이 재 원 교수 지도
석사학위 청구논문

신뢰할 수 있는 허가형 블록체인 기반 전자투표 시스템 설계 및 구현

2019

성신여자대학교 대학원
컴퓨터학과
강 희 정

신뢰할 수 있는 허가형 블록체인 기반 전자투표 시스템 설계 및 구현

이 재 원 교수 지도

이 논문을 석사학위논문으로 제출함

2019년 5월

성신여자대학교 대학원

컴퓨터학과

강 희 정

인 준 서

강희정의 석사학위 논문으로 인준함

2019년 5월

심사위원장 이 일 구 (서명 또는 인)

심 사 위 원 김 경 진 (서명 또는 인)

심 사 위 원 이 재 원 (서명 또는 인)

성신여자대학교 대학원

논 문 개 요

전자투표는 투표 참여 증대 및 편리성 제공, 개표 효율성등과 같은 효과 때문에 지속적으로 연구 되어왔다. 전자투표는 기존 종이투표와 다르게 개표과정이 전산에서 진행되기 때문에 투표의 신뢰성 보장이 중요하다. 전자투표의 신뢰성 보장을 위해 영 지식 증명(zero-knowledge proof), 비밀 공유 기법, 재 암호화 기법 등 다양한 정보보호 기술의 도입이 연구되어왔지만 기본적으로 중앙의 신뢰할 수 있는 기관에 의해 이루어지기 때문에 중앙 서버 공격으로 인한 위변조 가능성이 여전히 제시된다.

이에 최근 들어 네트워크를 구성하는 모든 참여자가 기록을 공유하여 위변조가 어려운 블록체인을 도입하여 해결하고자 하는 시도가 활발히 이어지고 있다. 하지만, 블록체인을 전자투표에 도입할 경우 네트워크를 구성하는 모든 참여자에게 투명하게 정보가 공개되는 블록체인의 특징을 고려한 보안성 연구가 필요하다. 투표는 정당한 투표권이 있는 정당한 투표자만 참여해야 하지만 Public 블록체인의 경우 검증되지 않은 사용자도 참여가능하며 기존의 거래내역을 추적해 개인이 식별될 가능성이 있기 때문에 전자투표에 적용되기 적합하지 않다. Private 블록체인의 경우 인증 된 사용자만 참여하는 것이 가능하기 때문에 투표에 적용되기 적합하지만 네트워크 참여자가 모두 정보를 공유한다는 블록체인의 기본적인 특성 때문에 신뢰성 있는 전자투표를 위해서는 연구가 필요하다.

따라서 본 논문에서는 신뢰할 수 있는 블록체인 기반 전자투표를 위한 전자투표 시스템을 제안하고자 한다. 제안하는 시스템은 ① 블록체인을 활용하여 중앙 서버의 조작 및 외부 공격으로 인한 위변조 가능성 방지했으며, ② 인증 된 사용자로만 구성되는 허가형 블록체인인 패브릭을 활용해 정당한 투표자들로만 네트워크를 구성했다. 또한, 한 노드에 의한 조작 가능성을

방지하기 위해 ③ 다자간 계산(multi-party algorithm)을 차용한 개념을 적용하여 여러 노드에서 집계하게 하였으며 ④ 분산된 노드에서 투표를 집계시 암호화 된 상태로 계산 가능 한 동형암호를 활용했다. 마지막으로 ⑤ 영수증을 발급해줌으로써 개별 검증성 달성했지만 ⑥다른 후보에 대한 랜덤 토큰을 같이 출력하여 영수증을 통한 유권자의 프라이버시를 보장했으며, ⑦ 전체 토큰의 개수와 결괏 값을 확인하여 전체 검증성을 달성함으로써 신뢰할 수 있는 블록체인 기반 전자투표 시스템을 제안한다.

목 차

표 차 례

그 림 차 례

제 1 장 서론

1. 연구 배경 및 목적

민주주의 시대에서 투표는 개인이 의사표현을 할 수 있는 가장 기본적이며 주요한 수단이다. 디지털 기술혁신에 따라 각종 분야에서 기존 종이로 진행되었던 투표를 전자투표로 전환하려는 시도가 있어지고 있다. 전자투표는 유권자에게 편리성 제공 및 투표 참여율 상승과 같은 장점으로 편리성과 실효성을 인정받으며 활발하게 연구되어오고 있다[1].

전자투표는 투표와 개표가 전자적으로 이뤄지기 때문에 편리하지만 보안 기술의 적용이 필수적이다. 특히, 기존의 전자투표는 투표 관련 정보가 중앙에 저장되기 때문에 여전히 해킹 조작 등 투·개표결과의 위·변조 의혹이나 불신이 제기되기도 한다. 실제로 보안성에 대한 우려 때문에 전자투표보다 종이투표를 선호하는 경우가 많아 전자투표의 확산을 저해하고 있다 [2]. 전자투표의 안정성을 보장하기 위해 영 지식 증명(zero-knowledge proof), 비밀 공유 기법, 재 암호화 기법 등 다양한 암호화 기법이 연구되고 있지만 실제 적용에 회의적인 반응을 얻고 있다. 현재 전자투표 시스템은 중앙에 의해 모든 투·개표과정이 이루어지기 때문에 본인의 투표가 정확히 전자투표 시스템에 반영되었는지 확신과 믿음을 얻지 못하기 때문이다[1].

블록체인 기술은 네트워크에 참여하는 모든 사람이 정보를 공유함으로써 데이터의 무결성 보장 및 누구나 투명하게 검증 가능하다. 따라서 블록체인 기술을 투표에 적용할 경우, 투·개표결과의 위·변조 방지 및 자신의 투표가 반영되었는지 아닌지 확인 가능하다. 하지만 전자투표에 블록체인을 도입할 경우, 기존 중앙 집중형 시스템과 달리 네트워크 참여자 모두에게 투명하게

정보를 공개하기 때문에 기밀성을 보장하지 않는 블록체인의 특성을 고려하여 적용해야한다. 기존의 비트코인 및 이더리움과 같은 Public 블록체인의 경우 검증되지 않은 사용자도 참여가능하며 투표자의 기존 거래내역을 추적해 개인이 식별될 가능성이 있기 때문에 전자투표에 적용되기 적합하지 않다. Private 및 permissioned 블록체인의 경우 인증 된 사용자만 참여하게 할 수 있다는 점에서 투표에 적용되기 적합하지만 모든 네트워크 참가자가 정보를 공유하는 블록체인을 특징 때문에 투표의 기밀성 보장이 고려되어 적용되어야 한다.

본 논문에서는 전자투표가 만족해야 할 안전성 성질을 만족하는 허가형(permissioned) 블록체인 기반 전자투표 시스템을 제안한다. 제안하는 시스템은 완전동형 암호 및 영수증(receipt)에 다른 후보의 랜덤 토큰을 출력하여 유권자의 기밀성과 보안성을 보장하고 토큰을 이용해 권한 관리 및 한 사람당 한 번의 투표만 하도록 보장한다. 또한, 영수증(receipt)을 통해 자신의 투표가 집계 되었는지 확인함으로써 개별 검증성을 달성하고 결과 값과 전체 토큰의 개수를 비교함으로써 전체 검증성을 달성한다. 마지막으로, 한 노드에서 부정행위를 막기 위해 다자간 계산(multi-calculation)을 차용한 개념을 적용하여 보다 신뢰할 수 있는 허가형 블록체인 기반 전자 시스템을 제안하는 것을 목표로 한다.

2. 논문 구성

논문의 구성은 다음과 같다. 2장에서는 전자투표와 블록체인의 전체적인 개요 및 유형에 대해 살펴본다. 추가적으로 본 논문에서 주요하게 다뤄지는 전자투표의 신뢰성을 보장하기 위한 고려사항을 자세히 살피고 제안하는 시스템에 활용되는 하이퍼레저 패브릭에 대해서도 살펴본다. 3장에서는 제안하는 시스템의 보안 이슈 및 요구사항을 분석하고, 4장에서는 이를 고려한 설계 및 구현에 대해 살펴본다. 마지막으로 결론 및 향후 연구를 통해 본 논문의 기여점과 한계점을 도출한다.

제 2 장 관련연구

1. 전자투표(E-Voting)

1.1 전자투표의 개요

전자투표는 투표 행위 및 집계 등 투표의 모든 측면에서 전자적인 수단을 활용한 것을 의미한다[3]. 전자투표는 기존 종이투표와 비교하여 접근성 및 용이성 향상으로 인한 투표율 증가, 개표과정 전산화로 인한 비용 절감, 선거절차 단순화와 같은 장점으로 주목 받으며 국제적으로 연구가 활발하게 이루어지고 있다.

우리나라의 경우, 2013년 선관위와 KT가 MOU를 체결하고 온라인 투표 시스템인 '케이보팅(K-Voting)'을 개발하였으나 투표 조작 가능성이 제시되며 보안성 우려를 받았다[4]. 전자투표는 안전성이 보장된 편리하고 신속한 투표가 핵심이므로 보안 기술이 투표 환경과 방식에 따라 적절히 적용되어야 한다[1]. 또한, 더욱 안전한 전자투표 설계를 위해 기밀성, 인증, 익명성과 같은 기본적인 정보보호 서비스에서 더 나아가 심도 있는 보안 기술이 고려되어야 한다.

1.2 전자 투표의 유형

전자투표는 이동성 및 네트워크화를 기준으로 크게 3가지 방식으로 분류할 수 있다. [표 1]은 전자투표 유형에 따른 주요 특징을 정리한 것이다.

[표 1] 전자투표 방식의 주요 특징[5]

구분	PSEV 방식	키오스크 방식	REV방식
투표 장치 (device)	전자투표기	전자투표기	모바일, 디지털 TV, PC
직접적인 선거관리 정도	상	중	하
기술적 안전성에 대한 쟁점 정도	하	중	상
특징	- 투표소와 개표소를 공공망을 통해 연결 - 네트워크에 대한 외부침입이 있을 수 있지만 공공망이기 때문에 통제가 수월	- 많은 사람이 모이는 마트, 학교, 도서관 등 공공장소에 투표기 설치 - 투표소에 선거관리자가 없음 - 사용기기에 특수한 전자적인 인증장치설치로 관리 부분을 해결	- 기술적 위험도가 높고, 관리인이 없이 자유롭게 투표하여 비밀투표 침해의 가능성이 있음

1.3 전자투표의 문제점 및 신뢰성 보장을 위한 고려사항

현재 전자투표의 문제점은 중앙 집중형이기 때문에 몇 가지 문제가 존재한다. 가장 큰 문제는 신뢰성의 문제이다. 현재 전자투표 시스템은 전산을 통해 중앙에서 이루어지기 때문에 눈에 보이지 않는 투표 내역 처리에 대한 신뢰 확보의 어려움 및 투표자 정보와 투표 내용에 대한 유출 등 보안상의 문제가 발생할 수 있다[17]. 또한, 한 기관에 저장되어 위협점이 하나이기 때문에 보안 및 조작 우려가 발생하기도 한다.

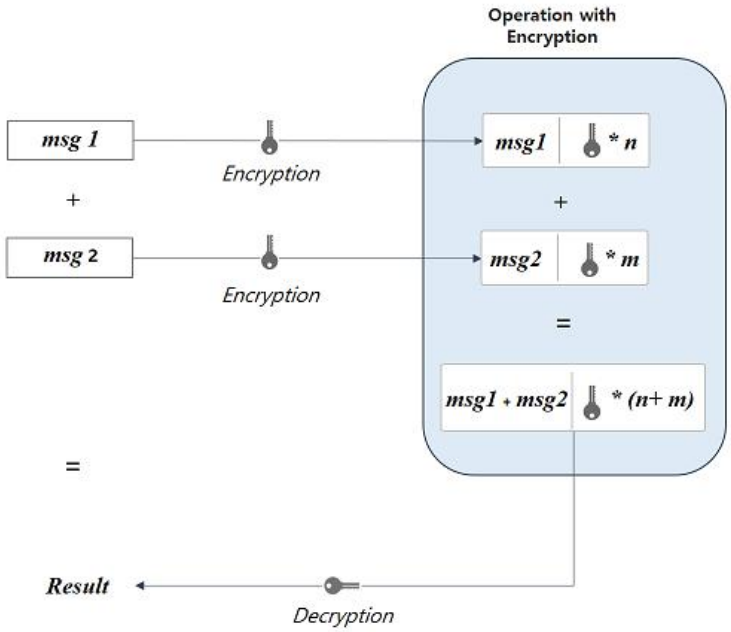
즉, 전자투표는 전자적인 수단을 이용하여 투·개표과정이 이루어지고 중앙 집중적 특성을 갖고 있기 때문에 투표 결과의 무결성 및 본인의 투표가 정확히 전자투표 시스템에 반영되었는지 대한 신뢰성이 중요하다. 전자투표의 신뢰성 보장을 위해서는 다음과 같은 사항이 고려되어야한다. 우선, 투표자의 비밀투표를 보장하기 위해 ①기밀성 보장과 자신의 투표가 제대로 반영되었다는 것에 대해 ②개별 및 전체 검증성이 고려 되어야한다. 추가적으로, ③영수증(receipt)을 통한 유권자의 프라이버시 노출 방지를 위해 추가 보안 기법의 적용도 고려되어야한다.

1.3.1 전자투표의 기밀성 보장

전자투표의 기밀성을 보장하는 방법은 크게 암호화와 익명화 두 가지로 나눌 수 있다 [6].

・암호화 방식

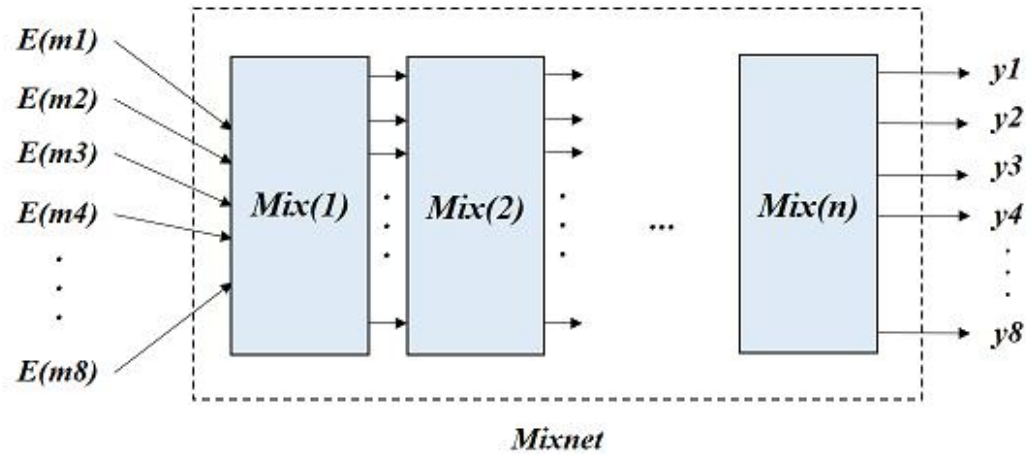
가장 기본적인 모든 투표를 암호화하고 복호화 하는 방식[7][8][9]은 검증하는데 상당한 시간이 소요되기 때문에 현실적이지 않다. 이를 해결하고자 복호화 없이 연산을 수행할 수 있는 동형암호[10]가 연구 되었다. 암호화된 상태에서 연산, 탐색, 분석이 불가능한 기존 암호화 기술과는 달리 동형암호화 알고리즘을 사용할 경우 암호화 된 상태에서도 연산을 수행할 수 있다 [11]. 동형암호의 원리는 아래 (그림 1)과 같다.



(그림 1) 동형암호의 원리

· 익명화 방식

투표를 익명성을 보장하는 채널을 통해 보내는 방식[12][13][14]은 검증 시간 측면에서 더 좋지만 투표를 집계하는 중앙기관에 대한 의존성 및 각각 투표자의 투표를 구별할 때 랜덤스트링을 사용하기 때문에 이로 인한 충돌이 생길 수 있다는 문제점이 있다. 이와 같은 익명성을 보장하는 방식으로는 대표적으로 Mix-net 방식이 있다. Chaum(1981)에 의해 처음 제안 된 Mix-net은 일련의 서버가 한 묶음의 메시지를 입력 받고 메시지 순서를 재배치하여 출력하는 것으로 shuffle network라고도 한다[15]. Mix-net을 전자투표에 활용하기 위해서는 복잡도에 대한 적절한 연구가 필요하다. (그림 2)는 Mix-net의 동작 방식이다.



(그림 2) Mix-net 동작방식

1.3.2 전자투표의 검증가능성

전자투표에서 검증가능성은 유권자의 투표가 결과에 정확히 반영되었음을 보장하는 것을 의미한다[1]. 이는 개별 검증성과 전체 검증성으로 세분화 할 수 있다. 개별 검증성은 유권자가 자신의 표가 제대로 집계 되었는지 검증할 수 있는 것을 의미하고, 전체 검증성은 최종 집계된 결과가 실제 투표 값의 합과 일치하는지를 검증할 수 있는 것을 의미한다[15].

• 동형암호를 이용한 집계 방식에서의 검증

동형암호에서는 $E[m_1m_2] = E[m_1]E[m_2]$을 만족하여 투표 값이 암호화 된 채로 집계가 이루어지기 때문에 전체 과정에서 비밀성을 유지할 수 있다. [표 2]는 유권자가 자신의 암호화된 투표 값이 바르게 암호화 되었고, 집계자가 바르게 집계했는지 증명하는 과정을 나타낸 것이다. INPUT 단계의 증명은 적절한 권한이 있는 투표자가 투표를 수행했고 투표 값에 대한 유효성에 대한 증명을 나타내며, OUTPUT 단계의 증명은 집계자가 올바르게 집계했다는 것을 유권자에게 증명하는 것이다. 이를 통해 전체 및 개별 검증성을 달성할 수 있다.

[표 2] 동형암호를 이용한 집계 방식에서의 검증[1]

Protocol TALLY	
INPUT	$E[v_i],...,E[v_n]$ + Validity Proofs
OUTPUT	$f(v_i,...,v_n)$ + Validity Proofs

1.3.3 유권자의 프라이버시 보장

전자투표에서 영수증(receipt)이란 유권자들의 조작 방지 및 개별 검증성을 보장하기 위해 제안된 개념으로 유권자들은 자신의 영수증을 통해 자신의 투표가 잘 반영되었는지 확인할 수 있다. 영수증은 개별 검증성을 보장해주지만 영수증을 통해 유권자가 누구에게 투표했는지를 알 수 있게 되는 문제가 발생한다. 따라서 유권자의 프라이버시를 보장하기 위해서는 영수증을 타인이 보더라도 누구에게 투표했는지 알 수 없어야한다.

전자투표에서는 투표에서는 영수증 발급 시 확률론적 암호화를 주로 이용하는데 이는 평문 공간이 매우 작은 유한집합으로 이루어져 있어 결정적 암호 알고리즘을 사용할 경우, CPA(Chosen Plaintext Attack)이나 CCA(Chosen Ciphertext Attack)을 당할 수 있기 때문이다[16]. 확률론적 암호화는 암호화 할 때 임의의 난수를 이용하는 방식으로 동일한 평문 m_1과 m_2가 있어도 암호화 결과인 c_1 = E[m_1]과 c_2 = E[m_2]는 같지 않다. [표 3]은 ElGamal 암호 방식을 적용한 확률론적 암호화의 예시이다.

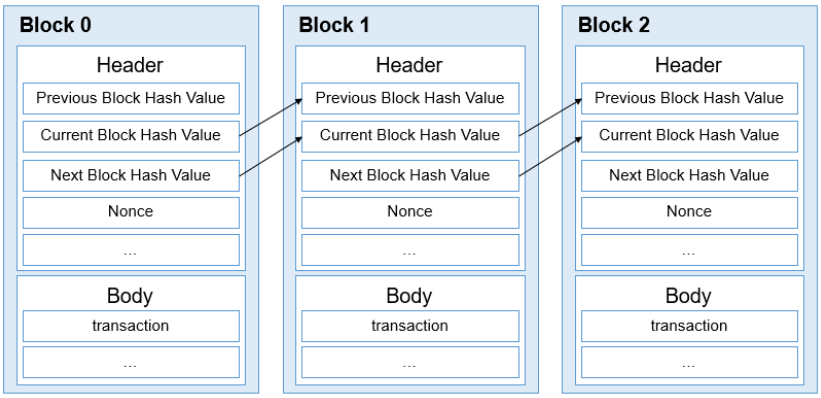
[표 3] ElGamal 암호 방식의 확률론적 암호화[16]

A	public information y_A, y_B, p, g	B
$y_A = y^{X_A} \bmod p$ *encryption* $r \in_R Z_{p-1}$ $K \equiv y^{r_B} \bmod p$ $C_1 \equiv g^{r_B} \bmod p$ $C_2 \equiv KM mod p$ $C=(C_1 \parallel C_2)$	C ⟶	$y_B \equiv y^{X_B} \bmod p$ $K \equiv C^{X_B} \bmod p$ $M \equiv C_2/K \bmod p$

2. 블록체인

2.1 블록체인 개요

블록체인은 2008년 Satoshi Nakamoto에 의해 제안된 비트코인의 기반 기술이다[18]. 블록체인의 블록은 헤더(Header)와 바디(Body)로 구성된다. 헤더(Header)이전 블록의 정보와 현재 블록의 정보가 함축적으로 담겨 있으며 바디(Body)는 여러개의 트랜잭션이 담겨 있다. 헤더(Header)를 통해 블록들이 유기적으로 연결되어 있어 조작 및 수정이 어렵기 때문에 무결성에 대한 신뢰성이 보장된다. (그림 3)은 블록의 구조를 나타내는 그림이다.



(그림 3) 블록의 구조

블록체인은 분산 시스템으로 다수의 노드가 정보를 공유함으로써 무결성을 보장한다. 블록체인은 정보를 중앙의 한 기관이 아닌 다수가 공동으로 소유하기 때문에 일부 시스템에 오류와 성능저하가 발생하더라도 전체 시스템에는 큰 영향을 주지 않는다. 또한, 네트워크 참여자가 같은 데이터를 공유하고 있기 때문에 수정이 발생해도 기록이 블록체인에 남아있기 때문에

부인방지 기능도 할 수 있다. 이러한 블록체인의 특징은 데이터 조작 및 해킹 등 외부의 악의적인 공격이 어렵게 만들기 때문에 보다 보안성이 높다고 평가받는다. [표 4]는 블록체인의 주요 특징을 정리한 표이다.

[표 4] 블록체인의 주요 특징[19]

	장점	단점
익명성	- 개인정보를 요구하지 않아 은행계좌 , 신용카드 등 기존 수단에 비해 높은 익명성 제공	- 불법 거래대금 결제 및 비자금 조성, 탈세가 가능ㅇ
P2P	- 공인된 제3자 없이 P2P 거래 가능 - 불필요한 수수료 절감	- 문제 발생 시 책임소재가 모호
확장성	- 오픈 소스에 의해 쉽게 구축·연결·확장 가능 - IT 구축비용 절감	- 결제처리 가능 거래건수가 실제경제의 거래규모 대비 미미
투명성	- 모든 거래기록에 공개적 접근 가능 - 거래 양성화 및 규제	- 거래 내역이 공개되어 원칙적으로는 모든 거래가 추적 가능 - 조합에 의한 재식별이 가능하여 완벽한 익명성 보장이 어려울 수 있음
보안성	- 장부를 공동으로 소유(무결성) - 보안관련 비용	- 개인키의 해킹 및 분실 등의 경우 일반적으로 해결방법 없음 - 기밀성 제공하지 않음
시스템 안정성	- 단일 실패점이 존재하지 않아 일부 참가 시스템에 오류 혹은 성능저하가 발생해도 전체 네트워크에 영향 미미	- 채굴이 대형 마이닝 풀에 집중 - 실시간, 대용량 처리의 어려움

2.2 블록체인 유형

블록체인의 유형은 크게 public, private, permissioned로 나눌 수 있다. Public 블록체인의 경우 누구나 참여가능하고, Private 및 permissioned 블록체인의 경우 인증 된 사용자만 참여할 수 있다. Private 및 permissioned의 경우 식별이 가능하기 때문에 전자투표에 적용 할 때, 이를 고려한 설계가 필요하다. [표 5]는 블록체인 유형별 특징을 정리한 표이며, [표 6]은 블록체인 플랫폼 별 특징을 정리한 표이다.

[표 5] 블록체인의 유형별 특징

	Public	permissioned	private
Management subject	All participants	Certified participants	central institution
transaction speed	slow	quick	quick
Network Scalability	difficult	nomal	easy
Identification	Anonymous	Identifiable	Identifiable
Use case	bitcoin, ethereum	hyperledger Fabric	Linq

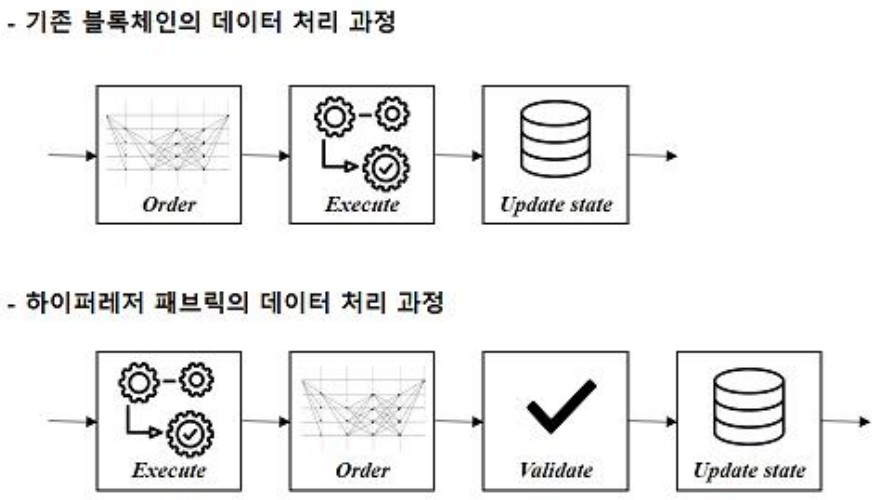
[표 6] 블록체인 플랫폼 별 특징[17]

	Bitcoin	Ethereum	Hyperledger fabric	Ripple	R3 Corda
Purpose	Payments blockchain	General purpose blockchain	General purpose blockchain	Payments blockchain	Specialized distributed ledger platform for financial industry
Type	Public	Public	permissioned	private	private
Digital currency	BTC	Ether, Token	Currency, tokens via chaincode	XRP	-
Mining reward	O	O	X	X	X
state	Transaction data	Account data	Key-value database	-	-
Privacy	Open	Open	Open to Private	Open	Private
Smart Contract	X	Solidity programming language	Multiple programming language (Go, Java, …)	X	Multiple programming language (Kotlin, Java, …)

2.3 하이퍼레저 Fabric

2.3.1 Fabric의 개요

하이퍼레저 패브릭은 허가형 프라이빗 블록체인으로 패브릭에서 제공하는 MSP(Membership Service Provider)라는 인증 관리 시스템에 등록된 사용자만 참여 할 수 있다[20]. 패브릭은 데이터를 처리 할 때, 3가지 단계로 나눠서 처리한다. 각 단계마다 역할을 할당받은 Peer들이 이를 실행하게 되는데 한 노드에서 모든 것을 실행했던 기존 블록체인과 비교하였을 때 노드의 부하를 줄일 수 있고 동시에 두 가지 이상의 작업을 수행하는 병렬 처리가 가능하기 때문에 시스템의 성능 또한 향상된다는 장점이 있다[21]. (그림 4)는 기존 블록체인과 하이퍼레저 패브릭이 데이터 처리 과정을 비교한 그림이다.



(그림 4) 기존 블록체인과 패브릭의 데이터 처리 과정 비교[21]

각 과정에서 수행하는 역할은 아래와 같다.

· 실행(Execute) : 트랜잭션 실행 및 결괏값을 검증 작업 수행

· 정렬(Order) : 검증 완료된 트랜잭션 취합 및 순서에 맞게 정렬한 후 블록을 생성하는 작업을 수행

· 검증(Validation) : 블록에 포함된 모든 트랜잭션에 대한 결괏값 및 인증서 검증을 수행하여 이상이 없을 경우 최신 블록을 업데이트

실행(Execute)단계에서는 보증(Endorsement) Peer가 이를 수행하며. 보증 Peer는 미리 지정하거나 랜덤으로 선정할 수 있다. 실행(Execute)단계에서는 생성된 트랜잭션을 체인코드를 통해 실행시켜 본 후 이상이 없으면 자신의 서명을 통해 보증한 트랜잭션을 반환한다.

이 트랜잭션은 후에 순서를 맞추는 **정렬(Order)단계**를 거쳐 **검증(Validation)단계**까지 넘어간다. 검증(Validation)단계에서는 보증(Endorsement) 정책을 충족시킨 트랜잭션만 유효한 것으로 간주하여 최종적으로 업데이트 하며, 다양한 방식의 보증 정책을 통해 보안성 및 신뢰성을 강화할 수 있다.

패브릭에서의 합의는 위 일련의 과정들을 의미한다. 비트코인, 이더리움이 PoW나 PoS와 같은 특정 알고리즘을 합의라고 지칭하는 것과 다르게 패브릭은 트랜잭션 생성부터 최신 블록이 peer에 저장되기까지의 모든 과정을 합의라고 지칭한다. 즉, 패브릭에서의 합의는 보증정책 확인(Endorsement) 후에 트랜잭션을 정해진 순서에 맞춰 정렬(Ordering)하고 정렬된 트랜잭션의 유효성 검증 후 최신 블록 업데이트(Validation)하는 일련의 과정을 의미한다. 아래는 [표 7]은 보증 정책의 예시이다.

[표 7] 패브릭 보증정책 예시[21]

example1)   *보증 그룹 = {peer1, peer2, peer3, peer4, peer5, peer6, peer7}*   *보증 정책 = • 보증 그룹의 모든 peer의 디지털 인증서를 획득해야 함*   *• 보증 그룹의 peer 중 1개의 디지털 인증서를 획득해야함*   ***example2)***   *보증 그룹 = {peer1=15, peer2=10, peer3=25, peer4=20, peer5=10, peer6=10, peer7=10}*   *보증 정책 = • 가중치 합계 50이상을 획득해야함*

2.3.2 Fabric의 구성요소

패브릭은 다양한 역할을 수행하는 구성요소들로 이루어져 있다. [표 8]은 패브릭의 주요 구성요소를 나타낸 것이다.

[표 8] 패브릭 주요 구성요소

구성요소	역할
peer	블록체인을 구성하는 네트워크 노드 중 하나
chaincode	이더리움의 스마트 컨트랙트 역할로 체인코드를 이용해 분산원장에 데이터를 기록하고 읽을 수 있음
Endorsement Policy	보증 정책을 활용하여 비즈니스 보안성, 신뢰성 등을 강화
Organization	네트워크 내에서 조직(Organization)을 구성할 수 있음
Channel	이해관계에 있는 조직만 정보를 공유할 수 있도록 함.
MSP	하이퍼레저 패브릭의 멤버십 관리 기술로 peer, orderer, Fabric-CA Admin등의 역할과 소속, 권한 등을 정의할 수 있음

하이퍼레저 패브릭은 버전이 업그레이드 됨에 따라 프라이버시와 기밀성을 보장해주는 프라이빗 데이터(PDC(Private Data Collection)를 제공하고 있으며, Fabric 2.0 alpha 버전에서는 FabToken[36]이라는 자체적인 토큰을 제공하고 있다.

제 3 장 보안 이슈 및 요구사항 분석

1. 선행연구 분석

블록체인에 전자투표를 활용한 사례연구는 국내외에서 활발하게 이루어지고 있다. 국내에서 public 블록체인인 이더리움 블록체인을 활용하여 전자투표 시스템을 구축한 연구는 유현우[27], 이루다[28], 박연아[17]의 연구가 있었다. 연구에서는 조작 및 해킹에 대한 무결성 확보는 달성했으나 기밀성에 대한 연구는 범위에 포함하지 않고 있다. 이러한 문제에 대한 해결을 위해 하현수[30]의 연구에서는 Public 블록체인 기반의 전자투표에서 Tor(The Onion Routing), Ring Signature, Stealth Addressing 기법을 사용하여 익명성을 보장함으로써 이 문제를 해결하였으며, 김세아[31]의 연구에서는 회원가입 시 새로운 계좌 주소를 생성한고 계좌를 암호화하여 데이터베이스에 저장하는 방식으로 기밀성을 확보하였다.

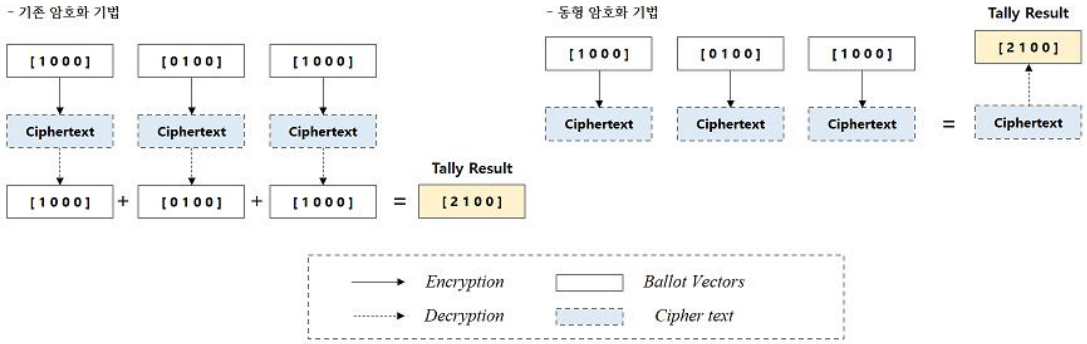
해외에는 유권자의 프라이버시 위주로 연구가 진행되고 있었다. Zijian Bao[33]가 진행한 연구에서는 비트코인 블록체인 기반에서 투표 시 키를 shuffling 하는 방식으로 기밀성을 보장하였고 , Patrick McCorry[34]와 Ali Kaan Koç[35]의 연구에서는 유권자의 프라이버시를 위한 스마트 컨트랙트의 설계 방안을 제안했다.

대부분의 국내외 연구가 public 블록체인을 기반이지만 본 논문은 전자투표에 조금 더 적합한 permissioned 블록체인을 기반으로 하고 있다는 것에 대해 차별점이 있으며, 다양한 관점에서 기밀성을 고려하여 보다 신뢰할 수 있는 블록체인 기반 전자투표를 설계 및 구현을 목표로 한다.

2. 보안 이슈사항

① 투표의 기밀성 보장

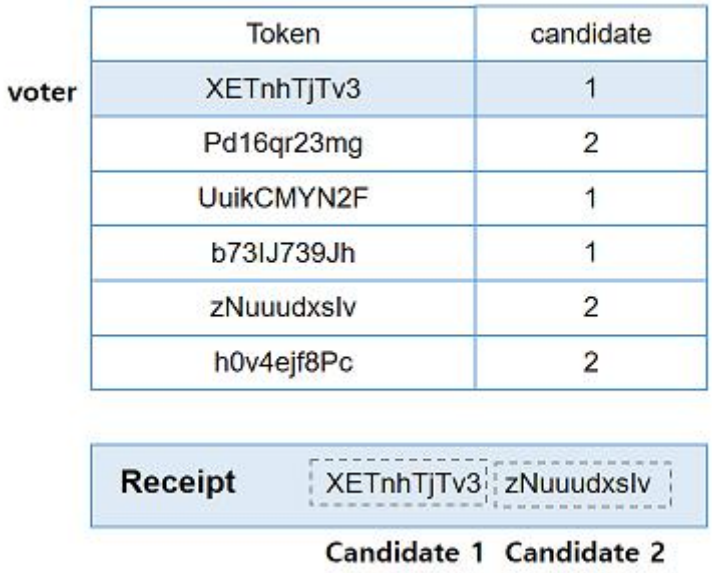
투표에서 비밀을 보장하는 것은 투표의 가장 기본적인 요소이다. 이를 해결하는 방법은 앞서 언급한 암호화와 익명화가 있다. 제안하는 시스템에서는 완전동형 암호를 사용하여 기밀성 이슈를 해결하고자 한다. 전자투표에 동형암호를 활용할 경우, 복호화 없이 집계가 가능하기 때문에 보다 기존 방식보다 보다 효율적이며 투표 값이 노출되지 않고도 결과계산이 가능하다는 장점이 있다. (그림 5)는 기존 암호화 기법의 투표 집계방식과 동형암호를 이용한 투표 집계방식을 비교한 그림이다.



(그림 5) 기존 암호화 기법과 동형 암호화 기법의 투표 집계 방식 비교

② 유권자의 프라이버시 보장

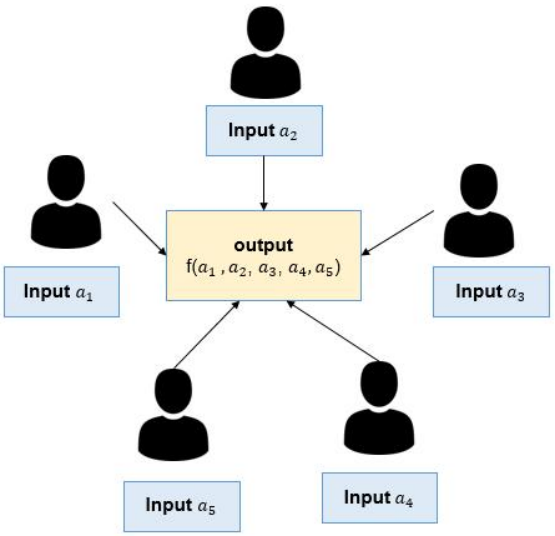
유권자는 자신의 투표가 제대로 집계되었는지를 확인할 수 있도록 영수증을 발급받는다. 하지만 이 영수증을 보고 유권자의 투표 값을 알 수 있거나 연결 지을 수 없어야한다. 본 시스템에서는 [22]에서 제안한 공개키를 랜덤으로 출력하는 방식을 차용해 이를 해결하고자 한다. 본 시스템에서는 공개키가 아닌 토큰 값을 랜덤으로 출력한다. 영수증에는 자신의 토큰 값과 다른 후보를 선택한 토큰 값이 출력되므로 영수증만 확인하고서는 투표자가 누구에게 투표했는지 알 수 없다. (그림 6)은 후보자가 2명인 경우 영수증을 출력하는 예시이다.



(그림 6) 영수증 출력 예시

③ 한 노드의 조작 이슈

블록체인의 경우 조작 및 수정이 어렵긴 하지만 노드수가 작은 프라이빗 및 컨소시엄 블록체인의 경우 불가능한 것은 아니다. 이러한 경우를 방지하기 위해 제안하는 시스템에서는 다자간 계산(multi-party computation)의 개념을 차용해 한 노드에서 모든 투표결과를 집계하는 것이 아니라 여러 노드가 암호화된 상태로 계산하여 최종 검증하는 방식을 제안한다. (그림 7)은 다자간 계산(multi-party computation)을 나타내는 그림이다.



(그림 7) 다자간 계산
(multi-party computation)

3. 요구사항 분석

제안하는 시스템의 최종 달성 목표는 투표 결과의 집계가 정확하게 이루어져야 한다는 것이다. 따라서 앞선 보안 이슈사항과 더불어 제안하는 시스템은 블록체인 기술을 전자투표에 도입 시 요구되는 사항도 만족해야 한다. [표 9]는 박연아[17]의 연구를 참고하여 제안하는 시스템이 만족해야하는 요구사항과 그것을 본 시스템에서 해결방안을 나타낸 것이다.

[표 9] 제안하는 시스템 요구사항 및 해결방안

요구사항	상세내용		해결방안
비밀성	유권자 이외의 누구도 유권자와 유권자가 선택한 투표결과를 연결 지을 수 없어야 한다.		완전동형 암호
보안성	악의적인 공격으로부터 투표데이터의 보안이 보장되어야 한다.		
공정성	어떤 상황도 투표에 영향을 주면 안 된다 (투표 도중 중간집계 정보가 공개되어 선거과정에 영향을 주는 상황이 없어야 한다)		
재사용 불가	각 유권자는 단 1회만 투표가능하다		token
적임성	투표할 자격이 있는 유권자만 투표에 참여할 수 있어야 한다.		
검증성	개별 검증성	유권자는 자신의 표가 실제 집계되었는지 검증 가능해야 한다.	영수증 (receipt)
	전체 검증성	최종 집계된 결과가 실제 투표 결과가 일치하는지를 검증 가능해야 한다.	token 값 비교
안정성	일부 노드가 부정한 행위를 행하려 해도 전체 투표시스템은 안정적으로 작동되어야 한다.		다자간 계산 응용
투명성	투표 및 개표 과정에 대한 객관적인 외부감시가 가능하도록 해야 한다.		블록체인 이용

전자투표에서 주요한 요구사항은 투표데이터의 보안이다. 따라서 제안하는 시스템에서는 완전동형 암호를 통해 투표데이터의 보안성 및 기밀성을 확보하였다. 중간 단계의 집계자들은 암호화 된 상태의 결과만 알 수 있고, 최종 집계자만 결과 값을 검증할 수 있기 때문에 공정성도 보장할 수 있다. 제안하는 시스템에서는 인증된 투표자에 대해 투표권인 토큰을 배부함으로써 각 유권자의 적임성을 보장하고 투표 시 토큰을 함께 전송해야함으로 1회만 투표 가능하다. 또한, 투표자는 투표 후 영수증을 받게 되는데 이를 통해 개별 검증이 가능하고, 전체 token 값을 비교함으로써 전체 검증성을 달성한다. 또한 일부 노드의 부정행위를 방지하기 위해 다자간 계산을 응용하여 여러 노드가 계산 후 최종 결과 값을 산출하는 방법을 활용했다. 마지막으로 블록체인을 활용함으로써 기존보다 투명한 투표 시스템을 제안한다.

제 4 장 제안하는 시스템 설계 및 구현

1. 시스템 설계

1.1 제안하는 시스템 범위

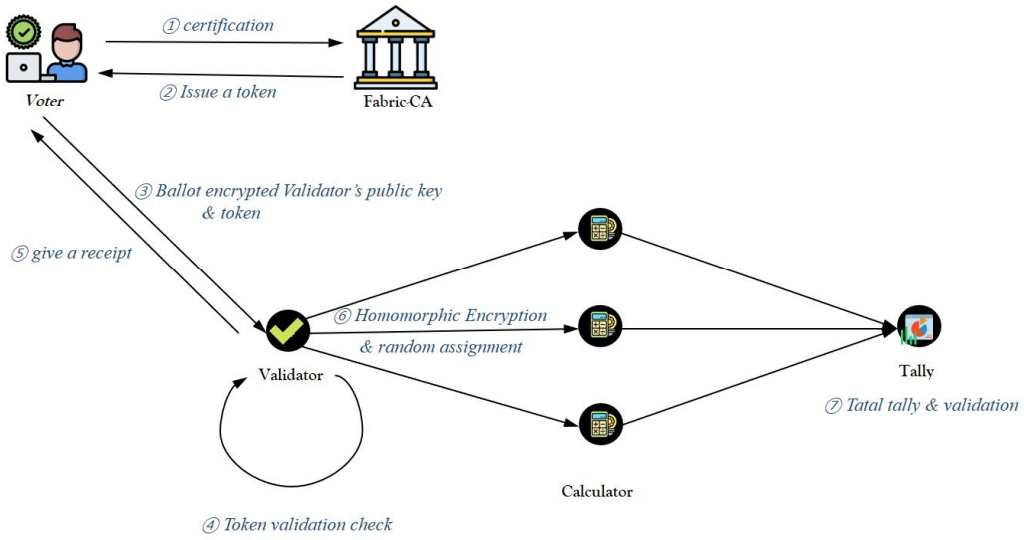
제안하는 시스템에서는 4개의 peer 와 peer-admin, 패브릭의 구성 노드인 orderer, orderer-admin 네트워크를 위해 필요한 kafka-zookeeper 그리고 Fabric-CA로, 총 9개의 노드로 구성되어 있다. 제안하는 시스템은 구현한 컴퓨터 메모리 제한 때문에 여러 투표자 노드를 구성하는 것은 한계가 있었다. 따라서 한 노드에 다중 토큰을 발급하는 방식으로 실험을 진행하였다. 추가적으로, 제안하는 시스템은 가상머신으로 노드를 구성하였으며 패브릭은 구현하는 컴퓨터의 성능에 의존적이므로 제안하는 모델에서는 컴퓨터의 성능과 관련 된 범위는 포함하지 않는다.

1.2 구성도 및 구성요소

제안하는 시스템은 사용자가 인증을 통해 투표권인 토큰을 부여 받고 투표를 하면 동형암호를 통해 다수의 노드에게서 계산되고 최종적으로 admin-peer에 의해 정확한 결괏 값이 집계된다. 제안하는 시스템의 구성요소는 [표 10]와 같으며 전체적인 구성도는 (그림 8)과 같다.

[표 10] 제안하는 시스템의 구성요소

구성노드	역할	구현노드
voter	투표자	peer0
validator	토큰 검증 및 검증 후 동형암호를 사용하여 caculator에게 전달	admin-org0
caculator	암호화 된 상태로 결과 집계	peer1, peer2, peer3
Tally	최종 결과 합산	admin-org1
fabric-ca	인증 기관 역할로 토큰 발급	fabric- ca
orderer / orderer-admin	패브릭의 구성 요소	orderer0/ admin-ordererorg0
kafka-zookeeper	패브릭의 구성 요소	kafka-zookeeper



(그림 8) 전체 구성도

- ①, ② : 인증 받은 노드에 대해 Fabric-CA는 토큰을 발행해준다.
- ③ : Voter는 Validator의 퍼블릭키를 이용해 자신의 투표 값을 암호화하여 발급 받은 토큰과 함께 전송한다.
- ④&⑤ : Validator는 token을 검증하여 정당한 투표자인지 확인한다. 정당성을 확인 한 경우, 후에 개별 검증성 달성하기 위해 영수증(receipt)를 반환해준다.
- ⑥ : 동형암호를 사용하여 암호화 한 뒤, Calculator에게 랜덤하게 값을 배정해준다.
- ⑦ : 복호화 한 집계 결과와 token의 balance를 확인함으로써 전체 검증성을 달성한다.

2. 시스템 구현

2.1 구현 환경

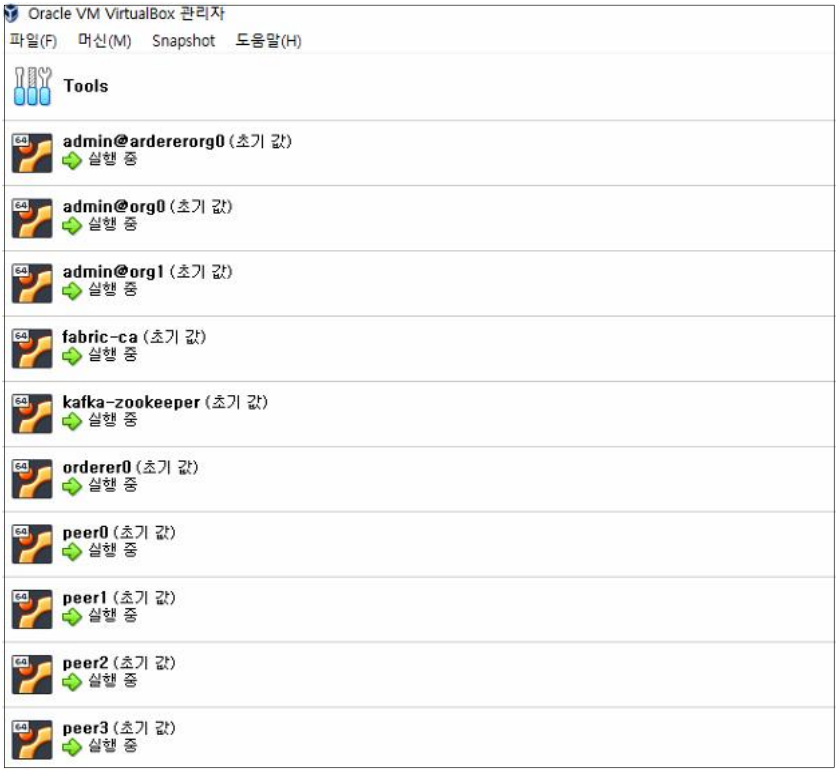
제안하는 시스템의 구현환경은 직관적인 이해를 위해 하나의 호스트 PC에 다수의 노드를 설치하는 도커(Docker) 기반의 환경이 아닌 버추얼박스(virtualBox)의 가상머신을 이용하여 패브릭 네트워크를 구축했다. 패브릭의 성능은 CPU에 의존적이며 본 시스템을 구현하기 위해서는 최소 32GB의 메모리와 400GB의 하드디스크 메모리가 필요하다. [표 11] 는 버추얼박스(virtualBox)를 구성하는 호스트 PC의 환경을 나타내는 표이며, [표 12]는 가상머신에서 하이퍼레저 패브릭의 구현 환경을 나타내는 표이다. 또한, (그림 9)은 본 시스템의 구현 노드를 나타내는 그림이다.

[표 11] Host PC 구현 환경

구분	상세내용
OS	Windows 10
프로세서	intel Core i7-8700
RAM	32GB
하드디스크	953GB

[표 12] Hyperledger Fabric 구현 환경

구분	상세내용
Hyperledger Fabric	v.1.3
Python	2.7.15
Go	go1.10.4 linux/amd64culr
Curl	7.58.0
docker	17.06.2-ce
docker-compose	1.24.0



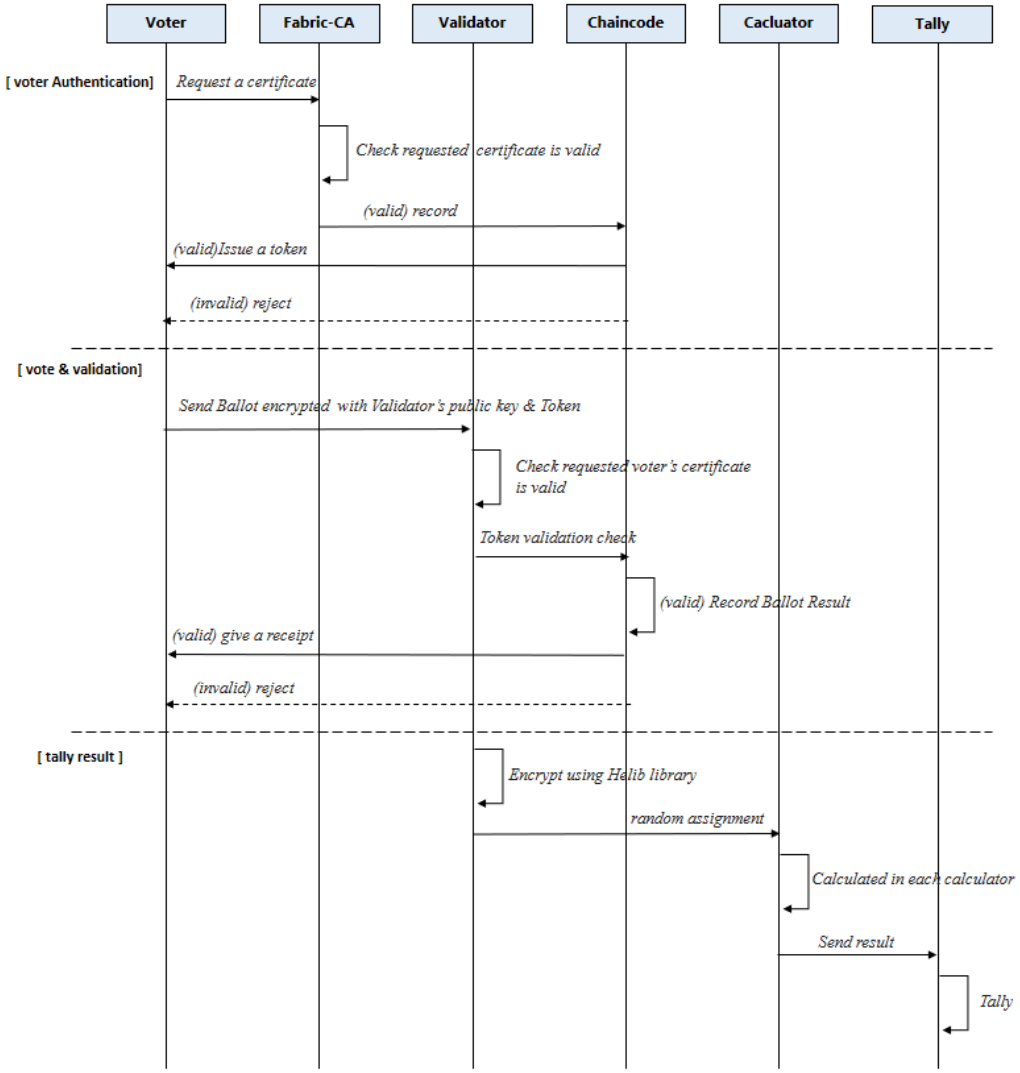
(그림 9) 가상머신 구현 노드

2.2 구현 방법

제안하는 시스템에서 유권자의 기밀성 및 보안성을 보장할 완전동형 암호는 HElib 라이브러리를 활용하여 구현하였다. 유권자의 권한 및 1인 1투표 원칙을 보장해줄 토큰 체인코드 구현은 Hyperledger Fabric 2.0 alpha 버전에 공개 된 FabToken의 체인코드[36]와 이더리움의 erc20[37] 토큰의 코드를 활용하여 구현하였으며, 전제척인 투표 체인코드는 [24]의 체인코드를 활용하여 구현하였다.

2.3 구현 내용

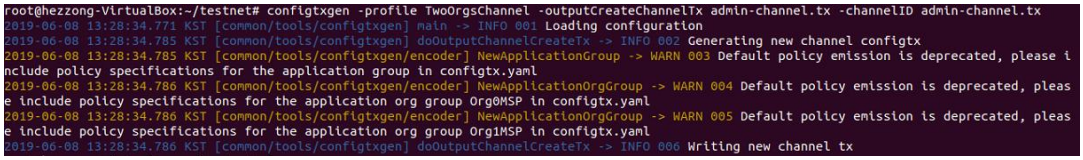
구현한 시스템은 크게 적절한 인증수단을 통해 투표자를 인증하고 투표권인 토큰을 발급해주는 **투표자 인증단계(voter Authentication)**, 투표자가 투표하면 투표자의 인증서 및 토큰 값을 검증하는 **투표 및 검증단계(vote & validation)**, 작은 단위로 집계 후 최종결과를 집계하는 **집계 단계(tally result)**, 총 3단계로 나눌 수 있다. 구현한 시스템의 전체적인 플로우 차트는 (그림 10)과 같다.



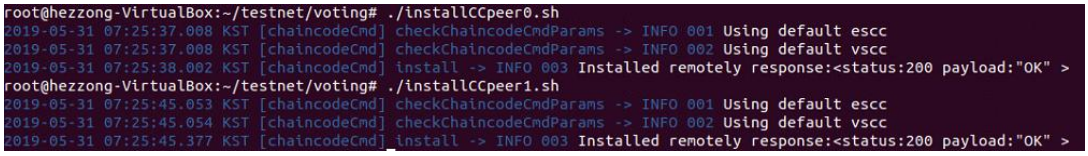
(그림 10) 전체 플로우차트(flowchart)

2.3.1 채널 생성 및 체인코드 설치

구현에 앞서 중간 결과가 노출되면 안 되기 때문에 전체 결과가 집계되기 전에 admin 노드 외에 다른 노드들은 체인코드에 쓰인 값을 알 수 없어야 한다. 따라서 본 시스템에서는 admin-channel을 생성하여 admin노드인 validator와 tally 노드만 접근 가능한 채널을 만들었다. 채널 생성 후 크게 토큰과 투표로 구성된 체인코드를 각 노드에 설치해주었다. (그림 11)은 채널 생성에 관한 결과 콘솔이며, (그림 12) 체인코드 생성에 관한 결과 콘솔이다.



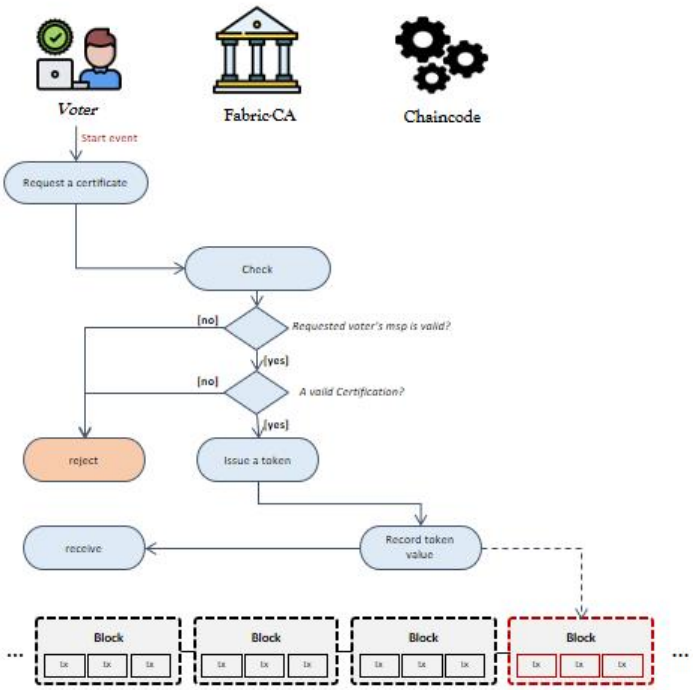
(그림 11) admin-channel 생성



(그림 12) chaincode 생성

3.2.2 투표자 인증단계(voter Authentication)

투표자 인증단계(voter Authentication)에서는 투표자의 인증서와 적절한 인증수단을 거쳐 유효한 사용자인지를 확인한다. 유효한 사용자일 경우, 투표권으로 사용되는 토큰을 발급해주며, 이 때, 영수증에 쓰이는 토큰 값을 체인코드에 기록하여 둔다. 만약 투표자의 인증서가 만료되었거나 유효하지 않은 사용자일 경우, 요청을 거부할 수 있다. (그림 13)은 투표자 인증단계(voter Authentication)를 나타내는 그림이다.



(그림 13) 투표자 인증단계(voter Authentication)

[표 13]은 토큰을 발급해주는 체인코드의 일부이다. 투표의 경우 1인 1투표의 원칙에 따라야하므로 Quantity는 1로 고정하였다. 토큰이 성공적으로 발급되었을 경우 투표자는 발급받은 토큰의 값을 (그림 14)과 같이 콘솔에서 확인할 수 있다.

[표 13] Issue Token chaincode

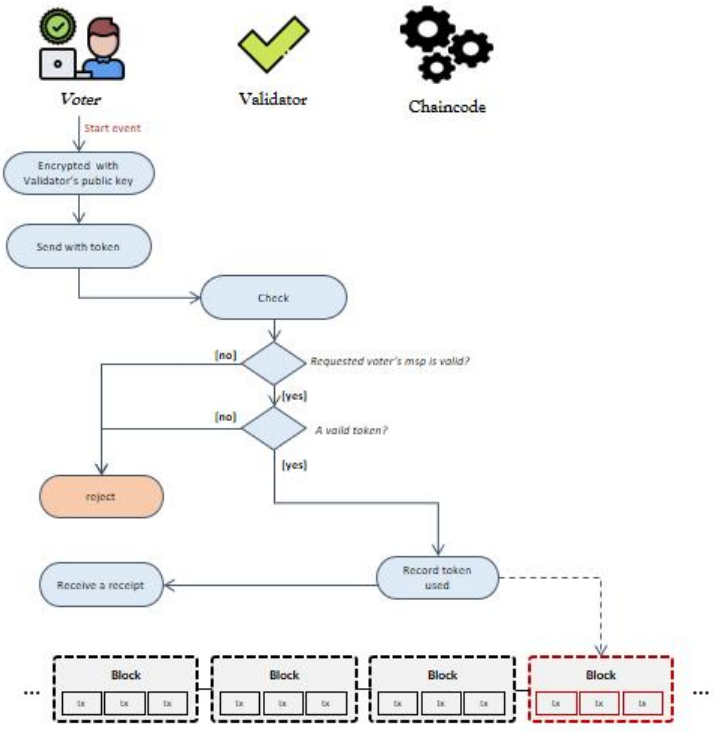
Issue Token chaincode

```
// issue
func (i *Issuer) RequestToken(tokensToIssue []*token.TokenToIssue)
(*token.TokenTransaction, error) {
        var outputs []*token.PlainOutput
        for _, tti := range tokensToIssue {
                outputs = append(outputs, &token.PlainOutput{
                        Owner:    tti.Recipient,
                        Type:     tti.Type,
                        Quantity: 1,
                })
        }

return &token.TokenTransaction{
        Action: &token.TokenTransaction_PlainAction{
            PlainAction: &token.PlainTokenAction{
                Data: &token.PlainTokenAction_PlainImport{

                                ...
```

(그림 14) 발급받은 토큰 확인

3.2.3 투표 및 검증단계(vote & validation)

투표 및 검증단계(vote & validation)에서는 투표자가 투표하면 투표자의 인증서 및 토큰 값을 검증하는 과정이 수행된다. 투표자는 Validator의 공개키로 자신의 투표값을 암호화하여 토큰과 함께 보낸다. Validator는 투표자의 인증서와 토큰 값이 올바른지 확인한다. 만약 모든 값이 올바를 경우, 토큰의 사용 여부를 기록하고 영수증을 반환하여 준다. 투표자의 인증서가 만료되었거나 유효하지 않은 토큰일 경우, 해당 투표는 기록하지 않는다. (그림 15)는 투표 및 검증단계(vote & validation)를 나타내는 그림이다.



(그림 15) 투표 및 검증단계(vote & validation)

앞서 언급했듯이 validator는 토큰의 유효성을 검사하고 유효하지 않은 토큰일 경우 reject를 유효할 경우 영수증을 반환한다. [표 14]는 투표 및 유효성을 검사하는 과정을 알고리즘으로 나타낸 것이며, (그림 16)은 영수증 반환 성공 시 출력되는 로그이다.

[표 14] 투표 및 유효성 검사

Voting

input: Token, Ballot, Voter's private key SK^{voter}, Validator's public key $PK^{validator}$, Validator's private key $SK^{validator}$
Output: A receipt

<Voter>

SK^{voter}(Ballot) ← **Encrypted**(Ballot) as SK^{voter}
$PK^{validator}$(SK^{voter}(Ballot), Token)
    ← **Encrypted**(SK^{voter}(Ballot) , Token) as $PK^{validator}$

<Validator>

SK^{voter}(Ballot), Token
    ← **Decrypted**(SK^{voter}(Ballot) , Token) as $SK^{validator}$

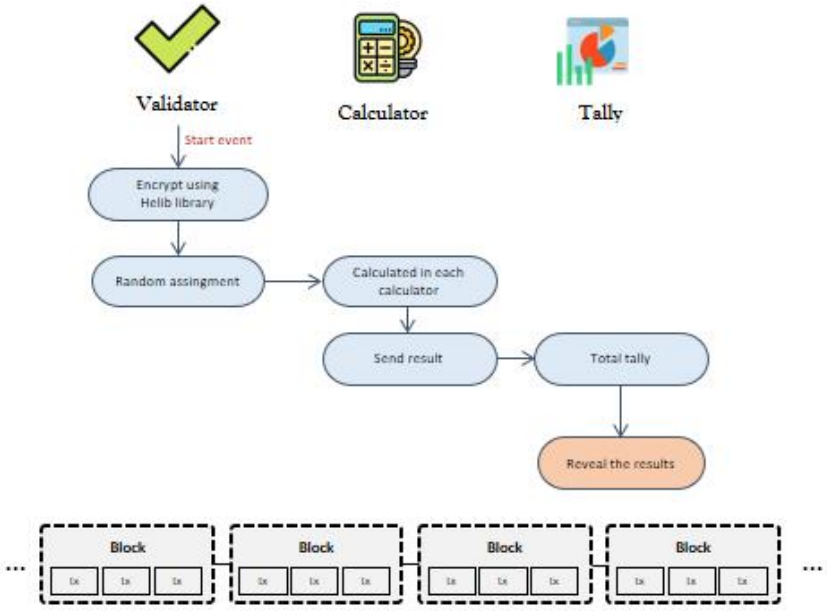
if (Verified(token)) = true **then**
    return receipt
else
    return false
end

(그림 16) 영수증 반환 로그

위 영수증(receipt)을 통해 체인코드의 기록을 보고 유권자는 자신의 투표가 올바르게 집계되었음을 알 수 있다. 이를 통해 개별 검증성을 달성하면서 다른 후보자들의 랜덤 토큰을 같이 출력하여 투표자의 프라이버시를 보장한다. 영수증 반환 후. validator는 HElib 라이브러리를 이용해 투표를 재암호화여 calculator를 랜덤하게 선택하여 보낸다.

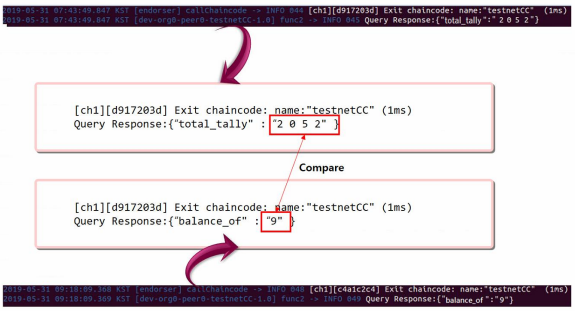
3.2.4 집계 단계(tally result)

집계 단계(tally result)에서는 작은 단위로 집계 후 최종결과를 집계한다. Validator가 Helib 라이브러리를 사용하여 랜덤 한 Calculator에게 값을 전달하고 각각의 Calculator는 암호화 된 상태로 나눠진 투표 값을 계산한다. 이를 Tally에서 최종적으로 합산하여 결과를 공개한다. (그림 17)은 집계 단계(tally result)를 나타내는 그림이다.



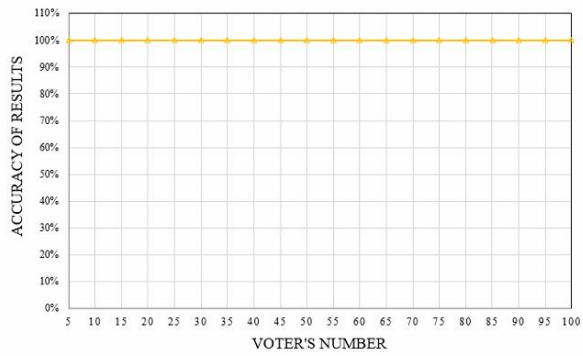
(그림 17) 집계 단계(tally result)

구현한 시스템에서는 전체 검증성을 달성하기 위해 token의 balance와 Tally 결과를 비교한다. (그림 18)은 token의 balance와 Tally 결과를 체인코드로 읽어서 비교하는 그림이다. 구현 시스템에서는 토큰의 값과 집계된 결과 값이 같은 것을 확인함으로써 전제 검증성을 달성했다.



(그림 18) 최종 집계 결과 값 비교

신뢰할 수 있는 전자투표는 투표자의 수에 상관없이 항상 정확한 결과를 도출해내야 한다. (그림 19)는 투표자 수에 따른 정확성 검증을 한 것이다. 제안하는 시스템에서는 투표자의 수 증가와 상관없이 정확한 결과를 도출하는 것을 확인 할 수 있었다.



(그림 19) 투표자 수에 따른 정확성 검증

제 5 장 결론 및 향후 연구

투표는 민주주의 시대에서 투표는 개인이 의사표현을 할 수 있는 가장 기본적이며 주요한 수단이다. 투표는 사회 구성원의 의견을 반영하는 과정을 담고 있기 때문에 투표 과정 및 결과의 신뢰성은 지속적인 화두로 떠오를 것이다. 최근에는 종이투표에서 전자투표로 전환되는 추세에 따라 전자투표의 신뢰성 확보를 위해 다양한 연구가 진행되고 있다. 특히 블록체인을 통해 전자투표의 신뢰성을 확보하기 위한 많은 연구가 진행되고 있지만 신뢰할 수 있는 블록체인 기반 전자투표를 위해서는 누구에게나 투명하게 정보가 공개되는 블록체인의 특성을 고려해 기밀성이라는 또 다른 이슈사항을 해결해야한다.

따라서 본 논문에서는 기밀성을 보장하지 않는 블록체인의 특성을 고려한 허가형 블록체인 기반 전자투표 시스템을 제안했다. 본 논문에서 제안한 시스템은 블록체인 기반의 전자투표로 기존 전자 투표보다 신뢰성을 높였으며 블록체인의 유형별 특징을 이해하고 전자투표에 가장 적합한 허가형 블록체인 기반의 전자투표 시스템을 제안했다. 또한 전자투표에 블록체인 도입 시 생길 수 있는 문제를 도출하고 각각의 문제에 대해 이를 해결방안을 제시했다. 제안하는 시스템은 완전동형 암호를 통해 비밀성, 보안성, 공정성을 보장했으며, 토큰을 통한 적임성 및 1인 1투표 원칙을 보장했다. 또한, 영수증(receipt)을 통해 개별 검증성을 달성 및 집계 결과와 토큰 값 비교로 전체 검증성을 달성했으며, 다자간 계산 개념을 통한 안정성을 확보함으로써 신뢰할 수 있는 블록체인 기반 전자투표를 가능하게 했다.

제안하는 시스템은 메모리 용량에 따른 가상 노드 추가에 한계점이 있었지만 한 노드에 다중토큰을 발급함으로써 다중 노드를 구성한 것과 유사환경을 구성하여 실험을 진행했다. 추후에는 Dapp 개발로 사용자 인터페이스

를 추가하고 패브릭의 보증 정책을 활용하여보다 보다 신뢰성 높은 전자투표를 구현할 계획이다.

참 고 문 헌

[1] 변진욱, “전자투표 현황 및 연구 동향”, 주간기술동향, Vol 1413, 2009.

[2] 과학기술정보통신부, “블록체인 적용한 온라인투표 시범 서비스 첫 개시,” 2018.

[3] 정진우, “전자투표의 효과와 문제점에 관한 탐색적 연구,” 행정논총, 제41권, 제4호, pp. 107-126, 2003.

[4] 한국경제, “선관위 '케이보팅' 보안 허술…"투표 조작도 가능“”, 2015.

[5] 조희정. "해외의 전자투표 추진 현황 연구", 사회연구 Vol 13, no 1 pp.45-72, 2007. 45-72.

[6] Zhang, Wenbin et al. “A Privacy-Preserving Voting Protocol on Blockchain.” 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) , pp. 401-408, 2018.

[7]J. D. Cohen and M. J. Fischer, “A robust and verifiable cryptographically secure election scheme,” pp. 372 - 382, 1985.

[8]J. C. Benaloh and M. Yung, “Distributing the power of a government to enhance the privacy of voters,” pp. 52 - 62, 1986.

[9]K. R. Iversen, “A Cryptographic Scheme for Computerized General Elections,” in Advances in Cryptology — CRYPTO ’91, pp. 405 - 419, 1992.

[10] Ronald L. Rivest, Len Adleman, and Michael L. Dertouzos “ ON DATA BANKS AND PRIVACY HOMOMORPHISMS”, 1978.

[11] 천정희 et al. "개인정보가 보호되는 동형암호기반 금융데이터분석". 금융정보연구, vol. 7, pp.33-60, 2018.

[12]A. Fujioka, T. Okamoto, and K. Ohta, “A practical secret voting

scheme for large scale elections," in Advances in Cryptology — AUSCRYPT '92, Berlin, Heidelberg, pp. 244 - 251, 1993.
[13]J. D. Cohen and M. J. Fischer, "A robust and verifiable cryptographically secure election scheme," pp. 372 - 382, 1985.
[14] J. C. Benaloh and M. Yung, "Distributing the power of a government to enhance the privacy of voters," pp. 52 - 62, 1986.
[15] 김은정 "준동형 암호를 이용한 전자투표 시스템", 고려대학교 대학원 석사학위 논문, 2009.
[16] 성균관 대학교, "전자투표 시스템의 영수증 발급 기술에 관한 연구 ", 정보통신부 보고서, 2008.
[17] 박연아, "전자투표 시스템 신뢰성 확보를 위한 블록체인기술 적용 사례 연구", 국민대학교 대학원 석사학위 논문, 2018.
[18] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system, 2008. URL: http://www. bitcoin. org/bitcoin. pdf (2012).
[19] 강승준," 블록체인 기술의 이해와 개발 현황 및 시사점", 정보통신산업진흥원 이슈리포트 vol13, 2018.
[20] 패브릭 공식문서(https://hyperledger-fabric.readthedocs.io/en/release-1.4)
[21] 윤대근, "하이퍼레저 패브릭으로 배우는 블록체인", 2018.
[22] 디사이퍼(https://medium.com/decipher-media), "공정한 선거를 위한 블록체인 기반 전자투표 시스템 제안", 2019.
[23] https://github.com/giou-k/Voting
[24] https://github.com/hyperledger/fabric/tree/release-1.4/token
[25] 정다운, "블록체인 기술을 활용한 전자투표시스템 개선방안" 순천향대학교 대학원 석사학위논문, 2017.
[26] 이재규, "블록체인을 활용한 해외직구 프로세스 개선방안 연구 -

Hyperledger를 중심으로 -", 숭실대학교 대학원 석사학위 논문, 2018.
[27] 유헌우, "블록체인 방식의 전자투표 시스템 구 성능 개선 방안 연구", 아주대학교 대학원 석사학위 논문, 2016.
[28] 이루다, "블록체인을 활용한 전자투표 시스템 구축", 상명대학교 대학원 석사학위 논문, 2017.
[29] 박우석, " Hyperledger Fabric 블록체인을 위한 TOTP기반 2차 인증 기법", 아주대학교 대학원 석사학위 논문, 2018.
[30] 하현수, 이선준, 정구익, 신용구, 김명호, 김영종. "Public Blockchain 기반의 익명성 전자투표 블록체인 플랫폼 모델" 한국정보과학회 학술발표논문집, pp.1176-1178. 2017.
[31] 김세아, 원예종, 이지은, 최병주. "블록체인 기반 전자투표 시스템 설계 및 구현", 한국정보과학회 학술발표논문집, pp.1931-1933, 2018.
[33] Zijian Bao, Bin Wang, Wenbo Shi, "A privacy-preserving, decentralized and functional Bitcoin e-voting protocol", 2018.
[34] McCorry, Patrick & Shahandashti, Siamak & Hao, Feng. "A Smart Contract for Boardroom Voting with Maximum Voter Privacy", 2017.
[35] Koç, Ali & Yavuz, Emre & Çabuk, Umut & Dalkılıç, Gökhan. "Towards Secure E-Voting Using Ethereum Blockchain", 10.1109/ISDFS.2018.8355340, 2018.
[36] https://github.com/hyperledger/fabric/blob/master/docs/source/token/FabToken.md
[37] https://github.com/s7techlab/cckit
[38] 신동진, "Hyperledger Fabric과 중첩형 무한 해시체인 기반의 일회용 패스워드를 이용한 클라이언트 인증기법", 단국대학교 대학원 석사학위 논문, 2018.

ABSTRACT

A Study on the Design and Implementation of Reliable Electronic Voting System Based on Permissioned Blockchain

Kang Hee Jung
Department of Computer Science
Graduate School of
Sungshin Women's University

Electronic voting has been studied continuously because of the effects such as increasing voting participation, providing convenience, and efficiency of counting votes. It is important to ensure the reliability of voting because e-voting is different from the conventional paper ballot and the process of counting votes is conducted in computer. In order to ensure the reliability of e-voting, the introduction of various information protection technologies has been studied such as zero-knowledge proof, secret sharing, and re-encryption. However, since it is basically performed by a central trusted institution, The possibility of forgery and falsification caused by the attack is still presented.

Recently, attempts have been actively made to solve the problem by introducing a blockchain in which all participants constituting the network share the record and are difficult to forge or falsify. However, if

blockchain is introduced into electronic voting, security research is needed. This is because the blockchain transparently discloses information to all participants in the network. Voting should be conducted only by voters who have the right to vote. However, the public blockchain is not suitable for electronic voting because unauthorized users are allowed to participate. Also, the existing transactions are tracked to identify individuals. Private blockchain are suitable for voting because only authorized users can participate, but research is needed for reliable electronic voting because of the basic characteristics of the block chain that all network participants share information.

Therefore, in this paper proposes an reliable electronic voting system based on blockchain. The proposed system uses ① blockchain to prevent the manipulation of the central server and forgery due to external attack, ② the network is composed of only valid voters by using hyperledger fabric. Also, in order to prevent the possibility of manipulation by one node, ③ we apply the concept of borrowing a multi-party algorithm. In addition, When counting votes, ④ we used Homomorphic Encryption which can be calculated in encrypted form. Lastly, we have achieved ⑤ individual verification by issuing a receipt. However, we have verified the ⑥ voter's privacy through receipt by outputting a random token value for the other candidates, and ⑦ confirmed the total number of tokens and the final value.