(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년03월27일
(11) 등록번호 10-1962686
(24) 등록일자 2019년03월21일

(51) 국제특허분류(Int. Cl.)
G06Q 50/26 (2012.01) *G07C 13/00* (2006.01)
(52) CPC특허분류
G06Q 50/26 (2013.01)
G07C 13/00 (2013.01)
(21) 출원번호 10-2017-0110274
(22) 출원일자 2017년08월30일
심사청구일자 2017년08월30일
(65) 공개번호 10-2019-0023894
(43) 공개일자 2019년03월08일
(56) 선행기술조사문헌
KR1020090001497 A*
US20160027229 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 송파구 올림픽로 435, 311동 2001호 (신천동,파크리오)
김동인
경기도 안양시 동안구 경수대로 498, 서부인터빌 101동 102호
이신철
대전광역시 유성구 은구비로 31, 508동 2102호
(74) 대리인
두호특허법인

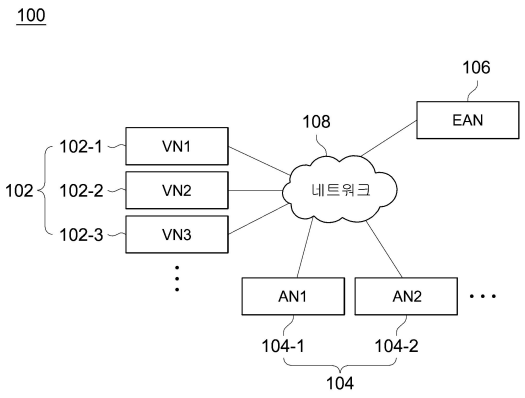
전체 청구항 수 : 총 20 항 심사관 : 최윤겸

(54) 발명의 명칭 **전자 투표 시스템 및 방법**

(57) 요 약

전자 투표 시스템 및 방법이 개시된다. 본 발명의 일 실시예에 따른 전자 투표 시스템은 전자 투표의 투표 결과에 대한 블록 체인을 구성하기 위한 초기 블록을 생성하여 배포하는 선거 관리 노드; 투표자로부터 복수의 후보자 중 어느 하나의 후보자에 대한 선택값을 포함하는 일반 트랜잭션을 생성하는 하나 이상의 투표 노드; 및 상기 하나 이상의 투표 노드로부터 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 집계하여 하나 이상의 블록을 생성하는 하나 이상의 집계 노드를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
G06Q 2230/00 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711058858
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발
연구과제명 (함수암호 3세부) 함수서명 설계기법 및 응용기술 연구
기 여 율 1/1
주관기관 고려대학교산학협력단
연구기간 2017.08.01 ~ 2018.05.31

명 세 서

청구범위

청구항 1

전자 투표의 투표 결과에 대한 블록 체인을 구성하기 위한 초기 블록을 생성하여 배포하는 선거 관리 노드;

투표자로부터 복수의 후보자 중 어느 하나의 후보자에 대한 선택값을 포함하는 일반 트랜잭션을 생성하는 하나 이상의 투표 노드; 및

상기 하나 이상의 투표 노드로부터 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 집계하여 하나 이상의 블록을 생성하는 하나 이상의 집계 노드를 포함하며,

상기 투표 노드 및 상기 집계 노드는 상기 집계 노드에서 생성된 상기 하나 이상의 블록을 검증하고, 검증된 블록을 상기 블록 체인에 연결하며,

상기 집계 노드는,

검증된 일반 트랜잭션을 현재 생성중인 블록에 추가하고, 기 설정된 블록 생성 주기에 도달한 경우, 베이스 트랜잭션을 생성하여 상기 현재 생성중인 블록에 추가하고, 생성된 상기 블록을 타 투표 노드 또는 타 집계 노드로 송신하는, 전자 투표 시스템.

청구항 2

청구항 1에 있어서,

상기 초기 블록은,

상기 전자 투표에 참여한 총 유권자 수, 상기 선거 관리 노드의 서명값, 상기 하나 이상의 집계 노드의 공개키 및 상기 복수의 후보자들 각각의 공개키 해시값을 포함하는, 전자 투표 시스템.

청구항 3

청구항 1에 있어서,

상기 일반 트랜잭션은,

상기 투표자의 PIN 번호, 상기 투표자가 선택한 후보자의 공개키 해시값, 상기 투표자의 개인키 서명값, 및 상기 투표자의 공개키를 포함하는, 전자 투표 시스템.

청구항 4

청구항 3에 있어서,

상기 투표 노드는,

상기 투표자로부터 입력받은 PIN 번호의 유효성을 검증하고, 상기 유효성이 검증된 상기 투표자로부터 후보자 선택값을 입력받아 상기 일반 트랜잭션을 생성하며, 생성된 상기 일반 트랜잭션을 타 투표 노드 또는 상기 집계 노드로 송신하는, 전자 투표 시스템.

청구항 5

청구항 4에 있어서,

상기 투표 노드는,

타 투표 노드로부터 상기 일반 트랜잭션이 수신되는 경우,

수신된 상기 일반 트랜잭션에 포함된 상기 PIN 번호와 중복되는 PIN 번호의 존재 여부, 후보자의 공개키 해시값의 유효 여부, 및 상기 투표자의 개인키 서명값의 유효 여부에 따라 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 타 투표 노드 또는 상기 집계 노드로 송신하는, 전자 투표 시스템.

청구항 6

청구항 5에 있어서,

상기 투표 노드는,

상기 일반 트랜잭션에 대한 검증 결과 중복된 PIN 번호가 존재하거나, 상기 후보자의 공개키 해시값이 유효하지 않거나, 또는 상기 투표자의 개인키 서명값이 유효하지 않을 것으로 판단되는 경우, 수신된 상기 일반 트랜잭션을 폐기하는, 전자 투표 시스템.

청구항 7

청구항 4에 있어서,

상기 집계 노드는,

타 투표 노드로부터 상기 일반 트랜잭션이 수신되는 경우,

수신된 상기 일반 트랜잭션에 포함된 상기 PIN 번호와 중복되는 PIN 번호의 존재 여부, 후보자의 공개키 해시값의 유효 여부, 및 상기 투표자의 개인키 서명값의 유효 여부에 따라 수신된 상기 일반 트랜잭션을 검증하는, 전자 투표 시스템.

청구항 8

삭제

청구항 9

청구항 7에 있어서,

상기 베이스 트랜잭션은,

상기 복수의 후보자들 각각의 공개키 해시값, 및 상기 베이스 트랜잭션이 속한 블록 내에서 집계된 상기 복수의 후보자들 각각의 득표수를 포함하는, 전자 투표 시스템.

청구항 10

청구항 7에 있어서,

상기 블록을 수신한 상기 투표 노드 또는 상기 집계 노드는,

수신된 상기 블록의 베이스 트랜잭션에 기록된 총 투표수와 수신된 상기 블록에 포함된 일반 트랜잭션으로부터 계산된 총 투표수의 일치 여부,

수신된 상기 블록의 베이스 트랜잭션에 기록된 상기 복수의 후보자 각각의 득표수와 수신된 상기 블록에 포함된 일반 트랜잭션으로부터 계산된 각 후보자별 득표수의 일치 여부,

블록 체인에 상기 블록에 포함된 PIN 번호와 중복된 PIN 번호가 존재하는지의 여부, 및

상기 블록에 포함된 머클 루트 해시값의 유효 여부를 판단함으로써 상기 수신된 블록을 검증하고,

검증된 블록에 자신의 서명값을 추가하여 타 투표 노드 또는 타 집계 노드로 송신하는, 전자 투표 시스템.

청구항 11

청구항 10에 있어서,

상기 블록을 수신한 상기 투표 노드 또는 상기 집계 노드는,

상기 검증된 블록에 포함된 서명값의 개수가 기 설정된 값 이상인 경우, 상기 검증된 블록을 상기 블록 체인에 연결하는, 전자 투표 시스템.

청구항 12

선거 관리 노드에서, 전자 투표의 투표 결과에 대한 블록 체인을 구성하기 위한 초기 블록을 생성하여 배포하는 단계;

투표 노드에서, 투표자로부터 복수의 후보자 중 어느 하나의 후보자에 대한 선택값을 포함하는 일반 트랜잭션을 생성하는 단계;

집계 노드에서, 상기 투표 노드로부터 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 집계하여 블록을 생성하는 단계; 및

상기 투표 노드 또는 상기 집계 노드에서, 생성된 상기 블록을 검증하고, 검증된 블록을 상기 블록 체인에 연결하는 단계를 포함하고,

상기 블록 생성 단계는,

검증된 일반 트랜잭션을 현재 생성중인 블록에 추가하는 단계; 및

기 설정된 블록 생성 주기에 도달한 경우, 베이스 트랜잭션을 생성하여 상기 현재 생성중인 블록에 추가하고, 생성된 상기 블록을 타 투표 노드 또는 타 집계 노드로 송신하는 단계를 더 포함하는, 전자 투표 방법.

청구항 13

청구항 12에 있어서,

상기 초기 블록은,

상기 전자 투표에 참여한 총 유권자 수, 상기 선거 관리 노드의 서명값, 상기 하나 이상의 집계 노드의 공개키 및 상기 복수의 후보자들 각각의 공개키 해시값을 포함하는, 전자 투표 방법.

청구항 14

청구항 12에 있어서,

상기 일반 트랜잭션은,

상기 투표자의 PIN 번호, 상기 투표자가 선택한 후보자의 공개키 해시값, 상기 투표자의 개인키 서명값, 및 상기 투표자의 공개키를 포함하는, 전자 투표 방법.

청구항 15

청구항 14에 있어서,

상기 일반 트랜잭션을 생성하는 단계는,

상기 투표자로부터 입력받은 PIN 번호의 유효성을 검증하고, 상기 유효성이 검증된 상기 투표자로부터 후보자 선택값을 입력받아 상기 일반 트랜잭션을 생성하며, 생성된 상기 일반 트랜잭션을 타 투표 노드 또는 상기 집계 노드로 송신하도록 구성되는, 전자 투표 방법.

청구항 16

청구항 15에 있어서,

상기 투표 노드는,

타 투표 노드로부터 상기 일반 트랜잭션이 수신되는 경우,

수신된 상기 일반 트랜잭션에 포함된 상기 PIN 번호와 중복되는 PIN 번호의 존재 여부, 후보자의 공개키 해시값의 유효 여부, 및 상기 투표자의 개인키 서명값의 유효 여부에 따라 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 타 투표 노드 또는 상기 집계 노드로 송신하는, 전자 투표 방법.

청구항 17

청구항 16에 있어서,

상기 투표 노드는,

상기 일반 트랜잭션에 대한 검증 결과 중복된 PIN 번호가 존재하거나, 상기 후보자의 공개키 해시값이 유효하지 않거나, 또는 상기 투표자의 개인키 서명값이 유효하지 않을 것으로 판단되는 경우, 수신된 상기 일반 트랜잭션을 폐기하는, 전자 투표 방법.

청구항 18

청구항 15에 있어서,

상기 블록 생성 단계는,

수신된 상기 일반 트랜잭션에 포함된 상기 PIN 번호와 중복되는 PIN 번호의 존재 여부, 후보자의 공개키 해시값의 유효 여부, 및 상기 투표자의 개인키 서명값의 유효 여부에 따라 수신된 상기 일반 트랜잭션을 검증하도록 구성되는, 전자 투표 방법.

청구항 19

삭제

청구항 20

청구항 18에 있어서,

상기 베이스 트랜잭션은,

상기 복수의 후보자들 각각의 공개키 해시값, 및 상기 베이스 트랜잭션이 속한 블록 내에서 집계된 상기 복수의 후보자들 각각의 득표수를 포함하는, 전자 투표 방법.

청구항 21

청구항 18에 있어서,

상기 블록 검증 및 블록 체인 연결 단계는,

수신된 상기 블록의 베이스 트랜잭션에 기록된 총 투표수와 수신된 상기 블록에 포함된 일반 트랜잭션으로부터 계산된 총 투표수의 일치 여부,

수신된 상기 블록의 베이스 트랜잭션에 기록된 상기 복수의 후보자 각각의 득표수와 수신된 상기 블록에 포함된 일반 트랜잭션으로부터 계산된 각 후보자별 득표수의 일치 여부,

블록 체인에 상기 블록에 포함된 PIN 번호와 중복된 PIN 번호가 존재하는지의 여부, 및

상기 블록에 포함된 머클 루트 해시값의 유효 여부를 판단함으로써 상기 수신된 블록을 검증하고,

검증된 블록에 자신의 서명값을 추가하여 타 투표 노드 또는 타 집계 노드로 송신하도록 구성되는, 전자 투표 방법.

청구항 22

청구항 21에 있어서,

상기 블록 검증 및 블록 체인 연결 단계는,

상기 검증된 블록에 포함된 서명값의 개수가 기 설정된 값 이상인 경우, 상기 검증된 블록을 상기 블록 체인에 연결하도록 구성되는, 전자 투표 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 신뢰성 있는 전자 투표 제공 기술과 관련된다.

배 경 기 술

[0003] 전자 투표란 집단의 구성원들의 의사를 묻는 방식 중 하나인 투표를 전자적인 방식에 의해 실시하는 것을 의미한다. 예를 들어, 대통령 선거를 전자 투표 방식으로 진행할 경우, 유권자들은 투표소에 설치된 투표 단말, 또는 투표 클라이언트가 설치된 개인 단말(개인용 컴퓨터, 또는 스마트폰 등의 이동 단말 등)을 이용하여 대통령 후보로 등록한 후보자들 중 한 명을 선택하게 된다.

[0004] 이러한 전자 투표의 경우 투표를 위한 별도의 투표용지 등을 사용하지 않으므로 기존의 아날로그 투표 방식에 비해 선거 비용을 절감할 수 있으며, 개표가 매우 빠르게 이루어진다는 장점이 있다. 그러나 전자 투표는 악의적인 집단에 의한 투표 결과의 위조, 변조 등의 문제가 있어 기존의 투표 방식을 대체하는 데 한계가 존재하였다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 대한민국 등록특허공보 제10-1167647호 (2012. 07.16)

발명의 내용

해결하려는 과제

[0007] 본 발명의 실시예들은 신뢰성 있는 전자 투표를 구현하기 위한 기술적인 수단을 제공하기 위한 것이다.

과제의 해결 수단

[0009] 예시적인 실시예에 따르면, 전자 투표의 투표 결과에 대한 블록 체인을 구성하기 위한 초기 블록을 생성하여 배포하는 선거 관리 노드; 투표자로부터 복수의 후보자 중 어느 하나의 후보자에 대한 선택값을 포함하는 일반 트랜잭션을 생성하는 하나 이상의 투표 노드; 및 상기 하나 이상의 투표 노드로부터 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 집계하여 하나 이상의 블록을 생성하는 하나 이상의 집계 노드를 포함하며, 상기 투표 노드 및 상기 집계 노드는 상기 집계 노드에서 생성된 상기 하나 이상의 블록을 검증하고, 검증된 블록을 상기 블록 체인에 연결하는, 전자 투표 시스템이 제공된다.

[0010] 상기 초기 블록은, 상기 전자 투표에 참여한 총 유권자 수, 상기 선거 관리 노드의 서명값, 상기 하나 이상의 집계 노드의 공개키 및 상기 복수의 후보자들 각각의 공개키 해시값을 포함할 수 있다.

[0011] 상기 일반 트랜잭션은, 상기 투표자의 PIN 번호, 상기 투표자가 선택한 후보자의 공개키 해시값, 상기 투표자의 개인키 서명값, 및 상기 투표자의 공개키를 포함할 수 있다.

[0012] 상기 투표 노드는, 상기 투표자로부터 입력받은 PIN 번호의 유효성을 검증하고, 상기 유효성이 검증된 상기 투표자로부터 후보자 선택값을 입력받아 상기 일반 트랜잭션을 생성하며, 생성된 상기 일반 트랜잭션을 타 투표 노드 또는 상기 집계 노드로 송신할 수 있다.

[0013] 상기 투표 노드는, 타 투표 노드로부터 상기 일반 트랜잭션이 수신되는 경우, 수신된 상기 일반 트랜잭션에 포함된 상기 PIN 번호와 중복되는 PIN 번호의 존재 여부, 후보자의 공개키 해시값의 유효 여부, 및 상기 투표자의 개인키 서명값의 유효 여부에 따라 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 타 투표 노드 또는 상기 집계 노드로 송신할 수 있다.

[0014] 상기 투표 노드는, 상기 검증 결과 중복된 PIN 번호가 존재하거나, 상기 후보자의 공개키 해시값이 유효하지 않거나, 또는 상기 투표자의 개인키 서명값이 유효하지 않을 것으로 판단되는 경우, 수신된 상기 일반 트랜잭션을 폐기할 수 있다.

[0015] 상기 집계 노드는, 타 투표 노드로부터 상기 일반 트랜잭션이 수신되는 경우, 수신된 상기 일반 트랜잭션에 포함된 상기 PIN 번호와 중복되는 PIN 번호의 존재 여부, 후보자의 공개키 해시값의 유효 여부, 및 상기 투표자의 개인키 서명값의 유효 여부에 따라 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 현재 생성중인 블록에 추가할 수 있다.

[0016] 상기 집계 노드는, 기 설정된 블록 생성 주기에 도달한 경우, 베이스 트랜잭션을 생성하여 상기 현재 생성중인 블록에 추가하고, 생성된 상기 블록을 타 투표 노드 또는 타 집계 노드로 송신할 수 있다.

[0017] 상기 베이스 트랜잭션은, 상기 복수의 후보자들 각각의 공개키 해시값, 및 상기 베이스 트랜잭션이 속한 블록 내에서 집계된 상기 복수의 후보자들 각각의 득표수를 포함할 수 있다.

[0018] 상기 블록을 수신한 상기 투표 노드 또는 상기 집계 노드는, 수신된 상기 블록의 베이스 트랜잭션에 기록된 총 투표수와 수신된 상기 블록에 포함된 일반 트랜잭션으로부터 계산된 총 투표수의 일치 여부, 수신된 상기 블록의 베이스 트랜잭션에 기록된 상기 복수의 후보자 각각의 득표수와 수신된 상기 블록에 포함된 일반 트랜잭션으로부터 계산된 각 후보자별 득표수의 일치 여부, 블록 체인에 상기 블록에 포함된 PIN 번호와 중복된 PIN 번호가 존재하는지의 여부, 및ㅍ상기 블록에 포함된 머클 루트 해시값의 유효 여부를 판단함으로써 상기 수신된 블록을 검증하고,ㅍ검증된 블록에 자신의 서명값을 추가하여 타 투표 노드 또는 타 집계 노드로 송신할 수 있다.

[0019] 상기 블록을 수신한 상기 투표 노드 또는 상기 집계 노드는, 상기 검증된 블록에 포함된 서명값의 개수가 기 설정된 값 이상인 경우, 상기 검증된 블록을 상기 블록 체인에 연결할 수 있다.

[0020] 다른 예시적인 실시예에 따르면, 선거 관리 노드에서, 전자 투표의 투표 결과에 대한 블록 체인을 구성하기 위한 초기 블록을 생성하여 배포하는 단계; 투표 노드에서, 투표자로부터 복수의 후보자 중 어느 하나의 후보자에 대한 선택값을 포함하는 일반 트랜잭션을 생성하는 단계; 집계 노드에서, 상기 투표 노드로부터 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 집계하여 블록을 생성하는 단계; 및 상기 투표 노드 또는 상기 집계 노드에서, 생성된 상기 블록을 검증하고, 검증된 블록을 상기 블록 체인에 연결하는 단계를 포함하는, 전자 투표 방법이 제공된다.

[0021] 상기 초기 블록은, 상기 전자 투표에 참여한 총 유권자 수, 상기 선거 관리 노드의 서명값, 상기 하나 이상의 집계 노드의 공개키 및 상기 복수의 후보자들 각각의 공개키 해시값을 포함할 수 있다.

[0022] 상기 일반 트랜잭션은, 상기 투표자의 PIN 번호, 상기 투표자가 선택한 후보자의 공개키 해시값, 상기 투표자의

개인키 서명값, 및 상기 투표자의 공개키를 포함할 수 있다.

[0023] 상기 일반 트랜잭션을 생성하는 단계는, 상기 투표자로부터 입력받은 PIN 번호의 유효성을 검증하고, 상기 유효성이 검증된 상기 투표자로부터 후보자 선택값을 입력받아 상기 일반 트랜잭션을 생성하며, 생성된 상기 일반 트랜잭션을 타 투표 노드 또는 상기 집계 노드로 송신하도록 구성될 수 있다.

[0024] 상기 투표 노드는, 타 투표 노드로부터 상기 일반 트랜잭션이 수신되는 경우, 수신된 상기 일반 트랜잭션에 포함된 상기 PIN 번호와 중복되는 PIN 번호의 존재 여부, 후보자의 공개키 해시값의 유효 여부, 및 상기 투표자의 개인키 서명값의 유효 여부에 따라 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 타 투표 노드 또는 상기 집계 노드로 송신할 수 있다.

[0025] 상기 투표 노드는, 상기 검증 결과 중복된 PIN 번호가 존재하거나, 상기 후보자의 공개키 해시값이 유효하지 않거나, 또는 상기 투표자의 개인키 서명값이 유효하지 않을 것으로 판단되는 경우, 수신된 상기 일반 트랜잭션을 폐기할 수 있다.

[0026] 상기 블록 생성 단계는, 수신된 상기 일반 트랜잭션에 포함된 상기 PIN 번호와 중복되는 PIN 번호의 존재 여부, 후보자의 공개키 해시값의 유효 여부, 및 상기 투표자의 개인키 서명값의 유효 여부에 따라 수신된 상기 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 현재 생성중인 블록에 추가하도록 구성될 수 있다.

[0027] 상기 블록 생성 단계는, 기 설정된 블록 생성 주기에 도달한 경우, 베이스 트랜잭션을 생성하여 상기 현재 생성중인 블록에 추가하고, 생성된 상기 블록을 타 투표 노드 또는 타 집계 노드로 송신하는 단계를 더 포함할 수 있다.

[0028] 상기 베이스 트랜잭션은, 상기 복수의 후보자들 각각의 공개키 해시값, 및 상기 베이스 트랜잭션이 속한 블록 내에서 집계된 상기 복수의 후보자들 각각의 득표수를 포함할 수 있다.

[0029] 상기 블록 검증 및 블록 체인 연결 단계는, 수신된 상기 블록의 베이스 트랜잭션에 기록된 총 투표수와 수신된 상기 블록에 포함된 일반 트랜잭션으로부터 계산된 총 투표수의 일치 여부,수신된 상기 블록의 베이스 트랜잭션에 기록된 상기 복수의 후보자 각각의 득표수와 수신된 상기 블록에 포함된 일반 트랜잭션으로부터 계산된 각 후보자별 득표수의 일치 여부, 블록 체인에 상기 블록에 포함된 PIN 번호와 중복된 PIN 번호가 존재하는지의 여부, 및 상기 블록에 포함된 머클 루트 해시값의 유효 여부를 판단함으로써 상기 수신된 블록을 검증하고, 검증된 블록에 자신의 서명값을 추가하여 타 투표 노드 또는 타 집계 노드로 송신하도록 구성될 수 있다.

[0030] 상기 블록 검증 및 블록 체인 연결 단계는, 상기 검증된 블록에 포함된 서명값의 개수가 기 설정된 값 이상인 경우, 상기 검증된 블록을 상기 블록 체인에 연결하도록 구성될 수 있다.

발명의 효과

[0032] 본 발명의 실시예들에 따르면, 전자 투표 결과가 변조되거나 위조되는 것을 방지하고 신뢰성 있는 전자 투표 시스템을 제공할 수 있다.

도면의 간단한 설명

[0034] 도 1은 본 발명의 일 실시예에 따른 전자 투표 시스템(100)의 구성을 설명하기 위한 블록도

도 2는 본 발명의 일 실시예에 따른 초기 블록(Genesis Block)의 구조를 설명하기 위한 예시도

도 3은 본 발명의 일 실시예에 따른 일반 블록의 구조를 설명하기 위한 예시도

도 4는 본 발명의 일 실시예에 따른 일반 트랜잭션 구조를 설명하기 위한 예시도

도 5는 본 발명의 일 실시예에 따른 베이스(Base) 트랜잭션 구조를 설명하기 위한 예시도

도 6은 본 발명의 일 실시예에 따른 각 투표 노드에서의 투표 및 일반 트랜잭션 생성 과정을 설명하기 위한 흐름도

도 7은 본 발명의 일 실시예에 따른 각 투표 노드에서의 일반 트랜잭션 검증 과정을 설명하기 위한 흐름도

도 8은 본 발명의 일 실시예에 따른 각 집계 노드, 또는 선거 관리 노드에서의 일반 트랜잭션 검증, 수집 및 블록 생성 과정(800)을 설명하기 위한 흐름도

도 9는 본 발명의 일 실시예에 따른 각 투표 노드, 집계 노드, 또는 선거 관리 노드에서의 블록 검증 과정(90

0)을 설명하기 위한 흐름도

도 10은 본 발명의 일 실시예에 따른 전자 투표 시스템에서 전술한 과정을 거쳐 블록 체인을 형성하는 과정을 설명하기 위한 예시도

발명을 실시하기 위한 구체적인 내용

[0035] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0036] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0038] 도 1은 본 발명의 일 실시예에 따른 전자 투표 시스템(100)의 구성을 설명하기 위한 블록도이다. 도시된 바와 같이, 본 발명의 일 실시예에 다른 전자 투표 시스템(100)은 하나 이상의 투표 노드(102), 하나 이상의 집계 노드(104) 및 선거 관리 노드(106)를 포함한다.

[0039] 투표 노드(102)(Voter Node, 또는 VN으로 줄여 칭함)는 전자 투표에 참여하는 투표자가 사용하는 단말이다. 일 실시예에서, 투표 노드(102)는 투표소 등에 설치된 투표 전용 장치일 수 있다. 다른 실시예에서, 투표 노드(102)는 투표자가 사용하는 데스크탑 컴퓨터, 노트북 컴퓨터, 태블릿, 스마트폰 등의 컴퓨팅 장치일 수 있다. 전자 투표시 투표자 인증을 위하여, 각 투표자들은 전자 투표일 이전에 별도의 투표자 검증 시스템(미도시)을 통하여 유권자 자격 검증 절차를 수행하고 PIN 번호를 부여받을 수 있다. 예를 들어, 상기 투표자 검증 시스템은 정부 기관, 또는 전자투표를 관리하는 별도의 공공 기관 등에서 제공되는 시스템일 수 있다. 보안을 위하여 PIN 번호와 각 유권자(투표자)의 개인 정보는 각각 다른 저장소에 저장될 수 있다. ₩해당 선거에 입후보한 후보자들은 그들의 공개키 해시값을 공개하기 위하여 투표 노드(102)를 이용하여 선거일 이전에 미리 투표를 진행할 수 있다.

[0040] 일 실시예에서, 투표 노드(102)는 투표자의 투표(선거에 입후보한 후보자들 중 어느 하나의 후보자를 선택하는 행위)에 따라 트랜잭션(transaction)을 생성한다. 이때 투표 노드(102)가 생성하는 트랜잭션은 후술할 베이스 트랜잭션과의 구분을 위하여 일반 트랜잭션이라고 칭하기로 한다. 또한, 투표 노드(102)는 타 투표 노드가 생성한 일반 트랜잭션 및 집계 노드(104)가 생성한 블록을 검증하는 역할을 수행한다.

[0041] 집계 노드(104)(Aggregator Node, 또는 AN으로 줄여 칭함)는 투표 노드(102)가 생성한 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 수집하여 블록을 생성한다. 또한 집계 노드(104)는 타 집계 노드가 생성한 블록을 검증하는 역할을 수행한다.

[0042] 선거 관리 노드(106)(Electoral Authority Node, 또는 EAN으로 줄여 칭함)는 전자 투표를 관리하는 주체에서 사용하는 단말이다. 선거 관리 노드(106)는 초기 블록(Genesis Block)을 생성하여 이를 네트워크를 통해 배포한다. 일 실시예에서, 초기 블록은 전자 투표의 결과로 생성되는 블록 체인(Block Chain)을 구성하는 가장 첫 번째 블록으로서, 전자 투표와 관련된 기본 정보를 포함한다.

[0043] 또한, 선거 관리 노드(106)는 전자 투표 과정에서 집계 노드(104)와 마찬가지로 투표 노드(102)가 생성한 일반 트랜잭션을 검증하고, 검증된 일반 트랜잭션을 수집하여 블록을 생성하며, 타 집계 노드가 생성한 블록을 검증하는 역할을 수행한다.

[0044] 일 실시예에서, 하나 이상의 투표 노드(102), 하나 이상의 집계 노드(104) 및 선거 관리 노드(106)는 하나 이상의 프로세서 및 그 프로세서와 연결된 컴퓨터 판독 가능 기록 매체를 포함하는 컴퓨팅 장치 상에서 구현될 수 있다. 컴퓨터 판독 가능 기록 매체는 프로세서의 내부 또는 외부에 있을 수 있고, 잘 알려진 다양한 수단으로 프로세서와 연결될 수 있다. 컴퓨팅 장치 내의 프로세서는 각 컴퓨팅 장치로 하여금 본 명세서에서 기술되는 예

시적인 실시예에 따라 동작하도록 할 수 있다. 예를 들어, 프로세서는 컴퓨터 판독 가능 기록 매체에 저장된 명령어를 실행할 수 있고, 컴퓨터 판독 가능 기록 매체에 저장된 명령어는 프로세서에 의해 실행되는 경우 컴퓨팅 장치로 하여금 본 명세서에 기술되는 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0045] 한편, 하나 이상의 투표 노드(102), 하나 이상의 집계 노드(104) 및 선거 관리 노드(106)는 통신 네트워크(108)를 통하여 서로 데이터를 송수신할 수 있다. 몇몇 실시예들에서, 통신 네트워크는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wire area networks), 셀룰러 네트워크, 모바일 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0047] 도 2는 본 발명의 일 실시예에 따른 초기 블록(Genesis Block)의 구조를 설명하기 위한 예시도이다. 전술한 바와 같이, 본 발명의 실시예들에서 초기 블록은 블록 체인을 구성하는 가장 첫 번째 블록으로서, 전자 투표와 관련된 기본 정보를 포함한다. 이와 같은 초기 블록은 선거 관리 노드(106)에 의해서만 생성될 수 있다. 도시된 바와 같이, 본 발명의 일 실시예에 따른 초기 블록은 헤더(Header) 영역 및 트랜잭션(Transaction) 영역을 포함한다.

[0048] 먼저, 헤더 영역에 포함되는 항목은 다음과 같다.

[0049] - Block ID: 초기 블록을 다른 블록과 구별하기 위한 식별자이다.

[0050] - Block Type: 해당 블록이 초기 블록인지, 또는 일반 블록인지를 구별하기 위한 값이 저장된다.

[0051] - Previous Hash: 본 블록과 연결된 이전 블록의 해시값이 저장되는 영역이나, 초기 블록의 경우 이전 블록이 없으므로 본 항목은 아무런 값도 가지지 않는다.

[0052] - Version: 전자 투표에 사용되는 블록체인의 버전을 나타낸다.

[0053] - Merkle Root: 초기 블록에 포함된 트랜잭션으로부터 생성된 머클 트리(Merkle Tree)의 루트 해시값이 저장된다.

[0054] - Timestamp: 초기 블록의 생성 시각을 나타낸다.

[0055] - All number of Voters: 해당 선거에 참여하기 위하여 PIN을 지급받은 총 유권자 수를 나타낸다.

[0056] - EAN Signature: 선거 관리 노드(Electoral Authority Node)의 서명값이다.

[0057] 초기 블록의 트랜잭션 영역에는 다음의 두 개의 트랜잭션을 포함한다.

[0058] - 1번째 트랜잭션(Tx1): 적합한 검증 절차를 통해 선정된 집계 노드들의 공개키들을 포함하는 트랜잭션이다.

[0059] - 2번째 트랜잭션(Tx2): 해당 선거에 입후보한 후보자들의 공개키 해시를 포함하는 트랜잭션이다.

[0061] 도 3은 본 발명의 일 실시예에 따른 일반 블록의 구조를 설명하기 위한 예시도이다. 본 발명의 실시예들에서, 일반 블록은 초기 블록 이후에 생성되는 블록으로서, 각 투표 노드(102)의 투표시 생성되는 트랜잭션이 저장된다. 일반 블록 또한 초기 블록과 마찬가지로 헤더(Header) 영역 및 트랜잭션(Transaction) 영역을 포함한다.

[0062] 먼저, 일반 블록의 헤더 영역에 포함되는 항목은 다음과 같다.

[0063] - Block ID: 해당 일반 블록을 다른 블록과 구별하기 위한 식별자이다.

[0064] - Block Type: 해당 블록이 초기 블록인지, 또는 일반 블록인지를 구별하기 위한 값이 저장된다.

[0065] - Previous Hash: 본 블록과 연결된 이전 블록의 해시값이 저장되는 영역이다.

[0066] - Version: 전자 투표에 사용되는 블록체인의 버전을 나타낸다.

[0067] - Merkle Root: 일반 블록에 포함된 트랜잭션들로부터 생성된 머클 트리(Merkle Tree)의 루트 해시값이 저장된다.

[0068] - Timestamp: 해당 일반 블록의 생성 시각을 나타낸다.

[0069] - Transaction Count: 해당 일반 블록에 포함되는 트랜잭션의 수를 나타낸다.

[0070] - Signatures: 해당 일반 블록을 검증한 노드(투표 노드, 집계 노드, 선거 관리 노드)의 서명값이 저장된다.

[0071] 일반 블록의 트랜잭션 영역에는 투표 노드에서 수행된 각 유권자들의 투표 결과가 트랜잭션 형태로 저장된다.

즉, 본 발명의 실시예에서 하나의 트랜잭션은 유권자들의 한 표와 대응된다.

[0073] 도 4는 본 발명의 일 실시예에 따른 일반 트랜잭션 구조를 설명하기 위한 예시도이다. 전술한 바와 같이, 본 발명의 실시예들에서 일반 트랜잭션은 투표 노드(102)에서의 투표 과정에서 생성되는 트랜잭션이다. 도시된 바와 같이, 본 발명의 일 실시예에 따른 일반 트랜잭션은 헤더(Header)와 본문(Body)을 포함한다.

[0074] 일반 트랜잭션의 헤더에는 다음과 같은 항목을 포함한다.

[0075] - Transaction ID: 해당 일반 트랜잭션을 다른 트랜잭션과 구별하기 위한 식별자이다.

[0076] - Transaction Type: 해당 트랜잭션의 종류를 나타내는 식별자로서, 해당 트랜잭션이 일반 트랜잭션인지 또는 베이스(Base) 트랜잭션인지를 구분하기 위하여 사용된다.

[0077] - Version: 전자 투표에 사용되는 블록체인의 버전을 나타낸다.

[0078] - Timestamp: 해당 일반 트랜잭션의 생성 시각을 나타낸다.

[0079] 일반 트랜잭션의 본문에는 다음과 같은 항목을 포함한다.

[0080] - PIN: 해당 트랜잭션을 생성한 투표자가 유권자 검증절차를 거쳐 지급받은 PIN이 저장된다.

[0081] - Candidate's Public Key Hash: 해당 트랜잭션을 생성한 투표자가 선택한 후보자의 공개키 해시값이 저장된다.

[0082] - Voter's Signature: 해당 투표자의 개인키 서명값이 저장된다.

[0083] - Voter's Raw Public Key: 해당 투표자의 공개키이며, 서명값 검증을 위해 사용된다.

[0085] 도 5는 본 발명의 일 실시예에 따른 베이스(Base) 트랜잭션 구조를 설명하기 위한 예시도이다. 본 발명의 실시예들에서 베이스 트랜잭션은 기 설정된 블록 생성 주기마다 집계 노드(104)에 의하여 생성되는 트랜잭션이다. 도시된 바와 같이, 일반 트랜잭션과 마찬가지로, 본 발명의 일 실시예에 따른 일반 트랜잭션은 헤더(Header)와 본문(Body)을 포함한다.

[0086] 베이스 트랜잭션의 헤더는 다음과 같은 항목을 포함한다.

[0087] - Transaction ID: 해당 베이스 트랜잭션을 다른 트랜잭션과 구별하기 위한 식별자이다.

[0088] - Transaction Type: 해당 트랜잭션의 종류를 나타내는 식별자로서, 해당 트랜잭션이 일반 트랜잭션인지 또는 베이스(Base) 트랜잭션인지를 구분하기 위하여 사용된다.

[0089] - Version: 전자 투표에 사용되는 블록체인의 버전을 나타낸다.

[0090] - Timestamp: 해당 베이스 트랜잭션의 생성 시각을 나타낸다.

[0091] 베이스 트랜잭션의 본문에는 다음과 같은 항목을 포함한다.

[0092] - Each Candidate's Public Key Hash: 각 후보자들의 공개키 해시값이다.

[0093] - Each Candidate's Number of Votes: 해당 베이스 트랜잭션이 속한 블록 내 트랜잭션 집계 결과로서, 해당 블록 내에서 각 후보자들의 득표수를 나타낸다.

[0095] 도 6은 본 발명의 일 실시예에 따른 각 투표 노드(102)에서의 투표 및 일반 트랜잭션 생성 과정(600)을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0096] 단계 602에서, 투표 노드(102)는 투표자로부터 PIN 번호를 입력받는다. 전술한 바와 같이, 상기 PIN 번호는 각 투표자들이 투표일 이전에 별도의 투표자 검증 시스템 등을 통하여 부여받은 것일 수 있다.

[0097] 단계 604에서, 투표 노드(102)는 입력된 상기 PIN 번호의 유효성을 검증한다. 일 실시예에서, 투표 노드(102)는 상기 투표자 검증 시스템과 연계하여 상기 PIN 번호의 유효성을 검증하도록 구성될 수 있다.

[0098] 만약 상기 604 단계의 수행 결과 입력된 PIN 번호의 유효성 검증에 성공한 경우, 단계 606에서 투표 노드(102)는 해당 선거에 입후보한 후보자들 중 하나의 후보자에 대한 투표자의 선택값을 입력받는다. 즉, 본 단계는 PIN 번호의 인증에 성공한 투표자가 실제 투표를 진행하는 단계이다. 이를 위하여 투표 노드(102)는 상기 투표자의

후보자 선택을 위한 적절한 사용자 인터페이스를 출력하도록 구성될 수 있다.

[0099] 한편 상기 604 단계의 수행 결과 입력된 PIN 번호의 유효성 검증에 성공하지 못한 경우, 단계 608에서 투표 노드(102)는 투표 과정을 종료하게 된다.

[0100] 단계 610에서, 투표 노드(102)는 투표자의 PIN 번호 및 후보자 선택값을 포함하는 일반 트랜잭션을 생성한다. 상기 일반 트랜잭션의 상세 구성에 대해서는 도 4에서 설명한 바와 같다.

[0101] 단계 612에서, 투표 노드(102)는 생성된 상기 일반 트랜잭션을 타 노드로 송신한다. 본 발명의 실시예들에서, 투표 노드(102)에서 생성된 일반 트랜잭션은 타 투표 노드(102), 집계 노드(104) 또는 선거 관리 노드(106) 중 어느 하나로 전송될 수 있다.

[0103] 도 7은 본 발명의 일 실시예에 따른 각 투표 노드(102)에서의 일반 트랜잭션 검증 과정(700)을 설명하기 위한 흐름도이다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0104] 단계 702에서, 투표 노드(102)는 전자 투표에 참여하는 타 투표 노드로부터 일반 트랜잭션을 수신한다.

[0105] 단계 704에서, 투표 노드(102)는 해당 시점의 블록 체인에 수신된 상기 일반 트랜잭션에 포함된 PIN 번호와 중복되는 PIN 번호가 존재하는지의 여부를 판단한다.

[0106] 상기 704 단계의 판단 결과 중복된 PIN 번호가 존재하지 않는 경우, 단계 706에서 투표 노드(102)는 상기 일반 트랜잭션에 포함된 후보자의 공개키 해시값이 유효한지의 여부를 판단한다. 일 실시예에서, 투표 노드(102)는 상기 일반 트랜잭션에 포함된 후보자의 공개키 해시값을 초기 블록의 공개키 해시값과 비교하여 상기 유효성 여부를 판단할 수 있다.

[0107] 상기 706 단계의 판단 결과 상기 공개키 해시값이 유효한 경우, 단계 708에서 투표 노드(102)는 상기 일반 트랜잭션에 포함된 투표자의 개인키 서명값을 검증한다. 일 실시예에서, 투표 노드는 상기 일반 트랜잭션에 포함된 투표자의 공개키를 이용하여 상기 개인키 서명값을 검증할 수 있다.

[0108] 상기 708 단계의 수행 결과 상기 개인키 서명값의 검증에 성공한 경우, 단계 710에서 투표 노드(102)는 수신한 상기 일반 트랜잭션을 타 노드로 송신한다. 본 발명의 실시예들에서, 투표 노드(102)는 상기 일반 트랜잭션을 타 투표 노드(102), 집계 노드(104) 또는 선거 관리 노드(106) 중 어느 하나로 전송할 수 있다.

[0109] 한편, 상기 704 단계에서 중복된 PIN 번호가 존재하거나, 상기 706 단계에서 공개키 해시값이 유효하지 않거나, 또는 상기 708 단계에서 서명값 검증에 실패한 경우, 단계 712에서 투표 노드(102)는 수신된 상기 일반 트랜잭션을 폐기한다.

[0111] 도 8은 본 발명의 일 실시예에 따른 각 집계 노드(104), 또는 선거 관리 노드(106)에서의 일반 트랜잭션 검증, 수집 및 블록 생성 과정(800)을 설명하기 위한 흐름도이다. 이하의 설명에서는 편의를 위해 집계 노드(104)에서 일반 트랜잭션을 검증하고 블록을 생성하는 것으로 가정하였으나, 이하의 단계들은 각 투표 노드(102) 및 선거 관리 노드(106)에서도 동일하게 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0112] 단계 802에서, 집계 노드(104)는 전자 투표에 참여하는 투표 노드(102)로부터 일반 트랜잭션을 수신한다.

[0113] 단계 804에서, 집계 노드(104)는 해당 시점에 생성 중인 블록에 이미 포함되어 있는 일반 트랜잭션 중 상기 802 단계에서 수신된 일반 트랜잭션의 PIN 번호와 중복되는 PIN 번호가 존재하는지의 여부를 판단한다.

[0114] 상기 804 단계의 판단 결과 중복된 PIN 번호가 존재하지 않는 경우, 단계 806에서 집계 노드(104)는 상기 일반 트랜잭션에 포함된 후보자의 공개키 해시값이 유효한지의 여부를 판단한다. 일 실시예에서, 집계 노드(104)는 상기 일반 트랜잭션에 포함된 후보자의 공개키 해시값을 초기 블록의 공개키 해시값과 비교하여 상기 유효성 여부를 판단할 수 있다.

[0115] 상기 806 단계의 판단 결과 상기 공개키 해시값이 유효한 경우, 단계 808에서 집계 노드(104)는 상기 일반 트랜잭션에 포함된 투표자의 개인키 서명값을 검증한다. 일 실시예에서, 투표 노드는 상기 일반 트랜잭션에 포함된 투표자의 공개키를 이용하여 상기 개인키 서명값을 검증할 수 있다.

[0116] 상기 808 단계의 수행 결과 상기 개인키 서명값의 검증에 성공한 경우, 단계 810에서 집계 노드(104)는 수신된 상기 일반 트랜잭션을 집계 노드(104)에서 현재 생성중인 블록에 추가한다.

[0117] 한편, 상기 804 단계에서 중복된 PIN 번호가 존재하거나, 상기 806 단계에서 공개키 해시값이 유효하지 않거나, 또는 상기 808 단계에서 서명값 검증에 실패한 경우, 단계 812에서 집계 노드(104)는 수신된 상기 일반 트랜잭션을 폐기한다.

[0118] 단계 814에서, 집계 노드(104)는 기 설정된 블록 생성 주기에 도달했는지의 여부를 판단한다. 만약 아직 블록 생성 주기가 아닌 경우, 집계 노드(104)는 802 단계로 돌아가 일반 트랜잭션의 수집하고 검증하는 과정을 반복한다.

[0119] 만약 상기 814 단계의 판단 결과 블록 생성 주기에 도달한 경우, 단계 816에서 집계 노드(104)는 일반 트랜잭션 수집을 멈추고 베이스 트랜잭션을 생성한다. 전술한 바와 같이, 상기 베이스 트랜잭션은 현재 생성된 블록의 마지막 트랜잭션으로서, 해당 블록 내에서의 각 후보자들의 득표수 집계 결과를 포함한다.

[0120] 단계 816에서, 집계 노드(104)는 생성된 상기 블록을 타 노드로 송신한다. 본 발명의 실시예들에서, 집계 노드(104)는 상기 블록을 타 투표 노드(102), 집계 노드(104) 또는 선거 관리 노드(106) 중 어느 하나로 전송할 수 있다.

[0122] 도 9는 본 발명의 일 실시예에 따른 각 투표 노드(102), 집계 노드(104), 또는 선거 관리 노드(106)에서의 블록 검증 과정(900)을 설명하기 위한 흐름도이다. 이하의 설명에서는 편의를 위해 집계 노드(104)에서 블록을 검증하는 것으로 가정하였으나, 이하의 단계들은 각 투표 노드(102) 및 선거 관리 노드(106)에서도 동일하게 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0123] 단계 902에서, 집계 노드(104)는 타 노드로부터 블록을 수신한다. 본 발명의 실시예들에서, 집계 노드(104)는 타 투표 노드(102), 집계 노드(104) 또는 선거 관리 노드(106) 중 어느 하나로부터 블록을 수신할 수 있다.

[0124] 단계 904에서, 집계 노드(104)는 수신된 블록에 포함된 베이스 트랜잭션의 총 투표수가 실제 블록이 포함하고 있는 트랜잭션으로부터 계산된 총 투표수와 일치하는지 여부를 판단한다.

[0125] 상기 904 단계의 판단 결과 일치하는 경우, 단계 906에서 집계 노드(104)는 베이스 트랜잭션에 기록된 각 후보자별 득표수가 실제 블록이 포함하고 있는 트랜잭션으로부터 계산된 각 후보자별 득표수와 일치하는지 여부를 판단한다.

[0126] 상기 906 단계의 판단 결과 일치하는 경우, 단계 908에서 집계 노드(104)는 블록 체인을 조회하여 블록 내에 포함된 PIN 번호 중 상기 블록 체인에 포함된 PIN 번호와 중복된 PIN 번호가 존재하는지의 여부를 판단한다.

[0127] 상기 908 단계의 판단 결과 중복된 PIN 번호가 존재하지 않는 경우, 단계 910에서 집계 노드(104)는 블록에 저장된 머클 루트 해시값을 검증함으로써 블록 내 트랜잭션의 위변조 여부를 확인한다.

[0128] 상기 910 단계의 검증 결과 머클 루트 해시값의 검증에 성공하는 경우, 단계 912에서 집계 노드(104)는 수신된 블록의 헤더에 자신의 서명값을 추가한다.

[0129] 한편, 상기 904 단계에서 총 투표수가 일치하지 않거나, 상기 906 단계에서 후보자별 득표수가 일치하지 않거나, 상기 908 단계에서 중복된 PIN 번호가 존재하거나, 또는 상기 910 단계에서 머클 루트 해시값의 검증에 실패한 경우, 단계 914에서 집계 노드(104)는 수신된 블록을 폐기한다.

[0130] 단계 916에서, 집계 노드(104)는 블록에 포함된 서명의 개수가 임계값 이상인지의 여부를 판단한다. 예를 들어, 상기 임계값은 상기 전자 투표에 참여하는 네트워크 내 전체 노드의 개수의 50%로 설정될 수 있다. 다만 본 발명의 실시예들은 특정 임계값에 한정되는 것은 아니다.

[0131] 상기 916 단계의 판단 결과 서명 개수가 임계값 이상인 경우, 단계 918에서 집계 노드(104)는 수신된 블록을 블록 체인에 연결한다.

[0132] 이와 달리 상기 916 단계의 판단 결과 서명 개수가 임계값 미만인 경우, 단계 920에서 집계 노드(104)는 수신된 상기 블록을 타 노드로 송신한다. 본 발명의 실시예들에서, 집계 노드(104)는 상기 블록을 타 투표 노드(102), 집계 노드(104) 또는 선거 관리 노드(106) 중 어느 하나로 전송할 수 있다.

[0134] 도 10은 본 발명의 일 실시예에 따른 전자 투표 시스템(100)에서 전술한 과정을 거쳐 블록 체인을 형성하는 과정을 설명하기 위한 예시도이다. 도시된 바와 같이, 투표 노드(102)에서의 투표자들의 투표 결과 일반 트랜잭션 TX1, TX2, TX3이 생성된다. 이 중 TX1, TX2는 집계 노드(104)에 의해 블록 2001에 추가되고, TX3은 다른 집계 노드(104)에 의해 블록 2002에 추가된다. 블록 생성 주기가 되면, 블록 2001을 생성한 집계 노드(104)는 TX1, TX2의 투표 결과를 종합하여 베이스 트랜잭션 BTX를 생성하여 블록 2001의 마지막 트랜잭션으로 추가하고 해당 블록을 블록 체인에 연결한다. 블록 체인의 첫 번째 블록인 Block 0은 초기 블록에 해당하며, Block 1부터는 일반 블록이 된다.

[0135] 이와 같이 블록 체인을 이용하여 투표 결과를 집계할 경우 악의적인 사용자가 투표 결과를 위조하거나 변조하는 것이 사실상 불가능하게 된다. 따라서 본 발명의 실시예들에 따를 경우 전자 투표에 있어 신뢰성과 안정성을 담보할 수 있다.

[0137] 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0138] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0140] 100: 전자 투표 시스템

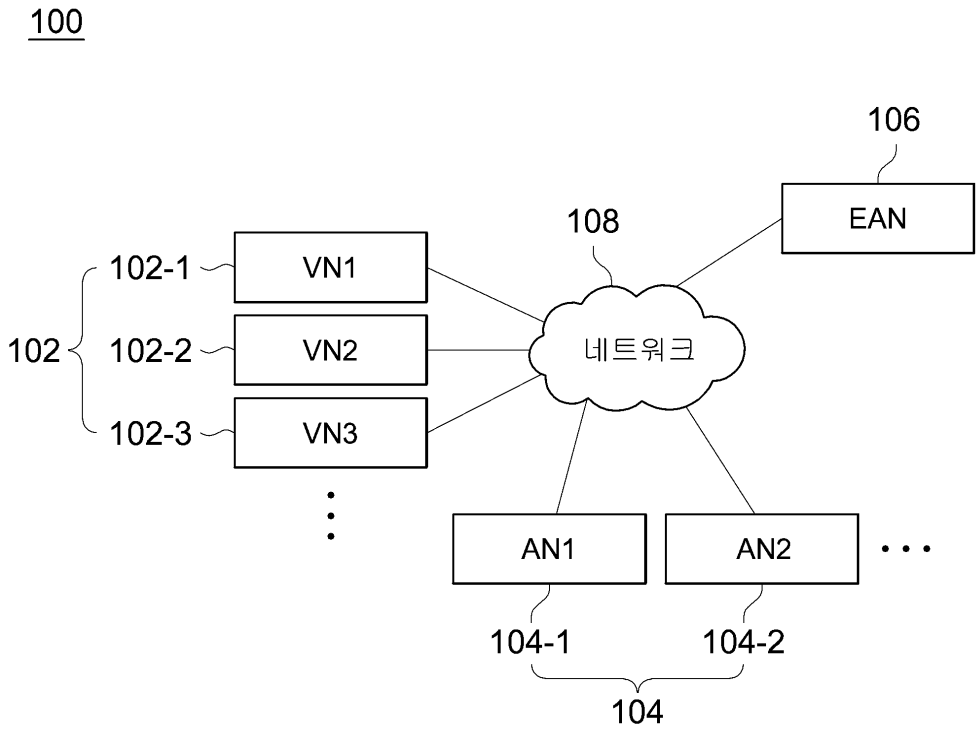
102: 투표 노드

104: 집계 노드

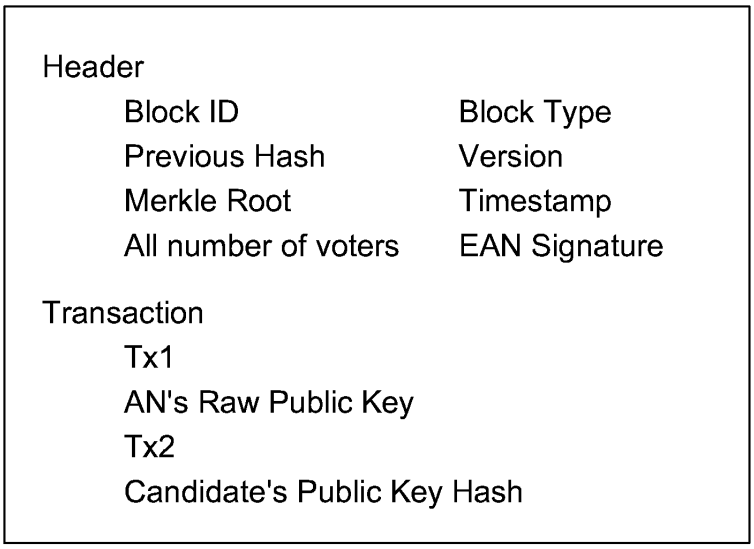
106: 선거 관리 노드

도면

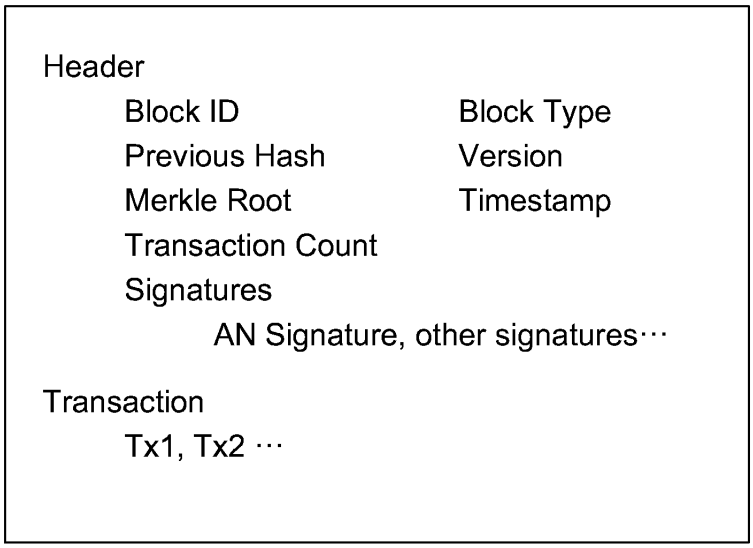
도면1


100
106
EAN
108
102-1
VN1
102
102-2
VN2
네트워크
102-3
VN3
AN1
AN2
104-1
104-2
104

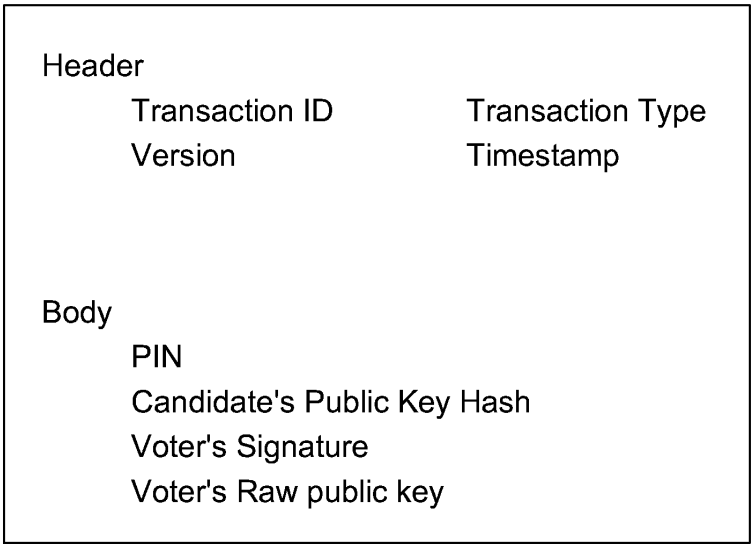
도면2


Header
Block ID
Block Type
Previous Hash
Version
Merkle Root
Timestamp
All number of voters
EAN Signature
Transaction
Tx1
AN's Raw Public Key
Tx2
Candidate's Public Key Hash

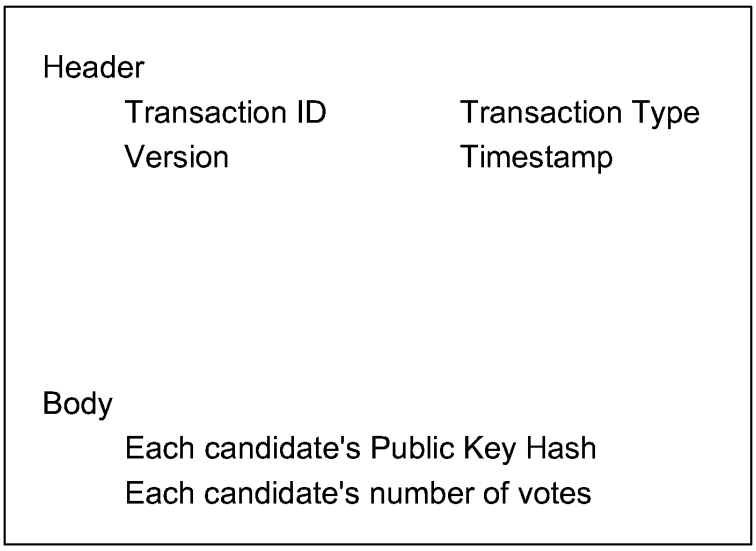
도면3


Header
Block ID
Block Type
Previous Hash
Version
Merkle Root
Timestamp
Transaction Count
Signatures
AN Signature, other signatures…
Transaction
Tx1, Tx2 …

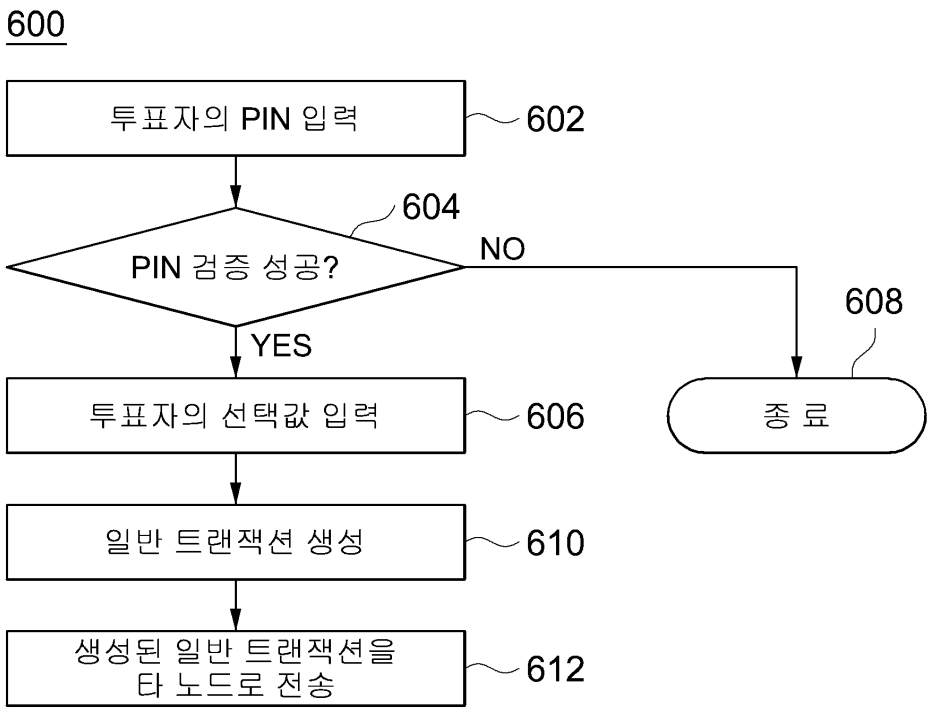
도면4


Header
Transaction ID
Transaction Type
Version
Timestamp
Body
PIN
Candidate's Public Key Hash
Voter's Signature
Voter's Raw public key

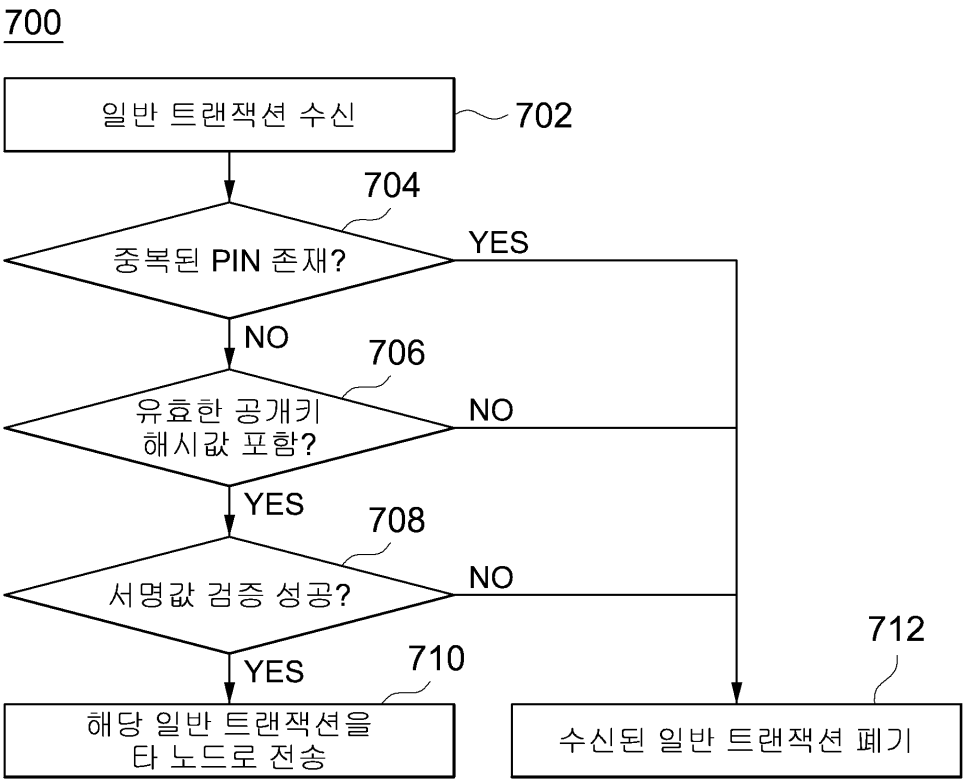
도면5


Header
Transaction ID
Transaction Type
Version
Timestamp
Body
Each candidate's Public Key Hash
Each candidate's number of votes

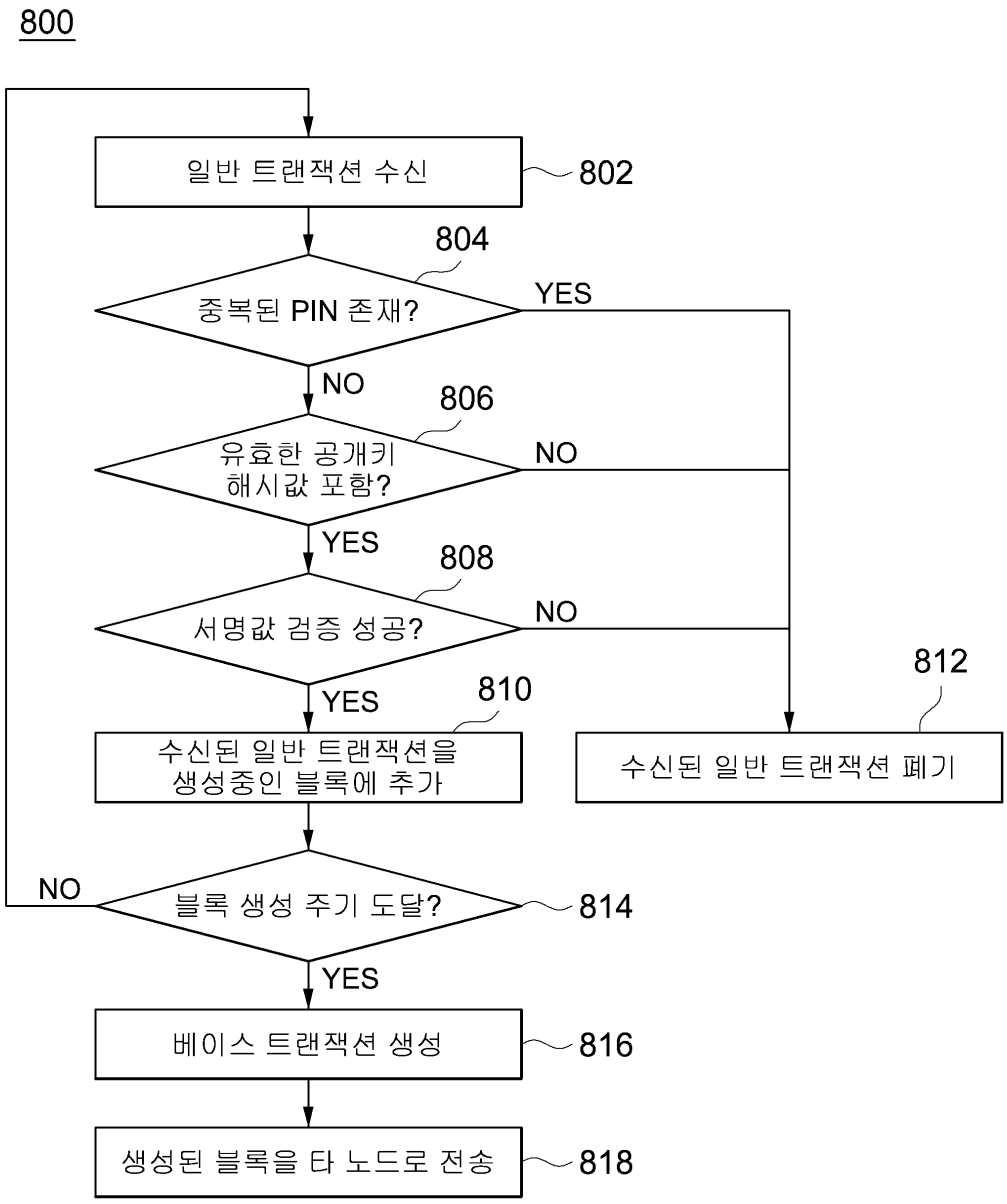
도면6


600
투표자의 PIN 입력
602
604
PIN 검증 성공?
NO
608
YES
투표자의 선택값 입력
606
종 료
일반 트랜잭션 생성
610
생성된 일반 트랜잭션을
타 노드로 전송
612

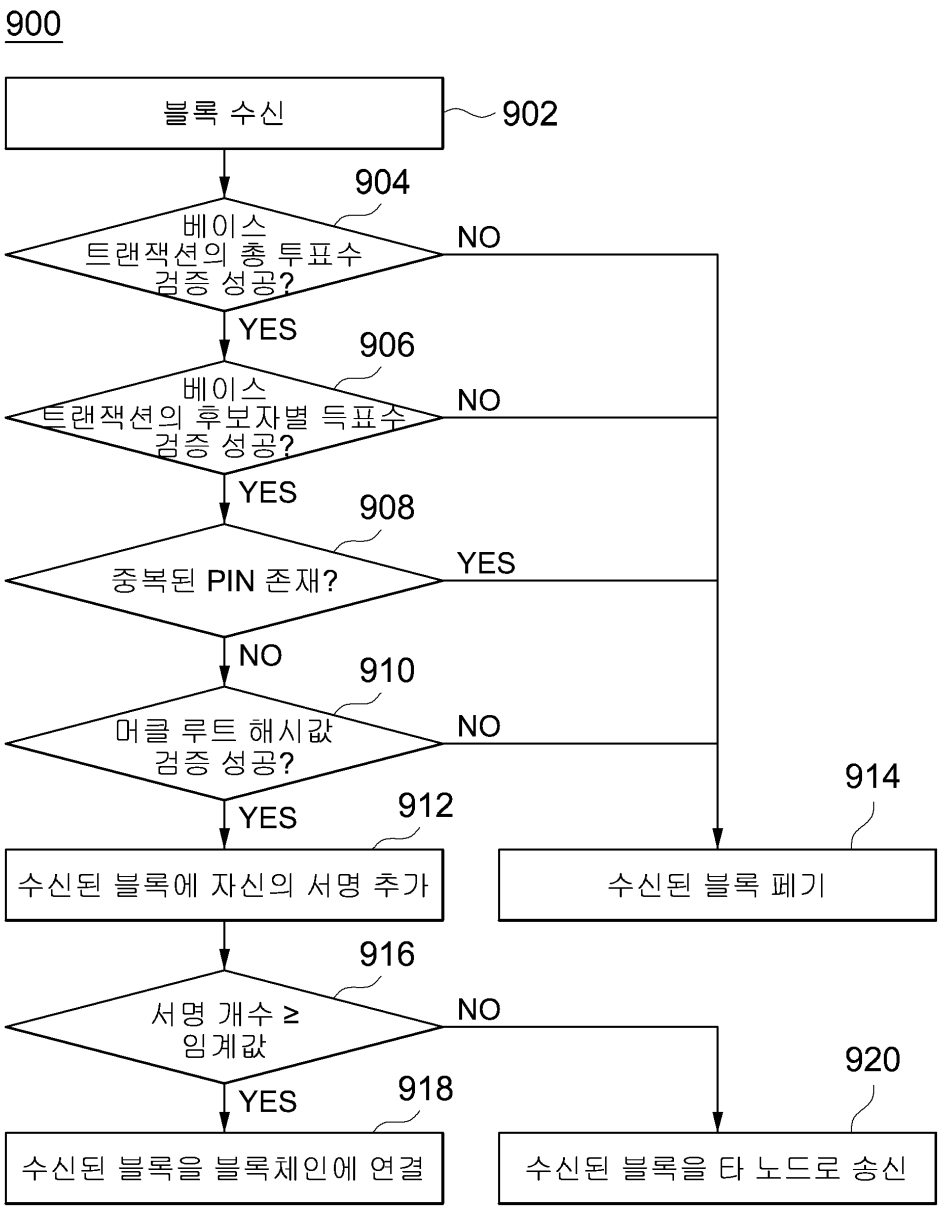
도면7


700
일반 트랜잭션 수신
702
704
중복된 PIN 존재?
YES
NO
706
유효한 공개키 해시값 포함?
NO
YES
708
서명값 검증 성공?
NO
YES
710
712
해당 일반 트랜잭션을 타 노드로 전송
수신된 일반 트랜잭션 폐기

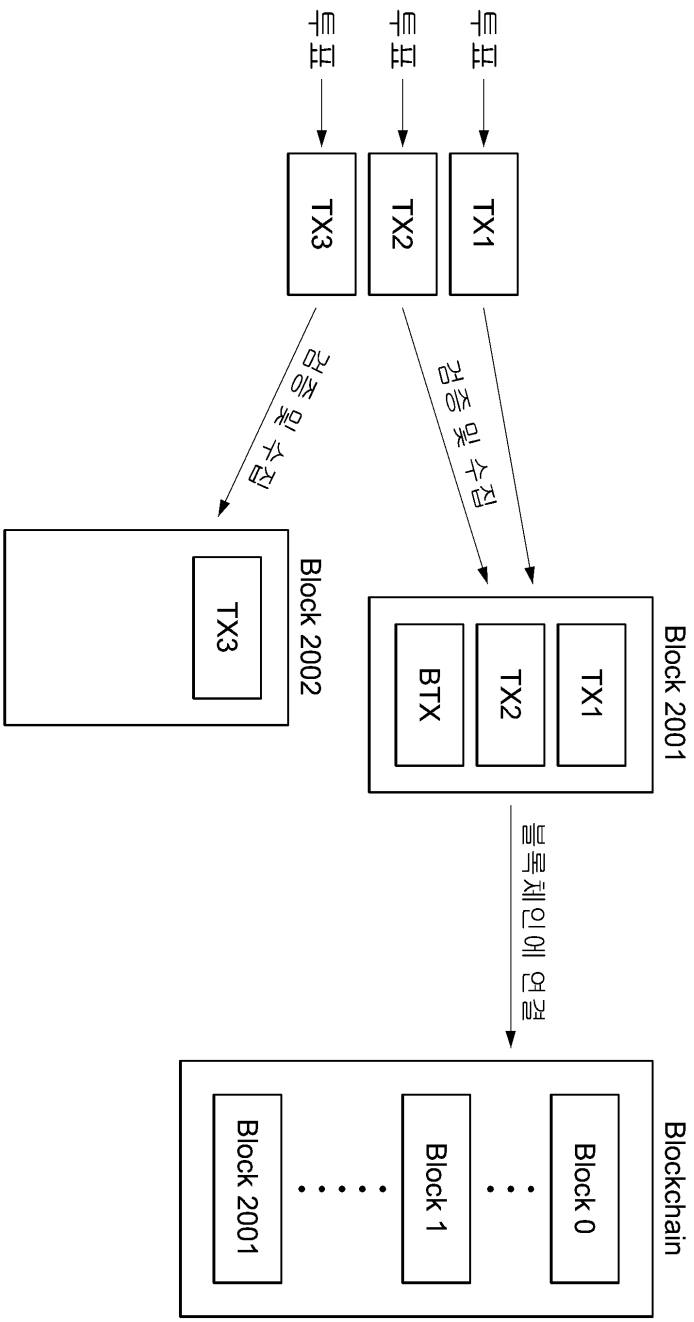
도면8


800
일반 트랜잭션 수신
802
804
중복된 PIN 존재?
YES
NO
806
유효한 공개키 해시값 포함?
NO
YES
808
서명값 검증 성공?
NO
YES
810
수신된 일반 트랜잭션을 생성중인 블록에 추가
812
수신된 일반 트랜잭션 폐기
NO
블록 생성 주기 도달?
814
YES
베이스 트랜잭션 생성
816
생성된 블록을 타 노드로 전송
818

도면9


900
블록 수신
902
904
베이스 트랜잭션의 총 투표수 검증 성공?
NO
YES
906
베이스 트랜잭션의 후보자별 득표수 검증 성공?
NO
YES
908
중복된 PIN 존재?
YES
NO
910
머클 루트 해시값 검증 성공?
NO
YES
912
914
수신된 블록에 자신의 서명 추가
수신된 블록 페기
916
서명 개수 ≥ 임계값
NO
YES
918
920
수신된 블록을 블록체인에 연결
수신된 블록을 타 노드로 송신

도면10


투표
투표
투표
TX1
TX2
TX3
검증 및 수집
검증 및 수집
Block 2001
BTX
TX2
TX1
Block 2002
TX3
블록체인에 연결
Blockchain
Block 0
Block 1
Block 2001