공학 석사학위 논문

블록체인 방식의 전자투표 시스템 구현 및 성능 개선 방안 연구

A Study on Performance Improvement and Implementation of Electronic Voting System using Blockchain

아 주 대 학 교 정보통신대학원

정보보호 전공

유 헌 우

블록체인 방식의 전자투표 시스템 구현 및 성능 개선 방안 연구

A Study on Performance Improvement and Implementation of Electronic Voting System using Blockchain

지도교수 김 학 범

공동지도교수 예 홍 진

이 논문을 공학 석사학위 논문으로 제출함.

2016 년 2 월

아 주 대 학 교 정보통신대학원

정보보호 전공

유 헌 우

유헌우의 공학 석사학위 논문을 인준함.

심사위원장 김 학 범 인

심 사 위 원 예 홍 진 인

심 사 위 원 손 태 식 인

아 주 대 학 교 정보통신대학원

2016 년 2 월

감사의 글

본 논문을 완성할 수 있도록 지도와 격려를 해주신 지도교수 김학범 교수님과 끝까지 아낌없는 조언과 지도를 해주셨던 예홍진 교수님께 진심을 다해 감사를 드립니다.

업무와 학업을 병행할 수 있도록 격려해준 직장 동료 및 선후배 분들이 큰 힘이 되었습니다.

마지막으로 하늘에서 가족을 항상 지켜주시는 아버지와 자식을 위해 평생 헌신하신 어머니 김금열 여사께 아들이 감사와 존경의 마음을 전해드립니다.

2016년 2월

아주대학교 정보통신대학원

유현우

국 문 요 약

전자투표제도는 선거의 모든 과정을 전자화 하는 종합적인 시스템으로써 유권자 대상 설정, 본인 확인, 투표, 개표, 검표과정 등 전자선거시스템 구축으로 이해할 수 있다. 이러한 전자투표 시스템이 유권자의 신뢰를 얻기 위해서는 기술적인 보안성과 안정성이 완벽히 구현되었을 때 가능할 수 있다.

따라서 본 논문에서는 전자투표 수용의 신뢰성을 보장하고 기술적 안전성을 담보할 수 있는 블록체인 방식의 “탈 중앙집중식 전자투표 시스템”을 제안한다.

블록체인 기술은 분산 데이터베이스로써 중앙 서버의 존재 없이 모든 사용자들이 데이터를 공유하고 직접 데이터를 업데이트 한다. 이러한 블록체인 기반에 전자투표 시스템을 구성하여 전자투표 데이터를 블록체인에 저장하게 되면 블록체인의 장점을 그대로 사용할 수 있는 탈 중앙집중식 전자투표 시스템을 개발 할 수 있다.
이러한 전자투표 시스템은 사이버 공격 및 네트워크 장애에 의해 파괴될 수 없고 사용자들의 합의에 의해 데이터가 업데이트 되므로 데이터 변조 및 부정행위가 원천적으로 차단되었다.

따라서 블록체인 기술을 적용한 전자투표 시스템은 기존의 전자투표 시스템의 장점과 종이투표 시스템의 장점을 모두 포함하고 있으며, 자발적 참여를 통한 검증을 수행하므로 유권자의 신뢰성을 높일 수 있다. 또한 다양한 플랫폼에 연동될 수 있도록 성능개선 작업을 통해 평균 87.6%의 성능 향상을 확인 할 수 있었다.

목 차

그림 차례

표 차례

제 1 장 서 론

제 1 절 연구배경 및 목적

대한민국은 현재 전자정부(Electronic Government)의 실현을 통하여 초고속 IT기반과 함께 국제적인 영향력과 명성을 얻고 있다. 또한 국민들의 정치참여 수단인 투표 부분에서도 이를 활용한 전자투표(Electronic Voting)의 제도적 도입이 이루어지고 있다.

전자투표는 90년대 중반부터 세계 주요 국가들이 도입을 하고 있으며, 현재는 약 50여 개국이 공직선거에 전자투표를 도입하여 활용하고 있다. 공직선거에 전자투표 제도를 도입하는 것은 국가별로 상이한 정치문화·제도와 시민사회 및 정치권의 이해관계에 따라 도입수준의 차이를 보이고 있으며, 현재 대한민국에서는 전자투표 시스템에 대한 신뢰부족 등으로 정치권, 예산관계부처, 일부 시민단체의 반대에 부딪혀 원활이 진행되지 못하고 있는 실정이다. 이는 투표제도가 전자화로 변화되는 과정에서 겪게 되는 정치·사회적 갈등 과정이라 볼 수 있을 것이다.

공직선거의 전자투표 도입은 기존의 종이투표에서 디지털 방식으로 전환되는 단순한 선거관리방식의 변화라기보다 국가 정책의 파급효과가 큰 정치적 성격이 강한 공공정책으로 평가되어야 할 필요성을 암시한다.[1)]

따라서 이러한 전자투표 시스템이 유권자의 신뢰를 얻기 위해서는 기술적인 보안성과 안정성이 완벽히 구현되었을 때 가능할 수 있을 것이다.

이두호의 “전자투표 수용 영향요인에 관한 연구”[2)]에서는 전자투표 수용의 영향요

1) 조희정, “미국의 전자투표와 기술 수용 정치:브라질·에스토니아와 비교를 중심으로”, 서강대학교 박사학위 논문, February 2007

2) 이두호, “전자투표 수용 영향요인에 관한 연구:정치인, 공무원, 일반인 영향경로 비교분석”, 중앙대학교 박사학위 논문, February 2012

인으로써 '기술신뢰 및 유용성[3] 인지'를 연구결과로 도출하였으며, 2007년 터치스크린 시범투표 사업예산이 국회에서 삭감된 것은 '주요 전자투표 시스템에 대한 충분한 검증미흡과 정치인들의 전자투표 기술에 대한 신뢰부족'에서 기인한 것으로 분석 하였다.

이로써 공직선거의 전자투표제 도입은 전자투표의 기술적 안정성에 대한 신뢰와 전자투표의 유용성에 대한 공감대가 형성되어야 한다는 것으로 볼 수 있다.

기존의 전자투표 시스템이 가지고 있던 보안성에 대한 문제를 해결하기 위해서 미래 기술 이슈로 떠오르고 있는 안정성이 검증된 블록체인 방식을 전자투표에 도입하였다.

따라서 본 논문에서는 전자투표 수용에 신뢰성을 보장하고 기술적 안전성 담보를 목적으로 하는 블록체인 방식의 "탈 중앙집중식 전자투표 시스템" 방향을 제시한다.

제 2 절 연구내용

전자투표 방식에는 정해진 투표소에서 전자투표를 할 수 있는 방식인 '투표소 전자투표(PSEV, Poll Site E-Voting)'와 투표소에 가지 않고 통신기기를 이용할 수 있는 곳이면 어디서든 사용할 수 있는 '원격 인터넷 투표(REV, Remote Internet E-Voting)' 방식으로 구분되어질 수 있으며, 각 방식에 따른 특징은 '표 1'과 같다.[4]

본 논문에서는 PSEV와 REV의 개념을 구분하지 않고 두 가지 방식을 모두 사용하는 전자투표 시스템을 제안하기 때문에 '전자투표'라 내용을 통칭하도록 하겠다.

3) 특정한 시스템을 사용하는 것이 개인의 업무성과를 향상시킬 것이라고 개인이 믿는 정도(Davis, 1986)
4) 박해영, "전자투표를 통한 국민주권 실현방안 연구", 창원대학교 박사학위 논문, December 2007

표 1. 전자투표 방식에 따른 특징

구 분	투표장소	선거 관리 정도	기술적 안정성 쟁점 정도	특 징
PSEV 방식	전자투표 기기가 설치된 공공장소	높음	낮음	투표소와 개표소를 공공망으로 연결, 네트워크에 대한 외부침입이 있을 수 있지만 공공망이기 때문에 통제가 용이하다. 많은 사람이 모이는 백화점, 영화관, 학교, 도서관 등 공공장소에 투표기 설치. 투표소에 선거관리자가 없다(키오스크). 사용기기에 특수한 전자적 인증장치설치로 관리부분을 해결한다.
REV 방식	인터넷, 모바일 등이 가능한 불특정 장소	낮음	높음	보안 침해의 위험성이 높으며, 관리인이 없이 자유롭게 투표하므로 비밀투표 침해의 가능성이 높다.

출처 : 박해영, “전자투표를 통한 국민주권 실현방안 연구”, December 2007

기존 인터넷을 구성하는 서버-클라이언트(Server-Client) 개념을 사용한다면 수많은 취약점을 노출하게 되고 악의적인 공격행위에 안전을 보장할 수 없으므로 중앙집중식이 아닌 P2P(Peer to Peer)방식을 사용한다. 이에 따라 분산시스템의 대표적 기술인 블록체인(Blockchain) 기술을 개량·확장하여 활용하도록 한다.

비트코인(Bitcoin)의 블록체인은 금융거래를 위한 데이터베이스(거래장부) 역할만 하고 있는 것에 반해 블록체인을 전자투표 시스템에 활용한다면 보다 안전하고 효율적인 전자투표 시스템의 데이터베이스를 만들 수 있다.

기존의 전자투표 시스템이 지닌 문제는 서비스가 중앙 관리 서버에 몰려있다는 점이다. 중앙 관리 서버가 멈추게 된다면 모든 클라이언트들도 무용지물이 될 수밖에

없게 되는데 이것이 서버-클라이언트 구조가 지닌 한계라 볼 수 있다.

따라서 이러한 전자투표 시스템의 데이터베이스를 P2P 네트워크에 분산시켜 놓는다면 서버-클라이언트 구조의 한계를 극복할 수 있을 것이다.

하지만 분산 데이터베이스는 각 노드(Node)[5]들이 데이터를 가지고 있기 때문에 해킹이나 데이터 변조에 취약한 부분이 있는데 이는 다른 노드들에게 검증을 하도록 하는 제 3자 검증을 통해 극복해 낼 수 있다. 이렇듯 블록체인 인프라는 검증하는 노드들이 많으면 많을수록 보안성이 높아지게 되는데 사용자들의 자발적인 참여 유도를 위하여 참여자에게 금전적 보상(25BTC X 검증 + 거래수수료)을 해줌으로써 현재의 비트코인의 블록체인 인프라가 거대하게 유지되고 있음을 보여주고 있다.

전자투표 시스템에서 데이터 저장 및 검증에 참여하는 자발적 노드들은 해당 선거에 관련된 사용자로 이루어질 것이다. 그 이유는 자발적인 참여의 동기가 분명하기 때문이다. 앞서 언급한 전자투표 도입에 가장 큰 요인은 기술적 신뢰성이기 때문에 투표자 본인이 직접 투표결과를 검증하고 싶은 동기가 분명할 것이기 때문이다.

본 논문은 1장에서 서론을 담고 2장에서 분산형 데이터베이스인 블록체인을 알아본다. 3장에서는 전자투표 시스템 모델을 구현하고 4장에서는 성능개선 모델을 제안하고 검증한다. 5장에서는 마지막으로 결론을 도출하고 차후과제를 알아보았다.

제 3 절 관련 연구

전자투표 시스템의 기존 연구들은 서버-클라이언트 방식의 시스템에 서버 보안 및 클라이언트 보안성을 높이는 방식으로 진행되어져 왔다. 그러나 본 논문에서는 기존 연구와 달리 서버가 없는 시스템(Non-Server Electronic Voting System)을 최초 제안한다. 따라서 본 연구가 제안하는 전자투표 시스템은 서버-클라이언트 방식보다 뛰어난 보안성을 기대할 수 있으며, 연구의 독창성이 있다고 할 수 있겠다.

5) 블록체인 네트워크상에 연결되어 있는 개개의 주체, 블록체인 네트워크에 참여하면 하나의 노드가 된다.

제 1 항 국내 전자투표의 현황

대한민국에서의 전자투표는 2002년 민주당 대통령후보 경선에서 인터넷투표가 실시되었고 2003년 참여정부의 전자정부 로드맵 31대 과제 중 '온라인 국민 참여 확대' 과제의 핵심 사업으로 선정되기도 하였으며, 이에 따라 2006년부터 중앙선거관리위원회(이하 선관위)가 주관기관으로 전자투표 시스템을 개발하여 각종 위탁선거에 시범 적용하는 등 점차적 발전을 거듭하고 있다.

선관위는 정당 간 협의를 이끌어 내기 위해 노력하였지만 반면에 정당들은 전자투표 제도 도입에 대하여 회의적인 입장을 보였다. 오로지 당리당략에 의해 행동하는 정당들은 전자투표 제도가 당선율에 부정적인 영향을 보일 것으로 인식하고 있으며, 특정 연령대에 활용이 몰릴 수 있다는 것이 그 이유에서다.

공직선거에 전자투표 제도를 도입하기 위해서는 정당 간 협의가 필수적이다.

공직선거법[6] 제278조 제4항은 '중앙선거관리위원회는 투표 및 개표 사무 관리를 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.'고 법으로 명시되어 있기 때문이다.

또한 전자투표 시스템에 대한 보안·기술적 불안감 및 네트워크 불안정에 대한 요인은 공직선거의 전자투표 제도 도입에 치명적인 악영향으로 작용하고 있다. 신뢰할 수 있는 기술과 시스템이 도입 된다면 시간과 비용을 획기적으로 절감하는 한편 지속적으로 떨어지고 있는 투표율을 높일 수 있는 전자투표의 장점을 기대할 수 있을 것이다.

선관위는 2012년 공직선거법 개정으로 통합선거인명부 활용 근거를 마련하여 '통합선거인명부시스템'을 구축하였다. 그 결과 2013년 4.24 재·보궐 선거의 부재자 투표를 시작으로 사전투표제를 시행하게 되었다.

---

6) 법제처, "공직선거법", http://www.law.go.kr/법령/공직선거법/(13497,20150813)

선거일에 앞서 4월 19 ~ 20일 시행된 사전투표 결과에서 국회의원 선거구 3곳의 평균 투표율은 6.93%로 집계되어 사전투표제 도입이 투표율 제고에 상당히 기여할 것이라는 평가를 받았다.[7] 이후 2014년 6.4 지방선거 투표율이 56.8%으로 기록하며 16년 만에 최고치 투표율을 기록하기도 하였다.[8]

사람들은 부재자 투표 신고를 하지 않고도 전국 부재자 투표소에서 사전투표를 할 수 있었고 유권자는 시간과 장소에 구애받지 않고 투표할 수 있었기에 투표율의 상승효과를 확인 할 수 있었던 것이다.

이는 앞으로 이루어질 전자투표 도입의 첫 단계라고 볼 수 있을 것이다.

누구나 인터넷을 쓸 수 있고 스마트폰과 태블릿PC가 널려 있는 디지털 시대에 살고 있는 요즘 굳이 투표장을 찾지 않아도 되고 언제나 투표를 행사할 수 있으며, 통계가 바로 집계되기에 투표 종료와 동시 결과도 확인 가능한 전자투표 시대를 머지않아 우리는 맞이할 것으로 예견할 수 있다.

2013년 선관위는 협력업체 KT와 MOU를 체결하고 온라인투표시스템인 '케이보팅(K-Voting)'을 공동으로 개발해 서비스를 제공하고 있다.[9]

'케이보팅(K-Voting)' 시스템은 각종 기관 및 단체의 다양한 의사결정 투표와 대표자 선출 선거 등에서 인터넷을 이용한 투표와 개표를 효율적이고 안전하게 실시할 수 있도록 지원하는 서비스이다.

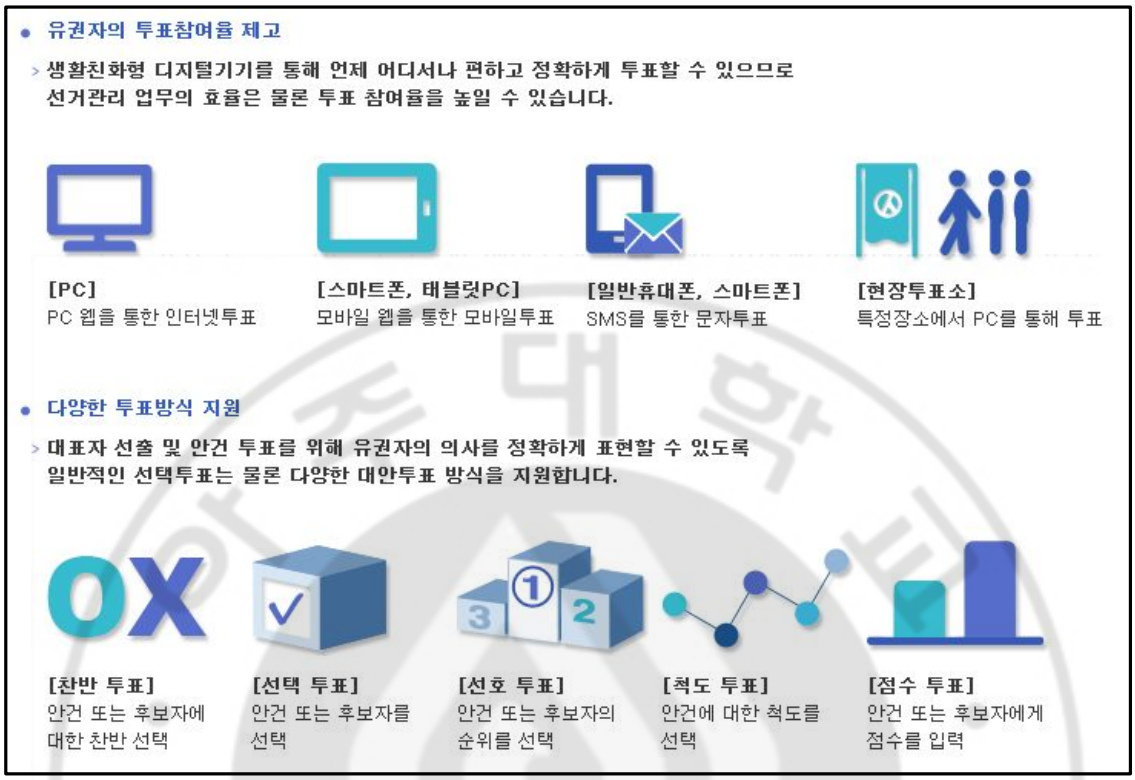
---

7) 트렌드 지식사전, "사전투표제", http://terms.naver.com/entry.nhn?docId=2070478&cid=55570&categoryId=55570
8) 김도경, "사전투표제가 투표율에 미치는 영향", 한국시민윤리학회보, 2014
9) 중앙선거관리위원회 온라인투표시스템 '케이보팅(K-Voting)', http://www.kvoting.go.kr

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

그림 1. 선관위 온라인투표시스템 '케이보팅(K-Voting)'

또한 다양한 투표 방법과 방식을 지원해주는 시스템으로 전자투표의 완성형 모델을 보여주고 있으며, 다양한 기관 및 단체가 비용을 지불하고 점차적으로 사용범위를 넓혀가고 있다.



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

그림 2. '케이보팅(K-Voting)' 시스템의 투표 방법 및 투표 방식

서울시는 2015년부터 모든 서울 아파트 단지의 입주자 대표 선출을 '케이보팅(K-Voting)' 시스템을 이용하도록 의무화 추진하였으며, 각종 학교기관의 학생임원 선거를 '케이보팅(K-Voting)' 시스템으로 활용하는 곳도 많아지고 있다. 이외에도 MBC위원장 선거, 지자체 정비사업의 주민 의사결정, 택시조합장 선거, 대한의사협회·교수협회 등 각종 협회장 선거, MBC '나는 가수다' 청중평가단 투표 등 다양한 민간분야 생활선거에도 전자투표가 점점 일상화되어지고 있다.[10)]

'케이보팅(K-Voting)'은 선거제도의 4대원칙과 IT 온라인 투표의 가이드라인을 충족한 시스템이라 홍보하고 있으며, 다음과 같은 전자투표의 특징을 부각시키고 있다.

10) 노컷뉴스, "40만 사용 선관위 온라인투표, 비밀 보장 안돼", http://www.nocutnews.co.kr/news/4452699, August 2015

표 2 . 전자투표의 특징

정확성	모든 정당한 유효투표는 투표결과에 정확히 집계됨
확인성	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

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

제 2 항 국내 전자투표의 사고사례

1. 사전투표

2014년 사전투표가 전국적으로 처음 시행된 6.4 지방선거 과정에서 '이중 투표' 논란이 일어났다. 경기 의정부에서 투표일에 한 유권자가 사전투표에서 관외자 투표를 한 것으로 적발하여 투표를 제지시켰지만 유권자는 투표를 하지 않았다며 투표를 강행했고 이후 조사결과 투표 사무원이 본인 확인 과정에서 동명이인을 오인한 것으로 해프닝이 종료 되었다. 또한 안양지역 유권자는 투표소를 찾았으나 사전투표자로 기록되어 있다며 투표를 하지 못했고 이후 조사결과 마찬가지로 투표 사무원이 동명이인을 가리지 못한 실수인 것으로 밝혀졌다.[11)]

이러한 이중투표 논란은 전자투표제의 도입이 된다면 시스템에서 중복투표가 허용되지 않으므로 일어나지 않을 것이며, 선관위의 허술한 관리감독에 대한 비난을 받

11) 동아일보, "'사전투표제' 편리해 졌지만 '이중투표' 논란에 허점 노출", http://news.donga.com/DKBNEWS/3/all/20140605/64030941/3, June 2014

지 않아도 될 것이다.

2. 케이보팅(K-Voting)

2015년 '케이보팅(K-Voting)' 시스템에서도 보안문제가 발생하였다. '케이보팅(K-Voting)' 개발업체인 '이맥소프트(Immacsoft)' 업체의 비리 조사에서 '케이보팅(K-Voting)' 시스템의 암호화 기술이 빠져있었던 것으로 밝혀진 것이다. 암호화 기술 검증에서 탑재되어 있어야할 키분할, 비트위임, 은닉서명 등 보안기술이 제외된 상황에서 2년간 운영된 점은 시스템을 이용한 사용자들의 투표결과 불신의 파장을 크게 일으켰다. 데이터베이스 관리자가 투표 값을 변경하여 결과를 조작 할 수도 있었기에 투표결과에 대한 검증 및 소송이 곳곳에서 일어났다. 현재 선관위는 해당 시스템의 보안기술을 보완하고 서비스를 재가동 하였다.[12)]

위 사례에서 보았듯이 전자투표에서 기술적 보안성이 얼마나 중요한 요소인지 알 수 있는 대목이다.

12) 서울경제, "구멍 뚫린 선관위 전자투표시스템", http://economy.hankooki.com/lpage/society/201508/e20150811180022142920.htm, August 2015

제 2 장 블록체인 고찰

제 1 절 비트코인의 블록체인

제 1 항 비트코인 개념 및 특징

비트코인은 2009년 나카모토 사토시(Nakamoto Satoshi)가 만든 디지털 통화이며, 통화를 발행하고 관리하는 중앙 장치가 존재하지 않는 구조를 가지고 있다. 대신, 비트코인의 거래는 P2P 기반 분산 데이터베이스에 의해 이루어지며, 공개키 암호 방식 기반으로 거래를 수행한다. 비트코인은 지갑 파일의 형태로 저장되며, 이 지갑에는 각각의 고유 주소가 부여되어 그 주소를 기반으로 비트코인의 거래가 이루어진다.[13] 여기서 이야기 하는 P2P 기반 분산 데이터베이스가 바로 블록체인을 이야기 하고 있다.

블록체인은 분산 데이터베이스의 한 형태로 지속적으로 성장하는 데이터 기록 리스트로써 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안되었다.[14] 비트코인의 블록체인은 비트코인의 거래내역을 모아 하나의 블록을 생성해 기록하고 블록을 주기적으로 생성해 앞쪽 블록과 연결하여 체인을 이루게 된다. 즉, 주기적으로 생성된 블록은 순서에 따라 연결되어 있기 때문에 데이터를 변조하려면 모든 블록체인 데이터를 변조해야 하는 어려움이 생기게 된다. 또한, 서버가 없이 운영되는 블록체인 데이터는 모든 참여자가 나누어서 가지고 있기 때문에 다수결 합의에서 승인을 얻으려면 전체 사용자의 51%이상의 컴퓨팅 파워로 변조를 시도해야 한다.

13) 위키피디아, “비트코인”, https://ko.wikipedia.org/wiki/비트코인, March 2011.
14) 위키피디아, “블록체인”, https://ko.wikipedia.org/wiki/블록체인, August 2015.

결론적으로 하나의 노드가 데이터 변조를 시도 할지라도 네트워크의 다수 노드와 경쟁에서 승리할 수 없기 때문에 데이터의 임의 조작이 불가능하다고 볼 수 있다.

나카모토 사토시의 “Bitcoin: A Peer-to-Peer Electronic Cash System” 논문에서 비트코인에 대한 소개를 다음과 같이 설명한다.[15]

‘P2P 디지털 화폐는 금융기관을 거치지 않는 온라인 지불 수단을 제공할 수 있으며, 비트코인은 P2P 네트워크를 이용하여 부정행위의 문제를 해결할 수 있다.

계속적으로 진행되고 있는 거래내역(Transaction)을 타임스탬프(Timestamp)와 같이 포함해서 해시(Hash)로 전환한 후 작업증명(Proof-of-work) 체인으로 연결함으로써 기록을 연속적으로 생성하게 되면 작업증명 과정을 되풀이하지 않는 한 수정 할 수 없게 될 것이다. 이 중 가장 긴 체인은 발생한 각 거래 순서를 입증해주기도 하며, 가장 많은 컴퓨팅 파워를 사용하여 만들어진 체인임을 증명하는 역할도 한다.

각 노드들 컴퓨팅 파워의 과반수가 협력하여 네트워크를 공격하지 않는 한 정직한 노드들이 항상 가장 긴 체인을 생성할 것이며, 체인 만들기 경쟁에서 정직한 노드들이 공격자를 항상 능가하게 될 것이다.’

위와 같이 나카모토 사토시는 분산 데이터베이스의 구조를 적용하여 중앙관리기관을 없앴고 부정행위를 막기 위하여 블록체인이라는 분산 컴퓨팅 메커니즘을 개발하여 적용시켰다.

그러나 전 세계인들의 비트코인에 대한 대부분의 관심은 ‘화폐’로써의 가능성에 초점이 맞춰져 있는데 즉, 신뢰의 제공 방식, 급등락 하는 가치 변동성, 실물 경제와의 연동 가능성 등이 주요 쟁점이 되고 있다. 하지만 비트코인이 작동하는 메커니즘은 기술적 측면에서도 매우 혁신적인 것이라 볼 수 있다.[16]

기존의 디지털 통화 알고리즘은 공개키 암호방식을 통한 소유권 관리를 중점으로 사용되어왔는데 비트코인은 ‘작업증명(Proof-of-work)’이라는 합의 알고리즘을 결합

15) Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2009.
16) 이성춘 외 2명, “비트코인(Bitcoin) 시스템 분석 노트”, KT경제경영연구소, December 2013

함으로써 보안성이 높은 탈 중앙화된 디지털 화폐를 구현했기 때문이다.

이것은 두 가지 문제를 동시에 해결할 수 있었다.

첫째, 네트워크상에 있는 모든 노드들이 비트코인의 장부 상태에 일어난 업데이트 상태를 공동으로 승인할 수 있도록 해주었다. 둘째, 누구든지 합의 프로세스에 참여할 수 있도록 허용해줌으로써 합의 결정권에 대한 정치적인 문제를 해결할 수 있었다.

따라서 간단하고 효과적인 합의 알고리즘을 제공해 주었고 '특정한 리스트에 등록되어있는 주체'라는 참여 조건을 허물고 매우 공정하고 경제적인 참여조건으로 대체하였다. 이로 인하여 시빌 공격(Sybil Attack)[17]도 방어해줄 수 있는 메커니즘을 제공해 주었다.

과거 P2P 네트워크로 운영되는 시스템은 바로 이 합의 알고리즘에 대한 문제에 직면하여 있었기 때문에 중앙통제 시스템 없이 의사 결정을 할 수 있는 분산 컴퓨팅 시스템은 불가능해 보였다. 하지만 블록체인의 작업증명 기술의 등장으로써 이러한 '비잔틴 장군의 문제[18]'를 해결할 수 있는 혁신적 시스템이 등장한 것이라 볼 수 있다.

17) 어떤 한 공격자가 여러 개의 식별자를 가지고 시스템이나 네트워크를 공격하는 방법의 총칭

18) Leslie Lamport, "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, http://www.cs.cornell.edu/courses/cs614/2004sp/papers/lsp82.pdf, July 1982

비트코인의 주요특징으로는 익명성, 무국경성, 탈중앙성, 분산네트워크, 투명성 등이 있으며, 세부내용은 '표 4'와 같다.

표 3. 비트코인의 주요특징

익명성 (Anonymity)	개인정보가 사용되지 않고 사용할 수 있는 시스템이므로 정보 유출에 안전하다. 또한 공개키 암호화 기술을 사용하여 모든 기록 전체를 암호화함으로써 내용을 식별할 수 없으므로 익명성을 제공한다.
무국경성 (Borderless)	국경에 구애받지 않는 네트워크로 연결되어 있어 범국가적으로 사용될 수 있는 시스템이다.
탈중앙성 (Decentralization)	중앙서버나 관리주체가 존재하지 않는다. 따라서 시스템을 장악하거나 데이터를 변조할 수 없다.
분산네트워크 (Distributed Network)	P2P시스템으로써 하나의 서버에 연결되어 있는 것이 아니라 근처의 노드들과 거미줄처럼 얽혀 있다. 따라서 단일 공격점이 존재하지 않기 때문에 시스템을 다운시키거나 파괴하는 것이 불가능하다.
투명성 (Transparency)	모든 것을 관찰하는 것이 가능하다. 누구나 모든 데이터를 조회할 수 있고 시스템이 구동되는 소스코드 자체가 오픈소스로 공개되어 있어 누구나 수정이 가능하다. 다만 새로운 룰이 적용되기 위해서는 80%이상의 수용(CPU기준)이 필요하다.

이러한 비트코인의 주요특징은 전자투표 시스템에서 필요로 할 조건을 모두 갖추고 있다. 따라서 비트코인의 기술적 메커니즘을 전자투표 시스템에 적용 한다면 '표 4'와 같은 특징을 적용시킬 수 있을 것이다.

표 4. 비트코인과 전자투표의 특징 비교

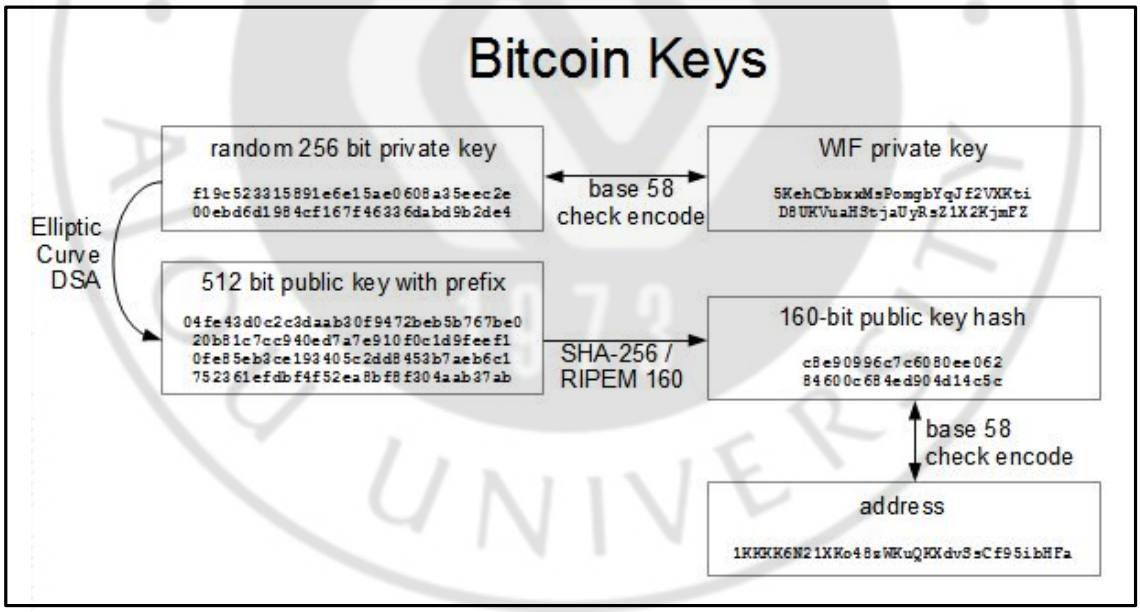
비트코인의 주요 특징	내 용	전자투표로 적용한 특징
익명성	투표 내용을 본인 이외 다른 이에게 노출시키지 않는다.	보안성 기밀성
무국경성	언제 어디서든 투표를 할 수 있다.	편의성 유용성
탈중앙성	중앙관리기관의 정치적 부정행위가 원천적으로 차단된다.	신뢰성
분산네트워크	시스템 오류로 인한 에러, 악의적 사용자의 공격행위, 전체 네트워크 파괴행위 등 보안사고 완벽 방어	안정성
투명성	누구든지 프로그램 내부를 볼 수 있으며, 누구든 개발에 참여할 수 있고 누구에게나 모든 것이 오픈되어 있어 모든이가 사용할 수 있다.	수용성

제 2 항 비트코인의 구조

비트코인은 크게 거래(Transaction) 메커니즘과 채굴(Mining) 메커니즘으로 나누어 질 수 있다.

1. 거래(Transaction) 메커니즘

비트코인의 거래는 공개키 기반구조(PKI, Public Key Infrastructure)를 따르고 있으며, 사용자는 지갑(Wallet)개념인 공개키와 비밀키를 생성한 후 비트코인 거래를 할 수 있다. 공개키는 사용자의 지갑주소가 되고 비밀키는 그 지갑의 비밀번호가 된다. 또한 실생활 사용에 편리성 및 저장용량을 줄이기 위하여 키 값을 변환하여 사용한다. 키 값의 변환과정은 다음과 같다.[19]



출처 : Ken Shirriff, “Bitcoins the hard way: Using the raw Bitcoin protocol”, http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html, Feb 2014

그림 3. 비트코인의 키 생성 과정

19) Ken Shirriff, “Bitcoins the hard way: Using the raw Bitcoin protocol”, http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html, February 2014

여기서 키 생성의 알고리즘은 타원 곡선 전자 서명 알고리즘(ECDSA, Elliptic Curve Digital Signature Algorithm)을 사용하고 있다. ECDSA는 타원 곡선 암호방식(ECC, Elliptic Curve Cryptosystem)을 사용하는 전자서명(DSA, Digital Signature Algorithm) 알고리즘이다. RSA(Rivest-Shamir-Adelmen) 방식보다 적은 비트수(ECDSA 160 bit : RSA 1,024 bit)로 대등한 안전성을 가지면서 빠른 처리속도를 가지고 있어 더욱 효율적이다.[20]

표 5. RSA와 ECC의 안정성 비교

Time to break in MIPS(Million Instruction Per Second) year	RSA/DSA (bits)	ECC (bits)	RSA vs ECC key size ratio
10^4	512	106	5:1
10^8	768	132	6:1
10^{11}	1,024	160	7:1
10^{20}	2,048	210	10:1
10^{78}	21,000	600	35:1

출처 : 심경아, "[정보보호] 타원곡선 암호시스템 급부상", 한국정보통신기술협회 기술표준 이슈, http://www.tta.or.kr/data/weekly_view.jsp?news_id=513, September 2001

비밀키의 생성은 256bit의 랜덤 값이 생성된다. 생성된 비밀키는 공개키(지갑 주소)를 생성하는 역할을 하므로 중복 값이 생겨서는 안 된다. 따라서 고유한 값을 생성할 수 있도록 암호학적 안전한 의사 난수 생성기(CSPRNG, Cryptographically-Secure Pseudo-Random Number Generator)를 사용하여 비밀키를 생성한다.

20) 네이버 지식백과, "타원 곡선 전자 서명 알고리듬", 한국정보통신기술협회 IT 용어사전

시스템에서 사용하는 형식인 WIF(Wallet Import Format)로 비밀키를 변환하는 과정은 다음과 같다.[21)]

가. ECDSA 비밀키를 생성한다.(32 byte)

0C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D

나. 앞쪽에 메인 네트워크일 경우 0x80 byte를 테스트 네트워크일 경우 0xef를 추가한다.

800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D

다. SHA-256 해싱을 수행한다.

8147786C4D15106333BF278D71DADAF1079EF2D2440A4DDE37D747DED5403592

다. 또다시 SHA-256 해싱을 수행한다.

507A5B8DFED0FC6FE8801743720CEDEC06AA5C6FCA72B07C49964492FB98A714

라. 앞쪽 4 byte를 체크섬으로 사용한다.

507A5B8D

마. 과정 '나'의 값인 확장된 비밀키에서 체크섬을 뒷부분에 추가한다.

800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D507A5B8D

바. Base58Check로 인코딩하여 WIF를 얻는다.

5HueCGU8rMjxEXxiPuD5BDku4MkFqeZyd4dZ1jvhTVqvbTLvyTJ

또한 WIF를 비밀키로 다시 변환하려면 해당 과정을 역으로 진행하면 된다.
그리고 WIF의 체크섬 검사 과정은 다음과 같다.

가. WIF를 가져온다.

5HueCGU8rMjxEXxiPuD5BDku4MkFqeZyd4dZ1jvhTVqvbTLvyTJ

나. Base58Check로 인코딩한다.

800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D507A5B8D

다. 뒷부분 4 byte를 체크섬으로 분리한다.

800C28FCA386C7A227600B2FE50B7CAE11EC86D3BF1FBE471BE89827E19D72AA1D

21) bitcoinwiki, "Wallet import format", https://en.bitcoin.it/wiki/Wallet_import_format, January 2012

라. SHA-256 해싱을 수행한다.

8147786C4D15106333BF278D71DADAF1079EF2D2440A4DDE37D747DED5403592

마. 또다시 SHA-256 해싱을 수행한다.

507A5B8DFED0FC6FE8801743720CEDEC06AA5C6FCA72B07C49964492FB98A714

바. 앞쪽 4 byte를 체크섬으로 분리한다.

507A5B8D

사. 과정 '나'에서 분리한 체크섬과 비교하여 동일하여야 한다.

507A5B8D

공개키는 비밀키를 통해 생성되어지며, 공개키를 가지고 지갑 주소를 만든다.

지갑 주소를 만드는 과정은 다음과 같다.[22)]

가. ECDSA 비밀키를 가져온다.

18E14A7B6A307F426A94F8114701E7C8E774E7F9A47E2C2035DB29A206321725

나. 비밀키에 대응하는 ECDSA 공개키를 생성한다.(65 byte, Version prefix 1 byte + X좌표에 해당하는 32 byte, Y좌표에 해당하는 32 byte)

0450863AD64A87AE8A2FE83C1AF1A8403CB53F53E486D8511DAD8A04887E5B23522C
D470243453A299FA9E77237716103ABC11A1DF38855ED6F2EE187E9C582BA6

다. SHA-256 해싱을 수행한다.

600FFE422B4E00731A59557A5CCA46CC183944191006324A447BDB2D98D4B408

라. RIPEMD-160 해싱을 수행한다.

010966776006953D5567439E5E39F86A0D273BEE

마. 앞쪽에 메인 네트워크일 경우 0x00을 추가한다.

00010966776006953D5567439E5E39F86A0D273BEE

바. SHA-256 해싱을 수행한다.

445C7A8007A93D8733188288BB320A8FE2DEBD2AE1B47F0F50BC10BAE845C094

22) bitcoinwiki, "Technical background of version 1 Bitcoin addresses", https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses, November 2011

사. 또다시 SHA-256 해싱을 수행한다.

D61967F63C7DD183914A4AE452C9F6AD5D462CE3D277798075B107615C1A8A30

아. 앞쪽 4 byte를 체크섬으로 분리한다.

D61967F6

자. 과정 '마'의 값인 확장된 RIPEMD-160 해시 값에서 체크섬을 뒷부분에 추가한다.

00010966776006953D5567439E5E39F86A0D273BEED61967F6

차. Base58Check로 인코딩하여 지갑주소를 얻는다.

16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM

위 과정을 통하여 지갑(공개키, 비밀키)을 생성했다면 거래를 수행할 수 있다.

다음은 거래에 대한 예로 사용자 Kim이 사용자 Lee에게 송금을 하는 과정이다.

가. Kim은 Lee의 지갑주소(공개키)를 획득한다.

나. Kim은 자신의 지갑 속에 값들을 선택하여 송금할 금액과 Lee의 지갑주소를 기입한다.

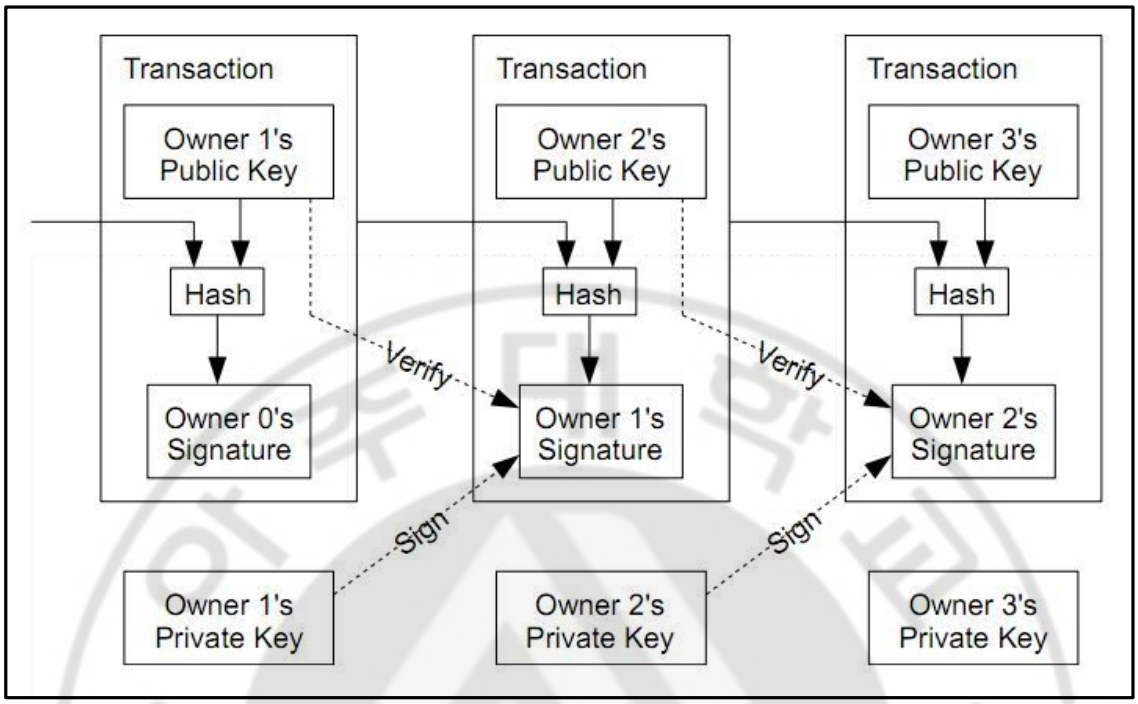
다. Kim은 비밀번호(비밀키)로 전자서명을 한다.

라. Kim은 해당 거래 내역을 블록체인(공공 거래장부) 네트워크에 공표한다.

블록체인에서 승인 작업이 정상적으로 이루어지면 Kim의 지갑에는 잔액이 남게 되고 Lee의 계좌에는 송금액이 남게 된다.

거래내역은 전자서명의 연속이라고 볼 수 있으며, 비밀키를 소유하고 있는 자가 금액의 주인이 된다. 다음 주인에게 금액을 넘기기 위해서는 지금까지의 거래내역에 다음 주인의 공개키를 덧붙인 뒤 자신의 비밀키로 전자서명 값을 첨부하여 넘기면 된다.

위의 거래 메커니즘을 도식하게 되면 '그림 6'과 같이 나타낼 수 있다.



출처 : Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2009.

그림 4. 비트코인의 거래 메커니즘

전자서명은 자신의 비밀키와 거래기록을 특정한 함수에 입력하여 생성하게 된다.

$$f(\text{비밀키}, \text{거래기록}) = \text{전자서명}$$

블록체인 네트워크에서 승인 과정은 전자서명(보내는 이), 거래기록, 공개키를 함수에 입력하여 실소유주 여부를 확인하는 과정이다.

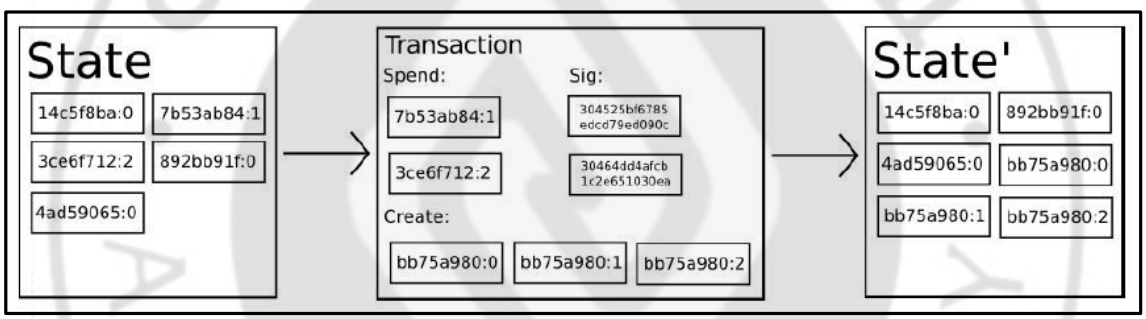
$$v(\text{전자서명}, \text{거래기록}, \text{공개주소}) = \text{참 or 거짓}$$

이러한 거래 과정은 기술적 관점으로 보았을 경우 하나의 상태변환 시스템(State Transition System)으로 생각해 볼 수 있다. 소유권 현황으로 이루어진 ‘상태(State)’

와 현 상태를 트랜잭션을 통해 새로운 상태로 출력하는 '상태변환 함수(State Transition Function)'를 구성해 볼 수 있는 것이다. 비트코인에서 상태는 계좌잔액표(Balance Sheet)이고 트랜잭션은 A에서 B로 X를 송금하는 요청이며, 상태변환 함수에 의해 A의 계좌에서 X를 감소하고 B에 계좌에서 X를 증가하는 내용이 될 수 있다. 만일 A의 계좌의 금액이 X 이하인 경우 상태변환 함수가 에러를 리턴 해야 한다.

이러한 상태 변환은 다음과 같이 정의 할 수 있다.

APPLY(S, TX) → S' or ERROR



출처 : Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform"

그림 5. 상태변환 시스템

Kim과 Lee의 상태는 각 10이고 Kim이 Lee에게 5만큼 이동하는 상태 변환은 다음과 같이 정의 할 수 있다.

APPLY({Kim:10, Lee:10}, "send 5 from Kim to Lee") = {Kim:5, Lee:15}

하지만 금액이 초과하는 등 조건이 불일치한다면 에러를 리턴 해야 한다.

APPLY({Kim:10, Lee:10}, “send 15 from Kim to Lee”) = ERROR

이러한 상태변환 시스템에서 상태는 생성되었지만 아직 사용되지 않은(소비되지 않은 트랜잭션 출력) 값을 UTXO(Unspent Transaction Outputs)라 한다. UTXO에는 소유자의 공개키 및 금액 값이 들어있으며 ‘그림 5’에서 살펴보았듯이 한 개 이상 입력(Input)과 출력(Output)이 존재한다. 입력에는 보내는 이의 UTXO 참조정보와 비밀키가 생성한 전자서명 정보가 있고 출력에는 새롭게 추가될 UTXO 정보를 가지고 있다.

상태 변환함수 APPLY(S, TX) → S’는 다음과 같이 정의할 수 있다.

가. TX 입력에서 참조된 UTXO가 S에 없다면 에러를 리턴

나. TX 입력에서 전자서명이 UTXO 소유자와 매치되지 않다면 에러를 리턴

다. 입력에 사용된 UTXO 총 금액 값의 합이 출력 UTXO 금액 값의 합보다 작으면 에러를 리턴

라. 입력에 사용된 UTXO가 삭제되고 출력 UTXO가 추가된 S를 리턴

여기서 ‘가’의 과정은 존재하지 않는 값을 트랜잭션에 사용되지 않도록 하기위한 것이고 ‘나’의 과정은 본인 소유의 값이 아닌 타인의 값을 트랜잭션에 사용되지 않도록 하기 위한 것이다.

예를 들어 Kim이 Lee에게 10만큼 값을 보낸다고 가정한다면 Kim의 계좌에서 총 합계가 10이상이 되는 UTXO 집합을 찾는다. Kim의 계좌에서 6, 3, 2가 표시된 3개의 UTXO가 존재한다면 이 3개의 UTXO가 트랜잭션의 입력에 들어가게 되고 2개의 출력이 생성되어진다. 출력 중 하나는 10이 표시된 새로운 UTXO가 생성되어지고 소유자는 Lee의 계좌가 된다. 그리고 다른 하나는 잔액 (6+3+2) - 10 = 1이 표시된 새로운 UTXO가 생성되며 소유자는 Kim의 계좌가 된다.

거래의 과정에서 부정행위(중복사용 등) 방지를 위해서는 모든 거래내역이 공개적으로 알려져 있어야 하고 처음부터 끝까지 검증을 필요로 하게 되는데 이과정이 블록체인 네트워크에서 이루어지게 되는 것이다. 검증은 보내는 이의 전자서명(비밀키)과 공개키가 일치하는지 여부를 확인하여 승인이 이루어진다. 이러한 과정이 채굴(Mining)과정에서 이루어진다.

2. 채굴(Mining) 메커니즘

탈 중앙집중식 시스템에서 가장 중요한 것이라 할 수 있는 부분은 P2P 네트워크를 통하여 승인하는 시스템을 만드는 것이다. 거래를 승인하기 위해 네트워크 노드들은 자발적으로 참여를 하게 되는데 이러한 작업을 채굴(Mining)이라고 한다. 참여자들은 채굴을 함으로써 비트코인의 경우 일정 보상을 받게 되므로 자발적 참여가 유도되고 있다.

네트워크 참여자들의 분산 합의 과정은 블록(Block)이라고 하는 트랜잭션 패키지를 약 10분 간격으로 지속적 생성하여 각 블록에 타임스탬프, 임의 값(Nonce), 이전 블록 참조 해시, 이전 블록 이후 발생한 모든 트랜잭션 목록 등을 포함시켜 넣는다. 이렇듯 이전 블록을 참조하면서 지속적으로 생성된 블록은 하나의 블록체인이 생성되며, 지속적으로 최신상태가 업데이트 된다.

여기서 블록을 채굴한다는 것은 다음 블록의 해시 값을 찾는다는 의미이고 해시 값의 첫 부분이 문자 '0'으로 이루어진 해시 값을 찾는 것이다. '0'의 개수가 많을수록 채굴은 어려워지고 반대로 0의 개수가 적은 해시 값 찾는 것이 수월해 진다.

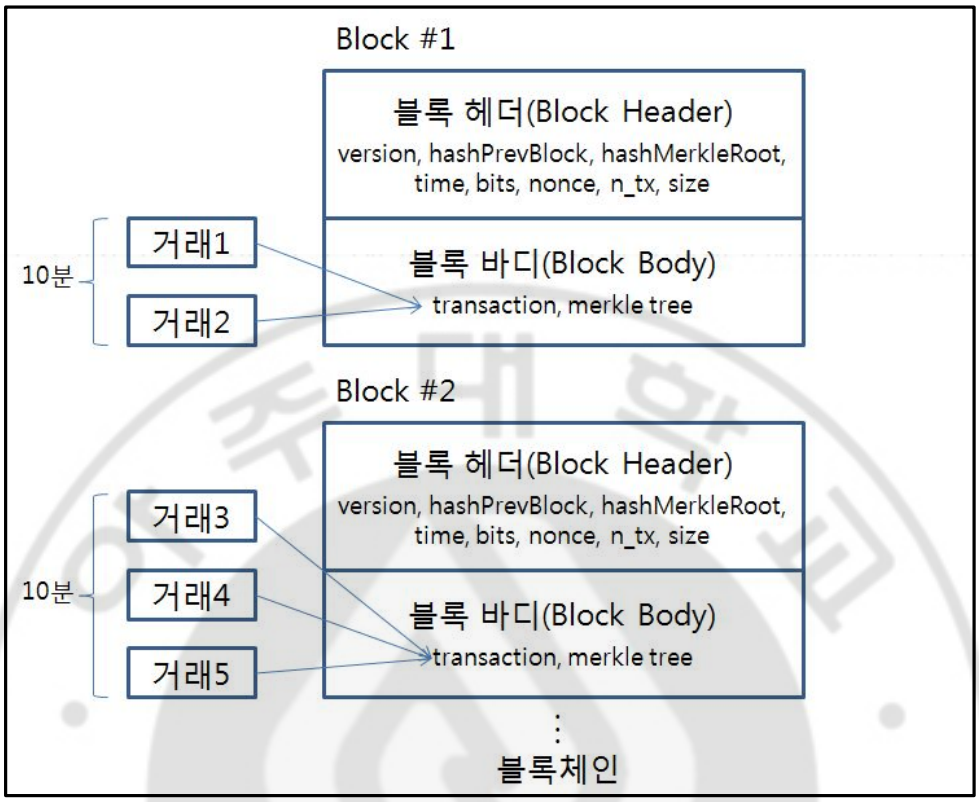


그림 6. 블록체인의 블록 내부 구조

블록체인에서 하나의 블록이 유효블록인지 확인하기 위한 알고리즘은 다음과 같이 정의할 수 있다.

가. 해당 블록에 의해 참조되는 이전 블록이 존재·유효한지 확인

나. 타임스탬프 값이 이전 블록의 타임스탬프 값보다 크고 2시간 이내인지 확인

다. 작업증명(Proof of work) 유효여부 확인

라. S[0]를 이전 블록의 마지막 상태가 되도록 설정

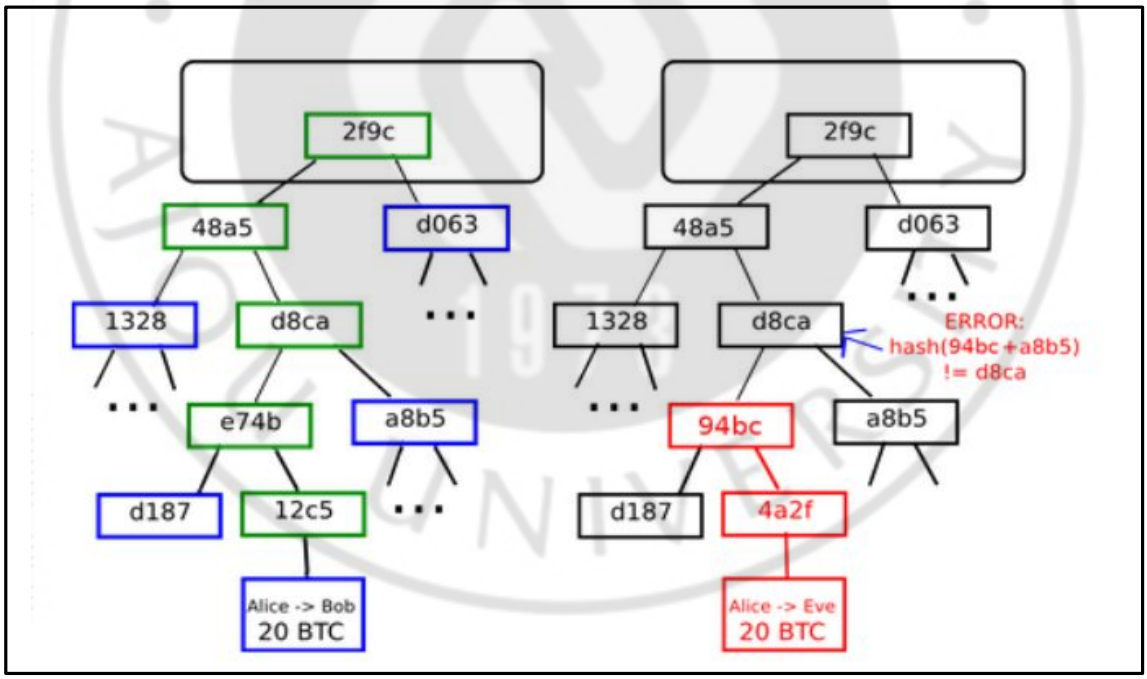
마. TX가 n개의 트랜잭션 목록을 구성하고 0부터 n-1까지 모든 i에 대하여 S[i+1]=APPLY(S[i], TX[i]) 의 집합 중 에러가 존재하면 거짓을 리턴하고 종료

바. 참을 리턴하고 S[n]을 이 블록의 마지막 상태로 등록

블록에 있는 각 트랜잭션은 유효한 상태 변환이 일어나야 하고 원시상태(Genesis

state)부터 해당 블록까지 모든 트랜잭션을 순차적으로 적용하여 최종 상태가 계산될 수 있다. 따라서 블록에 포함되는 트랜잭션의 순서는 매우 중요하게 된다. 만약 어떤 블록에 A와 B라는 트랜잭션이 있고 B가 A의 출력 UTXO를 소비한다고 하면 A가 B이전의 트랜잭션인 경우 유효하지만 그렇지 않을 경우 유효하지 않게 된다.

머클트리(Merkle Tree)는 블록체인을 효율적으로 사용하게 해주는 역할을 한다. 특히나 블록체인 전체용량은 계속적으로 증가하므로 작은 용량이 필요로 하는 모바일 플랫폼 등에서 사용하기 수월하게 해주는 역할을 할 것이다. 일정 시간이 지난 승인이 확정된 기존의 블록 데이터를 삭제하고 머클트리가 해시 값을 보장하기 때문이다. 또한 블록의 헤더만으로 작업증명을 검증하고 트랜잭션들의 겉가지만 다운로드하여 임의의 트랜잭션 상태를 알 수 있도록 할 수 있다.



출처 : Vitalik Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform”

그림 7. 머클트리(Merkle Tree) 구조

블록의 유효성 검증 알고리즘에서 작업증명의 조건은 SHA-256 암호화 알고리즘에서 다수의 0비트들로 시작되는 해시 값을 찾는 과정이다. 0비트의 목표 개수가 블록체인의 생성 난이도가 된다. 작업증명의 목적은 블록 생성을 어렵게 만들어 공격자들이 마음대로 블록체인을 조작하는 것을 방지하기 위한 것이다. SHA-256 암호화 알고리즘은 난수 함수로 설계되었기 때문에 해시 값을 찾는 유일한 방법은 블록 헤더의 임의 값(Nonce)을 계속 증가시켜 조건에 만족하는 해시 값을 찾는 방법뿐이다. 일반적으로 매 2,016개의 블록마다 0비트의 목표개수를 재조정하여 난이도를 조정하게 되고 평균적으로 10분마다 노드들이 새로운 블록을 생성할 수 있도록 한다. 난이도 조정은 다음과 같이 표현할 수 있다.

$$\text{new 목표개수} = \text{old 목표개수} \times \frac{\text{최근 2,016블록 생성 시간(초)}}{\text{2주(초)}}$$

새롭게 발견된 해시 값은 현재 블록 뒤를 잇는 다음 블록의 주소가 되고 현재 블록에 담긴 트랜잭션 내역들은 정상임을 확정하게 된다. 이렇듯 새 블록의 해시 값은 이전 해시 값과 이전 거래 해시 값들이 모두 들어 있으므로 원시상태부터 현재까지 모든 내역이 담겨있는 암호화된 값이라 볼 수 있다. 따라서 채굴(Mining)은 모든 거래내역을 업데이트 하는 행위라 볼 수 있겠다.

제 2 절 전자투표의 블록체인

제 1 항 블록체인의 구분

블록체인의 장점을 활용하기 위하여 세계의 많은 개발자들은 다양한 기능의 블록체인을 개발하고 있다. 해킹이 불가능한 분산 DB라는 장점은 '페이팔(Paypal)' 등 금융권에서도 주목하고 있으며, IBM·삼성 등 IT기업들이 사물인터넷(IoT)에 적용하

는 등 다양한 분야에 활용가능성을 넓혀가고 있다.

이러한 블록체인은 비트코인의 개발을 기점으로 3가지 종류로 나타낼 수 있다.

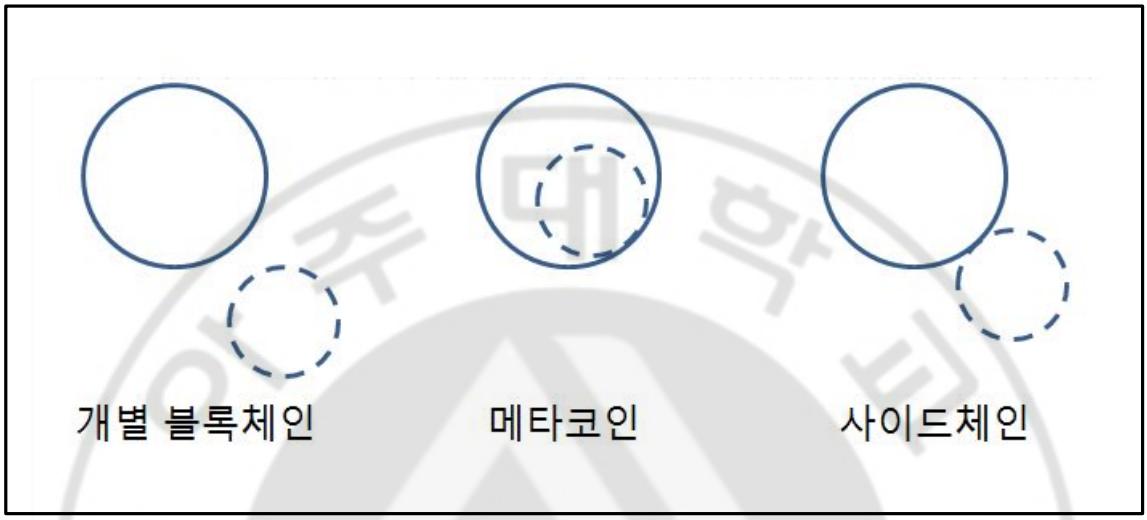


그림 8. 블록체인의 종류

개별 블록체인(Private Blockchain)은 비트코인의 블록체인을 모방하여 새롭게 개발하는 형태로써 주로 실험용이나 분산 어플리케이션(Dapp)을 개발하는데 사용되어지고 있다.(ex. Ethereum, Bitshares)

메타코인(Metacoin)은 비트코인의 블록체인 위에서 추가적 기능을 제공하는 것으로 비트코인 블록체인의 한계를 벗어날 수는 없지만 비트코인 네트워크의 안정성이 보장되어지는 형태이다.(ex. Counterparty, Omni)

사이드체인(Side-chain)은 개별 블록체인을 비트코인 블록체인에 연결하여 사용하는 것으로써 비트코인 블록체인의 데이터를 공유하는 동시에 개발에 대한 한계를 극복할 수 있는 형태이다.(ex. Factum, Blockstream)

또한 블록체인을 다양한 분야에 활용하기위해서는 필요 용도에 따라서 중앙집중식과 탈 중앙집중식으로 구분하여 활용할 수 있을 것이다. 즉, P2P 네트워크에 접속하는 각 노드들의 참여를 컨트롤함으로써 블록체인을 구분할 수 있다.

그림 9. 블록체인의 구분

무허가 블록체인(Permissionless Blockchain)은 블록을 채굴하는 검증자 노드들과 블록체인을 이용하는 사용자들이 특별한 허가 없이 자유롭게 네트워크에 참여하여 사용하는 것으로써 익명성과 탈 중앙집중식을 구현하는 블록체인이다.(ex. Bitcoin, Ethereum)

반허가 블록체인(Semi Permissioned Blockchain)은 검증자 노드들을 허가를 통하여 네트워크에 참여시키고 사용자는 자유롭게 참여하는 방식으로써 한정된 탈 중앙집중식을 구현하게 된다.(ex. Ripple)

허가 블록체인(Permission Blockchain)은 검증자 노드들과 사용자를 특정 중앙기관의 허가를 통하여 네트워크에 참여시키게 됨으로써 중앙집중식 구조를 따르게 되고 모든 작업을 컨트롤할 수 있다.

블록체인의 분산처리의 기술만이 필요할 경우 허가 블록체인을 사용하여 중앙집중식 방식으로 인증의 신뢰를 갖추게 될 수 있으며, 검증자는 검열이 가능하게 되므로 책임을 지게 되는 법적근거를 갖출 수 있다. 따라서 시빌공격에 대한 비용이 필요하지 않으며, 다량의 컴퓨팅 파워도 필요하지 않으므로 운영비용이 적은 장점이 있다.

무허가 블록체인은 모든 참여자의 익명성을 보장하기 때문에 검열이 불가능하게

되고 검증자와 사용자가 네트워크 참여를 자유롭게 할 수 있으므로 탈 중앙집중식 네트워크를 형성하게 된다. 따라서 시빌공격에 대한 비용이 필요하고 다량의 컴퓨팅 파워가 투입되므로 운영비용이 크다는 단점이 있다.

제 2 항 전자투표 블록체인의 구조

전자투표 시스템에 블록체인을 활용할 수 있도록 하기 위해서는 프로그래밍 코드 형태의 트랜잭션을 생성하여 블록체인에 저장하는 방식이 필요하다. 따라서 개발의 한계가 없고 필요시마다 새로운 분산 어플리케이션(Dapp)을 만들 수 있는 '개별 블록체인'을 활용한다.

사용용도에 따른 방식으로는 무허가 블록체인 방식을 사용한다면 전자투표에서 중요한 익명성을 보장해 줄 수 있지만 많은 운영비용이 발생하고 검증자 노드에 대한 검열이 불가능하여 법적근거에 문제가 될 수 있다. 또한 허가 블록체인 방식을 사용한다면 특정기관의 중앙집중식으로 인하여 가장 중요한 신뢰성과 무결성을 훼손하게 될 수 있으므로 전자투표 블록체인은 '반허가 블록체인'방식을 사용하여 검증자에 대한 정보를 공개하고 법적근거를 확보하는 동시에 사용자(투표자)에 대한 익명성을 보호하는 방식을 활용토록 하겠다.

제 3 장 전자투표 시스템 구현

제 1 절 전자투표 시스템 설계

제 1 항 전자투표 기능 구성

전자투표 시스템의 블록체인 개발을 위해서 '이더리움(Ethereum)' 플랫폼을 사용하며, 반허가 블록체인 방식을 따른다. 따라서 유권자는 자율적으로 참여가 가능하지만 검증자 노드는 사전에 자발적 참여 신청을 받아 신원확인 후 블록체인 네트워크에 참여토록 한다. 자발적 참여자가 없을 것을 대비하여 중앙기관(선관위)에서는 기본적으로 한 개의 노드로 참여를 한다. 따라서 검증자 노드는 자발적 참여자 수가 n이였을 경우 총 n+1이 될 것이다. 이 후 블록체인에 부정행위가 감지된다면 해당 검증자 노드는 공격행위를 한 것으로 간주하고 법적 제재를 당할 것이다. 하지만 블록체인의 작업증명이 있는 한 부정행위는 무산될 것이고 투표시스템은 안정적으로 지속될 것이다.

블록체인 네트워크에서 거래를 생성할 때 컨트랙트를 생성하게 되면 화폐의 전송이 아닌 프로그래밍 코드형태의 데이터를 전송할 수 있다. 이더리움 플랫폼은 해당 코드를 실행할 수 있는 컴파일러가 내장되어 있으므로 컨트랙트를 사용하면 블록체인 기술을 활용하는 프로그램을 만들 수 있다. 이런 컨트랙트 프로그래밍 코드는 블록체인의 거래 데이터와 동일하므로 해당 데이터를 임의로 조작할 수 없다. 따라서 데이터베이스 역할 뿐만이 아니라 프로그래밍 코드 역할도 안정성이 담보되는 시스템이라 할 수 있겠다.

전자투표 시스템의 구성은 총 5가지 기능으로 구분되어 진다.

1. 유권자 등록 2. 선거 등록 3. 투표 4. 집계 5. 개표

각 기능의 구성도는 다음과 같다.

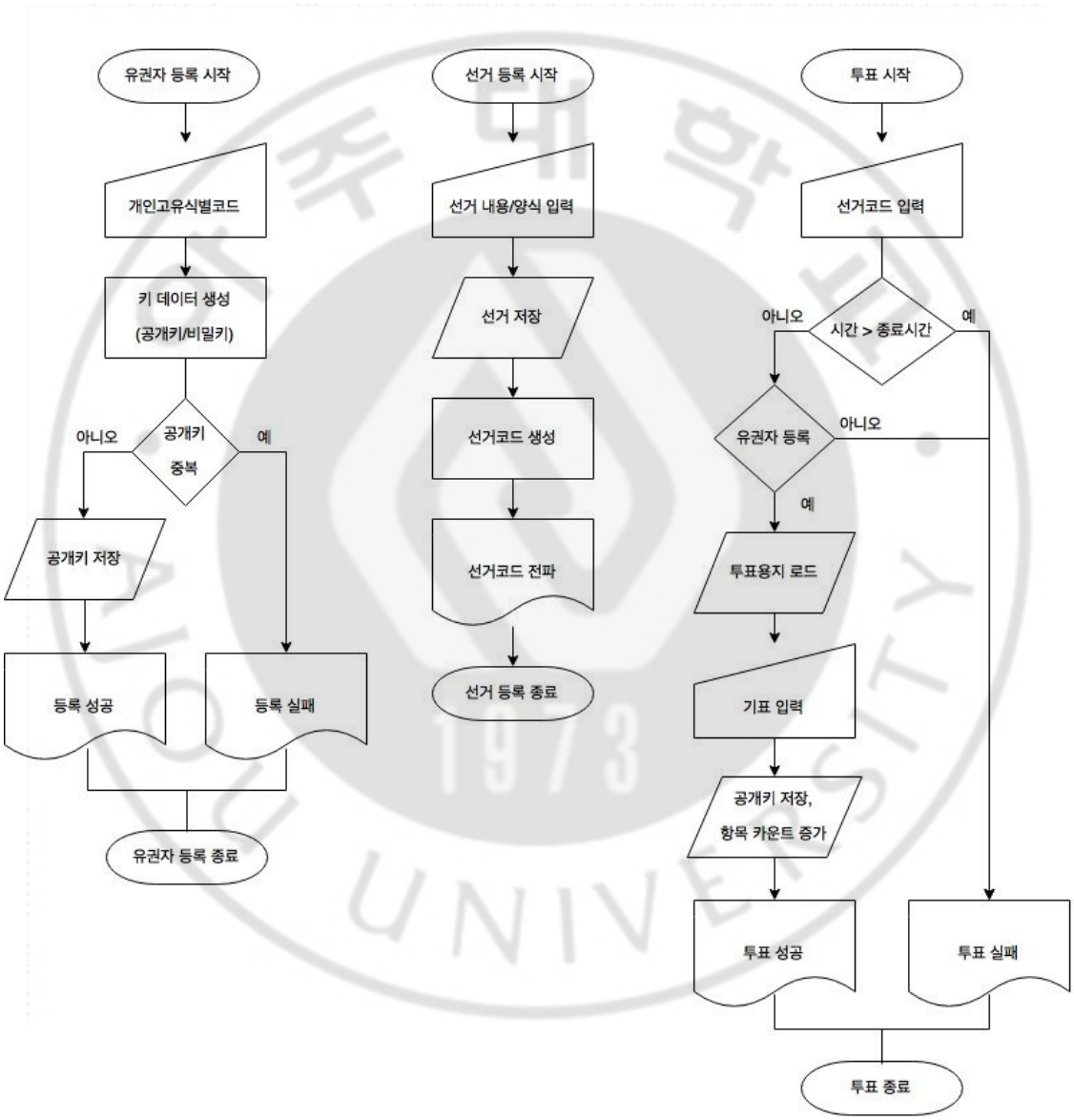


그림 10. 전자투표 시스템 기능 구성도 1

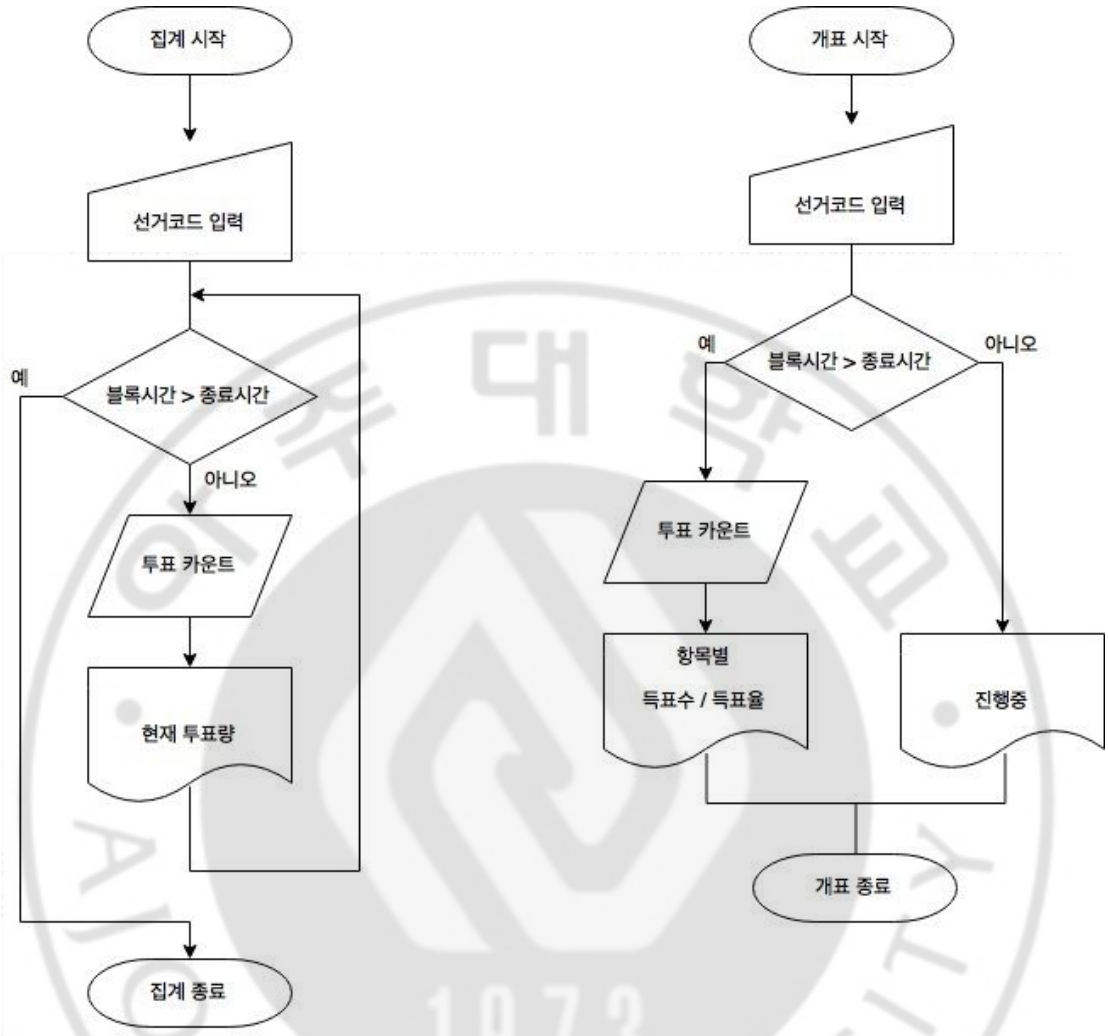


그림 11. 전자투표 시스템 기능 구성도 2

1. 유권자 등록

관리자는 투표권을 부여할 유권자 리스트를 확인하여 권한이 있는 유권자가 투표에 참여토록 유도하고 유권자는 투표 전 유권자 등록을 마친 후 신분확인 절차를 마치고 투표권을 행사하게 된다.

관리자는 블록체인에 유권자 데이터베이스로 사용할 컨트랙트를 생성한다.

```
contract regUser
{
    struct addr_type
    {
        uint addr_count;
        mapping(uint => address) addr;
    }
    mapping(address => addr_type) reg_user;

    function addr_set(address v_vote, address v_user)
    {
        addr_type v = reg_user[v_vote];

        v.addr_count++;
        v.addr[v.addr_count] = v_user;
    }

    function addr_get(address v_vote, uint v_index) constant returns (address retVal)
    {
        addr_type v = reg_user[v_vote];

        return v.addr[v_index];
    }

    function addrCnt_get(address v_vote) constant returns (uint retVal)
    {
        addr_type v = reg_user[v_vote];

        return v.addr_count;
    }
}
```

그림 12. 유권자 등록 컨트랙트

컨트랙트는 유권자 코드를 저장하는 addr_set 메소드와 조회하는 addr_get 메소드 및 등록된 총 유권자수를 조회하는 addrCnt_get 메소드로 구성하였다.

선거 코드에 의해 참조되는 연관 배열(associative array)을 만들고 해당 선거 코드마다 유권자 코드와 등록 유권자 수를 구조체로 만들어 3차원 배열이 되도록 한다.

사용자는 유권자 등록을 하게 되면 중복 및 조건 검사를 하고 이상이 없을 경우 해당 컨트랙트에 유권자 코드를 저장하게 된다. 향후 투표 시 유권자 등록 컨트랙트에 유권자 코드가 존재하게 되면 투표권이 있는 것으로 간주하게 된다.

2. 선거 등록

관리자는 선거 내용이 저장될 수 있는 선거 컨트랙트를 블록체인에 생성한다.

```
contract voteStorage
{
    struct v_value_type
    {
        uint v_count;
        mapping(uint => mapping(uint => string32)) v_value_str;
    }
    string32 endTime;
    uint addr_count;
    mapping(address => uint) addr;
    mapping(uint => string32) v_title;
    mapping(uint => v_value_type) v_value;

    function v_title_set(string32 s1, string32 s2, string32 s3, string32 s4, string32 s5)
    {
        v_title[0] = s1;
        v_title[1] = s2;
        v_title[2] = s3;
        v_title[3] = s4;
        endTime = s5;
    }

    function v_title_get(uint v_index) constant returns (string32 retVal)
    {
        if(v_index == 4)
            return endTime;
        else
            return v_title[v_index];
    }

    function v_value_set(uint v_index, string32 v_value1_1, string32 v_value1_2, string32 v_value2_1, string32 v_value2_2)
    {
        v_value[v_index].v_value_str[1][1] = v_value1_1;
        v_value[v_index].v_value_str[1][2] = v_value1_2;
        v_value[v_index].v_value_str[2][1] = v_value2_1;
        v_value[v_index].v_value_str[2][2] = v_value2_2;
    }

    function v_value_get(uint v_index, uint v_value1, uint v_value2) constant returns (string32 retVal)
    {
        return v_value[v_index].v_value_str[v_value1][v_value2];
    }

    function v_data_set(uint v_index, address v_user)
    {
        if(addr[v_user] != 0)
        {
            v_value[addr[v_user]].v_count--;
            addr_count--;
        }

        v_value[v_index].v_count++;

        addr[v_user] = v_index;
        addr_count++;
    }

    function v_data_get(uint v_index) constant returns (uint retVal)
    {
        if(v_index == 0)
            return addr_count;
        else
            return v_value[v_index].v_count;
    }
}
```

그림 13. 선거 컨트랙트

선거 컨트랙트도 역시 데이터는 get 메소드와 set 메소드로 저장하거나 조회하도록 구성하였다. 블록체인에 컨트랙트가 올라가게 되면 set 메소드를 사용하는 방법 이외의 데이터 조작은 불가능하다.

선거의 제목과 항목, 종료시간을 저장할 수 있는 문자열 변수를 만들고 유권자 코드로 참조되는 투표 값이 저장될 연관 배열(associative array)을 만들었다. 유권자 코드를 배열의 참조 값으로 사용하기 때문에 여러 번 재투표를 하여도 마지막 투표 값이 저장되어 투표 종료 시까지 투표를 수정할 수 있다. 또한 수정을 못하게 할 경우는 한번만 투표가 가능하게 할 수 있다.

주의할 점은 블록체인의 데이터는 모두에게 공개가 되므로 유권자 코드가 어떠한 값을 저장하고 있는지(투표에서 어떤 항목을 선택하였는지) 유추할 수 없도록 유권자 코드를 랜덤 코드 값으로 대체 시켜준다.

3. 투표, 집계, 개표

유권자는 블록체인 네트워크에 접속하여 유권자 등록 컨트랙트와 선거 컨트랙트를 액세스하여 언제 어디서든지 온라인으로 사용할 수 있는 탈 중앙집중식 전자투표 시스템을 사용해 투표하고 개표 값을 조회 할 수 있다.

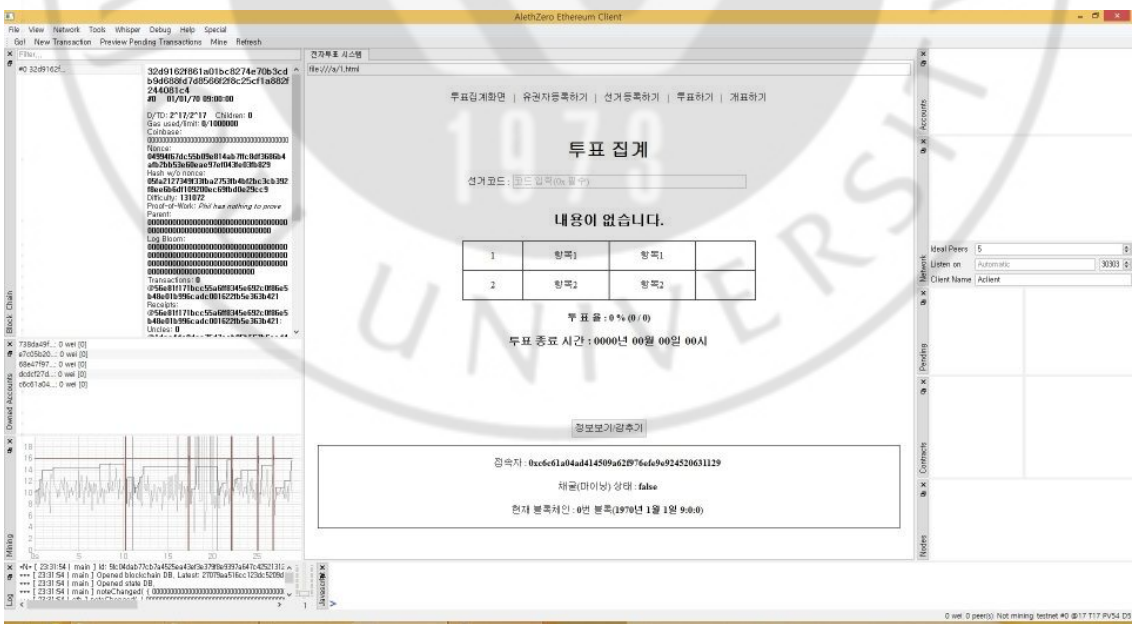


그림 14. 전자투표 시스템 연구 모델

제 2 항 개발 도구

테스트 환경으로 가상머신(VMware)을 사용하였으며, 노드별 사양은 다음과 같다.

표 6. 테스트 환경의 노드 사양

하드웨어	인텔 i7-4550U 1.5GHz 1 Core / 2GB RAM / 60GB HDD
소프트웨어	윈도우 Embedded 8.1 Industry Pro x64 / Aelthzero
프로그램 언어	HTML / CSS / Javascript / Web3 / Solidity

제 2 절 전자투표 시스템 구현

제 1 항 전자투표 모의 테스트

전자투표 모의 테스트는 관리자와 검증자(마이너), 유권자 입장에서 진행되며, 검증자는 보통 유권자 중에서 자발적 참여로 이루어 질 것이다. 주요 역할을 살펴보면 관리자는 선거를 생성하는 역할을 하고 검증자는 블록체인 네트워크를 구성하는 역할을 한다. 유권자는 투표권을 행사하는 역할을 하며, 모든 사용자는 공동의 동일한 데이터를 조회해 볼 수 있는 공공 분산 데이터베이스 시스템으로 이용할 수 있게 될 것이다.

전자투표 모의 테스트를 위한 연구 모델은 HTML 웹페이지로 인터페이스를 구성하였고 블록체인은 Solidity로 컨트롤 하였으며, HTML과 Solidity의 연동은 Web3 JSON으로 작성하였다.

전자투표 진행과정을 정리하면 다음과 같다.

그림 15. 전자투표 시스템 Activity Diagram

1. 선거 등록

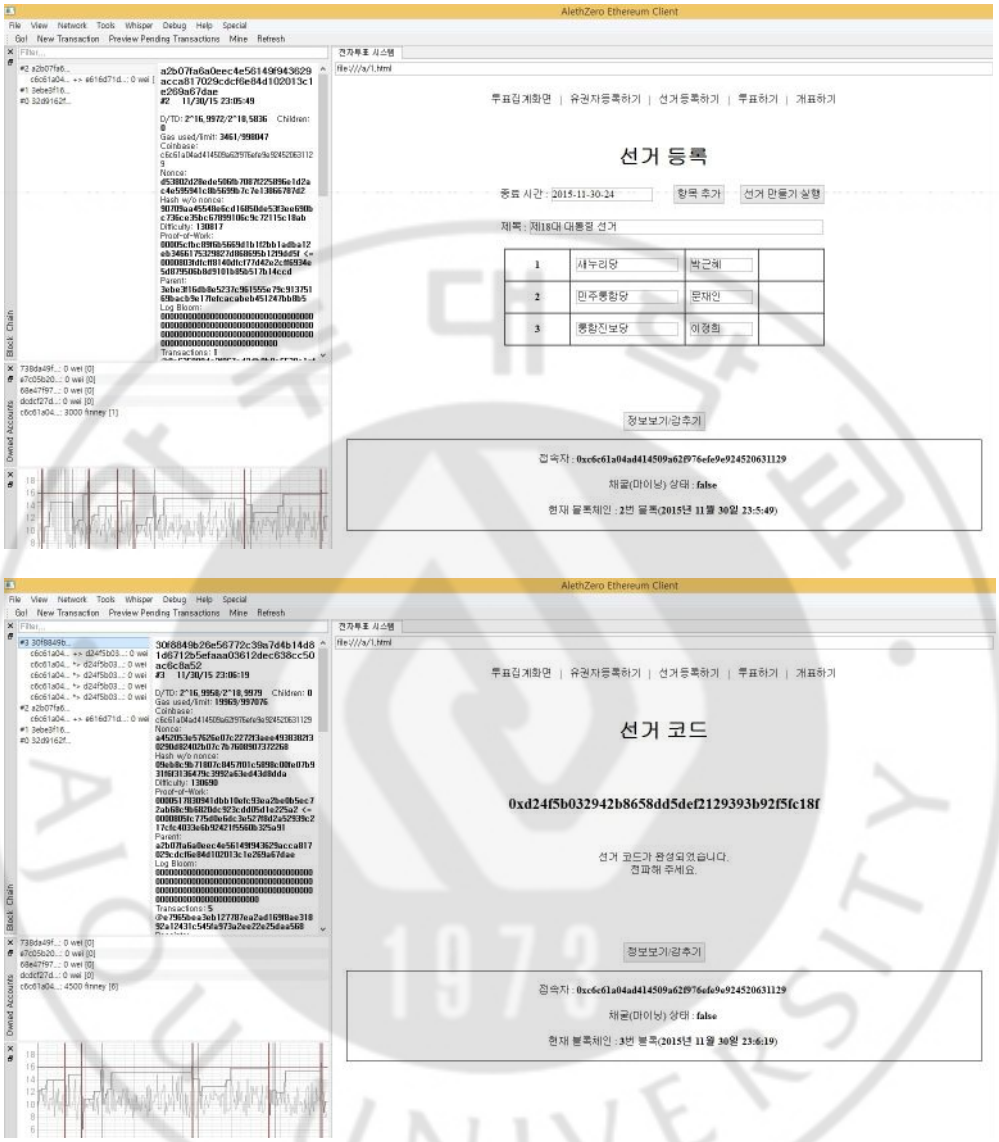


그림 16. 전자투표 시스템 - 선거 등록

관리자는 선거의 내용과 종료 날짜를 HTML 입력 폼에 입력하고 트랜잭션을 블록체인 네트워크에 전송하게 되면 선거 컨트랙트가 새로 생성되고 선거 코드를 획득한다. 생성된 선거 코드를 유권자에게 다양한 방법으로 전파를 한다.

2. 유권자 등록

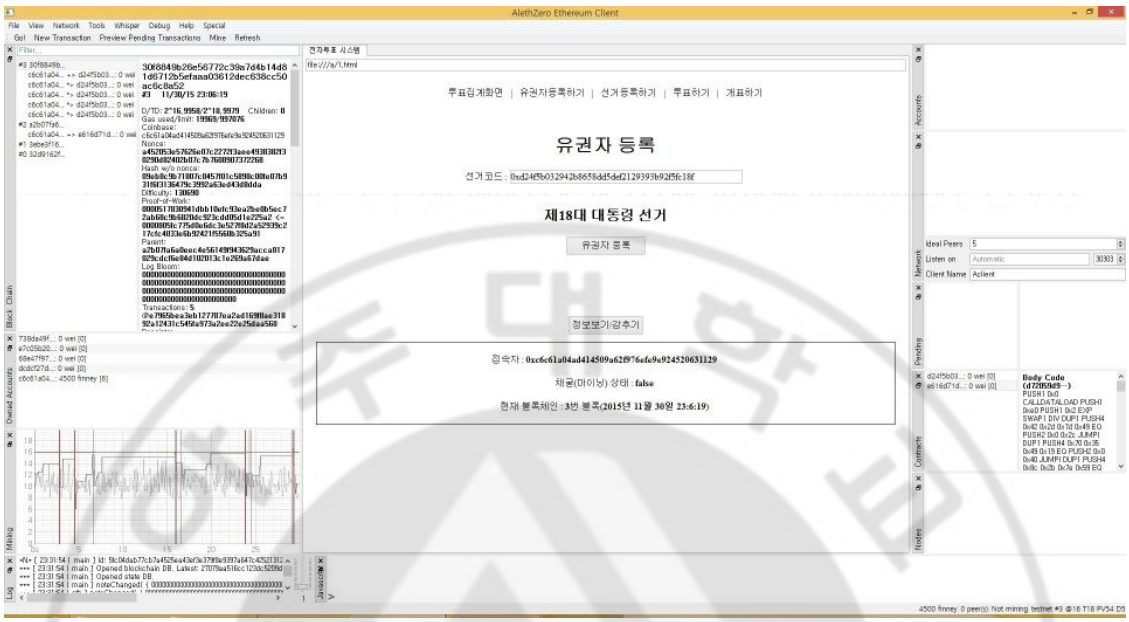


그림 17. 전자투표 시스템 - 유권자 등록

유권자는 선거 코드를 다양한 방법으로 획득하게 되면 유권자 등록 페이지에서 선거 코드를 입력한 후 유권자 등록을 한다.

3. 투표

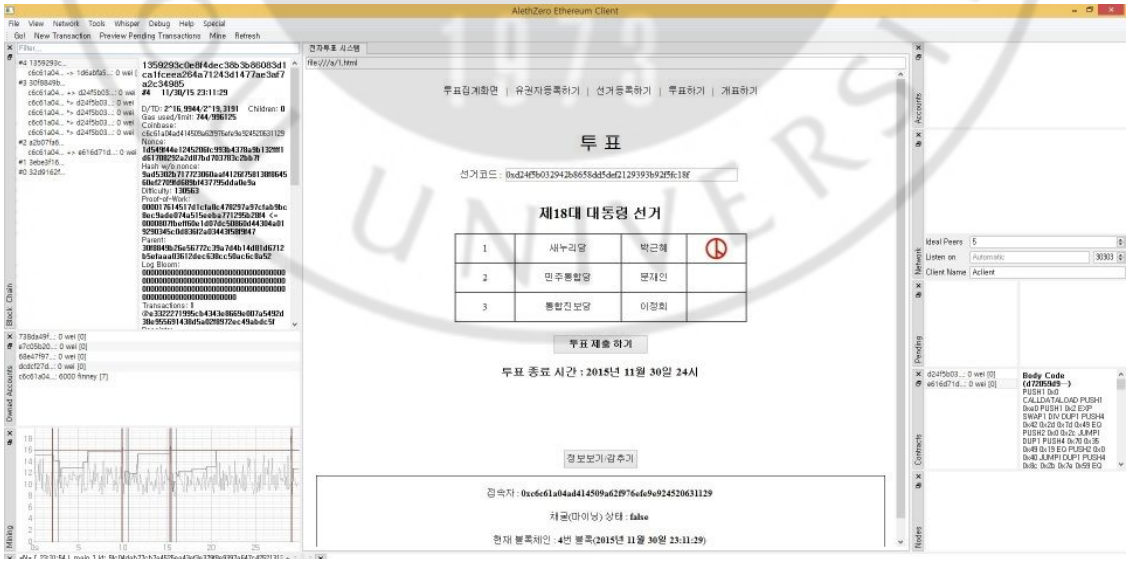


그림 18. 전자투표 시스템 - 투표

유권자가 투표하기 페이지에서 선거 코드를 입력하게 되면 블록체인에 저장되어 있는 선거 컨트랙트의 데이터를 get메소드로 불러오게 되며, 투표를 할 수 있는 기표용지를 화면에 만들어준다.

유권자는 투표 종료시간 이전 및 유권자 등록 목록에 등록된 계정 조건을 만족한다면 정상적 투표를 진행 할 수 있으며, 투표 데이터는 유권자 코드와 함께 트랜잭션을 만들어 선거 컨트랙트로 전송된다. 선거 컨트랙트는 set메소드를 호출하여 유권자 코드로 연관 배열에 매핑 시켜 투표데이터를 저장한다. 유권자는 투표시간 종료 전까지 재투표를 통하여 투표내용을 수정할 수 있다.

4. 투표 집계

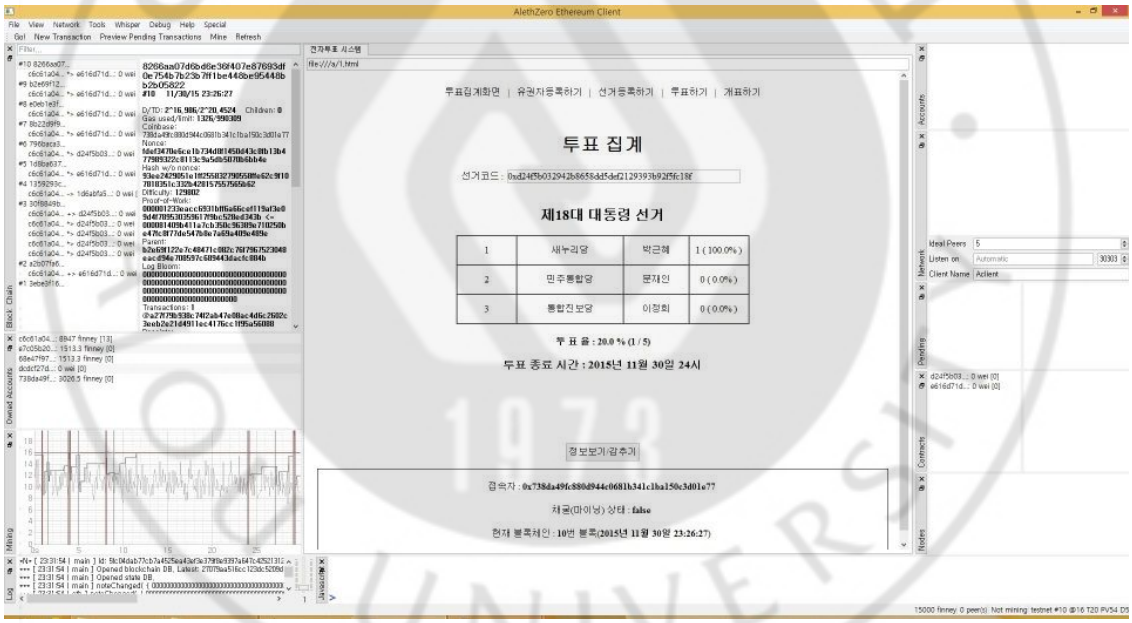


그림 19. 전자투표 시스템 - 투표 집계

집계 화면은 준 실시간으로 선거 컨트랙트의 get메소드를 호출하여 화면을 업데이트 시켜줌으로써 투표의 집계 내용을 모니터링 할 수 있다. 화면 업데이트 주기는 트랜잭션이 승인되는 새로운 블록 생성 시간으로 한다. 집계 화면은 실시간으로 투표에 영향을 줄 수 있는 부분이므로 공개와 비공개를 중앙기관(선관위)에서 선택하여야 할 것이다.

5. 개표

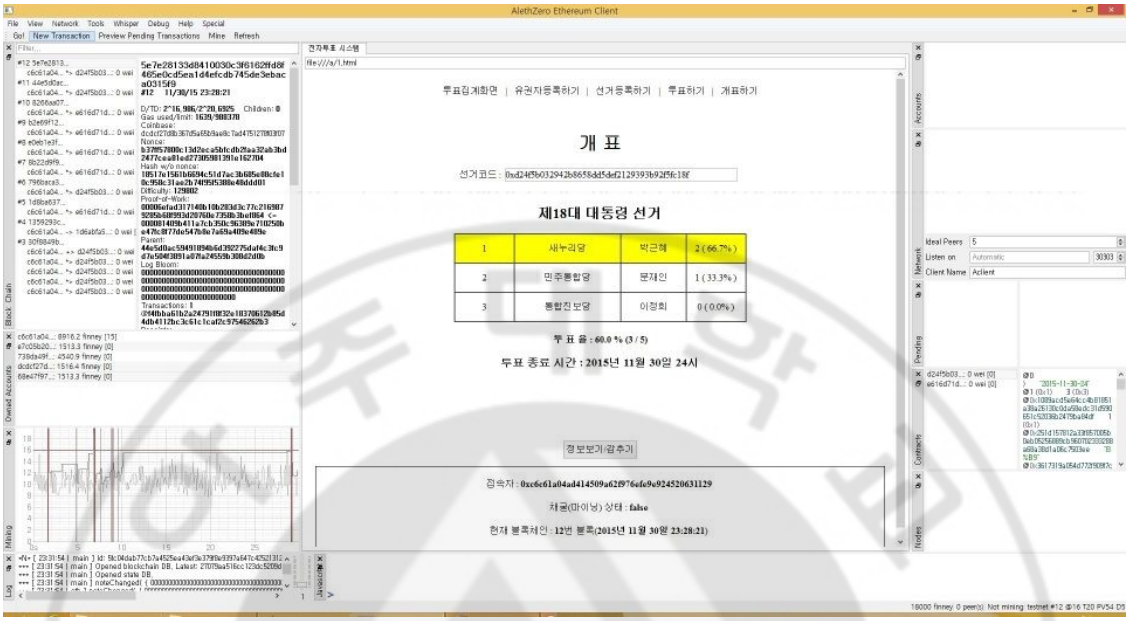


그림 20. 전자투표 시스템 - 개표

마지막으로 개표화면은 투표의 결과를 조회하는 화면으로써 선거 코드를 입력하게 되면 투표의 종료시간을 체크하여 투표시간이 끝났을 경우에 투표데이터를 조회하고 결과를 산정하여 화면에 출력한다.

각 항목의 득표수와 투표율(등록 유권자수/투표한 유권자수)을 산정할 수 있다.

제 2 항 전자투표 공격 테스트

전자투표 시스템에서 공격자가 자신이 원하는 투표결과를 만들기 위해서는 블록체인의 데이터를 변조·조작하여 재전파하는 방법이 있다. 초기 블록(Genesis Block)을 제외한 모든 블록들은 이전의 블록의 해시 값을 참조하기 때문에 데이터를 변조·조작 한다는 것은 그 시점부터 새로운 블록체인이 생성된다는 뜻이다.

따라서 블록의 데이터를 변조·조작하여 분기점(Fork)을 만들고 정상 블록체인과 경

합을 하게 된다.

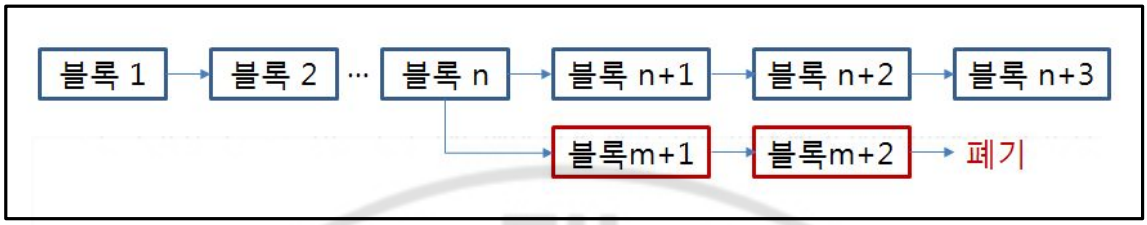


그림 21. 블록체인 분기(Fork)

실험 환경에서 사양이 동일한 노드를 3개를 생성하였고 블록체인으로 연결을 하였다. 그 중 1개의 노드에서 데이터를 변조·조작하여 블록체인에 분기(Fork)를 일으켰으나 정상 블록체인과의 경합에서 뒤처지며 정상 블록체인의 데이터로 동기화 되었다.

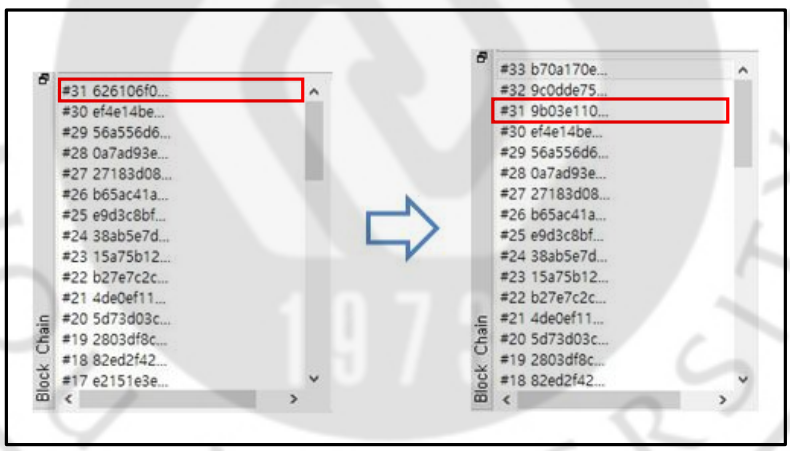


그림 22. 블록체인 분기(Fork) 동기화 결과

따라서 블록체인의 데이터 변조 및 중복 사용은 정상 블록체인과 경합에서 승리하여야 가능하며, 실패하게 되면 무력화 된다.

반허가 블록체인에서는 검증자에 대한 허가를 시행하기 때문에 1개의 노드 해시레이트(Hashrate)가 전체의 51%이상을 차지하지 않도록 관리자의 승인이 전제되어야 하며, 투표 종료까지 검증자들에 대한 해시레이트 모니터링이 이뤄져야 할 것이다.

제 3 항 전자투표 시스템 평가

전자투표 시스템을 구현하는데 블록체인 방식을 사용하였다. 해당 시스템은 중앙집중식(서버-클라이언트) 방식의 대표적 위험성인 데이터 변조·조작과 파괴·마비를 대응하는 안정적인 보안성을 기대할 수 있었다.

데이터 변조·조작은 검증노드(마이너)의 작업 증명을 통해 승인된 데이터를 모아 블록이란 저장소를 지속적으로 생성하여 저장하고 이전 블록을 참조하여 변조·조작에 대응하였다.

파괴·마비는 P2P 네트워크를 기반으로 시스템을 구축하였기 때문에 어느 한 공격지점(서버)을 공격자가 설정할 수 없었고 전체 노드가 동일한 데이터를 공유하고 있기 때문에 전체 노드를 파괴하기 전까지는 네트워크를 마비시킬 수 없었다.

표 7. 투표 방식에 따른 비교

구 분	종이투표	중앙집중식 전자투표	탈 중앙집중식 전자투표
투표율	낮다	높다	높다
개표 시간	길다	짧다	짧다
선거 비용	높다	낮다	낮다
데이터 집계 오류	높다[23]	낮다	낮다
데이터 변조·조작	낮다	높다	낮다
데이터 파괴·마비	낮다	높다	낮다
데이터 검증 (신뢰성)	비공개 (투표지 분류기)	비공개 (영업비밀)	공개 (오픈소스)

따라서 블록체인을 활용한 '탈 중앙집중식 전자투표 시스템'은 기존 방식의 '종이투표'와 '중앙집중식 전자투표'의 장점이 결합된 모습을 기대할 수 있었다. 더불어 데이터 검증 작업은 누구나 자발적으로 참여할 수 있기 때문에 기존의 시스템에서는 부족했었던 유권자의 신뢰성 확보를 추가적으로 얻을 수 있을 것이다.

23) 제18대 대선(2012. 12. 19) 4개 투표구에서 86표 집계 오류, (뉴시스, "선관위, 개표상황표에 '투표분류 종료시각' 삭제 논란", http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140602_0012957644&cID=10312&pID=10300)

제 4 장 전자투표 성능 개선 모델

제 1 절 연구 설계

제 1 항 문제점 및 성능 개선안

블록체인 방식을 활용한 전자투표 시스템은 탈 중앙집중식이므로 블록체인 네트워크에 참여중인 각 노드들의 컴퓨팅 자원을 기반으로 분산시스템이 구축된다. 따라서 서버의 자원만을 기반으로 구성된 중앙집중식 형태의 방식보다 컴퓨팅 자원이 많이 소모된다. 또한 금융거래 및 PC·전용장비에 최적화 되어 있는 블록체인 구성 방식은 익명성을 중점으로 하기 때문에 컴퓨팅 자원의 낭비가 높다.

전자투표 시스템은 투표 결과에 대한 익명성만 보장하면 되고 시스템 사용시간도 한정되어 있으며, 시스템 보안성을 중점으로 다양한 플랫폼(모바일)을 수용할 수 있어야 하기 때문에 컴퓨팅 자원의 낭비를 최대한 줄이고 성능을 향상 시켜야 한다.

따라서 컴퓨팅 자원을 효율적으로 활용할 수 있도록 다음과 같은 요구사항을 만족하는 성능 개선안을 제안한다.

표 8. 전자투표 성능 개선안 요구사항

구 분	요구사항	요구수준
1	컴퓨팅 파워	30%이상 감소
2	블록 충돌	
3	저장 용량	
4	네트워크 사용량	

현재 PC 대비 모바일(스마트폰)의 사양이 3분의2 수준[24]을 형성하고 있으므로 개선안의 요구수준은 각 30%이상 성능향상을 기대한다.

위 4가지 성능 개선 요구사항을 만족하는 개선안은 블록체인 네트워크에서 블록의 개수를 감소시키는 것으로 요구사항을 충족시킬 수 있다.

1번 요구사항 '컴퓨팅 파워'는 데이터가 없는 비어있는 블록 채굴을 최소화한다.

2번 요구사항 '블록 충돌'은 전체 블록의 수량을 감소시켜 충돌 확률을 줄인다.

3번 요구사항 '저장 용량'은 블록 1개당 1MB이내이므로 블록의 수량을 감소시켜 저장 용량을 줄인다.

4번 요구사항 '네트워크 사용량'은 블록 채굴에 대한 브로드캐스트를 감소시켜 네트워크 사용량을 감소시킨다.

전자투표 성능 개선안 메커니즘은 다음과 같다.

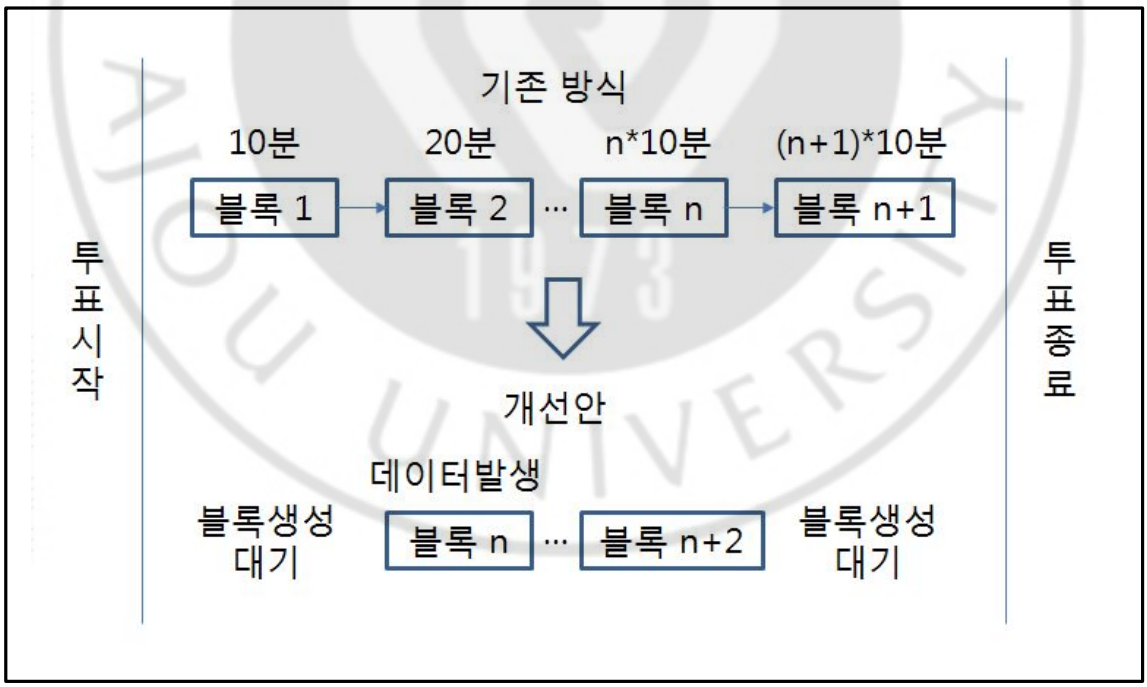


그림 23. 전자투표 성능 개선안 메커니즘

24) PC(코어i5) 3.3GHz : 모바일(갤럭시S6) 2.1GHz

제 2 항 실험 환경

모의실험을 위하여 테스트 환경에 같은 사양의 노드 3개를 생성 후 블록체인 네트워크를 구성하였다. 그리고 블록체인에 대한 로그를 수집하기 위해 수집서버를 연동하였다.

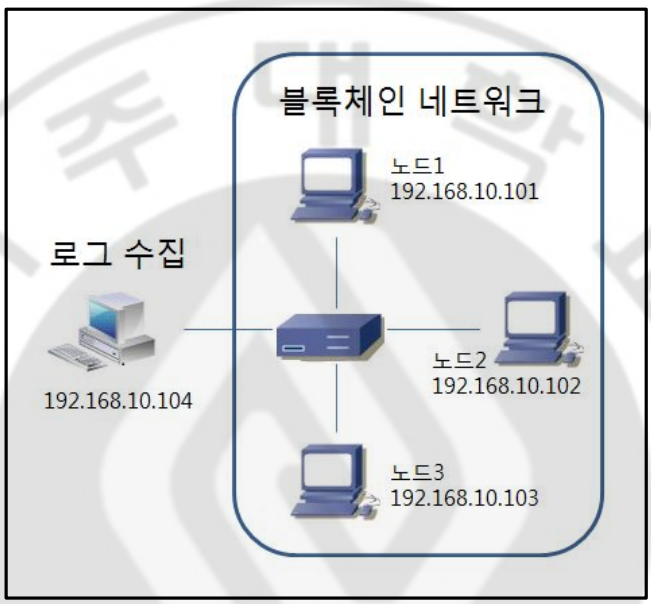


그림 24. 모의실험 구성도

제 2 절 연구 결과

제 1 항 성능 실험

전자투표 개선안의 성능 실험은 10분 동안 3개의 노드가 1번씩 투표(총 3회)한다는 가정 하에 진행 하였다. 또한 최상 / 최악의 조건을 상대로 데이터를 도출하였다.

최상의 조건은 1개의 블록에 모든 데이터가 몰리는 경우(모든 데이터가 한 개의 블록에 중첩되어 저장)이고 최악의 조건은 데이터가 중첩되지 않은 경우이다.

로그 수집서버에서 수집하는 블록체인 로그 정보는 다음과 같다.

표 9. 블록체인 로그 정보

블록 인덱스	블록 생성시간	해시레이트	블록 충돌 분기(Fork)

각 노드에는 web3와 Javascript를 활용하여 로그 저장 모듈을 구현하였다.

```
web3.eth.watch('chain').changed(
function()
{
    var number = web3.eth.number; // 블록 번호
    var hashrate =  web3.eth.hashrate; // 해쉬레이트
    var timeStamp = Number(web3.eth.block(number).timestamp + "000"); // 블록 시간
    timeStamp = new Date(timeStamp);
    timeStamp = timeStamp.toLocaleDateString()+' '+timeStamp.getHours()+':'+timeStamp.getMinutes()+':'+timeStamp.getSeconds();

    var fso = new ActiveXObject('Scripting.FileSystemObject');
    var file = fso.CreateTextFile('result.log', true);
    file.WriteLine(number+','+hashrate+','+timeStamp);
    file.Close();
}
);
```

그림 25. 블록체인 로그 저장 모듈

제 2 항 성능 평가

1. 컴퓨팅 파워

기존방식은 투표 종료 시까지 계속적으로 컴퓨팅 파워를 소모하였다.

하지만 개선안에서는 불필요한 블록을 생성하지 않도록 데이터가 발생하면 블록 생성을 수행하였다. 블록 충돌(Fork)이 일어날 수 있으므로 작업 증명은 3개의 블록이 생성된 후 다시 블록생성 대기상태로 전환한다.

결과적으로 총 소모되는 컴퓨팅 파워는 감소하게 된다.

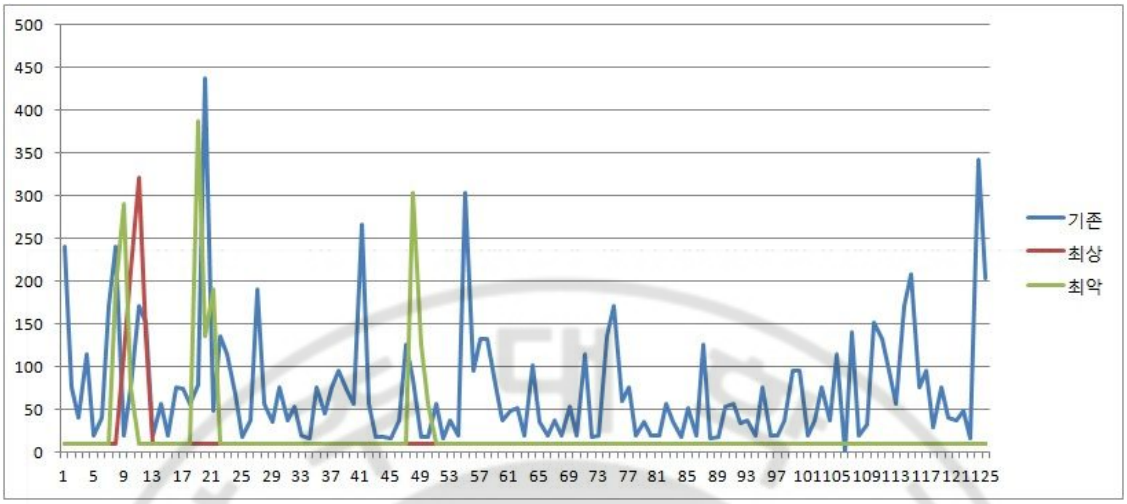


그림 26. 성능 개선안 컴퓨팅 파워 소모 비교

2. 블록 충돌

블록 충돌은 블록체인의 분기(Fork)와 같은 현상이다. 임의의 노드가 신규 블록을 채굴하여 브로드캐스팅 하는 시간 사이에 다른 노드도 신규 블록을 채굴하여 동시에 전파하였을 경우 발생한다. 결국 더 빠른 블록이 살아남고 늦은 블록은 폐기 된다. 결국 이 과정에서 발생한 자원 소모도 블록의 개수 감소를 통해 줄일 수 있다.

기존 방식에서는 2번의 충돌이 일어났으며, 개선안은 충돌이 일어나지 않았으므로 2번의 채굴 파워만큼 자원 낭비를 줄일 수 있었다.

3. 저장 용량

블록 1개의 최대 용량은 1MB이다. 블록체인의 블록 개수 감소는 전체 용량의 감소로 이어질 것이다. 다양한 플랫폼(모바일)에서 연동을 하기 위해서는 저장 용량 최적화가 중요한 화두가 될 것이다.

기존 방식에서는 총 126개의 블록이 채굴되었으며, 이것은 최대 126MB를 사용할 수 있다는 뜻이다. 하지만 개선안에서는 4~9MB의 적은 용량으로 효율적인 성능향

상을 볼 수 있었다.

4. 네트워크 사용량

네트워크 사용량도 저장 용량과 더불어 다양한 플랫폼(모바일)에 연동하는 중요한 요소 중 하나다. 기존 방식은 지속적인 블록 채굴 전파로 네트워크를 낭비하게 되는데 반해 개선안은 연결 세션만 유지하고 있으며 데이터가 발생할 시 네트워크 패킷을 사용하게 된다.

그림 27. 성능 개선안 네트워크 사용량 비교

종합적으로 전자투표 성능 개선안의 결과는 평균 87.6%의 성능 향상을 도출할 수 있었다. 이것으로 인해 다양한 플랫폼(모바일)에서도 연동이 가능해 질 수 있다.

표 10. 전자투표 성능 개선 비교

구 분	기존방식	개선안(최선/최악)	
컴퓨팅 파워	9,080kH/s	1,996kH/s(78% ↓)	2,917kH/s(68% ↓)
블록 충돌	1.6%(2/126)	0%(0/4)	0%(0/9)
저장 용량	126MB	4MB(97% ↓)	9MB(93% ↓)
네트워크 사용량	7,803Byte/s	294Byte/s(96% ↓)	474Byte/s(94% ↓)

제 5 장 결 론

본 논문은 기존의 온라인 전자투표 시스템의 보안성 문제를 해소하고 종이투표의 안정성을 모두 충족할 수 있는 데이터 처리 방향을 제시하였고 다양한 플랫폼(모바일)에 연동할 수 있도록 성능 향상 모델을 제안하였다.

또한 제안한 전자투표 시스템의 가장 중요한 특징은 중앙통제기관이 선거에 개입하지 못한다는 점이다. 즉, 정치적 영향을 받지 않는 전자투표 시스템을 구성하여 선거에서 가장 중요한 투명한 투표결과를 기대할 수 있도록 하는 것이다.

이로써 안전한 시스템이 개발된다 할지라도 대한민국의 공직선거에 바로 도입할 수 있는 요건이 충족되어진 것은 아닐 것이다.
전자투표제 도입에 무결성 보장 시스템이 큰 비중을 차지하고 있다하더라도 정치적인 사회배경과 문화 같은 수용해야 할 요건이 아직 많이 남아있어 앞으로 대한민국의 전자투표제 도입의 갈 길은 멀다고 볼 수 있기 때문이다.

이에 블록체인 방식의 “탈 중앙집중식 전자투표 시스템”에 방향이 앞으로의 대한민국 전자투표제 도입에 좋은 방향이 될 수 있기를 바란다.

본 논문의 연구모델은 블록체인의 기능에 대하여 중점을 두었으므로 보안코딩(Secure Coding)이 이루어지지 않았다. 실전에 투입되어질 프로그램은 보안코딩 작업이 필요할 것이며, 그 부분은 향후 오픈소스 프로젝트로 해결되어질 수 있다.

참 고 문 헌

1. 김도경, “사전투표제가 투표율에 미치는 영향”, 한국시민윤리학회보, 2014
2. 네이버 지식백과, “타원 곡선 전자 서명 알고리듬”, 한국정보통신기술협회 IT 용어사전
3. 노컷뉴스, “40만 사용 선관위 온라인투표, 비밀 보장 안돼”, http://www.nocutnews.co.kr/news/4452699, August 2015
4. 뉴시스, “선관위, 개표상황표에 ‘투표분류 종료시각’ 삭제 논란”, http://www.newsis.com/ar_detail/view.html?ar_id=NISX20140602_0012957644&cID=10312&pID=10300, June 2014
5. 동아일보, “‘사전투표제’ 편리해 졌지만 ‘이중투표’ 논란에 허점 노출”, http://news.donga.com/DKBNEWS/3/all/20140605/64030941/3, June 2014
6. 박해영, “전자투표를 통한 국민주권 실현방안 연구”, 창원대학교 박사학위 논문, December 2007
7. 법제처, “공직선거법”, http://www.law.go.kr/법령/공직선거법/(13497,20150813)
8. 서울경제, “구멍 뚫린 선관위 전자투표시스템”, http://economy.hankooki.com/lpage/society/201508/e20150811180022142920.htm, August 2015
9. 심경아, “[정보보호] 타원곡선 암호시스템 급부상”, 한국정보통신기술협회 기술표준이슈, http://www.tta.or.kr/data/weekly_view.jsp?news_id=513, September 2001
10. 이두호, “전자투표 수용 영향요인에 관한 연구:정치인, 공무원, 일반인 영향경로 비교분석”, 중앙대학교 박사학위 논문, February 2012
11. 이성춘 외 2명, “비트코인(Bitcoin) 시스템 분석 노트”, KT경제경영연구소, December 2013

12. 위키피디아, “블록체인”, https://ko.wikipedia.org/wiki/블록체인, August 2015.
13. 위키피디아, “비트코인”, https://ko.wikipedia.org/wiki/비트코인, March 2011.
14. 조희정, “미국의 전자투표와 기술 수용 정치:브라질・에스토니아와 비교를 중심으로”, 서강대학교 박사학위 논문, February 2007
15. 중앙선거관리위원회, “온라인투표시스템 ‘케이보팅(K-Voting)’”, http://www.kvoting.go.kr
16. 트렌드 지식사전, “사전투표제”, http://terms.naver.com/entry.nhn?docId=2070478&cid=55570&categoryId=55570
17. bitcoinwiki, “Technical background of version 1 Bitcoin addresses”, https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses, November 2011
18. bitcoinwiki, “Wallet import format”, https://en.bitcoin.it/wiki/Wallet_import_format, January 2012
19. Ken Shirriff, “Bitcoins the hard way: Using the raw Bitcoin protocol”, http://www.righto.com/2014/02/bitcoins-hard-way-using-raw-bitcoin.html, February 2014
20. Leslie Lamport, “The Byzantine Generals Problem”, ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, http://www.cs.cornell.edu/courses/cs614/2004sp/papers/lsp82.pdf, July 1982
21. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2009.
22. Vitalik Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform”, https://github.com/ethereum/wiki/wiki/White-Paper

Abstract

A Study on Performance Improvement and Implementation of Electronic Voting System using Blockchain

YOO, HEONWOO
Ajou University

Electronic voting system is a comprehensive set of electronic system targeted by the voters every step of the election, identification, voting, counting, etc. checklist process can be understood as establishing electronic election system. The electronic voting system technical security and stability in order to obtain the trust of the electorate can be when fully implemented.

In this paper, we propose a "de-centralized electronic voting system" chain of blocks that ensure the reliability of electronic voting can accept and ensure the technical safety.

Share data to all users without the presence of a central server as the block chain technique is a distributed database, and updates the data directly. When

using the electronic voting system configurations based on these blockchain stores in the blockchain the electronic voting data can develop a decentralized electronic voting system can be used as the benefits of the blockchain.

The electronic voting system can not be destroyed by cyber attacks and network failures because the data are updated by agreement of the user data tampering and cheating have been inherently blocked.

Therefore, the electronic voting system to apply technology blockchain contains all of the advantages and benefits of the traditional paper ballot system of electronic voting systems, so do the verification through voluntary participation can improve the reliability of the voters. Were also able to check the performance of the average 87.6% with the performance improvements to be linked to a variety of platforms.