BLOCKO

Blockchain Report
BLOCK-SHOT
November, 2020

특허 청구항으로 알아보는 미 우정국(United States Postal Service, USPS)의 블록체인 투표

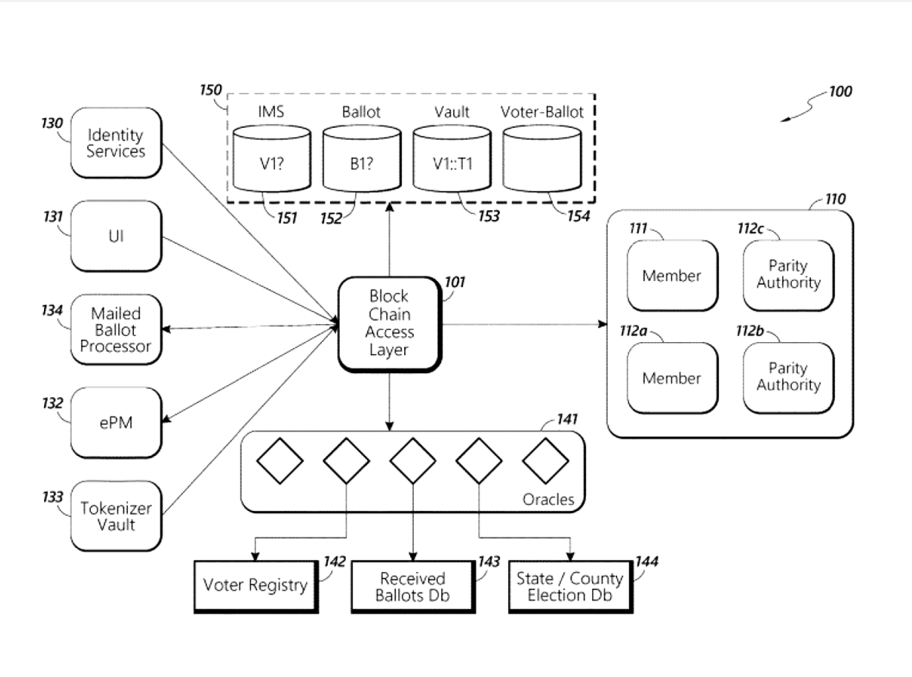
Copyright © 2020 BLOCKO. All rights reserved.

지난 11월 3일 시작돼 아직까지도 개표가 모두 끝나지 않은 미 대선. 민주당 조 바이든이 총 306석을 확보, 당선인으로 선언됐음에도 불구하고 트럼프 대통령은 선거 결과를 '사기(Fraud)'라며 불복하고 있다. 이에 미 국토안보부 산하 사이버안보·인프라안보국(CISA)을 비롯해 선거 안보를 담당하는 정부 기구들이 "이번 선거는 미국 역사상 가장 안전한 선거였다"는 성명을 발표하는 등 이번 대선 결과를 둘러싼 잡음은 끊이질 않는다. 이런 와중에 블록체인 기술을 도입해 논란이 된 부재자/우편 투표의 신뢰도를 높여야 한다는 목소리 역시 관심을 받고 있다.

미 우정국은 지난 2월 이미 투표에 블록체인을 적용하는 특허를 신청했다. "블록체인과 우편의 보안성을 활용해 신뢰성 갖춘 투표 시스템(A voting system can use the security of blockchain and the mail to provide a reliable voting system)" 구축이 가능하다는 내용의 '보안 투표 시스템(Secure Voting System)' 특허를 출원한 것. 명세서에는 투표인 등록부터 우편 투표 용지(ballot) 발송, 선거 결과 블록체인 저장, 스마트컨트랙트 기반 데이터 검증 등 선거 전반이 단계별로 세분화돼 청구됐다. 이번 리포트에서는 미 우정국의 특허 명세서에서 언급된 블록체인 기술과, 이를 기반으로 구성된 보안 투표 시스템에 대해서 알아보고자 한다. (특허 청구항은 대괄호로 표기하였다.)

Copyright © 2020 BLOCKO. All rights reserved.

[도식 1] 블록체인 기반 우편 투표의 시스템 구성도 예시(USPS)



(출처-United States Postal Service)

[0047] 도식 1은 블록체인 기반 우편 투표의 시스템 구성도의 예시이다. 시스템 아키텍처(100)에는 블록체인 엑세스 레이어(101)가 포함돼 있으며, 해당 레이어는 다양한 시스템 구성요소를 블록체인과 연동하고 비(非)블록체인 기능을 역시 관리하는 역할을 담당한다. 블록체인 엑세스 레이어는 각각의 블록체인 레이어 소프트웨어와 서버간 부하를 조절하는 로드 밸런서를 구동하는 여러 서버로 구성될 수도 있다...

[0048] ...블록체인은 접근이 쉽고, 위변조가 불가능한 방식으로 투표 행위 전반을 기록할 수 있기에 투표자, 선거 관계자, 선거 감사관 *auditor*을 비롯해 공인된 이해관계자 모두 투표 결과를 확인하고 검증하는데 활용될 수 있다.

[0049] ...이더리움 오픈 소프트웨어 플랫폼 혹은 유사한 다른 플랫폼에 기반한 블록체인이 활용될 수 있다. 해당 플랫폼은 튜링 완전한 *Turing complete* 블록체인

Copyright © 2020 BLOCKO. All rights reserved.

프로토콜을 포함한다. 블록체인 엑세스 레이어는 특정 조건이 달성되면 데이터를 블록체인에 기록하는 소프트웨어 컨트랙트(스마트 컨트랙트)를 활용한다...

[0050] 블록체인 엑세스 레이어(101)는 블록체인과 직접 연동이 가능한 구성 요소(110)와 유무선 통신을 통해 연결된다. 구성 요소(110)은 블록체인 엑세스 레이어와 소프트웨어 API 형태로 연동될 수 있다. 멤버(111)는 인증된 트랜잭션을 블록체인에 기록하는, 혹은 데이터를 원장 *ledger*에 기록하는 커미터 *committer* 역할을 담당하며, 각각의 멤버 소프트웨어와 로드밸런서를 구동하는 여러 서버로 구성될 수 있다. 해당 원장은 멤버 노드와 패리티 *parity* 노드간 분산돼 구성될 수 있다. 각각의 노드는 선거구 *election precincts* 혹은 선거 시스템이 관리/운영할 수 있다. 블록체인 원장은 공개적으로 분산되지 않고, 행정구역 단위의 선거 관리기관 간에만 분산 구축될 수도 있다.

[0051] 패리티 기관 *parity authorities*(112a-c)는 블록에 기록된 트랜잭션을 검증하는 역할을 담당한다. 패리티 기관은 권위 증명 *Proof of Authority(PoA)* 합의 알고리즘을 위해 활용될 수 있다. 권위 증명은 채굴자 *miner* 대신 관계 기관의 기관 노드 혹은 벨리데이터 *validator* 가 검증 및 블록 생성을 담당하는 방식이다. 라운드-로빈 *round-robin* 구조에 기반해 각각의 기관 노드는 새 노드를 생성하고 서명할 수 있는 타임 슬랏을 배정받는다. 최소한 5개의 기관 노드가 관계 기관에 분산되며, 각각의 기관은 하나 이상의 노드를 운영할 수 있다.

[0053] 신분 증명 서비스(130)은 투표자의 신분을 확인하고, 투표자의 시스템 등록 여부와 등록된 선거구에 해당하는 투표지 *ballot* 발급 여부를 확인한다. 투표자는 유저 인터페이스(131)를 통해 신분 정보나 신분증 등 관련 자료를 제출할 수 있다.

[0055] 신분 증명 서비스는 접수된 자료를 FBI, 신용평가사, 사회보장국, 차량국 사무소 등 신분 증명이 가능한 기관에 제출한다. 자료가 승인되면 신분 증명 서비스는 해당 투표자의 고유 투표자ID, 퍼블릭/프라이빗 키 쌍을 생성하고 저장한 뒤 해당 투표자에게 알린다. 관련 데이터는 JSON 데이터 구조 형태로 저장될 수 있다.

[0056] 전자 소인 *electronic postmark(ePM)* 시스템(132)은 우편으로 송부된 실물 투표 용지에 인쇄된 바코드 혹은 컴퓨터가 인식가능한 고유키를 생성하고

Copyright © 2020 BLOCKO. All rights reserved.

인증한다. 해당 바코드 혹은 고유키를 통해 전자 투표 및 투표자 확인이 가능하다.

[0057] 토크나이저 볼트(133)는 개별 투표자의 투표 결과를 토큰화한다. 전자 시스템을 통해 투표권을 행사하기 위해선 모든 투표자는 토크나이저 볼트에서 해당 선거와 연동해 발행한 토큰을 발급받아야 한다. 토큰은 특정 투표자의 전자 소인 *ePM*과 연동될 수 있다. 이를 통해 우편으로 접수된 투표지의 익명성을 유지하는 동시에 블록체인에 해당 투표지를 기록함으로 보안성을 더할 수 있다.

[0059] 토크나이저 볼트는 유사 익명 난독화 토큰 *pseudo-anonymous obfuscation token*을 발행할 수 있다...난독화 토큰은 투표자의 익명ID를 증명할 수 있는 믿을만한 알고리즘을 통해 발행돼야 하며, 해당 익명ID는 키 관리 서비스/키 볼트 *Key Management Service/Key Vault* 에 안전하게 저장된다. 난독화 토큰은 영지식증명 등의 형태로 발급될 수 있으며, 특정 투표자의 전자 소인과 연동될 수 있다.

[0060] 투표지 우편 접수 프로세서 *mailed ballot processor*(134)는 우편으로 접수된 투표지를 분석하고 인증하는 역할을 담당한다. 투표지 우편 접수 프로세서는 투표지에 부착된 바코드 등을 통해 접수된 투표지의 정보를 판별한다. 이를 통해 투표지가 기한 안에 접수됐는지, 어떤 선거구로 투표지가 이송돼야 하는지 등을 확인해 해당 선거구로 투표지가 발송될 수 있도록 한다.

[0062] 오라클 *oracles*(141)은 블록체인 기반 투표 시스템의 외부 시스템/구성 요소로부터 정보를 받아 블록체인 엑세스 레이어에 전송하는 소프트웨어 서비스를 의미한다. 오라클은 블록체인 엑세스 레이어는 API, REST-API, RabbitMQ 형태로 연동될 수 있다. 오라클과 연동될 수 있는 외부 시스템으로는 투표자 목록 *voter registry*(142), 접수 투표지 데이터베이스 *received ballots database*(143), 투표자-투표지 데이터베이스 *voter-ballot database*(154), 지역구 선거 데이터베이스 *jurisdiction election database*(144) 등이 포함된다.

[0063-67] 데이터베이스(150)은 블록체인 엑세스 레이어로 들어온 다양한 정보를 저장한다. 블록체인에 기록되지 않는 모든 정보들이 데이터베이스에

Copyright © 2020 BLOCKO. All rights reserved.

저장되며, 미 우정국 *United States Postal Service*를 비롯한 하나의 기관에서 관리, 운영된다. ▲유저 인터페이스(131)와 신분 증명 서비스(130)을 통해 접수된 투표자의 모든 정보가 저장된 신분 관리 서비스 데이터베이스 *identity management services database*(151) ▲투표지의 고유 정보, 양식 등이 저장된 투표지 데이터베이스 *ballot database*(152) ▲투표자와 해당 투표자의 고유 토큰 정보가 저장돼 선거 참여 가능 여부와 개별 투표자와 연동된 전자 소인 ePM 등이 저장된 보안 데이터베이스인 볼트 데이터베이스 *vault database*(153) ▲투표자가 모바일 앱, 웹사이트, 우편 또는 투표장의 선거 기기를 통해 제출한 투표지 및 투표자 정보가 기록돼 중복투표 등을 검증하는 투표자-투표지 데이터베이스 *voter-ballot database*(154)로 구성된다.

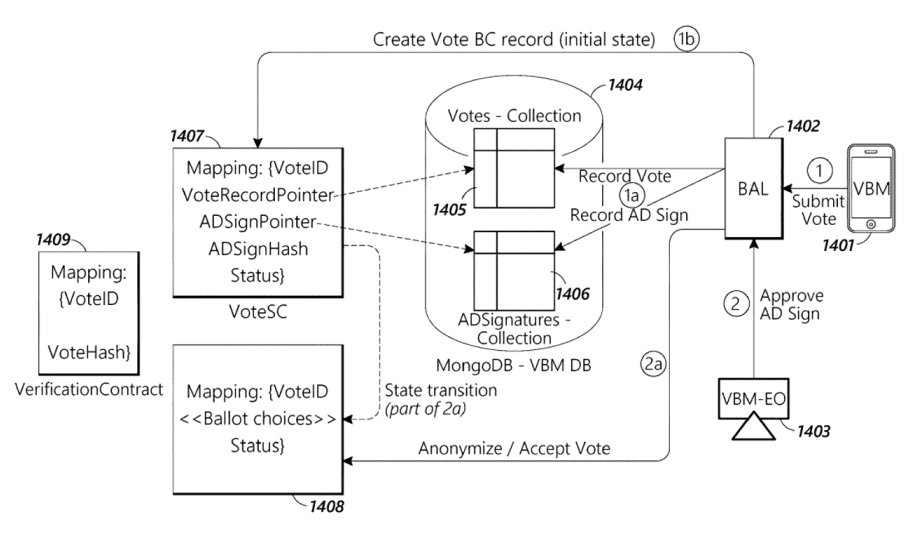
도식 1을 통해 본 미 우정국의 보안 투표 시스템은 퍼블릭 블록체인 혹은 (선거 관리 기관들에 분산 운영되는)프라이빗 블록체인에 기반해 투표 데이터를 기록하고 검증하며,

① 블록체인에 선거 결과를 기록하고 검증하는 노드 부(110),
② 신분 정보, 우편 처리 내역, 고유 토큰 및 전자 소인ePM 등을 발급하는 외부 시스템 부(130~133),
③ 오라클을 통해 데이터를 전송하는 외부 데이터베이스 부(141~144),
④ 투표자, 투표지, 신분 정보, 고유 토큰 등 투표와 연관된 각종 정보를 저장하며 하나의 기관이 관리 및 유지하는 보안 데이터베이스 부(150)

로 구성돼 있음을 알 수 있다.

Copyright © 2020 BLOCKO. All rights reserved.

[도식 14] 투표 결과 블록체인 기록(USPS)



(출처-United States Postal Service)

그렇다면 투표자들이 다양한 방법으로 제출한 투표 결과는 블록체인에 어떤 식으로 기록되는지 도식 14를 통해 알아보자.

[0118] 도식 14는 투표를 블록체인에 안전하게 기록하는 시스템을 나타낸다. 투표자는 태블릿이나 스마트폰, 개인PC를 비롯한 기타 컴퓨팅 기기를 통해 어플리케이션(1401)을 실행할 수 있다. 어플리케이션은 도식1에 묘사된 유저 인터페이스(131)과 동일한 목적을 지닌다. 해당 어플리케이션의 명칭은 "우편 투표 Vote By Mail, VBM." 투표자는 투표에 앞서 선거 관리기구를 통해 등록 후 VBM 어플리케이션을 다운받을 수 있다. 등록 과정에서 자필 서명 이미지 등 투표자의 서명이 전자적으로 저장되며, 선거 관리기관은 해당 서명을 통해 추후 투표지 및 투표자 인증에 활용한다. 투표자가 적법한 투표 기관에 성공적으로 등록되면 투표지 엑세스 토큰 *ballot access token* 등의 인증키를 받는다. 엑세스 토큰은 VBM 어플리케이션이나 해당 투표자에게 전송된 종이 서류를 통해 수령할 수 있으며, 해당 토큰을 통해 데이터베이스에 저장된 투표지에 접근할 수 있다. 엑세스 토큰은 각각의 투표자에게 개별적으로 발행되고 12자리 알파벳+

Copyright © 2020 BLOCKO. All rights reserved.

숫자+특수문자 조합의 형태나 VBM 어플리케이션을 통해 스캔이 가능한 QR 코드의 형태로 전달된다. 엑세스 토큰은 선거 중 단 한번만 사용할 수 있다.

[0119] VBM 어플리케이션이 설치된 후 투표자는 2차 바코드나 QR코드 등의 컴퓨터가 인식 가능한 코드를 수령하며, 해당 코드를 통해 특정 선거에 투표권을 행사할 수 있다. 코드에는BallotID, ElectionID, VoterID가 포함된다. VoterID는 투표자의 고유키값을, BallotID와 ElectionID는 투표자가 참여하게 될 선거와 투표권에 해당하는 키값을 나타낸다.

[0120-0122] 어플리케이션에 표시된 투표지 기록 후, 투표자의 물리 서명 저장을 위해 스타일러스나 손가락으로 작성된 디지털 서명을 하는 단계를 거친다. 투표지 기록이 끝나면 어플리케이션은 투표 결과를 블록체인 추상화 레이어 *Blockchain Abstraction Layer, BAL* (1402)혹은 블록체인 엑세스 레이어에 해당 값을 전달한다. 여기에서 ElectionID, BallotID, VoterID와 투표 결과는 각각 다른 시스템으로 전달된다...투표 데이터베이스 *voting databases*(1404)는 투표 결과 데이터베이스 *votes database*(1405)와 서명 데이터베이스 *signature database*(1406)로 이루어져 있다. 블록체인 추상화 레이어는 실제 투표결과를 투표 결과 데이터베이스로(1405), 투표자 신분 정보와 디지털 서명, VoterID값을 서명 데이터베이스(1406)으로 전송(도식 14의 1a)한다. 이러한 구분을 통해 투표의 익명성을 확보할 수 있다. 두 데이터베이스에 저장된 결과값은 언바운드 키 쌍 *unbound key pair* 기반으로 암호화돼 보안성을 높일 수 있다.

[0123] 블록체인 추상화 레이어는 투표 데이터베이스(1404)에 기록 entry을 추가하는 동시에 제출 투표 블록체인 *submitted vote blockchain*(1407)에도 기록을 추가(도식 14의 1b)한다. 블록체인 추상화 레이어는 제출된 투표지의 고유 voteID, 투표 결과 데이터베이스(1405)에 기록된 투표 결과에 상응하는 포인터 *VoteRecordPointer*, 서명 데이터베이스(1406)의 서명 값에 상응하는 포인터 *ADSign Pointer*, 투표자 디지털 서명의 해쉬값 *ADSign Hash*, 현재 제출된 총 투표 수 *Status*를 생성해 제출 투표 블록체인(1407)에 기록한다.

[0124] 모든 데이터가 투표 데이터베이스(1404)와 제출 투표 블록체인(1407)에 기록되면 블록체인 추상화 레이어는 선거 관리자 어플리케이션 *Election Official,*

Copyright © 2020 BLOCKO. All rights reserved.

VBM EO(1403)을 통해 개별 투표에 대한 완료 서명값을 전송한다. 선거 관리자는 해당 어플리케이션을 통해 투표자 등록 서명과 VBM을 통해 제출된 디지털 서명 ADSign을 비교해 올바른 투표자가 투표권을 행사했는지 검증하며, 승인 결과를 블록체인 추상화 레이어에 전송(도식 14의 2)한다.

[0125] 블록체인 추상화 레이어는 투표자 승인과 동시에, 승인 투표 블록체인 *accepted vote blockchain*(1408)에 기록을 추가한다. 승인 투표 블록체인은 VoteID, 투표지 투표 내역 *ballot choice*, 현재까지 제출된 선거 투표의 집계 내역 *tabulation of all the votes*을 저장한다. 해당 기록이 승인 투표 블록체인(1408)에 추가됨과 동시에, 실제 투표 내역과 투표자의 신분 정보를 연관지을 수 있는 모든 링크가 삭제된다.

도식 14는 투표 결과와 투표자 정보를 개별 데이터베이스에 저장하고, 결과값을 최종적으로 승인 투표 블록체인(1408)에 저장하기까지의 모든 단계가 각기 다른 블록체인에 기록돼 상호 대조가 가능하며 익명성 유지 역시 가능한 시스템을 나타낸다.

Copyright © 2020 BLOCKO. All rights reserved.

마무리

미국에서 우정국은 혁신과 거리가 먼, 최신 기술로 무장한 택배회사와 대비되는 느림보로 인식돼왔다. 이런 기관이 블록체인이라는 새로운 기술과 우편이라는 과거의 기술을 결합한 전자투표 특허를 출원했다는 사실(기술의 진보성을 떠나)에 대해 포브스 등 현지 미디어는 놀람을 표하기도 했다. 공개된 특허 명세서에는 이외에도 검증 스마트컨트랙트를 통한 투표 결과 검증 과정(도식 15)부터 자세한 투표자 등록 및 선거 관리 내용까지 언급돼있다.

한국은 어떨까. 블로코는 지난 2017년 7300여 명이 넘는 인원이 실시간으로 투표에 참여한 경기도 따복공동체지원 사업에 블록체인 기반 투표를 진행했으며, 중앙선거관리위원회는 2018년 온라인 투표에 블록체인 기술을 도입하는 시범 사업을 시작하기도 했다.

* 지난 4월자 블로코의 블록체인 리포트(블록체인 투표, 어디까지 왔나?)에서 다양한 전자 투표 방식과 블록체인 적용 시스템 예시를 확인할 수 있다.

Copyright © 2020 BLOCKO. All rights reserved.

블로코(BLOCKO) 소개

블로코는 2014년 설립된 블록체인 기술 전문 기업입니다. 블록체인 생태계 확장을 위해 한국은행, 한국전자통신연구원, 금융보안원, 금융결제원 등 다양한 국가 기관 및 기업체와 협력하고 있으며, 한국거래소와 신한금융그룹, 현대자동차그룹, 롯데카드, 경기도를 비롯해 국내외 대기업과 금융권, 공공 기관에 블록체인 기반 서비스를 구축한 국내 최대 블록체인 인프라 공급 기업입니다.

Copyright © 2020 BLOCKO. All rights reserved.

BLOCKO

Blockchain Report
BLOCK-SHOT
November, 2020

www.blocko.io
info@blocko.io
82 31 8016 6253

Copyright © 2020 BLOCKO. All rights reserved.