라인과 오프라인 투표에 참여하였음
4	스페인	2014년 이래	포데모스(Podemos) 정당은 내부 선거를 위해 블록체인기술을 사용하는 아고라(Agora) 투표를 사용하였음
5	우크라이나	2016년 2월	우크라이나와 미국에 기반을 둔 블록체인 업체들은 전자투표시스템(e-Vox)을 개발하기 위한 각서에 서명하였고, 크리에이터는 분산원장기술이 사기를 방지하고 선거를 보다 투명하게 만들 것이라고 주장함
6	미국	2016년 3월	유타주 공화당은 대선 후보자 선정을 위해 블록체인 기반의 온라인 투표시스템 사용함
		2016년 4월 8일~10일	텍사스주 자유당은 블록체인 기반 투표시스템 사용함

1) 한국이 주도하고 있는 본 국제 표준안(ITU-T X.stov)은 2017년 9월 ITU-T SG17 회의에서 신규 워크 아이템으로 채택되어 2020년 3월까지 국제 표준을 개발할 예정임

본 표준안에서 제시하는 DLT를 활용한 온라인투표시스템 모델의 주요 구성 요소는 투표 클라이언트(투표자), 선거 관리 클라이언트(선거 관리자), 투표 서버, 선거인 명부 서버, 비공개형 분산 원장 네트워크[노드(원장 서버), 데이터베이스, 합의 프로토콜 등)] 등 이다.([그림 1] 참조)



[그림 1] 분산원장기술을 활용한 온라인투표시스템 모델

본 표준안에서는 DLT를 활용한 온라인투표 모델에 근거한 온라인투표 과정에서 발생할 수 있는 잠재적인 보안 위협을 정보보호 측면에서 크게 5가지 범주로 분류하여 식별한다.

- 데이터 기밀성에 대한 위협
- 데이터 무결성에 대한 위협
- 서비스 가용성에 대한 위협
- 정보시스템에 대한 비인가된 접근
- 악의적인 행동

2018년 하반기 라포처 미팅(RGM)에서 일본에서 제안한 보안 위협 재분류에 관한 내용을 검토할 예정이고, 영국에서 제안한 온라인투표 활용사례에 관한 부록(Appendix)을 추가할 예정이다. 또한 과기정통부에서 최근 발주한 '온라인투표 시스템 시범사업(투명한 전자투표시스템, 중앙선거관리위원회)'을 통하여 개발 예정인 온라인투표 시스템을 국제 표준에 적극 반영할 예정이다.

향후 DLT를 활용한 온라인투표 서비스를 구축·운영할 경우 이해 당사자(서비스 제공자, 투표자, 선거 관리자 등)는 본 ITU-T 국제 표준안에서 제시한 보안 위협과 대응 방안을 고려함으로써 최신 기술에 의한 보안 사고를 예방할 수 있다.