관 인 생 략

출 원 번 호 통 지 서

출 원 일 자	2020.12.09
특 기 사 항	심사청구(유) 공개신청(무) 참조번호(P200252KR02)
출 원 번 호	10-2020-0171424 (접수번호 1-1-2020-1335836-16) (DAS접근코드685B)
출원인 명칭	광주과학기술원(3-1998-099381-5)
대리인 성명	김기문(9-2001-000068-8)
발명자 성명	장재혁 이흥노
발명의 명칭	블록체인 전자투표시스템, 그 시스템의 운용방법

특 허 청 장

<< 안내 >>

1. 귀하의 출원은 위와 같이 정상적으로 접수되었으며, 이후의 심사 진행상황은 출원번호를 통해 확인하실 수 있습니다.
2. 출원에 따른 수수료는 접수일로부터 다음날까지 동봉된 납입영수증에 성명, 납부자번호 등을 기재하여 가까운 우체국 또는 은행에 납부하여야 합니다.
※ 납부자번호 : 0131(기관코드) + 접수번호
3. 귀하의 주소, 연락처 등의 변경사항이 있을 경우, 즉시 [특허고객번호 정보변경(경정), 정정신고서]를 제출하여야 출원 이후의 각종 통지서를 정상적으로 받을 수 있습니다.
※ 특허로(patent.go.kr) 접속 > 민원서식다운로드 > 특허법 시행규칙 별지 제5호 서식
4. 특허(실용신안등록)출원은 명세서 또는 도면의 보정이 필요한 경우, 등록결정 이전 또는 의견서 제출기간 이내에 출원서에 최초로 첨부된 명세서 또는 도면에 기재된 사항의 범위 안에서 보정할 수 있습니다.
5. 외국으로 출원하고자 하는 경우 PCT 제도(특허·실용신안)나 마드리드 제도(상표)를 이용할 수 있습니다. 국내출원일을 외국에서 인정받고자 하는 경우에는 국내출원일로부터 일정한 기간 내에 외국에 출원하여야 우선권을 인정받을 수 있습니다.
※ 제도 안내 : http://www.kipo.go.kr-특허마당-PCT/마드리드
※ 우선권 인정기간 : 특허·실용신안은 12개월, 상표·디자인은 6개월 이내
※ 미국특허상표청의 선출원을 기초로 우리나라에 우선권주장출원 시, 선출원이 미공개상태이면, 우선일로부터 16개월 이내에 미국특허상표청에 [전자적교환허가서(PTO/SB/39)를 제출하거나 우리나라에 우선권 증명서류를 제출하여야 합니다.
6. 본 출원사실을 외부에 표시하고자 하는 경우에는 아래와 같이 하여야 하며, 이를 위반할 경우 관련법령에 따라 처벌을 받을 수 있습니다.
※ 특허출원 10-2010-0000000, 상표등록출원 40-2010-0000000
7. 종업원이 직무수행과정에서 개발한 발명을 사용자(기업)가 명확하게 승계하지 않은 경우, 특허법 제62조에 따라 심사단계에서 특허거절결정되거나 특허법 제133조에 따라 등록이후에 특허무효사유가 될 수 있습니다.
8.기타 심사 절차에 관한 사항은 동봉된 안내서를 참조하시기 바랍니다.

9200100006881011101000057050000000

특허출원서

【참조번호】 P200252KR02

【출원구분】 특허출원

【출원인】

【명칭】 광주과학기술원

【특허고객번호】 3-1998-099381-5

【대리인】

【성명】 김기문

【대리인번호】 9-2001-000068-8

【포괄위임등록번호】 2015-044266-2

【발명의 국문명칭】 블록체인 전자투표시스템, 그 시스템의 운용방법

【발명의 영문명칭】 Bolckchain e-voting system and manipulation method

【발명자】

【성명의 국문표기】 장재혁

【성명의 영문표기】 JANG, JE HYUK

【주민등록번호】 890921-1677213

【우편번호】 61005

【주소】 광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원
전기전자컴퓨터공학부

【발명자】

【성명의 국문표기】 이흥노

【성명의 영문표기】 LEE, HEUNG NO

【주민등록번호】 661120-1018916

【우편번호】 61005

【주소】 광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원

전기전자컴퓨터공학부

【출원언어】 국어

【우선권주장】

【출원국명】 KR

【출원번호】 10-2020-0146369

【출원일자】 2020.11.04

【증명서류】 미첨부

【우선권주장】

【출원국명】 US

【출원번호】 63/112,723

【출원일자】 2020.11.12

【증명서류】 우선권증명서류의 전자적 교환에 의한 첨부생략

【접근코드】 7434

【심사청구】 청구

【이 발명을 지원한 국가연구개발사업】

【과제고유번호】 1711116836

【과제번호】 2020-0-00958-001 (NN27150)

【부처명】 과학기술정보통신부

【과제관리(전문)기관명】 정보통신기획평가원

【연구사업명】 융합기술개발

【연구과제명】 일반 연산을 검증하고 트랜잭션 검증량과 저장 공간을 줄여주는 유니버셜 영지식 증명 서킷 기반 가상머신 개발

【기여율】 1/1

【과제수행기관명】 (주)온더

【연구기간】 2020.04.01 ~ 2020.12.31

위와 같이 특허청장에게 제출합니다.

대리인 김기문 (서명 또는 인)

【수수료】

【기본출원료】 0 면 46,000 원

【가산출원료】 30 면 0 원

【우선권주장료】 2 건 36,000 원

【심사청구료】 20 항 1,023,000 원

【합계】 1,105,000 원

【감면사유】 정부출연연구기관(50%감면)[1]

【감면후 수수료】 570,500 원

【발명의 설명】

【발명의 명칭】

블록체인 전자투표시스템, 그 시스템의 운용방법{Bolckchain e-voting system and manipulation method}

【기술분야】

본 발명은 볼록체인을 이용하는 전자투표시스템에 관한 것이다.

일 예로서 본 발명은 검표자가 필요없는 영지식 증명이 가능한 블록체인을 이용하는 전자투표시스템에 관한 것이다.

일 예로서 본 발명은 스마트 컨트렉트에 기반하는 블록체인을 이용하는 전자투표시스템에 관한 것이다.

일 예로서 본 발명은 검표자가 필요없는 영지식 증명이 가능하고 스마트 컨트렉트에 기반하는 투표시스템에 관한 것이다.

【발명의 배경이 되는 기술】

온라인시스템을 이용하는 전자투표시스템은 경제적이며 언제, 어디서든 의사표현을 할 수 있다는 장점이 있다. 그러나 투표의 다양한 기본원칙을 지키기 어렵다는 단점이 있다.

이 배경에서, 블록체인을 이용하는 전자투표시스템 및 그 시스템의 운용방법으로 공개특허번호 10202000008413가 알려져 있다. 상기 특허문헌에 의해서 온라인 투표의 실현 가능성을 제고하였으나, 선거관리 위원회의 신뢰성에 크게 의존하는 문제가 있다. 전자투표의 속성으로 볼 때, 선거관리 위원회의 신뢰성에 의존하는

것은 전자투표의 실제 적용을 어렵게 하는 큰 문제가 된다.

구체적으로, 상기 특허문헌의 투표 시스템은, 선거관리 위원회라는 신뢰받는 제 3 자(trusted third-party)에 의존한다. 예를 들어 선거관리 위원회는 투표자들의 DID들과 각각에 대응되는 투표권 데이터들을 모두 보관한다. 따라서 선거관리 위원회가 타인의 투표권을 사용할 수 있다. 즉, 선거관리 위원회의 조작에 의해서 전자투표의 신뢰성이 손상될 수 있다.

또한, 상기 선거관리 위원회가 컴퓨터 프로그램이고 서버라면, 해커에 의해 모든 기록들이 탈취 될 가능성을 배제할 수 없다.

또한, 선거관리 위원회가 임의로 특정 투표를 누락시킬 수도 있다.

위에서 본 바와 같이, 믿음을 기반으로 운영하는 선거관리 위원회가 타락하면 부정투표가 발생할 수 있다. 특히, 공신력이 없는 비정부, 또는 민간기구에 있어서는 큰 문제이다.

【선행기술문헌】

【특허문헌】

공개번호 1020200008413(2020.01.28) '비밀 선거가 보장된 블록체인 기반의 전자 투표를 수행하는 단말 장치 및 서버와, 전자 투표 방법'

【발명의 내용】

【해결하고자 하는 과제】

본 발명은 상기되는 배경에서 제안되는 것으로서, 선거관리 위원회에 의존하지 않는 블록체인 전자투표시스템, 그 시스템의 운용방법을 제안한다.

【과제의 해결 수단】

본 발명의 블록체인 전자투표시스템에는, 각각의 자기식별 비밀키 및 자기식별 공개키 및 그룹암호화 비밀키 및 그룹암호화 공개키를 가지는 적어도 두 개의 투표노드; 투표노드의 자기식별 데이터와 상기 공개키들을 상기 블록체인으로 업로드하는 관제센터; 상기 투표노드의공개키들과 및 비밀키들과 자기식별 데이터를 입력받아 상기 투표노드를 식별하고 식별번호를 생성하고 투표결과에 대한 그룹암호화를 수행하고 상기 과정의 공정성을 보장하는 영지식증거를 생성하는 제 1 스마트 컨트랙트 모듈; 및 상기 블록체인으로부터 상기 투표결과를 다운로드하여 상기 투표결과를 복호화하지 않고, 투표의 공정성과 집계결과를 확인하는 제 2 스마트 컨트랙트 모듈이 포함된다.

제 1 스마트 컨트랙트 모듈은, 상기 그룹암호화가 수행된 투표결과와 영지식증거들을 블록체인에 업로드할 수 있다.

본 발명의 블록체인 전자투표시스템의 운용방법에는, 상기 투표노드가 자기식별 공개키와 자기식별 비밀키와 그룹암호화 공개키와 그룹암호화 비밀키를 생성하는 것; 상기 투표노드가 자기식별 공개키와 그룹암호화 공개키를 상기 관제센터로 송신하는 것; 상기 관제센터가 블록체인에 상기 투표노드의 자기식별 공개키와 그룹암호화 공개키와 자기식별 데이터를 업로드하는 것; 상기 투표노드가 제 1 스마트 컨트랙트 모듈에 접속하여, 자기가 보유한 자기식별 데이터와 상기 블록체인에 업로드 된 자기식별 데이터를 대조하여 자기를 식별하는 것, 자기식별 공개키를 사용하여 고유한 투표노드 식별번호를 생성하는 것, 자기 식별 과정의 공정성과 투

표노드 식별번호의 고유함을 보장하는 제 1 영지식증거를 생성하는 것, 자기의 의사선택지를 작성하고 그룹암호화를 수행하는 것, 자기의 의사선택지 작성 과정과 그룹암호화 과정의 공정성을 보장하는 제 2 영지식증거를 생성하는 것; 상기 제 1 스마트 컨트랙트 모듈이 투표노드의 제 1 영지식증거와 제 2 영지식증거를 상기 블록체인으로 업로드하는 것, 투표노드의 투표결과를 상기 블록체인으로 업로드하는 것; 제 2 스마트 컨트랙트 모듈이 제 1 영지식증거와 제 2 영지식증거를 검토하는 것, 상기 투표결과들을 종합하여 검표를 수행하는 것이 수행된다.

【발명의 효과】

본 발명에 따르면, 투표의 속성을 지키고, 영지식증명을 지키고, 선거관리위원회 등의 제 3 자의 신뢰성에 의존하지 않는 전자투표를 구현할 수 있다.

【도면의 간단한 설명】

도 1은 실시예에 따른 블록체인 전자투표시스템의 구성도.

도 2는 실시예에 따른 전자투표시스템의 운용방법을 설명하는 흐름도.

도 3은 블록체인으로 업로드되는 투표노드의 업로드 데이터.

【발명을 실시하기 위한 구체적인 내용】

이하에서는 도면을 참조하여 본 발명의 구체적인 실시예를 상세하게 설명한다. 다만, 본 발명의 사상은 이하의 실시예에 제한되지 아니하고, 본 발명의 사상을 이해하는 당업자는 동일한 사상의 범위 내에 포함되는 다른 실시예를 구성요소의 부가, 변경, 삭제, 및 추가 등에 의해서 용이하게 제안할 수 있을 것이나, 이

또한 본 발명 사상의 범위에 포함된다고 할 것이다.

먼저, 본 발명의 실시에의 설명에 사용되는 다양한 기술요소를 정의한다.

<블록체인>

블록체인은 인터넷 피어 투 피어(peer-to-peer) 네트워크상에 존재하는 데이터베이스이다. 블록체인은 서로 연결된 블록들로 구성되고, 각 블록에는 다수의 트랜잭션이 존재한다. 상기 트랜잭션에는 데이터 및 스마트 컨트랙트 중의 적어도 하나가 기록되어 있다. 블록의 외부에는 검증대기 트랜잭션 풀이 존재한다. 상기 검증대기 트랜잭션 풀은 아직 검증받지 못한 트랜잭션들을 보관하는 임시 저장소이다. 블록체인에 기록된 데이터는 위변조가 불가능하다. 블록체인에 기록된 데이터를 읽기 위해 필요한 권한은 없다. 즉, 누구나 접근 가능하다.

사용자가 블록체인에 데이터를 업로드하는 절차는 검증, 출판(방송)의 단계를 거치며 구체적으로 다음과 같다. 먼저, 사용자가 데이터를 트랜잭션의 형태로 변환 후, 이를 검증대기 트랜잭션 풀에 삽입하고, 검증대기 트랜잭션 풀을 공유한다. 다수의 검증자들이 검증대기 트랜잭션 풀의 트랜잭션들을 검증한다. 검증대기 트랜잭션의 검증이 종료되면, 검증자들 간의 합의를 통해 검증대기 트랜잭션을 블록에 출판한다. 사용되는 블록체인이 공적(public) 블록체인인 경우 검증자는 불특정 다수의 채굴자이며, 사적(private) 블록체인인 경우 검증자는 사전에 선별된 블록체인 관리자 일 수 있다.

<영지식 증명>

영지식 증명(zero-knowledge proof)은 증명 프로토콜로써 증명자가 검증자에

게 어떤 명제(statement)가 참임을 납득시키는 프로토콜이다. 이때, 영지식 증명 프로토콜은 검증자에게 그 명제가 참 혹은 거짓이라는 사실 외의 다른 정보는 일절 전달하지 않는 영지식(zero-knowledge) 특성을 가져야 한다.

공개된 정보와 비공개 정보로 구성된 어떤 명제를 S라 할 때, 어떤 증명 프로토콜이 영지식 증명 프로토콜이 되기 위한 필요충분조건, 완전성(completeness). 건실성(soundness), 및 영지식성(zero-knowledge)이다.

영지식 증명 프로토콜은 증명과정과 검증과정의 두 과정으로 구분할 수 있다. 상기 증명과정은 증명자가 명제 S가 참임을 스스로 검증한 후, 그 증거를 생성하는 과정이다. 상기 검증과정은 검증자가 증명자로부터 증거를 받아 증거에 문제가 없는지를 확인하는 과정이다. 만약 증거에 문제가 없다면, 증명자가 명제 S의 자가검증을 잘 수행했다는 사실이 수학적으로 보장되어 있어야 한다.

<투표노드 식별번호>

투표노드가 식별번호를 생성할 때 활용하는 서명 알고리즘을 포함한다. 여기서 상기 투표노드는 상기 투표자가 투표를 행하도록 하는 자원을 예로 들 수 있다.

상기 서명 알고리즘의 예는 RSA(Rivest-Shamir-Adleman) 암호화와 ECDSA(Elliptic Curve Digital Signature Algorithm) 암호화가 있을 수 있다. 그 외의 다른 방법도 적용될 수 있다.

실시예에서는 RSA를 활용한 서명 알고리즘을 사용할 수 있다. 구체적으로 설명한다.

모든 투표노드는, p, 및 q의 자기식별 공개키, s의 자기식별 비밀키를 가지

고 있다. 여기서, 상기 키는 투표노드의 식별번호 생성을 위하여 필요하다. 투표노드의 개인식별 데이터 m을 서명하여 고유 식별번호를 생성하는 과정(sign)은, sing(m,s):=m^smodq 로 정의할 수 있다. 상기 p, q, 및 s는 임의의 두 소수(prime number)를 이용하여 RSA방식을 따라서 제공될 수 있다.

어떤 식별번호 M이 고유함을 검증하는 과정은 verify(M,p,q):=(M^pmodq)^(mmodq)이고, 여기서 ^는 두 피연산자가 같으면 1을 출력하고 다르면 0을 출력하는 연산자이다. 하나의 투표노드에 대하여 하나의 자기식별 공개키만이 블록체인에 업로드되어 있기 때문에, 상기 검증과정은 투표노드 식별번호의 고유함을 증명할 수 있다.

<그룹암호화>

그룹암호화는 투표내용의 암호화 및 검표에 사용된다. 상기 그룹 암호화는 투표 내용을 복호화하지 않고도 투표결과의 집합계산이 가능하도록 하는 암호화이다. 실시예의 그룹암호화는 소정의 예에 지나지 않고 다른 방안도 가능하다.

실시예에서의 그룹암호화의 과정을 설명한다.

먼저, 모든 투표노드는 두 개의 그룹암호화 공개키와 하나의 그룹암호화 비밀키를 가질 수 있다. 여기서, 상기 키는 그룹암호화에 필요하다. 상기 투표노드들 중 i번째 투표노드는 그룹암호화 비밀키로서 임의의 정수인 sk_i를 가질 수 있다. i번째 투표노드는 상기 비밀키를 이용하여 하나의 그룹암호화 공개키(예를 들어, $pk_i:=g^{ski}$)를 제공할 수 있다. 여기서, g는 투표를 행하는 투표노드들의 그룹 G의 암호화 베이스이고, 모든 투표노드에게 공개되는 정보이다. 그룹 G는 N개의 투표노드

들로 구성된 그룹이다. 상기 암호화 베이스 g는 정수이다. 상기 암호화 베이스는 관제센터로부터 제공될 수 있다.

모든 투표노드의 상기 공개키를 이용하여, 다른 하나의 그룹암호화 공개키(yk_i)를 제공할 수 있다. 수학식 1을 이용하여 i번째 투표노드의 다른 하나의 공개키 yk_i를 제공할 수 있다.

【수학식 1】

$$yk_i := \frac{\prod_{j=i+1}^{N} pk_j}{\prod_{j=1}^{i-1} pk_j}$$

여기서, yk_i는 i번째 투표노드의 다른 하나의 공개키이고, pk_i는 i번째 투표노드의 하나의 공개키이고, N은 그룹 G에 속한 투표노드의 수이다.

상기 G그룹의 그룹암호화(ENC)는 수학식 2로 주어질 수 있다.

【수학식 2】

$$ENC_{G(i)} := (yk_i)^{sk_i} \, g^{m_i}$$

여기서 m_i는 G그룹의 i번째 투표노드가 신고자 하는 메시지, 즉 의사선택 내용이다.

검표는 수학식 3으로 수행될 수 있다.

【수학식 3】

$$G\text{의 구성원 } i=1,\cdots,m \text{에 대해, } \prod_{i=1}^{N} ENC_{G(i)}(m_i) = g^{\sum_{i=1}^{N} m_i}$$

여기서, $ENC_{G(i)}$는 G그룹의 i번째 투표노드의 암호화메시지이다.

상기 그룹암호화를 예를 들어 설명한다. 3명으로 구성된 어떤 투표자 그룹이 있다. i는 1에서 3까지이다. 각각의 투표노드는 그룹암호화를 위하여, 두 개의 공개키와 하나의 비밀키를 공유한다. 상기 암호화베이스는 3으로 예를 든다.

각각의 그룹원의 공개키와 비밀키를 각각,

비밀키 $sk_1 = 7$,

공개키 $pk_1 := g^{sk_1} = 3^7 = 2187$, $sk_2 = 5$,

$pk_2 := g^{sk_2} = 3^5 = 243$, 및

비밀키 $sk_3 = 4$,

공개키 $pk_3 := g^{sk_3} = 3^4 = 81$ 로 할 수 있다.

위와 같이 각 그룹원의 비밀키와 공개키가 정해지면, 상기 수학식 1을 이용하여, 각 그룹원의 그룹공개키(yk_i)를 생성할 수 있다.

각 그룹원의 그룹공개키는, 각각, $yk_1 = pk_2 \cdot pk_3 = 3^5 \cdot 3^4 = 3^9$,

$yk_2 = \frac{pk_3}{pk_1} = \frac{3^4}{3^7} = 3^{-3}$, 및 $yk_3 = \frac{1}{pk_1 \cdot pk_2} = \frac{1}{3^7 3^5} = 3^{-12}$ 가 될 수 있다.

각 그룹원의 투표는 어떤 의사결정으로서 5점 만점의 점수를 투표하고, 집계결과 후 만점은 15점으로 한다. 각 그룹원은 예를 들어, m_1은 2점, m_2는 4점, 및 m_3

는 1점으로 투표하였다.

i번째 그룹원의 그룹암호화(ENC)는 상기 수학식 2로 수행될 수 있다.

수학식 2로 수행되는 각 그룹원의 그룹암호화결과는,

1번째 그룹원의 의사결정 암호화 $ENC_{G(1)} = (yk_1)^{sk_1} g^{m_1} = (3^9)^7 3^2 = 3^{65}$

2번째 그룹원의 의사결정 암호화 $ENC_{G(2)} = (yk_2)^{sk_2} g^{m_2} = (3^{-3})^5 3^4 = 3^{-11}$

3번째 그룹원의 의사결정 암호화 $ENC_{G(3)} = (yk_3)^{sk_3} g^{m_3} = (3^{-12})^4 3^1 = 3^{-47}$

로 주어질 수 있다.

검표(또는 집계)는 수학식 3으로 주어질 수 있다. 수학식 3을 이용하여 각 그룹원의 검표를 수행하면,

집계:
$$\prod_{i=1}^{3} ENC_{G(i)} = ENC_{G(1)} \cdot ENC_{G(2)} \cdot ENC_{G(3)} = 3^{65} \cdot 3^{-11} \cdot 3^{-47} = 3^7.$$

로 집계됨을 알 수 있다.

결국, 집계결과는 3^7이며 밑을 3(암호화베이스)으로 하는 이산 log를 취하면 7이 계산된다. 이 결과에 따르면, 집계 과정에서 그룹암호화의 결과를 복호화하지 않기 때문에 각 투표노드의 의사가 무엇인지 알 수 없다. 그에 불구하고 그룹전체의 투표결과를 알 수 있다.

실시예에서 적용하는 그룹암호화는 다른 방법을 사용할 수 있는 것은 물론이다.

<스마트 컨트랙트>

스마트 컨트랙트는 프로그램의 형태로 제공될 수 있다. 입력을 받아 정해진 연산을 수행한 후 출력물을 새로운 트랜잭션에 기록하고 업로드할 수 있다. 스마트 컨트랙트가 지원하는 연산은 튜링완전(turing-complete) 언어가 지원하는 모든 연산을 포함하며, 영지식증명 프로토콜에 사용되는 연산을 포함한다. 상기 스마트 컨트랙트가 수행되는 자원을 스마트 컨트랙트 모듈이라고 할 수 있다. 상기 스마트 컨트랙트는 관제센터가 제공할 수 있다.

실시예에서 상기 스마트 컨트랙트 모듈에는 투표를 실행하는 제 1 스마트 컨트랙트 모듈, 및 검표를 실행하는 제 2 스마트 컨트랙트 모듈이 포함될 수 있다.

도 1은 실시예에 따른 블록체인 전자투표시스템의 구성도이다.

도 1을 참조하면, 상기 관제센터(2)는 그룹 G의 상기 암호와 베이스(g)를 각 투표노드에게 제공할 수 있다(원문자 1). 상기 관제센터(2)는 각 투표노드(1)의 공개키를 입수하고(원문자 2), 관제선터가 보유하고 있는 각 투표노드(1)의 식별정보(DID:Digital ID, 홍채, 및 지문 등의 정보일 수 있다)와 함께 블록체인(3)에 업로드할 수 있다(원문자 3). 상기 관제센터(2)는 상기 스마트 컨트랙트를 블록체인(3)에 업로드할 수 있다(원문자 3).

상기 제 1 스마트 컨트랙트 모듈(41)은 모든 투표노드의 정보를 다운로드한다(원문자 4). 상기 제 1 스마트 컨트랙트 모듈(41)은 각각의 투표노드와 접속하여, 각 투표자에 대한 해당투표자식별($voteID_i$), 해당투표자식별의 영지식 증명($proof\_voteID_i$), 및 투표내용수록을 수행할 수 있다. 상기 제 1 스마트 컨트랙트 모듈(41)은, 그룹공개키(yki) 생성, 그룹암호화 수행($ENC_{G(i)}(vote_i)$), 및 그룹암호

화의 영지식 증명(proof_voteENCi)을 수행할 수 있다.

상기 투표노드(1)는 상기 스마트 컨트랙트 모듈(41)에 접속한다. 상기 투표노드(1)는, 스마트 컨트랙트로, 투표노드 자신이 보유하고 있는 DID, 서명을 위한 공개키와 비밀키, 그룹암호화를 위한 공개키와 비밀키를 업로드한다(원문자 5).

상기 제 1 스마트 컨트랙트 모듈(41)은 투표결과를 블록체인(3)으로 업로드 한다(원문자 6). i번째 투표노드의 투표결과($ballot_i$)에는, 투표자식별정보($voteID_i$), 해당투표자의 영지식 증명($proof\_voteID_i$), 투표실행시각(time_publish), 그룹공개키(yki) 생성, 그룹암호화정보($ENC_{G(i)}(vote_i)$), 및 그룹암호화의 영지식 증명(proof_voteENCi)을 업로드 한다. 상기 그룹암호화정보에는 그룹공개키가 적용되어 있다. 상기 그룹암호화정보는 상기 투표노드의 의사선택지가 수록될 수 있다.

투표가 종료된 뒤에는, 검표를 수행할 수 있다. 상기 제 2 스마트 컨트랙트 모듈(42)에 의해서 검표가 수행될 수 있다. 상기 제 2 스마트 컨트랙트 모듈(42)은 상기 관제센터(2)로부터 검토를 위한 비밀키(s0)를 입수한다. 상기 제 2 스마트 컨트랙트 모듈(42)은 블록체인의 수록정보를 이용하여 검토를 수행할 수 있다.

상기 제 2 스마트 컨트랙트 모듈은 동일한 식별번호가 표기된 두 개의 입력이 있으면 가장 최신의 투표결과(balloti)만을 인정한다. 이를 통하여 어느 투표노드가 두 번의 투표를 하였을 때 최신 정보를 이용함으로서, 투표노드가 최후로 표명한 진정한 의사를 파악할 수 있다.

상기 제 2 스마트 컨트랙트 모듈(42)은 메시지를 복호하지 않고 투표결과를

알 수 있다. 이에 대해서는 상기 그룹암호화를 통하여 상세하게 설명한 바가 있다.

도 1 및 관련 기술요소를 참조하여 실시예에 따른 블록체인 전자투표시스템의 운용방법을 설명한다.

도 2는 실시예에 따른 전자투표시스템의 운용방법을 설명하는 흐름도이다.

실시예의 운용방법은 신뢰받는 검표자가 필요하지 않다. 실시예의 운용방법은, 투표의 특성이 제 3 자의 신뢰성에 의존하지 않는다. 실시예의 운용방법은 투표를 주최하는 관제센터와 투표에 참여하는 투표노드가 있다. 관제센터는 검표에 사용되는 자신만의 비밀 키(s0)를 보유할 수 있다. 투표란 관제센터가 사전에 정의한 안건과 그에 관한 의사선택지를 바탕으로 투표노드들의 의사를 묻고 결과를 종합하는 절차일 수 있다. 투표노드는, 한 개의 의사에 다수의 표를 줄 수 있다. 한 명의 투표자가 투표할 수 있는 표의 수는 최대 S_{max}개로 제한될 수 있다. 투표자의 수는 N명이며, 투표자 명단은 투표가 시행되기 이전에 정해질 수 있다. 주최자는 투표가 시행되기 이전부터 모든 투표자의 개인 인증 데이터를 보유할 수 있다. 주최자가 보유중인 투표자의 개인 인증 데이터를 S-DIDi라 칭할 수 있다. 본인인증 데이터의 예는 홍채 이미지, 지문 이미지, 증명사진 이미지, 음성 데이터, 및 공인인증 데이터 중의 적어도 하나가 될 수 있으며, 이에 제한되지 않는다. N명의 투표자에 대해, 투표자의 개인 인증 데이터를 DIDi라 칭할 수 있다. 실시예의 운용방법은 투표노드가 모든 투표과정의 공정성에 대한 자가 검증을 수행한 후에 그 영지식 증거를 블록체인에 업로드할 수 있다.

먼저, 상기 관제센터(2)는 상기 암호와 베이스(g)를 각 투표노드에게 제공할

수 있다(S1). 상기 투표노드(1)는 서명을 위한 공개키(pi, qi) 및 비밀키(si)를 생성할 수 있다. 상기 투표노드(1)는 상기 암호화 베이스(g)를 이용하여, 그룹암호화를 위한 공개키(pki) 및 비밀키(ski)를 생성할 수 있다. 상기 투표노드는 공개키를 상기 관제센터로 송신할 수 있다(S2).

상기 관제센터(2)는 블록체인(3)에 각 투표노드의 데이터를 도 3과 같이 업로드할 수 있다(S3). 상기 블록체인(3)으로 업로드되는 다른 데이터도, 내용은 다르지만 마찬가지로 구조로 업로드될 수 있다.

상기 관제센터(2)는 스마트 컨트랙트를 업로드할 수 있다(S3). 상기 스마트 컨트랙트에는 투표를 위한 컨트랙트와 검토를 위한 컨트랙트가 포함될 수 있다. 상기 투표노드의 데이터에는, 상기 관제센터가 미리 보유하고 있는 각 투표노드(1)의 식별정보(DID:Digital ID)를 업로드할 수 있다.

상기 제 1 스마트 컨트랙트 모듈(41)에 의해서 투표가 수행될 수 있다. 상기 표노드는 상기 제 1 스마트 컨트랙트 모듈(41)를 이용하여 투표할 수 있다.

상기 제 1 스마트 컨트랙트 모듈(41)은 각각의 투표노드와 접속하여, 각각의 투표노드를 식별하여 고유 식별번호를 생성하는 것, 각각의 투표노드의 의사선택지를 작성하는 과정이 수행될 수 있다(S4). 상기 식별번호 생성 및 의사선택지의 작성에는 영지식 증명이 수행될 수 있다.

더 구체적으로, 각 투표노드의 식별정보를 비교하여 투표노드를 확인하는 것(Cert), 각 투표자에 대한 해당투표노드의 식별(voteIDi), 해당투표노드의 영지식 증명(proof_voteID), 및 투표내용수록(x입력)을 수행할 수 있다.

여기서, 상기 투표내용수록에는 마지막은 하나의 필드(L+1)를 추가할 수 있다. 상기 추가 필드가 영이 아니면 추후에 기권표로 취급할 수 있다. 이를 통하여 상기 투표노드는 기권표를 투표할 수도 있다.

이후에 각 필드값의 합이 최대값(Smax)를 넘지 않는지를 판단할 수 있다. 상기 각 필드값의 합이 상기 최대값을 넘으면 이상이 있는 것으로서 무효처리할 수 있다.

이후에, 상기 그룹공개키를 생성(yki), 상기 그룹공개키를 이용하여 그룹암호화를 수행(ENC), 및 상기 그룹암호화의 영지식 증명(proof_voteENC)을 수행할 수 있다.

이후에, 마지막으로 투표노드를 확인하는 것(Cert), 해당투표노드의 영지식 증명(proof_voteID), 및 상기 그룹암호화의 영지식 증명(proof_voteENC)의 어느 하나라도 영이 발생하면 에러로 취급하여 다시 할 수 투표를 진행할 수 있다.

정상적으로 투표가 종료되면, 개인식별정보(DIDi), 비밀키(si, ski)를 삭제한다.

투표가 종료하면, 상기 제 1 스마트 컨트랙트 모듈(41)은, 블록체인(3)으로 소정의 정보를 업로드한다(S5). 업로드되는 정보에는, 투표자식별정보(voteIDi), 해당투표자의 영지식 증명(proof_voteID), 투표실행시각(time_publish), 그룹공개키(yki) 생성, 그룹암호화정보($ENC_{G(i)}$(votei)), 및 그룹암호화의 영지식 증명(proof_voteENCi)이 포함될 수 있다.

상기 투표과정(S4), 및 투표결과가 업로드되는 과정(S5)은, 상기 제 1 스마

트 컨트랙트 모듈에 의해서 수행되는 것으로서, 상세한 내용은 수학식 4를 참조할 수 있다.

【수학식 4】

INPUTS: DID_i, p_i, q_i, s_i, $\mathbf{vote}_i = (x_{i,1}, \cdots x_{i,L+1})$, pk_i, sk_i

INITIALIZATION: $voteID_i = null$ and $isvalid = 0$

PROCESS:

1. Download $\mathbf{voter}_i = (hash(S\_DID_i), pk_i, p_i, q_i)$ for all i from blockchain.
2. $Cert = hash(DID_i) \wedge hash(S\_DID_i)$.
3. If $Cert = 1$, do
   A. $voteID_i = sign(hash(DID_i), s_i)$
   B. $proof\_voteID_i = ZKP(\text{process2}, verify(voteID_i, p_i, q_i))$
   C. If $x_{i,L+1} \neq 0$, do $x_{i,1} = 0, x_{i,2} = 0, \cdots, x_{i,L} = 0$
   D. If $\sum_{l=1}^{L} x_{i,l} \leq S_{\max}$, do $isvalid = 1$
   E. $yk_i = \left(\prod_{j=i+1}^{N} pk_j\right) \Big/ \left(\prod_{j=1}^{i-1} pk_j\right)$
   F. $ENC_{G(i)}(\mathbf{vote}_i) = (yk_i)^{sk_i} g^{\mathbf{vote}_i}$
   G. $proof\_voteENC_i = ZKP\left(\text{process3-C}, \text{process3-D}, DEC_{G(i)}\left(ENC_{G(i)}(\mathbf{vote}_i)\right)\right)$
4. If $Cert = 0$ or $ZKP\_verify(proof\_voteID_i) = 0$ or $ZKP\_verify(proof\_voteENC_i) = 0$, then return an error message.
5. Delete $\mathbf{vote}_i$, DID_i, s_i, sk_i

OUTPUT: Upload $voteID_i, ENC_{G(i)}(\mathbf{vote}_i), proof\_voteID_i, proof\_voteENC_i$ to blockchain

수학식 4에서 ZKP(연산)는 입력 연산의 연산 과정의 공정성을 보장하는 영지식증거를 생성하는 함수이다.

수학식 4에서 ZKP_verify(증거)는 입력 영지식증거의 타당성을 검증하는 함수이다.

모든 투표노드의 투표가 종료된 뒤에는, 검표를 수행할 수 있다.

상기 제 2 스마트 컨트랙트 모듈(42)에 의해서 검표가 수행될 수 있다. 상기 제 2 스마트 컨트랙트 모듈(42)은 상기 관제센터(2)로부터 검토를 위한 비밀키(s0)와 블록체인의 수록정보를 입수할 수 있다(S6).

상기 제 2 스마트 컨트랙트 모듈(42)은, 자신이 가진 비밀키(s0)와 입수한 비밀키가 서로 다른 경우에는, 검표를 거부할 수 있다.

상기 제 2 스마트 컨트랙트 모듈(42)은, 블록체인으로 정보를 입수하여 수록된 정보를 알아낼 수 있다. 이때 상기 정보는 블록체인의 각 블록의 정보를 연결하여 단일의 정보를 생성하는 것을 의미할 수 있다. 이때 상기 정보는 암호화된 그룹암호화 정보를 개별적으로 복호화하는 것을 의미하지 않을 수 있다.

상기 제 2 스마트 컨트랙트 모듈(42)은 상기 의사 선택지의 복호화가 없이 의사 선택지의 집계결과를 알아낼 수 있다(S7). 상기 그룹암호화에 의해서 상기 작용이 수행되는 것은 이미 살펴본 바와 같다.

상기 제 2 스마트 컨트랙트 모듈(42)은, 해당투표노드의 영지식 증명(proof_voteIDi)의 검증(ZKP_verify(proof_voteIDi)), 및 상기 그룹암호화의 영지식 증명(proof_voteENCi)의 검증(ZKP_verify(proof_voteENCi))을 수행할 수 있다.

상기 제 2 스마트 컨트랙트 모듈은 동일한 투표자에 대하여 두 개의 입력이 있으면 가장 최신의 투표결과(balloti)를 이용한다. 이를 통하여 어느 투표노드가 두 번의 투표를 하였을 때 최선정보를 이용함으로서, 투표노드의 진정한 의사를 파악할 수 있다.

이후에, 상기 제 2 스마트 컨트랙트 모듈(42)은 집계결과를 블록체인(3)에 업로드할 수 있다(S8)

투표시스템이 가져야 하는 투표의 특성은 다음과 같다.

정확성: 모든 정당한 유효투표는 투표결과에 정확히 집계.

확인성: 투표결과 위조방지를 위한 투표결과 검증수단이 필요.

완전성: 부정 투표자에 의한 방해 차단하고 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.

본 발명의 시스템 및 운용방법이 상기 각 특성을 지키는 것을 설명한다.

먼저, 상기 정확성을 담보하는 요인을 다음과 같이 예시할 수 있다.

투표자가 투표 스마트 컨트랙트를 이용하여 투표의 유효성을 자가검증할 수 있다. 투표의 유효성 자가검증을 수행한 증거를 생성할 수 있다. 불특정 다수의 블록체인 검증자(채굴자)에 의해 투표의 유효성 증거를 검증받을 수 있다. 검표 스마트 컨트랙트 모듈이 투표의 유효성 증거를 한 번 더 검증할 수 있다. 검증받은 증거와 암호화된 투표내용은 함께 블록체인에 기록되어 불변할 수 있다. 모든 투표는 검표 스마트컨트랙트에 의해 일괄적으로 집계할 수 있다.

상기 확인성을 담보하는 요인을 다음과 같이 예시할 수 있다.

투표내용이 투표대상자에 의해 작성되었다는 증거가 암호화된 투표데이터와

함께 블록체인에 기록되어 불변할 수 있다. 투표데이터가 조작될 경우 증거의 검증이 불가능하므로 무효표로 처리할 수 있다. 누구나 투표데이터와 증거를 검증한 후 집계 결과를 재생산 할 수 있다.

상기 완전성을 담보하는 요인을 다음과 같이 예시할 수 있다.

모든 투표자는 투표내용을 작성 후 합법한 투표임을 자가검증하고 그 증거를 블록체인에 기록할 수 있다. 투표내용이 부정할 경우 증거가 검증 불가능할 수 있다. 검증 불가능한 증거와 함께 기록된 투표내용은 무효처리할 수 있다.

상기 단일성을 담보하는 요인을 다음과 같이 예시할 수 있다.

모든 투표자는 개인인증을 자가수행한 후 그 증거를 투표내용과 함께 블록체인에 기록할 수 있다. 개인인증 증거가 검증 불가능할 경우 함께 기록된 투표내용은 무효처리할 수 있다.

상기 합법성을 담보하는 요인을 다음과 같이 예시할 수 있다.

투표자별로 고유의 의사 선택지 식별번호가 있다. 의사 선택지 식별번호는 투표자의 비밀 키를 사용하여 생성하며, 사전에 등록된 투표자의 공개 키를 사용하여 검증 가능해야 할 수 있다. 한 명의 투표자는 한 개의 공개키만을 사전 등록하므로, 한 명의 투표자는 하나의 식별번호만을 생성할 수 있다. 투표자는 자신의 공개 키를 사용하여 식별번호의 유효성을 자가 검증하고, 그 증거를 생성한 후, 식별번호와 함께 블록체인에 기록할 수 있다. 식별번호의 유효성에 관한 증거가 검증 불가능한 경우, 함께 기록된 투표는 무효처리할 수 있다.

상기 기밀성을 담보하는 요인을 다음과 같이 예시할 수 있다.

투표자가 의사 선택 식별번호를 자신의 비밀 키를 이용하여 직접 생성할 수 있다. 투표자는 의사 선택 식별번호만을 블록체인에 기록하므로, 비밀 키를 모르는 제 3 자는 투표자와 식별번호 간의 관계를 유추할 수 없다. 투표내용은 암호화되어 공개되고, 검표 및 개표시에도 그 내용이 복호화되지 않으므로, 제 3 자가 식별번호와 투표내용간의 관계를 유추할 수 없다.

상기 공정성을 담보하는 요인을 다음과 같이 예시할 수 있다.

모든 투표내용은 암호화되어 업로드 될 수 있다. 검표 및 개표를 포함한 투표 전 과정을 통틀어 투표내용이 복호화되지 않을 수 있다. 그룹암호화에 의해 모든 투표가 완료되지 않으면 투표 내용의 집계가 불가능할 수 있다.

상기되는 내용에 따르면 본 발명 투표시스템 및 그 운용방법의 장점이 이해될 수 있다.

【산업상 이용가능성】

본 발명에 따르면 영지식 증명을 지키고, 제 3 자의 신뢰도에 영향을 받지 않는 상태로 전자투표시스템을 운영할 수 있다.

【부호의 설명】

1: 투표노드

2: 관제센서

3: 블록체인

41, 42: 스마트 컨트랙트 모듈

【청구범위】

【청구항 1】

각각의 비밀키 및 공개키를 가지는 적어도 두 개의 투표노드;

암호화 베이스를 상기 투표노드로 제공하는 관제센터;

상기 투표노드가 상기 암호화 베이스를 이용하여 생성한 그룹암호화를 위한 공개키 및 비밀키를 입력받아 상기 투표노드의 투표에 대한 그룹암호화를 수행하고,

상기 그룹암호화가 수행된 투표결과를 블록체인에 업로드하도록,

스마트 컨트랙트가 수행되는 제 1 스마트 컨트랙트 모듈; 및

상기 블록체인으로부터 상기 투표결과를 다운로드하여 상기 투표결과를 복호화하지 않고, 투표의 집계결과를 확인하는 제 2 스마트 컨트랙트 모듈이 포함되는 블록체인 전자투표시스템.

【청구항 2】

제 1 항에 있어서,

상기 관제센터는, 상기 투표노드의 제 1 개인식별정보를 미리 수록하여 상기 블록체인으로 업로드하고,

상기 투표노드는, 자신이 가지는 제 2 개인식별정보를 상기 제 1 스마트 컨트랙트 모듈로 업로드하여,

상기 제 1 스마트 컨트랙트 모듈은, 상기 제 1, 2 개인식별정보를 비교하여 투표노드를 확인하는 블록체인 전자투표시스템.

【청구항 3】

제 1 항에 있어서,

상기 관제센터가, 검표를 위한 비밀키를 상기 제 2 스마트 컨트랙트 모듈로 제공하는 블록체인 전자투표시스템.

【청구항 4】

제 1 항에 있어서,

상기 제 1 스마트 컨트랙트 모듈은, 상기 투표노드에 대한 투표노드식별(voteIDi), 및 투표노드식별에 대한 영지식 증명(proof_voteID)을 수행하는 블록체인 전자투표시스템.

【청구항 5】

제 1 항에 있어서,

상기 제 1 스마트 컨트랙트 모듈은, 상기 그룹암호화의 영지식 증명(proof_voteENCi)을 수행하는 블록체인 전자투표시스템.

【청구항 6】

제 1 항에 있어서,

상기 스마트 컨트랙트는 상기 관제센터가 블록체인을 통하여 공급하는 블록체인 전자투표시스템.

【청구항 7】

제 1 항에 있어서,

상기 제 1 스마트 컨트랙트 모듈은, 투표노드식별정보(voteIDi), 투표노드식별정보의 영지식 증명(proof_voteID), 투표실행시각(time_publish), 그룹암호화정

보($ENC_{G(i)}$(votei)), 및 그룹암호화 정보의 영지식 증명(proof_voteENCi)을 상기 블록체인으로 업로드하는 블록체인 전자투표시스템.

【청구항 8】

제 1 항에 있어서,

상기 제 2 스마트 컨트랙트 모듈은, 상기 집계결과를 상기 블록체인에 업로드하는 블록체인 전자투표시스템.

【청구항 9】

제 1 항에 있어서,

상기 제 2 스마트 컨트랙트 모듈은 상기 집계결과는 상기 블록체인에 업로드하는 블록체인 전자투표시스템.

【청구항 10】

관제센터가 같은 암호와 베이스를 적어도 두 개의 투표노드 각각에게 제공하는 것;

상기 투표노드가 상기 암호화 베이스를 이용하여, 그룹암호화를 위한 공개키(pki) 및 비밀키(ski)를 생성하는 것;

상기 투표노드가 공개키를 상기 관제센터로 송신하는 것;

상기 관제센터가 블록체인에 상기 투표노드의 데이터를 업로드하는 것;

상기 투표노드가 제 1 스마트 컨트랙트 모듈에 접속하여, 자기를 식별하여 서명하는 것, 자기의 의사선택지를 작성하고 그룹암호화를 수행하는 것;

상기 제 1 스마트 컨트랙트 모듈이 투표결과를 상기 블록체인으로 업로드하

는 것;

제 2 스마트 컨트랙트 모듈이 검표를 수행하는 것이 수행되는 블록체인 전자투표시스템의 운용방법.

【청구항 11】

제 10 항에 있어서,

상기 투표노드가 서명을 위한 공개키(pi, qi) 및 비밀키(si)를 생성하여, 상기 관제센터 및 상기 제 1 스마트 컨트랙트 모듈로 전송하는 블록체인 전자투표시스템의 운용방법.

【청구항 12】

제 10 항에 있어서,

상기 제 1, 2 스마트 컨트랙트 모듈의 스마트 컨트랙트는, 상기 관제센터가 상기 블록체인에 업로드하는 블록체인 전자투표시스템의 운용방법.

【청구항 13】

제 10 항에 있어서,

상기 투표노드의 데이터에는, 상기 관제센터가 미리 보유하고 있는 각 투표노드의 식별정보가 포함되고,

상기 투표노드는, 상기 제 1 스마트 컨트랙트 모듈에게 자신이 식별정보를 전송하여,

상기 제 1 스마트 컨트랙트 모듈은, 두 개의 식별정보를 비교하여 투표노드를 확인하는 것이 수행되는, 블록체인 전자투표시스템의 운용방법.

【청구항 14】

제 10 항에 있어서,

상기 투표노드가 상기 제 1 스마트 컨트랙트 모듈에 접속하여, 상기 서명의 작업에 대한 영지식증명 및 상기 의사선택지의 작업에 대한 영지식 증명이 더 수행되는, 블록체인 전자투표시스템의 운용방법.

【청구항 15】

제 10 항에 있어서,

상기 의사선택지에는, 기권표를 식별하는 하나의 필드가 더 추가되는 블록체인 전자투표시스템의 운용방법.

【청구항 16】

제 10 항에 있어서,

투표의 종료 후에, 상기 개인식별정보(DIDi), 비밀키(si, ski)는 삭제되는 블록체인 전자투표시스템의 운용방법.

【청구항 17】

제 10 항에 있어서,

상기 제 1 스마트 컨트랙트 모듈이 상기 블록체인으로 업로드하는 정보에는, 투표실행시각(time_publish)이 포함되는 블록체인 전자투표시스템의 운용방법.

【청구항 18】

제 10 항에 있어서,

상기 제 2 스마트 컨트랙트 모듈은 상기 관제센터로부터 검표를 위한 비밀키

(s0)를 입수하는 블록체인 전자투표시스템의 운용방법.

【청구항 19】

제 10 항에 있어서,

상기 제 2 스마트 컨트랙트 모듈은, 해당투표노드의 영지식 증명(proof_voteIDi)의 검증(ZKP_verify(proof_voteIDi)), 및 상기 그룹암호화의 영지식 증명(proof_voteENCi)의 검증(ZKP_verify(proof_voteENCi))을 수행하는 블록체인 전자투표시스템의 운용방법.

【청구항 20】

제 10 항에 있어서,

상기 제 2 스마트 컨트랙트 검표결과를 상기 블록체인이 업로드하는 블록체인 전자투표시스템의 운용방법.

【요약서】

【요약】

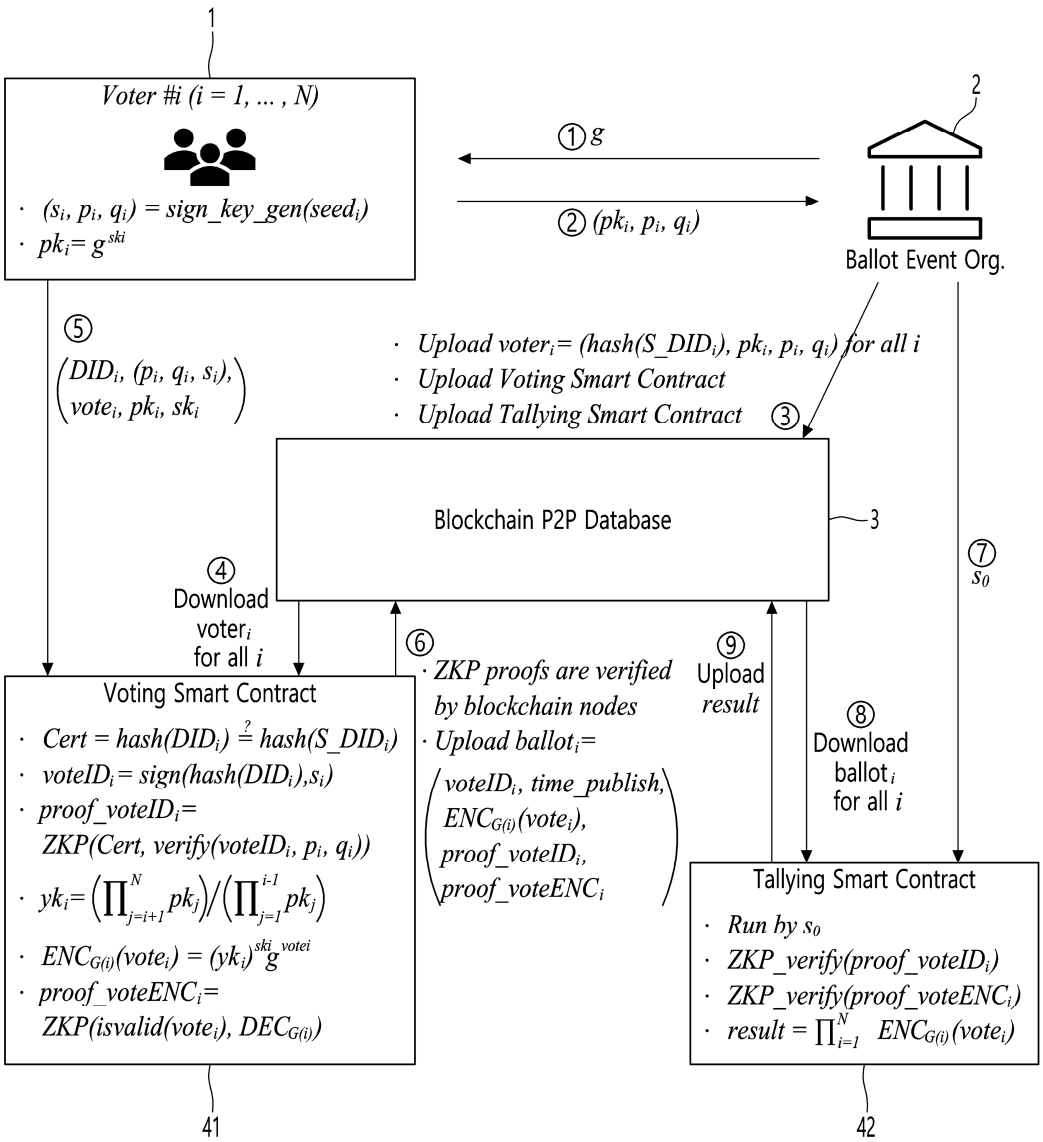
본 발명의 블록체인 전자투표시스템에는, 각각의 비밀키 및 공개키를 가지는 적어도 두 개의 투표노드; 투표노드의 식별정보를 블록체인으로 업로드하는 관제센터; 상기 투표노드의 공개키들과 비밀키들과 자가식별 데이터를 입력받아 상기 투표노드를 식별하고 식별번호를 생성하고 투표결과에 대한 그룹암호화를 수행하고 상기 과정의 공정성을 보장하는 영지식증거를 생성하는 제 1 스마트 컨트랙트 모듈; 및 상기 블록체인으로부터 상기 투표결과를 다운로드하여 상기 투표결과를 복호화하지 않고, 투표의 공정성과 집계결과를 확인하는 제 2 스마트 컨트랙트 모듈이 포함된다.

【대표도】

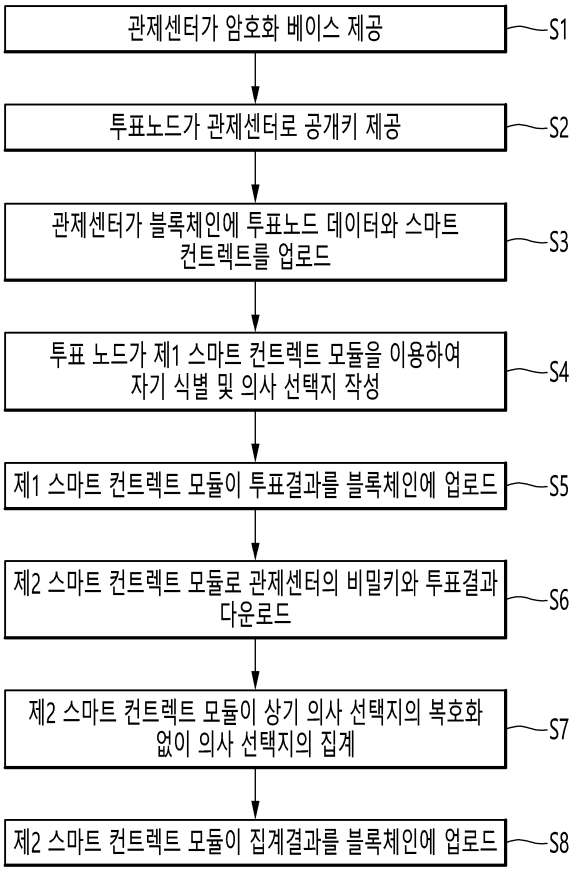
도 1

【도면】

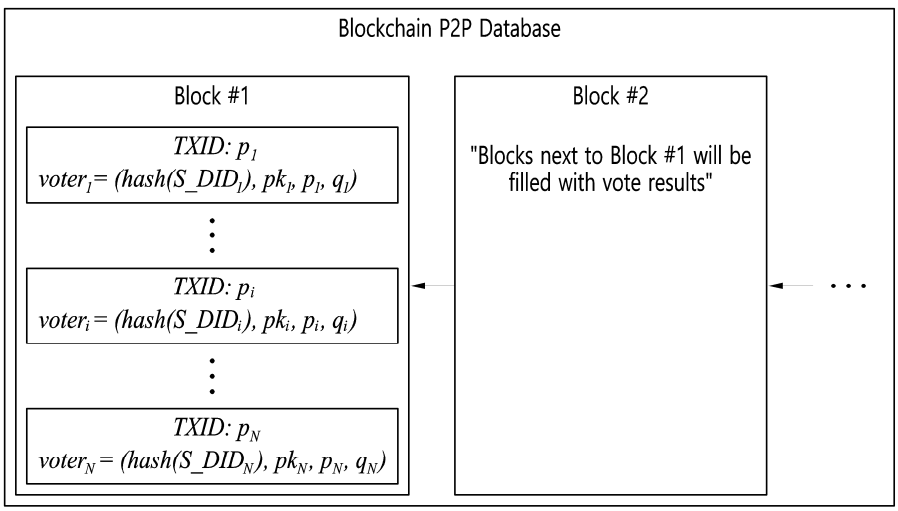
【도 1】


1
Voter #i (i = 1, ... , N)
· $(s_i, p_i, q_i) = sign\_key\_gen(seed_i)$
· $pk_i = g^{ski}$
① g
② (pk_i, p_i, q_i)
2
Ballot Event Org.
⑤
$(DID_i, (p_i, q_i, s_i), vote_i, pk_i, sk_i)$
· Upload $voter_i = (hash(S\_DID_i), pk_i, p_i, q_i)$ for all i
· Upload Voting Smart Contract
· Upload Tallying Smart Contract
③
Blockchain P2P Database
3
④ Download $voter_i$ for all i
⑥
· ZKP proofs are verified by blockchain nodes
· Upload $ballot_i$ = $(voteID_i, time\_publish, ENC_{G(i)}(vote_i), proof\_voteID_i, proof\_voteENC_i)$
⑦ s_0
⑨ Upload result
⑧ Download $ballot_i$ for all i
Voting Smart Contract
· $Cert = hash(DID_i) \stackrel{?}{=} hash(S\_DID_i)$
· $voteID_i = sign(hash(DID_i), s_i)$
· $proof\_voteID_i = ZKP(Cert, verify(voteID_i, p_i, q_i))$
· $yk_i = \left(\prod_{j=i+1}^{N} pk_j\right) / \left(\prod_{j=1}^{i-1} pk_j\right)$
· $ENC_{G(i)}(vote_i) = (yk_i)^{ski} g^{votei}$
· $proof\_voteENC_i = ZKP(isvalid(vote_i), DEC_{G(i)})$
41
Tallying Smart Contract
· Run by s_0
· $ZKP\_verify(proof\_voteID_i)$
· $ZKP\_verify(proof\_voteENC_i)$
· $result = \prod_{i=1}^{N} ENC_{G(i)}(vote_i)$
42

【도 2】


관제센터가 암호화 베이스 제공
S1
투표노드가 관제센터로 공개키 제공
S2
관제센터가 블록체인에 투표노드 데이터와 스마트 컨트렉트를 업로드
S3
투표 노드가 제1 스마트 컨트렉트 모듈을 이용하여 자기 식별 및 의사 선택지 작성
S4
제1 스마트 컨트렉트 모듈이 투표결과를 블록체인에 업로드
S5
제2 스마트 컨트렉트 모듈로 관제센터의 비밀키와 투표결과 다운로드
S6
제2 스마트 컨트렉트 모듈이 상기 의사 선택지의 복호화 없이 의사 선택지의 집계
S7
제2 스마트 컨트렉트 모듈이 집계결과를 블록체인에 업로드
S8

【도 3】


Blockchain P2P Database
Block #1
TXID: p_1
$voter_1 = (hash(S\_DID_1), pk_1, p_1, q_1)$
TXID: p_i
$voter_i = (hash(S\_DID_i), pk_i, p_i, q_i)$
TXID: p_N
$voter_N = (hash(S\_DID_N), pk_N, p_N, q_N)$
Block #2
"Blocks next to Block #1 will be filled with vote results"