(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0087913
(43) 공개일자 2020년07월22일

(51) 국제특허분류(Int. Cl.)
G06Q 50/26 (2012.01) *G07C 13/00* (2006.01)
H04L 9/06 (2006.01) *H04L 9/30* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06Q 50/26 (2013.01)
G07C 13/00 (2013.01)
(21) 출원번호 10-2019-0003894
(22) 출원일자 2019년01월11일
심사청구일자 2019년01월11일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
장주욱
서울특별시 서대문구 가재울미래로 2, 206동 202호 (남가좌제1동, DMC파크뷰자이)
송재근
서울특별시 강서구 등촌로39길 63-26 206호 (등촌동,아름채)
한동희
서울특별시 서대문구 이화여대 2길 26-8 401호
(74) 대리인
이지연

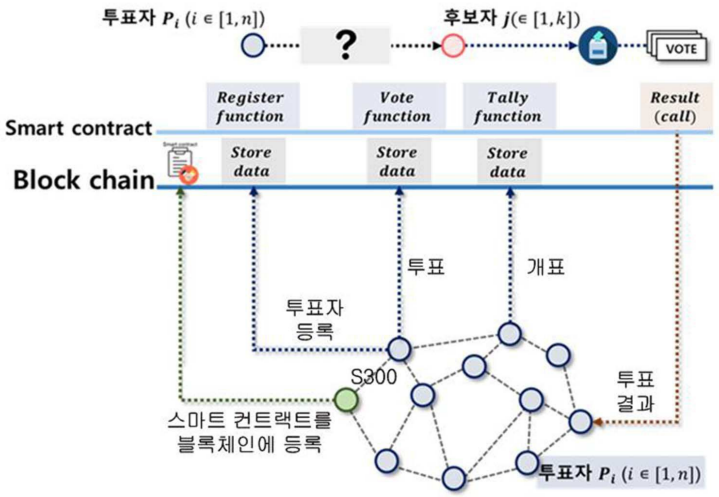
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **블록체인 네트워크를 기반으로 한 비밀 전자 투표 시스템 및 방법**

(57) 요 약

본 발명은 블록체인 네트워크를 기반으로 한 비밀 전자 투표 시스템에 관한 것이다. 상기 비밀 전자 투표 시스템을 구성하는 각 노드는, 투표 프로세스를 코드화하여 스마트 컨트랙트로 작성하고, 스마트 컨트랙트를 포함하는 트랜잭션을 생성하여 블록체인에 저장하는 투표 프로세스 등록 모듈; 예비 투표자인 노드가 블록체인 내 스마트 컨트랙트에 투표자로 등록하는 투표자 등록 모듈; 투표자로 등록된 노드가 다수의 후보자 중 하나를 선택하고 투표하여 블록체인 내 스마트 컨트랙트에 기록하는 투표 모듈; 모든 투표자들이 블록체인 내 스마트 컨트랙트에 등록한 투표 정보들을 이용하여 개표하는 개표 모듈;을 구비한다. 상기 투표 프로세스는, 예비 투표자들에 대하여 투표자 등록을 위하여 사용되는 비대화형 영지식 증명 함수, 투표자들의 투표를 위하여 사용되는 1-out-of-k 비대화형 영지식 증명 함수 및 완전 탐색 방식의 개표 함수를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 9/3033 (2013.01)
H04L 9/3218 (2013.01)
H04L 2209/463 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 NRF-2016R1D1A1B01009027
부처명 교육부
연구관리전문기관 한국연구재단
연구사업명 이공학개인기초연구지원사업
연구과제명 블록체인 알고리즘의 개선 및 차세대 활용 기법의 연구
기 여 율 1/1
주관기관 서강대학교 산학협력단
연구기간 2018.03.01 ~ 2019.02.28

명 세 서

청구범위

청구항 1

예비 투표자들이 노드로 참여하여 구성된 블록체인 네트워크를 기반으로 한 비밀 전자 투표 시스템에 있어서, 블록체인 네트워크를 구성하는 각 노드는,

투표 프로세스를 코드화하여 스마트 컨트랙트로 작성하고, 스마트 컨트랙트를 포함하는 트랜잭션을 생성하여 블록체인 네트워크에 전파하고 사전 설정된 합의 알고리즘에 따라 블록을 생성하여 블록체인에 저장하는 투표 프로세스 등록 모듈;

예비 투표자인 노드가 블록체인 내 스마트 컨트랙트에 투표자로 등록하는 투표자 등록 모듈;

투표자로 등록된 노드가 다수의 후보자 중 하나를 선택하고 투표하여 블록체인 내 스마트 컨트랙트에 기록하는 투표 모듈;

모든 투표자들이 블록체인 내 스마트 컨트랙트에 등록한 투표 정보들을 이용하여 개표하는 개표 모듈;

을 구비하는 것을 특징으로 하는 블록체인 네트워크를 기반으로 한 비밀 전자 투표 시스템.

청구항 2

제1항에 있어서, 상기 투표 프로세스 등록 모듈에 의해 블록체인 내 스마트 컨트랙트에 저장되는 투표 프로세스는,

예비 투표자들에 대하여 투표자 등록을 위하여 사용되는 비대화형 영지식 증명 함수, 투표자들의 투표를 위하여 사용되는 1-out-of-k 비대화형 영지식 증명 함수 및 완전 탐색 방식의 개표 함수를 포함하는 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 시스템.

청구항 3

제1항에 있어서, 상기 투표자 등록 모듈은,

예비 투표자인 노드가 개인 투표키 x_i 를 이용하여 공개 투표키와 증명에 쓰이는 공개값들을 포함하는 입력 인자값을 구하고, 상기 입력 인자값으로 상기 스마트 컨트랙트에 저장된 비대화형 영지식 증명 함수를 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록하는 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 시스템.

청구항 4

제3항에 있어서, 상기 입력 인자값은 공개 투표키 X_i, 증명에 쓰이는 공개값들 W, r 이며,

공개 투표키 X_i는 $g^{x_i} \bmod p$ 이며, 공개값 W는 $W = g^{w} \bmod p$ 이며, 공개값 $r(=w - x_i c)$인 것을 특징으로 하며,

여기서, p는 예비투표자에 의해 생성되는 소수이며, q는 $q \mid (p-1)$ 를 만족하는 소수이며, g, h 는 Prime-order q의 곱셈 순환군(Multiplicative cyclic groups)인 G의 생성원이며, w는 임의의 비밀값으로서 $w \in Z_q$를 만족하는 값들 중 선택되는 값이며, c는 해시 함수를 이용하여 생성하는 랜덤한 값이며, Zq는 q에 대한 수의 집합으로 1,2,쪋, q-1을 가지는 수의 집합인 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 시스템.

청구항 5

제1항에 있어서, 상기 투표 모듈은,

등록된 투표자들이 선택하는 후보에 대하여 투표를 수행하기 위해 개인 투표키 x_i를 이용하여 입력 인자값들을 구하고, 상기 입력 인자값으로 상기 스마트 컨트랙트에 기록된 1-out-of-k 비대화형 영지식 증명 함수를 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록하는 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 시스템.

청구항 6

제5항에 있어서, 상기 투표 모듈에서의 1-out-of-k 비대화형 영지식 증명 함수의 입력 인자값은 x, y, c, $a_{1,2,\ldots,k-1,k}$, $b_{1,2,\ldots,k-1,k}$, $c_{1,2,\ldots,k-1,k}$, $r_{1,2,\ldots,k-1,k}$인 것을 특징으로 하며,

여기서, $(x,y)=(g^{x_i}, h^{x_i} \cdot g^{v_i})$이며, v_j는 투표자가 선택한 후보자의 후보값이며, p는 예비투표자에 의해 생성되는 소수이며, q는 $q|(p-1)$를 만족하는 소수이며, g, h는 Prime-order q의 곱셈 순환군(Multiplicative cyclic groups)인 G의 생성원이며, w는 임의의 비밀값으로서 $w \in Z_q$를 만족하는 값들 중 선택되는 값이며, c는 해시 함수를 이용하여 생성하는 랜덤한 값이며, $a_{1,2,\ldots,k-1,k}$ $b_{1,2,\ldots,k-1,k}$은 투표자가 투표한 값에 따라 투표의 비밀성을 유지하기 위한 진짜 투표값과 가짜 투표값들의 집합을 나타내며 c는 자신이 투표한 후보자의 값과 앞선 투표값들의 집합을 해시 함수를 통해 해싱한 값이며, $c_{1,2,\ldots,k-1,k}$ $r_{1,2,\ldots,k-1,k}$은 자신이 한 투표가 유효함을 입증하기 위해 c값을 통해 생성되는 값인 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 시스템.

청구항 7

제1항에 있어서, 상기 개표 모듈은,

투표자의 투표가 종료된 후 완전 탐색 방식으로 각 투표자에 의해 실행되어 개표되는 것을 특징으로 하며,

블록체인 내 스마트 컨트랙트에 기록된 1-out-of-k 비대화형 영지식 증명으로 검증받은 모든 투표자의 투표 결과값인 w값과 각 후보자에 대응되는 변수인 후보값 v_j를 이용하여 계산되는 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 시스템.

청구항 8

예비 투표자들이 노드로 참여하여 구성된 블록체인 네트워크를 기반으로 한 비밀 전자 투표 방법에 있어서,

(a) 블록체인 네트워크를 구성하는 노드가, 투표 프로세스를 코드화하여 스마트 컨트랙트로 작성하고, 스마트 컨트랙트를 포함하는 트랜잭션을 생성하여 블록체인 네트워크에 전파하고 사전 설정된 합의 알고리즘에 따라 블록을 생성하여 블록체인의 최초 블록으로 저장하는 단계;

(b) 예비 투표자인 노드들이 블록체인 내 스마트 컨트랙트에 투표자로 등록하는 단계;

(c) 투표자로 등록된 노드들이 다수의 후보자 중 하나를 선택하고 투표하여 블록체인 내 스마트 컨트랙트에 등록하는 단계;

(d) 블록체인 내 스마트 컨트랙트에 등록된 투표 정보들을 이용하여 개표하는 단계;

를 구비하는 것을 특징으로 하는 블록체인 네트워크를 기반으로 한 비밀 전자 투표 방법.

청구항 9

제8항에 있어서, 상기 블록체인 내 스마트 컨트랙트에 저장되는 투표 프로세스는,

예비 투표자들에 대한 투표자 등록을 위하여 사용되는 비대화형 영지식 증명 함수, 투표자들의 투표를 위하여 사용되는 1-out-of-k 비대화형 영지식 증명 함수 및 완전 탐색 방식의 개표 함수를 포함하는 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 방법.

청구항 10

제8항에 있어서, 상기 (b) 단계는,

예비 투표자인 노드가 개인 투표키 x_i 를 이용하여 공개 투표키와 증명에 쓰이는 공개들값을 포함하는 입력 인자값을 구하고, 상기 입력 인자값으로 상기 스마트 컨트랙트에 저장된 비대화형 영지식 증명 함수를 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록하는 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 방법.

청구항 11

제8항에 있어서, 상기 (c) 단계는,

등록된 투표자들이 선택하는 후보에 대하여 투표를 수행하기 위해 개인 투표키 x_i를 이용하여 입력 인자값들을 구하고, 상기 입력 인자값으로 상기 스마트 컨트랙트에 기록된 1-out-of-k 비대화형 영지식 증명 함수를 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록하는 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 방법.

청구항 12

제8항에 있어서, 상기 (d) 단계는,

투표자의 투표가 종료된 후 완전 탐색 방식으로 각 투표자에 의해 실행되어 개표되는 것을 특징으로 하며,

블록체인 내 스마트 컨트랙트에 기록된 1-out-of-k 비대화형 영지식 증명으로 검증받은 모든 투표자의 투표 결과값인 u값과 각 후보자에 대응되는 변수인 후보값 v_j를 이용하여 계산되는 것을 특징으로 하는 블록체인 네트워크를 기반으로 하는 비밀 전자 투표 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 네트워크를 기반으로 한 비밀 전자 투표 시스템에 관한 것으로서, 더욱 구체적으로는 투표자들이 참여 노드로서 블록체인 네트워크를 구성한 후 투표 프로세스를 코드화 하여 스마트 컨트랙트로 작성하여 블록체인에 기록하고, 스마트 컨트랙트의 투표 프로세스를 통해 예비투표자 등록, 투표자 투표 및 개표 과정을 진행하고 모든 투표자의 투표 결과를 블록체인 내의 스마트 컨트랙트에 기록 및 저장함으로써, 계약 이행의 강제성 및 신뢰성을 보장할 수 있으며 비밀 투표를 진행할 수 있는 비밀 전자 투표 시스템에 관한 것이다.

배 경 기 술

[0002] 공공 인터넷과 같은 무선 통신 기술이 발달함에 따라, 기존의 종이 투표 방식을 대신하는 전자투표에 대한 연구가 다양하게 진행되고 있다. 전자투표는 네트워크를 이용한 전자식 투표로, 통신 가능한 단말기를 이용하여 투표가 가능하므로, 시간적, 공간적 제약이 없다는 장점이 있다.

[0003] 하지만, 이러한 장점에도 불구하고, 종래의 전자투표 방식은 여러 문제점이 발견되고 있다. 특히, 종래의 전자투표 시스템은 투표자가 투표한 후보자를 숨기고 다수의 후보자 중 하나의 후보자에게 투표했다는 사실을 증명하는 것이 매우 어렵다. 또한, 종래의 전자 투표 시스템은 투표 프로세스를 총괄하는 중앙 서버가 존재하기 때문에, 중앙 서버에 단일 장애점(Single Point of Failure)이나 데이터의 위조 및 변조의 문제가 있다. 또한, 중앙 서버없이 투표자들끼리 네트워크를 구성하여 전자 투표 시스템을 설계하더라도, 투표 과정에서 모두가 투표했다는 사실을 확인하는 것이 매우 어렵다. 해커 등에 의해 악의적인 목적으로 노드가 점령당하는 경우 투표 내용이 포함된 패킷이 조작되거나 훼손될 수 있으며, 전자 투표를 행사한 대상의 단말기를 역추적하여 어떤 사람이 어떠한 후보자에게 투표했는지에 대한 정보가 유출될 수 있다.

[0004] 한편, 영지식 증명(zero knowledge proof; ZKP)이란 주로 암호학에서 어느 증명자가 상대방 검증자에게 어떤 명제(statement)가 참이라는 것을 증명할 때, 그 명제의 참 거짓 여부를 제외한 어떤 지식도 노출시키지 않는 상

호 작용의 절차를 의미한다. 어떠한 명제가 참이라는 것을 증명하려는 쪽을 증명자(prover)라고 하고, 증명 과정에 참여하여 증명자와 정보를 주고 받는 쪽을 검증자(verifier)라고 한다. 영지식 증명에 참여하는 당사자들이 상대방을 속이려는 목적으로 프로토콜을 임의로 변경하는 경우, 당사자들이 부정직하다 또는 정직하지 않다고 한다. 그 외의 경우에는 정직하다고 한다.

[0005] 영지식 증명은 세 가지 성질, 즉 완전성, 건실성 및 영지식성을 만족하여야 한다. 완전성(completeness)은, 어떤 명제가 참이면, 정직한 증명자는 정직한 검증자에게 이 사실을 납득시킬 수 있어야 하는 것이다. 건실성(soundness)은, 어떤 명제가 거짓이면, 어떠한 부정직한 증명자라도 정직한 검증자에게 이 문장이 사실이라고 납득시킬 수 없어야 하는 것이다. 마지막으로, 영지식성(zero-knowledgeness)은, 어떤 명제가 참이면, 검증자는 문장의 참 거짓 이외에는 아무것도 알 수 없어야 하는 것이다.

[0006] 한편, 블록체인(Blockchain)은 공공 거래 장부라고도 불리우는데, 블록(block)에 데이터를 담아 체인(chain) 형태로 연결한 것으로서, 수많은 노드에 이를 동시에 복제해 저장하는 분산형 데이터 저장 기술이다. 블록체인 기술은 중앙 집중형 서버에 거래 기록을 보관하지 않고 거래에 참여하는 모든 사용자에게 거래 내역을 보내 주며, 거래때마다 모든 거래 참여자들이 정보를 공유하고 이를 대조함으로써 데이터 위조 및 변조를 방지할 수 있게 된다.

[0007] 블록체인을 저장하는 다수 개의 노드들로 이루어지는 블록체인 네트워크에 있어서, 하나의 노드가 전자 서명된 트랜잭션을 브로드캐스팅하면, 이를 수신한 모든 노드들은 작업 증명 과정을 진행하게 되고, 이에 따라 최초로 논스값을 찾은 노드는 블록체인 네트워크의 다른 노드들에 의해 검증된 후 블록 생성 권한을 갖게 된다. 블록 생성 권한을 가진 노드는 트랜잭션을 포함한 블록 생성 정보를 블록체인 네트워크의 모든 노드들로 브로드캐스팅하게 되고, 이를 수신한 모든 노드들은 트랜잭션을 포함하는 블록을 생성하고 자신의 블록체인에 상기 생성된 블록을 연결시켜 저장하게 된다.

[0008] 이에 본 발명은 블록체인 네트워크를 기반으로 하여 영지식 증명을 이용하여 비밀 전자 투표 시스템을 제안하고자 한다.

선행기술문헌

특허문헌

[0009] (특허문헌 0001) 한국등록특허공보 제 10-1837169호

(특허문헌 0002) 한국등록특허공보 제 10-1908677호

발명의 내용

해결하려는 과제

[0010] 전술한 문제점을 해결하기 위한 본 발명의 목적은 블록체인 네트워크를 기반으로 하여, 다수의 후보자와 다수의 투표자들에 대하여 비대화형 영지식 증명을 이용한 투표자 등록 과정, 1-out-of-k 비대화형 영지식 증명을 이용한 투표 과정 및 완전 탐색 방식의 개표 과정을 포함하는 투표 프로세스를 코드화하여 스마트 컨트랙트에 작성하여 블록체인에 기록하고, 이를 통해 다수의 후보자에 대한 비밀 전자 투표를 안전하게 진행할 수 있도록 하는 비밀 전자 투표 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0011] 전술한 기술적 과제를 달성하기 위한 본 발명의 제1 특징에 따른 비밀 전자 투표 시스템은 예비 투표자들이 노드로 참여하여 구성된 블록체인 네트워크를 기반으로 한 비밀 전자 투표 시스템에 관한 것으로서, 상기 블록체인 네트워크를 구성하는 각 노드는, 투표 프로세스를 코드화하여 스마트 컨트랙트로 작성하고, 스마트 컨트랙트를 포함하는 트랜잭션을 생성하여 블록체인 네트워크에 전파하고 사전 설정된 합의 알고리즘에 따라 블록을 생성하여 블록체인에 저장하는 투표 프로세스 등록 모듈; 예비 투표자인 노드가 블록체인 내 스마트 컨트랙트에 투표자로 등록하는 투표자 등록 모듈; 투표자로 등록된 노드가 다수의 후보자 중 하나를 선택하고 투표하여 블록체인 내 스마트 컨트랙트에 등록하는 투표 모듈; 모든 투표자들이 블록체인 내 스마트 컨트랙트에 등록한 투표 정보들을 이용하여 개표하는 개표 모듈;을 구비한다.

[0012] 전술한 제1 특징에 따른 비밀 전자 투표 시스템에 있어서, 상기 투표 프로세스 등록 모듈에 의해 블록체인 내 스마트 컨트랙트에 저장되는 투표 프로세스는, 예비 투표자들에 대하여 투표자 등록을 위하여 사용되는 비대화형 영지식 증명 함수, 투표자들의 투표를 위하여 사용되는 1-out-of-k 비대화형 영지식 증명 함수 및 완전 탐색 방식의 개표 함수를 포함하는 것이 바람직하다.

[0013] 전술한 제1 특징에 따른 비밀 전자 투표 시스템에 있어서, 상기 투표자 등록 모듈은, 예비 투표자인 노드가 개인 투표키 x_i 를 이용하여 공개 투표키와 증명에 쓰이는 공개값들을 포함하는 입력 인자값을 구하고, 상기 입력 인자값으로 상기 스마트 컨트랙트에 저장된 비대화형 영지식 증명 함수를 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록하는 것이 바람직하다.

[0014] 전술한 제1 특징에 따른 비밀 전자 투표 시스템에 있어서, 상기 투표 모듈은, 등록된 투표자들이 선택하는 후보에 대하여 투표를 수행하기 위해 개인 투표키 x_i를 이용하여 입력 인자값들을 구하고, 상기 입력 인자값으로 상기 스마트 컨트랙트에 기록된 1-out-of-k 비대화형 영지식 증명 함수를 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록하는 것이 바람직하다.

[0015] 전술한 제1 특징에 따른 비밀 전자 투표 시스템에 있어서, 상기 개표 모듈은, 투표자의 투표가 종료된 후 완전 탐색 방식으로 각 투표자에 의해 실행되어 개표되는 것을 특징으로 하며, 블록체인 내 스마트 컨트랙트에 기록된 1-out-of-k 비대화형 영지식 증명으로 검증받은 모든 투표자의 투표 결과값인 u값과 각 후보자에 대응되는 변수인 후보값 v_j를 이용하여 계산되는 것이 바람직하다.

[0016] 본 발명의 제2 특징에 따른 비밀 전자 투표 방법은, 예비 투표자들이 노드로 참여하여 구성된 블록체인 네트워크를 기반으로 한 비밀 전자 투표 방법에 관한 것으로서, (a) 블록체인 네트워크를 구성하는 노드가, 투표 프로세스를 코드화하여 스마트 컨트랙트로 작성하고, 스마트 컨트랙트를 포함하는 트랜잭션을 생성하여 블록체인 네트워크에 전파하고 사전 설정된 합의 알고리즘에 따라 블록을 생성하여 블록체인의 최초 블록으로 저장하는 단계; (b) 예비 투표자인 노드들이 블록체인 내 스마트 컨트랙트에 투표자로 등록하는 단계; (c) 투표자로 등록된 노드들이 다수의 후보자 중 하나를 선택하고 투표하여 블록체인 내 스마트 컨트랙트에 등록하는 단계; (d) 블록체인 내 스마트 컨트랙트에 등록된 투표 정보들을 이용하여 개표하는 단계; 를 구비한다.

발명의 효과

[0017] 본 발명에 따른 전자 투표 시스템은 스마트 컨트랙트 기술을 활용하여 투표 프로세스를 코드화하여 스마트 컨트랙트로 작성하여 블록체인에 기록함으로써, 실행할 때 계약 이행의 강제성 및 신뢰성을 보장할 수 있게 된다. 이로 인해 투표 프로세스가 기록된 스마트 컨트랙트를 실행함으로써 진행되는 예비 투표자의 등록 및 투표자의 투표를 수행할 수 있게 된다.

[0018] 또한, 본 발명에 따른 전자 투표 시스템은 모든 투표자의 투표가 종료된 시점에 개표를 진행하기 위하여, 블록체인에 기록된 스마트 컨트랙트 내의 개표 관련 코드를 실행함으로써, 투표자가 스스로 개표를 진행할 수 있고, 이 결과로 각 후보자에 대한 투표수를 확인할 수 있게 된다.

[0019] 또한, 본 발명에 따른 전자 투표 시스템은 예비 투표자가 투표자로서 등록하기 위하여 스마트 컨트랙트 내의 비대화형 영지식 증명을 실행하고, 투표자가 투표를 수행할 때는 스마트 컨트랙트 내의 1-out-of-k 비대화형 영지식 증명을 실행함으로써, 투표자가 다수의 후보자 중 하나에 대하여 투표한 사실은 확인할 수 있지만 투표한 후보가 누구인지는 숨길 수 있게 된다.

[0020] 또한, 이 모든 트랜잭션은 블록으로 구성되어 사전 설정된 합의 알고리즘에 따라 블록체인에 저장되고 공유하게 되므로, 인증 및 부인 방지, 무결성을 보장할 수 있을 뿐만 아니라 악의적인 공격자의 해킹 및 데이터 위/변조 시도가 원천적으로 차단될 수 있게 된다.

[0021] 또한, 본 발명에 따른 전자 투표 시스템은 단일의 중앙 서버를 사용하지 않기 때문에 중앙 서버에 의한 단일 장애점의 문제가 발생되는 것을 방지할 수 있게 된다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 전체 시스템을 설명하기 위하여 도시한 모식도이다.

도 2는 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 각 노드가 블록체인에 기록된 스마트 컨트랙트를 통해 수행하는 전자 투표 과정을 전체적으로 도시한 순서도이다.

도 3은 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 투표자 등록 모듈(30)의 동작을 순차적으로 설명하는 순서도이며, 도 4는 투표자 등록 모듈에서 예비투표자와 검증자간의 증명 과정을 설명하는 순서도이다.

도 5는 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 각 후보자에 대응되는 후보값을 설정하는 과정을 설명하기 위하여 도시한 모식도이다.

도 6은 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 투표 모듈(40)을 통해 각 투표자들이 투표를 수행하는 과정을 순차적으로 도시한 순서도이다.

도 7은 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 투표자들이 투표를 수행하기 위하여 1-out-of-k 비대화형 영지식 증명을 수행할 때의 투표자측의 증명 과정을 도시한 순서도이다.

도 8은 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 투표자들이 투표를 수행하기 위하여 1-out-of-k 비대화형 영지식 증명을 수행할 때의 검증자측의 증명 과정을 도시한 순서도이다.

도 9는 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 개표 모듈(50)의 동작을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 본 발명에 따른 블록체인 네트워크를 기반으로 한 전자 투표 시스템은 투표에 참여하고자 하는 투표자들이 노드로서 블록체인 네트워크를 구성하고 투표 프로세스를 코드화하여 스마트 컨트랙트를 작성하여 최초에 블록체인에 기록하게 되며, 상기 투표 프로세스는 비대화형 영지식 증명, 1-out-of-k 비대화형 영지식 증명과 완전 탐색 방식의 개표 과정을 포함하는 것을 특징으로 한다.

[0024] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 블록체인 네트워크를 기반으로 한 전자 투표 시스템의 구성 및 동작에 대하여 구체적으로 설명한다.

[0025] 도 1은 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 전체 시스템을 설명하기 위하여 도시한 모식도이며, 도 2는 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 각 노드가 블록체인에 기록된 스마트 컨트랙트를 통해 수행하는 전자 투표 과정을 전체적으로 도시한 순서도이다.

[0026] 도 1 및 도 2를 참조하면, 본 발명에 따른 블록체인 네트워크를 기반으로 한 전자 투표 시스템(1)은 투표하고자 하는 예비 투표자들이 노드로서 구성한 블록체인 네트워크(10)를 기반으로 이루어지며, 각 노드는 블록체인(20), 투표 프로세스 등록 모듈(30), 투표자 등록 모듈(40), 투표 모듈(50), 개표 모듈(60)을 구비한다.

[0027] 상기 블록체인(20)은 투표 프로세스를 코드화한 스마트 컨트랙트, 투표자들에 대한 정보, 투표자들의 투표 정보, 개표 정보 등을 저장한 블록들을 사슬 형태로 연결하여 순차적으로 저장한 데이터 저장소이다.

[0028] 상기 투표 프로세스 등록 모듈(30)은 사전 설정된 투표 프로세스를 코드화하여 스마트 컨트랙트로 작성하고 이를 트랜잭션으로 생성하여 블록체인 네트워크에 전파하고 사전 설정된 합의 알고리즘에 따라 블록체인의 최초 블록으로 기록한다. 상기 코드화되어 스마트 컨트랙트에 기록되는 투표 프로세스는 투표자 등록을 위한 비대화형 영지식 증명 함수, 투표자들의 투표를 위한 1-out-of-k 비대화형 영지식 증명 함수 및 완전 탐색 방식의 개표 함수를 포함한다.

[0029] 상기 투표자 등록 모듈(40)은, 블록체인 네트워크에 참여하는 예비 투표자들이 투표에 참여하기 위하여 투표자로 등록을 진행하는 모듈로서, 각 예비투표자들은 개인 투표키 x_i를 이용하여 3개의 입력 인자값(공개 투표키 X_i, 증명에 쓰이는 공개값 W, r)을 구하고, 상기 입력 인자값으로 비대화형 영지식 증명을 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록한다. 한편, 상기 개인 투표키 x_i는 예비투표자들이 블록체인 네트워크에 참여할 때 생성되는 고유한 키로 본인만이 알 수 있는 값이다.

[0030] 상기 투표 모듈(50)은, 상기 투표자 등록 모듈을 통해 등록된 투표자들은 선택하는 후보에 대하여 투표를 수행하기 위해 개인 투표키 x_i를 이용하여 입력 인자값(x, y, c, $\alpha_{1,2,\ldots,k-1,k}$, $b_{1,2,\ldots,k-1,k}$ $c_{1,2,\ldots,k-1,k}$

$r_{1,2,\ldots,k-1,k}$)을 구하고, 상기 입력 인자값으로 1-out-of-k 비대화형 영지식 증명을 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록한다. 이 때 기록된 모든 투표자의 u값으로 이후에 개표를 진행하게 된다.

[0031] 상기 개표 모듈(60)은 완전 탐색 방식으로 각 투표자에 의해 개표를 진행하는 것으로서, 블록체인 내 스마트 컨트랙트에 기록된 1-out-of-k 비대화형 영지식 증명으로 검증받은 모든 투표자의 u값을 곱함으로써 시작된다. 곱한 값은 소거법에 의하여 $g^{\Sigma v_i}$이 되는데 이때 v_j는 각 후보자에 대응되는 변수인 후보값으로 여기서는 투표자들이 투표한 모든 후보값을 더한 것이 지수가 된다. 완전 탐색 방식을 적용함으로써 후보자들 중 가장 큰 후보값부터 제수(divisor)로 두고 $g^{\Sigma v_i}$를 피제수(dividend) 두어 나눗셈을 수행한다. 이때 나눠지는 횟수를 해당 후보값에 대응되는 후보자의 투표 수로 집계할 수 있고, 해당 나눗셈 과정을 다음으로 큰 후보값을 제수로 둠으로써 가장 작은 후보값까지 반복 수행한다. 이 결과로 각 후보자에 대한 투표 수를 집계할 수 있다.

[0032] 한편, 본 발명에 따른 전자 투표 시스템을 구성하는 각 모듈에 의해 진행되는 과정에서 각 노드들이 생성하는 모든 트랜잭션은 해당 노드의 개인키와 결합하여 서명된 후 블록체인 네트워크에 전파되고, 송신 노드 이외의 모든 노드들이 트랜잭션의 유효성을 검증하고, 일정 기간동안 트랜잭션을 모아 블록의 생성 권한을 얻기 위한 작업 증명(Proof of Work)이라는 합의 과정을 통해 블록으로 구성되어 다시 블록체인 네트워크로 전파된다. 이후 상기 전파된 블록은 모든 노드로부터 유효성을 확인받은 후 n개의 블록으로 이루어진 블록체인에 n+1번째 블록으로 이어지게 된다. 그 결과, 블록체인에 기록되는 모든 트랜잭션 및 데이터는 무결성을 보장받고 블록체인 네트워크의 모든 노드들은 블록체인의 기록들을 공유하게 된다. 한편, 본 발명에서는 합의 알고리즘으로 작업 증명(Proof of Work) 방식을 사용하는 것을 예시적으로 설명하고 있으나, 이것에 한정하는 것은 아니며 다른 합의 알고리즘도 사용될 수 있다.

[0033] 또한, 블록체인에 데이터를 기록하는 것은 해당 트랜잭션에서 스마트 컨트랙트 내 함수를 호출할 때 함수의 입력값에 따른 출력값을 스마트 컨트랙트에 state로써 기록(혹은 변경)하는 것이기 때문에 스마트 컨트랙트에 기록하는 것과 동일한 것이고, 이때 스마트 컨트랙트에 기록된 값은 블록체인에 기록한 것과 동일한 것이기 때문에 기록된 값의 무결성을 보장받는다.

[0034] 이하, 도 3 및 도 4를 참조하여 본 발명의 바람직한 실시예에 따른 전자 투표 시스템의 투표자 등록 모듈(30)에 대하여 구체적으로 설명한다.

[0035] 도 3은 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 투표자 등록 모듈(30)의 동작을 순차적으로 설명하는 순서도이며, 도 4는 투표자 등록 모듈에서 예비투표자와 검증자간의 증명 과정을 설명하는 순서도이다.

[0036] 도 3을 참조하면, 예비 투표자들이 투표에 참여하기 위해 투표자 등록 모듈(30)을 통해 투표자로서 등록을 진행하게 된다. 이때 개인 투표키 x_i를 이용하여 3개의 입력 인자값(공개 투표키 X_i, 증명에 쓰이는 공개값 W, r)으로 비대화형 영지식 증명을 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록하는 과정으로 비대화형 영지식 증명은 구체적으로 다음과 같이 진행된다.

[0037] 먼저, 블록체인 네트워크에 참여하는 예비 투표자는 소수 p를 생성한 후 $q|(p-1)$를 만족하는 소수 q를 선택한다. 그리고 Prime-order q의 곱셈 순환군(Multiplicative cyclic groups)을 G이라 하고, G의 생성원을 g,h 라고 한다. 이로써 초기값인 (p, q, g, h)가 생성된다(단계 300 및 도 4의 ①,②,③). 상기 g, h 는 G의 생성원으로, g는 투표 자격 증명 과정과 이후 투표 과정에서 모두 사용되는 값이고, h는 투표 과정에서 사용되는 값이다.

[0038] 다음, 예비 투표자는 개인 투표키 $x_i \in Z_q$와 공개 투표키 $g^{x_i} \bmod p$를 생성하고, 이번 증명에서만 사용될 임의의 비밀값 $w \in Z_q$를 선택하고 공개값 $W = g^w \bmod p$를 생성한다(단계 310 및 도 4의 ④). 개인 투표키 x_i와 비밀값 w는 투표자만 알고 있는 값으로, 이 값을 검증자에게 알리지 않고 오직 생성된 공개 투표키 X_i와 공개값 W를 검증자에게 보내게 된다. 그리고 해시 함수를 이용하여 투표자가 조작할 수 없는 랜덤한 값 c를 생

성하고 $r(=w-x_i c)$을 생성한다(단계 320 및 도 4의 ⑤,⑥). 여기서, Zq는 q에 대한 수의 집합으로 1,2, 쩐, q-1 를 가지고 있는 수의 집합으로 이루어진다.

[0039] 다음, 스마트 컨트랙트 내 비대화형 영지식 증명 함수를 실행하는 트랜잭션을 생성하고(단계 330), 검증자에게 보낼 값들을 상기 비대화형 영지식 증명 함수의 입력 인자값으로 트랜잭션에 추가한다(단계 340). 이때, 검증자에게 보낼 값으로는 W,r을 포함하게 된다.

[0040] 다음, 해당 트랜잭션을 자신의 개인키로 서명한 후 블록체인 네트워크에 전파하고(단계 350), 작업증명(POW) 과정을 거쳐 해당 트랜잭션을 블록으로 구성한 후 블록체인에 다시 전파하고(단계 352), 이를 수신한 모든 노드들에 의해 블록의 유효성을 검증받고(단계 354), 일정 개수 이상의 노드들이 해당 블록에 대해 승인하면 블록 체인에 마지막 블록으로 연결하여 저장 및 공유하게 된다(단계 356).

[0041] 한편, 스마트 컨트랙트의 비대화형 영지식 증명 함수의 입력 인자값을 수신한 스마트 컨트랙트는, 비대화형 영지식 증명 함수를 실행하여 검증자로서 검증을 진행하게 된다(단계 370 및 도 4의 ⑦,⑧). 이 때, 해시 함수로 c를 생성한 후 (도 4의 ⑦) W와 $g^r X_i^c$가 동일한지 검증함으로써(도 4의 ⑧) 투표자가 개인 투표키 x_i를 보유하고 있다는 사실을 검증하면서 해당 사실 외의 정보를 얻지 못한다. 다음, 상기 비대화형 영지식 증명 함수의 동작 후 해당 검증 사실과 예비투표자에 대한 공개 투표키를 블록체인 내 스마트 컨트랙트에 기록함으로써, 예비 투표자에 대하여 투표자로서의 등록을 완료하게 된다(단계 372).

[0042] 도 5는 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 각 후보자에 대응되는 후보값을 설정하는 과정을 설명하기 위하여 도시한 모식도이다.

[0043] 도 5를 참조하면, 본 발명에 따른 전자 투표 시스템은 다수의 후보자를 두기 위하여 각 후보자에 대응되는 후보값(v)을 설정하기 위하여, j번째 후보자에 대한 후보값(vj)은, 수학식 1과 같이 정해진다.

수학식 1

[0044]
$$v_j = 2^{m(j-1)}$$

[0045] 여기서, m은 투표자가 n명인 경우, $2^m > n$ 을 만족하는 최소의 정수이다.

[0046] 이하, 도 6 내지 도 8을 참조하여 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 투표 모듈(40)을 통해 각 투표자들이 투표를 수행하는 과정을 구체적으로 설명한다.

[0047] 상기 투표 모듈(40)은 등록된 투표자들이 선택하는 후보에 대하여 투표를 수행하기 위해 개인 투표키 x_i를 이용하여 입력 인자값(x, y, c, $a_{1,2,\ldots,k-1,k}$, $b_{1,2,\ldots,k-1,k}$, $c_{1,2,\ldots,k-1,k}$, $r_{1,2,\ldots,k-1,k}$)으로 1-out-of-k 비대화형 영지식 증명을 실행하는 지시 사항을 트랜잭션으로 생성하고 블록체인 내 스마트 컨트랙트에 기록하는 과정으로 1-out-of-k 비대화형 영지식 증명은 다음과 같이 진행된다. 이때 1-out-of-k 비대화형 영지식 증명은 2가지를 증명하는 방식으로 먼저 투표자가 알고 있는 비밀 투표키가 참이라는 것을 검증자에게 증명할 때 해당 사실 외의 다른 어떤 것도 드러내지 않는다. 또한 동시에 k개의 후보자에 대하여 선택한 후보자를 드러내지 않고 k개 중 하나를 선택했다는 사실을 증명하게 된다.

[0048] 도 6은 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 투표 모듈(40)을 통해 각 투표자들이 투표를 수행하는 과정을 순차적으로 도시한 순서도이며, 도 7은 투표자들이 투표를 수행하기 위하여 1-out-of-k 비대화형 영지식 증명을 수행할 때의 투표자측의 증명 과정을 도시한 순서도이며, 도 8은 투표자들이 투표를 수행하기 위하여 1-out-of-k 비대화형 영지식 증명을 수행할 때의 검증자측의 증명 과정을 도시한 순서도이다.

[0049] 도 6을 참조하면, 먼저, 투표자는 소수 p를 생성한 후 $q|(p-1)$를 만족하는 소수 q를 선택한다. 그리고 Prime-order q의 곱셈 순환군(Multiplicative cyclic groups)을 G이라 하고, G의 생성원을 g, h 라고 한다.

이로써 초기값인 (p, q, g, h)가 생성된다(단계 600).

[0050] 투표자는 개인 투표키 x_i로 $(x,y)=(g^{x_i}, h^{x_i} \cdot g^{v_i})$를 생성하는데(단계 610), 이때 y를 생성하는데 들어간 v_j는 투표자가 선택한 후보자의 후보값이 된다. 개인 투표키 x_i를 이용하여 입력 인자값(x, y, c, $a_{1,2,\ldots,k-1,k}$, $b_{1,2,\ldots,k-1,k}$, $c_{1,2,\ldots,k-1,k}$, $r_{1,2,\ldots,k-1,k}$)을 구하고, 상기 입력 인자값으로 1-out-of-k 비대화형 영지식 증명을 실행하는 지시 사항을 트랜잭션으로 생성한다(단계 620). 다음, 검증자에게 보낼 값들을 1-out-of-k 비대화형 영지식 증명 함수의 입력 인자값으로 트랜잭션에 추가한다(단계 630).

[0051] 여기서, 상기 입력 인자값(x, y, c, $a_{1,2,\ldots,k-1,k}$, $b_{1,2,\ldots,k-1,k}$, $c_{1,2,\ldots,k-1,k}$, $r_{1,2,\ldots,k-1,k}$)은 도 7에 도시된 바와 같이, x 및 y는 $(x,y)=(g^{x_i}, h^{x_i} \cdot g)$ 에 따라 계산되고, a 및 b는 자신이 선택한 투표자에 따라, 선택한 투표자의 경우

[0052] $a_1 = g^w$, $b_1 = h^w$ 가 되며, 그외 다른 경우는 각각 $a_i = g^{r_i} x^{c_i}$, $b_i = h^{r_i} y^{c_i}$ 이며, 이때 r과 c는 Zq에 속해있는 투표자 값을 의미한다.

[0053] $a_{1,2,\ldots,k-1,k}$, $b_{1,2,\ldots,k-1,k}$ 은 투표자가 투표한 값에 따라 투표의 비밀성을 유지하기 위한 진짜 투표값과 가짜 투표값들의 집합을 나타내며 c는 자신이 투표한 후보자의 값과 앞선 투표값들의 집합을 해시 함수를 통해 해싱한 값이며, $c_{1,2,\ldots,k-1,k}$, $r_{1,2,\ldots,k-1,k}$은 자신이 한 투표가 유효함을 입증하기 위해 c값을 통해 생성되는 값이다.

[0054] 다음, 해당 트랜잭션을 자신의 개인키로 서명한 후 블록체인 네트워크에 전파하고(단계 640), 작업증명(POW) 과정을 거쳐 해당 트랜잭션을 블록으로 구성한 후 블록체인에 다시 전파하고(단계 642), 이를 수신한 모든 노드들에 의해 블록의 유효성을 검증받고(단계 644), 일정 개수 이상의 노드들이 해당 블록에 대해 승인하면 블록 체인에 마지막 블록으로 연결하여 저장 및 공유하게 된다(단계 646).

[0055] 한편, 스마트 컨트랙트의 1-out-of-k 비대화형 영지식 증명 함수의 입력 인자값을 수신한 스마트 컨트랙트는, 1-out-of-k 비대화형 영지식 증명 함수를 실행하여 검증자로서 검증을 진행하게 된다(단계 670). 따라서 투표자는 개인 투표키 x_i와 x를 이용하여 첫 번째 증명을, y를 이용하여 두 번째 증명을 진행하게 된다. 또한 k명의 후보자가 있을 때 실제 투표자가 선택한 후보자의 후보값에 대해서만 진짜 증명을 수행하고, 나머지 (k-1)명의 후보자에 대해서는 투표자가 값 형식에 맞춰 임의로 만든 값을 검증자에게 넘겨줌으로써 검증할 수 있도록 한다. 검증자는 k번의 검증을 수행하게 되는데 이 중 어떤 것이 실제 선택한 후보자의 후보값에 대한 검증인지는 모르지만 k번의 검증 중에 하나로 속해 있다고 판단한다.

[0056] 상기 1-out-of-k 비대화형 영지식 증명 함수를 실행한 후 해당 검증 사실과 투표자의 w값을 블록의 형태로 블록체인 내 스마트 컨트랙트에 기록한다(단계 672)

[0057] 이하, 도 9를 참조하여 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 개표 모듈(50)의 동작을 구체적으로 설명한다.

[0058] 도 9는 본 발명의 바람직한 실시예에 따른 전자 투표 시스템에 있어서, 개표 모듈(50)의 동작을 도시한 순서도이다.

[0059] 도 9를 참조하면, 개표 모듈(50)은 투표가 끝난 후 완전 탐색 방식으로 각 투표자에 의해 개표를 진행하게 되는데, 블록체인 내 스마트 컨트랙트에 기록된 1-out-of-k 비대화형 영지식 증명으로 검증받은 모든 투표자의 w값을 호출하여 곱함으로써 시작된다. 곱한 값은 소거법에 의하여 $g^{\Sigma v_i}$이 되는데 이때 v_j는 각 후보자에 대응되는

변수인 후보값으로 여기서는 투표자들이 투표한 모든 후보값을 더한 것이 지수가 된다. 완전 탐색 방식을 적용함으로써 후보자들 중 가장 큰 후보값부터 제수(divisor)로 두고 $g^{\Sigma v_i}$를 피제수(dividend) 두어 나눗셈을 수행한다. 이때 나눠지는 횟수를 해당 후보값에 대응되는 후보자의 투표 수로 집계할 수 있고, 해당 나눗셈 과정을 다음으로 큰 후보값을 제수로 둠으로써 가장 작은 후보값까지 반복 수행한다. 이 결과로 각 후보자에 대한 투표 수를 집계할 수 있다.

[0060] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나, 이는 단지 예시일 뿐 본 발명을 한정하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 그리고, 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0061] 1 : 전자 투표 시스템

10 : 블록체인 네트워크

20 : 블록체인

30 : 투표 프로세스 등록 모듈

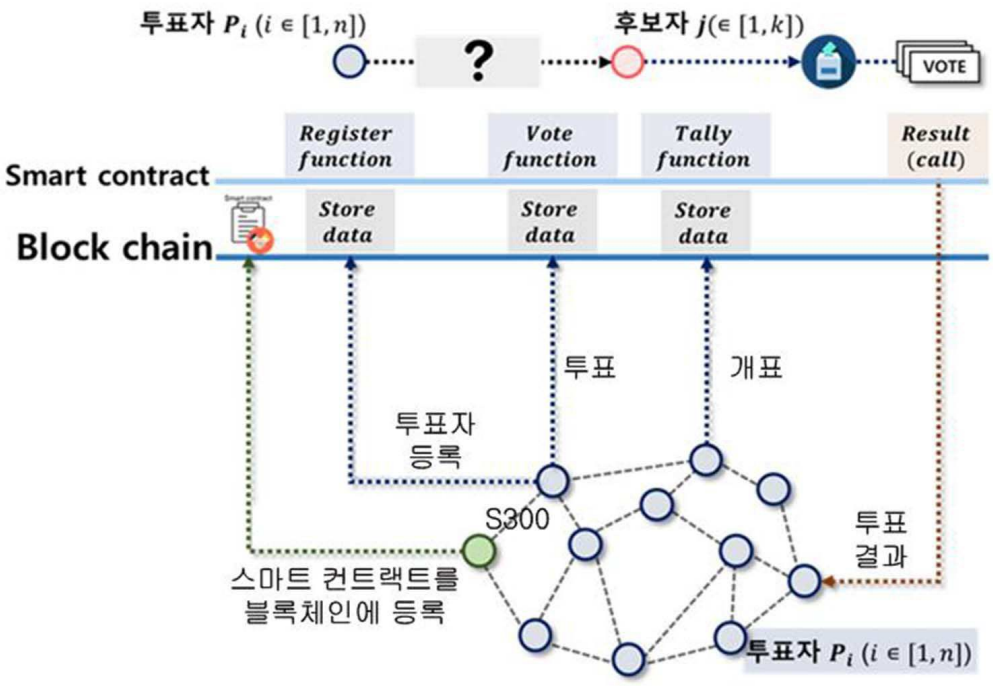
40 : 투표자 등록 모듈

50 : 투표 모듈

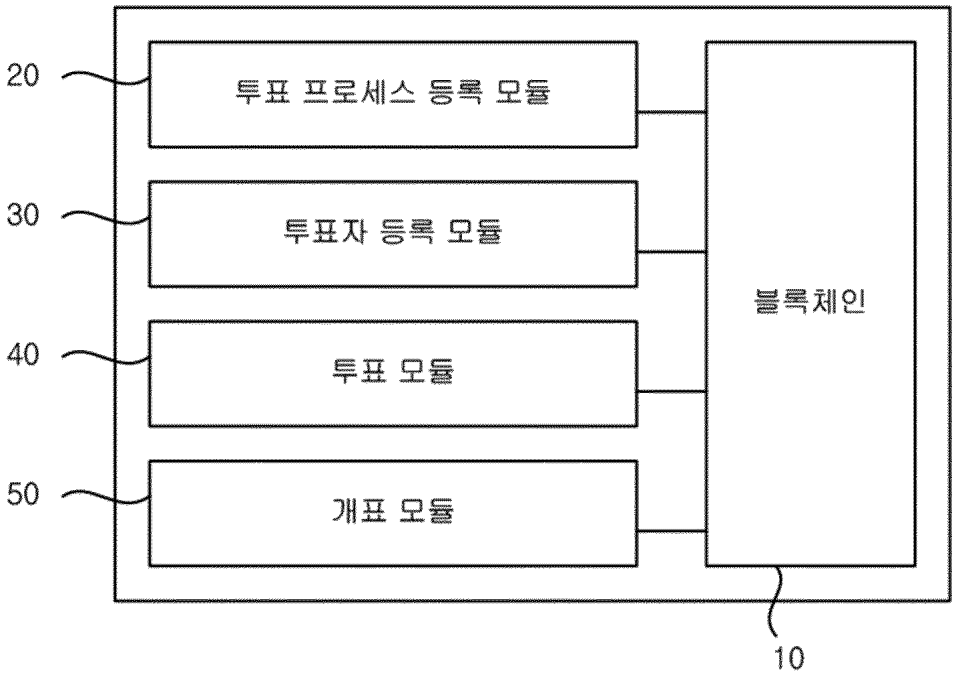
60 : 개표 모듈

도면

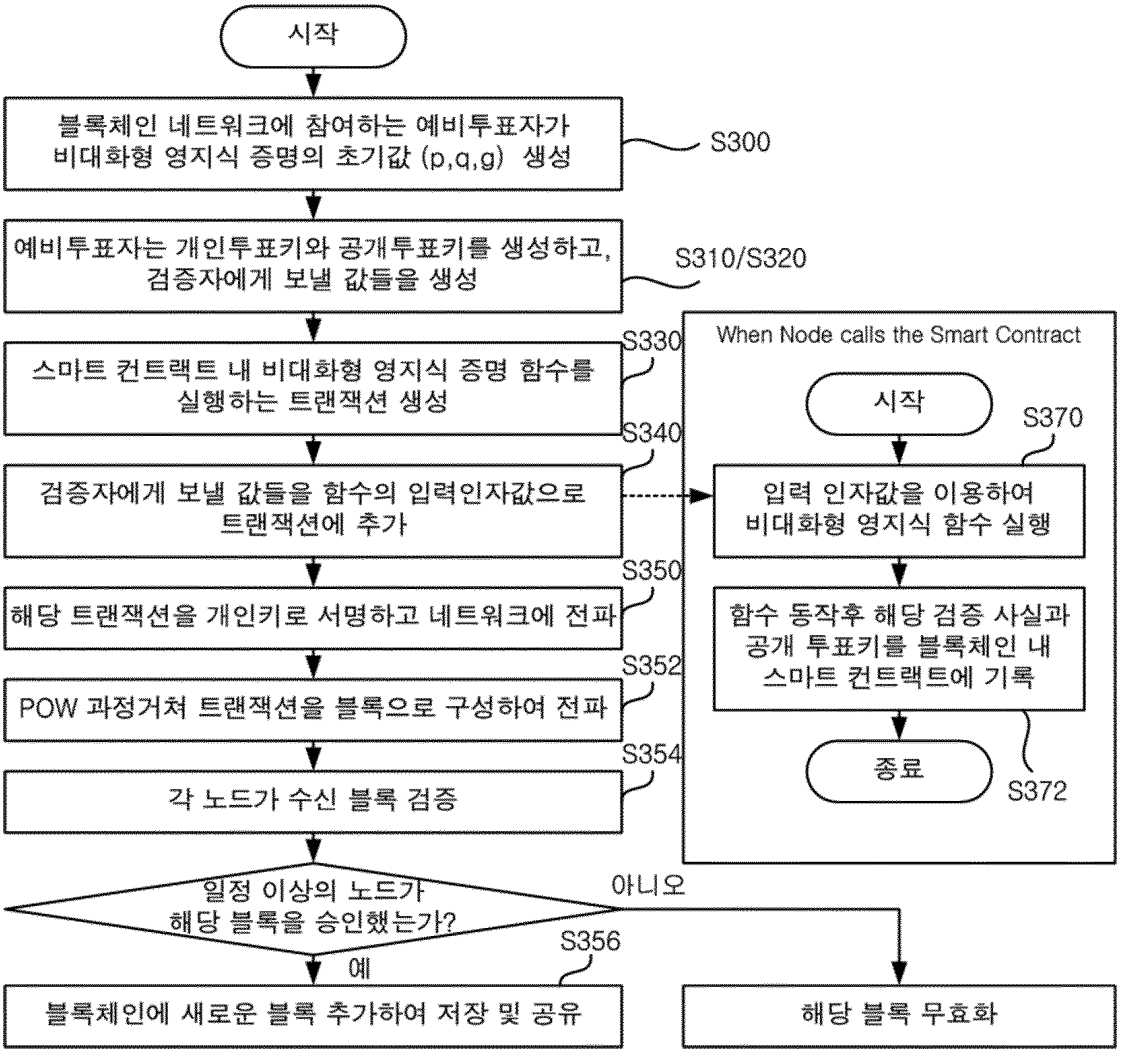
도면1



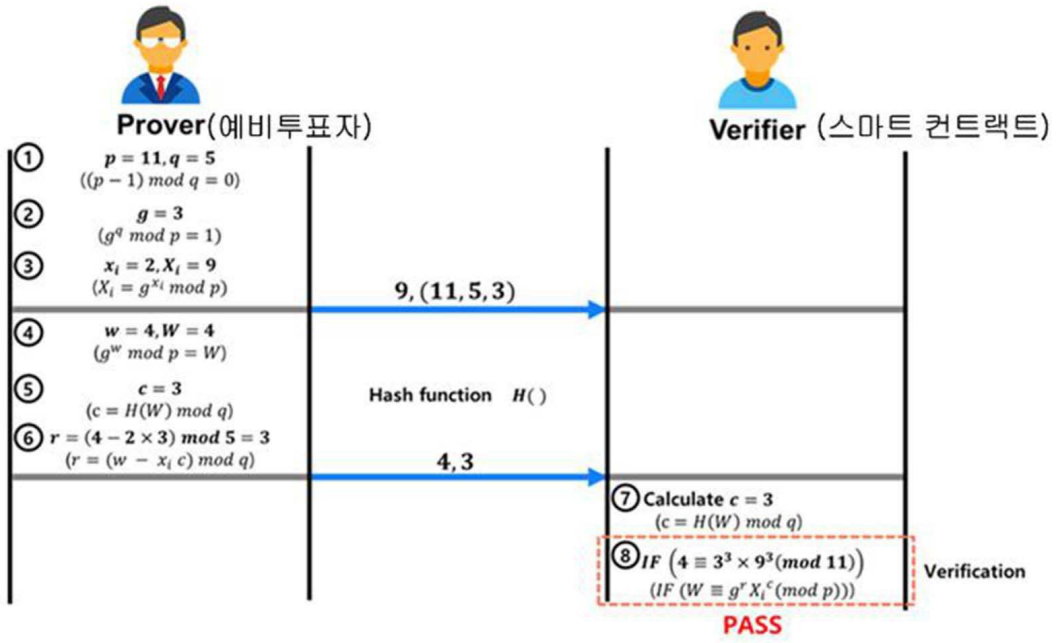
도면2


20
투표 프로세스 등록 모듈
30
투표자 등록 모듈
40
투표 모듈
50
개표 모듈
블록체인
10

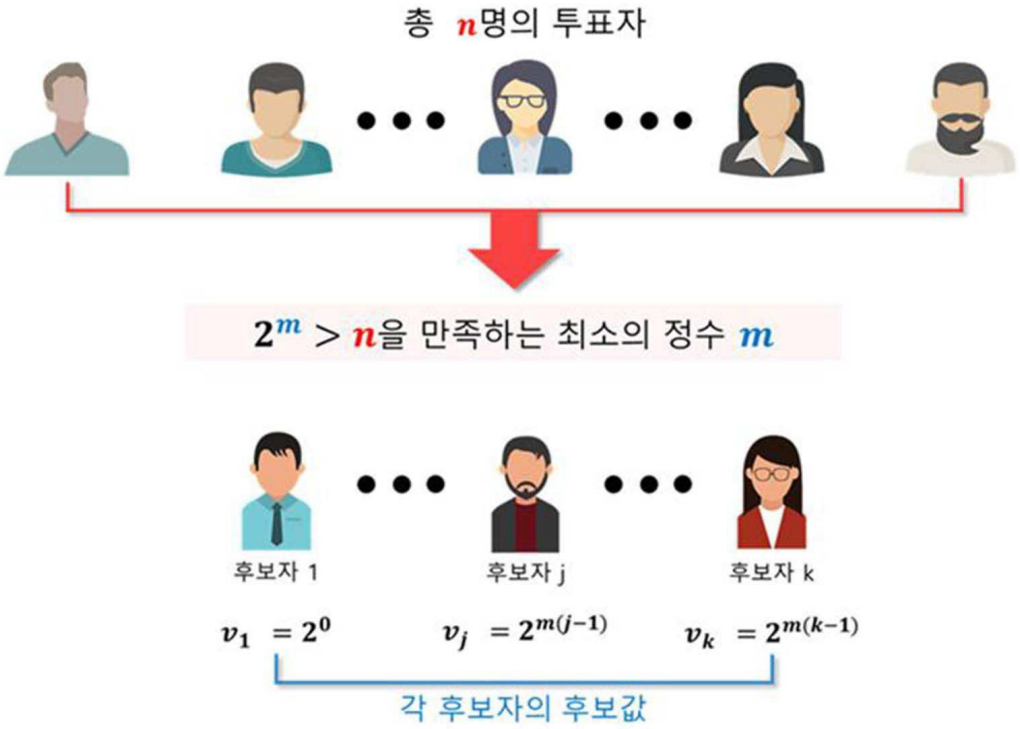
도면3


시작
블록체인 네트워크에 참여하는 예비투표자가 비대화형 영지식 증명의 초기값 (p,q,g) 생성
S300
예비투표자는 개인투표키와 공개투표키를 생성하고, 검증자에게 보낼 값들을 생성
S310/S320
스마트 컨트랙트 내 비대화형 영지식 증명 함수를 실행하는 트랜잭션 생성
S330
검증자에게 보낼 값들을 함수의 입력인자값으로 트랜잭션에 추가
S340
해당 트랜잭션을 개인키로 서명하고 네트워크에 전파
S350
POW 과정거쳐 트랜잭션을 블록으로 구성하여 전파
S352
각 노드가 수신 블록 검증
S354
일정 이상의 노드가 해당 블록을 승인했는가?
아니오
예
S356
블록체인에 새로운 블록 추가하여 저장 및 공유
해당 블록 무효화
When Node calls the Smart Contract
시작
S370
입력 인자값을 이용하여 비대화형 영지식 함수 실행
함수 동작후 해당 검증 사실과 공개 투표키를 블록체인 내 스마트 컨트랙트에 기록
종료
S372

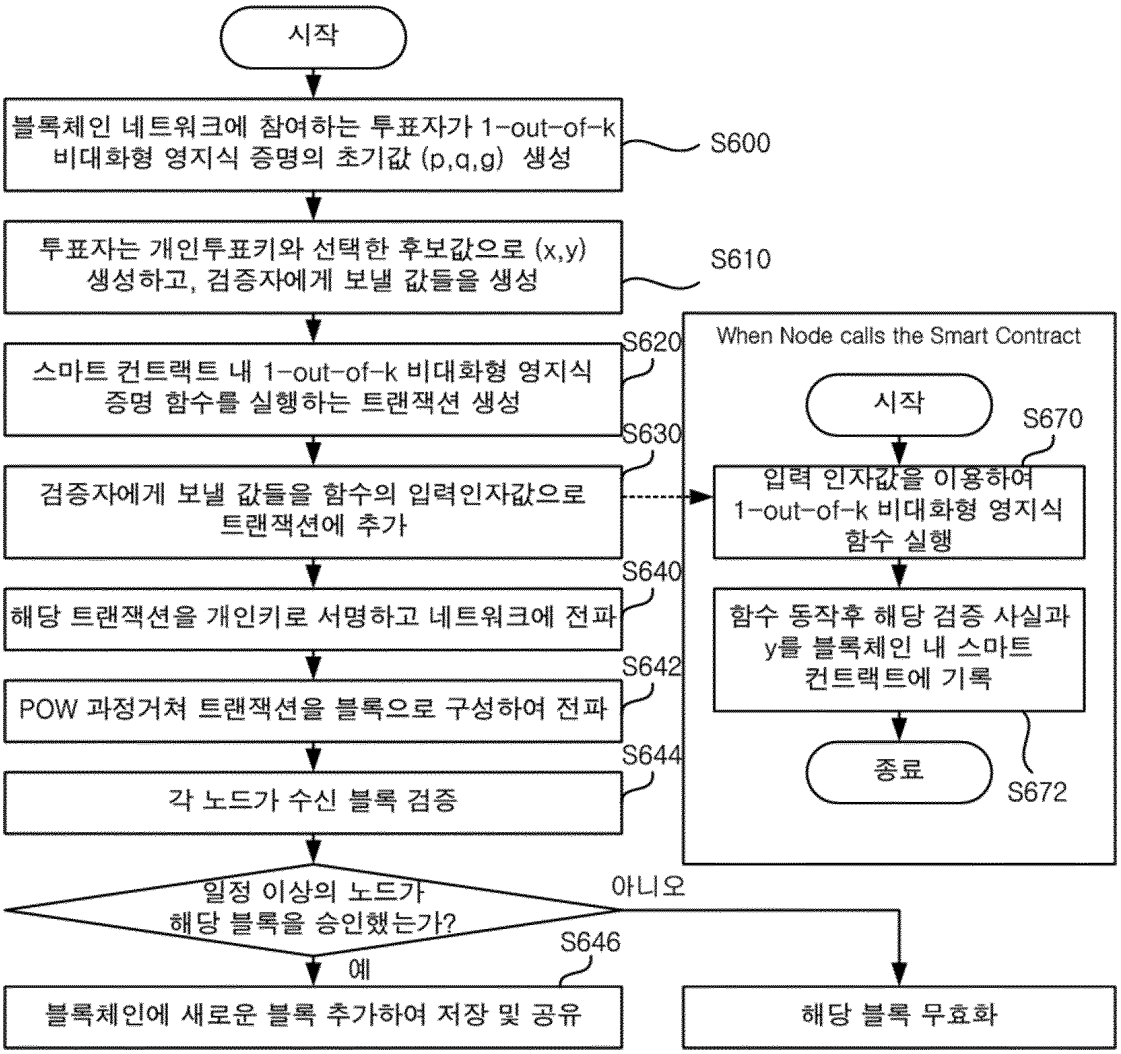
도면4


Prover(예비투표자)
Verifier (스마트 컨트랙트)
① $p = 11, q = 5$ $((p-1) \bmod q = 0)$
② $g = 3$ $(g^q \bmod p = 1)$
③ $x_i = 2, X_i = 9$ $(X_i = g^{x_i} \bmod p)$
9, (11, 5, 3)
④ $w = 4, W = 4$ $(g^w \bmod p = W)$
⑤ $c = 3$ $(c = H(W) \bmod q)$
Hash function $H()$
⑥ $r = (4 - 2 \times 3) \bmod 5 = 3$ $(r = (w - x_i c) \bmod q)$
4, 3
⑦ Calculate $c = 3$ $(c = H(W) \bmod q)$
⑧ $IF\ (4 \equiv 3^3 \times 9^3 (mod\ 11))$ $(IF\ (W \equiv g^r X_i^c (mod\ p)))$
Verification
PASS

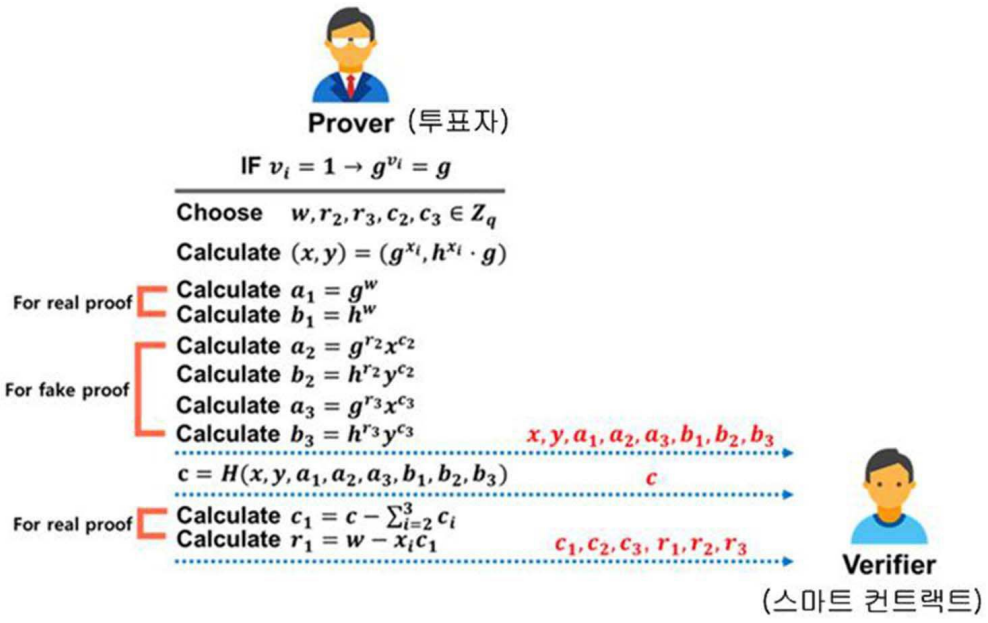
도면5


총 n명의 투표자
$2^m > n$을 만족하는 최소의 정수 m
후보자 1
후보자 j
후보자 k
$v_1 = 2^0$
$v_j = 2^{m(j-1)}$
$v_k = 2^{m(k-1)}$
각 후보자의 후보값

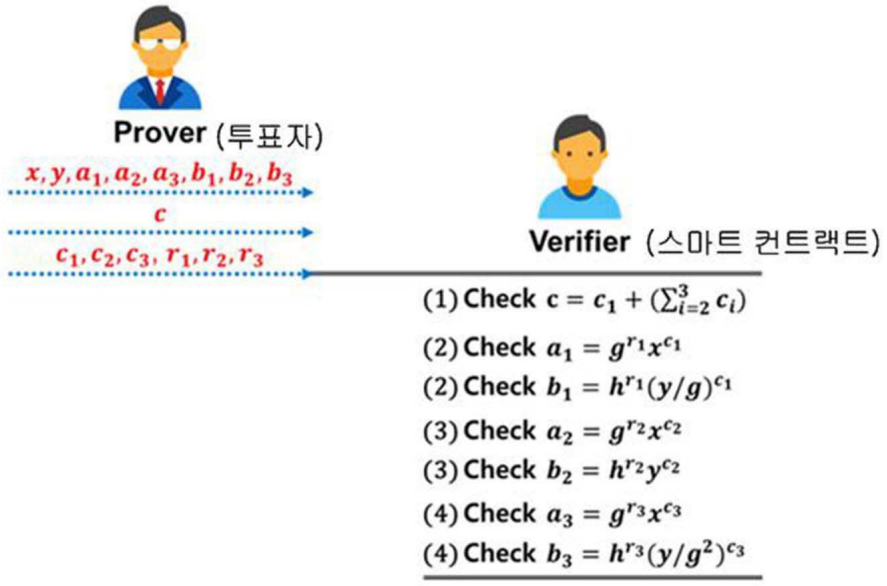
도면6


시작
블록체인 네트워크에 참여하는 투표자가 1-out-of-k 비대화형 영지식 증명의 초기값 (p,q,g) 생성
S600
투표자는 개인투표키와 선택한 후보값으로 (x,y) 생성하고, 검증자에게 보낼 값들을 생성
S610
스마트 컨트랙트 내 1-out-of-k 비대화형 영지식 증명 함수를 실행하는 트랜잭션 생성
S620
검증자에게 보낼 값들을 함수의 입력인자값으로 트랜잭션에 추가
S630
해당 트랜잭션을 개인키로 서명하고 네트워크에 전파
S640
POW 과정거쳐 트랜잭션을 블록으로 구성하여 전파
S642
각 노드가 수신 블록 검증
S644
일정 이상의 노드가 해당 블록을 승인했는가?
아니오
예
S646
블록체인에 새로운 블록 추가하여 저장 및 공유
해당 블록 무효화
When Node calls the Smart Contract
시작
S670
입력 인자값을 이용하여 1-out-of-k 비대화형 영지식 함수 실행
함수 동작후 해당 검증 사실과 y를 블록체인 내 스마트 컨트랙트에 기록
종료
S672

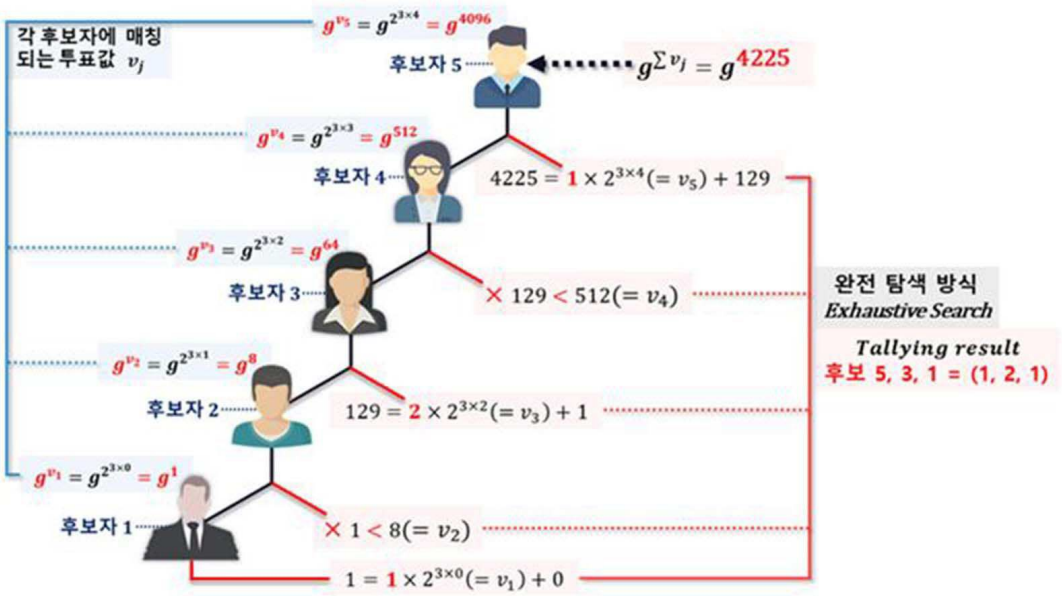
도면7


Prover (투표자)
IF $v_i = 1 \rightarrow g^{v_i} = g$
Choose $w, r_2, r_3, c_2, c_3 \in Z_q$
Calculate $(x, y) = (g^{x_i}, h^{x_i} \cdot g)$
For real proof
Calculate $a_1 = g^w$
Calculate $b_1 = h^w$
For fake proof
Calculate $a_2 = g^{r_2} x^{c_2}$
Calculate $b_2 = h^{r_2} y^{c_2}$
Calculate $a_3 = g^{r_3} x^{c_3}$
Calculate $b_3 = h^{r_3} y^{c_3}$
$x, y, a_1, a_2, a_3, b_1, b_2, b_3$
$c = H(x, y, a_1, a_2, a_3, b_1, b_2, b_3)$
c
For real proof
Calculate $c_1 = c - \sum_{i=2}^{3} c_i$
Calculate $r_1 = w - x_i c_1$
$c_1, c_2, c_3, r_1, r_2, r_3$
Verifier
(스마트 컨트랙트)

도면8


Prover (투표자)
$x, y, a_1, a_2, a_3, b_1, b_2, b_3$
c
$c_1, c_2, c_3, r_1, r_2, r_3$
Verifier (스마트 컨트랙트)
(1) Check $c = c_1 + (\sum_{i=2}^{3} c_i)$
(2) Check $a_1 = g^{r_1} x^{c_1}$
(2) Check $b_1 = h^{r_1} (y/g)^{c_1}$
(3) Check $a_2 = g^{r_2} x^{c_2}$
(3) Check $b_2 = h^{r_2} y^{c_2}$
(4) Check $a_3 = g^{r_3} x^{c_3}$
(4) Check $b_3 = h^{r_3} (y/g^2)^{c_3}$

도면9


각 후보자에 매칭 되는 투표값 v_j
$g^{v_5} = g^{2^{3\times4}} = g^{4096}$
후보자 5
$g^{\sum v_j} = g^{4225}$
$g^{v_4} = g^{2^{3\times3}} = g^{512}$
후보자 4
$4225 = 1 \times 2^{3\times4} (= v_5) + 129$
$g^{v_3} = g^{2^{3\times2}} = g^{64}$
후보자 3
$\times\ 129 < 512 (= v_4)$
$g^{v_2} = g^{2^{3\times1}} = g^{8}$
후보자 2
$129 = 2 \times 2^{3\times2} (= v_3) + 1$
$g^{v_1} = g^{2^{3\times0}} = g^{1}$
후보자 1
$\times\ 1 < 8 (= v_2)$
$1 = 1 \times 2^{3\times0} (= v_1) + 0$
완전 탐색 방식
Exhaustive Search
Tallying result
후보 5, 3, 1 = (1, 2, 1)