(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년09월06일
(11) 등록번호 10-2575305
(24) 등록일자 2023년09월01일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/14* (2012.01)
G06Q 20/42 (2012.01) *H04L 9/40* (2022.01)
(52) CPC특허분류
G06Q 20/38215 (2013.01)
G06Q 20/145 (2013.01)
(21) 출원번호 10-2021-0097902
(22) 출원일자 2021년07월26일
심사청구일자 2021년07월26일
(65) 공개번호 10-2023-0016425
(43) 공개일자 2023년02월02일
(56) 선행기술조사문헌
KR101933134 B1*
KR1020190038939 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 광진구 능동로 209 세종대학교 대양AI센터 708호
이신철
서울특별시 광진구 뚝섬로49길 68, 203호(자양동, 연준빌)
(74) 대리인
두호특허법인

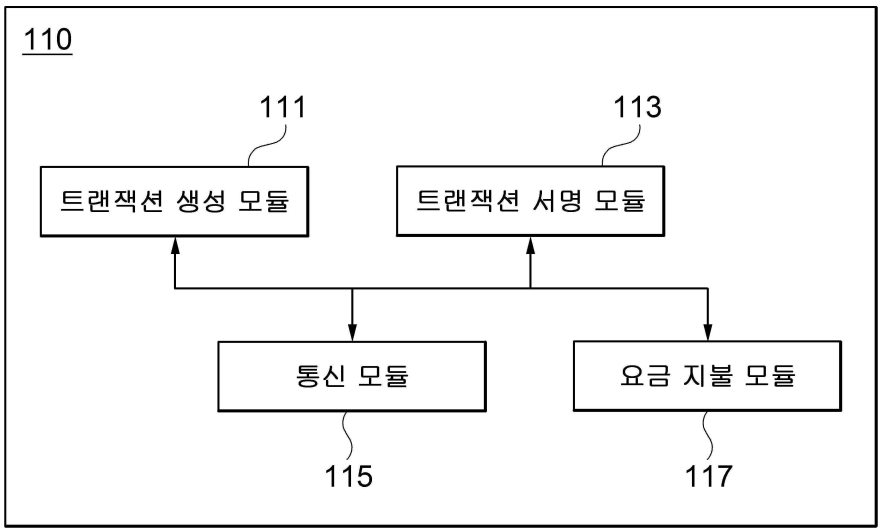
전체 청구항 수 : 총 30 항 심사관 : 박성웅

(54) 발명의 명칭 **요금 처리 방법과 이를 수행하기 위한 컴퓨팅 장치**

(57) 요 약

요금 처리 방법과 이를 수행하기 위한 컴퓨팅 장치가 개시된다. 일 실시예에 따른 사용자 단말로 동작되는 컴퓨팅 장치는, 인증서로 인증된 가명(Pseudonym) 및 상기 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 트랜잭션 생성 모듈; 상기 생성된 트랜잭션에 서명하는 트랜잭션 서명 모듈; 상기 서명된 트랜잭션을 상기 블록체인 망에 게시하는 통신 모듈; 및 상기 블록체인 망에 포함된 청구 센터로부터 상기 가명 앞으로 청구된 에너지 요금을 지불하는 요금 지불 모듈을 포함한다.

대 표 도 - 도2



(52) CPC특허분류
G06Q 20/3825 (2013.01)
G06Q 20/3829 (2013.01)
G06Q 20/383 (2013.01)
G06Q 20/42 (2013.01)
H04L 63/0421 (2013.01)
H04L 63/0823 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711117818
과제번호 2020R1F1A1072275
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)(R&D)
연구과제명 무인항공기를 위한 블록체인 기반 보안 강화 기술 개발
기 여 율 1/2
과제수행기관명 세종대학교
연구기간 2020.06.01 ~ 2021.02.28
이 발명을 지원한 국가연구개발사업
과제고유번호 1711126109
과제번호 2018-0-01423-004
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 대학ICT연구센터육성지원사업
연구과제명 지능형 비행로봇 융합 기술 연구
기 여 율 1/2
과제수행기관명 세종대학교 산학협력단
연구기간 2021.01.01 ~ 2021.12.31
공지예외적용 : 있음

명 세 서

청구범위

청구항 1

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 사용자 단말로 동작되는 컴퓨팅 장치로서,

인증서로 인증된 가명(Pseudonym) 및 상기 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 트랜잭션 생성 모듈;

상기 생성된 트랜잭션에 서명하는 트랜잭션 서명 모듈;

상기 서명된 트랜잭션을 상기 블록체인 망에 게시하는 통신 모듈; 및

상기 블록체인 망에 포함된 청구 센터로부터 상기 가명 앞으로 청구된 에너지 요금을 지불하는 요금 지불 모듈을 포함하며,

상기 통신 모듈은,

상기 블록체인 망에 포함된 인증 기관으로부터 상기 가명에 대한 인증서를 획득하고,

상기 트랜잭션 생성 모듈은,

상기 가명을 생성하고, 상기 가명, 상기 가명에 대한 인증서 및 상기 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는, 컴퓨팅 장치.

청구항 2

삭제

청구항 3

청구항 1항에 있어서,

상기 트랜잭션 서명 모듈은,

트랜잭션 공개키 및 상기 트랜잭션 공개키에 대응되는 트랜잭션 개인키를 생성하고, 상기 트랜잭션을 상기 트랜잭션 개인키로 서명하는, 컴퓨팅 장치.

청구항 4

청구항 1항에 있어서,

상기 요금 지불 모듈은,

상기 블록체인 망에서 사용 가능한 암호화폐를 이용하여 상기 에너지 요금을 지불하는, 컴퓨팅 장치.

청구항 5

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 청구 센터로 동작되는 컴퓨팅 장치로서,

상기 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 상기 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 가명 검증 모듈;

상기 검증된 가명에 대응되는 에너지 사용 정보를 식별하는 식별 모듈; 및

상기 검증된 가명 중 적어도 일부 가명으로 상기 식별된 에너지 사용 정보에 따른 에너지 요금을 청구하는 요금 청구 모듈을 포함하는, 컴퓨팅 장치.

청구항 6

청구항 5항에 있어서,

상기 가명 검증 모듈은,

상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하고, 상기 가명에 대한 상기 블룸 필터의 보고 결과에 기초하여 상기 가명의 유효성을 검증하는, 컴퓨팅 장치.

청구항 7

청구항 5항에 있어서,

상기 가명 검증 모듈은,

상기 블록체인에서 상기 가명이 포함된 트랜잭션을 탐색하고, 상기 가명에 대한 인증서를 검증함으로써 상기 가명의 유효성을 검증하는, 컴퓨팅 장치.

청구항 8

청구항 5항에 있어서,

상기 청구에 따라 지불된 에너지 요금과 상기 에너지 요금이 지불된 가명에 대한 에너지 소비 데이터를 확인함으로써 상기 청구에 따라 지불된 에너지 요금의 정상 지불 여부를 검증하는 요금 검증 모듈을 더 포함하는, 컴퓨팅 장치.

청구항 9

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 사용자 단말로 동작되는 컴퓨팅 장치로서,

복수의 가명(Pseudonym)들에 대한 인증을 위해 선불 요금을 지불하는 요금 지불 모듈;

종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 트랜잭션 생성 모듈;

상기 생성된 트랜잭션에 서명하는 트랜잭션 서명 모듈; 및

상기 서명된 트랜잭션을 상기 블록체인 망에 게시하는 통신 모듈을 포함하는, 컴퓨팅 장치.

청구항 10

청구항 9항에 있어서,

상기 통신 모듈은,

상기 블록체인 망에 포함된, 인증 기관을 겸하는 청구 센터로부터 상기 가명들 각각에 대한 인증서를 획득하고,

상기 트랜잭션 생성 모듈은,

상기 가명들을 생성하고, 상기 가명들의 조합, 상기 조합에 포함된 가명들 각각에 대한 인증서 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는, 컴퓨팅 장치.

청구항 11

청구항 9항에 있어서,

상기 트랜잭션 서명 모듈은,

트랜잭션 공개키 및 상기 트랜잭션 공개키에 대응되는 트랜잭션 개인키를 생성하고, 상기 트랜잭션을 상기 트랜잭션 개인키로 서명하는, 컴퓨팅 장치.

청구항 12

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 청구 센터로 동작되는 컴퓨팅 장치로서,

인증된 사용자 단말로부터 선불 요금을 징수하는 요금 징수 모듈; 및

상기 선불 요금이 지불된 경우, 상기 인증된 사용자 단말에 대응되는 복수의 가명(Pseudonym)들 각각에 대해 종류에 따라 가격이 상이한 복수의 인증서를 발급하되, 상기 발급된 인증서들의 총 가격이 상기 선불 요금과 대응되는 것을 특징으로 하는 인증서 발급 모듈을 포함하는, 컴퓨팅 장치.

청구항 13

청구항 12항에 있어서,

상기 블록체인 망에 종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션이 게시된 경우, 상기 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 상기 마지막 블록 내 가명들의 조합의 유효성을 검증하는 가명 검증 모듈; 및

상기 검증된 가명들의 조합에 대응되는 에너지 사용 정보를 식별하는 식별 모듈을 더 포함하는, 컴퓨팅 장치.

청구항 14

청구항 13항에 있어서,

상기 가명 검증 모듈은,

상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하고, 상기 가명들의 조합에 대한 상기 블룸 필터의 보고 결과에 기초하여 상기 가명들의 조합의 유효성을 검증하는, 컴퓨팅 장치.

청구항 15

청구항 13항에 있어서,

상기 가명 검증 모듈은,

상기 블록체인에서 상기 가명들의 조합이 포함된 트랜잭션을 탐색하고, 상기 가명들의 조합에 포함된 가명들 각각에 대한 인증서를 검증함으로써 상기 가명들의 조합의 유효성을 검증하는, 컴퓨팅 장치.

청구항 16

청구항 13항에 있어서,

상기 검증된 가명들의 조합으로 인한 선불 요금과 상기 검증된 가명들의 조합에 대응되는 에너지 소비 데이터를 확인함으로써 에너지 요금의 정상 지불 여부를 검증하는 요금 검증 모듈을 더 포함하는, 컴퓨팅 장치.

청구항 17

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 사용자 단말로 동작되는 컴퓨팅 장치에서 수행되는 방법으로서,

인증서로 인증된 가명(Pseudonym) 및 상기 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 단계;

상기 생성된 트랜잭션에 서명하는 단계;

상기 서명된 트랜잭션을 상기 블록체인 망에 게시하는 단계; 및

상기 블록체인 망에 포함된 청구 센터로부터 상기 가명 앞으로 청구된 에너지 요금을 지불하는 단계를 포함하고,

상기 트랜잭션을 생성하는 단계는,

상기 가명을 생성하는 단계;

상기 블록체인 망에 포함된 인증 기관으로부터 상기 가명에 대한 인증서를 획득하는 단계; 및

상기 가명, 상기 가명에 대한 인증서 및 상기 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 단계를 포함하는, 요금 처리 방법.

청구항 18

삭제

청구항 19

청구항 17항에 있어서,

상기 트랜잭션에 서명하는 단계는,

트랜잭션 공개키 및 상기 트랜잭션 공개키에 대한 트랜잭션 개인키를 생성하는 단계; 및

상기 트랜잭션을 상기 트랜잭션 개인키로 서명하는 단계를 포함하는, 요금 처리 방법.

청구항 20

청구항 17항에 있어서,

상기 요금을 지불하는 단계는,

상기 블록체인 망에서 사용 가능한 암호화폐를 이용하여 상기 에너지 요금을 지불하는, 요금 처리 방법.

청구항 21

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 청구 센터로 동작되는 컴퓨팅 장치에서 수행되는 방법으로서,

상기 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 상기 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 단계;

상기 검증된 가명에 대응되는 에너지 사용 정보를 식별하는 단계; 및

상기 검증된 가명 중 적어도 일부 가명으로 상기 식별된 에너지 사용 정보에 따른 에너지 요금을 청구하는 단계를 포함하는, 요금 처리 방법.

청구항 22

청구항 21항에 있어서,

상기 가명의 유효성을 검증하는 단계는,

상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하는 단계; 및

상기 가명에 대한 상기 블룸 필터의 보고 결과에 기초하여 상기 가명의 유효성을 검증하는 단계를 포함하는, 요금 처리 방법.

청구항 23

청구항 21항에 있어서,

상기 가명의 유효성을 검증하는 단계는,

상기 블록체인에서 상기 가명이 포함된 트랜잭션을 탐색하는 단계; 및

상기 가명에 대한 인증서를 검증함으로써 상기 가명의 유효성을 검증하는 단계를 포함하는, 요금 처리 방법.

청구항 24

청구항 21항에 있어서,

상기 청구에 따라 지불된 에너지 요금과 상기 에너지 요금이 지불된 가명에 대한 에너지 소비 데이터를 확인함으로써 상기 청구에 따라 지불된 에너지 요금의 정상 지불 여부를 검증하는 단계를 더 포함하는, 요금 처리 방법.

청구항 25

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 사용자 단말로 동작되는 컴퓨팅 장치에서 수행되는 방법으로서,

복수의 가명(Pseudonym)들에 대한 인증을 위해 선불 요금을 지불하는 단계;

종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 상기 가명들의 조합에 대응

되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 단계;

상기 생성된 트랜잭션에 서명하는 단계; 및

상기 서명된 트랜잭션을 상기 블록체인 망에 게시하는 단계를 포함하는, 요금 처리 방법.

청구항 26

청구항 25항에 있어서,

상기 트랜잭션을 생성하는 단계는,

가명들을 생성하는 단계;

상기 블록체인 망에 포함된, 인증 기관을 겸하는 청구 센터로부터 상기 가명들 각각에 대한 인증서를 획득하는 단계; 및

상기 가명들의 조합, 상기 조합에 포함된 가명들 각각에 대한 인증서 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 단계를 포함하는, 요금 처리 방법.

청구항 27

청구항 25항에 있어서,

상기 트랜잭션에 서명하는 단계는,

트랜잭션 공개키 및 상기 트랜잭션 공개키에 대응되는 트랜잭션 개인키를 생성하는 단계; 및

상기 트랜잭션을 상기 트랜잭션 개인키로 서명하는 단계를 포함하는, 요금 처리 방법.

청구항 28

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비하며, 블록체인 망을 구성하는 청구 센터로 동작되는 컴퓨팅 장치에서 수행되는 방법으로서,

인증된 사용자 단말로부터 선불 요금을 징수하는 단계; 및

상기 선불 요금이 지불된 경우, 상기 인증된 사용자 단말에 대응되는 복수의 가명(Pseudonym)들 각각에 대해 종류에 따라 가격이 상이한 복수의 인증서를 발급하는 단계를 포함하되,

상기 발급된 인증서들의 총 가격은 상기 선불 요금과 대응되는 것을 특징으로 하는, 요금 처리 방법.

청구항 29

청구항 28항에 있어서,

상기 블록체인 망에 종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션이 게시된 경우, 상기 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 상기 마지막 블록 내 가명들의 조합의 유효성을 검증하는 단계; 및

상기 검증된 가명들의 조합에 대응되는 에너지 사용 정보를 식별하는 단계를 더 포함하는, 요금 처리 방법.

청구항 30

청구항 29항에 있어서,

상기 가명들의 조합의 유효성을 검증하는 단계는,

상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하는 단계; 및

상기 가명들의 조합에 대한 상기 블룸 필터의 보고 결과에 기초하여 상기 가명들의 조합의 유효성을 검증하는 단계를 포함하는, 요금 처리 방법.

청구항 31

청구항 29항에 있어서,

상기 가명들의 조합의 유효성을 검증하는 단계는,

상기 블록체인에서 상기 가명들의 조합이 포함된 트랜잭션을 탐색하는 단계; 및

상기 가명들의 조합에 포함된 가명들 각각에 대한 인증서를 검증함으로써 상기 가명들의 조합의 유효성을 검증하는 단계를 포함하는, 요금 처리 방법.

청구항 32

청구항 29항에 있어서,

상기 검증된 가명들의 조합으로 인한 선불 요금과 상기 검증된 가명들의 조합에 대응되는 에너지 소비 데이터를 확인함으로써 에너지 요금의 정상 지불 여부를 검증하는 단계를 더 포함하는, 요금 처리 방법.

발명의 설명

기 술 분 야

[0001] 개시되는 실시예들은 블록체인 기반의 요금 처리 기술에 관한 것이다.

배 경 기 술

[0003] 통상적으로, 현대사회를 살아가는 구성원들은 가정이나 회사에서 다양한 형태의 에너지를 사용하고, 이에 대한 요금을 일, 월 또는 연 단위로 납부한다.

[0004] 이와 관련하여 종래에는, 에너지의 공급과 에너지 네트워크에 대한 전반적인 운영을 담당하는 기관이 각 사용자에게 에너지의 사용에 따른 요금을 청구(Billing)하면, 각 사용자는 해당 기관으로 청구된 요금을 지불(Payment)했다. 예를 들어, 전기에너지의 경우, 한국전력(KEPCO)에서 각 사용자들에게 전기 요금을 월별로 청구하면, 각 사용자들은 청구된 정기 요금을 한국전력에 납부해왔다.

[0005] 이처럼, 에너지와 관련된 요금의 처리가 특정한 기관으로 중앙화(Centralization)됨에 따라, 에너지 네트워크에 속한 사용자들의 개인 정보가 해당 기관으로 집중되게 되었고, 이는 해당 기관이 해킹될 경우 각 사용자의 개인 정보가 노출되는 위험성을 야기했다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 한국 등록특허공보 제10-2010571호(2019.08.07 등록)

발명의 내용

해결하려는 과제

[0008] 개시되는 실시예들은 에너지의 사용에 따른 요금 청구 및 지불 과정에서 블록체인을 기반으로 탈중앙화(Decentralization)된 요금 처리 기법을 제공하기 위한 것이다.

과제의 해결 수단

[0010] 개시되는 제1 실시예에 따른 사용자 단말은, 인증서로 인증된 가명(Pseudonym) 및 상기 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 트랜잭션 생성 모듈; 상기 생성된 트랜잭션에 서명하는 트랜잭션 서명 모듈; 상기 서명된 트랜잭션을 상기 블록체인 망에 게시하는 통신 모듈; 및 상기 블록체인 망에 포함된 청구 센터로부터 상기 가명 앞으로 청구된 에너지 요금을 지불하는 요금 지불 모듈을 포함한다.

[0011] 상기 통신 모듈은, 상기 블록체인 망에 포함된 인증 기관으로부터 상기 가명에 대한 인증서를 획득하고, 상기 트랜잭션 생성 모듈은, 상기 가명을 생성하고, 상기 가명, 상기 가명에 대한 인증서 및 상기 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성할 수 있다.

[0012] 상기 트랜잭션 서명 모듈은, 트랜잭션 공개키 및 상기 트랜잭션 공개키에 대응되는 트랜잭션 개인키를 생성하고, 상기 트랜잭션을 상기 트랜잭션 개인키로 서명할 수 있다.

[0013] 상기 요금 지불 모듈은, 상기 블록체인 망에서 사용 가능한 암호화폐를 이용하여 상기 에너지 요금을 지불할 수 있다.

[0014] 상기 제1 실시예에 따른 청구 센터는, 상기 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 상기 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 가명 검증 모듈; 상기 검증된 가명에 대응되는 에너지 사용 정보를 식별하는 식별 모듈; 및 상기 검증된 가명 중 적어도 일부 가명으로 상기 식별된 에너지 사용 정보에 따른 에너지 요금을 청구하는 요금 청구 모듈을 포함한다.

[0015] 상기 가명 검증 모듈은, 상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하고, 상기 가명에 대한 상기 블룸 필터의 보고 결과에 기초하여 상기 가명의 유효성을 검증할 수 있다.

[0016] 상기 가명 검증 모듈은, 상기 블록체인에서 상기 가명이 포함된 트랜잭션을 탐색하고, 상기 가명에 대한 인증서를 검증함으로써 상기 가명의 유효성을 검증할 수 있다.

[0017] 상기 청구 센터는, 상기 청구에 따라 지불된 에너지 요금과 상기 에너지 요금이 지불된 가명에 대한 에너지 소비 데이터를 확인함으로써 상기 청구에 따라 지불된 에너지 요금의 정상 지불 여부를 검증하는 요금 검증 모듈을 더 포함할 수 있다.

[0018] 개시되는 제2 실시예에 따른 사용자 단말은, 복수의 가명(Pseudonym)들에 대한 인증을 위해 선불 요금을 지불하는 요금 지불 모듈; 종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 트랜잭션 생성 모듈; 상기 생성된 트랜잭션에 서명하는 트랜잭션 서명 모듈; 및 상기 서명된 트랜잭션을 상기 블록체인 망에 게시하는 통신 모듈을 포함한다.

[0019] 상기 통신 모듈은, 상기 블록체인 망에 포함된, 인증 기관을 겸하는 청구 센터로부터 상기 가명들 각각에 대한 인증서를 획득하고, 상기 트랜잭션 생성 모듈은, 상기 가명들을 생성하고, 상기 가명들의 조합, 상기 조합에 포함된 가명들 각각에 대한 인증서 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성할 수 있다.

[0020] 상기 트랜잭션 서명 모듈은, 트랜잭션 공개키 및 상기 트랜잭션 공개키에 대응되는 트랜잭션 개인키를 생성하고, 상기 트랜잭션을 상기 트랜잭션 개인키로 서명할 수 있다.

[0021] 상기 제2 실시예에 따른 청구 센터는, 인증된 사용자 단말로부터 선불 요금을 징수하는 요금 징수 모듈; 및 상기 선불 요금이 지불된 경우, 상기 인증된 사용자 단말에 대응되는 복수의 가명(Pseudonym)들 각각에 대해 종류에 따라 가격이 상이한 복수의 인증서를 발급하되, 상기 발급된 인증서들의 총 가격이 상기 선불 요금과 대응되는 것을 특징으로 하는 인증서 발급 모듈을 포함한다.

[0022] 상기 청구 센터는, 상기 블록체인 망에 종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션이 게시된 경우, 상기 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 상기 마지막 블록 내 가명들의 조합의 유효성을 검증

하는 가명 검증 모듈; 및 상기 검증된 가명들의 조합에 대응되는 에너지 사용 정보를 식별하는 식별 모듈을 더 포함할 수 있다.

[0023] 상기 가명 검증 모듈은, 상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하고, 상기 가명들의 조합에 대한 상기 블룸 필터의 보고 결과에 기초하여 상기 가명들의 조합의 유효성을 검증할 수 있다.

[0024] 상기 가명 검증 모듈은, 상기 블록체인에서 상기 가명들의 조합이 포함된 트랜잭션을 탐색하고, 상기 가명들의 조합에 포함된 가명들 각각에 대한 인증서를 검증함으로써 상기 가명들의 조합의 유효성을 검증할 수 있다.

[0025] 상기 청구 센터는, 상기 검증된 가명들의 조합으로 인한 선불 요금과 상기 검증된 가명들의 조합에 대응되는 에너지 소비 데이터를 확인함으로써 에너지 요금의 정상 지불 여부를 검증하는 요금 검증 모듈을 더 포함할 수 있다.

[0026] 개시되는 제1 실시예에 따른 사용자 단말의 요금 처리 방법은, 인증서로 인증된 가명(Pseudonym) 및 상기 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 단계; 상기 생성된 트랜잭션에 서명하는 단계; 상기 서명된 트랜잭션을 상기 블록체인 망에 게시하는 단계; 및 상기 블록체인 망에 포함된 청구 센터로부터 상기 가명 앞으로 청구된 에너지 요금을 지불하는 단계를 포함한다.

[0027] 상기 트랜잭션을 생성하는 단계는, 상기 가명을 생성하는 단계; 상기 블록체인 망에 포함된 인증 기관으로부터 상기 가명에 대한 인증서를 획득하는 단계; 및 상기 가명, 상기 가명에 대한 인증서 및 상기 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 단계를 포함할 수 있다.

[0028] 상기 트랜잭션에 서명하는 단계는, 트랜잭션 공개키 및 상기 트랜잭션 공개키에 대한 트랜잭션 개인키를 생성하는 단계; 및 상기 트랜잭션을 상기 트랜잭션 개인키로 서명하는 단계를 포함할 수 있다.

[0029] 상기 요금을 지불하는 단계는, 상기 블록체인 망에서 사용 가능한 암호화폐를 이용하여 상기 에너지 요금을 지불할 수 있다.

[0030] 상기 제1 실시예에 따른 청구 센터의 요금 처리 방법은, 상기 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 상기 마지막 블록 내 가명(Pseudonym)의 유효성을 검증하는 단계; 상기 검증된 가명에 대응되는 에너지 사용 정보를 식별하는 단계; 및 상기 검증된 가명 중 적어도 일부 가명으로 상기 식별된 에너지 사용 정보에 따른 에너지 요금을 청구하는 단계를 포함한다.

[0031] 상기 가명의 유효성을 검증하는 단계는, 상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하는 단계; 및 상기 가명에 대한 상기 블룸 필터의 보고 결과에 기초하여 상기 가명의 유효성을 검증하는 단계를 포함할 수 있다.

[0032] 상기 가명의 유효성을 검증하는 단계는, 상기 블록체인에서 상기 가명이 포함된 트랜잭션을 탐색하는 단계; 및 상기 가명에 대한 인증서를 검증함으로써 상기 가명의 유효성을 검증하는 단계를 포함할 수 있다.

[0033] 상기 청구 센터의 요금 처리 방법은, 상기 청구에 따라 지불된 에너지 요금과 상기 에너지 요금이 지불된 가명에 대한 에너지 소비 데이터를 확인함으로써 상기 청구에 따라 지불된 에너지 요금의 정상 지불 여부를 검증하는 단계를 더 포함할 수 있다.

[0034] 개시되는 제2 실시예에 따른 사용자 단말의 요금 처리 방법은, 복수의 가명(Pseudonym)들에 대한 인증을 위해 선불 요금을 지불하는 단계; 종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 단계; 상기 생성된 트랜잭션에 서명하는 단계; 및 상기 서명된 트랜잭션을 상기 블록체인 망에 게시하는 단계를 포함한다.

[0035] 상기 트랜잭션을 생성하는 단계는, 가명들을 생성하는 단계; 상기 블록체인 망에 포함된, 인증 기관을 겸하는 청구 센터로부터 상기 가명들 각각에 대한 인증서를 획득하는 단계; 및 상기 가명들의 조합, 상기 조합에 포함된 가명들 각각에 대한 인증서 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성하는 단계를 포함할 수 있다.

[0036] 상기 트랜잭션에 서명하는 단계는, 트랜잭션 공개키 및 상기 트랜잭션 공개키에 대응되는 트랜잭션 개인키를 생성하는 단계; 및 상기 트랜잭션을 상기 트랜잭션 개인키로 서명하는 단계를 포함할 수 있다.

[0037] 상기 제2 실시예에 따른 청구 센터의 요금 처리 방법은, 인증된 사용자 단말로부터 선불 요금을 징수하는 단계; 및 상기 선불 요금이 지불된 경우, 상기 인증된 사용자 단말에 대응되는 복수의 가명(Pseudonym)들 각각에 대해

종류에 따라 가격이 상이한 복수의 인증서를 발급하는 단계를 포함하되, 상기 발급된 인증서들의 총 가격은 상기 선불 요금과 대응되는 것을 특징으로 한다.

[0038] 상기 청구 센터의 요금 처리 방법은, 상기 블록체인 망에 종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 상기 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션이 게시된 경우, 상기 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 상기 마지막 블록 내 가명들의 조합의 유효성을 검증하는 단계; 및 상기 검증된 가명들의 조합에 대응되는 에너지 사용 정보를 식별하는 단계를 더 포함할 수 있다.

[0039] 상기 가명들의 조합의 유효성을 검증하는 단계는, 상기 마지막 블록의 블룸 필터(Bloom Filter)를 조회하는 단계; 및 상기 가명들의 조합에 대한 상기 블룸 필터의 보고 결과에 기초하여 상기 가명들의 조합의 유효성을 검증하는 단계를 포함할 수 있다.

[0040] 상기 가명들의 조합의 유효성을 검증하는 단계는, 상기 블록체인에서 상기 가명들의 조합이 포함된 트랜잭션을 탐색하는 단계; 및 상기 가명들의 조합에 포함된 가명들 각각에 대한 인증서를 검증함으로써 상기 가명들의 조합의 유효성을 검증하는 단계를 포함할 수 있다.

[0041] 상기 청구 센터의 요금 처리 방법은, 상기 검증된 가명들의 조합으로 인한 선불 요금과 상기 검증된 가명들의 조합에 대응되는 에너지 소비 데이터를 확인함으로써 에너지 요금의 정상 지불 여부를 검증하는 단계를 더 포함할 수 있다.

발명의 효과

[0043] 개시되는 실시예들에 따르면, 에너지의 사용에 따른 요금 청구 및 지불 과정에서 블록체인을 이용함으로써, 청구 센터가 사용자 단말의 정보를 독점하고 청구서 발부 작업이 중앙화(Centralization)되는 것을 방지할 수 있다.

[0044] 또한 개시되는 실시예들에 따르면, 사용자 단말을 직접적으로 식별 가능한 정보 대신 가명(Pseudonym)을 이용하여 에너지 요금을 지불함으로써, 에너지 요금 청구 및 지불 과정에서 사용자 단말과 에너지 사용 정보의 관계가 노출되는 것을 방지할 수 있다.

[0045] 또한 개시되는 실시예들에 따르면, 여러 종류의 단위 가격을 갖는 토큰(Token)을 이용하여 에너지 요금의 선불을 가능케 함으로써, 기존의 에너지 요금 청구 및 지불 과정을 단순화하고 스마트그리드(smart grids)에 특화된 요금 지불 구조를 구현할 수 있다.

도면의 간단한 설명

[0047] 도 1은 제1 실시예에 따른 요금 처리 시스템을 설명하기 위한 블록도

도 2는 제1 실시예에 따른 사용자 단말을 설명하기 위한 블록도

도 3 및 도 4는 제1 실시예에 따른 청구 센터를 설명하기 위한 블록도

도 5는 일 실시예에서 블록에 블룸 필터를 생성하는 상태를 나타내는 도면

도 6은 제2 실시예에 따른 요금 처리 시스템을 설명하기 위한 블록도

도 7은 제2 실시예에 따른 사용자 단말을 설명하기 위한 블록도

도 8 내지 도 10은 제2 실시예에 따른 청구 센터를 설명하기 위한 블록도

도 11은 제1 실시예에 따른 사용자 단말의 요금 처리 방법을 설명하기 위한 흐름도

도 12 및 도 13은 제1 실시예에 따른 청구 센터의 요금 처리 방법을 설명하기 위한 흐름도

도 14는 제2 실시예에 따른 사용자 단말의 요금 처리 방법을 설명하기 위한 흐름도

도 15 내지 도 17은 제2 실시예에 따른 청구 센터의 요금 처리 방법을 설명하기 위한 흐름도

도 18은 일 실시예에 따른 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0048] 이하, 도면을 참조하여 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 개시되는 실시예들은 이에 제한되지 않는다.

[0049] 실시예들을 설명함에 있어서, 관련된 공지기술에 대한 구체적인 설명이 개시되는 실시예들의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 개시되는 실시예들에서의 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 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.

[0050] 이하의 설명에 있어서, 신호 또는 정보의 "전송", "통신", "송신", "수신" 기타 이와 유사한 의미의 용어는 일 구성요소에서 다른 구성요소로 신호 또는 정보가 직접 전달되는 것뿐만이 아니라 다른 구성요소를 거쳐 전달되는 것도 포함한다.

[0051] 특히 신호 또는 정보를 일 구성요소로 "전송" 또는 "송신"한다는 것은 그 신호 또는 정보의 최종 목적지를 지시하는 것이고 직접적인 목적지를 의미하는 것이 아니다. 이는 신호 또는 정보의 "수신"에 있어서도 동일하다. 또한 본 명세서에 있어서, 2 이상의 데이터 또는 정보가 "관련"된다는 것은 하나의 데이터(또는 정보)를 획득하면, 그에 기초하여 다른 데이터(또는 정보)의 적어도 일부를 획득할 수 있음을 의미한다.

[0052] 또한, 제1, 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로 사용될 수 있다.

[0053] 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성 요소는 제2 구성 요소로 명명될 수 있고, 유사하게 제2 구성 요소도 제1 구성 요소로 명명될 수 있다.

[0054] 도 1은 제1 실시예에 따른 요금 처리 시스템(100)을 설명하기 위한 블록도이다.

[0055] 도 1을 참조하면, 제1 실시예에 따른 요금 처리 시스템(100)은 사용자 단말(110)의 에너지 요금을 후불로 처리하는 시스템으로서, 사용자 단말(110), 청구 센터(120), 인증 기관(130) 및 마이너 노드(140)를 포함한다. 또한, 사용자 단말(110)은 통신 네트워크(150)를 통해 청구 센터(120), 인증 기관(130) 및 마이너 노드(140)와 상호 통신 가능하게 연결된다.

[0056] 한편 개시되는 실시예에서, 블록체인은 프라이빗(Private) 블록체인일 수 있으나, 이에 한정되는 것은 아니며, 퍼블릭(Public) 블록체인 또는 컨소시움(Consortium) 블록체인일 수도 있다.

[0057] 사용자 단말(110)은 사용자가 사용한 에너지와 관련된 에너지 사용 정보를 블록체인 망에 게시하고, 에너지 요금을 지불하는 개체(Entity)를 의미한다. 도시된 블록체인 망이 프라이빗 블록체인에 기반하는 경우, 사용자 단말(110)은 프라이빗 블록체인에 기 등록된 개체이며, 블록체인 망을 이용하는 개체 사이에 사용자 단말(110)이 기 등록된 개체임을 증명할 인증 수단을 공유하는 것으로 전제한다.

[0058] 한편, 사용자 단말(110)은 에너지 사용 정보를 블록체인 망에 게시함에 있어서, 사용자 단말(110) 자체를 식별할 수 없도록 가명(Pseudonym)을 사용한다. 이때, '가명'은 임의 생성된 난수를 포함하는 정보일 수 있으나, 반드시 이에 한정되는 것은 아니며, 실시예에 따라서는 특정한 규칙에 따라 생성된 정보일 수도 있다. 또한, 해당 문서에서는 '가명'의 데이터 타입을 한정하지 않음에 유의해야 한다.

[0059] 일 실시예에 따르면, 사용자 단말(110)은 사용자의 에너지 사용량을 포함한 에너지 사용 정보를 감지할 수 있는 스마트 미터(smart meter)이거나, 스마트 미터를 포함하는 하드웨어일 수 있다. 예컨대, 사용자 단말(110)은 하나의 독립된 하드웨어로서, 개인용 컴퓨터(Personal Computer), 랩탑(Laptop Computer), 스마트폰(Smart Phone), 태블릿(Tablet) PC, 스마트 밴드(Smart Band)나 스마트 워치(Smart Watch) 등의 웨어러블 디바이스(Wearable Device)의 형태일 수 있다. 이외에도 상기 정의를 만족하는 하드웨어라면 사용자 단말에 속하는 것으로 해석된다.

[0060] 청구 센터(120)는 사용자 단말(110)이 게시한 에너지 사용 정보에 따라 사용자 단말(110) 앞으로 에너지 요금을

청구하고, 이를 징수하는 개체를 의미한다.

[0061] 이때, 청구 센터(120)는 블록체인 망을 이용하는 개체들 사이에서 사전에 공개된 동적 가격(dynamic pricing) 정보를 기반으로 시간에 따른 에너지 요금을 파악하고, 사용자 단말(110) 앞으로 청구할 에너지 요금을 산출한다.

[0062] 구체적으로, '동적 가격 정보'는 시간에 따른 단위 에너지 사용량 당 에너지 요금 정보를 포함하며, 만일 동적 가격 정보에 변경이 발생할 경우 사용자 단말(110) 앞으로 청구할 에너지 요금 산출에 앞서 블록체인 망에 변경된 동적 가격 정보가 공유되는 것으로 전제한다.

[0063] 인증 기관(130)은 사용자 단말(110)이 생성하는 가명에 대해 인증서를 발급하는 개체를 의미한다. 일 실시예에서, 도시된 블록체인 망이 프라이빗 블록체인을 기반으로 하는 경우, 인증 기관(130)은 블록체인 망을 구성하는 참여자가 사전 등록된 참여자인지 검증하기 위한 인증서를 발급할 수도 있다.

[0064] 일 실시예에 따르면, 인증 기관(130)은 사용자 단말과 상호 간 블라인드 서명을 수행함으로써 가명에 대한 인증서를 발급할 수 있다. 예시적으로, 상세한 발급 과정은 다음과 같이 진행될 수 있다.

[0065] (1) 인증 기관(130)은 사전 정의된 블라인드 서명 키 생성 알고리즘을 실행하고, 이에 따라 공개 검증키(cvk)와 개인 서명키(csk)를 획득

[0066] (2) 인증 기관(130)은 cvk를 블록체인 망에 공개하고, csk를 비밀로 유지

[0067] (3) 인증 기관(130) 및 인증 기관(130)에 대해 인증된 사용자 단말(110)이 인증할 가명의 수 v에 동의

[0068] (4) 인증 기관(130)은 사용자 단말(110)이 선택한 가명 pk에 대해, 사용자 단말(110)을 수신자(receiver)로 하고, 인증 기관(130)을 서명자(signer)로 하여 인증서 s를 발급

[0069] (5) 인증할 가명들 중 나머지 가명 각각에 대해 (4)의 과정을 반복

[0070] 마이너 노드(140)는 블록체인 상에서 유효성이 검증된 트랜잭션을 블록에 기록하여 공유하는 작업을 수행하는 장치를 의미한다.

[0071] 구체적으로, 마이너 노드(140)는 블록체인 망에서 각 사용자 단말(110)들이 전송하는 트랜잭션들을 수집하여 블록을 생성할 수 있으며, 생성한 블록을 블록체인에 연결할 수 있다.

[0072] 일 실시예에 따르면, 마이너 노드(140)는 블록을 구성하는 각 트랜잭션에 포함된 사용자 관련 정보와 가명을 이용하여 블룸 필터(Bloom Filter)를 생성할 수 있다. 즉, 마이너 노드(140)는 각 트랜잭션에 포함된 사용자 관련 정보 및 가명을 블룸 필터의 멤버(Member)로 하여 블룸 필터를 생성할 수 있다. 이때, 블룸 필터는 소정 멤버가 집합에 속하는지 여부를 검사하기 위해 사용되는 확률적 자료 구조를 의미할 수 있다. 이와 관련해서는, 이하의 도 5를 참조하여 후술하기로 한다.

[0073] 통신 네트워크(150)는 블록체인 망에 접근하는 사용자 단말(110)과 블록체인 망에 포함된 개체들 사이에서 데이터 교환을 가능하게 하는 유선 또는 무선의 네트워크를 의미한다.

[0074] 이하의 실시예들에서, 통신 네트워크(150)는 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.

[0075] 도 2는 제1 실시예에 따른 사용자 단말(110)을 설명하기 위한 블록도이다.

[0076] 도시된 바와 같이, 제1 실시예에 따른 사용자 단말(110)은 트랜잭션 생성 모듈(111), 트랜잭션 서명 모듈(113), 통신 모듈(115) 및 요금 지불 모듈(117)을 포함한다.

[0077] 도시된 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0078] 또한, 일 실시예에서, 트랜잭션 생성 모듈(111), 트랜잭션 서명 모듈(113), 통신 모듈(115) 및 요금 지불 모듈(117)은 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0079] 트랜잭션 생성 모듈(111)은 인증서로 인증된 가명 및 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을

생성한다.

[0080] 일 실시예에 따르면, 트랜잭션 생성 모듈(111)은 가명을 생성할 수 있으며, 이때 '가명'은 사용자 단말(110)과 일대일 대응되는 사용자 단말(110)의 공개키일 수 있다. 그러나 실시예에 따라서는, 하나의 사용자 단말(110)에 여러 개의 가명이 대응될 수도 있다.

[0081] 한편 일 실시예에 따르면, 트랜잭션 생성 모듈(111)은 가명, 가명에 대한 인증서 및 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성할 수 있으며, 이때 가명에 대한 인증서는 블록체인 망에 포함된 인증 기관(130)으로부터 후술할 통신 모듈(115)에 의해 획득될 수 있다.

[0082] 즉 다시 말하면, 트랜잭션 생성 모듈(111)에 의해 생성된 트랜잭션은 사용자 단말(110)을 식별할 수 있는 직접적인 정보를 포함하지 않기 때문에, 사용자 단말(110)의 에너지 사용 정보나 에너지 요금이 블록체인 망에 포함된 개체들에게 노출되는 것을 방지할 수 있다.

[0083] 트랜잭션 서명 모듈(113)은 트랜잭션 생성 모듈(111)에 의해 생성된 트랜잭션에 서명한다.

[0084] 일 실시예에 따르면, 트랜잭션 서명 모듈(113)은 트랜잭션 공개키 및 트랜잭션 공개키에 대응되는 트랜잭션 개인키를 생성하고, 트랜잭션 생성 모듈(111)에 의해 생성된 트랜잭션을 트랜잭션 개인키로 서명할 수 있다. 이때, 트랜잭션 공개키는 블록체인 망 내에 등록되어 블록체인 망에 포함된 개체들에게 공개될 수 있다.

[0085] 이를 통해, 블록체인 망에 포함된 마이너 노드(140)는 트랜잭션 공개키를 이용하여 트랜잭션 개인키로 서명된 트랜잭션의 유효성을 검증할 수 있고, 유효한 트랜잭션들로 블록을 구성할 수 있다.

[0086] 통신 모듈(115)은 트랜잭션 서명 모듈(113)에 의해 서명된 트랜잭션을 블록체인 망에 게시한다.

[0087] 일 실시예에 따르면, 통신 모듈(115)은 블록체인 망을 통해 가명에 대한 인증서를 획득할 수도 있다.

[0088] 구체적으로, 통신 모듈(115)은 사용자 단말(110)과 블록체인 망 사이에서 통신 네트워크(150)를 통해 정보를 송신 또는 수신하는 통신 인터페이스를 제공할 수 있다.

[0089] 요금 지불 모듈(117)은 블록체인 망에 포함된 청구 센터(120)로부터 가명 앞으로 청구된 에너지 요금을 지불한다. 이때, 에너지 요금의 지불 역시 가명 명의로 이루어지는 것이지, 사용자 단말(110)의 명의로 이루어지는 것이 아님에 유의해야 한다.

[0090] 일 실시예에 따르면, 요금 지불 모듈(117)은 통신 모듈(115)이 청구 센터(120)로부터 에너지 요금을 청구하는 요청을 수신하면, 청구 센터(120) 명의의 계좌나 코인 지갑, 또는 청구 센터(120)가 접근할 수 있는 계좌나 코인 지갑으로 에너지 요금을 지불할 수 있다.

[0091] 일 실시예에 따르면, 요금 지불 모듈(117)은 블록체인 망에서 사용 가능한 암호화폐를 이용하여 에너지 요금을 지불할 수 있다.

[0092] 예를 들어, 요금 지불 모듈(117)은 비트코인(bitcoin), 이더리움(etherium) 등 기존의 암호화폐를 이용하거나, 해당 블록체인 망에서 자체적으로 채택한 새로운 암호화폐를 이용하거나, 이 두 방식을 조합하여 기존의 암호화폐 및 새로운 암호화폐를 함께 이용함으로써 에너지 요금을 지불할 수 있다.

[0093] 도 3 및 도 4는 제1 실시예에 따른 청구 센터(120)를 설명하기 위한 블록도이다.

[0094] 먼저, 도 3에 도시된 청구 센터(120)는 가명 검증 모듈(121), 식별 모듈(123) 및 요금 청구 모듈(125)을 포함한다.

[0095] 가명 검증 모듈(121)은 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 마지막 블록 내 가명의 유효성을 검증한다.

[0096] 일 실시예에 따르면, 가명 검증 모듈(121)은 블록체인 망의 블록체인을 구성하는 마지막 블록의 블룸 필터를 조회하고, 가명에 대한 블룸 필터의 보고 결과에 기초하여 가명의 유효성을 검증할 수 있다.

[0097] 다른 실시예에 따르면, 가명 검증 모듈(121)은 블록체인 망의 블록체인에서 가명이 포함된 트랜잭션을 탐색하고, 가명에 대한 인증서를 검증함으로써 가명의 유효성을 검증할 수 있다.

[0098] 식별 모듈(123)은 검증된 가명에 대응되는 에너지 사용 정보를 식별한다.

[0099] 요금 청구 모듈(125)은 검증된 가명 중 적어도 일부 가명으로, 식별된 에너지 사용 정보에 따른 에너지 요금을

청구한다.

[0100] 즉 다시 말하면, 에너지 요금의 청구 대상이 되는 가명은 검증된 가명 전체일 수도 있으나, 검증된 가명 중 일부일 수도 있으므로, 요금 청구 모듈(125)은 검증된 가명 중 에너지 요금의 청구 대상인 가명에 대해서 에너지 요금을 청구할 수 있다.

[0101] 이를 통해, 에너지 요금을 청구하는 일련의 작업을 수행하는 청구 센터(120)는 에너지 요금을 청구하는 과정에서 사용자 단말(110)의 식별을 필요로 하지 않는다.

[0102] 한편, 도 4는 사용자 단말(110)이 지불한 요금을 검증하는 기능을 추가로 수행하는 청구 센터(120)를 도시한 것으로, 도 4에 도시된 청구 센터(120)는 도 3의 청구 센터(120)에 포함된 모듈에 더하여 요금 검증 모듈(127)을 추가로 포함할 수 있다.

[0103] 요금 검증 모듈(127)은 요금 청구 모듈(125)의 청구에 따라 사용자 단말(110)로부터 지불된 에너지 요금과, 에너지 요금이 지불된 가명에 대한 에너지 소비 데이터를 확인함으로써 에너지 요금의 정상 지불 여부를 검증한다.

[0104] 일 실시예에 따르면, 요금 검증 모듈(127)의 검증 결과, 에너지 요금이 정상 지불된 것으로 판단되는 경우, 요금 검증 모듈(127)은 에너지 요금을 지불한 가명을 요금 지불 완료 상태로 처리하고 요금 청구와 관련된 프로세스를 종료할 수 있다.

[0105] 한편 일 실시예에 따르면, 요금 검증 모듈(127)의 검증 결과, 에너지 요금 지불에 이상이 존재하는 것으로 판단되는 경우, 요금 검증 모듈(127)은 요금 청구 모듈(125) 또는 요금 환불 모듈(미도시)와 연계하여 요금 청구와 관련된 프로세스를 추가 진행할 수 있다.

[0106] 구체적으로, 지불된 에너지 요금이 실제 에너지 소비 데이터에 따라 지불되어야 할 에너지 요금보다 적은 경우, 요금 검증 모듈(127)은 요금 청구 모듈(125)에 부족분의 에너지 요금을 추가로 청구할 것을 명령하는 신호를 전송할 수 있고, 이에 반응하여 요금 청구 모듈(125)은 사용자 단말(110)로 부족분의 에너지 요금을 추가로 청구할 수 있다.

[0107] 반면, 지불된 에너지 요금이 실제 에너지 소비 데이터에 따라 지불되어야 할 에너지 요금보다 많은 경우, 요금 검증 모듈(127)은 요금 환불 모듈(미도시)에 초과분의 에너지 요금을 환불할 것을 명령하는 신호를 전송할 수 있고, 이에 반응하여 요금 환불 모듈(미도시)은 사용자 단말(110) 명의의 계좌나 코인 지갑, 또는 사용자 단말(110)이 접근할 수 있는 계좌나 코인 지갑으로 초과분의 에너지 요금을 환불할 수 있다.

[0108] 상기 도 3 및 도 4에 도시된 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0109] 또한, 상기 도 3 및 도 4에 도시된 실시예에서, 가명 검증 모듈(121), 식별 모듈(123), 요금 청구 모듈(125) 및 요금 검증 모듈(127)은 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0110] 도 5는 일 실시예에서 블록에 블룸 필터를 생성하는 상태를 나타내는 도면이다.

[0111] 도 5를 참조하면, 블록체인의 첫 번째 블록(S1)이 6개의 트랜잭션으로 구성되고, 마지막 트랜잭션은 5개의 트랜잭션(T1 ~ T5)에 포함된 사용자 관련 정보를 기반으로 생성된 제1 블룸 필터(BF1)일 수 있다.

[0112] 여기서, 두 번째 블록(S2)을 첫 번째 블록(S1)에 연결하는 경우, 마이너 노드(140)는 첫 번째 블록(S1)의 제1 블룸 필터(BF1)에 두 번째 블록(S2)의 5개의 트랜잭션(T1 ~ T5)에 포함된 사용자 관련 정보를 추가하여 제2 블룸 필터(BF2)를 생성할 수 있다. 이때, 제2 블룸 필터(BF2)는 두 번째 블록(S2)의 마지막 트랜잭션일 수 있다.

[0113] 그리고, 세 번째 블록(S3)을 두 번째 블록(S2)에 연결하는 경우, 마이너 노드(140)는 두 번째 블록(S2)의 제2 블룸 필터(BF2)에 세 번째 블록(S3)의 5개의 트랜잭션(T1 ~ T5)에 포함된 사용자 관련 정보를 추가하여 제3 블룸 필터(BF3)를 생성할 수 있다. 이때, 제3 블룸 필터(BF3)는 세 번째 블록(S3)의 마지막 트랜잭션일 수 있다.

[0114] 이러한 방식으로 블룸 필터를 생성하면, 블록체인에서 각 블록의 블룸 필터는 이전 블록의 블룸 필터가 누적된 값을 가지게 된다. 이 경우, 블록체인의 마지막 블록의 블룸 필터는 블록체인에 포함된 각 트랜잭션들에 포함된 사용자 관련 정보들을 멤버로 하게 되므로, 멤버쉽 체크가 필요한 경우 블록체인의 마지막 블록의 블룸 필터를

이용하여 용이하게 수행할 수 있게 된다.

[0115] 즉, 블록체인 내에서 소정 사용자에 대한 멤버쉽 체크가 필요한 경우, 블록체인의 마지막 블록의 블룸 필터를 조회하고, 소정 사용자의 사용자 관련 정보(예를 들어, 사용자의 가명 등)에 대해 블룸 필터가 예스(Yes) 또는 노(No)를 보고하는지를 확인하여 멤버쉽 체크를 진행할 수 있다. 블룸 필터가 예스(Yes)로 보고하는 경우, 마이너 노드(140)는 해당 사용자가 유효한 멤버인 것으로 판단할 수 있다. 블룸 필터가 노(No)로 보고하는 경우, 마이너 노드(140)는 해당 사용자가 유효하지 않은 멤버인 것으로 판단할 수 있다.

[0116] 여기서, 각 블록의 블룸 필터는 이전 블록의 블룸 필터가 누적된 상태이므로, 어떤 시점에서는 블룸 필터의 긍정 오류(False Positive)가 무시할 수 없는 수준에 도달할 수 있게 된다. 이에, 마이너 노드(140)는 블룸 필터의 긍정 오류가 기 설정된 임계 값을 초과하는 경우, 블룸 필터의 크기를 키울 수 있다.

[0117] 구체적으로, 마이너 노드(140)는 소정 블록에 대해 블룸 필터를 생성하는 경우, 이전 블록의 블룸 필터를 조회하여 긍정 오류(False Positive)를 산출할 수 있다. 여기서, 긍정 오류(FP)는 하기의 수학식을 통해 산출할 수 있다.

[0118] [수학식]

$$FP = (1 - (1 - \frac{1}{M})^{l-N})^{l}$$

[0119]

[0120] 여기서, M은 현재 블룸 필터의 크기를 나타내고, l은 블룸 필터를 위한 해쉬 함수의 수를 나타내며, N은 블룸 필터의 축적된 수를 나타낸다.

[0121] 마이너 노드(140)는 산출된 긍정 오류(FP)가 기 설정된 임계 값을 초과하는 경우, 블룸 필터의 크기를 리사이징(Resizing) 할 수 있다. 즉, 블룸 필터의 크기를 현재 블룸 필터의 크기보다 크게 리사이징 할 수 있다. 이때, 마이너 노드(140)는 블록체인의 모든 트랜잭션(즉, 첫 번째 블록에서 현재 블록에 포함된 모든 트랜잭션)들에 포함된 사용자 관련 정보들을 사용하여 블룸 필터를 재구성할 수 있다. 블룸 필터의 크기는 블룸 필터의 크기의 성장 속도에 따라 조정될 수 있다.

[0122] 한편, 개시되는 실시예에서는 블룸 필터로 카운팅 블룸 필터(Counting Bloom Filter)를 사용할 수도 있다. 일반적인 블룸 필터는 멤버의 삭제가 불가능하나, 카운팅 블룸 필터는 멤버의 삭제가 가능하다.

[0123] 예시적인 실시예에서, 사용자 단말(110 또는 210)은 특정 사용자 관련 정보의 삭제를 마이너 노드(140)에 요청할 수 있다. 이를 위해, 블록체인의 트랜잭션은 멤버의 삽입 요청인지 삭제 요청인지를 나타내는 필드를 포함할 수 있다. 마이너 노드(140)는 트랜잭션의 해당 필드에서 멤버의 삽입 요청인지 삭제 요청인지를 확인하여 삭제 요청인 경우 해당 셀에서 해당 멤버의 해쉬값에 대응하는 카운트를 줄일 수 있다. 만약, 멤버의 삽입 요청인 경우, 마이너 노드(140)는 해당 멤버의 해쉬 값에 해당하는 각 셀의 카운트를 증가시킬 수 있다.

[0124] 또한, 개시되는 실시예에서는 취소된 멤버를 위한 블룸 필터를 별도로 사용할 수도 있다. 이 경우, 2개의 블룸 필터가 존재할 수 있다. 즉, 유효한 멤버를 위한 블룸 필터(유효 멤버 블룸 필터)와 취소된 멤버를 위한 블룸 필터(취소 멤버 블룸 필터)가 있을 수 있다.

[0125] 사용자 단말(110 또는 210)은 특정 사용자 관련 정보에 대해 삭제 또는 추가를 마이너 노드(140)에 요청할 수 있다. 마이너 노드(140)는 트랜잭션에서 멤버의 삽입 요청인지 삭제 요청인지를 나타내는 필드를 확인하여 삭제 요청이면 해당 사용자 관련 정보를 취소 멤버 블룸 필터에 추가하고, 삽입 요청이면 해당 사용자 관련 정보를 유효 멤버 블룸 필터에 추가할 수 있다.

[0126] 개시되는 실시예에 의하면, 사용자 단말(110 또는 210)이 사용자 관련 정보를 포함하는 트랜잭션을 서명하여 블록체인 망에 브로드캐스팅 하고, 블록체인 망의 마이너 노드(140)에서 트랜잭션을 기반으로 각 블록에 대해 블룸 필터를 생성함으로써, 탈 중앙화된(Decentralized) 방식으로 블룸 필터를 생성할 수 있게 된다.

[0127] 또한, 블록체인의 각 블록에서 이전 블록의 블룸 필터를 누적시킴으로써, 블록체인의 마지막 블록의 블룸 필터를 확인하면 해당 블록체인 망에 대해 멤버쉽 체크를 용이하게 수행할 수 있게 된다. 또한, 블룸 필터를 통해 사용자 멤버쉽의 삭제 및 추가 기능을 제공할 수 있게 된다.

[0128] 도 6은 제2 실시예에 따른 요금 처리 시스템(200)을 설명하기 위한 블록도이다.

[0129] 도 6을 참조하면, 제2 실시예에 따른 요금 처리 시스템(200)은 사용자 단말(110)의 에너지 요금을 선불로 처리

하는 시스템으로서, 사용자 단말(210), 청구 센터(220) 및 마이너 노드(140)를 포함한다. 또한, 사용자 단말(210)은 통신 네트워크(150)를 통해 청구 센터(220) 및 마이너 노드(140)와 상호 통신 가능하게 연결된다.

[0130] 이때, 마이너 노드(140) 및 통신 네트워크(150)는 도 1을 참조하여 설명한 바와 동일 또는 유사한 기능을 수행하므로, 이에 관련한 중복되는 설명은 생략하기로 한다.

[0131] 한편 개시되는 실시예에서, 블록체인은 프라이빗(Private) 블록체인일 수 있으나, 이에 한정되는 것은 아니며, 퍼블릭(Public) 블록체인 또는 컨소시움(Consortium) 블록체인일 수도 있다.

[0132] 사용자 단말(210)은 도 1의 사용자 단말(110)과 유사하게, 사용자가 사용한 에너지와 관련된 에너지 사용 정보를 블록체인 망에 게시하되, 사용자 단말(210) 자체를 식별할 수 없도록 가명을 사용한다.

[0133] 그러나, 사용자 단말(210)은 청구 센터(220)로부터 에너지 요금의 청구를 수신한 이후에 에너지 요금을 지불하는 것이 아니라, 에너지 사용 정보를 게시하기에 앞서 미리 청구 센터(220)로부터 에너지 요금 지불에 필요한 복수의 토큰(Token)을 구매하여, 이후 에너지 사용 정보에 상응하도록 토큰들을 조합하여 이용한다.

[0134] 일 실시예에 따르면, '토큰'은 사용자 단말(210)에 대응되는 가명에 부가되는 정보일 수 있으며, 화폐와 마찬가지로 종류에 따라 단위가 상이하게 책정될 수 있다. 이때, 토큰의 종류 및 대응되는 단위는 실시예에 따라 다양하게 설정될 수 있으며, 해당 문서에서 특정 개수의 종류 및 특정 수치의 단위로 한정되지 않음에 유의해야 한다.

[0135] 청구 센터(220)는 블록체인 망에서 사용자 단말(210)로부터 지불되는 선불 요금에 상응하는 복수의 토큰을 사용자 단말(210)로 판매할 수 있다.

[0136] 일 실시예에 따르면, '토큰'이 사용자 단말(210)에 대응되는 가명을 인증하는 역할을 수행하는 경우, 청구 센터(220)는 인증 기관을 겸하여 동작하게 될 수 있다.

[0137] 도 7은 제2 실시예에 따른 사용자 단말(210)을 설명하기 위한 블록도이다.

[0138] 도시된 바와 같이, 제2 실시예에 따른 사용자 단말(210)은 요금 지불 모듈(211), 트랜잭션 생성 모듈(213), 트랜잭션 서명 모듈(215) 및 통신 모듈(217)을 포함한다.

[0139] 도시된 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0140] 또한, 일 실시예에서, 요금 지불 모듈(211), 트랜잭션 생성 모듈(213), 트랜잭션 서명 모듈(215) 및 통신 모듈(217)은 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0141] 요금 지불 모듈(211)은 복수의 가명들에 대한 인증을 위해 선불 요금을 지불한다.

[0142] 트랜잭션 생성 모듈(213)은 종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성한다.

[0143] 일 실시예에 따르면, 트랜잭션 생성 모듈(213)은 인증의 대상이 되는 가명들을 생성할 수 있고, 이와 관련하여 후술할 통신 모듈(217)은 블록체인 망에 포함된, 인증 기관을 겸하는 청구 센터(220)로부터 가명들 각각에 대한 인증서를 획득할 수 있다.

[0144] 일 실시예에 따르면, 트랜잭션 생성 모듈(213)은 생성된 가명들의 조합, 조합에 포함된 가명들 각각에 대한 인증서 및 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성할 수 있다.

[0145] 이에 따르면, 요금 지불 모듈(211)이 지불한 선불 요금은 가명들에 대해 인증서를 발급받기 위해 지불된 것으로서, 인증서들은 총 가격이 기 지불된 선불 요금과 대응되도록 발급된다.

[0146] 일 실시예에 따르면, 트랜잭션 생성 모듈(213)은 동적 가격 정보에 따라 특정 시간대의 에너지 요금을 파악한 이후, 사용자 단말(210)이 미리 선불 요금 지불을 통해 보유 중인 복수의 가명-인증서 쌍 중에서 에너지 요금과 가격이 일치하도록 가명-인증서 쌍을 조합하여 트랜잭션을 생성할 수 있다.

[0147] 예를 들어, 사용자 단말(210)이 선불 요금을 지불함으로써 각각 1 테더(Tether), 5 테더, 10 테더에 해당하는 인증서 여러 개를 이용하여 복수의 가명-인증서 쌍을 보유 중이라 가정하자. 만일 특정 시간대의 에너지 사용

정보에 따른 에너지 요금이 17 테더라면, 트랜잭션 생성 모듈(213)은 10 테더에 해당하는 인증서로 인증된 가명 1개, 5 테더에 해당하는 인증서로 인증된 가명 1개, 1 테더에 해당하는 인증서로 인증된 가명 2개를 조합하여 해당 시간대의 에너지 사용 정보와 함께 트랜잭션을 생성할 수 있다. 즉, 제1 실시예에서 통신 모듈(217)에 의해 블록체인 망에 게시되는 가명이 1개였다면, 제2 실시예에서는 복수개의 가명이 게시되게 된다.

[0148] 트랜잭션 서명 모듈(215)은 트랜잭션 생성 모듈(213)에 의해 생성된 트랜잭션에 서명한다.

[0149] 일 실시예에 따르면, 트랜잭션 서명 모듈(215)은 트랜잭션 공개키 및 트랜잭션 공개키에 대응되는 트랜잭션 개인키를 생성하고, 트랜잭션을 생성된 트랜잭션 개인키로 서명할 수 있다.

[0150] 통신 모듈(217)은 트랜잭션 서명 모듈(215)에 의해 서명된 트랜잭션을 블록체인 망에 게시한다.

[0151] 도 8 내지 도 10은 제2 실시예에 따른 청구 센터(220)를 설명하기 위한 블록도이다.

[0152] 먼저, 도 8에 도시된 대로 제2 실시예에 따른 청구 센터(220)는 요금 징수 모듈(221) 및 인증서 발급 모듈(223)을 포함한다.

[0153] 요금 징수 모듈(221)은 인증된 사용자 단말로부터 선불 요금을 징수한다.

[0154] 인증서 발급 모듈(223)은 인증된 사용자 단말로부터 선불 요금이 지불된 경우, 인증된 사용자 단말에 대응되는 복수의 가명들 각각에 대해 종류에 따라 가격이 상이한 복수의 인증서를 발급한다.

[0155] 이때, 인증서 발급 모듈(223)은 발급된 인증서들의 총 가격이 기 지불된 선불 요금과 대응되는 것을 특징으로 한다.

[0156] 구체적으로, 가명에 대해 발급하는 인증서는 블라인드 서명(blind signature)인 관계로, 인증서 발급 모듈(223)은 선불 요금에 대응되는 가격만큼의 인증서들을 발급할 뿐, 어느 인증서로 어느 가명을 서명하는지는 알 수 없다. 다만, 사용자 단말(210)이 청구 센터(220)로부터 인증서를 발급받기 위해서는 사전에 사용자 인증을 해야 하므로, 청구 센터(220)는 인증서를 발급받는 사용자 단말(210) 자체는 식별할 수 있다.

[0157] 하지만, 이를 통해 청구 센터(220)가 사용자 단말(210)을 식별하더라도, 실제 사용자 단말(210)의 식별은 선불 요금 지불과 인증서 발급에 관해서만 이루어지는 바, 이후에 사용자 단말(210)이 에너지를 사용함에 따라 블록체인 망에 가명들의 조합을 이용하여 트랜잭션을 게시함에 있어서는 사용자 단말(210)을 식별할 수 있는 정보는 블록체인 망에 게시되지 않음에 유의해야 한다.

[0158] 한편, 인증서 발급 모듈(223)이 각 가명에 대해 종류별로 가격이 상이한 인증서를 발급하는 기법은 다음의 (1) 및 (2)를 포함한다. 다만, 인증서 발급 기법은 이에 한정되는 것은 아니다.

[0159] (1) 인증서로 가명을 서명함으로써, 인증서의 가격을 나타내는 정보를 가명에 부가 및 명시

[0160] 예를 들어, 인증서 발급 모듈(223)은 가명이 난수 값 '8294012'인 경우, 5 테더에 해당하는 인증서를 해당 가명에 발급하여 '8294012||5'라는 가명-인증서 쌍을 생성할 수 있다.

[0161] (2) 인증서의 가격별로 인증서를 발급한 인증 기관의 공개키 종류를 달리하여 설계

[0162] 특히, (2) 기법은 (1)에 비해 보안상의 이점이 있는데, 인증서를 통한 서명이 블라인드 서명인 관계로 (1) 기법의 경우 악의적인 사용자 단말의 도용으로 인해 선불 요금과 실제 발급되는 인증서의 가격이 대응되지 않는 문제가 발생할 우려가 있다. 따라서, 가명에 인증서의 가격을 나타내는 정보를 부가, 명시하기보다는 인증서의 공개키로 인증서의 가격을 확인하는 (2) 기법이 도용 관련 문제에서 보다 자유롭다.

[0163] 일 실시예에 따르면, (2) 기법은 다음과 같은 (2-1)과 (2-2) 기법으로 구체화될 수 있다.

[0164] (2-1) 인증서의 가격별로 공개키 종류를 달리하되, 하나의 인증 기관에서 한 종류의 공개키만을 생성하도록 설계

[0165] 예컨대 (2-1) 기법에 따르면, 인증 기관 A는 1 테더에 해당하는 인증서의 공개키만을 생성하고, 인증 기관 B는 5 테더에 해당하는 인증서의 공개키만을 생성하며, 인증 기관 C는 10 테더에 해당하는 인증서의 공개키만을 생성할 수 있다.

[0166] (2-2) 인증서의 가격별로 공개키 종류를 달리하되, 하나의 인증 기관에서 여러 종류의 공개키를 생성하도록 설계

[0167] 예컨대 (2-2) 기법에 따르면, 하나의 인증 기관에서 각각 1 테더, 5 테더, 10 테더에 해당하는 인증서의 공개키들을 모두 생성할 수 있다.

[0168] 한편, 도 9는 게시된 트랜잭션 내 가명들의 유효성을 검증하고 에너지 사용 정보를 식별하는 기능을 추가로 수행하는 청구 센터(220)를 도시한 것으로, 도 9에 도시된 청구 센터(220)는 도 8의 청구 센터(220)에 포함된 모듈에 더하여 가명 검증 모듈(225) 및 식별 모듈(227)을 추가로 포함할 수 있다.

[0169] 가명 검증 모듈(225)은 블록체인 망에 종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션이 게시된 경우, 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 마지막 블록 내 가명들의 조합의 유효성을 검증한다.

[0170] 일 실시예에 따르면, 가명 검증 모듈(225)은 마지막 블록의 블룸 필터를 조회하고, 가명들의 조합에 대한 블룸 필터의 보고 결과에 기초하여 가명들의 조합의 유효성을 검증할 수 있다.

[0171] 다른 실시예에 따르면, 가명 검증 모듈(225)은 블록체인에서 가명들의 조합이 포함된 트랜잭션을 탐색하고, 가명들의 조합에 포함된 가명들 각각에 대한 인증서를 검증함으로써 가명들의 조합의 유효성을 검증할 수 있다.

[0172] 식별 모듈(227)은 가명 검증 모듈(225)에 의해 검증된 가명들의 조합에 대응되는 에너지 사용 정보를 식별한다.

[0173] 한편, 도 10은 에너지 요금의 정상 지불 여부를 검증하는 기능을 추가로 수행하는 청구 센터(220)를 도시한 것으로, 도 10에 도시된 청구 센터(220)는 도 9의 청구 센터(220)에 포함된 모듈에 더하여 요금 검증 모듈(229)을 추가로 포함할 수 있다.

[0174] 요금 검증 모듈(229)은 가명 검증 모듈(225)에 의해 검증된 가명들의 조합으로 인한 선불 요금과, 검증된 가명들의 조합에 대응되는 에너지 소비 데이터를 확인함으로써 에너지 요금의 정상 지불 여부를 검증한다.

[0175] 일 실시예에 따르면, 요금 검증 모듈(229)의 검증 결과, 에너지 소비 데이터에 따른 에너지 요금이 선불 요금 이내인 것으로 판단되는 경우, 요금 검증 모듈(229)은 트랜잭션으로 게시된 가명들의 조합에 대해 사용 완료 상태로 처리할 수 있다.

[0176] 한편 일 실시예에 따르면, 요금 검증 모듈(229)의 검증 결과, 에너지 소비 데이터에 따른 에너지 요금이 선불 요금을 초과하는 것으로 판단되는 경우, 요금 검증 모듈(229)은 요금 청구 모듈(미도시)과 연계하여 요금 청구와 관련된 프로세스를 추가 진행할 수 있다.

[0177] 상기 도 8 내지 도 10에 도시된 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0178] 또한, 상기 도 8 내지 도 10에 도시된 실시예에서, 요금 징수 모듈(221), 인증서 발급 모듈(223), 가명 검증 모듈(225), 식별 모듈(227) 및 요금 검증 모듈(229)은 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0179] 도 11은 제1 실시예에 따른 사용자 단말(110)의 요금 처리 방법을 설명하기 위한 흐름도이다.

[0180] 우선, 사용자 단말(110)은 인증서로 인증된 가명 및 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성한다(1110).

[0181] 일 실시예에 따르면, 사용자 단말(110)은 가명을 생성하고, 블록체인 망에 포함된 인증 기관으로부터 가명에 대한 인증서를 획득한 다음, 가명, 가명에 대한 인증서 및 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성할 수 있다.

[0182] 이후, 사용자 단말(110)은 생성된 트랜잭션에 서명한다(1120).

[0183] 일 실시예에 따르면, 사용자 단말(110)은 트랜잭션 공개키 및 트랜잭션 공개키에 대한 트랜잭션 개인키를 생성하고, 트랜잭션을 트랜잭션 개인키로 서명할 수 있다.

[0184] 이후, 사용자 단말(110)은 서명된 트랜잭션을 블록체인 망에 게시한다(1130).

[0185] 이후, 사용자 단말(110)은 블록체인 망에 포함된 청구 센터로부터 가명 앞으로 청구된 에너지 요금을 지불한다(1140).

[0186] 도 12 및 도 13은 제1 실시예에 따른 청구 센터(120)의 요금 처리 방법을 설명하기 위한 흐름도이다.

[0187] 먼저 도 12를 참조하면, 청구 센터(120)는 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 마지막 블록 내 가명의 유효성을 검증한다(1210).

[0188] 일 실시예에 따르면, 청구 센터(120)는 마지막 블록의 블룸 필터를 조회하고, 가명에 대한 블룸 필터의 보고 결과에 기초하여 가명의 유효성을 검증할 수 있다.

[0189] 다른 실시예에 따르면, 청구 센터(120)는 블록체인에서 가명이 포함된 트랜잭션을 탐색하고, 가명에 대한 인증서를 검증함으로써 가명의 유효성을 검증할 수 있다.

[0190] 이후, 청구 센터(120)는 검증된 가명에 대응되는 에너지 사용 정보를 식별한다(1220).

[0191] 이후, 청구 센터(120)는 검증된 가명 중 적어도 일부 가명으로, 식별된 에너지 사용 정보에 따른 에너지 요금을 청구한다(1230).

[0192] 한편 도 13을 참조하면, 추가적인 실시예에 따른 청구 센터(120)는 청구에 따라 지불된 에너지 요금과, 에너지 요금이 지불된 가명에 대한 에너지 소비 데이터를 확인함으로써 청구에 따라 지불된 에너지 요금의 정상 지불 여부를 검증한다(1340).

[0193] 한편, 도 13의 단계 1310 내지 1330은 도 12를 참조하여 설명한 단계 1210 내지 1230과 실질적으로 대응되는 바, 이에 관한 중복되는 설명은 생략하기로 한다.

[0194] 도 14는 제2 실시예에 따른 사용자 단말(210)의 요금 처리 방법을 설명하기 위한 흐름도이다.

[0195] 우선, 사용자 단말(210)은 복수의 가명들에 대한 인증을 위해 선불 요금을 지불한다(1410).

[0196] 이후, 사용자 단말(210)은 종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합 및 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성한다(1420).

[0197] 일 실시예에 따르면, 사용자 단말(210)은 가명들을 생성하고, 블록체인 망에 포함된, 인증 기관을 겸하는 청구 센터로부터 가명들 각각에 대한 인증서를 획득한 다음, 가명들의 조합, 조합에 포함된 가명들 각각에 대한 인증서 및 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성할 수 있다.

[0198] 이후, 사용자 단말(210)은 생성된 트랜잭션에 서명한다(1430).

[0199] 일 실시예에 따르면, 사용자 단말(210)은 트랜잭션 공개키 및 트랜잭션 공개키에 대응되는 트랜잭션 개인키를 생성하고, 트랜잭션을 트랜잭션 개인키로 서명할 수 있다.

[0200] 이후, 사용자 단말(210)은 서명된 트랜잭션을 블록체인 망에 게시한다(1440).

[0201] 도 15 내지 도 17은 제2 실시예에 따른 청구 센터(220)의 요금 처리 방법을 설명하기 위한 흐름도이다.

[0202] 먼저 도 15를 참조하면, 청구 센터(220)는 인증된 사용자 단말로부터 선불 요금을 징수한다(1510).

[0203] 이후, 청구 센터(220)는 인증된 사용자 단말로부터 선불 요금이 지불되었는지를 판단한다(1520).

[0204] 이후, 인증된 사용자 단말로부터 선불 요금이 지불된 경우, 청구 센터(220)는 인증된 사용자 단말에 대응되는 복수의 가명들 각각에 대해 종류에 따라 가격이 상이한 복수의 인증서를 발급한다(1530). 이때, 발급된 인증서들의 총 가격은 기 지불된 선불 요금과 대응된다.

[0205] 한편 도 16을 참조하면, 추가적인 실시예에 따른 청구 센터(220)는 블록체인 망에 '종류에 따라 가격이 상이한 복수의 인증서 중 어느 하나로 인증된 가명들의 조합' 및 '가명들의 조합에 대응되는 에너지 사용 정보'를 포함하는 트랜잭션이 게시되었는지를 판단한다(1640).

[0206] 이후, 상술한 트랜잭션이 게시된 경우, 청구 센터(220)는 블록체인 망의 블록체인을 구성하는 마지막 블록을 참조하여, 마지막 블록 내 가명들의 조합의 유효성을 검증한다(1650).

[0207] 일 실시예에 따르면, 청구 센터(220)는 마지막 블록의 블룸 필터를 조회하고, 가명들의 조합에 대한 블룸 필터의 보고 결과에 기초하여 가명들의 조합의 유효성을 검증할 수 있다.

[0208] 다른 실시예에 따르면, 청구 센터(220)는 블록체인에서 가명들의 조합이 포함된 트랜잭션을 탐색하고, 가명들의 조합에 포함된 가명들 각각에 대한 인증서를 검증함으로써 가명들의 조합의 유효성을 검증할 수 있다.

[0209] 이후, 청구 센터(220)는 검증된 가명들의 조합에 대응되는 에너지 사용 정보를 식별한다(1660).

[0210] 한편, 도 16의 단계 1610 내지 1630은 도 15를 참조하여 설명한 단계 1510 내지 1530과 실질적으로 대응되는 바, 이에 관한 중복되는 설명은 생략하기로 한다.

[0211] 또한 도 17을 참조하면, 추가적인 실시예에 따른 청구 센터(220)는 검증된 가명들의 조합으로 인한 선불 요금과, 검증된 가명들의 조합에 대응되는 에너지 소비 데이터를 확인함으로써 에너지 요금의 정상 지불 여부를 검증한다(1770).

[0212] 한편, 도 17의 단계 1710 내지 1760은 도 16을 참조하여 설명한 단계 1610 내지 1660과 실질적으로 대응되는 바, 이에 관한 중복되는 설명은 생략하기로 한다.

[0213] 상기 도시된 흐름도 도 11 내지 도 17에서는 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.

[0214] 도 18은 일 실시예에 따른 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0215] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 이때, 컴퓨팅 장치(12)는 제1 실시예에 따른 사용자 단말(110)일 수도 있고, 제2 실시예에 따른 사용자 단말(210)일 수도 있다.

[0216] 한편, 컴퓨팅 장치(12)는 제1 실시예에 따른 청구 센터(120)일 수도 있으며, 제2 실시예에 따른 청구 센터(220)일 수도 있다.

[0217] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0218] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0219] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0220] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.

[0221] 한편, 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.

[0222] 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 청구범위 뿐만 아니라 이 청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0224] 10: 컴퓨팅 환경

12: 컴퓨팅 장치

14: 프로세서

16: 컴퓨터 판독 가능 저장 매체

18: 통신 버스

20: 프로그램

22: 입출력 인터페이스

24: 입출력 장치

26: 네트워크 통신 인터페이스

100, 200: 요금 처리 시스템

110, 210: 사용자 단말

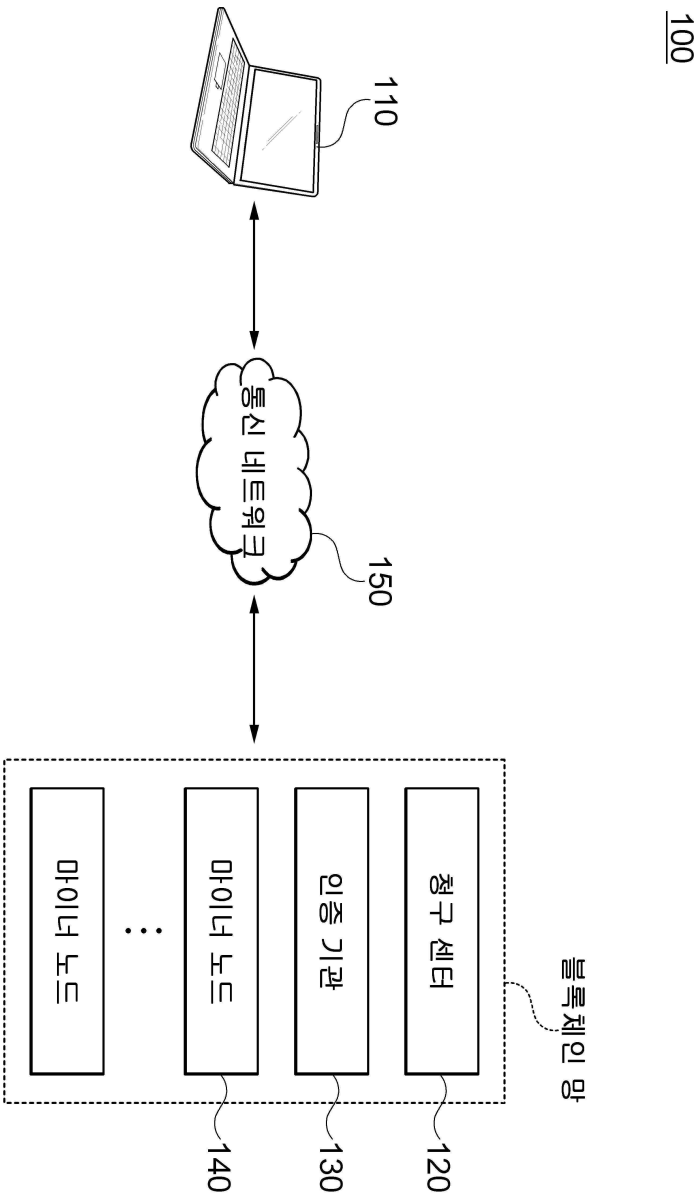
120, 220: 청구 센터

130: 인증 기관

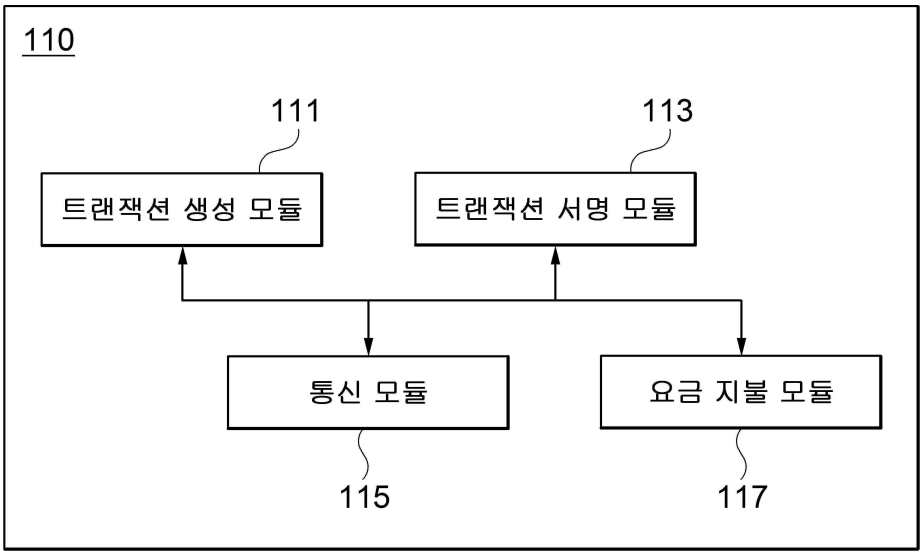
140: 마이너 노드

도면

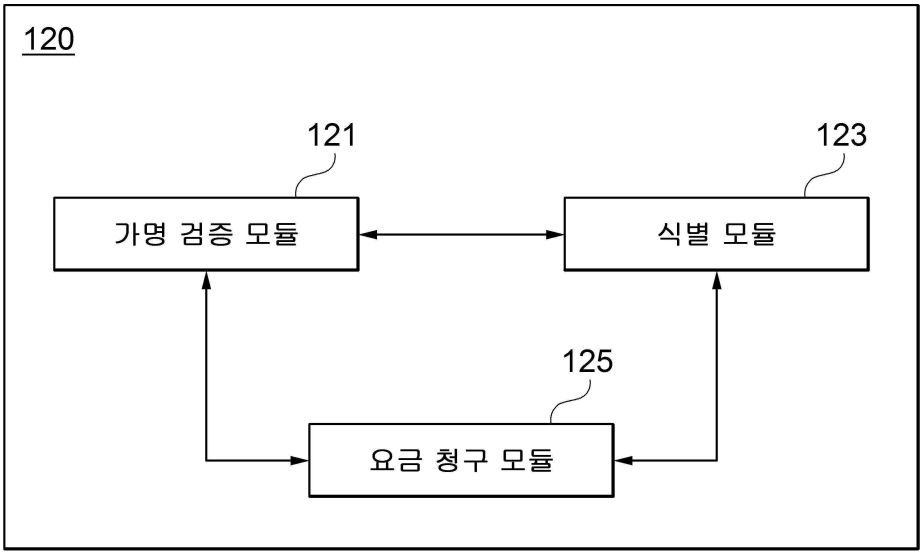
도면1



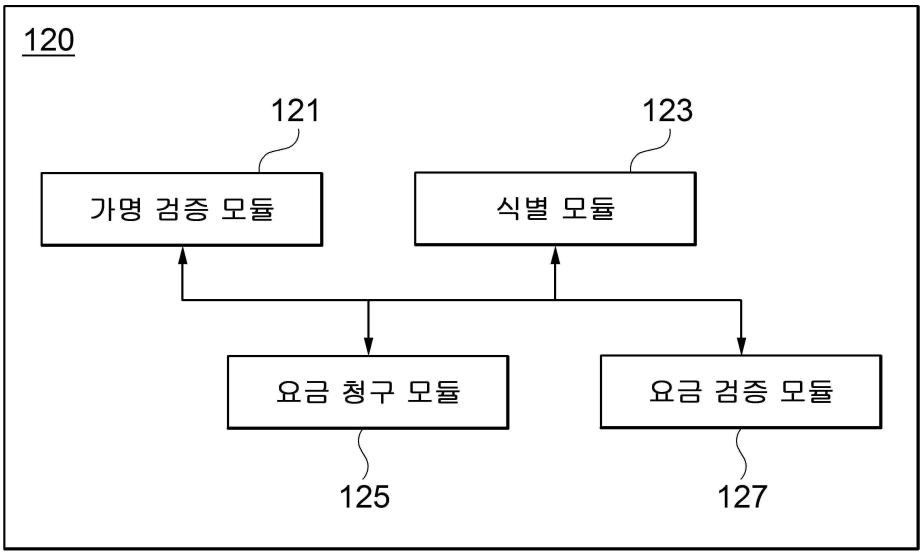
도면2


110
111
113
트랜잭션 생성 모듈
트랜잭션 서명 모듈
통신 모듈
요금 지불 모듈
115
117

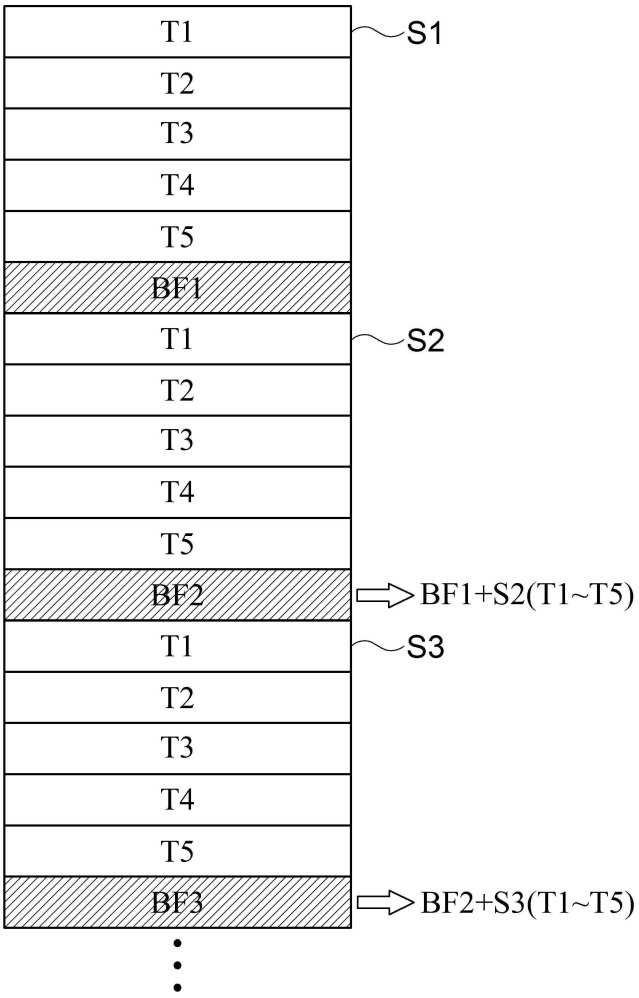
도면3


120
121
123
가명 검증 모듈
식별 모듈
125
요금 청구 모듈

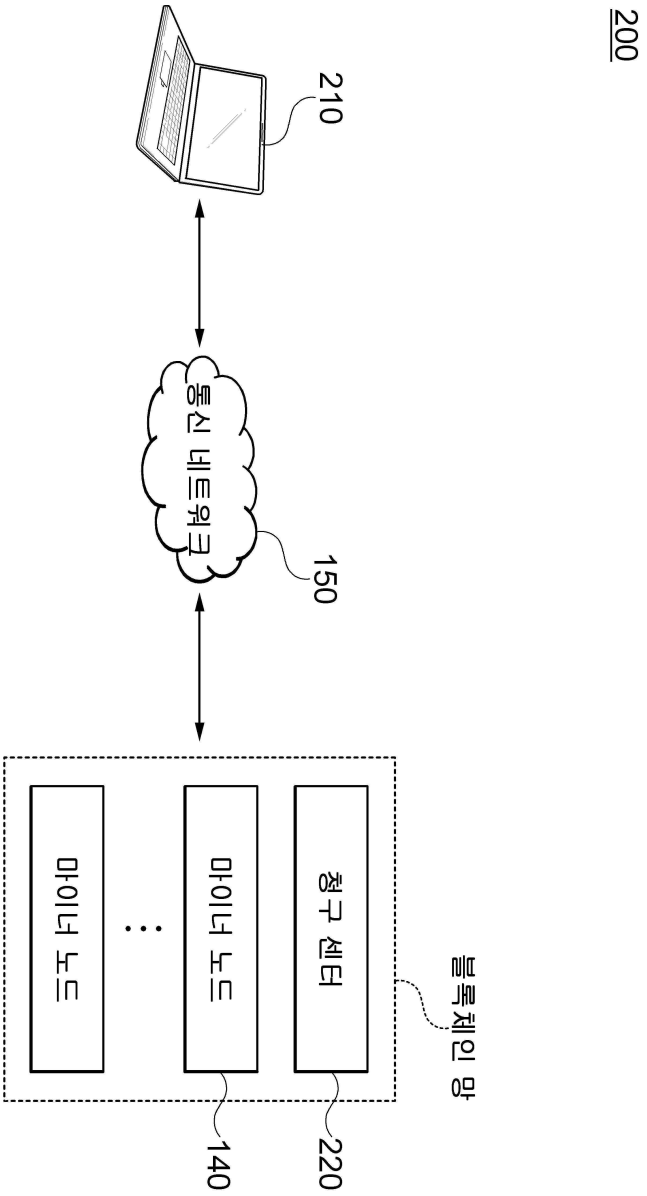
도면4


120
121
123
가명 검증 모듈
식별 모듈
요금 청구 모듈
요금 검증 모듈
125
127

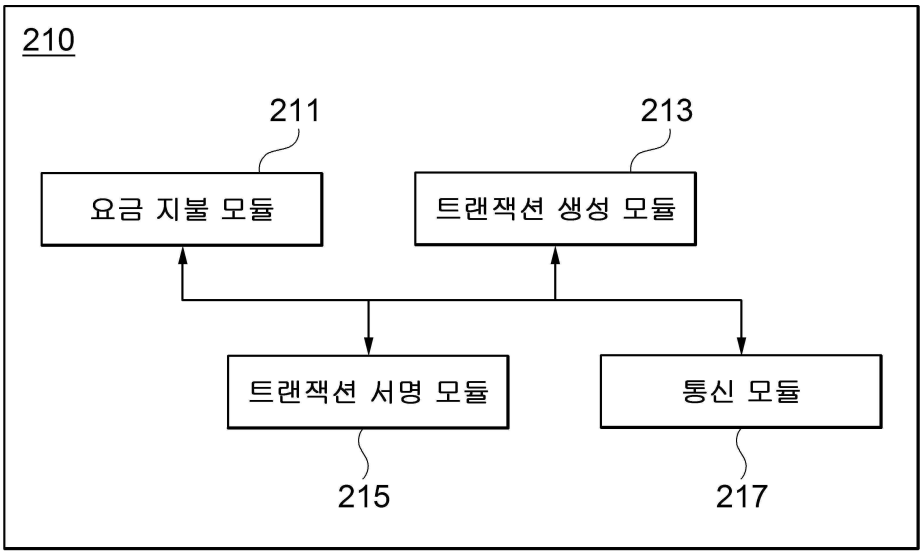
도면5


T1
T2
T3
T4
T5
BF1
T1
T2
T3
T4
T5
BF2
T1
T2
T3
T4
T5
BF3
S1
S2
S3
BF1+S2(T1~T5)
BF2+S3(T1~T5)

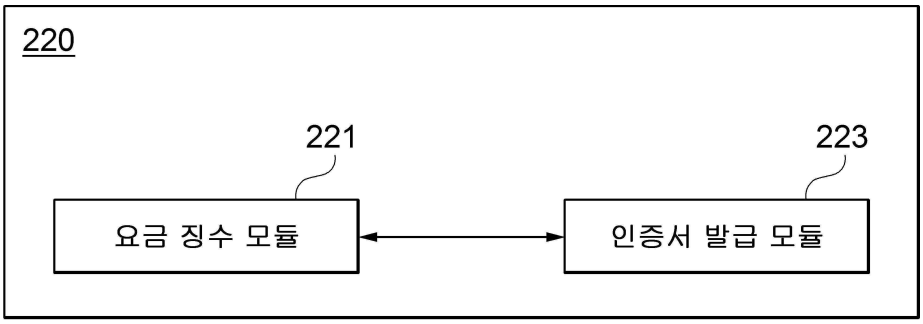
도면6



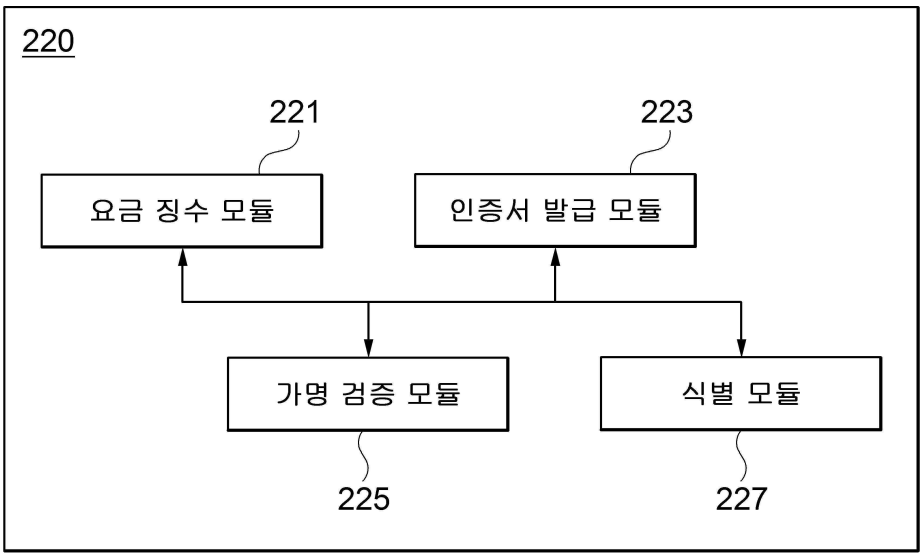
도면7


210
211
213
요금 지불 모듈
트랜잭션 생성 모듈
트랜잭션 서명 모듈
통신 모듈
215
217

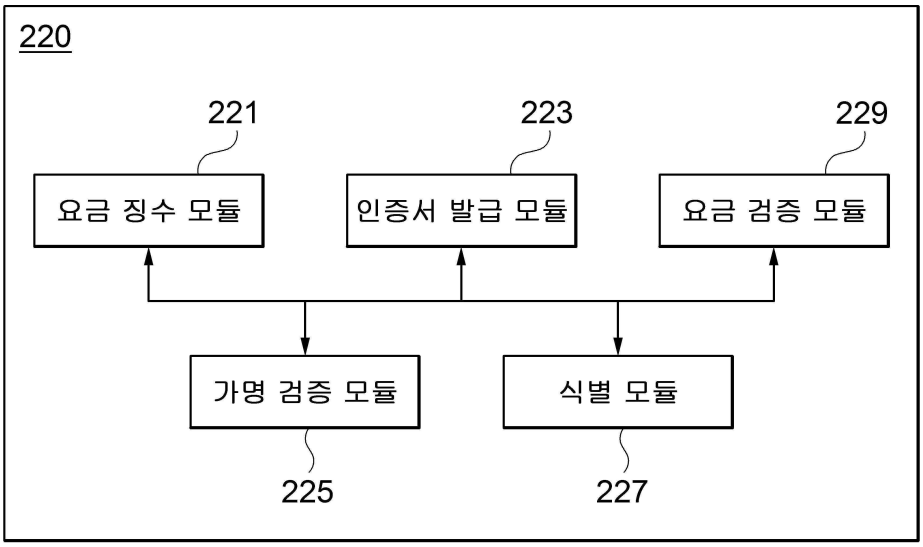
도면8


220
221
223
요금 징수 모듈
인증서 발급 모듈

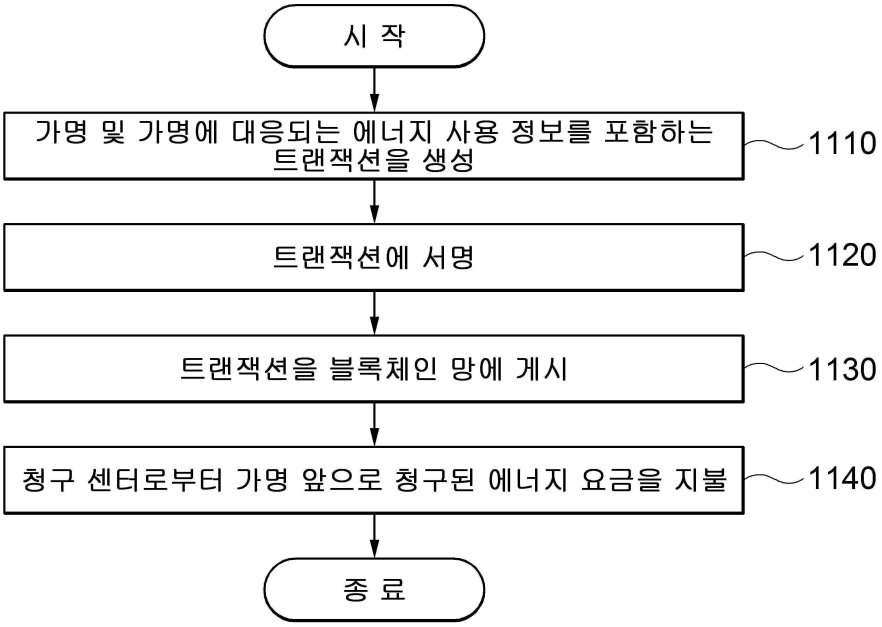
도면9


220
221
223
요금 징수 모듈
인증서 발급 모듈
가명 검증 모듈
식별 모듈
225
227

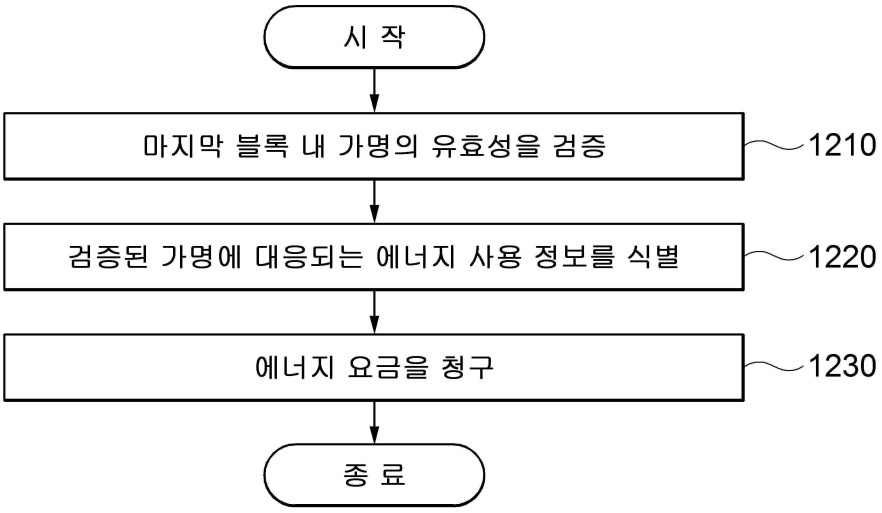
도면10


220
221
223
229
요금 징수 모듈
인증서 발급 모듈
요금 검증 모듈
가명 검증 모듈
식별 모듈
225
227

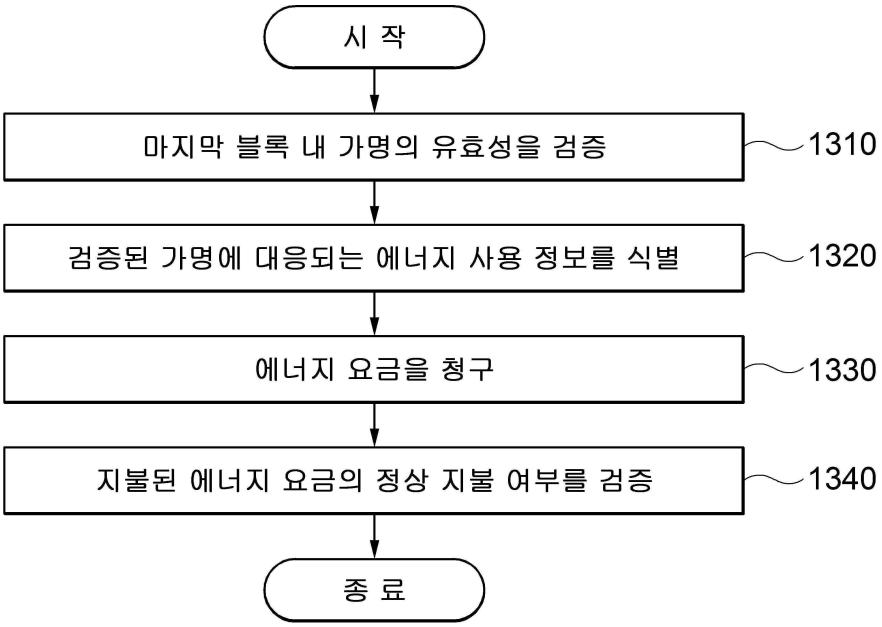
도면11


시 작
가명 및 가명에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성
1110
트랜잭션에 서명
1120
트랜잭션을 블록체인 망에 게시
1130
청구 센터로부터 가명 앞으로 청구된 에너지 요금을 지불
1140
종 료

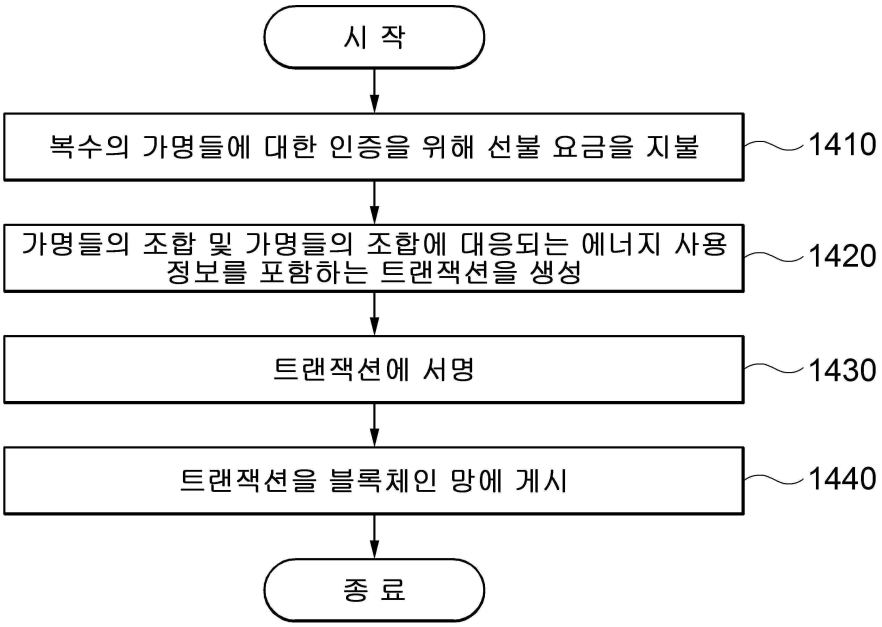
도면12


시 작
마지막 블록 내 가명의 유효성을 검증
1210
검증된 가명에 대응되는 에너지 사용 정보를 식별
1220
에너지 요금을 청구
1230
종 료

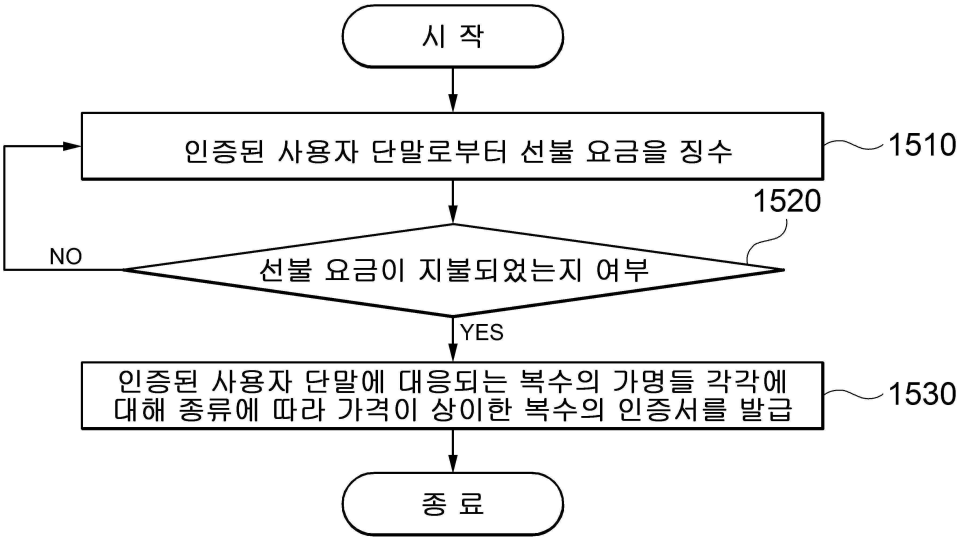
도면13


시 작
마지막 블록 내 가명의 유효성을 검증
1310
검증된 가명에 대응되는 에너지 사용 정보를 식별
1320
에너지 요금을 청구
1330
지불된 에너지 요금의 정상 지불 여부를 검증
1340
종 료

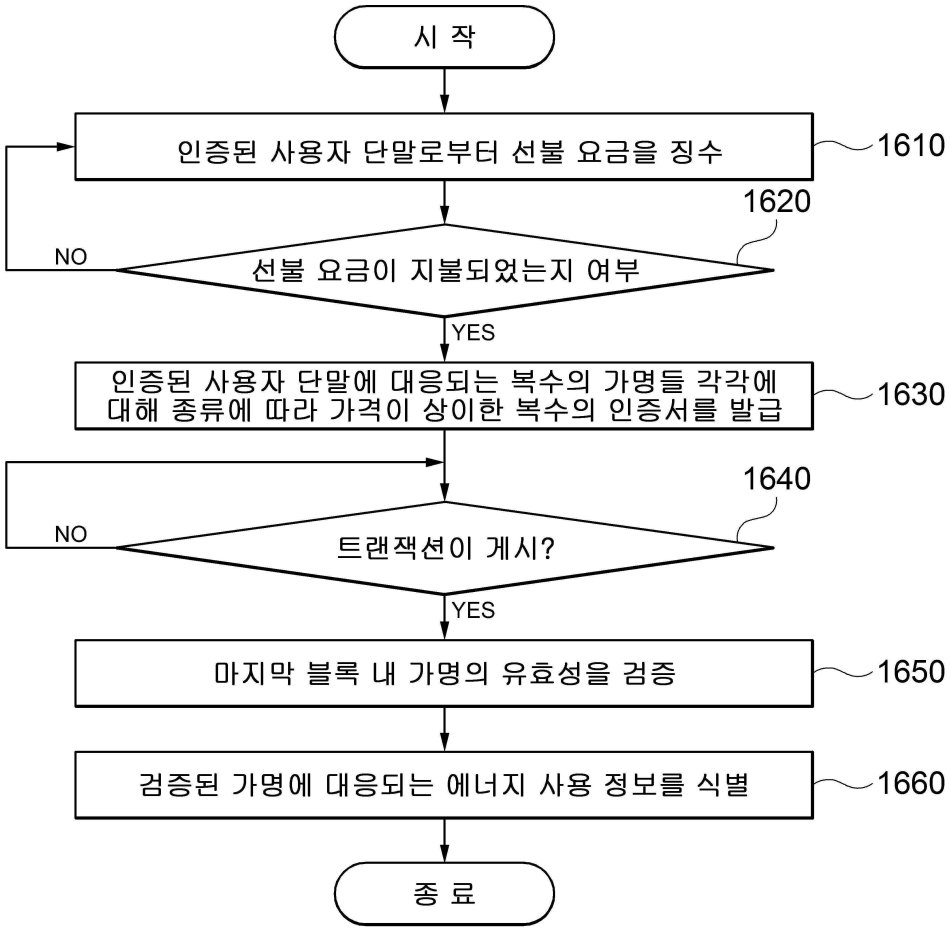
도면14


시 작
복수의 가명들에 대한 인증을 위해 선불 요금을 지불
1410
가명들의 조합 및 가명들의 조합에 대응되는 에너지 사용 정보를 포함하는 트랜잭션을 생성
1420
트랜잭션에 서명
1430
트랜잭션을 블록체인 망에 게시
1440
종 료

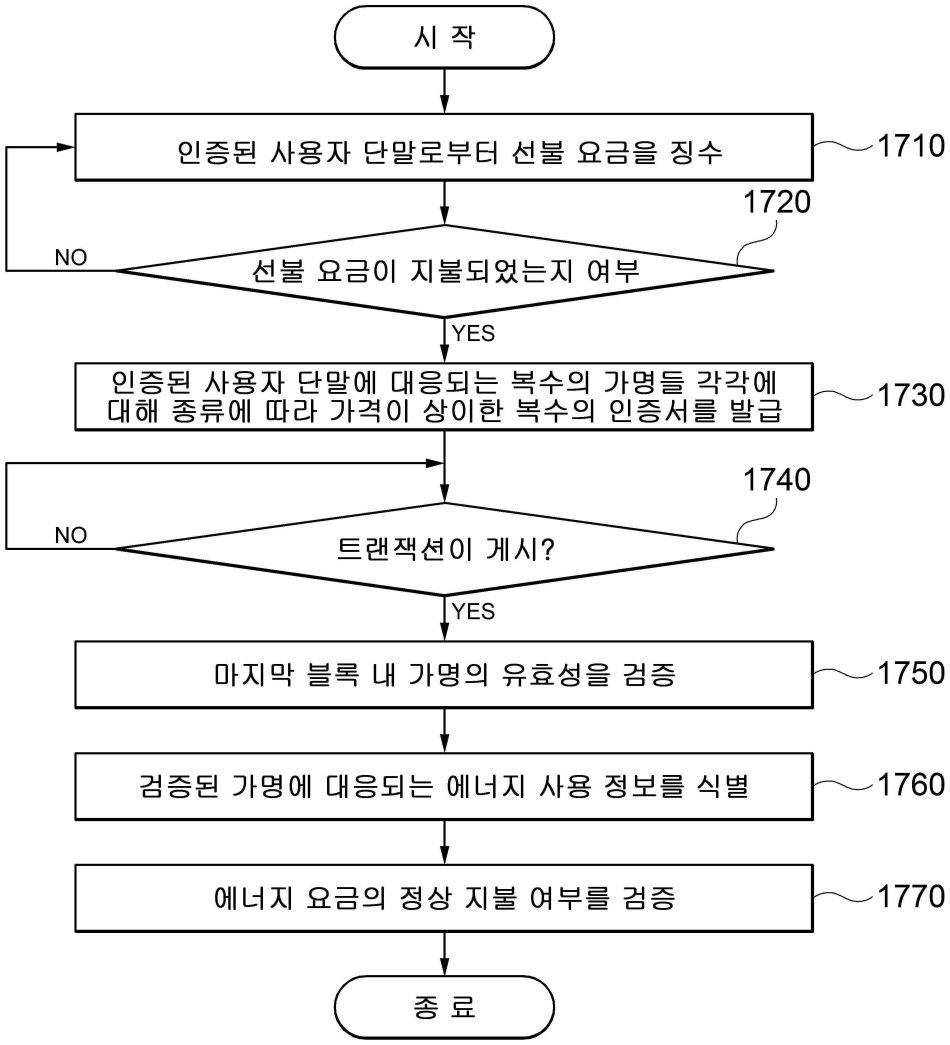
도면15


시 작
인증된 사용자 단말로부터 선불 요금을 징수
1510
1520
NO
선불 요금이 지불되었는지 여부
YES
인증된 사용자 단말에 대응되는 복수의 가명들 각각에 대해 종류에 따라 가격이 상이한 복수의 인증서를 발급
1530
종 료

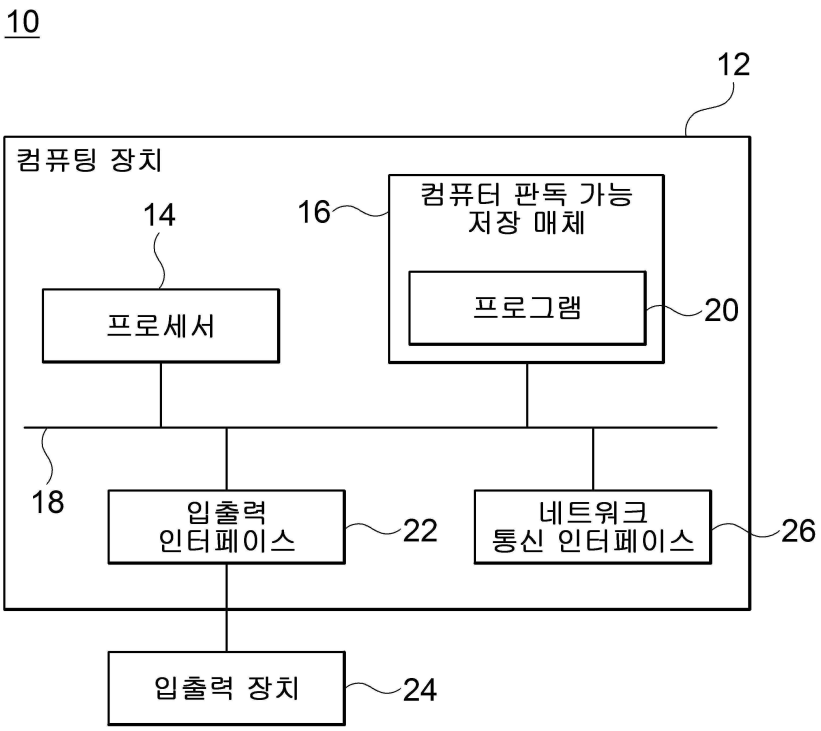
도면16


시 작
인증된 사용자 단말로부터 선불 요금을 징수
1610
1620
NO
선불 요금이 지불되었는지 여부
YES
인증된 사용자 단말에 대응되는 복수의 가명들 각각에 대해 종류에 따라 가격이 상이한 복수의 인증서를 발급
1630
1640
NO
트랜잭션이 게시?
YES
마지막 블록 내 가명의 유효성을 검증
1650
검증된 가명에 대응되는 에너지 사용 정보를 식별
1660
종 료

도면17


시 작
인증된 사용자 단말로부터 선불 요금을 징수
1710
1720
NO
선불 요금이 지불되었는지 여부
YES
인증된 사용자 단말에 대응되는 복수의 가명들 각각에 대해 종류에 따라 가격이 상이한 복수의 인증서를 발급
1730
1740
NO
트랜잭션이 게시?
YES
마지막 블록 내 가명의 유효성을 검증
1750
검증된 가명에 대응되는 에너지 사용 정보를 식별
1760
에너지 요금의 정상 지불 여부를 검증
1770
종 료

도면18


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능
저장 매체
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24