



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0084165
(43) 공개일자 2019년07월16일

(51) 국제특허분류(Int. Cl.)
G08C 17/02 (2006.01) H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G08C 17/02 (2013.01)
H04L 9/0825 (2013.01)
(21) 출원번호 10-2017-0176943
(22) 출원일자 2017년12월21일
심사청구일자 2017년12월21일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
장주욱
서울특별시 서대문구 가재울미래로 2, 206동 202호 (남가좌제1동, DMC파크뷰자이)
한동희
서울특별시 서대문구 이화여대 2길 26-8 401호
피승재
서울특별시 양천구 목동서로 130 목동아파트 407동 203호
(74) 대리인
이지연

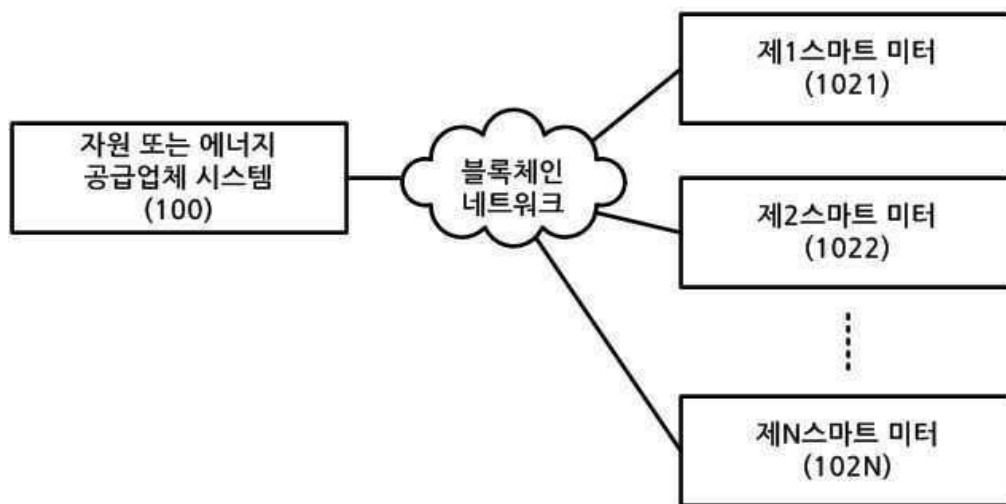
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **블록체인을 이용한 원격 검침 방법 및 시스템**

(57) 요약

본 발명에 따르는 블록체인을 이용한 원격 검침 방법은, 자원 또는 에너지 공급업체 시스템 및 제1 내지 제N스마트 미터를 블록체인 네트워크로 구성하는 단계; 상기 자원 또는 에너지 공급업체 시스템은 블록체인을 이용한 원격 검침을 위한 지불함수가 규정하며 상기 블록체인 네트워크에 참여한 스마트 미터들에 대한 주소정보를 기록한 스마트 컨트랙트를 생성하여 상기 스마트 미터들로 전송하는 단계; 상기 스마트 미터들이 상기 스마트 컨트랙트가 수신되면 블록체인에 기록하는 단계; 상기 스마트 미터들 중 어느 하나는 스마트 컨트랙트내 지불함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자원 또는 에너지 공급에 대한 검침값과 자신의 주소정보를 추가하고, 개인키로 서명하고, 작업증명과정을 거쳐 블록으로 구성하여 상기 블록체인 네트워크를 통해 상기 자원 또는 에너지 공급업체 시스템으로 전송하는 단계;를 구비함을 특징으로 한다.

대표도 - 도1



(52) CPC특허분류

H04L 9/3263 (2013.01)

H04L 2209/38 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 NRF-2016R1D1A1B01009027

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 이공학개인지초연구지원사업

연구과제명 블록체인 알고리즘의 개선 및 차세대 활용기법의 연구

기 여 율 1/1

주관기관 서강대학교 산학협력단

연구기간 2017.06.01 ~ 2018.02.28

명세서

청구범위

청구항 1

블록체인을 이용한 원격 검침 방법에 있어서,

자원 또는 에너지 공급업체 시스템 및 제1 내지 제N스마트 미터를 블록체인 네트워크로 구성하는 단계;

상기 자원 또는 에너지 공급업체 시스템은 블록체인을 이용한 원격 검침을 위한 지불함수가 규정하며 상기 블록체인 네트워크에 참여한 스마트 미터들에 대한 주소정보를 기록한 스마트 컨트랙트를 생성하여 상기 스마트 미터들로 전송하는 단계;

상기 스마트 미터들이 상기 스마트 컨트랙트가 수신되면 블록체인에 기록하는 단계;

상기 스마트 미터들 중 어느 하나는 스마트 컨트랙트내 지불함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자원 또는 에너지 공급에 대한 검침값과 자신의 주소정보를 추가하고, 개인키로 서명하고, 작업증명과정을 거쳐 블록으로 구성하여 상기 블록체인 네트워크를 통해 상기 자원 또는 에너지 공급업체 시스템으로 전송하는 단계;를 구비함을 특징으로 하는 블록체인을 이용한 원격 검침 방법.

청구항 2

제1항에 있어서,

자원 또는 에너지 공급업체 시스템이 상기 지불함수를 호출하는 트랜잭션이 수신되면, 상기 트랜잭션에 포함된 주소정보를 토대로 상기 트랜잭션이 유효한지 체크하는 단계; 및

상기 트랜잭션이 유효하면, 상기 트랜잭션에 포함된 검침값에 대응되는 과금금액을 결정하고, 상기 스마트 미터의 주소정보에 대응되게 트랜잭션 수신날짜와 검침값과 과금금액을 대응되게 저장하고, 상기 주소정보에 대응되는 잔고의 금액을 상기 과금금액에 대응되게 감액하고 상기 자원 또는 에너지 공급업체의 잔고의 금액을 상기 과금금액에 대응되게 증액하는 단계;를 더 구비함을 특징으로 하는 블록체인을 이용한 원격 검침 방법.

청구항 3

제1항에 있어서,

상기 스마트 미터들 중 어느 하나는 스마트 컨트랙트내 쿼리함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자신의 주소정보와 쿼리날짜정보를 추가하고, 개인키로 서명하고, 작업증명과정을 거쳐 블록으로 구성하여 상기 블록체인 네트워크를 통해 상기 자원 또는 에너지 공급업체 시스템으로 전송하는 단계; 및

상기 자원 또는 에너지 공급업체 시스템이 상기 쿼리함수를 호출하는 트랜잭션이 수신되면, 상기 트랜잭션에 포함된 주소정보를 토대로 상기 트랜잭션이 유효한지를 체크하고, 상기 트랜잭션이 유효하면 상기 트랜잭션에 포함된 주소정보와 쿼리날짜정보에 대응되게 기록된 스마트 미터의 검침값과 과금금액정보를 상기 스마트 미터로 반환하는 단계;를 더 구비함을 특징으로 하는 블록체인을 이용한 원격 검침 방법.

청구항 4

제1항에 있어서,

블록체인 네트워크에 참여하지 않은 상태의 스마트 미터가 고유한 공개키와 개인키 쌍을 생성하고, 자신의 주소정보와 공개키와 개인키 쌍을 공개키로 암호화하여 디지털 서명정보를 생성하여 상기 블록체인 네트워크를 통해 상기 자원 또는 에너지 공급업체 시스템으로 전송하는 단계; 및

상기 자원 또는 에너지 공급업체 시스템이 상기 디지털 서명정보가 수신되면, 수신한 디지털 서명정보를 공개키로 복호화하여 유효한지 여부를 판단하고, 상기 공개키로 복호화된 디지털 서명정보에 포함된 스마트 미터의 주소정보를 상기 스마트 컨트랙트에 추가하여 상기 스마트 미터를 블록체인 네트워크에 새로이 참여시키는 단계;를 더 구비함을 특징으로 하는 블록체인을 이용한 원격 검침 방법.

청구항 5

제4항에 있어서,

블록체인 네트워크에 로그인하지 않은 상태의 스마트 미터가 스마트 컨트랙트내의 로그인 함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자신의 주소정보를 추가하여 개인키로 서명하고, 작업증명과정을 거쳐 블록으로 구성하여 상기 블록체인 네트워크로 전파하는 단계; 및

상기 블록체인 네트워크에 속한 스마트 미터 및 자원 또는 에너지 공급업체 시스템이, 상기 블록체인 네트워크를 통해 수신된 블록을 블록체인에 기록하며, 상기 블록체인에 블록 형태의 로그인함수를 호출하는 트랜잭션이 기록되었으면, 상기 트랜잭션에 포함된 주소정보가 스마트 컨트랙트내에 기록되었는지를 체크하고, 상기 주소정보가 스마트 컨트랙트에 기록되었으면 상기 주소정보의 스마트 미터에 대한 로그인 완료를 통지하는 단계;를 더 포함함을 특징으로 하는 블록체인을 이용한 원격 검침 방법.

청구항 6

제1항에 있어서,

자원 또는 에너지 공급업체 시스템이 스마트 컨트랙트내의 날짜 업데이트 함수를 호출하는 트랜잭션을 생성하고, 자신의 주소정보를 상기 트랜잭션에 추가하고, 상기 트랜잭션을 개인키로 서명하고, 작업증명과정을 거쳐 블록으로 구성하여 상기 블록체인 네트워크를 통해 상기 블록체인 네트워크의 스마트 미터들로 전송하는 단계; 및

상기 블록체인 네트워크에 속한 스마트 미터들이 상기 블록체인 네트워크를 통해 수신된 블록을 블록체인에 기록하며, 상기 블록체인에 블록 형태의 날짜 업데이트 함수를 호출하는 트랜잭션이 기록되었으면, 상기 트랜잭션에 포함된 주소정보가 자원 또는 에너지 공급업체 시스템을 지시하면, 스마트 컨트랙트의 날짜를 업데이트하는 단계;를 더 구비함을 특징으로 하는 블록체인을 이용한 원격 검침 방법.

청구항 7

제1항 내지 제6항 중 어느 한 항에 있어서,

상기 블록체인 네트워크에 속한 스마트 미터들 또는 자원 또는 에너지 공급업체 시스템이,

트랜잭션의 생성시마다

트랜잭션을 자신의 개인키로 서명하여 블록체인 네트워크로 전파하고,

상기 블록체인 네트워크를 통해 트랜잭션이 수신될 때마다 트랜잭션이 유효한지 검증한 후에 수신된 트랜잭션을 저장하고,

미리 정해진 주기마다 수신되어 저장된 트랜잭션에 대해 작업증명과정을 거쳐 블록을 구성하여 블록을 블록체인 네트워크로 전파하고,

상기 블록체인 네트워크를 통해 블록이 수신될 때마다 수신된 블록이 유효한지 검증하고, 상기 수신된 블록이 유효하면 자신의 블록체인에 기록함을 특징으로 하는 블록체인을 이용한 원격 검침방법.

청구항 8

블록체인을 이용한 원격 검침 시스템에 있어서,

블록체인 네트워크로 구성된 자원 또는 에너지 공급업체 시스템; 및 제1 내지 제N스마트 미로 구성되며,

상기 자원 또는 에너지 공급업체 시스템은 블록체인을 이용한 원격 검침을 위한 지불함수가 규정하며 상기 블록체인 네트워크에 참여한 스마트 미터들에 대한 주소정보를 기록한 스마트 컨트랙트를 생성하여 상기 스마트 미터들로 전송하고,

상기 스마트 미터들은 상기 스마트 컨트랙트가 수신되면 블록체인에 기록하고,

상기 스마트 미터들 중 어느 하나는 스마트 컨트랙트내 지불함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자원 또는 에너지 공급에 대한 검침값과 자신의 주소정보를 추가하고, 개인키로 서명하고, 작업증명과정을 거쳐 블록으로 구성하여 상기 블록체인 네트워크를 통해 상기 자원 또는 에너지 공급업체 시스템으로 전송함을

특징으로 하는 블록체인을 이용한 원격 검침 시스템.

청구항 9

제8항에 있어서,

상기 자원 또는 에너지 공급업체 시스템은, 상기 지불함수를 호출하는 트랜잭션이 수신되면, 상기 트랜잭션에 포함된 주소정보를 토대로 상기 트랜잭션이 유효한지 체크하고,

상기 트랜잭션이 유효하면, 상기 트랜잭션에 포함된 검침값에 대응되는 과금금액을 결정하고, 상기 스마트 미터의 주소정보에 대응되게 트랜잭션 수신날짜와 검침값과 과금금액을 대응되게 저장하고, 상기 주소정보에 대응되는 잔고의 금액을 상기 과금금액에 대응되게 감액하고 상기 자원 또는 에너지 공급업체의 잔고의 금액을 상기 과금금액에 대응되게 증액함을 특징으로 하는 블록체인을 이용한 원격 검침 시스템.

청구항 10

제8항에 있어서,

상기 스마트 미터들 중 어느 하나는 스마트 컨트랙트내 쿼리함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자신의 주소정보와 쿼리날짜정보를 추가하고, 개인키로 서명하고, 작업증명과정을 거쳐 블록으로 구성하여 상기 블록체인 네트워크를 통해 상기 자원 또는 에너지 공급업체 시스템으로 전송하고,

상기 자원 또는 에너지 공급업체 시스템은 상기 쿼리함수를 호출하는 트랜잭션이 수신되면, 상기 트랜잭션에 포함된 주소정보를 토대로 상기 트랜잭션이 유효한지를 체크하고, 상기 트랜잭션이 유효하면 상기 트랜잭션에 포함된 주소정보와 쿼리날짜정보에 대응되게 기록된 스마트 미터의 검침값과 과금금액정보를 상기 스마트 미터로 반환함을 특징으로 하는 블록체인을 이용한 원격 검침 시스템.

청구항 11

제8항에 있어서,

상기 블록체인 네트워크에 참여하지 않은 상태의 스마트 미터는 고유한 공개키와 개인키 쌍을 생성하고, 자신의 주소정보와 공개키와 개인키 쌍을 공개키로 암호화하여 디지털 서명정보를 생성하여 상기 블록체인 네트워크를 통해 상기 자원 또는 에너지 공급업체 시스템으로 전송하고,

상기 자원 또는 에너지 공급업체 시스템이 상기 디지털 서명정보가 수신되면, 수신한 디지털 서명정보를 공개키로 복호화하여 유효한지 여부를 판단하고, 상기 공개키로 복호화된 디지털 서명정보에 포함된 스마트 미터의 주소정보를 상기 스마트 컨트랙트에 추가하여 상기 스마트 미터를 블록체인 네트워크에 새로이 참여시킴을 특징으로 하는 블록체인을 이용한 원격 검침 시스템.

청구항 12

제11항에 있어서,

상기 블록체인 네트워크에 로그인하지 않은 상태의 스마트 미터는 스마트 컨트랙트내의 로그인 함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자신의 주소정보를 추가하여 개인키로 서명하고, 작업증명과정을 거쳐 블록으로 구성하여 상기 블록체인 네트워크로 전파하고,

상기 블록체인 네트워크에 속한 스마트 미터 및 자원 또는 에너지 공급업체 시스템은, 상기 블록체인 네트워크를 통해 수신된 블록을 블록체인에 기록하며, 상기 블록체인에 블록 형태의 로그인함수를 호출하는 트랜잭션이 기록되었으면, 상기 트랜잭션에 포함된 주소정보가 스마트 컨트랙트내에 기록되었는지를 체크하고, 상기 주소정보가 스마트 컨트랙트에 기록되었으면 상기 주소정보의 스마트 미터에 대한 로그인 완료통지함을 특징으로 하는 블록체인을 이용한 원격 검침 시스템.

청구항 13

제8항에 있어서,

자원 또는 에너지 공급업체 시스템은 스마트 컨트랙트내의 날짜 업데이트 함수를 호출하는 트랜잭션을 생성하고, 자신의 주소정보를 상기 트랜잭션에 추가하고, 상기 트랜잭션을 개인키로 서명하고, 작업증명과정을

거쳐 블록으로 구성하여 상기 블록체인 네트워크를 통해 상기 블록체인 네트워크의 스마트 미터들로 전송하고,

상기 블록체인 네트워크에 속한 스마트 미터들은 상기 블록체인 네트워크를 통해 수신된 블록을 블록체인에 기록하며, 상기 블록체인에 블록 형태의 날짜 업데이트 함수를 호출하는 트랜잭션이 기록되었으면, 상기 트랜잭션에 포함된 주소정보가 자원 또는 에너지 공급업체 시스템을 지시하면, 스마트 컨트랙트의 날짜를 업데이트함을 특징으로 하는 블록체인을 이용한 원격 검침 시스템.

청구항 14

제8항 내지 제13항 중 어느 한 항에 있어서,

상기 블록체인 네트워크에 속한 스마트 미터들 또는 자원 또는 에너지 공급업체 시스템은,

트랜잭션의 생성시마다

트랜잭션을 자신의 개인키로 서명하여 블록체인 네트워크로 전파하고,

상기 블록체인 네트워크를 통해 트랜잭션이 수신될 때마다 트랜잭션이 유효한지 검증한 후에 수신된 트랜잭션을 저장하고,

미리 정해진 주기마다 수신되어 저장된 트랜잭션에 대해 작업증명과정을 거쳐 블록을 구성하여 블록을 블록체인 네트워크로 전파하고,

상기 블록체인 네트워크를 통해 블록이 수신될 때마다 수신된 블록이 유효한지 검증하고, 상기 수신된 블록이 유효하면 자신의 블록체인에 기록함을 특징으로 하는 블록체인을 이용한 원격 검침 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 수도나 전기, 가스, 열 등과 같은 자원 또는 에너지 공급량을 원격 검침하는 기술에 관한 것으로, 더욱 상세하게는 수도나 전기, 가스, 열 등과 같은 자원 또는 에너지 공급량을 검침하는 스마트 미터들과 자원 또는 에너지 공급업체의 시스템을 블록체인 네트워크로 구성하여 IOT(Internet of Things) 네트워크의 보안성 및 신뢰성을 향상시키며, 스마트 미터들과 자원 또는 에너지 공급업체 시스템 사이에 검침일 설정, 검침과 지불에 대한 스마트 컨트랙트를 적용하여 데이터의 인증, 부인방지, 무결성을 제공하는 블록체인을 이용한 원격 검침 방법 및 시스템에 관한 것이다.

배경 기술

[0002] 과거의 전기, 수도, 가스, 열량(난방) 등의 자원 또는 에너지 사용량을 검침하는 방법은 매월 검침원이 수용가를 일일이 방문하면서 해당 계량기를 확인하고, 적산수치를 읽어 검침기록부에 수기한 후, 컴퓨터에 입력하여 계산된 과금 내역을 고지서를 통해 청구하는 과정으로 이루어졌고, 아직도 이러한 직독식 검침방법이 일부 지역에서 사용되고 있다.

[0003] 상기한 직독식 검침방법에서 검침기록부에 수기하는 대신에 PDA에 입력하는 방식이 사용되고 있으나, PDA에 입력키를 눌러 입력하는 방식은 입력과정에서 입력자의 실수나 PDA의 입력정보 인식 오류로 인한 많은 민원이 발생되고 있다.

[0004] 이에 따라 인터넷망이나 전력망을 이용하여 검침하는 방법도 고려되고 있다.

[0005] 이러한 기술로는 대한민국 특허청에 수도계량기 원격검침시스템을 명칭으로 하여 특허등록된 제 1012254560000(2013.01.17)호가 있다. 이는 수도계량기; 수도 관로 내에 삽입되며, 상기 수도 관로 내 압력 데이터를 검출하는 압력계 및 압력변환기; 상기 수도계량기에 일체형으로 결합되며, 전자감응센서를 이용하여 유량 데이터를 검출하는 신호검출기 및 통신망을 통해 관리 서버에 연결하며, 상기 신호검출기에서 출력되는 상기 유량 데이터를 분석하고, 상기 유량 데이터의 분석 결과를 분석 데이터로 가공하며, 상기 가공된 분석 데이터를 상기 관리 서버로 전송하는 자료수집 분석 및 송출기를 포함하는 것을 특징으로 하는 수도계량기 원격검침시스템을 개시하고 있다.

[0006] 그리고 대한민국 특허청에 도로조명 무선 원격관제시스템을 이용한 상하수도 무인검침서비스 통합관제시스템을

명칭으로 하여 특허등록된 제1016851900000(2016.12.05)호가 있다. 이는 개별적으로 각각 운영되고 있는 도로조명 무선 원격관제시스템과 상수도 원격검침시스템을 매우 저렴한 비용으로 하나의 통합 시스템으로 운영할 수 있도록 하여 시스템 구축비용은 물론 통신 및 유지보수비용을 크게 절감하면서도 도로조명 무선 원격시스템을 기반으로 하여 보다 다양한 대민무인서비스를 통합적으로 운영할 수 있는 구조를 갖도록 한 도로조명 무선 원격관제시스템을 이용한 상수도 무인검침서비스 통합관제시스템을 개시하고 있다.

[0007] 이와 같이 종래에는 다양한 형태의 무인 원격 검침을 위한 기술이 제안되어 상용화되고 있다. 그러나 원격 검침을 위해 사용되는 네트워크에 대한 보안성과 신뢰성이 미흡한 문제가 있었고, 악의적인 공격자에 의해 데이터의 위/변조 가능성이 높은 문제도 있었다.

[0008] 상기한 바와 같이 종래에는 무인 원격 검침을 위한 시스템에 대한 보안성과 신뢰성을 향상시키고 데이터의 무결성, 악의적인 공격자의 데이터 위/변조를 원천적으로 방지할 수 있게 하는 기술의 개발이 절실하게 요망되었다.

선행기술문헌

특허문헌

- [0009] (특허문헌 0001) 대한민국 특허등록 제1012254560000호
(특허문헌 0002) 대한민국 특허등록 제1016851900000호
(특허문헌 0003) 대한민국 특허등록 제10-1685190호
(특허문헌 0004) 대한민국 특허공개 제1020100022625호

발명의 내용

해결하려는 과제

- [0010] 본 발명은 수도나 전기, 가스, 열 등과 같은 자원 또는 에너지 공급량을 검침하는 스마트 미터들과 자원 또는 에너지 공급업체의 시스템을 블록체인 네트워크로 구성하여 IOT(Internet of Things) 네트워크의 보안성 및 신뢰성을 향상시키며, 스마트 미터들과 자원 또는 에너지 공급업체 시스템 사이에 검침일 설정, 검침과 지불에 대한 스마트 컨트랙트를 적용하여 데이터의 인증, 부인방지, 무결성을 제공하는 블록체인을 이용한 원격 검침 방법 및 시스템을 제공하는 것을 그 목적으로 한다.

과제의 해결 수단

- [0011] 상기한 목적을 달성하기 위한 본 발명에 따르는 블록체인을 이용한 원격 검침 방법은, 자원 또는 에너지 공급업체 시스템 및 제1 내지 제N스마트 미터를 블록체인 네트워크로 구성하는 단계; 상기 자원 또는 에너지 공급업체 시스템은 블록체인을 이용한 원격 검침을 위한 지불함수가 규정하며 상기 블록체인 네트워크에 참여한 스마트 미터들에 대한 주소정보를 기록한 스마트 컨트랙트를 생성하여 상기 스마트 미터들로 전송하는 단계; 상기 스마트 미터들이 상기 스마트 컨트랙트가 수신되면 블록체인에 기록하는 단계; 상기 스마트 미터들 중 어느 하나는 스마트 컨트랙트내 지불함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자원 또는 에너지 공급에 대한 검침값과 자신의 주소정보를 추가하고, 개인키로 서명하고, 작업증명과정을 거쳐 블록으로 구성하여 상기 블록체인 네트워크를 통해 상기 자원 또는 에너지 공급업체 시스템으로 전송하는 단계;를 구비함을 특징으로 한다.

발명의 효과

- [0012] 본 발명은 수도나 전기, 가스, 열 등과 같은 자원 또는 에너지 공급량을 검침하는 스마트 미터들과 자원 또는 에너지 공급업체의 시스템을 블록체인 네트워크로 구성하여 IOT(Internet of Things) 네트워크의 보안성 및 신뢰성을 향상시키며, 스마트 미터들과 자원 또는 에너지 공급업체 시스템 사이에 검침일 설정, 검침과 지불에 대한 스마트 컨트랙트를 적용하여 데이터의 인증, 부인방지, 무결성을 제공할 수 있는 효과를 야기한다.

도면의 간단한 설명

- [0013] 도 1은 본 발명의 바람직한 실시예에 따르는 블록체인을 이용한 원격 검침 시스템의 구성도.

도 2는 본 발명의 바람직한 실시예에 따르는 스마트 미터의 구성도.

도 3은 본 발명의 바람직한 실시예에 따르는 스마트 컨트랙트의 구조도.

도 4 내지 도 10은 본 발명의 바람직한 실시예에 따르는 블록체인을 이용한 원격 검침 및 지불 방법의 절차도.

발명을 실시하기 위한 구체적인 내용

- [0014] 본 발명은 수도나 전기, 가스, 열 등과 같은 자원 또는 에너지 공급량을 검침하는 스마트 미터들과 자원 또는 에너지 공급업체의 시스템을 블록체인 네트워크로 구성하여 IOT(Internet of Things) 네트워크의 보안성 및 신뢰성을 향상시키며, 스마트 미터들과 자원 또는 에너지 공급업체 시스템 사이에 검침일 설정, 검침과 지불에 대한 스마트 컨트랙트를 적용하여 데이터의 인증, 부인방지, 무결성을 제공한다.
- [0015] <블록체인을 이용한 원격 검침 시스템의 구성>
- [0016] 본 발명의 바람직한 실시예에 따르는 블록체인을 이용한 원격 검침 시스템의 구성을 도 1을 참조하여 상세히 설명한다.
- [0017] 상기 블록체인을 이용한 원격 검침 시스템은 자원 또는 에너지 공급업체 시스템(100)과 제1 내지 제N스마트 미터(1021~102N)로 구성되며, 상기 자원 또는 에너지 공급업체 시스템(100)과 제1 내지 제N스마트 미터(1021~102N)는 본 발명의 바람직한 실시예에 따라 블록체인 네트워크를 형성하는 노드들로 동작한다.
- [0018] 상기 자원 또는 에너지 공급업체 시스템(100)은 제1 내지 제N스마트 미터(1021~102N)와 통신하여 블록체인을 이용한 원격 검침 서비스를 제공한다. 본 발명에 따르는 블록체인을 이용한 원격 검침은 스마트 컨트랙트 기록 및 초기설정, 블록체인 네트워크에 신규 노드인 스마트 미터를 참여시키고, 블록체인 네트워크에 신규 노드인 스마트 미터가 로그인하도록 하고, 원격검침 및 과금, 과금금액 지불을 가능하게 하고, 날짜 업데이트를 이행하고, 쿼리를 처리하는 기능으로 구성된다. 특히 각 과정마다 생성되는 트랜잭션은 블록으로 변환되어 블록체인 네트워크를 통해 전파되어 블록체인 네트워크의 노드들인 스마트 미터들(1021~102N) 및 자원 또는 에너지 공급업체 시스템(100)의 블록체인에 기록되며, 이는 트랜잭션을 부인방지 및 무결성있게 기록함과 악의적 공격자에 의한 데이터 위변조가 불가능한 상태로 기록될 수 있게 된다.
- [0019] <스마트 미터의 구성>
- [0020] 상기한 도 1의 제1 내지 제N스마트 미터(1021~102N)의 구성 및 동작은 동일하므로, 어느 한 스마트 미터의 구성만을 도 2를 참조하여 상세히 설명한다.
- [0021] 상기 스마트 미터는 제어장치(200)와 메모리부(202)와 검침장치(204)와 통신장치(206)로 구성된다. 상기 제어장치(200)는 상기 스마트 미터의 각부에 대해 전반적으로 제어함은 물론이며, 본 발명의 바람직한 실시예에 따라 블록체인 네트워크에 참여하여 블록체인을 이용한 원격 검침 서비스를 위한 동작을 이행한다.
- [0022] 상기 메모리부(202)는 상기 제어장치(200)의 제어 프로그램의 실행을 위한 각종 정보를 저장하는 저장영역을 제공한다.
- [0023] 상기 검침장치(204)는 수도 등과 같은 자원 또는 전기, 가스, 온수 등과 같은 에너지를 제공량을 검침하고, 그 검침정보를 상기 제어장치(200)에 제공한다.
- [0024] 상기 통신장치(206)는 상기 제어장치(200)와 블록체인 네트워크 사이의 통신을 담당한다.
- [0025] <스마트 컨트랙트의 구조>
- [0026] 도 3은 본 발명의 바람직한 실시예에 따르는 스마트 컨트랙트의 구조를 도시한 것이다.
- [0027] 상기 스마트 컨트랙트는 계약 조건 및 조건에 따른 동작을 명시하는 함수들과 블록체인 멤버 리스트를 포함한다. 예를들어, Function A의 경우에는 지불 함수로서 스마트 미터에서 사용 가능한 함수이고, Function B의 경우에는 날짜를 갱신하는 함수로서 자원 또는 에너지 공급업체 시스템(100)에서 사용 가능한 함수이다. 또한 상기 Function A를 사용하는 스마트 미터는 제한될 수도 있다. 그리고 상기 각 함수에는 함수의 결과정보를 블록체인내의 노드들에게 전파하기 위한 이벤트가 배치된다. 상기 이벤트는 스마트 컨트랙트내 호출된 함수에 대한 결과정보 또는 스마트 컨트랙트 생성자가 임의로 정한 정보를 블록체인내의 노드들로 제공하기 위한 것이다. 상기 블록체인 멤버 리스트 Blockchain_member.list는 리스트로 정의되어 스마트 미터들의 블록체인 네트워크 주소정보를 저장하는 형태이며, 자원 또는 에너지 공급업체 시스템(100)은 새로이 인증된 스마트 미터가 추

가될 때마다 추가된 스마트 미터의 주소정보를 상기 블록체인 멤버 리스트에 기록한다.

[0028] <블록체인을 이용한 원격 검침 방법의 절차>

[0029] 상기한 바와 같이 구성되는 본 발명의 바람직한 실시예에 따르는 블록체인을 이용한 원격 검침 시스템에 적용가능한 원격 검침 방법을 도면을 참조하여 상세히 설명한다.

[0030] -스마트 컨트랙트 기록 및 초기설정 과정-

[0031] 먼저 본 발명의 바람직한 실시예에 따라 스마트 컨트랙트를 블록체인 네트워크에 기록하고 초기설정을 이행하는 과정을 도 4를 참조하여 설명한다.

[0032] 자원 또는 에너지 공급업체 시스템(100)은 스마트 컨트랙트를 생성하며(300단계), 이 스마트 컨트랙트에는 원격 검침을 위한 함수들과 블록체인 네트워크에 속하는 스마트 미터들의 주소정보들이 기록된다. 상기 스마트 컨트랙트가 생성되면, 상기 자원 또는 에너지 공급업체 시스템(100)은 상기 스마트 컨트랙트를 작업증명과정(POW, Proof of work)를 거쳐 블록으로 구성하고, 상기 블록으로 변환된 스마트 컨트랙트를 블록체인 네트워크의 노드들 각각으로 전송한다(302단계). 상기 노드들 각각은 블록의 유효성을 검증하고 그 검증결과에 따라 자신의 블록체인에 해당 블록을 다음 블록으로 이어 기록한다(304단계). 이로서 본 발명의 스마트 컨트랙트는 부인방지 및 무결성있게 기록함과 악의적 공격자에 의한 데이터 위변조가 불가능한 상태로 기록될 수 있게 된다.

[0033] 이후 상기 자원 또는 에너지 공급업체 시스템(100)은 스마트 컨트랙트내 초기설정함수를 호출하는 트랜잭션을 생성하고(308단계), 상기 트랜잭션에 초기설정날짜(년,월), 검침일 및 자원 또는 에너지 공급단가를 상기 생성한 트랜잭션에 추가한다(310단계). 이후 상기 자원 또는 에너지 공급업체 시스템(100)은 상기 트랜잭션을 블록체인 네트워크의 노드들로 전송한다(312단계).

[0034] 상기 블록체인 네트워크의 노드들, 즉 스마트 미터들 각각은 초기설정함수를 호출하는 트랜잭션이 수신되면(316단계), 자원 또는 에너지 공급업체 시스템(100)이 송신한 초기설정함수를 호출하는 트랜잭션인지를 체크한다(318단계). 상기 초기설정함수를 호출하는 트랜잭션이 자원 또는 에너지 공급업체 시스템(100)이 송신한 초기설정함수이면, 상기 스마트 미터들은 상기 트랜잭션에 포함된 초기설정날짜, 검침일 및 공급단가를 스마트 컨트랙트에 기록함과 아울러 상기 초기설정함수에 기록된 초기설정날짜 및 자원 또는 에너지 공급단가를 기록하고 초기설정완료 이벤트를 발생한다(322,324단계). 상기 초기설정완료 이벤트는 자신의 주소정보와 초기설정완료료를 지시하는 응답정보를 상기 자원 또는 에너지 공급업체 시스템(100)으로 반환하는 것일 수 있다.

[0035] 상기한 바와 다르게 상기 초기설정함수를 포함하는 트랜잭션이 자원 또는 에너지 공급업체 시스템(100)이 송신한 초기설정함수가 아니면, 상기 스마트 미터들은 거절 이벤트를 발생한다. 상기 거절이벤트는 자신의 주소정보와 초기설정거부를 지시하는 응답정보를 상기 자원 또는 에너지 공급업체 시스템(100)으로 반환하는 것일 수 있다.

[0036] -블록체인 네트워크에 신규 노드 참여과정-

[0037] 그리고 본 발명의 바람직한 실시예에 따라 상기한 블록체인 네트워크에 신규 노드인 스마트 미터를 참여시키는 과정을 도 5를 참조하여 설명한다.

[0038] 신규 노드로 참여하고자 하는 스마트 미터는 고유한 공개키와 개인키 쌍을 생성하고, 자신의 주소정보, 공개키와 개인키 쌍을 공개키로 암호화하여 디지털 서명정보를 생성하여 자원 또는 에너지 공급업체 시스템(100)으로 전송하여 블록체인 네트워크 참여를 요청한다(400,402단계).

[0039] 상기 디지털 서명정보를 수신한 자원 또는 에너지 공급업체 시스템(100)은 상기 디지털 서명정보를 공개키로 복호화하여 유효한지 여부를 판단하고, 상기 디지털 서명정보가 유효하면, 상기 디지털 서명정보에 포함된 주소정보를 스마트 컨트랙트의 블록체인 멤버 리스트 Blockchain_member.list에 추가하여 기록함으로써 상기 인증요청한 스마트 미터를 블록체인 네트워크에 참여시킨다(404,408,412,414단계). 이와 같이 갱신된 스마트 컨트랙트에 대한 정보는 블록체인 네트워크에 포함된 노드들의 블록체인에 기록된다.

[0040] -블록체인 네트워크에 로그인하는 과정-

[0041] 그리고 본 발명의 바람직한 실시예에 따라 상기한 블록체인 네트워크에 스마트 미터가 로그인하는 과정을 도 6을 참조하여 설명한다.

[0042] 로그인하고자 하는 스마트 미터는 스마트 컨트랙트내 로그인 함수를 호출하는 트랜잭션을 생성하고(500단계),

상기 트랜잭션에 자신의 주소정보를 추가하고 개인키로 서명한다(502,504단계). 이후 상기 스마트 미터는 상기 트랜잭션을 작업증명과정(POW)을 거쳐 블록으로 구성하여 블록체인 네트워크의 노드들로 전송하며, 상기 블록체인 네트워크의 노드들은 상기 블록으로 변환된 트랜잭션을 블록체인에 기록한다(506,508단계).

[0043] 상기 블록체인 네트워크의 노드들, 즉 자원 또는 에너지 공급업체 시스템(100)이나 스마트 미터들은 블록체인에 새로운 트랜잭션이 기록되면(512단계), 그 트랜잭션이 로그인함수를 호출하는 트랜잭션이고(514단계), 상기 트랜잭션에 포함된 주소정보가 스마트 컨트랙트내에 신규 추가된 노드에 대한 주소정보인지를 체크한다(518단계). 상기 블록체인 네트워크의 노드들은 상기 트랜잭션에 포함된 주소정보가 스마트 컨트랙트내에 신규 추가된 노드에 대한 주소정보이면, 상기 스마트 미터에 대한 로그인을 승인하고 로그인 완료 이벤트를 생성한다(520단계). 상기 로그인 완료 이벤트는 상기 자신의 주소정보와 로그인 완료 대상의 노드의 주소정보를 포함하는 로그인 승인 통지정보를 블록체인 네트워크의 자원 또는 에너지 공급업체 시스템(100)으로 제공하는 것일 수 있다.

[0044] 상기한 바와 다르게 상기 트랜잭션에 포함된 주소정보가 스마트 컨트랙트내에 신규 추가된 노드에 대한 주소정보가 아니면, 상기 스마트 미터에 대한 로그인을 거절하고 거절 이벤트를 생성한다(522단계). 상기 거절 이벤트는 상기 자신의 주소정보와 로그인 거절 대상의 노드의 주소정보를 포함하는 로그인 거절 통지정보를 블록체인 네트워크의 자원 또는 에너지 공급업체 시스템(100)으로 제공하는 것일 수 있다.

[0045] -검침 및 지불과정-

[0046] 그리고 본 발명의 바람직한 실시예에 따라 블록체인 네트워크에 스마트 미터가 자원 또는 에너지 사용량에 대한 검침 및 지불을 이행하는 과정을 도 7을 참조하여 설명한다.

[0047] 자원 또는 에너지 사용량에 대한 지불을 이행하고자 하는 스마트 미터는 지불 함수를 호출하는 트랜잭션을 생성하고(600단계), 상기 트랜잭션에 자신의 주소정보와 미리 설정된 검침주기내 검침값을 추가하고 개인키로 서명한다(602,604단계). 여기서 상기 검침값은 검침장치에 의해 획득된다.

[0048] 이후 상기 스마트 미터는 상기 트랜잭션을 작업증명과정(POW)을 거쳐 블록으로 구성하여 블록체인 네트워크의 노드들로 전송하며, 상기 블록체인 네트워크의 노드들은 상기 블록으로 변환된 트랜잭션을 블록체인에 기록한다(606,608단계).

[0049] 상기 자원 또는 에너지 공급업체 시스템(100)은 블록체인에 새로운 트랜잭션이 기록되면, 그 트랜잭션이 지불함수를 호출하는 트랜잭션이고, 상기 트랜잭션에 포함된 주소정보가 스마트 컨트랙트내에 기록된 주소정보이고 개인키가 유효한지를 체크한다(612단계). 상기 자원 또는 에너지 공급업체 시스템(100)은 트랜잭션이 지불함수를 호출하는 트랜잭션이고, 상기 트랜잭션에 포함된 주소정보가 스마트 컨트랙트내에 기록된 주소정보이고 개인키가 유효하면, 상기 트랜잭션에 포함된 검침값에 대한 과금금액을 산출하고(614,618단계), 상기 트랜잭션에 포함된 주소정보에 따르는 고객의 잔고를 상기 과금금액만큼 감소시키고 자원 또는 에너지 공급업체 시스템(100)의 잔고를 상기 과금금액만큼 증액시켜 지불을 완료한다(620단계). 또한 상기 자원 또는 에너지 공급업체(100)는 상기 주소정보와 검침값, 트랜잭션이 수신된 검침일, 과금금액 등을 대응되게 기록하여, 스마트 미터측의 쿼리에 대응할 수 있게 한다. 이후 상기 자원 또는 에너지 공급업체(100)는 상기 지불 완료에 따른 지불 완료 이벤트를 발생한다(622단계). 상기 지불 완료 이벤트는 지불요청한 노드로 지불완료되었음을 통지하는 정보를 전송하는 것일 수 있다.

[0050] -날짜 업데이트 과정-

[0051] 그리고 본 발명의 바람직한 실시예에 따라 상기한 블록체인 네트워크의 노드들에 대한 날짜를 업데이트하는 과정을 도 8을 참조하여 설명한다.

[0052] 상기 자원 또는 에너지 공급업체 시스템(100)은 스마트 컨트랙트내 날짜 업데이트 함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자신의 주소정보를 추가한다(700,702단계). 이후 상기 자원 또는 에너지 공급업체 시스템(100)은 상기 트랜잭션을 개인키로 서명한 후에 작업증명과정(POW)을 거쳐 블록으로 구성하고, 상기 블록으로 변환된 트랜잭션을 블록체인 네트워크의 노드들로 전송하여 블록체인에 블록으로 변환된 트랜잭션을 기록한다(704, 706, 708단계).

[0053] 상기 스마트 미터들 각각은 블록체인에 새로운 트랜잭션이 기록되었으면(710단계), 상기 새로운 트랜잭션이 에너지 공급업체 시스템에 의해 생성된 날짜 업데이트 함수를 호출하는 트랜잭션인지를 체크한다(712단계). 상기 새로운 트랜잭션이 상기 에너지 공급업체 시스템에 의해 생성된 날짜 업데이트 함수를 호출하는 트랜잭션이면, 상기 스마트 미터들 각각은 자신의 블록체인에 기록된 스마트 컨트랙트에 기록된 MONTH가 12인지를 체크한다.

상기 MONTH가 12이면, 상기 스마트 미터들 각각은 상기 스마트 컨트랙트에 기록된 YEAR를 1증가하고 MONTH는 1로 초기화한다. 이와달리 상기 MONTH가 12가 아니면, 상기 스마트 미터들 각각은 상기 스마트 컨트랙트에 기록된 MONTH를 1증가한다. 이후 스마트 미터들 각각은 날짜 업데이트 완료 이벤트를 발생한다(722단계). 상기 날짜 업데이트 완료 이벤트는 상기 자신의 주소정보를 포함하는 날짜 업데이트 완료 통지정보를 블록체인 네트워크의 자원 또는 에너지 공급업체 시스템(100)으로 제공하는 것일 수 있다.

[0054] 상기한 바와 다르게 날짜 업데이트 함수를 호출하는 트랜잭션이 에너지 공급업체 시스템(100)에 의해 생성된 것이 아니면, 상기 스마트 미터들 각각은 날짜 업데이트를 거절하는 거절이벤트를 발생한다(714단계).

[0055] -쿼리 처리 과정-

[0056] 그리고 본 발명의 바람직한 실시예에 따라 상기한 블록체인 네트워크의 노드들 중 하나인 스마트 미터로부터의 쿼리를 처리하는 과정을 도 9를 참조하여 설명한다.

[0057] 상기 블록체인 네트워크의 노드들 중 하나인 스마트 미터는 스마트 컨트랙트내 쿼리함수를 호출하는 트랜잭션을 생성하고, 상기 트랜잭션에 자신의 주소정보 및 쿼리날짜를 추가한다(800,802단계). 이후 상기 스마트 미터는 상기 트랜잭션을 개인키로 서명한 후에 작업증명과정(POW)을 거쳐 블록으로 구성하고, 상기 블록으로 변환된 트랜잭션을 블록체인 네트워크의 노드들로 전송하여 블록체인에 블록으로 변환된 트랜잭션을 기록한다(804, 806, 808단계).

[0058] 상기 자원 또는 에너지 공급업체 시스템(100)은 블록체인에 새로운 트랜잭션이 기록되면, 상기 새로운 트랜잭션이 쿼리함수를 호출하는 트랜잭션이고 상기 트랜잭션을 생성한 스마트 노드가 스마트 컨트랙트에 주소정보가 기록된 유효한 스마트 노드인지를 체크한다(814,816단계).

[0059] 상기 새로운 트랜잭션이 쿼리함수를 호출하는 트랜잭션이고 상기 트랜잭션을 생성한 스마트 노드가 유효한 스마트 노드이면, 상기 자원 또는 에너지 공급업체 시스템(100)은 상기 트랜잭션에 포함된 주소정보와 쿼리날짜, 즉 검침값이 제공된 검침일에 대응되게 기록된 검침값, 과금금액, 주소정보를 포함하는 응답정보를 생성하여 상기 스마트 노드로 전송하는 응답 이벤트를 발생한다(820단계).

[0060] <트랜잭션을 블록체인에 기록하는 과정>

[0061] 본 발명에 따르는 블록체인을 이용한 원격 검침은 스마트 컨트랙트 기록 및 초기설정 과정, 블록체인 네트워크에 신규 노드인 스마트 미터를 참여시키는 과정, 블록체인 네트워크에 신규 노드인 스마트 미터가 로그인하는 과정, 원격검침 및 과금, 과금금액 지불과정, 날짜 업데이트 과정, 쿼리 처리 과정으로 구성되며, 각 과정마다 트랜잭션이 블록으로 변환되어 블록체인 네트워크를 통해 전파되어 블록체인 네트워크의 노드들인 스마트 미터들(1021~102N) 및 자원 또는 에너지 공급업체 시스템(100)의 블록체인에 기록되며, 이는 트랜잭션을 부인방지 및 무결성있게 기록함과 악의적 공격자에 의한 데이터 위변조가 불가능한 상태로 기록될 수 있게 된다.

[0062] 이제 본 발명의 바람직한 실시예에 따라 상기 트랜잭션을 블록체인에 기록하는 과정을 도 10을 참조하여 설명한다.

[0063] 상기 블록체인 네트워크의 노드들 각각은 블록체인을 이용한 원격 검침을 위해 트랜잭션이 생성되면, 상기 트랜잭션을 자신의 개인키로 서명하여 블록체인 네트워크로 전파한다(900,902단계).

[0064] 상기 블록체인 네트워크의 노드들 각각은 트랜잭션이 수신되면, 상기 트랜잭션의 개인키 서명을 토대로 유효여부를 판단하고, 상기 트랜잭션이 유효하면 상기 트랜잭션을 저장한다(904, 906,908단계). 이와달리 상기 트랜잭션이 유효하지 않으면 거절이벤트를 발생하여 블록체인 네트워크로 전파한다(910단계).

[0065] 상기 블록체인 네트워크의 노드들 각각은 미리 정해진 주기마다 해당 주기동안 수신된 트랜잭션이 있는지를 체크한다(912,914단계). 상기 주기동안 수신된 트랜잭션이 있으면, 상기 블록체인 네트워크의 노드들은 수신된 트랜잭션에 대해 작업증명과정(POW)을 거쳐 블록으로 구성한다(916단계). 상기 블록체인 네트워크의 노드들 각각은 작업증명과정(POW)을 거쳐 생성된 블록을 블록체인 네트워크로 전파한다(918단계).

[0066] 상기 블록체인 네트워크의 노드들 각각은 새로운 블록이 전파되었으면, 수신된 블록이 유효한지를 체크하고, 수신된 블록이 유효하면 수신된 블록을 자신을 갖고 있는 N개의 블록을 포함하는 블록체인의 N+1블록으로 이어 기록한다(916단계). 상기한 바와 달리 상기 수신된 블록이 유효하지 않으면 거절 이벤트를 발생하여 블록체인 네트워크로 전파한다(914단계).

부호의 설명

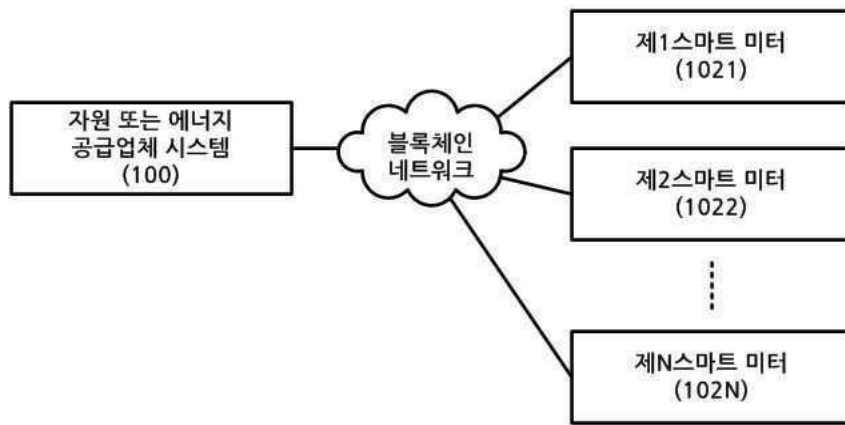
[0067]

100 : 자원 또는 에너지 공급업체 시스템

1021~102N : 제1 내지 제N스마트 미터

도면

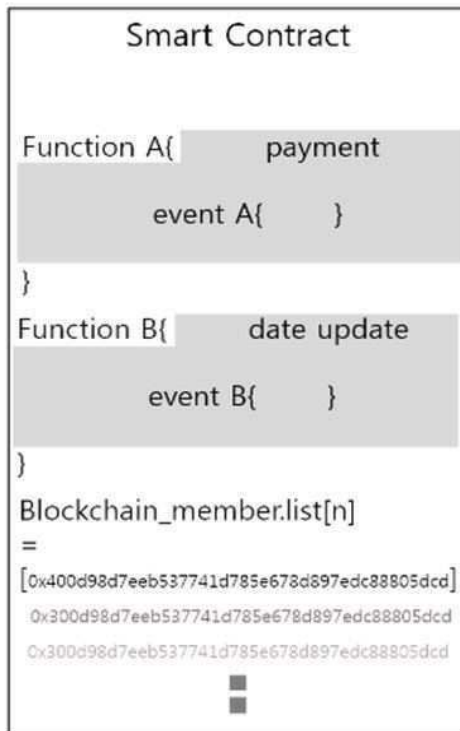
도면1



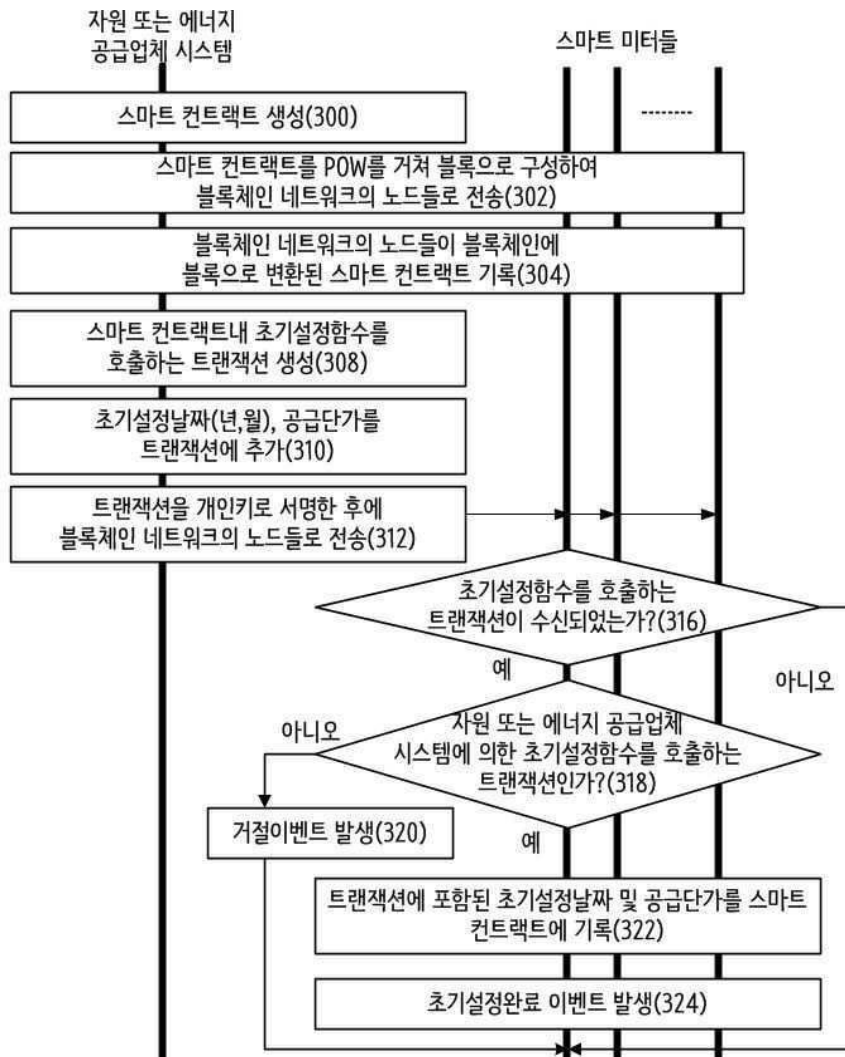
도면2



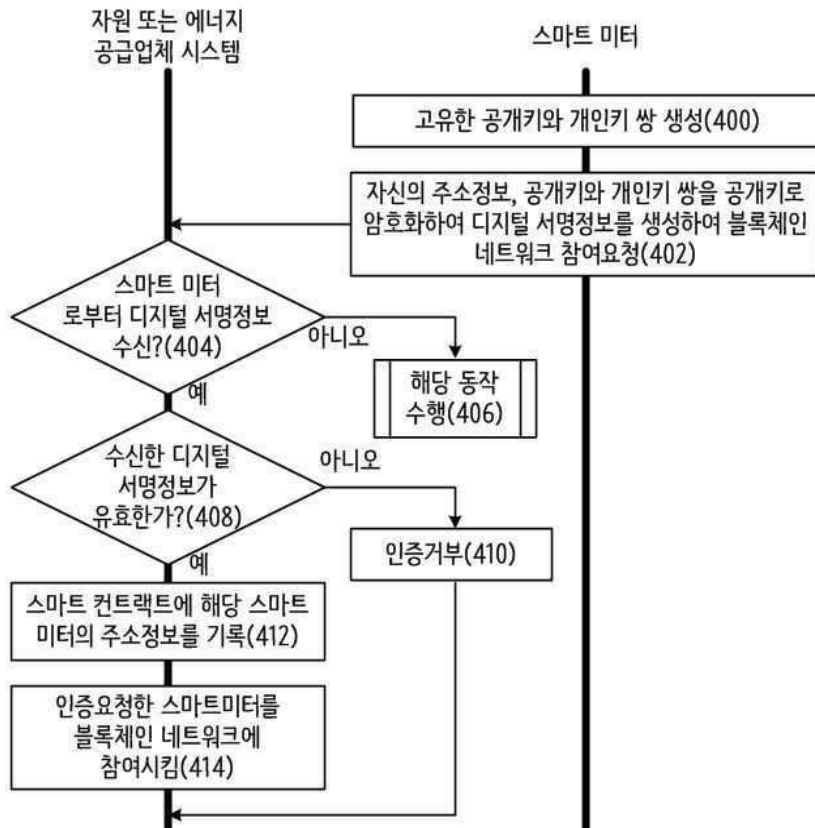
도면3



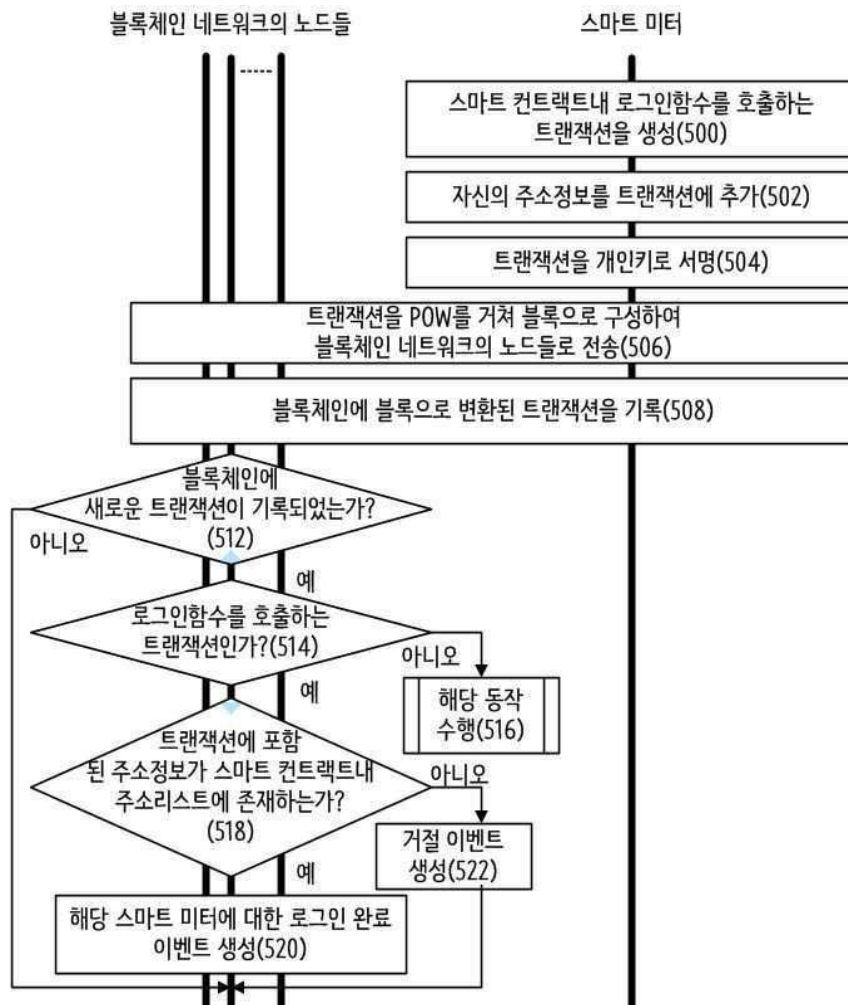
도면4



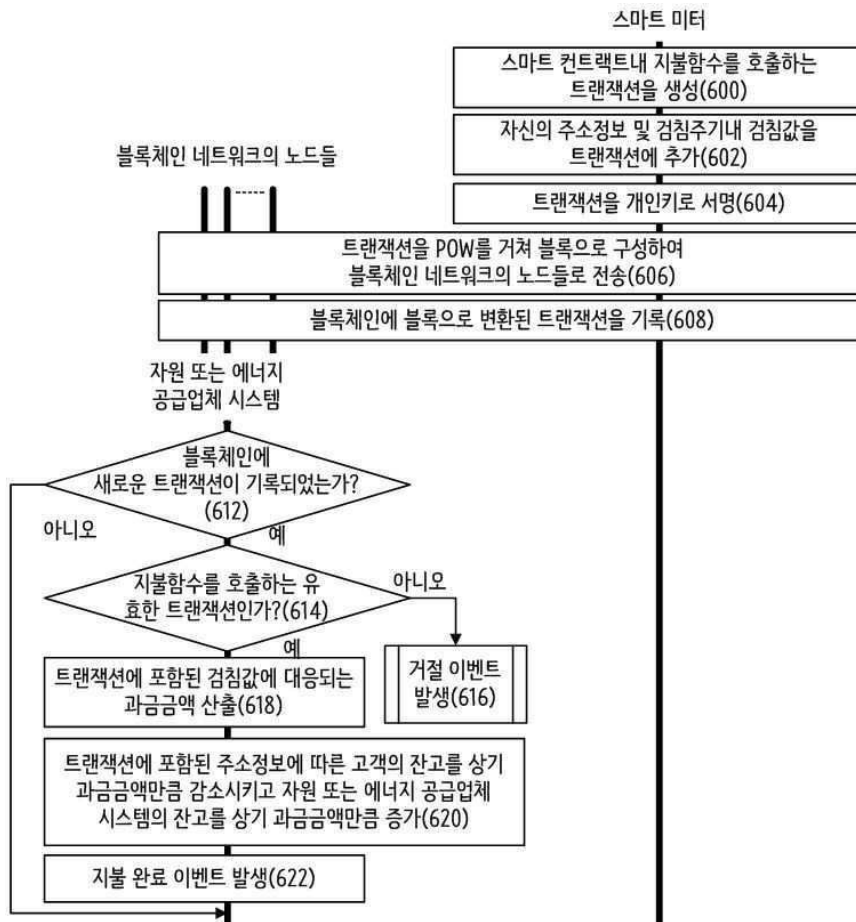
도면5



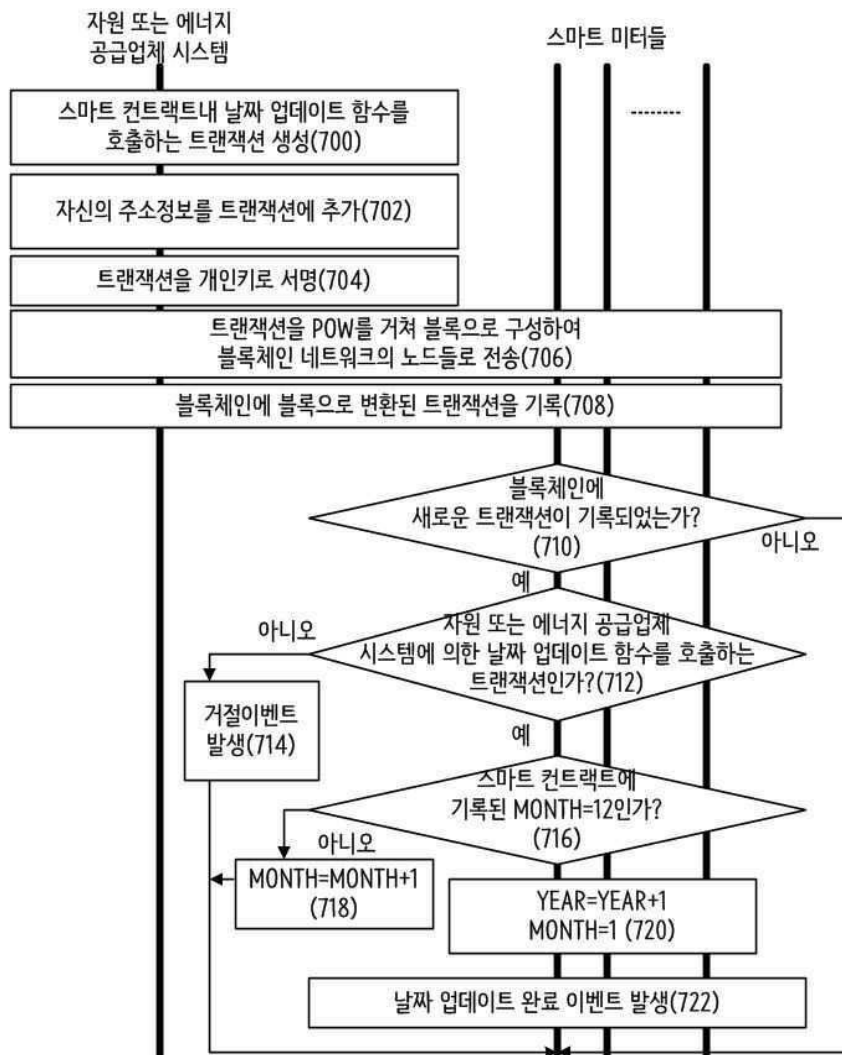
도면6



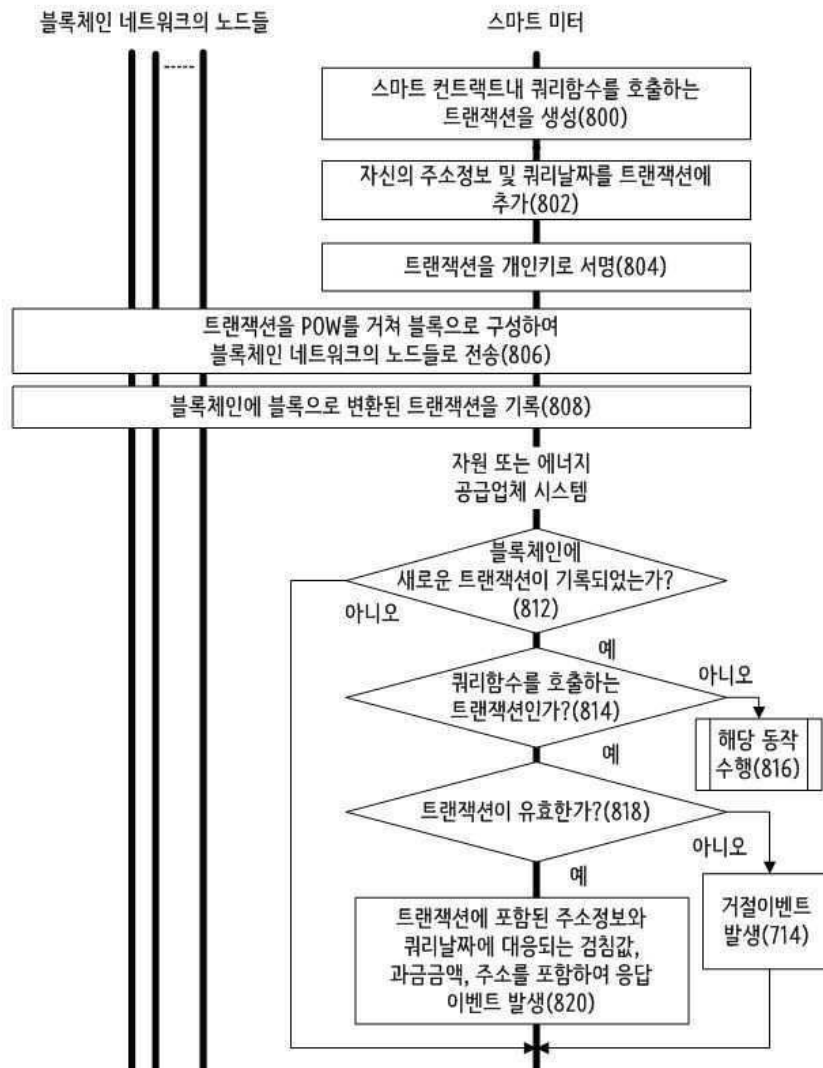
도면7



도면8



도면9



도면10

