블록체인 방식을 활용한 온라인 투표시스템 적용 가능성 연구

2017

한국인터넷정보학회

2017년도 선거연수원 연구용역보고서

블록체인 방식을 활용한 온라인 투표시스템 적용 가능성 연구

2017.09.29

한국인터넷정보학회

2017년도 선거연수원 연구용역보고서

블록체인 방식을 활용한 온라인 투표시스템 적용 가능성 연구

책 임 연 구 위 원 : 홍 승 필 (성신여자대학교 교수)

공 동 연 구 위 원 : 민 경 식 (한국인터넷진흥원 팀장)

김 혜 리 (성신여자대학교 박사과정)

연 구 기 간 : 2017. 06. 01.~2017. 09. 30.

연 구 단 체 : 한국인터넷정보학회

목 차

표 목 차

그 림 목 차

요 약 문

다양한 장점을 지닌 온라인 투표 시스템이 더 많은 분야에서 널리 활용되기 위해서는 기술적 안정성에 대한 신뢰와 전자투표의 유용성에 대한 공감대가 형성되어야 할 것이다. 특히 전자투표 기술에 대한 “신뢰” 확보는 기존 전자투표 시스템의 보안성 문제를 해결해야 한다. 최근 보안성 강화를 위해서 미래 기술 이슈로 떠오르고 있는 “블록체인” 방식을 투표에 활용하고자 하는 움직임이 대두되고 있다. 따라서 본 연구에서는 선거의 신뢰성과 투명성, 효율성 제고방안으로 블록체인 기술을 온라인 투표 시스템에 도입하기 위한 그 가능성을 타진해 보는 데 그 목적이 있다.

이를 위해서는 우선 블록체인 기술과 온라인투표시스템에 대한 조사, 온라인 선거 사례 및 블록체인 기술을 활용한 온라인 선거 사례조사를 진행하였다. 미국, 스페인, 우크라이나, 에스토니아 등의 블록체인 방식의 온라인투표시스템 활용 사례를 분석하였다. 이를 통해 블록체인 기술을 투표에 적용하면, 투표가 완료된 즉시 결과를 확인할 수 있고, 투표 관리 비용이 획기적으로 줄어들며, 투표를 둘러싼 부정이나 조작 논란을 해소할 수 있음을 확인할 수 있었다. 그러나 아직은 국가 단위의 공직선거 보다는 정책결정과정이나 정당에서 후보를 뽑는 중·소규모의 민간투표에 활용이 가능하다는 결론도 얻을 수 있었다.

국내 사례에서도 블록체인 기술을 온라인 투표 시스템에 도입하기 위해서는 먼저 해결해야 할 과제들이 있음을 확인하였다. 우선, 제도적인 측면에서는 직접 선거의 원칙, 비밀 선거의 원칙, 자유 선거의 원칙, 개표 과정에서 기존의 법·제도와 상충하는 문제점 들을 찾을 수 있었다. 또한 기술적인 측면에서는 정보격차가 초래하는 평등 선거 원칙의 문제, 익명성의 문제, 키 관리의 문제 등을 꼽을 수 있다. 또한 이러한 문제들이 선제적으로 해결 되어야 블록체인 기술이 가진 장점을 기대할 수 있는 효과적인 온라인 투표 시스템이 될 수 있을 것이다.

본 연구를 통해 국내에서도 해외 사례와 같이 우선 법적인 제약이 많지 않은 민간선거, 위탁선거에서부터 도입하는 것이 적합할 것이라는 결론을 얻을 수 있었다. 현실적인 방안으로는 중앙선거관리위원회에서 제공하고 있는 k-voting 시스템에 블록체인 기술을 적용하여, 아파트 단지의 동대표 선거, 대학교의 학생회장 선거, 더 나아가면 주주총회나 이사회의 의사결정과정에 먼저 활용해 보는 것을 제안한다. 이러한 사례를 통해 확보된 신뢰와 경험을 기반으로 향후 더 큰 대규모 선거나 공직선거에도 활용할 수 있는 인프라 구축을 통해 더욱 신뢰성이 확보된 상태에서 블록체인에 기반한 온라인 투표 시스템 도입을 제안한다.

제 1 장 연구개요

1. 추진 배경 및 목적

전자투표는 90년대 중반부터 세계 주요 국가들이 도입을 하고 있으며, 현재는 약 50여개국이 공직선거에 전자투표를 도입하여 활용하고 있다. 공직선거에서 전자투표 활용은 기존의 종이투표에서 디지털 방식으로 전환되는 단순한 선거관리방식의 변화만을 의미하지는 않는다. 국가 정책의 파급효과가 큰 정치적 성격이 강한 공공정책으로 평가되어야 할 필요성 있다. 따라서 이러한 전자투표 시스템이 유권자의 신뢰를 얻기 위해서는 기술적인 보안성과 안정성이 완벽히 구현되었을 때 가능할 수 있다.

대한민국에서 전자투표는 2002년 민주당 대통령후보 경선에서 인터넷투표가 실시되었다. 2003년에는 참여정부의 전자정부 로드맵 31대 과제 중 '온라인 국민참여 확대' 과제의 핵심 사업으로 선정되기도 하였다. 이에 따라 2006년부터 중앙선거관리위원회가 주관기관으로 전자투표 시스템을 개발하여 각종 위탁선거에 시범 적용하는 등 점진적으로 발전하여 왔다.

(그림 1) 온라인투표시스템 '케이보팅(K-Voting)'

자료 : 케이보팅(K-Voting), http://www.kvoting.go.kr

중앙선거관리위원회는 2013년 10월부터 온라인투표시스템 K-voting을 운영하고 있는데, 이를 통한 민간선거 지원에도 적극적이다. 온라인투표시스템 K-voting은 학교, 아파트, 마을, 협동조합 등과 같은 생활 공동체의 대표를 선출하는 것뿐 만 아니라 특정 의제에 대한 의견수렴 및 정책결정을 위해 활용되되고 있다. 또한 정당의 대표를 선출하거나 대통령 후보를 선출하는 경선에도 온

라인투표시스템을 지원하고 있다. 온라인 시스템의 장점으로는 1) 유권자의 투표 참여율 제고, 2) 다양한 투표 방식 지원, 3) 투개표의 안전성과 신뢰성이 보장을 들 수 있다. 이외에도 K-voting은 선거제도의 4대원칙과 IT 온라인 투표의 가이드라인을 충족시키는 시스템으로 평가되고 있다. 온라인 시스템은 다음과 같은 전자투표의 특징을 갖고 있다.

[표 1] 온라인투표의 특징

특징	내용
정확성	모든 정당한 유효투표는 투표결과에 정확히 집계됨
검증성	투표결과 위조방지를 위한 투표결과 검증수단이 필요
완전성	부정 투표자에 의한 방해 차단, 부정투표는 미집계
단일성	투표권이 없는 유권자의 투표참여 불가
합법성	정당한 투표자는 오직 1회만 참여 가능
기밀성	투표자와 투표결과의 비밀관계 보장
공정성	투표 중의 집계결과가 남은 투표에 영향을 주지 않음

자료 : 케이보팅(K-Voting) 서비스 개요, http://www.kvoting.go.kr

오늘날 정보통신기술 발전이 가져온 환경 변화에 따라 온라인 투표시스템의 도입은 피할 수 없는 시대적 흐름이다. 누구나 인터넷을 쓸 수 있고 스마트폰과 태블릿 PC가 널리 보급된 디지털 시대에 살고 있다. 이미 우리는 굳이 투표소를 정해진 날에 방문하지 않고도 언제나 투표를 행사할 수 있으며, 앞으로는 온라인개표시스템 활용으로 투표 종료와 동시 개표결과 확인이 가능한 온라인 투표 시대를 머지않아 직접 경험할 수 있을 것이다.

다양한 장점을 지닌 온라인 투표 시스템이 더 많은 분야에서 널리 활용되기 위해서는 기술적 안정성에 대한 신뢰와 전자투표의 유용성에 대한 공감대가 형성되어야 할 것이다. 특히 전자투표 기술에 대한 “신뢰” 확보는 매우 중요하다. 기존의 전자투표 시스템이 가지는 보안성에 대한 문제점은 반드시 해결되어야 한다. 이를 위해서 미래 기술 이슈로 떠오르고 있는 “블록체인” 방식을 투표에 활용하고자 하는 움직임이 대두되고 있다.

기존에 금융 분야에서 활발히 적용하던 블록체인 기술이 점차 다른 분야로도 확대되고 있다. 특히, 투표관련 분야에서 활발히 적용되고 있다. 온라인 투표에 블록체인 기술을 도입하면 많은 이점이 예상되며, 금융 분야에 이어 블록체인 기술을 적용할 수 있는 분야로 기대되고 있다. 특히, 생활선거분야에서 활용되고 있는 온라인투표시스템의 보안성 및 신뢰성 향상을 위한 신기술 활용이 필요한 시점에서 블록체인 기술은 이에 대한 대안이 될 수 있을 것이다.

따라서 본 연구에서는 신뢰성과 투명성, 효율성을 높이기 위한 방안으로 블록체

인 기술을 온라인 투표 시스템에 도입하기 위한 그 가능성을 타진해 보는 데 그 목적이 있다. 이를 위해서는 우선 블록체인 기술과 온라인투표시스템에 대한 조사, 온라인 선거 사례 및 블록체인 활용 온라인 선거에 관한 사례 등에 대한 조사를 진행하였다. 이러한 자료 조사 및 분석과 함께 주요 국가의 블록체인 활용 온라인 선거 사례를 분석하였다. 그리고 이를 국내에 도입하기 위해 법적 · 기술적 문제점을 분석 후 그에 대한 정책적 방안을 제안하고자 한다.

2. 연구 대상 및 내용

본 연구에서 진행하는 내용은 다음과 같다.

○ 블록체인의 기본원리와 투표시스템 구축에 활용 가능한 기술의 범위와 내용
○ 블록체인 방식을 활용한 온라인투표시스템의 기능과 구성
○ 블록체인 방식의 온라인투표시스템을 활용한 투표의 범위와 장점
○ 블록체인 방식의 온라인투표시스템의 효과와 해결과제 분석
○ 블록체인 방식의 온라인투표시스템의 활용해외사례: 미국·스페인·우크라이나·에스토니아 등
○ 한국선거에서 블록체인 방식의 온라인투표시스템의 도입을 위한 제도적, 기술적, 정책적 제언과 시사점

3. 기대 효과

블록체인 기술의 도입은 공공서비스 분야에도 많은 변화를 불러일으킬 것으로 예상됨에 따라 여러 국가에서 도입을 검토 중이다. 본 연구는 온라인투표시스템이라는 구체화된 대상에 대한 실증적인 연구이며, 공공서비스에 대한 기술 분야 및 법·정책에 대한 연구가 함께 이루어진다는 점에서 기존 연구와 차별성을 갖고 있다. 본 연구를 통해 산출된 결과물은 다음과 같은 활용 방안을 기대할 수 있다.

○ 온라인투표시스템(K-Voting) 및 전자투표 제도개선 참고자료로 활용

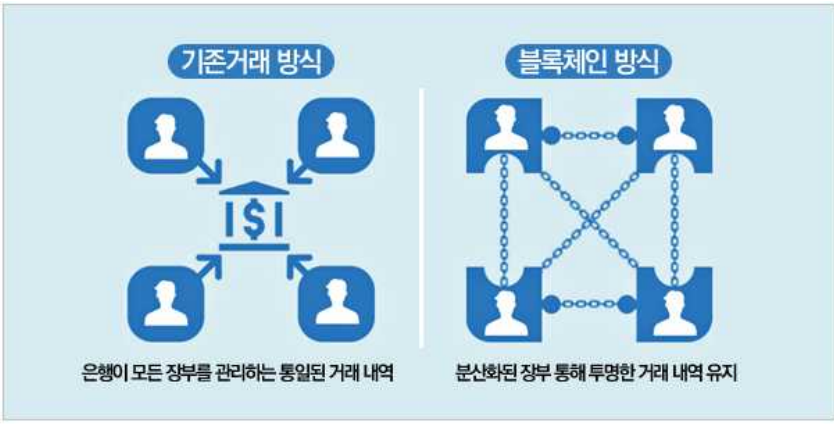
○ 유권자 중심의 투표시스템 구축과 투표참여 제고를 위한 정책방안으로 활용

○ 국민 참여를 통한 선거의 신뢰성 및 안전성 제고 방안으로 활용

제 2 장 블록체인 방식의 온라인투표시스템 관련 연구

1. 블록체인 기술 개요

블록체인(Blockchain)이란 데이터를 거래할 때 중앙집중형 서버에 기록을 보관하는 기존 방식과 달리 거래 참가자 모두에게 내용을 공개하는 분산형 디지털 장부를 말한다. 블록체인에 참여한 모든 구성원이 네트워크를 통해 서로 데이터를 검증하고 저장함으로써 특정인의 임의적인 조작이 어렵도록 설계된 저장 플랫폼이라 할 수 있다. 이러한 상호분산원장(mutual distributed ledger)을 통하여 기존 중앙집중형 네트워크 기반의 인프라를 뛰어넘는 높은 보안성·확장성·투명성 등을 보장한다.



(그림 2) 기존 거래 방식과 블록체인 방식의 거래방식의 차이

자료 : SW중심사회

1) 블록체인 기술 특징

블록체인 기술을 이해하기 위해 기억해야 할 중요한 특징은 크게 2가지가 있다.

① 블록은 시간별로 정렬돼 있다.

거래 기록이 '블록'이라는 단위로 정리돼 시간별로 이어져 있는 것이 블록체인의 특징이다. 한 블록에는 앞의 블록과 뒤의 블록과 연결되는 연결 정보가 포함돼 있으며, 앞 블록의 내용을 변경하면 뒤에 이어지는 모든 블록을 다시 생성해야 한다. 따라서 과거 블록의 내용을 조작하는 것은 어렵다. 반대로 과거의 어느 시점에 거래 기록이 존재한다면 그것은 그 시점에 거래가 이루어졌다는 것을 객관적으로 알 수 있는데 이 역시 중요한 점이다.

② 분산형 원장 구조다

블록체인은 분산형 원장 구조이며, 그 블록체인 네트워크에 참가한 모든 사람이 모든 거래내역을 기록한 원장을 소유한다. 그렇기 때문에 블록체인 기술을 활용하면 별도의 거래관리 기관 없이 분산화 된 거래장부인 블록체인에 의해 작동되기 때문에 시스템 유지비용이 적고 해킹을 원천 차단할 수 있다는 장점이 있다. 분산 원장 환경에서는 사용자가 송금거래를 요청하면, 거래 정보가 기록된 하나의 블록을 생성하여 네트워크상의 모든 참여자에게 블록을 전송한다. 이 때 각 참여자가 전송된 블록을 승인하게 되면 기존 블록체인에 거래 기록이 추가되면서 거래가 완료된다. 기존 블록체인에 담겨 있는 거래정보를 수정하기 위해서는 전체 비트코인 네트워크 참여자의 과반수가 동일한 정보임을 확인해 줘야 하기 때문에 해커가 전 세계 네트워크 참여자의 블록체인을 동시에 해킹하는 것은 사실상 불가능하다. 즉, 해커가 디지털 장부를 조작하려 해도 수천, 수 억명의 흩어져 있는 장부를 한꺼번에 조작할 수 없기 때문에 상대적으로 안전하다고 볼 수 있다.

또한, P2P(Peer to Peer) 방식으로 작동되기 때문에 금융회사 입장에서는 기존과 같은 중앙전산망을 갖추지 않고도 낮은 비용으로 안전한 금융거래가 가능하다. 단기적으로 연간 20억 달러(약 23조원)를 절감할 수 있을 것으로 예상되며[1], 금융서비스 제공시 2020년까지 연간 150~200억 달러의 비용을 절감할 수 있을 것으로 보여진다[2]. 뿐만 아니라, 소비자 입장에서도 금융서비스를 이용할 때 훨씬 편리해진 서비스와 함께 향상된 속도, 수수료 절감 등 다양한 혜택을 기대할 수 있다.

[표 2] 블록체인 기술의 특징

구분	주요내용
보안성 (Secure)	정보를 다수가 공동으로 소유하여 해킹 불가능 → 보안관련 비용 절감
투명성 (Transparent)	모든 거래 기록에 공개적 접근 가능 → 거래 양성화 및 규제비용 절감
확장성 (Scalable)	공개된 소스에 의해 쉽게 구축·연결·확장 가능→ IT 구축 비용 절감
신속성 (Instantaneous)	거래의 승인 기록은 다수의 참여에 의해 자동 실행 → 신속성 극대화
탈중개성 (P2P-based)	공인된 제3자의 공증 없이 개인 간 거래 가능 → 불필요한 수수료 절감

자료 : 정보통신기술진흥센터

1) 출처 : 영국 <파이낸셜 타임스>
2) 출처 : 스페인 <산탄데르은행>

이러한 다양한 이점 때문에 이미 많은 글로벌 금융회사들은 블록체인 기술에 대한 본격적인 연구와 투자를 확대하기 시작했다. 대표적으로 골드만삭스, 바클레이즈, JP모간체이스, 시티그룹, UBS 등 40여개 글로벌 금융회사가 R3 CEV로 불리는 블록체인 컨소시엄을 구성하여 블록체인 표준 플랫폼 공동개발 및 테스트를 진행 중이다. 미국 나스닥은 2015년 10월 블록체인 기반의 장외주식 거래소를 구축하였고, 미국 증권거래소는 오버스탁이라는 회사에 블록체인이 적용된 인터넷 공모 주식 발행권한을 부여하고 있다.

블록체인 기술은 비트코인 등 공용 블록체인(1세대), 사설 블록체인(2세대)을 거쳐, 2017년부터 스마트 블록체인(3세대)로의 진입이 예상되고 있다. 이에 따라 금융부문뿐만 아니라, 다양한 제품 및 서비스의 생산·소비·유통·관리 등의 측면에서 기존 산업의 모습을 크게 변화시킬 것으로 전망되고 있다.

[표 3] 블록체인 기술 발전 전망

구분	1세대	2세대	3세대
종류	공용(Public) 블록체인	사설(Private) 블록체인	스마트(Smart) 블록체인
주요 기술 내용	. 분산합의기술 (작업증명/지분증명/위임지분증명 기술) . 동기 p2p 네트워크	. 제한적 분산합의기술 (PBFT(Pratical Byzantine Fault Tolerance), 연방 합의 기술) . 동기/비동기 p2p 네트워크	. 고기능 고효율 분산합의 기술 . 개인정보보호, 비밀유지 . 추적 기술 . 자금세탁방지 기술 . 안정적 동기/비동기 p2p 네트워크
적용 가능 서비스	. 디지털 화폐 . 외환송금 . 스마트계약	. 개인의료정보 관리 . 자산증명/소유권증명	. 정부 및 공공서비스 . 개인정보/비밀유지 지원 서비스
주요 기업	Bitcoin, Ethereum, Bitshare	Ripple, R3 CEV, ADEPT	–

자료 : 미래창조과학부 보도자료

2) 블록체인 유형

블록체인은 참여 네트워크의 성격, 범위 등에 따라 여러 가지 형태가 존재하고 사용용도에 맞게 응용이 가능하다. 블록체인을 유형별로 보면, 흔히 알려진 퍼블릭 블록체인 외에도 컨소시엄 블록체인 및 프라이빗 블록체인이 있다. 다음은 그에 대해 정리한 자료이다.

[표 4] 블록체인 유형 별 특징

	퍼블릭 블록체인	컨소시엄 블록체인	프라이빗 블록체인
관리 주체	모든 거래 참여자 (탈중앙화)	컨소시엄에 소속된 참여자	한 중앙기관이 모든 권한 보유
거버넌스	한번 정해진 룰을 바꾸기 매우 어려움	컨소시엄 참여자들의 합의에 따라 상대적으로 용이하게 룰을 바꿀 수 있음	중앙기관의 의사결정에 따라 용이하게 룰을 바꿀 수 있음
거래 속도	네트워크 확장이 어렵고 거래속도가 느림	네트워크 확장이 쉽고 거래 속도가 빠름	네트워크 확장이 매우 쉽고 거래 속도가 빠름
데이터 접근	누구나 접근 가능	허가받은 사용자만 접근가능	허가받은 사용자만 접근가능
식별성	익명성	식별 가능	식별 가능
거래 증명	PoW, PoS와 같은 알고리즘에 따라 거래 증명자가 결정되며, 거래 증명자가 누구인지 사전에 알 수 없음	거래증명자가 인증을 거쳐 알려진 상태이며, 사전에 합의된 규칙에 따라 거래검증 및 블록생성이 이루어짐	중앙기관에 의하여 거래증명이 이루어짐
활용 사례	비트코인	R3 CEV	나스닥의 비상장 주식거래소 플랫폼인 링크(Linq)

자료 : 코빗, the FinTech, CoinDesk, 금융보안원

퍼블릭 블록체인은 공개형 블록체인으로 누구나 참여할 수 있는 블록체인이다. 따라서 모든 참여자는 자유로운 자료 열람과 거래가 가능하다. 하지만 검증되지 않은 다수의 사용자가 참여하므로 고도화된 암호화 검증이 필요하여 네트워크의 확장이 어렵고 속도가 느리다. 또한 퍼블릭 블록체인은 완벽한 분산형 구조를 이루고 있다. 네트워크 참여자가 익명성의 성격을 띠기 때문에 중앙 시스템의 제어가 필요한 금융 서비스에 적합하지 않다. 따라서 블록체인의 비용 절감과 같은 장점은 살리되 금융서비스에서 필요한 시스템 제어 권한이나 주도권도 잃지 않을 수 있는 컨소시엄과 프라이빗 블록체인에 주목 할 필요가 있다.

프라이빗 블록체인은 익명성을 제공했던 퍼블릭 블록체인과 달리 주체의 식별이 가능하다. 또한 거래의 처리 속도가 빠르며 네트워크 확장이 용이하여 사용자가 원하는 대로 커스터마이징 할 수 있기 때문에 금융 서비스에 적합하여 최근 기업과 은행권의 관

심을 모으고 있다. 프라이빗 블록체인은 소유자가 블록체인을 생성하고 관리하는 블록체인으로 블록체인 소유자가 블록체인을 중앙 시스템처럼 관리하고자 경우 적합하다.

컨소시엄 블록체인은 퍼블릭 블록체인과 프라이빗 블록체인의 중간 형태이다. 소유자가 모든 권한을 가지게 되는 형태인 프라이빗 블록체인과 달리 미리 선정된 노드들이 권한을 가지게 되는 블록체인이라고 할 수 있다. 따라서 컨소시엄 블록체인은 분산형 구조를 유지하면서 제한된 참여를 통해 보안을 강화할 수 있고 퍼블릭 블록체인에서 제기된 느린 거래 속도와 네트워크 확장성의 문제도 해소시켜주기 때문에 은행들 간 거래 용도로 활용할 수 있다.

3) 블록체인 합의(Consensus) 알고리즘

블록체인은 기본적으로 분산 시스템이다. 분산 컴퓨팅으로 이루어진 비행기 예매 시스템에 합의 알고리즘이 없다고 가정해 보자. 손님 A와 손님 B가 같은 자리a를 동시에 예매 하였을 때 합의 알고리즘이 없다면 들어온 시스템에 따라 자리 a를 예매한 사람이 달라진다. 이런 시스템 오류와 무결성을 보장하기 위하여 합의 문제를 해결하는 합의 알고리즘이 생겨났다.

블록체인은 각 노드에서 만든 블록의 정당성을 검토하고 네트워크 전체에서 공유하는 블록체인에 반영하기 위해 이 합의 알고리즘을 사용한다. 블록체인에서 사용되고 있는 대표적인 합의 알고리즘에는 다음과 같은 것들이 있다.

① PoW(Proof of Work)

비트코인을 시작으로 많은 블록체인 기반 기술이 채택하고 있는 합의 알고리즘이다. 블록을 만들어 배포한 후 많은 참가자가 사용하는 것을 올바른 블록으로 정의하기 때문에 참가자의 수에 영향을 받지 않고 얼마든지 참가자를 늘릴 수 있다. 반면 네트워크 상태에 따라 일부분에 불일치가 생긴 경우, 결과가 불확실하게 되는 점이나 성능이 나오지 않는다는 단점이 있다.

② PoS(Proof of Stake)

이더리움이 채택한 알고리즘이다. 화폐량을 더 많이 소유하고 있는 승인자가 우선하여 블록을 생성할 수 있는 특징이 있다. 이것은 '대량 통화를 소유하고 있는 참가자는 그 통화 가치를 지키기 위해 시스템의 신뢰성을 손실하지 않을 것이다'라는 전제를 바탕으로 하고 있다. 기본적인 구조는 PoW와 다르지 않지만 화폐량에 따라 해시 계산의 난이도가 낮아지기 때문에 PoW와 비교하여 자원 소비가 작아지는 장점이 있다.

③ PBFT(Practical Byzantine Fault Tolerance)

PBFT는 PoW나 PoS와 마찬가지로 Byzantine Fault[3] 모델이지만 PoW와 PoS의 단점인 결과의 불확실성과 성능 문제를 해결한 것이다. Hyperledger Fabric과 Eris 등 컨소시엄형에서 이용하고 있는 블록체인 기반 기술에 많이 채택되고 있다.

PBFT는 네트워크의 모든 참가자를 미리 알고 있어야 한다. 참가지 중 1명이 프라이머리(Primary, 리더)가 되고 자신을 포함한 모든 참가자에게 요청을 보낸다. 그 요청에 대한 결과를 집계한 뒤 다수의 값을 사용해 블록을 확정한다. 부정한 노드 수를 f개라고 하면 노드 수는 3f+1개여야 하며, 확정에는 f+1개 이상의 노드가 필요하다. PoW/PoS는 남은 1개에서도 동작을 계속하지만 PBFT는 필요 수를 충족하지 못하면 정지한다.

PoW나 PoS와는 달리 다수결로 의사결정한 뒤 블록을 만들기 때문에 블록체인의 분기가 발생하지 않는다. 따라서 한 번 확정된 블록은 변경되지 않기 때문에 최종 결과를 확보할 수 있다. 그리고 PoW와 같이 조건을 만족시킬 때까지 계산을 반복하지 않아도 되기 때문에 매우 고속으로 동작한다. 부정 사용을 하고자 해도 과반수를 획득해야 하며 만약 프라이머리가 거짓말을 한다 해도 모든 참가자가 리더의 움직임을 감시해 거짓말이라고 판단한다면 다수결로 리더 교체를 신청할 수 있기 때문에 장애에 매우 강력한 내성을 가진 알고리즘이다.

반면 언제나 참가자 전원과 의사소통을 해야 하기 때문에 참가자가 증가하면 통신량이 증가하고 처리량이 저하된다. PoW나 PoS는 수천 개의 노드를 만들 수 있지만 PBFT는 수십개의 노드가 한계이다.

4) 블록체인 기술 구조 및 개발 플랫폼 현황

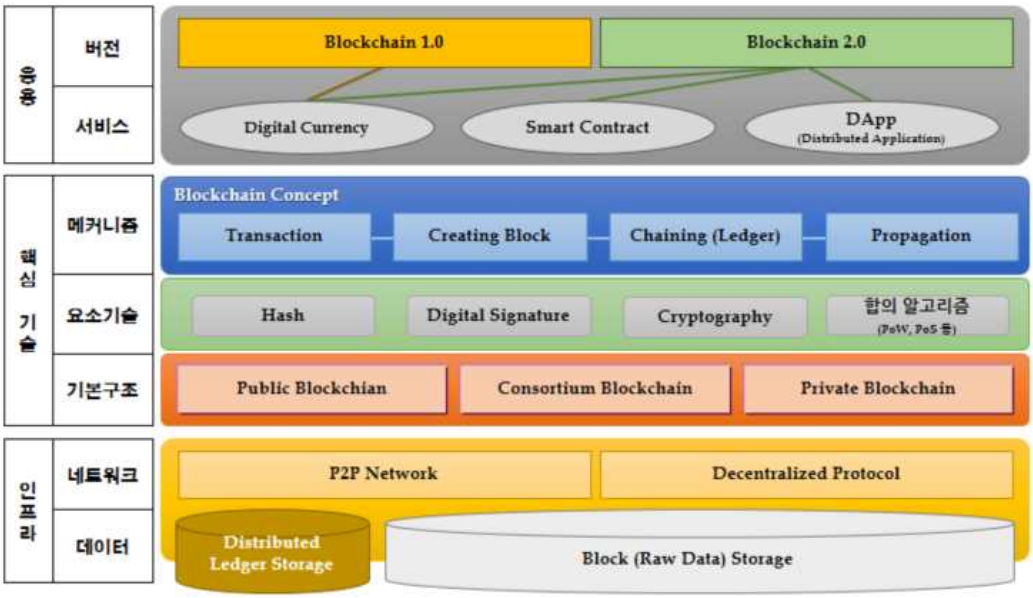
블록체인은 공인된 제3자 없이도 거래 기록의 무결성 및 신뢰성을 확보하기 위해 해시(Hash)[4], 전자서명(Digital Signature)[5], 암호화Cryptography) 등의 보안 기술을 활용한 분산형 네트워크 인프라를 기반으로 다양한 응용서비스를 구현할 수 있는 구조를 가지고 있다.

---

3) 비잔틴 장군 문제(Byzantine General Problem) : 분산 컴퓨팅 환경에서 악의적인 노드가 분산 시스템에 참여한 상황을 모델링한 문제. 비잔틴 장군 문제를 해결한 시스템은 악의적인 노드가 분산 시스템에 참여한 상황에서도 전체 시스템은 신뢰도 있는 서비스를 제공할 수 있다는 것을 보장한다.

4) 임의의 길이의 입력 메세지를 고정된 길이의 출력 값으로 압축시키는 기술로 데이터의 무결성 검증 및 메시지 인증에 사용된다.

5) 전자 서명은 작성자로 기재된 자가 그 전자문서를 작성하였다는 사실과 작성내용이 송·수신과정에서 위변조 되지 않았다는 사실을 증명하는 기술이다.



(그림 3) 블록체인의 요소

* MS 클라우드 블록체인 서비스, LG CNS 블록체인 개념도 참조

이러한 블록체인 기술은 본래 비트코인(Bitcoin)[6]이라는 전자화폐를 안전하게 저장하고 사용하기 위하여 고안된 보안 기술이었다. 비트코인의 핵심기술로써 디지털 통화(Digital Currency)의 발행·유통·거래가 주 기능이었던 기존의 블록체인 1.0은 기존 비트코인의 한계를 극복하고 다양한 영역으로의 확장을 목표로 하는 블록체인 2.0으로 진화 · 발전해나가고 있다.

블록체인 2.0의 대표적인 기술로는 이더리움(Ethereum)이 있으며, 디지털통화의 기능과 더불어 비트코인의 거래 스크립트를 다양한 형태로 프로그램 가능하게 만든 스마트 컨트랙트(Smart Contract)를 구현하다. 이더리움은 블록체인 기반 위에서 부동산 계약, 온라인 투표 등 다양한 분산 어플리케이션을 개발하고 구동할 수 있는 플랫폼으로 확장되었다. 여기서 이야기하고 있는 블록체인 플랫폼이란 블록체인 서비스를 개발, 테스트할 수 있도록 블록체인 시스템의 구성요소(분산 네트워크, 통신 프로토콜 등) 및 필요기능(거래정보 검증, 합의, 노드관리 기능 등)을 제공하는 환경을 말한다. 블록체인 서비스 개발 시 플랫폼을 활용함으로써 개발 편의성과 서비스 간 상호 호환성, 안정성을 확보할 수 있다.

본 연구에서는 블록체인 기술을 온라인 투표 시스템에 적용할 때의 기술적 이슈 분석 및 기술적 도입방안을 알아보기 위하여 블록체인 개발 플랫폼 현황에 대한 조사를 진행하였다. 블록체인 기반 플랫폼 중에서도 비트코인을 구현한 Bitcoin Core, 분산 응용프로그램 플랫폼으로 많은 실증 실험에 사용되고 있는 이더리움, 그리고 리눅스 재단 주도로 개발되고 있는 컨소시엄형 블록체인 Hyperledger Fabric을 다음

6) 블록체인 기반의 디지털 가상화폐

의 표와 같이 정리하였다.

[표 5] 블록체인 플랫폼 비교

	Bitcoin Core	이더리움	Hyperledger Fabric
블록체인 분류	공용, 컨소시엄, 개인	공용, 컨소시엄, 개인	컨소시엄, 개인
합의 알고리즘	Proof of Work(PoW)	Proof of Work(PoW) 이후 Proof of Stake(PoS)로 변경 예정	Practical Byzantine Fault Tolerance (PBFT)
결제 완료성	없음. 각 노드[7]가 각각의 블록을 만들기 때문에 블록체인이 분기되는 경우 확정된 트랜잭션이 번복될 수 있음	없음. 각 노드가 각각의 블록을 만들기 때문에 블록체인이 분기되는 경우 확정된 트랜잭션이 번복될 수 있음	있음. 갱신시 합의를 확정하기 때문에 결제 완료성 있음
성능	블록 생성 간격은 10분 단위지만 '확정됐다'고 판단하기 위해서는 어느 정도 블록을 이어나가야 하기 때문에 1시간정도 소요	블록 생성 간격은 12초 단위지만 '확정됐다'고 판단하기 위해서는 어느 정도 블록을 이어나가야 하기 때문에 몇 분 정도 소요	갱신 시 합의를 확정하기 때문에 성능이 좋으며, CPU 자원도 효율적으로 사용함.
계정 관리	참가자(계정)는 각 노드에서 관리되고 공유되지 않음. 따라서 참가자 유입을 제한하는 기능은 존재하지 않음	참가자(계정)는 각 노드에서 관리되고 공유되지 않음. 따라서 참가자 유입을 제한하는 기능은 존재하지 않음	멤버쉽 서비스가 사용자와 노드를 등록. PKI[8] 기반 증명서를 발행
최소 구성대수	1대부터 작동. 장애 복구를 위해서는 최소 2대 필요	1대부터 작동. 장애 복구를 위해서는 최소 2대 필요	PBFT에서 1대의 장애 복구를 위해서는 최소 4대 필요
데이터 모델	계약 자체도 블록체인에 포함돼 전파됨. 정보는 UTXO(Unspent Transaction Output) 방식으로 유지되므로 집계하기 위해서는 모든 블록을 참조해야 함	계약 자체도 블록체인에 포함돼 전파됨. 정보는 UTXO(Unspent Transaction Output) 방식으로 유지되므로 집계하기 위해서는 모든 블록을 참조해야 함	블록체인과 월드 스테이트로 구성됨. 월드 스테이트는 키 밸류 스토어이며, 트랜잭션 완료시 상태를 보존할 수 있음
정보	트랜잭션[9]의 내용은	트랜잭션의 내용은	트랜잭션은 암호로

	Bitcoin Core	이더리움	Hyperledger Fabric
은닉화	공개정보가 됨	공개정보가 됨	은닉할 수 있음. 각 트랜잭션은 트랜잭션 증명서로 서명되므로 요청자를 추적할수 없음
스마트 컨트랙트 개발	비트코인 트랜잭션은 스크립트 언어[10]로 실행됨. 매우 간단한 언어로 루프 처리나 분기 구분에 제한이 있음. 따라서 확장성이 부족함. 하지만 안전성과 유효성, 용이성의 관점에서 의도적으로 제한하고 있는 부분도 있음	계약이라고 불리는 프로그램을 개발함. 개발언어는 Solidity라는 전용 언어를 주로 사용. 소스 코드는 Ethereum Virtual Machine(EVM)이라는 가상 머신에서 동작하기 때문에 플랫폼에 의존하지 않음. Gas라는 일종의 연료 개념이 있어 일정 처리 비용 안에서 동작시켜야 함	체인 코드라는 프로그램을 개발함. 개발언어는 Go와 자바. 향후 자바스크립트가 추가될 예정. 소스로부터 네이티브 코드를 생성해 직접 실행함. 도커 컨테이너 안에서 실행됨

자료 : 블록체인 구조와 이론(위키북스)

5) 비금융분야 블록체인 활용

블록체인은 앞서 이야기한 것처럼 금융분야 뿐만 아니라 자동계약·저작권·계약체결·기타 법적 거래 등 다양한 분야에서 적용 가능성이 있다.

① 자산등록부(asset register)

분산원장은 자산의 내역, 거래내역 그리고 유효성을 관리하는 안정성과 신뢰성이 요구되는 장부에 이용될 수 있으며, 이 기술은 소유권과 출처를 증명하는데 이용될 수 있다. 영국의 스타트업인 Everledger사는 다이아몬드 업계의 사기와 도난문제를 해결하기 위해 이 기술을 사용 중이다. 이 외에도 토지소유권, 선하증권, 자동차 리스, 금 거래, 에너지, 주식, 기타자산 등록부의 존재 여부 또는 유지 및 관리 비용과 관련 없이 전자적으로 대표될 수 있

7) 블록체인 네트워크에 직접 참여하는 사용자

8) PKI(Public Key Infrastructure) : 공개키 기반 구조. PKI는 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하기 위한 복합적인 보안 시스템 환경을 말한다. 즉, 암호화와 복호화키로 구성된 공개키를 이용해 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 시스템을 말한다

9) 트랜잭션(transaction) : 데이터통신 시스템에서 데이터통신 시스템에서 관리의 대상이 되는 기본적인 정보를 기록한 기본파일(master file)에 대해서 그 내용에 추가, 삭제 및 갱신을 가져오도록 하는 행위(거래)를 트랜잭션이라 한다. 예를 들면, 입하, 출하, 매상, 반품, 임금, 출금, 정정 등의 데이터를 말하며, 이동정보라고도 한다.

10) 스크립트 언어(script language) : 컴파일(compile)을 하지 않고, 작성해서 바로 실행시킬 수 있는 언어. 컴파일하지 않고 변수 타입을 선언하지 않는다는 특징이 있다. 대표적인 스크립트 언어로는 자바 스크립트, Perl, Tcl/Tk 등이 있다.

고, 저장될 수 있고, 거래될 수 있는 모든 자산에 분산원장 기술의 적용이 가능하다.

② 신원등록부(identity registers)

분산원장은 각종 서비스에서 디지털인증을 간소화함으로써 정확한 신원확인 및 신원도용에 의한 피해를 줄이는 데 도움을 준다. 신원관련 데이터의 관리 및 통제를 용이하게 한다.

③ 지적재산(intellectual property)

분산원장 기술은 지적재산의 등록과 라이선스 등의 분야에서 다양한 잠재적 사용가능성이 있으며, 저작권과 관련된 권리에도 이용될 수 있다.

④ 정부 및 정부기관의 이용(government and agency use)

에스토니아의 디지털 신원시스템인 이-레지던스(e-Residency)는 블록체인 기술을 온라인 정부시스템에 접근을 인증하는 용도로 이용하고 있다. 에스토니아 정부는 '키 없는 전자서명 인프라(KSI)'를 통해 전자시민권을 개발 중이다. KSI는 시민들이 정부가 관리하는 DB에 접근하여 자신들의 정보에 대한 정확성 여부를 직접 확인할 수 있다. 또한 내부 관리자가 불법적으로 네트워크에 침입할 수 없게 하여 시민들이 전자상거래 등록이나 전자세금계산서와 같은 디지털 서비스를 활용할 수 있도록 하고 있다. 에스토니아 이외에도 미국의 경우는 의료정보의 기록 및 공유 부문, 우크라이나의 경우는 투표 시스템의 운영관리부문, 영국의 경우도 모든 공공서비스 분야 등에 블록체인 기술을 적용시키기 위해 연구 및 개발 중이다.

[표 6] 정부 주도 블록체인 활용 사례

구분	사례 소개
전자투표	- 투표 진행 결과를 블록체인에 기록하여 투명성을 유지할 수 있도록 하여, 정당 투표, 상원의원 선거 등에 활용 - (관련 국가) 덴마크, 호주 등
전자화폐	- 국가별 중앙은행에서 발행·관리하는 공식적인 화폐로 활용(예정) - (관련 국가) 영국, 필리핀 등
전자시민권	- 블록체인에 개인의 신원 정보를 저장하여, 정부 기관에 의해 디지털 신원확인이 가능하도록 활용 - (관련 국가) 에스토니아 등
소유권 기록	- 토지의 소유권을 블록체인에 등록하여 안전하게 저장·관리하는데 활용

구분	사례 소개
	- (관련 국가) 온두라스 등
기록물 관리	- 정부에서 작성, 발행한 문서 등 기록물 관리를 위해 블록체인을 활용 - (관련 국가) 영국(맨섬), 영국(디지털서비스청), 미국(버몬트 州) 등

자료 : 금융보안원

⑤ 전자공증

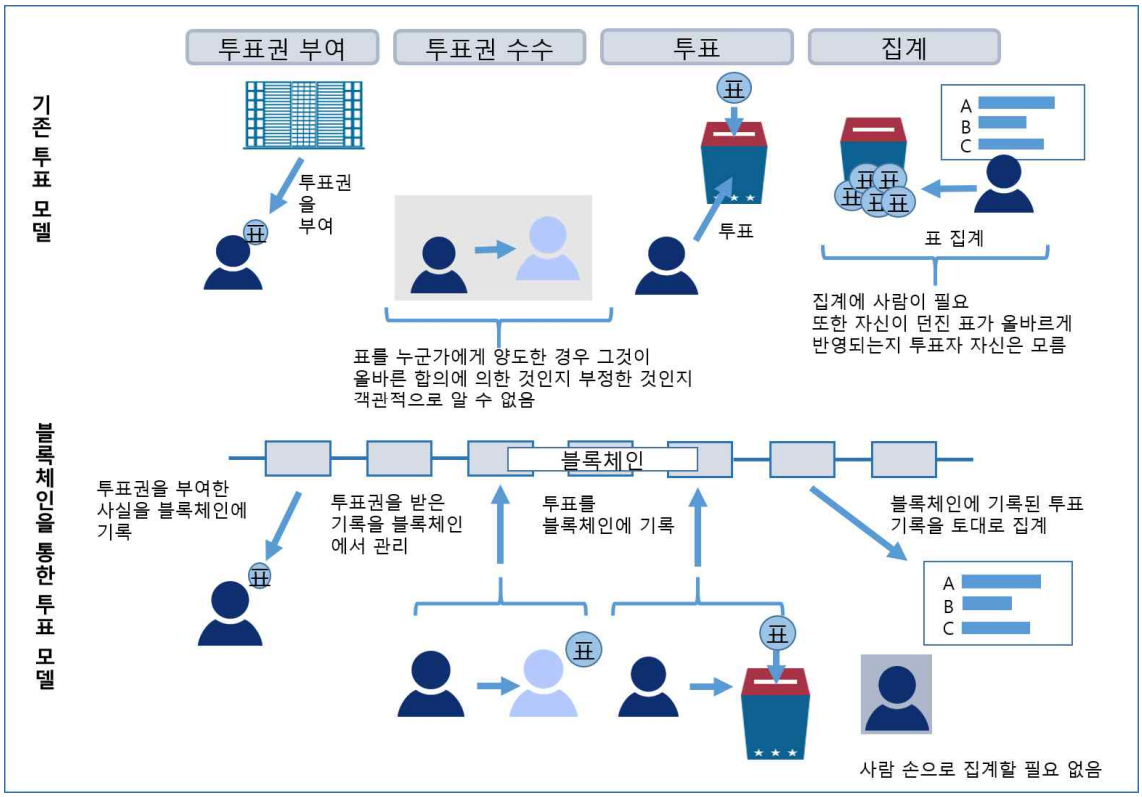
블록체인 기술의 타임스탬프와 해쉬 함수를 이용하여 인증서, 계약서 등 공적 증명이 필요한 문서 또는 각종 파일들을 증명할 수 있는 전자공증이 가능하다. 기업들은 전자공증시스템을 자체 구축하기보다는 위탁하여 운영하는 경우가 대부분인데, 집중관리기관인 위탁운영기관이 해킹 등으로 데이터가 위·변조될 위험이 존재한다. 그러나 블록체인을 이용할 경우 저장된 데이터의 불변성을 이용하여 전자공증시스템을 구축하는 것이 가능하므로 데이터 관리의 안전성이 제고된다.

⑥ 스마트 계약(Smart Contracts)

스마트 계약은 블록체인을 통해 일정 조건을 만족시키면 거래가 자동으로 실행되도록 프로그래밍한다. 자동화된 계약시스템으로 소유권 이전, 상속, 증여, 물품구매 등에 폭넓게 활용되고 있으며, 최근에는 사물인터넷과 연계되어 이용되고 있다. 스마트 계약에서는 조건에 의해 거래가 자동적으로 성립되므로 중간관리자에 의한 사기 피해를 막을 수 있다. 거래정보 기록이 보존되기 때문에 계약서 위조·사고기록 조작 등과 같은 악의적 행위의 방지가 가능하여 신용리스크와 상대방 리스크를 감소시킬 수 있다.

2. 블록체인 방식을 활용한 온라인 투표 시스템

블록체인은 신뢰성을 가장 중요시하는 금융거래에서 사용될 수 있을 정도의 신뢰성을 갖추고 있음이 증명되었다. 블록체인은 공정성과 투명성, 확실성은 물론 중간자가 존재하지 않더라도 높은 신뢰성을 가지고 있다. 이러한 이점을 선거에 적용시켜 직접민주주의 요소를 강화시킨 형태로 제시된 것이 '블록체인 온라인 투표 시스템'이다. 블록체인을 활용해 투표권한 부여나 투표 집계 등에 응용함으로써 업무를 더 효율화 할 수 있다는 장점이 있다.



(그림 4) 기존 투표 모델과 블록체인을 사용한 투표 모델

자료 : 블록체인 구조와 이론(위키북스)

블록체인 기반 온라인 투표 시스템은 기존의 전자투표 시스템에서 발전한 형태를 위하게 된다. 이러한 점에 주목하여 온라인 투표 시스템의 기능과 구성, 블록체인이 온라인투표시스템에 도입되었을 때 가지는 기능과 구성을 소개하고자 한다.

1) 온라인 투표 시스템 개요

온라인 투표 시스템이란 투표소를 직접 방문해 본인 확인을 거친 후, 교부 받은 투표용지에 기표하여 투표함에 넣는 기존의 투표방식을 대체하여, 유권자가 시간과

장소의 구애 없이 PC와 이동통신 단말기를 이용하여 웹과 모바일 환경에서 다양한 의견수렴 및 대표자 선출을 지원하는 시스템이다. 임원 선출, 정관 개정, 안건 결정 등에 있어 구성원의 의사를 정확히 반영할 수 있도록 일반적인 투표뿐만 아니라 찬반투표 등 다양한 투표를 효율적이고 안전하게 실시할 수 있도록 지원한다. 기존 선거 방식과 마찬가지로 투표과정 전반에 걸쳐 유권자의 기본권인 보통, 평등, 직접, 비밀 선거의 원칙이 준수되어야 한다. 온라인 투표 시스템에서는 감시 기관 없이 사용자들이 원하는 공간에서 자유로이 진행되기 때문에, 네트워크상에서 본인확인과 유권자의 자유로운 의사에 의한 투표를 확보하는 것이 중요한 요소이다. 또한 유권자들의 투표정보가 오류 없이 정확하게 개표과정에 전달되어야 하며, 투표 내용이 정확하고 신속하게 집계되어야 한다.

국내 대표적인 온라인 투표 시스템은 선거관리위원회의 온라인투표서비스(이하, K-voting)를 활용하는 것이다. K-voting은 선거관리위원회에 신청한 기관·단체에 대하여 PC와 이동통신단말기를 이용한 웹과 모바일 환경에서 전자투표와 개표를 실시할 수 있도록 온라인투표시스템을 지원 및 제공하는 서비스이다. K-voting에서는 투·개표 관리 서비스를 제공한다. 투표 시간이 종료되면, 투표율 확인 등 선거인에 대한 요약 정보와 선거 결과를 바로 확인가능하다. K-voting 서비스는 유권자당 450원의 저렴한 비용으로 이용할 수 있다. 그리고 진행이 간편하고, 기존 종이 투표가 갖는 장소적 제약을 극복하여 어디에서나 투표가 가능하다. 이러한 장점으로 인해 투표율 상승 기대와 민주성을 제고할 수 있다는 점에서 활용도가 높을 것으로 예상이 된다.

가. 온라인 투표시스템의 장점

① 투표의 편리성 증대 및 투표율 향상

온라인 투표 시스템은 기존의 투표 방식이 갖는 공간적, 시간적 한계를 극복할 수 있다. 유권자는 투표소에 가지 않아도 컴퓨터, 스마트폰 등 온라인 매체를 활용하여 자신이 지지하는 후보자를 선택할 수 있다. 투표방법도 클릭만 하면 되므로 투표 시간이 대폭 줄어든다. 또한 언제 어디서나 편리하게 투표할 수 있으며 지역 주민들이 정해진 시간에 한 곳에 모여야 하는 불편을 덜 수 있다. 뿐만 아니라 편의성과 접근가능성 향상으로 바쁜 일정 때문에 투표소를 직접 방문하지 못하는 유권자, 노인, 장애인, 여행 중인 유권자 등의 투표참여 가능성도 높일 수 있다. 이러한 편의성은 전체적인 투표율 향상에 기여할 수 있다.

역대 대선 투표율을 살펴보면, 30대 이하의 젊은 유권자들의 투표율이 다른 연령층에 비해 낮다는 사실을 알 수 있다. 한국뿐만 아니라 대부분 국가에서

젊은 유권자들의 투표율이 저조하지만, 인터넷의 이용자가 주로 젊은 층이라는 특성을 고려할 때, 온라인투표시스템은 20, 30대의 유권자들을 투표에 참여를 촉진시킬 수 있다.

또한 온라인 투표시스템은 투표 결정에 필요한 정보를 유권자들에게 손쉽게 전달할 수 있다. 온라인투표시스템을 통해 기존 투표 방식보다는 더 많은 정보를 유권자에게 제공할 수 있고, 더 많은 정보를 바탕으로 유권자가 투표에 참여할 수 있도록 지원이 가능하다.

② 투표 관리업무의 효율성 증대

온라인 투표 시스템은 투표 및 개표과정에서 정확성과 신속성을 향상시킬 수 있다. 결국 선거관리업무에 투입되는 인력과 시간을 단축시켜 예산을 절약할 수 있다. 투표용지를 일일이 수작업으로 확인하는 작업이 필요 없고, 투표시스템에서 자동적으로 이루어지므로 신속하고 실수를 방지할 수 있다. 따라서 무엇보다도 정확한 개표결과에 따라 선거소송을 미연에 방지할 수 있고 선거결과의 정당성 또한 높일 수 있다. 또한 초기에 온라인투표시스템을 도입하기 위한 막대한 개발비용이 소요되는 경우도 있지만, 장기적으로는 예산 절감 효과가 더 크다.

나. 온라인 투표시스템의 단점

① 보안 문제 및 신뢰 확보의 문제(직접 선거 원칙의 위반)

사람들이 투표 방식에 대해 믿음을 갖기 위해서는 그 방식이 안전하고 정확해야 한다. 그리고 투표 결과가 유권자의 정확한 의사를 그대로 반영하였다는 것이 증명되어야 한다. 휴대전화 혹은 공인인증서 인증 시스템과 같은 본인인증방식이 온라인 투표 시스템에서의 부정선거를 막기 위해 활용되고 있지만, 본인확인이나 투표내용의 완벽한 보안을 지원하기는 어렵다. 온라인상에서 사생활 침해가 늘고 있고, 사람들의 개인정보가 유출되는 온라인 환경에서 투표를 진행한다면 다른 사람의 개인정보를 도용해 대리투표, 중복투표 등과 같은 일이 발생할 수 있기 때문이다. 또한 온라인 투표 시스템은 해커나 바이러스 등의 사이버 공격에 취약하다. 특정인이 소프트웨어를 이용해 의도적으로 중앙전산시스템에 과부하를 발생시키는 서비스거부 공격(DOS : Denial of Service Attack)에 의해 유권자와 중앙컴퓨터 간의 의사소통을 불가능하게 할 가능성이 존재한다. 온라인 선거시스템의 또 다른 우려사항은 운영기구에 대한 불신이다. 해킹이 아닐지라도 정부의 통제와 조작의 가능성이 존재하기 때

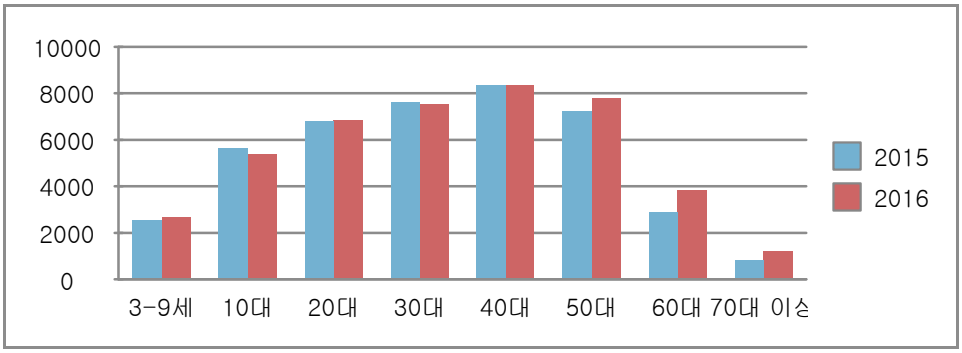
문이다. 강력한 감시기구가 운영되지 않는다면 선거관리자가 선거 결과에 영향을 미칠 수 있다. 특정 후보에 대한 득표수 조작 등의 가능성이 있고, 이처럼 안정성과 보안에 대한 불신이 생기게 된다면, 투표결과에 대한 신뢰 역시 확보할 수 없게 된다.

② 투표의 비밀보장 문제(비밀 선거 원칙의 위반)

투표는 강압이나 제 3자의 간섭 없이 자유롭고 공정하게 치러져야 하고, 이를 위해 투표 비밀 보장은 필수 요소이다. 기존의 투표 방식은 투표소에서 담당 공무원 감독 하에 투표가 진행되기 때문에, 이중투표 위험성이 낮다. 투표의 비밀성 보장, 날인된 투표용지 등 상대적으로 안전한 투표방식을 제공한다. 반면 온라인투표시스템에서 진행되는 투표는 감시 기구의 통제를 벗어난 투표방식으로, 투표 행태를 공공적인 성격에서 사적인 성격으로 바꿀 수 있다. 사적인 성격으로 인해 투표자들의 편리함은 극대화될 수 있지만, 원격에서 진행되는 투표는 제3자에 의해 비밀 투표의 원칙을 훼손할 가능성이 존재한다. 온라인투표시스템은 대부분 아무런 감시가 이루어 지지 않는 사적인 공간들에서 진행되기 때문에 유권자의 자율적 의사 결정을 위협할 수 있는 부정선거의 위험성이 존재할 수 있다. 조작의 어려움으로 인해 타인의 도움을 받는 과정 또한 비밀선거의 원칙에 어긋날 수 있다.

③ 디지털 격차의 문제 (선거의 평등원칙 위반)

온라인 투표 시스템을 본격적으로 사용하게 된다면 디지털 격차가 우려될 수밖에 없다. 인터넷을 통한 투표 참여는 각 사회계층 및 집단의 정치적 참여 기회에 불균등한 영향을 미칠 수 있다. 컴퓨터나 스마트폰에 익숙한 젊은층이나 교육수준이 높은 계층은 손쉽게 온라인상에서 투표 할 수 있다. 그러나 컴퓨터나 스마트폰, 인터넷에 익숙하지 않은 계층에게는 부담으로 작용할 가능성이 크기 때문이다. 특히 고령자나 저학력 계층의 투표율 하락을 야기할 수 있고, 이는 불평등의 문제를 야기한다. 2016년도 연령별 인터넷 이용자수를 조사한 결과 60대, 70대는 다른 연령대에 비해 확연하게 낮은 비율을 기록하고 있다.



(그림 5) 2016년도 연령별 인터넷 이용자 현황

자료 : 한국인터넷진흥원

디지털 격차로 인한 불평등은 개개인의 투표권이 재산, 신분, 성별, 교육정도 등의 영향을 받지 않고 모두에게 동일하게 권리를 부여해야 하는 평등 선거 원칙을 위반할 수 있다. 또한 기술적 문제와 달리 디지털 격차는 한 순간에 해결하기는 힘들다는 문제가 존재한다.

다. 온라인 투표 시스템의 기능

온라인 투표 시스템은 인터넷이 상용화되기 시작하며 그 효율성 때문에 관심을 받기 시작했다. 이후 오랜 시간이 흘렀고 인터넷의 안정성이 검증되었다. 그럼에도 불구하고 온라인투표시스템이 공직선거 사용되는 나라는 손에 꼽을 수 있을 정도로 적다. 온라인 투표 시스템을 사용하는 나라 중, 에스토니아는 2005년부터 전자 투표를 실시하고 2007년에는 온라인투표시스템을 허용한 나라다. 2015년 국회의원 선거에서 전체 투표자의 30.5%가 온라인 투표 시스템을 사용했다.[11)]

온라인 투표 시스템은 기존 투표지를 사용한 투표와 비교했을 때 다양한 부가적 기능을 가지고 있다. 유권자의 **투표참여율 제고**, **개표의 신속성**, **비용 절감**과 **장애 유권자의 접근성 향상** 등의 기능이 그것이다.

첫째, 유권자의 투표참여율 제고는 실제 사례를 통해 확인할 수 있다. 2004년 미 대통령 선거에서 '전자투표기'가 종이 기반 광학스캐너기계가 놓친 투표를 발견해 2000년 선거보다 1백만 이상 투표자 수가 더 많았다는 MIT의 연구결과[12)]가 있다. 이러한 '분실 표' 뿐만 아니라 유권자의 투표참여율 자체도 매우 높일 수 있다. 대구공업대학교의 연구결과에 따르면,[13)] 일반적으로 마련되어 있는 투표소나 지정장소에서 PC를 이용하는 이전방식과 비교하면, 스마트폰으로 온라인 선거를 진행하는

11) Digital Voting with the use of Blockchain Technology - The Economist, Plymouth University

12) Friel, Brian (November 2006)Let The Recounts Begin, National Journal Archived June 19, 2005, at the Wayback Machine.

13) 내가 있는 곳이 곧 투표소! 온라인투표 서비스 http://blog.nec.go.kr/220953201059

경우, 투표율이 기존의 40%대에서 75.5%로 증가하여 거의 2배에 가까운 투표율 증가를 보였다.

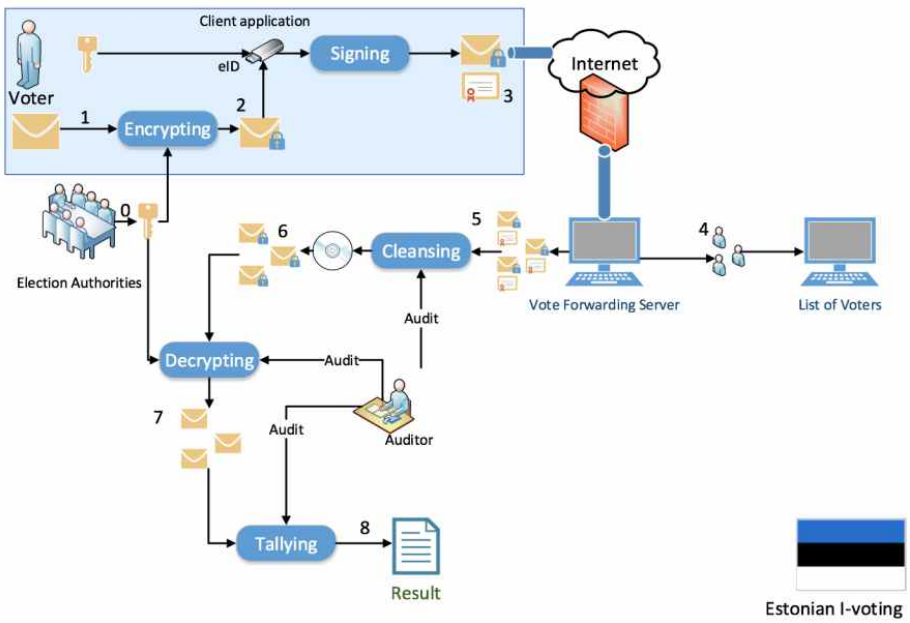
둘째, 개표의 신속성은 온라인투표시스템의 가장 큰 장점이라고 할 수 있다. 선거관리를 하는 사람들이 수작업으로 개표해야했던 이전의 선거 시스템과 달리 투표종료와 거의 동시에 집계되어 기존 선거 개표의 절반도 되지 않는 시간에 개표 결과를 알 수 있다.

셋째, 비용절감은 온라인투표시스템의 특성에서 나온다. 온라인 투표 시스템은 투표용지를 필요로 하지 않고, 개표하는 사람도 필요치 않는다. 실제로 2014년 서울시 맑은 아파트 2단계 사업 추진계획에 따르면 아파트 입주자 대표 선거에서 1가구 5천 원가량의 선거 위탁비용이 1000원도 되지 않을 것이라고 발표했다.

마지막으로 **장애 유권자의 접근성 향상**은 인터넷만 연결되어 있다면 다양한 기기를 통해 투표참여가 가능하다는 데에 있다. 심지어 에스토니아에서는 지금된 보안카드를 통해 카드 리더기에 카드를 삽입한 후 투표를 할 수도 있고, SIM카드가 해당 보안카드를 대신하기도 했다.

라. 온라인 투표 시스템의 구성

비교적 가장 오랜 기간 동안 온라인 투표 시스템을 사용해 온 에스토니아의 온라인 투표 시스템의 구성은 다음과 같다.



(그림 6) 에스토니아의 온라인 투표 시스템 구성도

자료 : Digital Voting with the use of Blockchain Technology

카드(key)를 통해 유권자가 투표소에 엑세스한 후 해당 사이트(투표사이트)에서 PIN번호를 입력해 본인확인을 받는다. 유권자로 확인되면, 4번까지 자신의 투표를 수정가능하다. 식별 카드가 없는 경우, 선거일 전일 휴대전화를 통한 인증을 마치면 된다. 이후 유권자가 투표를 완료하면, 투표 값은 publicly accessible vote를 통과해 투표결과 저장 서버에 전달되기까지 암호화되고, 투표기간이 종료되면 네트워크와 연결이 끊어진 개표서버로 전송된다. 이후 서버가 개표를 마치면 결과를 출력한다.

이러한 에스토니아의 시스템은 일반적인 온라인 투표 시스템의 구성을 모두 갖추고 있다. 유권자 확인, 투표, 암호화, 개표와 결과확인이 온라인 투표 시스템을 구성하는 요소라고 볼 수 있다.

2) 블록체인 방식을 활용한 온라인투표시스템의 기능과 구성

K-voting은 간편하게 투·개표를 진행할 수 있고 인터넷 및 통신망을 기반으로 하는 서비스이다. 온라인투표시스템은 통신상황이나 중앙 서버의 불의의 장애가 발생 할 수 있어 서비스를 사용할 때 선거인과 관리자의 숙지가 필수적이다. 또한 서버가 해킹 당해 투표에 대한 결과를 수정하거나 삭제 할 수 있어 무결성에 대한 이슈도 존재한다. 블록체인을 현재의 K-voting 시스템에 적용한다면, 중앙 서버에 의해 시스템이 구동되지 않기 때문에 한 개의 컴퓨터의 네트워크가 불안해도 다른 네트워크에 영향을 주지 않으므로 안정적인 선거 시스템을 운영할 수 있다. 또한 모든 유권자가 투표 결과에 대한 이력을 공유하기 때문에 해킹이 불가능해 무결성을 보장할 수 있다. 이러한 장점은 신뢰가 중요한 선거시스템에 활용할 수 있다.

온라인투표시스템에 블록체인이 도입된다는 것은 기존의 온라인투표시스템의 기능보다 더 많은 기능을 블록체인 온라인투표시스템이 해낼 수 있음을 의미한다. 블록체인은 기본적으로 공정성과 투명성, 확실성을 가지고 있다. 이에 더해 기존 온라인투표시스템의 한계점으로 지적되는 보안성 측면에 있어서 문제가 발생할 확률이 기존 시스템에 비해 매우 낮다.

이러한 개선점을 바탕으로 블록체인 방식을 활용한 온라인투표시스템의 기능과 구성에 대해 알아보고자 한다.

가. 블록체인 방식을 활용한 온라인투표시스템의 기능

블록체인 온라인투표시스템은 기존 온라인투표시스템의 기능을 모두 갖추고 있다. 여기서 이야기 하고 있는 온라인투표시스템의 기능은 유권자의 투표참여율 제고, 개표의 신속성, 비용 절감과 장애 유권자의 접근성 향상 등이다. 이러한 기능은 온라인을 기반으로 장소에 구애받지 않고 투표를 할 수 있다는 점에서 동일한 기능이기

때문이다.

이에 추가하여 블록체인 선거 시스템은 온라인투표시스템이 가지는 해킹을 통한 위변조의 위험성에서 비교적 자유롭다. 블록체인은 모든 거래가 모든 사용자에게 기록되는 '분산거래장부'를 특징으로 한다. 이런 블록체인의 특성이 해킹과 그로인한 위·변조 위험에서 기존의 온라인투표시스템보다 자유로울 수 있다.

신뢰 대상의 변경도 블록체인 온라인투표시스템의 기능 중 하나다. 중앙서버의 관리자가 존재하고 그를 전적으로 신뢰해야했던 기존 온라인투표시스템에 반해 유권자 모두가 투표 과정과 결과를 스스로 검증할 수 있다. 투표의 위변조가 불가능할 뿐만 아니라, 신뢰의 대상이 중앙서버의 관리자에서 시스템 그 자체로 옮겨간다. 이를 통해 투표 참여자들 사이에서 정책 결정사항에 대한 신뢰와 공감대 형성은 더 향상될 것으로 전망된다.

나. 블록체인 방식을 활용한 온라인투표시스템의 구성

블록체인 온라인투표시스템은 2가지 시스템으로 나뉜다. Private한 선거 시스템과 Public한 시스템으로 나뉘는데 이는 플랫폼을 기준으로 구분한다. 특정 선거 방식과 유권자의 구체적인 특성을 반영하도록 고안된 새로운 맞춤 전자투표 시스템은 Private 방식이다. 비트코인이나 이더리움과 같은 기존에 확립된 블록체인 시스템에서 전자투표 시스템을 만드는 것은 Public방식이다. Public 시스템을 이용할 경우, 블록체인의 보안성이 사용자 수에 비례한다는 점을 통해 소수의 유권자가 참여하는 선거에 대해 안전하게 사용할 수 있다. Private 시스템은 참여 기준, 범위, 공개여부를 제한할 수 있어 유권자가 아닌 사람들의 참여나 열람을 막을 수 있다.

다음은 두 가지 방식을 적용한 사례를 정리한 것이다.

① Public 방식 적용사례: 따복 공동체 주민제안공모사업 블록체인 투표(Blocko)

실제 정책선거과정에 블록체인 온라인투표시스템이 적용된 사례가 경기도의 따복 공동체 사례이다. 이 사례는 CoinStack이라는 블록체인 기반 시스템을 제공하는 업체 Blocko에서 담당해 어플리케이션 제작과 블록체인을 통한 온라인투표시스템을 제작했다. Blocko에 따르면 오프라인 투표자(주민대표 1인)와 온라인 투표(공동체 주민 9인) 모두 블록체인 시스템을 통해 집계하였다. 주민대표는 우선순위 방식으로, 공동체 주민은 1인 최대 6회의 '좋아요' 선택 방식으로 투표를 한다. 즉, 공동체주민 투표권자 9명의 지갑에 6원씩 넣어주고 1계좌당 1원씩만 '송금'할 수 있는 시스템인 것이다. 해당 투표권, 즉 6원의 잔고는 투표권자가 수령하게 되는 투표용지 내의 QR코드를 통해서만 주어진다. 해당 과정을 모두 거친 후 투표 집계는 단순히 각 공동체 사업안 계좌의 잔액이 가장 큰 것

을 채택한다. 815명의 오프라인 심사원과 7,335명의 구성원이 참여하는 시스템이기에 Public방식을 채택하였다.

② Private 방식 적용사례: FMV 블록체인 온라인투표시스템

FMV는 블록체인 온라인투표시스템을 제공하는 미국의 스타트업이다. Forbes[14]와 Nasdaq[15], Discovery[16]와 The Huffington Post[17] 등에서 블록체인 온라인투표시스템은 선거에 들어가는 비용을 획기적으로 줄이게 되었다. 그리고 더욱 공정하고 투명하면서 편리하고 빠른 선거가 가능할 것이라 평가받고 있다. FMV는 블록체인 온라인투표시스템에 있어서는 독보적인 언론 노출도를 자랑하며 계속해서 투자가 늘어나고 있다. 이 업체의 블록체인 온라인투표시스템은 가중치 부여 투표가 가능하다는 특징까지 가졌다[18]. 비트코인이나 이더리움과 같은 플랫폼을 이용하지 않고, 1인 1표와 가중치 투표 모두 가능하다. 독자적인 시스템을 구성하는 FMV는 Private 방식의 블록체인 온라인투표시스템이라고 할 수 있다. 기본적으로 블록체인 장부작성 방식과 거의 동일하게 작동한다는 것을 알 수 있다.[19]

이렇듯 블록체인 기반 온라인투표시스템은 기존의 온라인투표시스템의 맹점을 보완함과 동시에 온라인투표시스템 이상의 비용절감이 가능할 것으로 그 효과가 예상된다. 물론, 가까운 미래에는 블록체인을 활용한 투표가 국가적 규모 선거보다는 중소규모의 민간선거, 위탁선거에 활용될 가능성이 훨씬 높다고 본다. 아직까지 보안문제, 접근권한, 익명성 확보 방안에서 해결되지 않은 문제점이 남아 있어서 낙관적인 전망은 시기상조이다. 그리고 해당 투표결과에 대한 대중의 신뢰성을 확보하는 방안도 필요하다.

또한 블록체인 기술이라는 신기술이 도입되는 것이므로 고려해야할 요소가 많다. 범국가적 규모에서 도입하기 위해서는 헌법 원칙과 함께 다양한 법률과 제도를 고

---

14) https://www.forbes.com/sites/realspin/2016/08/30/block-the-vote-could-blockchain-technology-cybersecure-elections/#1cba0f802ab3 Block The Vote: Could Blockchain Technology Cybersecure Elections?(Forbes, Jackie Burns Koven)

15) http://www.nasdaq.com/article/four-ways-the-blockchain-will-make-the-world-a-better-place-cm757443 Four Ways the Blockchain Will Make the World a Better Place(Nasdaq, BitCoin Magazine)

16) https://newswatchtv.com/2016/06/10/tech-news-discovery-channel-follow-my-vote/ (Follow My Vote - A New Voting Software | NewsWatch Review, NewsWatchTelevision, Discovery video clip)

17) http://www.huffingtonpost.com/pradeep-aradhya/are-we-ready-for-a-global_b_9591580.html (Distributed Ledger Visible To All? Ready for Blockchain?, Pradeep Aradhya)

18) https://followmyvote.com/its-alive-follow-my-vote-launches-blockchain-voting-software-on-the-bitshares-blockchain/ (Follow my Vote 홈페이지)

19) https://followmyvote.com/infographics/blockchain-technology-breakdown-infographic/(Follow my Vote 홈페이지)

려해 블록체인 온라인투표시스템을 구축할 필요가 있다. 이러한 측면에서 블록체인 온라인투표시스템의 구축과 활용에는 난관이 많을 것으로 예측되고 있다[20]. 그럼에도 불구하고 블록체인 온라인투표시스템이 가지는 장점과 기능은 기존 온라인투표시스템의 단점을 보완할 수 있기 때문에 많은 곳에서 블록체인투표시스템이 개발되고 있는 중이다.

3) 블록체인 방식의 온라인투표시스템의 범위와 장점

블록체인 방식을 온라인투표시스템에 적용하면 블록체인에 투표권한을 기록, 저장하는 등 전자적 관리를 구현할 수 있다. 그리고 투표 여부나 집계 등에도 활용해 선거관리업무를 더 효율화 할 수 있다.

블록체인 온라인투표시스템이 가지는 장점은 다음과 같다.

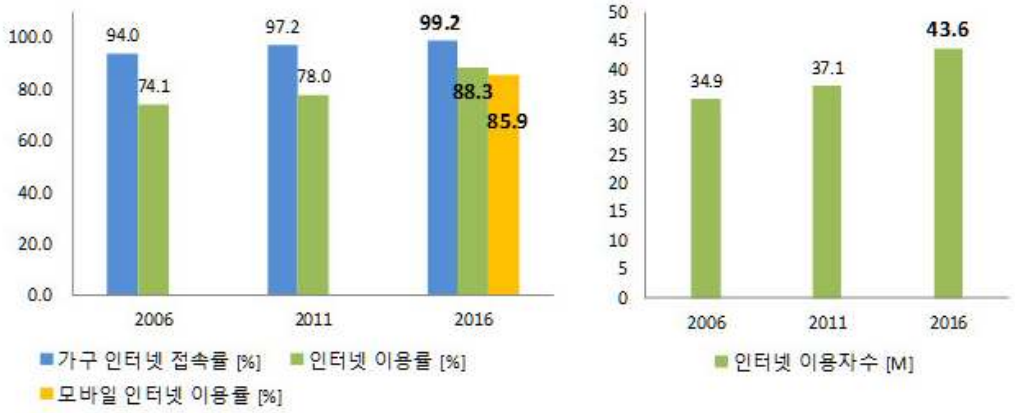
① 시간 및 비용 절감

블록체인 방식의 온라인투표시스템은 기존 투표에 비해 시간과 비용을 절약할 수 있는 장점이 있다. 온라인투표시스템에 블록체인 기술을 적용하면, 선거 프로세스를 간소화하여 기존의 선거 방식보다 빠르게 진행될 수 있기 때문이다. 복잡한 투표 프로세스를 블록체인에 등록하면, 자동화 처리가 가능하다. 기존의 투표방식은 개표관리자의 개표까지는 일정시간이 소요되지만, 블록체인 서버에 투표를 하게 되면 투표를 하고 조회까지 할 수 있어 특정 시간 이후에 발표되는 결과를 기다리지 않아도 된다. 뿐만 아니라 기존 해외여행자, 선교사, 미군 등 해외에 거주하는 유권자는 우편투표에 의존하였다. 그러나 블록체인 방식의 온라인 선거시스템을 활용하면, 투표를 등록, 수행하는 프로세스가 간소화 될 수 있다. 실제 2016년 미국 텍사스 주 자유당의 대선후보 선정과 유타 주 공화당의 대선후보 선정에 블록체인 방식의 온라인투표시스템을 적용한 결과, 투표 프로세스가 간소화되는 효과를 확인할 수 있었다.

투표 프로세스의 간소화로 인해 투표 비용 절감 효과도 예상할 수 있다. 블록체인 방식의 온라인 선거시스템을 통해 기존의 투표에서 사용되는 투표 및 개표 관리비용을 절감할 수 있다. 실제로 국내에서 시행된 경기도 따복공동체 주민 제안 공동사업을 위한 투표에서 블록체인 기술을 온라인 투표에 활용함에 따라 투표관리기구 운영 및 투표 결과 수집에 필요한 많은 비용을 절감하였다. 선거과정에서 요구되는 비용뿐만 아니라 초기에 블록체인 방식의 선거시스템을 구축하는

20) What if blockchain technology revolutionised voting? (European Union, 2016)

비용도 크지 않은 것으로 나타났다. 스마트폰 및 인터넷은 블록체인 방식의 온라인투표시스템을 적용하기 위한 최소한의 요구사항이지만 기존 장비를 이용할 수 있기 때문이다.



(그림 7) 2016년 인터넷 이용실태

자료 : 미래창조과학부

미래창조과학부의 '2016년 인터넷 이용실태조사'에 따르면 전체국민의 88.3%가 인터넷을 이용하고 있으며, 가구 인터넷 접속률은 99.2%로 거의 모든 가구에서 인터넷 접속이 가능하다고 밝혔다. 국민들의 스마트폰과 컴퓨터 보유율로 만 6세 이상의 국민의 85%가 보유하고 있다는 조사결과도 발표했다. 이렇듯 많은 국내 사용자들이 이미 인터넷과 스마트폰을 사용하고 있으므로 블록체인 방식의 온라인 선거시스템의 초기 인프라 구축비용을 절감할 수 있다. 기존의 온라인투표시스템과 달리 블록체인 방식의 온라인투표시스템은 중앙서버 및 보안 시스템의 구축비용 또한 절감할 수 있다.

② 시민 참여 증대

블록체인 방식의 온라인투표시스템을 통해 시민의 투표참여를 증대시킬 수 있다. 현재 시행되는 직접투표는 모든 사람이 참여하기 힘들지만, 투표방식에 블록체인을 활용하면 물리적 한계를 극복하고 더 많은 사람들의 정책결정과정에 참가가 가능해진다. 예를 들어, 여태까지 시행되어온 국내의 공동체 공모 사업에서는 공동체 대표자 1인이 결정하고 투표하는 반민주주의 방식이었다. 하지만 앞서 소개했던 블록체인 방식의 온라인 선거시스템을 통해 시행된 따복 공동체 주민제안 공모사업 심사에서는 공동체 대표 815명뿐만 아니라 구성원 7,335명도 사업내용을 학습하고, 직접 투표에 참여하였다. 이렇듯 투명하고 공정한 주민투표 시스템 방법으로 경기도에서 추진하는 사업에 주민의 직접 참여 및 투표가 가능하게 되었다. 이렇듯 블록체인 방식의 온라인 선거시스템은 구성원 전체가

각자 의사에 따라 투표할 수 있으므로 직접 민주주의 방식의 정치참여가 가능해진다.

③ 보안성 및 신뢰성 확보

온라인투표시스템에서는 투표의 비밀보장 및 개인정보 보안 문제, 투표권의 남용과 조작의 우려가 존재한다. 기존의 온라인투표시스템은 득표수 조작 및 해킹에 의한 공격 등 위험으로부터 완벽한 보안을 확보하기 어렵지만, 블록체인을 활용해 우려되는 보안문제를 해결 될 수 있다.

블록체인의 탈중앙화된 정보공유 시스템은 자체적으로 무결성 및 보안성의 확보가 가능하다. 기존의 온라인투표시스템은 중앙서버 및 중앙 데이터베이스에서 투표 값을 관리하고 처리하여, 투표에 대한 결과가 조작될 수 있는 위험성이 존재한다. 하지만 블록체인방식의 온라인투표시스템은 중앙서버 및 중앙 데이터베이스에 모든 투표 값을 보관하지 않고, P2P(Peer to Peer)방식으로 분산된 네트워크에서 투표에 참여하는 모든 사람들에게 공개되므로 투표가 투명하게 진행될 수 있다.

또한 블록체인방식의 온라인투표시스템에서는 투표 값이 다른 투표 값의 블록들과 해시 함수를 이용해 연결된 구조를 가진다. 그러므로 이를 임의로 수정하거나 누락시키는 것이 불가능하다. 해시함수란 컴퓨터 암호화 기술의 일종으로 임의 길이의 입력 값을 고정된 길이의 출력 값으로 바꾸는 알고리즘이다. 해시 함수는 데이터로부터 해시값을 구하는 한방향 계산은 쉽지만, 역계산은 매우 어렵기 때문에 어떤 방식으로도 입력 값을 추론하거나 계산할 수 없다. 즉 투표 내역들에 대한 블록의 연결은 현재 블록에 이전 블록의 해시값이 포함되는 구조로 위변조가 어려워 투표가 투명하게 진행될 수 있다.

블록체인을 활용해 득표수에 대한 조작뿐만 아니라 해킹으로부터도 안전성을 확보할 수 있다. 온라인 투표는 중앙 데이터베이스에서 모든 데이터를 한곳에 보관 및 관리를 하기 때문에 해커들이 단 하나의 데이터베이스에 침입하게 될 경우, 치명적인 피해가 발생하게 된다. 반면 블록체인 시스템은 해킹 난이도가 매우 높으며 수천 개의 컴퓨터를 동시에 해킹하는 데에 비용이 많이 들 뿐만 아니라 사실상 불가능하다. 그 외에도 공유된 투표 내역에 대해서 개인 혹은 타인의 행동을 통제하는 수단을 제공하기 위해 전자키와 전자서명을 통해 암호학적으로 보안성을 유지한다. 일부 시스템에 오류 또는 성능저하가 발생하더라도 전체 네트워크가 타격을 입을 가능성은 희박하여 안전성 높은 서비스를 제공할 수 있다.

이렇듯 블록체인이 적용된 온라인투표시스템은 투명성 및 보안성이 향상될 뿐만 아니라 실행된 투표이력은 영구보존이 가능하다. 그리고 투표 결과나 투표에

대한 투표 참여자들의 수용성이 증가하게 될 것이며, 투명성 있는 투표 결과로 선거관리기구에 대한 신뢰를 높일 수 있다.

3. 블록체인 방식의 온라인투표시스템 활용 해외사례

1) 미국

2016년 미국 텍사스 주 자유당의 대선후보 선출과 유타 주 공화당의 대선후보 선출과정에 블록체인 방식의 온라인투표시스템을 활용하였다. 블록체인 기술이 제공하는 편의 때문에 기존보다 더 많은 유타 공화당원이 투표권을 행사하기 위해 온라인으로 등록했다고 발표되었다. 기존에는 해외여행자, 선교사, 미군 등 해외에 있는 시민들은 우편으로 발송된 투표용지에 의존해야 했지만, 블록체인 활용 온라인 선거 덕분에 투표를 등록하고 수행하는 프로세스가 간소화되었다고 평가받고 있다. 두 사례에 대한 내용은 다음과 같다.

가. 유타주 공화당 대선후보 선정

2016년 미국 사상 최초로 주 정당에서 블록체인 방식의 온라인투표시스템을 활용한 인터넷 투표가 실시되었다. 온라인투표 솔루션을 제공하는 영국 업체 Smartmatic이 앤드- 투-앤드 (end-to-end) 암호화와 프라이빗(private) 블록체인을 사용해 온라인 투표 인프라를 제공하였다.

① 주요 이점

유타 주 주민들은 대부분 모르몬 교(예수그리스도 후기성도) 교인으로 많은 주민들이 선교 사업을 위해 대부분 해외에 거주하므로 우편 투표에 의존해 왔다. 하지만 실제 위치와 관계없이 스마트 폰, 태블릿 또는 PC / 노트북을 소유한 등록 유권자는 플랫폼에 액세스하여 손쉽게 온라인으로 투표 할 수 있었다. 또한 온라인 투표용지에서 각 후보자에 대한 정보에 관한 링크가 제공되어 기존 투표보다 더 쉽고 빠르게 정보를 얻을 수 있었다.

② 투표 방법

기존의 방식처럼 투표소를 방문하여 투표하거나, 공화당 홈페이지(utah.gop)에 접속하여 현지 시간으로 오전 7시부터 11시 사이에 방문하여 투표 할 수 있다. 유권자가 미리 온라인 투표 시스템에 등록하면, 시스템 선거 당일에 유권자의 휴대전화 또는 이메일로 고유한 PIN 코드를 송신해 준다. 투표는 당일 홈페이지에 접속하여 진행 할 수 있으며 영어와 스페인어로 지원된다.

1) AUTHENTICATION – 본인확인 단계

이름, 생년월일, PIN 코드를 입력 후 제출하여 확인 절차를 거친다. 유권자의 신분을 확인 후 간단한 소개와 인증 후 30분 이내 투표 할 수 있음을 안내한다.

2) CHOICES – 선택

후보자들의 이름과 링크가 표시되어 있다. 링크를 통해 후보자의 정보를 확인 할 수 있고, 한 명의 후보자를 선택 할 수 있다.

3) VOTING – 투표

2)단계에서 자신이 선택한 후보자를 확인할 수 있다. 선택을 변경하고 싶다면 뒤로 가기(BACK) 버튼을 통해 선택을 변경 할 수 있다. 선택한 후보가 맞는다면 투표하기(Cast Vote) 버튼을 눌러 투표를 완료한다.

4) 개표

투표가 완료된다면 투표 확인증(Voter Receipt)이 발급된다. 투표 확인증에는 자신이 투표한 후보의 이름과, 투표 확인증 번호가 제공된다.

5) 검표

모든 투표가 종료되면 유권자들은 투표 확인증 번호를 통해 공개 게시판에서 자신의 투표가 제대로 반영되었는지 확인 할 수 있다.

③ 결과

공화당은 80,000달러를 지출하여 Smartmatic과 계약 했고, 총 150,000 달러를 사용하여 온라인 투표를 진행하였다. 총 59,000명의 유타 공화당원이 온라인으로 등록하였고, 온라인 투표에 등록한 유권자의 90%가 코커스(caucus)에 참여하였다.

관계당국은 투표 당일 유권자의 IDN이 확인되지 않아 온라인 투표에 응한 40,000 명의 유타주 주민 중 약 10,000 명이 인증 단계에서 어려움을 겪었다고 밝혔다. 대부분의 유권자들이 PIN 코드를 스팸 메시지 또는 스펨 메일로 수신하였거나, 사전 등록 단계에서 등록이 제대로 되지 않았지만 완료되었다고 생각한 문제로 밝혀졌다.

④ 쟁점 및 해결과제

온라인 투표의 위험과 단점으로 민간 기업에게 투표관리 및 운영을 맡기는 문제가 제기되었다. 라인 투표를 통해 모든 종류의 개인 정보 침해가 일어 날 수 있다는 논란도 제기되었다. 기존의 투표소 부스에서 이루어지는 투표는 유권자 혼자 들어가서 투표한다. 그러므로 자신의 투표내용을 증명하거나 투표소가 외부와 단절되어 있기 때문에 투표 비밀이 보장된다. 그러나 온라인 투표는 화면을 공유하거나 투표 확인증을 통해 나의 투표 결과를 타인에게 증명이 가능함으로써 뇌물을 받거나 투표를 강요하는 행위가 더 쉽다는 의견이 나오기도 했다.

보안 문제 또한 논란이 되었다. 투표가 완료되면, 앤드- 투-앤드(end-to-end) 암호화와 프라이빗(private) 블록체인을 사용하기 때문에 발생 할 수 있는 모든 결과의 불일치와 오류가 모니터링 되지만, 투표하는 과정에서 일어날 수 있는 보안 문제가 이번 투표에서 지적되었다. 유권자들이 투표에 사용하는 개인 기기들이 대부분 완벽한 보안을 갖추지 못하기 때문에, 사람들이 투표하는 과정은 멀웨어(Malware)[21] 및 원격 제어에 매우 취약하다.

나. 텍사스 주 자유당 대선 후보 선출

텍사스 자유당은 Blockchain Technologies Corporation(BTC)의 블록체인 기반 투표 시스템을 사용하여 회장, 부회장, 비서 및 재무를 포함한 250 명의 대의원과 100명의 대안 후보를 선출하였다.

① 주요 이점

물리적 증거를 얻기 위해 종이 투표용지를 그대로 사용하여 신뢰성을 높였다. 블록체인 기반의 기록에는 타임 스탬프(Time stamp)[22]가 찍혀 서명되어 있기 때문에 투표 후 조작이 불가능하다. 투표 결과의 스냅 샷은 도표화 된 시점에 즉시 블록체인에 업로드 되어 투명하고 독립적으로 검증 가능한 이력 추적이 가능하다.

---

21) 바이러스나 트로이 목마와 같이 시스템에 해를 입히거나 시스템을 방해하기 위해 특별히 설계된 소프트웨어, 또는 데이터·컴퓨터·네트워크를 위험에 노출시킬 수 있는 코드. 악성 소프트웨어(malicious software), 또는 악성 코드(malicious code)에서 나온 말로, 남에게 피해를 입히기 위해 개발된 소프트웨어를 의미한다.

22) 타임 스탬프(Time stamp) : 어느 시점에 데이터가 존재했다는 사실을 증명하기 위하여 특정 위치에 표시하는 시각. 공통적으로 참고하는 시각에 대해 시간의 기점을 표시하는 시간 변위 매개 변수이다.

② 투표 방법

기존의 텍사스 자유당은 주정부 사무소 후보자 선출, 자유당 전국 대회 대표 후보 선출, 주 전역 임원 후보자 선출 및 주 자유당 집행위원회 구성원 60명이 선출되었으며 주 상원 의원에 선거구별로 투표가 실시되었다.

각 후보자는 대회장에서 지명되었으므로 대회 자체에서 투표용지를 설계하고 인쇄해야했다. 하나의 투표용지에는 83 명의 후보자가 있었고, 전국 대회에 71 명을 선출하기 위해 2 차례의 승인이 필요했다.

1) 투표

현장에서 지명 된 후보자 이름을 특수 투표용지에 인쇄, 종이 투표한다.

2) 개표

고속 스캐너를 사용해 OMR 투표용지를 스캔한다. 모든 투표용지는 플로린 코인에 기록됩니다. 투표용지에 포함 된 해시 이미지와 투표 결과는 타임스탬프 및 서명 과 함께 블록체인에 업로드한다.

3) 검표

Blockchain Technologies Corporation(BTC)은 https://voteleaks.org/ 페이지를 통해 투표 관련 블록체인 데이터베이스에 기록된 투표에 관한 문의를 할 수 있다. 이름, 연락처, 투표 장소, 투표소, 날짜와 시간과 내용을 작성하고 기재된 연락처로 답변 받을 수 있다.

사건보고 시스템을 통해 제출된 모든 문의 글은 전부 공개되어 블록체인에 업로드 되고, 수정, 삭제, 영구적으로 기록되어 누구나 확인 할 수 있다.

③ 결과

현재 미국에서 14개 주에서는 15년 이상 된 투표 기기 시스템을 이용하여 서거를 실시하고 있다. 그리고 43개 주에서는 최소 10년 이상 된 투표 기기 시스템을 사용하고 있어서 많은 유지 보수비용을 감당해야 했다. 블록체인 기반의 투표 기기를 도입함으로써 더 낮은 비용으로 더 투명한 선거가 이루어졌다.

또한 기존의 투표 방식을 보존하여 유권자의 혼란을 막을 수 있었으며, 물리적인 증거와 더불어 투표용지 기록 백업을 통해 투명하고 독립적으로 검증 할

수 있어 신뢰성을 높였다.

2) 스페인

2014년 돌풍을 일으킨 스페인 신생 정당 포데모스(podemos)는 시민 참여를 촉진하고 공정한 투표 시스템 구현을 위해 블록체인을 적용한 '아고라 투표(Agora Voting)'시스템을 만들었다. 포데모스는 당 내 의사 결정 시스템 및 온라인 투표에 이 시스템을 도입했다. 당 내 집행부 26명은 모두 아고라 투표(Agora Voting)를 통해 온라인 투표로 선출되었으며 이 투표에는 5만 5000명이 참여했다. 아고라 투표(Agora Voting)는 현재 nVotes라고 불리며 사용자는 웹을 통해 편리하게 유권자 등록 및 투표를 진행 할 수 있다.

① 주요 이점

아고라 투표(Agora Voting)는 소프트웨어 투표 시스템으로 다양한 개인정보보호 및 보안 수준을 제공하고, 선택 사항 위임, 여러 유형의 질문, 다중 인증 시스템 및 고급 API와 같은 여러 사례에 적용 할 수 있다. 포데모스 정당은 아고라 투표(Agora Voting)를 통한 검토가 가능하고, 투명하며, 완전하게 입증 가능한 전자 선거를 진행했다.

또한, 아고라 투표(Agora Voting)를 이용하면 100만개 이상의 조직에서 200만 명 이상의 유권자가 온라인으로 투표 할 수 있다. 컴퓨터, 태블릿 및 스마트폰에서 이용 가능하기 때문에 쉽게 투표할 수 있으며 포데모스 정당은 정당 예비 선거를 수행할 때도 이 시스템을 이용한다. 아래는 아고라 투표(Agora Voting)의 특징을 정리한 표이다.

[표 7] 아고라 투표 특징

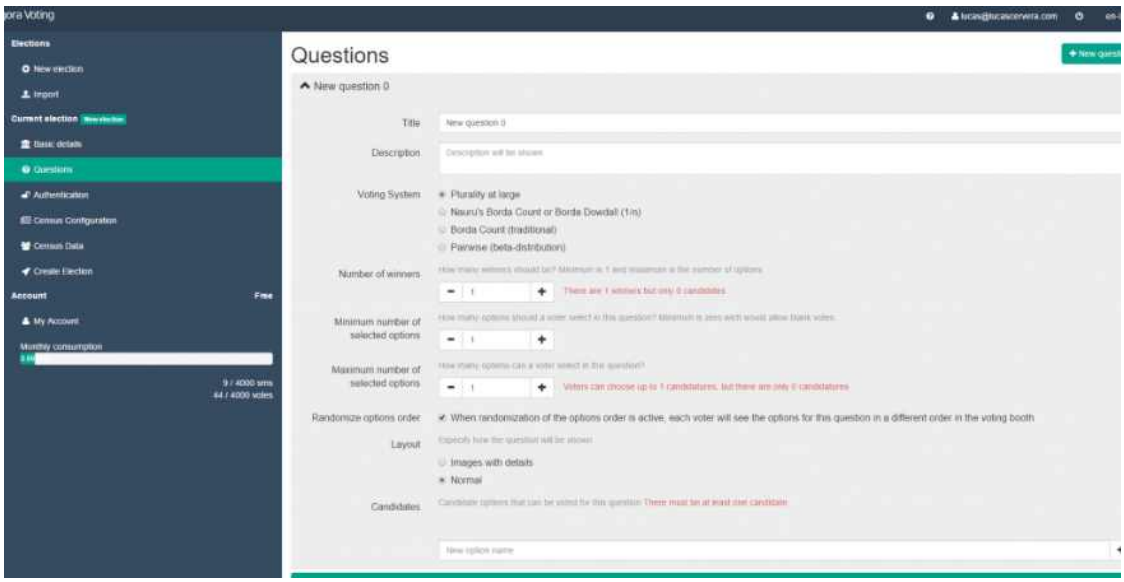
특징	내용
관리적 특징	**유권자 인증 및 허가** 아고라 보팅은 ID카드, SMS 인증, 전자메일 인증등 여러 옵션을 통해 유권자의 본인 확인 실시
	안전한 프라이빗 투표 투표용지는 웹 브라우저에서 암호화
	검증가능하고 투명한 결과 블록체인을 통해 결과를 검증할 수 있으며 투명하게 공개
	다양한 장치에서 이용가능 사용자는 노트북, 개인용 PC, 모바일 기기 등 다양한 장치에서 투표 가능

기술적 특징	**확장성** 다양한 투표에서 이용 할 수 있어 뛰어난 확장성을 가지며 모듈형 소프트웨어로 설계되어 있어 외부 인증 도구 등 다른 툴과 쉽게 통합 가능
	편의성 웹 기반의 인터페이스로 편리하게 투표 가능
	보안성 관리, 검증 메커니즘이 있으며 투표 내용을 변경하려면 많은 사람들이 동의가 필요하기 때문에 불가능

자료 : Agora-voting, http://tools.dcentproject.eu/pdfs/electronic-voting.pdf

② 투표 방법

nVotes(아고라 투표)의 사용자 유형에는 전체 선거과정을 관리하는 관리자와 투표를 할 수 있는 유권자로 나뉜다. 관리자는 실제 선거가 시작되면 변경사항을 적용 할 수 없으므로 모의 선거를 진행 후 실제 선거에 도입할 수 있다. 모의 선거 에서는 데이터가 유권자등록 양식, 투표 부스, 집계 결과 페이지 등에 올바르게 표시되는지 확인하고 유권자 등록 및 전체 선거과정에 대한 시뮬레이션을 할 수 있다. 모의 선거가 검증 되면 관리자는 실제 선거 만들기 버튼을 클릭하여 실제 선거를 만들 수 있으며 원하는 유권자 범위를 선택 가능하다. 사용자는 이메일 및 SMS를 통해 인증과정을 거쳐 투표를 할 수 있다. 아래 그림은 nVotes의 대시보드 및 투표 방법에 대한 상세한 설명이다.



(그림 8) nVotes의 Dashboard

자료 : https://nvotes.com/doc/en/

1) 유권자 등록

오프라인 유권자 등록, 온라인 유권자 등록 모두 가능하다.

2) 유권자 본인 확인

여러 인증 및 서명 메커니즘을 사용할 수 있으며 때로는 둘 이상을 동시에 사용한다. 하드웨어 토큰인 FIDO U2F 토큰을 표준으로 사용하며, 사용이 간편하며 이중 인증 및 강력한 암호화 보안 이점을 모두 제공한다. 우편으로 자격 증명을 포함한 인증 코드 증명서를 배달 받거나, 정부 발급 디지털 인증서 또는 스마트 카드, 전자 ID 카드를 사용한다.

3) 투표

클라이언트 측 암호화를 사용하면 투표용지가 서버를 거치지 않고 모든 것이 유권자 컴퓨터에서 처리된다. 투표소는 여러 개의 잠금 장치와 키 암호로 보호되어 각 선거관리위원회의 참여를 요구한다. 투표를 보내기 전에 봉인 된 후, 투표 확인증이 클라이언트에서 생성된다. 투표지 찾기 도구는 나중에 투표 확인을 위해 사용할 수 있다. 투표용지를 보내고 기록하기 전에 유권자는 제 3 자 컴퓨터에서 투표용지가 올바르게 부호화 되고 암호화 되었는지를 수학적으로 확인할 수 있다.

4) 개표

서버는 자격 증명을 확인하고 투표를 확인합니다. 확인이 완료 되면 유권자의 컴퓨터에서 암호화 된 투표용지를 디지털 투표함에 보내고, 투표는 사용자 컴퓨터에서 암호화되었고 해독은 독립된 선거관리위원회 참여가 필요하기 때문에 선거관리인조차도 열 수 없다. 유효한 투표용지는 디지털 투표함에서 수집되고 추출되어 선거관리위원회에 보내진다. 재암호화, 믹싱, 셔플링 등 프로세스를 실행해 재암호화, 익명화한다. 재암호화와 셔플 증빙을 확인해 익명의 투표 결과 세트가 초기의 투표용지 세트와 동일하다는 것 또한 검증한다. 투표가 각 선거관리위원회에 의해 항상 익명으로 처리되면, 모든 선거관리위원회는 투표용지를 공동으로 해독, 집계 메커니즘을 적용하여 투표 결과를 산출한다.

5) 검표

선거 당국은 투표지 해독에 대한 검증 가능한 증거를 제공하고, 모든 정보는 하나의 파일에 온라인으로 게시되어 누구나 다운로드하여 사용할 수 있으므로 전체 프로세스를 독립적으로 확인할 수 있다.

③ 결과

2014년 3월 설립 된 스페인 신생정당 포데모스는 아고라 투표(Agora Voting) 온라인 투표 플랫폼을 사용해 네트워크, 디지털 전략을 성공시켰고, 창당 100일 만에 2014년 5월 유럽 의회선거에서 총 1,200,000표를 득표하며 총 54석 중 5석을 석권하며 '네트워크로 연결 된 대중의 힘'이라는 현대 정치의 전혀 새로운 성공사례로 기록되었다.

3) 우크라이나

우크라이나는 정부 차원에서 블록체인 기반의 투표 시스템을 개발 중이다. 개발도상국 민주주의 국가인 우크라이나는 블록체인 기반의 투표 시스템을 도입하는 첫 번째 국가이다. 우크라이나 정부는 청원 및 정책 투표를 위한 블록체인 기반의 선거 플랫폼(Blockchain-based election platform)을 사용하겠다는 계획을 발표[23]하고 여러 단계의 절차를 블록체인 기반의 스마트 컨트랙트에 적용한다.

① 주요 이점

우크라이나의 블록체인 기반 투표 프로토타입인 E-vox는 이더리움 기반의 스마트 계약을 활용했다. 기존의 컬러드 코인을 활용해 블록체인 기반 투표 시스템을 구현하는 것과 달리 스마트 계약을 활용하기 때문에 투표 종료 즉시, 법안이 개정 될 수 있어 비정부 이니셔티브라고 불리기도 한다.

② 투표 방법

현재 E-Vox는 예비 선거, 전자 탄원서, 지역 전자 투표 등 중·소지역규모에 맞춰 개발하고 있다.

1) 유권자 확인 유권자 부정투표를 방지하기 위해 정부 발행 디지털 서명 및 BankIDs라는 우크라이나에서 합법적으로 인식되는 디지털 서명을 통해 통합적으로 유권자 신원 확인한다. 투표 이외 청원서나 기타 여론조사는 전화번호를 통해서 확인한다. 2) 투표 직접 투표를 하기 위해 상점에 있는 지불 키오스크를 통해서 투표를 한다. 투표를 할 때, 유권자 확인을 했을 때 사용했던 합법적으로 인정되는 디지털 서명으로 서명을 하여 블록체인 네트워크에 투표에 대한 정보를 전송한다.

23) Ukraine Government Plans to Trial Ethereum Blockchain-Based Election Platform, Bitcoin Magazine, 2016.02.16

③ 결과

2016년 6월 E-vox는 우크라이나 지역 협의회인 NaRada를 위한 전자 투표 시스템에 대한 개념 증명 단계이다. 현재 지역 의회에 무료로 오픈소스를 제공하여 우크라이나 법률의 요구 사항과 필요한 경우 지방 의회의 대표들이 구체적인 사항을 시스템에 적용하고 있다. 또 우크라이나의 Balta 시의회는 E-vox:NaRada를 설치하여 블록체인 기반 투표 시스템을 도입하는 최초의 시의회가 되었다. 블록체인 기반 투표 시스템은 의회 의사결정과정에서 분산적이고 투명하게 접근 가능한 시스템을 구축할 수 있었다. 투표 과정 또는 의사 결정과정에서 제 3자의 영향을 최소화하거나 제거할 수 있게 되었다.

4) 에스토니아

에스토니아는 전 세계적으로 40여 개국이 추진하고 있는 전자투표 사례 가운데 가장 선진적인 인터넷 방식의 투표를 시행하고 있는 국가이다. 총 인구 134만 명의 작은 규모를 이용해 정부의 정책 관리나 추진에 있어서 다른 국가에 비해 용이하다는 특수성이 존재 한다. 인터넷 투표 뿐만 아니라 다양한 전자민주주의 프로그램을 시행하면서 전 세계적으로 주목을 받고 있는 전자민주주의 강국이다.

에스토니아는 1999년부터 인터넷을 통해 투표를 할 수 있는 웹 기반의 투표시스템을 구축했고 사전 투표로도 인터넷 투표가 가능하게 되었다. 기존에 인터넷 투표는 정보 격차에 따라 젊은 층의 유권자만 참여할 가능성이 있기 때문에 평등 선거에 위배된다는 문제점이 제기되었다. 그리고 해킹에 대한 문제 그리고 비밀선거에 대한 원칙을 위배할 수 있다는 등 문제점이 제기되었지만 에스토니아는 높은 정보화 수준으로 디지털에 익숙하지 않은 유권자가 다른 국가에 비해 상대적으로 적다. 그러므로 앞에서 제기된 문제에도 불구하고 투표율 상승과 민주주의운영에 미치는 긍정적 효과로 인해 도입이 진행되고 있다.

에스토니아는 전국민 ID 카드 프로젝트를 통해 유권자의 대부분이 디지털 인증서가 들어 있는 ID 카드를 소유하고 있기 때문에 블록체인 기반의 투표 시스템을 구축할 수 있게 되었다.

① 주요 이점

에스토니아의 투표 서비스는 두 개의 별개의 블록체인을 사용한다. 하나는 유권자가 등록을 했는지, 투표를 안 한 유권자를 확인하기 위한 트랜잭션을 기록하고 다른 하나는 투표 내용(어떤 정당에 투표를 했는지)이 포함되어 있는 블록체인이다. 이러한 이유로 투표를 했을 때 유권자의 익명성을 보장할 수 있다.

② 투표 방법

에스토니아 시민들은 ID 카드로 블록체인을 활용한 전자투표를 이용해 세계 어느 곳에서도 로그인 후 투표가 가능하다.

1) 유권자 본인확인 유권자의 ID 카드를 리더기에 투입하여 웹사이트에 접근하여 투표 할 자격이 있는지 확인 한다. 유권자의 컴퓨터에 카드 리더기가 없다면 휴대폰으로 접근 가능

이때, 트랜잭션은 유권자가 등록 할 때 생성되고 정부 마이너가 투표 권한을 생성할 때 생성된다.

2) 투표

웹사이트를 통해 유권자는 투표한다. 투표 일 4일 전까지 투표를 하거나 투표한 것을 바꿀 수 있다.

블록체인 기반의 투표 네트워크는 전국단위, 선거구 단위 및 지역단위의 세 가지 추상적인 계층으로 나뉜다. 지역단위는 전국의 모든 디지털 투표소를 포함하여 각각은 선거구 노드와 연관된다. 지역 노드는 오직 연관된 선거구 노드의 아래에 있는 지역 노드와 선거구 노드끼리만 통신한다. 선거구 단위는 선거구 단계에 있는 것으로 여겨지는 모든 노드를 포함하여 서로의 위치에 따른 하위 집합으로 연결된다. 국가 단위는 위치에 얽매이지 않는 노드의 집합이고 트랜잭션을 채굴하고 블록체인에 블록을 추가한다. 모든 선거구 노드는 국가 노드와 통신할 수 있고 국가 노드는 서로 통신할 수 있다.

3) 검표 및 개표

투표는 공개적으로 접근 가능한 투표 포워딩 서버에서 온라인 투표 기간이 끝날 때까지 암호화되고 저장되는 투표 저장 서버로 옮겨간다. 후에 서버에서 모든 식별가능한 정보가 삭제되고 모든 네트워크로부터 단절된 투표 카운팅 서버로 DVD에 의해 운반된다. 투표 카운팅 서버에서는 투표를 복호화하고 카운트를 한 뒤 결과를 집계한다. 이러한 모든 과정은 로그화 되고 검표작업은 감시 된다.

안전한 투표를 위해 공개키와 개인키에 기반한 암호화 방식을 사용하여 데이터가 블록체인 내에서 분리되어 있는 구조이다. 선거구 노드가 키 쌍을 생성하여 공개키는 투표소 노드에 배포가 되고 공개키를 사용하여 해당 투표소의 모든 투표를 암호화한다. 그 후 데이터는 블록체인 내에 암호화 형식으로 저장되어 투표 마감 시간이 끝나기 전에 투표 데이터를 해독하는 것을 방지한다. 투표 마감시간이 지나면 선거구 노드 내의 소프트웨어는 블록체인 네트워크가 데이터를 해독하도록 하기 위해 개인키를 발행하여 득표수를 집계할 수 있다.

③ 결과

에스토니아의 블록체인 기반의 전자투표는 선거 보안에서 유일하고 중요한 사례 연구를 대표한다. 2007년 국회의원 선거 전자투표율이 5.5%에 불과했지만 2011년 25%까지 높아졌다. 또한 유럽 의회 선거에서는 에스토니아 1/3의 투표자가 98개국에서 블록체인 전자투표를 통해 선거를 참여했다.

④ 쟁점사항

기존의 에스토니아 I-voting 시스템에서 밝혀진 잠재적 악의성 공격을 막기 위해 공격 매개체의 크기를 최소화하는 서비스와 시스템을 보완하기 위해 블록체인 기반의 전자 투표 시스템을 설계하였다. 블록체인의 51% 공격은 연구팀이 제안한 설계에 잠재적인 위협이 된다. 누군가가 이론적으로 디지털 투표 마이닝 해시 비율의 대부분을 제어하여 공용 장부를 조작할 수 있도록 이끄는 것에 대한 위협이 존재하지만 연구팀은 네트워크에 연결되는 노드의 위치와 사람들의 위치를 확인하고 추적하는 보안을 강화하였다.

제 3 장 블록-체인 방식의 온라인투표시스템 도입을 위한 해결 과제

대부분의 민주주의 국가에서 선거는 보통, 평등, 직접, 비밀, 자유선거 다섯 가지 기본원칙을 따르고 있다. 보통선거는 일정한 나이가 된 모든 국민에게 선거권을 주는 원칙으로 우리나라는 만 19세 이상의 성인이면 누구나 선거에 참여할 수 있다. 평등선거는 신분이나 재산, 성별, 학력 등 조건에 관계없이 한 사람이 한 표씩 투표할 수 있는 원칙이다(one man, one vote). 직접 선거는 다른 사람이 대신 투표 할 수 없고 자신이 직접 투표를 해야 한다는 원칙으로 투표소에서 본인 여부를 확인하고 투표용지를 배부하는 방식이 직접선거의 원칙을 따르고 있는 사례이다. 마지막으로 비밀선거는 자신이 어떤 후보를 선택했는지 비밀이 보장되어야 하는 원칙이다.

본 장에서는 선거의 다섯 가지 원칙을 기반으로 제도적, 기술적인 쟁점사항을 도출하여 신뢰할 수 있는 블록체인 방식의 온라인투표시스템을 도입을 하고자 한다.

1. 제도적 현황 및 이슈

전자투표는 90년대 중반부터 세계 주요 국가들이 도입을 하고 있으며, 현재는 약 50여 개국이 공직선거에 전자투표를 도입하여 활용하고 있다. 전자투표를 종이투표제도의 전자화로 이해할 경우, '종이투표(서면)'란 개념 속에 전자문서가 포함될 수 있는가 따라서 현행법상 전자투표가 허용되는가 하는 점이 먼저 문제된다. 만일 종이투표의 개념 속에 전자문서가 포함된다고 본다면, 전자거래기본법 제4조에서 전자문서에 서면으로서의 효력을 인정하고 있어 관련법률 개정 없이도 전자투표는 가능하게 될 것이다. 그리고 종이투표제도에서 말하는 서면에는 전자서면이 포함되지 않는다고 해석할 경우, 전자투표제도를 도입하기 위해서는 별도의 입법이 요구되게 될 것이다.

그러므로 이번 장에서는 온라인투표시스템을 공직 선거에 활용하는 경우, 발생할 수 있는 쟁점사항을 도출해 보기 위하여 국내의 제도적 현황을 분석해 보고, 이슈를 정리하고자 한다.

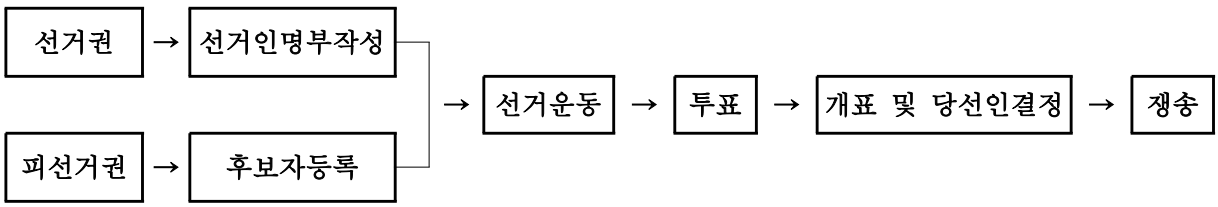
가. 선거 관련 국내 제도 현황

현재 국내법에서 선거와 관련한 법은 공직선거법, 정당법, 정치자금법, 선거관리위원회법, 공직선거관련규칙(당내경선 위탁사무 관리규칙, 선거방송토론위원회의 구성 및 운영에 관한 규칙, 인터넷선거보도심의위원회의 구성 및 운영에 관한

규칙), 주민투표법, 주민소환에 관한법률, 지방교육자치에 관한 법률, 국민투표법, 국가공무원법 등이 있다.

① 제도적 측면의 선거 절차

- 선거 절차



선거관리위원회는 선거를 치르기 위해 선거권을 가진 자를 확인·공증하고 선거인의 범위를 형식적으로 확정하는 명부로써 구·시·군의 장은 선거일전 일정시기가 되면 투표구별로 선거인을 작성해야 한다. 작성된 선거인 명부는 선거권자가 해당 선거에서 투표할 권리를 가지고 있는 가를 확인하고 선거인의 투표여부를 확인·관리를 하기 위한 용도로 활용한다.

후보자 등록은 후보자가 되고자 하는 자나 정당은 법정서류를 통해 관할선거구위원회에 후보자등록을 신청하고 피선거권 자격을 조사한 후 등록을 수리하면 후보자의 신분을 갖게 된다. 후보자가 되기 위해서는 피선거권을 보유해야 하고, 정당 또는 선거권자의 추천을 받아야 하며, 기탁금을 납부하고 후보자등록 제한사항에 해당되지 않아야 한다.

위의 모든 절차가 끝나면 선거운동 후 투표를 한 후 개표를 한다. 이후 대통령선거 및 국회의원선거의 효력에 관해 이의가 있는 선거인·정당 또는 후보자는 선거일부터 30일 이내에 해당 선거구선거관리위원회위원장을 피고로 하여 대법원에 선거소송을 제기하는 쟁송을 할 수 있다.

② 제도적 측면의 투표 유형

선거인은 직접 또는 우편의 방법으로 투표할 수 있다. 투표의 유형으로는 일반 선거인의 투표, 거소투표, 선상투표, 사전투표 등의 방법이 존재한다. 먼저 일반 선거인의 투표는 투표시간은 오전 6시부터 오후 6시(보궐선거 시에는 오후 8시)이고 투표소에서 대기하고 있는 선거인에게는 번호표를 부여하여 투표를 한 후 닫는다. 선거인이 투표를 하기 위해서는 주민등록증 또는 사진이 붙어있는 신분증명서를 제시하여 본인임을 확인하고 서명이나 날인을 하여 투표용지를 수령한다. 이 때 본인 확인이 되지 않은 선거인에게는 투표용지를 교부해서는 안된다. 투표관리관은 투표용지에 일련번호를 날인하여 교부를 한다. 선거인은 투표용지를 받은 후 기표소에 들어가 1인의 후보자를 선택하여 투표용지의 해당 란에 기표한 후 그 자리에서 다른 사람에게 보이지 않도록 접어 투표함에 넣으면 투표 절차는 끝난다. 이때 투표용지가 훼손되거나 오손되어도 투표용지를 재교부하지 않는다.

제155조(투표시간) ① 투표소는 선거일 오전 6시에 열고 오후 6시(보궐선거등에 있어서는 오후 8시)에 닫는다. 다만, 마감할 때에 투표소에서 투표하기 위하여 대기하고 있는 선거인에게는 번호표를 부여하여 투표하게 한 후에 닫아야 한다.<개정 2004.3.12>

② 사전투표소는 사전투표기간 중 매일 오전 6시에 열고 오후 6시에 닫는다. 이 경우 제1항 단서의 규정은 사전투표소에 이를 준용한다.<개정 2012.10.2, 2014.1.17, 2014.2.13>

③ 투표를 개시하는 때에는 투표관리관은 투표함 및 기표소내외의 이상유무에 관하여 검사하여야 하며, 이에는 투표참관인이 참관하여야 한다. 다만, 투표개시시각까지 투표참관인이 참석하지 아니한 때에는 최초로 투표하러 온 선거인으로 하여금 참관하게 하여야 한다.<개정 2005.8.4>

④ 사전투표소에서 투표를 개시하는 때에는 사전투표관리관은 사전투표함 및 기표소내외의 이상유무에 관하여 검사하여야 하며, 이에는 사전투표참관인이 참관하여야 한다. 다만, 사전투표개시시각까지 사전투표참관인이 참석하지 아니한 때에는 최초로 투표하러 온 선거인으로 하여금 참관하게 하여야 한다.<개정 2005.8.4, 2010.1.25, 2014.1.17>

⑤ 사전투표·거소투표 및 선상투표는 선거일 오후 6시(보궐선거등에 있어서는 오후 8시)까지 관할구·시·군선거관리위원회에 도착되어야 한다.<개정 2004.3.12., 2014.1.17>

제157조(투표용지수령 및 기표절차<개정 2011.7.28>) ① 선거인은 자신이 투표소에 가서 투표참관인의 참관 하에 주민등록증(주민등록증이 없는 경우에는 관공서 또는 공공기관이 발행한 증명서로서 사진이 첩부되어 본인임을 확인할 수 있는 여권·운전면허증·공무원증 또는 중앙선거관리위원회규칙으로 정하는 신분증명서를 말한다. 이하 "신분증명서"라 한다)을 제시하고 본인임을 확인받은 후 선거인명부에 서명이나 날인 또는 무인하고 투표용지를 받아야 한다.<개정 2011.7.28>

② 투표관리관은 선거일에 선거인에게 투표용지를 교부하는 때에는 사인날인란에 사인을 날인한 후 선거인이 보는 앞에서 일련번호지를 떼어서 교부하되, 필요하다고 인정되는 때에는 100매 이내의 범위안에서 그 사인을 미리 날인해 놓은 후 이를 교부할 수 있다.<개정 1998.4.30, 2004.3.12, 2005.8.4>

③ 투표관리관은 신분증명서를 제시하지 아니한 선거인에게 투표용지를 교부하여서는 아니된다.<개정 2005.8.4>

④ 선거인은 투표용지를 받은 후 기표소에 들어가 투표용지에 1인의 후보자(비례대표국회의원선거와 비례대표지방의회의원선거에 있어서는 하나의 정당을 말한다)를 선택하여 투표용지의 해당 란에 기표한 후 그 자리에서 기표내용이 다른 사람에게 보이지 아니하게 접어 투표참관인의 앞에서 투표함에 넣어야 한다.<개정 2002.3.7, 2004.3.12, 2005.8.4>

⑤ 투표용지를 교부받은 후 그 선거인에게 책임이 있는 사유로 훼손 또는 오손된 때에는 다시 이를 교부하지 아니한다.

⑥ 선거인은 투표소의 질서를 해하지 아니하는 범위 안에서 초등학생 이하의 어린이와 함께 투표소(초등학생인 어린이의 경우에는 기표소를 제외한다)안에 출입할 수 있으며, 시각 또는 신체의 장애로 인하여 자신이 기표할 수 없는 선거인은 그 가족 또는 본인이 지명한 2인을 동반하여 투표를 보조하게 할 수 있다.<개정 2000.2.16, 2004.3.12>

⑦ 제6항의 경우를 제외하고는 같은 기표소안에 2인 이상이 동시에 들어갈 수 없다.

⑧ 투표용지의 날인·교부방법 및 기표절차 그 밖에 필요한 사항은 중앙선거관리위원회규칙으로 정한다.<개정 2005.8.4>

거소투표는 신체장애 등으로 투표소를 방문하기가 어려운 유권자가 자신이 머무는 곳에서 투표할 수 있도록 한 제도이다. 거소투표 신고를 할 수 있는 선거인은 1)신체에 중대한 장애가 있어 거동할 수 없는 사람, 2)병원·요양소·수용소·교도소 또는 구치소에 기거하는 사람, 3)사전투표소와 투표소에 가서 투표할 수 없을 정도로 멀리 떨어진 영내 또는 함정에 근무하는 군인이나 경찰공무원, 4)중앙선관위 규칙으로 정한 외딴 섬에 거주하는 사람으로 거소신고인명부에 등재돼 있어야 한다.

제158조의2(거소투표) 거소투표자는 관할 구·시·군선거관리위원회로부터 송부 받은 투표용지에 1명의 후보자(비례대표국회의원선거 및 비례대표지방의회의원선거에서는 하나의 정당을 말한다)를 선택하여 투표용지의 해당 칸에 기표한 다음 회송용 봉투에 넣어 봉함한 후 등기우편으로 발송하여야 한다.

선상투표는 사전투표일 또는 선거일에 투표소에서 투표할 수 없는 선원을 대상으로 선상에서 실시하는 투표방법이다. 해외취업선·원양어선·외항여객선·외항화물선 등 대한민국 국민이 선장으로 있는 배(대한민국 국적 원양어업 및 외항 여객·화물운송사업 선박, 외국 국적 선박)에 승선한 선원은 선상투표 선거권자가 된다. 투표방법은 선상에서 FAX를 사용하여 투표지를 선거관리위원회에 전송하여 투표하는 방식으로 진행된다.

제158조의3(선상투표) ① 선장은 선거일 전 8일부터 선거일 전 5일까지의 기간(이하 “선상투표기간”이라 한다) 중 해당 선박의 선상투표자의 수와 운항사정 등을 고려하여 선상투표를 할 수 있는 일시를 정하고, 해당 선박에 선상투표소를 설치하여야 한다. 이 경우 선장은 지체 없이 선상투표자에게 선상투표를 할 수 있는 일시와 선상투표소가 설치된 장소를 알려야 한다.<개정 2015.8.13>

② 선장은 선상투표소를 설치할 때 선상투표자가 투표의 비밀이 보장된 상태에서 투표한 후 팩시밀리로 선상투표용지를 전송할 수 있도록 설비하여야 한다.

③ 선장은 선상투표가 진행되는 동안에는 해당 선박에 승선하고 있는 선원 중 대한민국 국민으로서 공정하고 중립적인 사람 1명 이상을 입회시켜야

한다. 다만, 해당 선박에 승선하고 있는 대한민국 국민이 1명뿐인 경우에는 그러하지 아니하다.

④ 선장은 제1항에 따른 선상투표소에서 선상투표자가 가져 온 선상투표용지의 해당 서명란에 제3항 본문에 따른 입회인(이하 “입회인”이라 한다)과 함께 서명한 다음 해당 선상투표자에게 교부하여야 한다. 이 경우 선상투표소에서 투표하기 전에 미리 기표하여 온 선상투표용지는 회수하여 별도의 봉투에 넣어 봉함한다.

⑤ 제4항에 따라 선상투표용지를 교부받은 선상투표자는 선거인 확인란에 서명한 후 1명의 후보자(비례대표국회의원선거에서는 하나의 정당을 말한다)를 선택하여 선상투표용지의 해당란에 기표한 다음 선상투표소에 설치된 팩시밀리로 직접 해당 시·도선거관리위원회에 전송하여야 한다.

⑥ 제5항에 따라 전송을 마친 선상투표자는 선상투표지를 직접 봉투에 넣어 봉함한 후 선장에게 제출하여야 한다.

⑦ 선장은 해당 선박의 선상투표를 마친 후 입회인의 입회 아래 제6항에 따라 제출된 선상투표지 봉투와 제4항 후단에 따른 선상투표용지 봉투를 구분하여 함께 포장한 다음 자신과 입회인이 각각 봉인한 후 보관하여야 한다.

⑧ 선장은 해당 선박의 선상투표를 마친 때에는 선상투표관리기록부를 작성하여 선거일 전일까지 해당 선박의 선박원부를 관리하는 지방해양항만청의 소재지(대한민국국적취득조건부 나용선의 경우 해당 선박회사의 등록지, 외국국적 선박은 선박관리업 등록을 한 지방해양항만청의 소재지를 말한다)를 관할하는 시·도선거관리위원회에 팩시밀리로 전송하고, 국내에 도착하는 즉시 선상투표관리기록부와 제7항에 따라 보관 중인 봉투를 해당 시·도선거관리위원회에 제출하여야 한다. 이 경우 국내에 도착하기 전이라도 외국에서 국제우편을 이용하여 제출할 수 있다.

⑨ 시·도선거관리위원회는 제5항에 따른 선상투표지를 수신할 팩시밀리에 투표의 비밀이 보장될 수 있도록 기술적 장치를 하여야 한다.

⑩ 시·도선거관리위원회는 제5항에 따라 수신된 선상투표지의 투표부분은 절취하여 봉투에 넣고, 표지부분은 그 봉투에 붙여서 봉함한 후 선상투표자의 주소지 관할 구·시·군선거관리위원회에 보내야 한다. 이

경우 투표한 선거인을 알 수 없는 선상투표지는 봉투에 넣어 봉함한 후 그 사유를 적은 표지를 부착하여 보관한다.

⑪ 시·도선거관리위원회는 선상투표지 관리록에 선상투표지 수신상황과 발송상황을 적어야 한다.

⑫ 구·시·군선거관리위원회는 선거일 투표마감시각까지 시·도선거관리위원회로부터 송부된 선상투표지를 접수하여 우편투표함에 투입하여야 한다.

⑬ 선상투표기간 개시일 전에 국내에 도착한 선상투표자는 중앙선거관리위원회규칙으로 정하는 서류를 첨부하여 관할 구·시·군선거관리위원회에 신고한 후 선거일에 주소지를 관할하는 투표구에 설치된 투표소에서 투표할 수 있다. 이 경우 해당 선박에서 선상투표용지를 미리 교부받은 사람은 관할 구·시·군선거관리위원회에 신고할 때에 그 투표용지를 반납하여야 한다.<신설 2015.8.13>

⑭ 선상투표의 투표절차, 투표의 비밀을 보장하기 위한 팩시밀리의 기술적 요건, 선상투표관리기록부 및 선상투표지 관리록의 작성·제출, 선상투표기간 개시일 전에 국내에 도착한 선상투표자의 투표절차, 그 밖에 필요한 사항은 중앙선거관리위원회규칙으로 정한다.<개정 2015.8.13.>

나. 제도적 측면에서의 이슈

블록체인 기반의 선거시스템은 기존의 투표와는 다른 절차를 가지고 있다. 선거인의 본인 확인 방식은 물론 투·개표 방식이 모두 다르다. 그러므로 공직 선거에 이를 바로 적용 하는 경우 기존의 제도에 비추었을 때 발생할 수 있는 논쟁사항이 있을 수 있다. 아래의 이슈는 국내의 공직선거법을 기반으로 제도적 측면에서 분석 했다.

① 직접 선거 원칙의 이슈

블록체인을 활용한 선거시스템을 도입한 해외사례를 살펴보면 유권자의 신분확인 절차가 복잡하다. 유권자의 고유 정보가 담긴 공인 인증 ID카드를 지정된 리더기에 인식을 하거나 PIN 번호 인증, 은행 정보 등을 활용하여 신분확인을 하고 있다.

하지만 우리나라 공직선거법에 따르면 선거인은 자신의 투표소에서 투표참관인에게 주민등록증이나 여권·운전면허증·공무원 등의 신분증명서를 제시 후 지문인식이나 전자서명을 해야 한다. 하지만 모바일이나 태블릿으로 원격투표를 진행한다면, 본인이 신분증을 가지고 있는지 타인이 가지고 있는지 확인이 불가능할 수 있다.

> **제157조(투표용지수령 및 기표절차<개정 2011.7.28>)** ① 선거인은 자신이 투표소에 가서 투표참관인의 참관하에 주민등록증(주민등록증이 없는 경우에는 관공서 또는 공공기관이 발행한 증명서로서 사진이 첩부되어 본인임을 확인할 수 있는 여권·운전면허증·공무원증 또는 중앙선거관리위원회규칙으로 정하는 신분증명서를 말한다. 이하 “신분증명서”라 한다)을 제시하고 본인임을 확인받은 후 선거인명부에 서명이나 날인 또는 무인하고 투표용지를 받아야 한다.

② 비밀 선거 원칙의 이슈

원격 투표를 진행한다면 기존의 투표 방식에 비해 비밀 선거의 원칙을 위배할 수 있는 몇 가지 문제가 존재한다. 투표참관인이 없기 때문에 선거인의 행동을 통제하기가 어려워 공직선거법의 제166조의2, 제167조의 사항을 확인하기가 힘들다. 전자 매체로 투표를 할 때 선거인이 화면을 캡처하는 것은 기술적으로 방지가 가능하지만 화면 자체를 촬영하는 일은 확인하기 어렵다.

또 기존의 투표소처럼 기표소가 따로 설치되어 있지 않기 때문에 투표 비밀이 보장되는지 다른 사람으로부터 침해가 되는지를 확인할 수 없다. 이러한 문제는 다른 사람의 강압에 의해 투표를 하게 된다면, 1인 1표의 원칙을 훼손하기 때문에 비밀의 원칙은 물론 평등의 원칙도 위배할 수 있다.

제166조의2(투표지 등의 촬영행위 금지) ① 누구든지 기표소 안에서 투표지를 촬영하여서는 아니 된다.
② 투표관리관 또는 사전투표관리관은 선거인이 기표소 안에서 투표지를 촬영한 경우 해당 선거인으로부터 그 촬영물을 회수하고 투표록에 그 사유를 기록한다.<개정 2014.1.17.>

제167조(투표의 비밀보장) ① 투표의 비밀은 보장되어야 한다.
② 선거인은 투표한 후보자의 성명이나 정당명을 누구에게도 또한 어떠한 경우에도 진술할 의무가 없으며, 누구든지 선거일의 투표마감시각까지 이를 질문하거나 그 진술을 요구할 수 없다. 다만,
텔레비전방송국·라디오방송국·「신문 등의 진흥에 관한 법률」 제2조제1호가목 및 나목에 따른 일간신문사가 선거의 결과를 예상하기 위하여 선거일에 투표소로부터 50미터 밖에서 투표의 비밀 이 침해되지 않는 방법으로 질문하는 경우에는 그러하지 아니하며 이 경우 투표마감시각까지 그 경위와 결과를 공표할 수 없다.<개정 1995.12.30, 2000.2.16, 2004.3.12, 2005.8.4, 2010.1.25, 2012.2.29>
③ 선거인은 자신이 기표한 투표지를 공개할 수 없으며, 공개된 투표지는 무효로 한다.

③ 자유선거의 원칙

사용자 식별기술을 개발하더라도 유권자가 투표를 하는 공간은 공개되지 않거나 일부만 공개된다. 이는 타의에 의한 투표를 하거나 대리 투표 가능성이 존재하여 직접선거의 원칙과 공직선거법에서 규정한 선거의 자유방해죄를 위배할 가능성이 높다.

제237조(선거의 자유방해죄) ① 선거에 관하여 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 500만원 이상 3천만원 이하의 벌금에 처한다.<개정 2010.1.25.>

...생략...

3. 업무·고용 기타의 관계로 인하여 자기의 보호·지휘·감독하에 있는 자에게 특정 정당이나 후보자를 지지·추천하거나 반대하도록 강요한 자

④ 개표 과정에서 쟁점사항

공직선거법에 따르면 개표를 진행할 때 후보자별 득표수는 공표 이전에 보도할 수 없게 되어 있다. 하지만 블록체인 기반의 투표시스템은 투표를 하는 과정 자체가 전자 방식이기 때문에 개표 시작과 함께 득표율 및 결과가 노출되는 문제가 있을 수 있다.

제178조(개표의 진행<개정 2011.7.28>) ① 개표는 투표구별로 구분하여 투표수를 계산한다.<개정 2002.3.7>

...생략...

③ 후보자별 득표수(비례대표국회의원선거 및 비례대표지방의회의원선거에 있어서는 정당별 득표수를 말한다. 이하 이 조에서 같다)의 공표는 구·시·군선거관리위원회위원장이 투표구별로 집계·작성된 개표상황표에 의하여 투표구 단위로 하되, 출석한 구·시·군선거관리위원회위원 전원은 공표 전에 득표수를 검열하고 개표상황표에 서명하거나 날인하여야 한다. 다만, 정당한 사유없이 개표사무를 지연시키는 위원이 있는 때에는 그 권한을 포기한 것으로 보고, 개표록에 그 사유를 기재한다.<개정 2002.3.7, 2004.3.12, 2005.8.4, 2011.7.28>

④ 누구든지 제3항에 따른 후보자별 득표수의 공표전에는 이를 보도할 수 없다. 다만, 선거관리위원회가 제공하는 개표상황 자료를 보도하는 경우에는 그러하지 아니하다.<개정 2002.3.7, 2014.1.17>

⑤ 개표절차 및 개표상황표의 서식 기타 필요한 사항은 중앙선거관리위원회규칙으로 정한다.

⑤ 관련 법·제도의 개정

마지막으로 현재 공직선거법에서는 선거 절차가 분산화가 되는 것을 염두해 두지 않았다. 현재 선거 절차에 따르면 개표의 과정은 기계장치나 전산조직을 활용하지만 모든 선거인이 투표하는 방식은 종이 투표를 활용한다. 투표시스템에 블록체인을 도입하기 위해서는 관련 법·제도를 개정 및 제정을 해야 신뢰할 수 있는 투표시스템을 구축할 수 있을 것이다.

제278조(전산조직에 의한 투표·개표) ① 중앙선거관리위원회는 투표 및 개표 기타 선거사무의 정확하고 신속한 관리를 위하여 사무전산화를 추진하여야 한다.

② 투표사무관리의 전산화에 있어서는 투표의 비밀이 보장되고 선거인의 투표가 용이하여야 하며, 정당 또는 후보자의 참관이 보장되어야 하고, 기표착오의 시정, 무효표의 방지 기타 투표의 정확을 기할 수 있도록 하여야 한다.

③ 개표사무관리의 전산화에 있어서는 정당 또는 후보자별 득표수의 계산이 정확하고, 투표결과를 검증할 수 있어야 하며, 정당 또는 후보자의 참관이 보장되어야 한다.

④ 중앙선거관리위원회는 투표 및 개표 사무관리를 전산화하여 실시하고자 하는 때에는 이를 선거인이 알 수 있도록 안내문 배부·언론매체를 이용한 광고 기타의 방법으로 홍보하여야 하며, 그 실시여부에 대하여는 국회에 교섭단체를 구성한 정당과 협의하여 결정하여야 한다. 다만, 제158조제2항·제3항 및 제218조의19제1항·제2항에 따른 본인여부 확인장치 및 투표용지 발급기와 제178조제2항에 따른 기계장치 또는 전산조직의 사용에 대하여는 그러하지 아니하다.<개정 2002.3.7, 2005.8.4, 2014.1.17, 2015.8.13>

⑤ 중앙선거관리위원회는 제4항의 협의를 위하여 국회에 교섭단체를 구성한 정당이 참여하는 전자선거추진협의회를 설치·운영할 수 있다.<신설 2005.8.4>

⑥ 투표 및 개표 기타 선거사무관리의 전산화에 있어서 투표 및 개표절차와 방법, 전산전문가의 투표 및 개표사무원 위촉과 전산조직운영프로그램의 작성·검증 및 보관, 전자선거추진협의회의 구성·기능 및 운영 그 밖에 필요한 사항은 중앙선거관리위원회규칙으로 정한다.<개정 2005.8.4>

2. 기술적 현황 및 이슈

앞에서 살펴본 해외사례에서도 살펴봤듯이 여러 국가에서 블록체인 기술을 선거에 도입하려는 연구가 계속 되고 있다. 에스토니아를 제외한 미국, 스페인 그리고 우크라이나에서는 중·소규모의 민간선거, 정당투표에 적용되었고 대부분이 당내 의사결정이나 후보를 선정하는 데에 사용되었다.

기존 오프라인 투표에 비해 물리적인 한계를 극복했기 때문에 시민 참여가 증가하고 본인확인 절차나 투표를 하기 위한 투표 절차가 간소해진 효과가 나타났다. 하지만 국가 차원에서 전국단위선거에 이를 사용하고자 한다면 블록체인 플랫폼도 구축해야 하며, 모든 국민이 블록체인 플랫폼에 접근할 수 있는 환경을 만들어야 한다. 예를 들어 한국에서는 스마트폰이나 인터넷, PC방 등은 매우 널리 보급돼 있지만 모든 세대가 이런 기술을 사용할 수 있는 것은 아니다. 그리고 투표의 기밀성을 담보해야 하는 구조도 함께 구축해야 한다. 이렇게 풀어야 할 문제가 있기 때문에 투표에 대한 활용은 외국사례와 같이 소규모 수준의 선거에서 먼저 이루어져야 한다.

본 장에서는 블록체인 기반의 투표 기술을 분석한 뒤 투표시스템에 도입하는 경우 발생할 수 있는 기술적인 쟁점사항을 도출하였다.

가. 블록체인 기반의 투표 기술

① 투표 시스템을 위한 블록체인 유형

블록체인은 크게 Private 네트워크와 Public 네트워크 두 가지 방식으로 구성되어 있다. Private 네트워크 선거는 선거인의 특징에 맞춘 시스템을 개발할 수 있다. 선거인의 구체적인 특성이 존재한다면 맞춤 전자투표 시스템을 만드는 방식을 활용할 수 있다. Private 네트워크는 블록체인의 규칙을 변경하거나 선거의 방식을 수정하는 작업을 쉽게 진행할 수 있다. 또한 권한 생성을 할 수 있기 때문에 높은 수준의 개인정보보호를 제공할 수 있다.

다음으로 Public 네트워크는 블록체인의 대표적인 가상통화인 비트코인과 같이

기존에 존재하는 블록체인에서 전자 투표 시스템을 만든다. Public 네트워크의 장점은 완전한 분산화 되어있기 때문에 결과를 조작하기가 Private 네트워크에 비해 더 어렵다. 또한 블록체인 특성상 사용자가 많을수록 신뢰도가 높아진 다는 점을 고려하여 소수의 유권자가 참여하는 선거에 신뢰를 담보할 수 있는 방식으로 Public 네트워크를 활용할 수 있다.

② 해외 국가 사례로 살펴본 블록체인 기반의 투표 기술

기존의 블록체인 기술을 투표시스템에 도입한 사례들을 살펴보면 대부분 중·소 규모의 민간선거이다. 기존에 존재하는 Public 네트워크에 선거시스템을 구축한다면, 선거인에 대한 인증 및 정보보호 시스템을 따로 구축해야하기 때문에 대부분의 선거시스템은 Private 네트워크에 구축되어 있다.

해외 사례에서는 투표 과정에서 어떠한 기술을 사용하고 있는지를 분석하였다. 그럼 어떤 방식으로 블록체인을 도입하고 있는지 살펴본다.

(선거인 확인 절차) 대부분의 국가에서는 선거인의 이름, 생년월일, 고유 식별번호, 공인 인증 된 전자 ID 카드 등을 통해 본인 확인을 진행한다. 투표의 신뢰를 높이기 위해 본인확인을 한 가지 요소가 아닌 다중 요소(Multi-factor) 본인 확인을 도입한 곳도 존재한다. 전자 기반의 본인확인 방식은 상대적으로 신뢰하기 힘들기 때문에 기존 투표소와 같이 투표 참관인이 직접 본인확인을 하는 방식도 사용하고 있다.

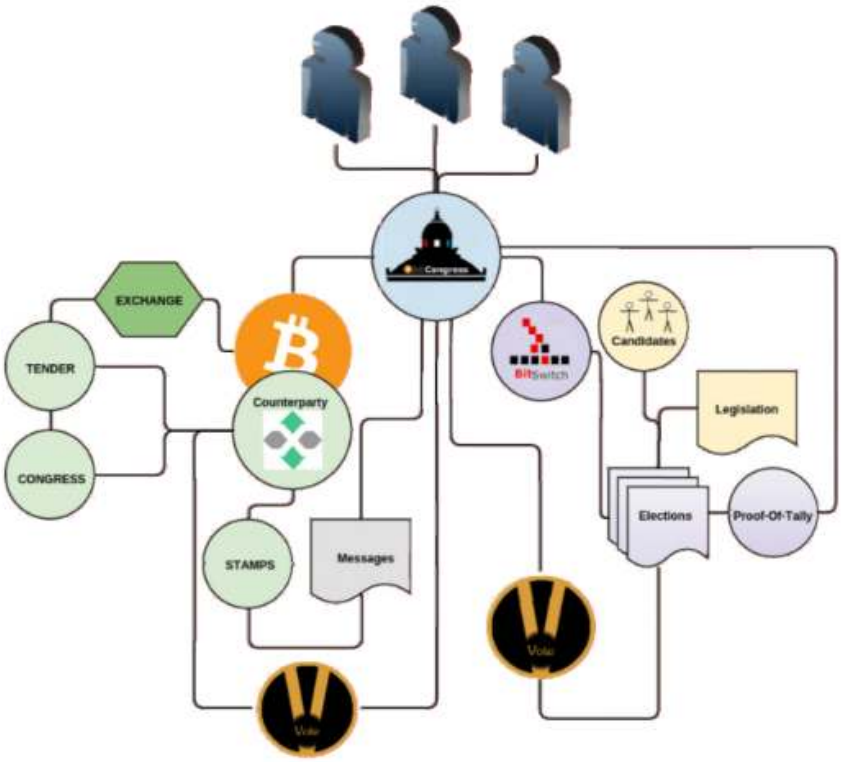
(투표) 투표는 모바일이나 PC 등의 디지털 매체를 이용해 진행한다. 투표 내역은 선거인의 디지털 서명으로 암호화를 한 뒤 블록체인에 저장을 한다. 미국에서는 기존의 종이 투표용지에 선거인이 투표 하면 스캐너를 이용해 투표용지를 스캔하여 블록체인에 기록하는 방식을 사용했다. 이는 기존의 온라인 투표 및 원격 투표의 단점을 해결하는 사례로 참고할 수 있을 것이다.

(개표) 개표하는 과정은 개표를 하는 자격 인증을 실시한 후 투표를 확인한다. 확인이 완료되면 관리자(국가, 지역구)의 키를 이용해 암호화를 풀어 투표 결과를 확인한다. 대부분의 국가에서는 체인을 두 가지로 나눈다. 하나는 투표율을 계산하기 위한 체인이고, 다른 하나는 어떤 후보에게 투표했는지 보관하는 체인을 가지고 있다. 이는 선거인의 익명성을 보장해주기 위한 방안으로 고안된 기술이다.

③ 해외 기업 사례로 살펴본 블록체인 기반 투표 기술

- BitCongress

(개요) BitCongress은 블록체인 기반의 투표 및 법안을 분산된 방식으로 저장하는 플랫폼을 구현하였다. BitCongress는 IoT 장치, 전화, 태블릿, TV 등의 매체를 이용하여 입법, 투표를 진행할 수 있다.



(그림 9) BitCongress의 블록체인 기반 투표 시스템

※ 출처 : http://bitcongress.org/

(본인 확인 절차) BitCongress는 신뢰할 수 있는 중앙기관을 통해 유권자의 신분을 확인하고 중복 투표와 투표조작이 이루어지지 않도록 감시한다. 선거 조작을 관리하기 위해 투표지를 보내는 Bitcoin 주소를 추적하는 유권자 신원 시스템을 사용한다.

(투표) 투표는 다중 서명 스마트 계약 통해 유권자가 후보자나 법안을 선택하는 것으로 진행된다. 스마트계약의 공개키로 투표를 수락하고, 등록하고, 투표자의 공개키로 처리하여 개표한다.

- **Followmyvote**

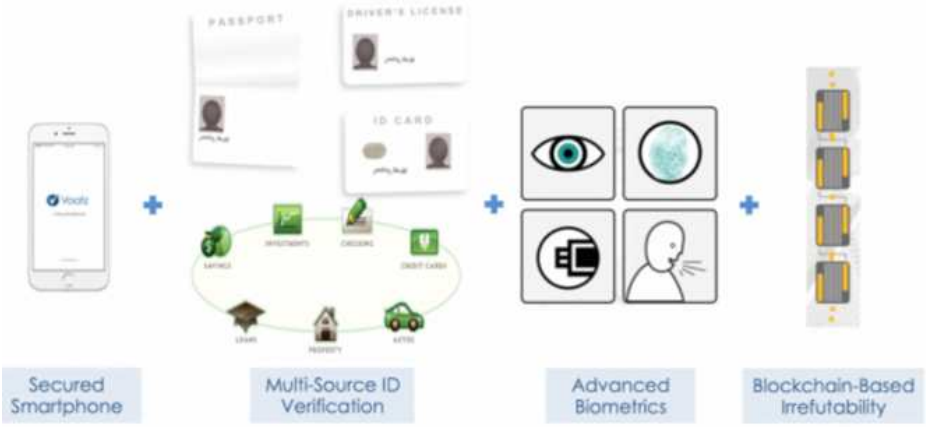
(개요) followmyvote는 블록체인 기술을 활용해 선거시스템을 구축한 미국의 스타트업 기업이다. 선거 결과가 실제로 정확한지 확인하고 선거인이 독립적으로 투표하였는지를 확인할 수 있는 시스템을 가지고 있다.

(본인 확인 절차) followmyvote의 블록체인 투표 시스템은 선거인이 선택한 개인 디바이스(PC, 노트북, 스마트폰·태블릿)에 개인 투표소를 다운로드 받아 디바이스를 통해 선거인의 신분 확인절차를 진행한다.

(투표) 본인 확인 절차를 완료하고 신원이 확인되면 유권자는 투표용지를 요청할 수 있다. 투표용지를 작성한 후 블록체인 투표함에 제출한다. 유권자는 선거가 마감되기 전에 투표 내용을 바꾸기 위해 재입장할 수 있다.

- **Voatz**

(개요) Voatz사는 블록체인 기반으로 원격 투표 기술을 제공하는 회사이다. 스마트폰과 태블릿을 통해 원격 투표가 가능하도록 하는 시스템을 개발 하였다. 기존의 투표 시스템 회사인 Clear Ballot사와 협력하여 2016년 민간 및 지방 자치단체 선거에서 블록체인 기반의 투표시스템을 시범 운영 하였다.



(그림 10) Voatz의 블록체인 기반 투표시스템

※ 출처: https://developer.ibm.com/startups/2016/11/08

(본인 확인 절차) Voatz사는 스마트폰, Multi-Source ID 확인 절차, 생체인식, 블록체인을 활용하여 모바일 중심의 보안, 유권자의 익명성 등의 기술을 지원한다. 유권자는 ID카드·여권·운전면허증과 같은 신분증을 이용해 본인 확인 절차를 거친다. 이 후 홍채, 지문, 음성인식과 같은 생체 인증을 통해 Multi-Source ID 확인 절차를 거친다. 이 절차를 통해 유권자의 신원이 확인 되면 선거를 위한 토큰이 제공된다. 투표가 종료되면 시스템에서 삭제된다.

(투표) 유권자가 단말기를 통해 투표를 진행하면 Voatz Server 네트워크에서는 유권자의 신원을 확인 후, 등록을 하고 투표에 대한 정보를 블록체인 상에 올린다. 투표가 완료되면 유권자에게 선거 관련 정보를 공지하고 관리자는 블록체인에 올라간 데이터 인증을 통해 신뢰할 수 있는 선거 시스템을 제공하고 있다.

나. 기술적 측면에서 쟁점사항

선거시스템에 블록체인을 활용한다면, 시민의 투표 참여 증가, 투표 절차 간소화, 투표율 증가의 효과가 있을 것으로 예상하고 있다. 기존 시스템에서는 모든 사람이 투표에 참여하기 힘든 물리적인 한계를 가지고 있었다. 그러나 기존의 한계상황을 극복하고 더 많은 시민이 참가할 수 있어 투표율이 증가할 수 있다. 그리고 투표 프로세스가 간소화되어 투표 비용의 절감의 효과도 기대할 수 있다. 블록체인 특성상 모두가 투표의 무결성을 보장할 수 있기 때문에 투표가 변경되거나 제거가 되지 않았다는 것을 확인할 수 있다.

하지만 블록체인 기반의 투표 시스템은 확실한 검증이 되지 않았기 때문에 도입을 할 때 고려해야할 쟁점사항이 존재한다.

① 블록체인 플랫폼 구축의 문제

현존하는 대부분의 블록체인 기반의 투표 시스템은 대부분 중·소규모 단위에 도입되고 있다. 전국적인 국가 규모에서는 확실한 실험 결과가 존재하지 않는다. 우리나라 투표 프로세스에 블록체인을 도입하기 위해서는 먼저 만 19세 이상의 선거인이 감당할 수 있는 블록체인 시스템을 구축해야 한다.

블록체인 시스템을 구축하기 위해서는 먼저 블록체인 유형을 선택을 해야 한다. public 블록체인을 선택한다면 인증 프로세스나 선거인의 익명성을 보장해줄 기술을 따로 구축을 해야 할 것이다. private 블록체인을 선택한다면 네트워크 인증 과정에서 누락되는 선거인이 없도록 표준화해야 할 것이다. 현재 블록체인 기술을 도입한 투표 시스템이 많지 않고 검증되지 않았기 때문에 시스템의 표준 역시 필요하다.

② 평등 선거 원칙과 관련된 쟁점사항

온라인 투표를 사용할 네트워크 인프라는 잘 구축되어 있지만 PC나 모바일 사용에 익숙하지 않은 계층에서 온라인 투표는 부담으로 작용할 수 있다. 특히 노인이나 저학력 계층의 투표율 하락을 야기할 수 있고 이는 정치적 불평등 문제를

제기할 수 있다. 이러한 문제는 정치적 갈등 요인으로 작용할 수 있다. 또한 원격 투표 시 선거인의 본인 여부를 확인하기 힘들기 때문에 대리투표나 중복투표 가능성으로 인해 평등선거 원칙을 위배여부가 제기될 수 있다.

위에서 살펴본 온라인 투표의 단점에서와 마찬가지로 디지털 격차는 단시간에 해결하기 힘든 문제이다. 그러므로 블록체인 기반의 투표시스템을 도입할 때 매뉴얼이나 교육·훈련에 대한 방법도 생각해봐야 할 것이다.

③ 익명성의 문제

비밀투표가 문제가 쟁점화 되지 않는 중·소규모의 민간선거, 정당투표에서는 블록체인 기반의 투표시스템이 문제가 되지 않을 수 있다. 그러나 총선·대선 등 범국가적인 규모에서는 추적이 가능해 비밀 투표의 원칙을 위배할 가능성이 있다.

블록체인은 공개키, 개인키에 개인정보가 연결되어 있지 않기 때문에 익명성 보장이 장점이기도 하다. 그러나 블록체인은 모든 참가자가 장부를 공유하기 때문에 선거인의 개인정보를 통해 인증을 하게 되면, 선거인의 정보와 투표 내역에 대해 추정하는 것이 가능한 문제점이 제기될 수 있다.

④ 키 관리의 문제

블록체인은 기존의 공인인증서 시스템과 마찬가지로 비대칭키 암호체계를 활용하여 블록체인에 트랜잭션을 올릴 때 본인의 개인키로 전자서명을 하고 있다. 투표시스템에서도 선거인이 본인이 투표한 것이 맞다는 것을 증명하기 위해 선거인의 개인키를 이용한다. 투표할 때 사용하는 암호 키를 생성하는 과정이나 제공하는 과정에서 키 관리에 대한 이슈도 존재한다. 선거인이 직접 키를 관리해야하는지 선거관리위원회에서 키를 관리할 것인지를 정해 안전하게 키 관리를 할 방안을 모색해야 할 것이다.

이런 문제를 해결하기 위하여 에스토니아는 키 없는 전자 서명 인프라(KSI)를 구축하였다. 이를 블록체인 기술과 통합해 정부에서 발행한 ID카드로 세계 어느 곳에서나 로그인 후 투표가 가능한 시스템을 구축했다.

⑤ 대중의 신뢰 확보의 문제

기존의 투표 시스템은 선거관리위원회가 투표의 모든 프로세스를 관리하는 구조이다. 블록체인이 도입된다면 블록체인이 내놓는 투표 결과가 오류가 없이 집계됐음을 신뢰를 해야 한다. 블록체인은 기존의 서버와 다른 구조를 가지고 있다. 또한 선거인에게는 생소한 기술이고 직관적으로 이해하기 힘들다. 이러한 요인으

로 블록체인 기술에 대해 대중의 신뢰를 확보하기가 쉽지 않다. 그러므로 투표 절차와 선거결과에 대한 정당성 확보가 필요하다.

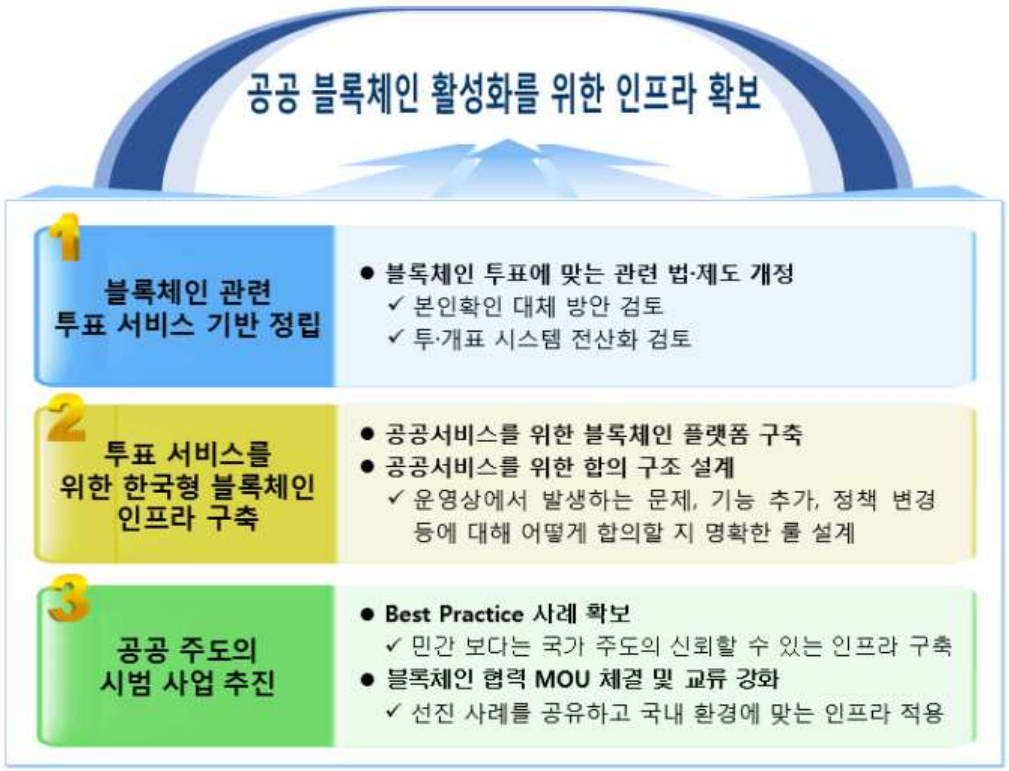
3. 시사점

본 연구를 통해 국내에 블록체인 기반의 투표 시스템을 도입하기 위해서는 제도적·기술적 쟁점이 존재한다는 것을 확인할 수 있었다. 이미 블록체인 기술을 도입한 국가나 기업의 사례를 살펴보면, 본인 확인 절차나 투표에 대한 신뢰성을 해결하기 위해 많은 기술을 도입하고 있었다. 블록체인 기술이 무결성을 지원해주기 때문에 투표의 신뢰성을 높일 수 있을 것으로 예상되었다. 그러나 선거의 익명성의 문제, 기존의 전자 투표에서도 문제점으로 제기되었던 강압에 의한 투표, 디지털 격차의 문제를 근본적으로는 해결해주지 못하는 상황이다. 여전히 법·제도적으로 몇 가지 쟁점사항이 존재하고 있다. 이러한 쟁점들이 기술적으로 해결 가능하더라도 현행법상 분산화 된 기술을 도입하는 것은 문제가 될 수 있다. 법적으로도 안전한 투표시스템을 도입하기 위해서는 먼저 법·제도의 개정 및 제정이 필요할 것으로 보인다.

마지막으로 해외 사례를 통해 대부분의 블록체인 투표는 정책의 의사결정을 하거나 정당에서 후보를 뽑는 중·소규모의 투표가 진행되고 있다. 따라서 국내에서 블록체인 기반의 투표시스템을 도입하기 위해서는 굳이 비밀 투표가 필요하지 않고 소규모 인원으로 선거인의 인증이 쉬운 방식을 활용하는 정당 투표, 주민투표와 같은 의사결정과정에 블록체인을 도입하는 것이 제도적·기술적으로 가능성이 높을 것이라고 판단된다.

제 4 장 결론

1. 한국선거에서 블록체인 방식의 온라인투표시스템의 도입을 위한 제언



(그림 11) 한국선거에서 블록체인 방식의 온라인투표시스템의 도입을 위한 제언

온라인 투표는 유권자들이 시간과 장소에 구애를 받지 않고 개인용 디바이스를 이용해 투표를 할 수 있는 방식으로 편리함과 투표율 향상, 투표 관리가 모두 전산화 되어 투표 관리업무의 효율성을 증대 시키는 장점을 가지고 있다. 하지만 보안 문제, 신뢰 확보의 문제, 비밀보장의 문제 등으로 인해 범국가적인 규모의 투표에는 도입하기 힘들다. 블록체인은 거래 참가자 모두가 데이터를 공유하는 분산형 디지털 장부로 모든 구성원이 같은 내용을 공유하는 방식이다. 기존의 온라인 투표를 도입했을 때 문제가 되었던 보안과 신뢰의 문제를 해결해줄 것이다.

블록체인의 대표적인 특성을 살펴보면, 모든 사람이 장부를 공유하기 때문에 해킹이 거의 불가능하다. 특정 컴퓨터가 공격을 받거나 멈춘다고 해서 데이터 유실이 일어나지 않기 때문에 안전한 플랫폼을 구축할 수 있다. 또한 데이터를 위조 변조를 위해서 해커는 네트워크 참가자의 과반의 데이터를 수정해야 하는데 이는 현존하는 컴퓨터로는 사실상 불가능하다고 알려져 있어 투표의 신뢰도를 높일 수

있을 것이다. 하지만 3장에서 살펴본 것과 같이 국내 공직선거에 블록체인을 도입을 하기 위해 해결할 과제가 많다는 것을 확인할 수 있었다. 4장에서는 한국선거에 블록체인 방식의 온라인투표시스템을 도입하기 위한 제도적, 기술적, 정책적 제언을 제안하였다.

가. 제도적 제언

① 본인확인 대체 방안 검토

온라인투표시스템에서의 가장 큰 문제점은 본인이 직접 투표를 했는지, 투표 과정이 비밀로 진행 되었는지와 같은 본인확인절차이다. 공직선거법에서는 법적으로 직접 본인의 신분증명서를 투표참관인에게 제출하고 확인을 받도록 되어있다. 그러나 온라인투표시스템에서는 이 조항을 따르기에는 기술적으로 한계가 있기 때문에 현재의 공직선거법 제152조제2항을 개정할 필요가 있다. 즉 현행 “투표관리관은 본인임을 확인하고 선거인명부에 서명 또는 날인한 선거인에게 선거인명부등재 번호표를 교부하여 투표하게 할 수 있다.”의 법조항을 개정하여 비대면 확인절차나 대체할 수 있는 제도를 검토해 봐야 할 것으로 사료된다.

또 다른 방안으로는 온라인 투표가 아직 불안하다고 판단하면, 지금처럼 투표소에 직접 방문하여 투표하고, 투표 결과를 현장에서 블록체인에 직접 담는 방식으로 투표 시스템을 구축할 수 있다.

② 투·개표 시스템 전산화 검토

공직선거는 모두 국내의 공직선거법을 따라야 하기 때문에 블록체인 기술을 선거시스템에 도입을 하기 위해서는 공직선거법의 개정이 필요하다. 현재의 공직선거법은 제278조(전산조직에 의한 투·개표)에서 보듯 투표에 온라인시스템을 도입하는 것을 금지하고 있지는 않다. 공직선거관리규칙 제16장의2 전자투표 및 개표에 관한 특례를 살펴보면, 전자투표를 하기 위해서는 전자투표기가 필요하다고 언급 되어 있다. 그러므로 현재 상황으로 원격 투표는 공직선거에서 불가능하다고 볼 수 있다. 더욱 더 안전한 투표시스템을 구축하기 위해서는 법적으로 온라인 투표시스템의 요구사항을 구체적으로 설정할 필요가 있다.

나. 기술적 제언

① 공공서비스를 위한 블록체인 플랫폼 구축

실제 공직 선거가 시스템적으로 이루어지기 위해서는 우선적으로 신뢰할 수 있는 국가 주도의 공공서비스 플랫폼이 먼저 구축되어야 할 것이다. 선거뿐만 아니라 공공 서비스에서는 무엇보다도 보안과 신뢰가 중요하다. 그렇기 때문에 블록체인 핵심기술을 활용하여 정부 및 공공서비스를 위한 표준 플랫폼 구축을 제안한다. 이것을 오픈 플랫폼 형태로 발전시켜 블록체인 기술을 도입하려는 공공기관에서 쉽게 서비스를 개발 할 수 있도록 할 필요가 있다고 본다. 국가 인프라로서의 블록체인을 각종 정부 시스템으로 점차 확대하는 방안을 제안한다.

특히 온라인 전자투표는 비밀투표원칙에 위배가 되는 부분이 존재하기 때문에 투표시스템을 따로 구축하는 것도 좋은 방법이다. 현재 기술로서는 블록체인이 익명성을 보장할 수 있다고 알려졌지만 모든 사람이 투표내용을 공유하기 때문에 비밀이 완전히 보장되지는 않고 있다. 이에 처음 블록체인을 구축할 때 선거인과 투표 결과가 매칭 되지 않도록 분리하는 방안을 적용하는 것도 좋은 방법이 될 것이다.

② 공공 서비스를 위한 합의 구조 설계

블록체인에서 합의 구조는 핵심 중의 핵심이다. 여기서 합의 구조란 크게 두 가지로 나눌 수 있다. 하나는 블록을 생성하는 과정에서 어떤 정보를 블록에 저장할 것인가를 결정할 때 작동하는 합의 구조다. 비트코인은 현재 비트코인 네트워크에 참여하고 있는 서버의 51%의 정보가 기록되면 그 정보를 진본이라고 확정하는 구조를 가지고 있다.

두 번째는 블록체인의 코드 자체, 즉 블록체인에 적용된 로직과 정책 과제를 수정하는 것과 관련된 합의 구조가 필요하다. 비트코인을 포함한 현존하는 블록체인 프로젝트 대부분이 운영상에 발생하는 문제, 기능 추가, 정책 변경 등에 대해 어떻게 합의할지 명확한 규칙이 없는 경우가 대부분이다. 따라서 공공서비스를 위한, 특히 투표 시스템에 블록체인 기술을 적용하기 위해서는 설계과정에서 그 운영에 대한 의사결정 구조를 구축해야 할 필요가 있다.

다. 정책적 제언

① 공공 주도의 시범 사업 추진

블록체인 기술을 공공 주도로 적용할 수 있는 분야에서 선도적으로 적용하기 위한 시범 사업을 추진하여 Best Practice를 전파 하는 방안을 고려해 볼 수 있겠다. 블록체인 기술은 거래 투명성 부문에서 높은 효과를 기대할 수 있기 때문에 특히 투표 분야에 적용하면 블록체인의 특성과 장점을 잘 활용할 수 있다. 나아가 투표가 완료된 즉시 투표 결과를 확인 가능하기 때문에 투표 관리 비용이 획기적으로 줄어들며, 투표를 둘러싼 부정이나 조작 논란을 해소함으로써 불필요한 소모적 논쟁을 줄일 수 있다. 그러나 투표는 공정하고 신뢰성을 확보해야 한다는 점에서 모두가 믿을 수 있는 기반 인프라의 확보가 먼저 필요하다. 그러므로 이는 기업이나 민간 보다는 국가 주도의 신뢰할 수 있는 인프라 구축이 필요하다. 인프라 구축이후, 시범 사업을 추진하여 Best Practice 사례를 확보하는 방향으로 진행해야 한다. 공공서비스의 경우, 높은 수준의 보안과 안정성을 필요로 한다. 투표의 경우는 더욱 그러하기 때문에 이는 민간에서 진행하기에는 다소 어려움이 있다.

블록체인 핵심기술을 활용하여 정부 및 공공서비스를 위한 표준 플랫폼을 구축하고, 국내외 각종 컴플라이언스를 만족시킬 수 있는 기술을 적용해야 한다.

나아가 비교적 블록체인구축 사례를 많이 공유한 미국, 캐나다, 독일, 에스토니아 등의 국가와 블록체인 협력 MOU를 체결하고 교류를 강화할 필요가 있다. 특히 공공 서비스 사업 추진을 통해 확보된 선도 블록체인 서비스를 많이 보유한 곳을 중심으로 선진 사례를 공유하고, 그것을 기반으로 국내 환경에 맞도록 발전시켜 적용해야 할 것이다.

② 기존의 K-voting 서비스를 활용

선거관리위원회에서 운영 중인 K-voing 서비스는 온라인투표 서비스로 선거관리위원회에 신청한 기관, 단체의 선거를 대상으로 PC와 이동통신단말기를 이용해 투표관리, 이용기관 관리자 대상 교육, 시스템 기술지원을 제공하는 서비스이다. 공직선거에서는 활용하고 있지 않지만 소규모 단체에도 지원 하고 있다. 아파트 동 대표 선거는 물론 다양한 단체의 대표자선출 같은 투표를 언제, 어디서나 참여할 수 있는 장점을 가지고 있다.

블록체인은 개개인의 투표참여 기록과 투표결과가 서로 매칭되지 않도록 구성되어 있다. 기존 방식의 온라인 투표시스템은 서버가 중앙에 있기 때문에 투표 결과가 조작이나 변조가 될 가능성이 제기되고 있다. 그러므로 더욱 안전한 온라인 투표 시스템을 구축하기 위해서는 블록체인기술 도입으로 보안성을 높일 수 있는

방안이 될 수 있다.

현재 K-voting은 선거인 명부 작성, 후보자 정보 수집, 투표 매체 결정, 인증방법, 투표 준비부터 선거 개표, 개표 결과 조회 등 온라인투표에 필요한 서비스를 제공해주고 있기 때문에 기존의 프로세스에 블록체인을 도입하여 시범으로 운영하는 것을 제안한다.

③ 정책결정 수단으로 블록체인 도입

지금까지는 투표에 블록체인 기술을 활용하는 방안을 살펴보았다. 지금부터는 조금 변형시킨 방안으로 블록체인을 활용하는 방법을 제언 하고자 한다. 블록체인 기술의 스마트 컨트랙트 기능을 이용하면, 블록체인에 저장된 법안 개정을 직접민주투표를 통해 수정할 수 있다. 스마트 컨트랙트는 계약에 대한 조건을 컴퓨터 코드로 작성하기 때문에 조건이 맞으면 바로 실행할 수 있는 강제성을 가지고 있다.

투표에 스마트 컨트랙트를 적용 한다면, 선거인에 대한 조건을 설정할 수도 있다. 그리고 투표 기간이 마감 되면, 자동으로 투표가 마감되고 곧 바로 개표 결과를 알 수 있다. 이러한 기능은 법률을 수정하거나 시스템을 수정하는 등의 다양한 방법으로 활용할 수 있다. 이러한 기능을 투표시스템에 적용을 한다면, 정책이 결정되면 원하는 시간에 실시간으로 정책이 수정될 수 있도록 기술적으로 활용이 가능하다.

이에 공동체 구성원들이 공통의 룰이나 규칙, 정책결정을 위한 수단으로 활용하는 방안을 제안한다. 이러한 기능이 완성된다면 블록체인이 진정한 의미에서 사회운영 및 의사결정 시스템을 구축할 수 있는 기술로 작동할 수 있다.

라. 결론

앞서 살펴본바와 같이 블록체인 기반의 투표시스템은 여러 가지 장점을 가지고 있다. 무엇보다도 투표 결과를 위·변조할 수 없다는 것이 가장 큰 장점일 것이다. 또한 투표가 완료된 즉시 투표 결과를 확인 가능하기 때문에 투표 관리 비용이 획기적으로 줄어든다. 투표를 둘러싼 부정이나 조작 논란을 해소함으로써 불필요한 소모적 논쟁을 줄일 수 있다.

블록체인 기술을 활용하면 기명 투표, 무기명 투표 등 원하는 대로 시스템을 구축할 수 있다. 즉, 투표의 목적에 맞게 유연한 방법을 제공할 수 있다는 것도 또 다른 장점이다. 투표 결과가 실시간으로 공개되어 결과에 영향을 미치는 것이 부담스럽다면, 필요에 따라 종료 시간에 맞춰 결과를 공개하는 것도 가능하다.

우리나라에서는 2000년 초 공직선거법 개정으로 전자투표가 언급되기 시작하였다. 공직선거법 제278조에서는 전자투표를 위해서 비밀투표보장, 선거인의 투표용이성, 정당·후보자의 참관보장, 투표 및 개표의 정확성, 검증가능성 등 안전하고 믿을 수 있는 전자투표를 위한 원칙이 제시되었다. 법 개정 이후, 투표지분류기, 개표업무, 본인확인 절차 등은 전산방법에 의하여 진행하고 있다. 하지만 지금까지의 공직선거에서 선거인이 전자적 방식으로 투표에 참여한 적은 한 번도 없었다. 이는 전자투표를 도입했을 때 해킹 등의 보안 문제가 존재하고 국민의 신뢰가 형성 되어야 하는 문제가 있기 때문이다. 그러므로 지금까지 선거인이 투표 할 때는 여전히 종이투표방식을 활용하고 있다는 것을 알 수 있었다.

블록체인이 보안이나 해킹에 대한 문제를 해결할 수 있는 기술이라고 낙관적인 전망이 많다. 그러나 여전히 블록체인 기반의 투표시스템도 기술적, 제도적 쟁점사항이 존재한다. 더구나 대중들의 신뢰를 획득하는 것은 단기간에 해결할 수 있는 문제가 아니다.

이러한 이유로 국내에서 블록체인에 기반 한 전자투표의 도입은 전국적인 대규모 선거에서 시작하는 것보다 법적으로 제약이 적은 중·소규모의 민간선거에서부터 시작하는 것이 더 현실적이라고 생각된다. 먼저 중앙선거관리위원회에서 제공하고 있는 k-voting 시스템에 블록체인을 적용하는 방안을 고려할 필요가 있다. 현재와 같이 아파트 단지의 동 대표를 뽑는 선거, 대학교의 학생회장을 뽑는 선거, 더 나아가면 주주총회나 이사회의 의사 결정에 먼저 활용해 보는 방안을 제안한다.

끝으로, 블록체인은 분산원장 기술이다. 중앙집중형이 아닌 분산화된 시스템으

로써, 중앙의 관리기관이 필요 없다는 것이 가장 큰 장점이다. 이를 공공서비스에 도입하게 되면 정부의 역할이 줄어들지 않을까 하는 우려가 있다. 그러나 정부의 역할은 소멸되기 보다는 바뀔 것이라 생각된다. 이해관계를 달리하는 수많은 계층, 집단들 사이의 갈등을 조정하고, 외부의 공격을 항상 감시하고 그것에 대응하며 사회의 최종적인 신뢰를 탐지하는 역할을 누군가는 해야 한다. 이는 기술적으로 해결할 수 있는 부분이 아니다. 특히, 투표와 같은 공공서비스에 블록체인 기술을 도입하게 되면, 그러한 변화에 적합한 중앙선거관리위원회의 새로운 R&R(Role&Responsibility)에 대한 재정의가 이루어져야 할 것이다.

참 고 문 헌

[1] 한국인터넷진흥원, “2016 인터넷이용실태조사”, 2016

[2] R. Verbij, “Dutch e-voting opportunities”, University of Twente, 2014

[3] Kaveh Waddell, “How Electronic Voting Could Undermine the Election”, 2016.08.29.(https://www.theatlantic.com/technology/archive/2016/08/how-electronic-voting-could-undermine-the-election/497885/)

[4] 한국정보화진흥원, “블록체인 활용 전자투표 주요사례 및 시사점”, 한국정보화진흥원 스페셜 리포트, 2017

[5] 한국정보화진흥원, “Beyond 비트코인, 블록체인 기술의 무한확장”, 2016

[6] 조희정, “전자민주주의와 인터넷 투표 : 에스토니아 사례를 중심으로”, 한국정당회보 제7권 제2호 통권 13호, 2008

[7] http://gn.nec.go.kr/gn/hoewon/sub6.jsp?brdType=R&bbIdx=34401

[8] 김용철, “전자민주주의: 인터넷 투표의 활용 가능성과 문제점”, 민주주의와 인권 제2권 2호, 2002

[9] http://www.coindesk.com/libertarian-party-texas-logs-votes-presidential-electors-blockchain/

[10] 정승화, “블록체인 기술기반의 분산원장 도입을 위한 법적 과제-금융산업을 중심으로-”, 한국금융법학회지 제13권 제2호 , 2016

[11] 금융보안원, “블록체인 개발 플랫폼 현황 및 활용 사례”, 2016.

[12] https://bitcoinmagazine.com/articles/agora-voting-proposes-bitcoin-based-voting-system-1390288011/

[13] 전명산, “블록체인 거버먼트”, 알마 출판사, 2017

[14] 조희정, “미국의 전자투표와 기술 수용 정치:브라질·에스토니아와 비교를 중심으로”, 서강대학교 박사학위 논문, 2007

[15] 금융보안원, “블록체인 응용기술 개발 현황 및 산업별 도입 사례”, 2017

[16] 아카하네 요시하루, 아이케이 마나부, “블록체인 구조와 이론”, 위키북스, 2017

[17] 안기환, “한국에서 전자투표 도입에 관한 탐색적 연구”, 전남대학교 석사학위 논문, 2017

<인터넷 홈페이지>

중앙선거관리위원회 : http://www.nec.go.kr

중앙선거관리위원회 온라인투표시스템 : http://www.kvoting.go.kr

VOTEWATCHER : http://votewatcher.com

Agora Voting : https://agoravoting.com

O2WEBS 전자투표시스템 : http://www.votesystem.net

Digital Voting with the use of Blockchain Technology : https://www.economist.com/sites/default/files/plymouth.pdf

followmyvote : https://followmyvote.com/online-voting-technology/blockchain-technology/

BitCongress : http://www.bitcongress.com/