(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2021 년 6 월 3 일 (03.06.2021)

WIPO | PCT

(10) 국제공개번호
WO 2021/107304 A1

(51) 국제특허분류:
G06Q 50/06 (2012.01) *H04L 9/06* (2006.01)

(21) 국제출원번호: PCT/KR2020/007773

(22) 국제출원일: 2020 년 6 월 16 일 (16.06.2020)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2019-0156426 2019 년 11 월 29 일 (29.11.2019) KR

(71) 출원인: 인하대학교 산학협력단 (**INHA-INDUSTRY PARTNERSHIP INSTITUTE**) [KR/KR]; 22212 인천시 미추홀구 인하로 100, Incheon (KR).

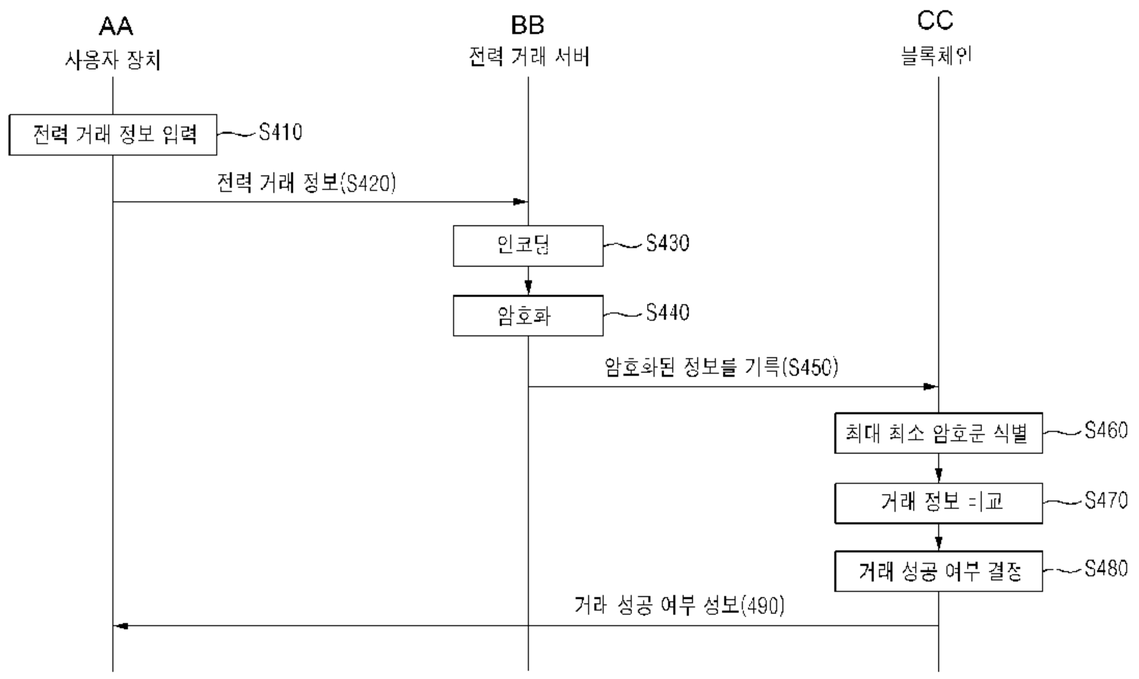
(72) 발명자: 이문규 (**LEE, Mun Kyu**); 22212 인천시 미추홀구 인하로 100, Incheon (KR). 손예별 (**SON, Ye Byoul**); 22212 인천시 미추홀구 인하로 100, Incheon (KR).

(74) 대리인: 양성보 (**YANG, Sungbo**); 06099 서울시 강남구 선릉로125길 14 삼성빌딩 2층 피앤티특허법률사무소, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,

(54) **Title:** BLOCKCHAIN-BASED ELECTRIC POWER TRANSACTION SYSTEM AND METHOD

(54) **발명의 명칭:** 블록체인 기반 전력 거래 시스템 및 방법



S410 ... Input electrical power transaction information
S420 ... Electrical power transaction information
S430 ... Encoding
S440 ... Encryption
S450 ... Record encrypted information
S460 ... Identify minimum and maximum cipher texts
S470 ... Compare transaction information
S480 ... Determine whether transaction has been successfully completed
S490 ... Information on whether transaction has been successfully completed
AA ... User device
BB ... Electrical power transaction server
CC ... Blockchain

(57) **Abstract:** Disclosed are a blockchain-based electric power transaction system and method. The blockchain-based electric power transaction system, according to one aspect of the present invention, comprises: a user device for receiving electric power transaction information; an electric power transaction server which receives the electric power transaction information from the user device, encodes the electric power transaction information, and encrypts the encoded information; and a blockchain which inputs a ciphertext pair in a seller list or a buyer list upon receiving the ciphertext pair from the electric power transaction server, determines whether a transaction has been successfully completed by using seller ciphertext pairs and buyer ciphertext pairs in the seller list and the buyer list, and transmits information on whether the transaction has been successfully completed to the electrical power transaction server.

[다음 쪽 계속]

WO 2021/107304 A1

SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(57) 요약서: 블록체인 기반 전력 거래 시스템 및 방법이 개시된다. 본 발명의 일 측면에 따른 블록체인 기반 전력 거래 시스템은, 전력 거래 정보를 입력받는 사용자 장치, 상기 사용자 장치로부터 전력 거래 정보를 수신하고, 상기 전력 거래 정보를 인코딩하며, 상기 인코딩된 정보를 암호화하는 전력 거래 서버, 상기 전력 거래 서버로부터 암호문 쌍을 수신하면, 상기 암호문 쌍을 판매자 목록 또는 구매자 목록에 입력하고, 상기 판매자 목록 및 구매자 목록에 있는 판매자 암호문 쌍들 및 구매자 암호문 쌍들을 이용하여 거래 성공 여부를 결정하며, 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 블록체인을 포함한다.

명세서

발명의 명칭: 블록체인 기반 전력 거래 시스템 및 방법

기술분야

[1] 본 발명은 블록체인 기반 전력 거래 시스템 및 방법에 관한 것으로서, 보다 상세하게는 블록체인 기술 기반의 전력거래 환경에서 거래 당사자 이외의 제3자 는 거래내용을 모르면서도 결과의 무결성 증명에 기여할 수 있는 블록체인 기반 전력 거래 시스템 및 방법에 관한 것이다.

[2]

배경기술

[3] 스마트 그리드 시스템(Smart Grid System)은 전력회사와 수용가를 이어주는 양방향 시스템으로, 수용가 측에 설치되어 있는 다양한 기기들의 데이터를 중간단계의 데이터집중장치(DCU)를 통하여 수집한 후, 수집된 데이터를 전력회사 서버에 전송하고 반대로 서버에서 수용가로 데이터를 전송하는 양방향 인프라를 말한다. 이러한 스마트 그리드 기술은 다양한 분산자원과 소비자 사이에 여러 정보를 전달하고 의향을 전달함으로써 전력망 운용의 효율을 증대시키는데 많은 역할을 하고 있다. 하지만, 이러한 스마트 그리드 기술은 물리적인 전력망을 운영하는데 초점을 두고 있기 때문에 전력거래에 대한 정산 및 과금의 실시간성은 부족하며, 또한 현물에 대한 금융거래이기 때문에 금융시스템을 따로 구축해야 한다는 문제점 역시 여전히 가지고 있다.

[4] 블록체인 기술이란, 신뢰할 수 있는 제3자 없이도 데이터를 검증할 수 있는 기술이다. 블록 하나에는 이용하고자 하는 거래(데이터)와 이전 블록에 대한 정보를 담고 있으며, 이 블록이 유효함을 정해진 방식으로 검증하여 모든 사람들이 블록이 유효함을 확인한다. 검증을 위한 대표적인 예로는 Proof-of-Work(PoW)라는 특정 난이도에 맞는 hash값을 찾는 방법이 있다. 이 hash값을 찾기 위해서는 computing power를 이용해야 하며, 많은 computing power를 쓴 사용자가 유효한 블록을 검증하였다고 판단하고 블록체인에 블록을 연결하여 공개한다.

[5] 이러한 방식을 이용하여 블록체인은 은행과 같은 제3의 특정 기관이나 관리자 없이 금전적인 거래를 가능하게 하며, 이를 이용한 대표적인 예로 비트코인이 있다. 비트코인은 단순한 금전적인 거래뿐 아니라 데이터를 블록에 올릴 수 있다는 점을 이용하여 간단한 계약을 할 수 있는 거래 또한 가능하게 한다. 이후 등장한 이더리움 블록체인은 비트코인의 단점인 간단한 계약만을 이용할 수 있다는 점을 없애고, 완전한 프로그래밍을 가능하게 하여 다양한 프로그램을 구현할 수 있게 제작하여 암호화폐로의 역할뿐 아니라 플랫폼의 역할도 할 수 있게 되었다. 이러한 장점으로 인해, 간단한 계약거래가 아닌 의료정보 열람 및 공유, 자기소개서 공유 등 좀 더 복잡한 계약 또한 쉽게 구현하고 이용하는 것도

가능하다. 따라서 현재 다양한 분야에서 이 기술을 접목시켜, 제 3자의 개입 없이 P2P 거래가 가능하게 하기 위한 프로젝트들을 진행 중이다.

[6] 그러나 데이터를 블록체인 상의 블록에 올리면, 데이터 내용이 거래 당사자만이 아니라 블록체인을 사용하고 있는 모두에게 공개되는 문제가 생긴다. 즉, 블록체인은 무결성 문제를 효과적으로 해결하지만 데이터의 기밀성 문제가 야기된다.

[7] 이에, 거래 당사자 이외의 제 3자는 거래내용을 모르면서도 거래 결과의 무결성을 증명할 수 있는 기술 개발이 요구되고 있다.

[8] 본 발명과 관련된 선행기술로는 등록특허공보 제10-1848896호(2018.04.13 공고, 발명의 명칭 : 블록체인을 이용한 선불형 전력 판매 및 전력 사용 방법)가 있다.

[9]

발명의 상세한 설명

기술적 과제

[10] 본 발명은 전술한 문제점을 개선하기 위하여 안출된 것으로, 본 발명의 일 측면에 따른 목적은 블록체인 기술 기반의 전력거래 환경에서 거래 당사자 이외의 제 3자는 거래내용을 모르면서도 결과의 무결성 증명에 기여할 수 있도록 하는 블록체인 기반 전력 거래 시스템 및 방법을 제공하는 것이다.

[11] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

[12]

과제 해결 수단

[13] 본 발명의 일 측면에 따른 블록체인 기반 전력 거래 시스템은, 전력 거래 정보를 입력받는 사용자 장치, 상기 사용자 장치로부터 전력 거래 정보를 수신하고, 상기 전력 거래 정보를 인코딩하며, 상기 인코딩된 정보를 암호화하는 전력 거래 서버, 상기 전력 거래 서버로부터 암호문 쌍을 수신하면, 상기 암호문 쌍을 판매자 목록 또는 구매자 목록에 입력하고, 상기 판매자 목록 및 구매자 목록에 있는 판매자 암호문 쌍들 및 구매자 암호문 쌍들을 이용하여 거래 성공 여부를 결정하며, 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 블록체인을 포함한다.

[14] 본 발명에서 상기 전력 거래 서버는, 상기 전력 거래 정보의 거래 희망 금액을 인코딩하여 제1 벡터 및 제2 벡터를 생성하는 인코딩부, 상기 제1 벡터에 대한 비밀키를 생성하고, 상기 제2 벡터에 대한 암호문을 생성하며, 상기 생성된 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인에 전송하는 암호화부를 포함할 수 있다.

[15] 본 발명에서 상기 인코딩부는, 상기 거래 희망 금액을 기 설정된 단위 전력당

거래 금액 범위와 비교하고, 그 비교결과를 기초로 상기 거래 희망 금액을 인코딩하여 제1 벡터 및 제2 벡터를 생성할 수 있다.

[16] 본 발명에서 상기 암호화부는, 키 생성 알고리즘을 이용하여 상기 제1 벡터에 대한 비밀키를 생성하고, 암호화 알고리즘을 이용하여 상기 제2 벡터에 대한 암호문을 생성한 후, 상기 비밀키 및 암호문을 포함하는 암호문 쌍을 상기 블록체인으로 전송할 수 있다.

[17] 본 발명에서 상기 블록체인은, 상기 전력 거래 서버로부터 암호문 쌍을 수신하면, 상기 암호문 쌍의 요청자를 확인하여, 판매자 목록 또는 구매자 목록에 기록하는 기록 처리부, 상기 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 최솟값에 대한 판매자 암호문 쌍을 찾고, 상기 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 최댓값에 대한 구매자 암호문 쌍을 찾는 비교부, 상기 최솟값에 대한 판매자 암호문 쌍 및 상기 최댓값에 대한 구매자 암호문 쌍을 함수 복호화 연산하여, 거래 성공 여부를 결정하고, 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 거래 처리부를 포함할 수 있다.

[18] 본 발명에서 상기 비교부는, 상기 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 판매자 암호문 쌍에 인코딩된 판매 희망 금액들 간의 대소를 비교함으로써 상기 판매자 목록 중 최솟값에 대한 판매자 암호문 쌍을 찾고, 상기 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 구매자 암호문 쌍에 인코딩된 구매 희망 금액들 간의 대소를 비교함으로써 상기 구매자 목록 중 최댓값에 대한 구매자 암호문 쌍을 찾을 수 있다.

[19] 본 발명에서 상기 거래 처리부는, 상기 최솟값에 대한 판매자 암호문 쌍 및 상기 최댓값에 대한 구매자 암호문 쌍을 함수 복호화하여 내적을 산출하고, 상기 산출된 내적에 기초하여 해당 판매자와 구매자 간의 거래 성공 여부를 결정할 수 있다.

[20] 본 발명에서 상기 거래 처리부는, 상기 최솟값에 대한 판매자 암호문 쌍의 비밀키와 상기 최댓값에 대한 구매자 암호문 쌍의 암호문에 대해 함수 복호화 연산을 적용함으로써 상기 판매자 목록 중 최솟값에 대해 인코딩된 제1 벡터 및 상기 구매자 목록 중 최댓값에 대해 인코딩된 제2 벡터의 내적 결과를 산출하고, 상기 산출된 내적이 '1'인 경우 상기 판매자와 구매자 간의 거래 성공으로 결정하며, 상기 내적이 '0'인 상기 판매자와 구매자 간의 거래 실패로 결정할 수 있다.

[21] 본 발명에서 상기 거래 처리부는, 상기 판매자와 구매자 간의 거래 성공으로 결정한 경우, 상기 판매자의 주소 및 전력 거래 정보, 상기 구매자의 주소 및 전력 거래 정보를 상기 전력 거래 서버로 전송할 수 있다.

[22] 본 발명의 다른 측면에 따른 블록체인 기반 전력 거래 방법은, 전력 거래 서버가 사용자 장치로부터 전력 거래 정보를 수신하면, 상기 전력 거래 정보를

인코딩하고, 상기 인코딩된 정보를 암호화하는 단계, 블록체인이 상기 전력 거래 서버로부터 암호문 쌍을 수신하면, 상기 암호문 쌍을 판매자 목록 또는 구매자 목록에 입력하고, 상기 판매자 목록 및 구매자 목록에 있는 판매자 암호문 쌍들 및 구매자 암호문 쌍들을 이용하여 거래 성공 여부를 결정하며, 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 단계를 포함한다.

[23] 본 발명에서 상기 전력 거래 정보를 인코딩하고, 상기 인코딩된 정보를 암호화하는 단계는, 상기 전력 거래 서버가 상기 전력 거래 정보의 거래 희망 금액을 인코딩하여 제1 벡터 및 제2 벡터를 생성하는 단계, 상기 전력 거래 서버가 상기 제1 벡터에 대한 비밀키를 생성하고, 상기 제2 벡터에 대한 암호문을 생성하며, 상기 생성된 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인에 전송하는 단계를 포함할 수 있다.

[24] 본 발명은 상기 제1 벡터 및 제2 벡터를 생성하는 단계에서, 상기 전력 거래 서버는, 상기 거래 희망 금액을 기 설정된 단위 전력당 거래 금액 범위와 비교하고, 그 비교결과를 기초로 상기 거래 희망 금액을 인코딩하여 제1 벡터 및 제2 벡터를 생성할 수 있다.

[25] 본 발명은 상기 생성된 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인에 전송하는 단계에서, 상기 전력 거래 서버는 키 생성 알고리즘을 이용하여 상기 제1 벡터에 대한 비밀키를 생성하고, 암호화 알고리즘을 이용하여 상기 제2 벡터에 대한 암호문을 생성한 후, 상기 비밀키 및 암호문을 포함하는 암호문 쌍을 상기 블록체인으로 전송할 수 있다.

[26] 본 발명에서 상기 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 단계는, 상기 블록체인이 상기 전력 거래 서버로부터 암호문 쌍을 수신하면, 상기 암호문 쌍의 요청자를 확인하여, 판매자 목록 또는 구매자 목록에 기록하는 단계, 상기 블록체인이 상기 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 최솟값에 대한 판매자 암호문 쌍을 찾고, 상기 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 최댓값에 대한 구매자 암호문 쌍을 찾는 단계, 상기 블록체인이 상기 최솟값에 대한 판매자 암호문 쌍 및 상기 최댓값에 대한 구매자 암호문 쌍을 함수 복호화 연산하여, 거래 성공 여부를 결정하고, 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 단계를 포함할 수 있다.

[27] 본 발명은 상기 최댓값에 대한 구매자 암호문 쌍을 찾는 단계에서, 상기 블록체인은, 상기 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 판매자 암호문 쌍에 인코딩된 판매 희망 금액들 간의 대소를 비교함으로써 상기 판매자 목록 중 최솟값에 대한 판매자 암호문 쌍을 찾고, 상기 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 구매자 암호문 쌍에 인코딩된 구매 희망 금액들 간의 대소를 비교함으로써 상기 구매자 목록 중 최댓값에 대한 구매자 암호문 쌍을 찾을 수 있다.

[28] 본 발명은 상기 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는

단계에서, 상기 블록체인은 상기 최솟값에 대한 판매자 암호문 쌍 및 상기 최댓값에 대한 구매자 암호문 쌍을 함수 복호화하여 내적을 산출하고, 상기 산출된 내적에 기초하여 해당 판매자와 구매자 간의 거래 성공 여부를 결정할 수 있다.

[29] 본 발명은 상기 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 단계에서, 상기 블록체인은 상기 최솟값에 대한 판매자 암호문 쌍의 비밀키와 상기 최댓값에 대한 구매자 암호문 쌍의 암호문에 대해 함수 복호화 연산을 적용함으로써 상기 판매자 목록 중 최솟값에 대해 인코딩된 제1 벡터 및 상기 구매자 목록 중 최댓값에 대해 인코딩된 제2 벡터의 내적 결과를 산출하고, 상기 산출된 내적이 '1'인 경우 상기 판매자와 구매자 간의 거래 성공으로 결정하며, 상기 내적이 '0'인 상기 판매자와 구매자 간의 거래 실패로 결정할 수 있다.

[30] 본 발명은 상기 판매자와 구매자 간의 거래 성공으로 결정한 경우, 상기 판매자의 주소 및 전력 거래 정보, 상기 구매자의 주소 및 전력 거래 정보를 상기 전력 거래 서버로 전송할 수 있다.

[31]

발명의 효과

[32] 본 발명의 일 실시예에 따른 블록체인 기반 전력 거래 시스템 및 방법은, 블록체인 기반의 함수암호 기법을 이용하여 거래 데이터를 암호화하여 보호함과 동시에, 거래 당사자 이외의 제 3자는 거래 내용을 모르면서도 결과의 무결성 증명에 기여할 수 있다. 즉, 암호화된 상태에서 크기 비교가 가능하기 때문에 거래 내용을 제 3자가 확인하지 못하더라도 크기 비교의 결과는 알 수 있고, 이로 인해 블록체인의 기밀성 문제를 해결할 수 있다.

[33] 한편, 본 발명의 효과는 이상에서 언급한 효과들로 제한되지 않으며, 이하에서 설명할 내용으로부터 통상의 기술자에게 자명한 범위 내에서 다양한 효과들이 포함될 수 있다.

[34]

도면의 간단한 설명

[35] 도 1은 본 발명의 일 실시예에 따른 블록체인 기반 전력 거래 시스템을 개략적으로 나타낸 도면이다.

[36] 도 2는 본 발명의 일 실시예에 따른 전력 거래 서버를 개략적으로 나타낸 블록도이다.

[37] 도 3은 본 발명의 일 실시예에 따른 스마트 컨트랙트를 실행하는 블록체인을 설명하기 위한 블록도이다.

[38] 도 4는 본 발명의 일 실시예에 따른 블록체인 기반 전력 거래 방법을 설명하기 위한 도면이다.

[39]

발명의 실시를 위한 최선의 형태

[40] 이하, 첨부된 도면들을 참조하여 본 발명의 일 실시예에 따른 블록체인 기반 전력 거래 시스템 및 방법을 설명한다. 이 과정에서 도면에 도시된 선들의 두께나 구성요소의 크기 등은 설명의 명료성과 편의상 과장되게 도시되어 있을 수 있다.

[41] 또한, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례에 따라 달라질 수 있다. 그러므로 이러한 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[42] 또한, 본 명세서에서 설명된 구현은, 예컨대, 방법 또는 프로세스, 장치, 소프트웨어 프로그램, 데이터 스트림 또는 신호로 구현될 수 있다. 단일 형태의 구현의 맥락에서만 논의(예컨대, 방법으로서만 논의)되었더라도, 논의된 특징의 구현은 또한 다른 형태(예컨대, 장치 또는 프로그램)로도 구현될 수 있다. 장치는 적절한 하드웨어, 소프트웨어 및 펌웨어 등으로 구현될 수 있다. 방법은, 예컨대, 컴퓨터, 마이크로프로세서, 집적 회로 또는 프로그래밍가능한 로직 디바이스 등을 포함하는 프로세싱 디바이스를 일반적으로 지칭하는 프로세서 등과 같은 장치에서 구현될 수 있다. 프로세서는 또한 최종-사용자 사이에 정보의 통신을 용이하게 하는 컴퓨터, 셀 폰, 휴대용/개인용 정보 단말기(personal digital assistant: "PDA") 및 다른 디바이스 등과 같은 통신 디바이스를 포함한다.

[43]

[44] 도 1은 본 발명의 일 실시예에 따른 블록체인 기반 전력 거래 시스템을 개략적으로 나타낸 도면이다.

[45] 도 1을 참조하면, 본 발명의 일 실시예에 따른 블록체인 기반 전력 거래 시스템은 사용자 장치(100), 전력 거래 서버(300) 및 블록체인(400)을 포함한다.

[46] 사용자 장치(100)는 전력을 구매하는 구매자 또는 전력을 판매하는 판매자일 수 있다. 사용자는 전력의 구매를 원하는지 또는 판매를 원하는지의 거래 방식, 거래하고자 하는 전력량과 거래 희망 금액을 입력할 수 있다. 이때 거래 금액의 범위는 한정되어 있을 수 있다.

[47] 사용자 장치(100)는 거래 방식, 거래량 및 거래 희망 금액을 포함하는 전력 거래 정보를 통신망을 통해 전력 거래 서버(300)로 전송한다.

[48] 도 1에서는 이해의 편의를 위해 하나의 사용자 장치(100)만을 도시하였으나, 다수의 사용자 장치(100)들이 구성될 수 있다.

[49] 전력 거래 서버(300)는 사용자 장치(100)로부터 전력 거래 정보를 수신하면, 그 전력 거래 정보를 인코딩하고, 인코딩된 정보를 암호화한다. 즉, 전력 거래 서버(300)는 전력 거래 정보의 거래 희망 금액을 인코딩하여 제1 벡터 및 제2 벡터를 생성한다. 그런 후, 전력 거래 서버(300)는 제1 벡터에 대한 비밀키를 생성하고, 제2 벡터에 대한 암호문을 생성하며, 생성된 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인(400)에 전송한다.

[50] 이러한 전력 거래 서버(300)에 대한 상세한 설명은 도 2를 참조하기로 한다.

[51] 한편, 도 1에서는 전력 거래를 관리하는 장치를 전력 거래 서버(300)로 칭하여 설명하였으나, 이는 플랫폼, 스마트폰, 스마트 미터, 서버 등이 될 수 있다. 또한, 단순한 플랫폼을 거치는 것 이외에, 다수의 플랫폼을 거쳐서 사용자와 블록체인(400)을 연결하는 것 또한 가능하다.

[52] 블록체인(400)은 전력 거래 서버(300)로부터 암호문 쌍을 수신하면, 암호문 쌍을 판매자 목록 또는 구매자 목록에 입력하고, 판매자 목록 중 최솟값을 제시한 판매자의 암호문 쌍을 식별하며, 구매자 목록 중 최댓값을 제시한 구매자의 암호문 쌍을 식별하고, 판매자 목록 중 최솟값을 제시한 판매자의 암호문 쌍 및 구매자 목록 중 최댓값을 제시한 구매자의 암호문 쌍을 이용하여 거래 성공 여부를 결정하며, 거래 성공 여부 정보를 전력 거래 서버(300)로 전송한다.

[53] 블록체인(400)은 전력 거래 서버(300)에서 암호화된 정보에 대해 최적 매칭을 수행하여 전력 매매가 이루어지도록 할 수 있다. 이때, 블록체인(400)은 함수암호(functional encryption)를 이용하여, 암호화된 거래 정보에 대한 비교를 통해 거래가 매칭되도록 할 수 있다.

[54] 함수암호란, 평문 a와 평문 b를 암호화하여 암호문 벡터 A와 암호문 벡터 B를 생성할 때, 특정 함수에 입력하게 되면 암호화에 이용한 키나 평문 a, b를 모르더라도 a, b에 대한 특정 연산값이 나올 수 있도록 하는 암호 기법이다. 즉, 함수암호란, a와 b의 암호문으로부터 함수 f(a,b)를 계산하되 a와 b 자체의 값은 알 수 없는 기법을 말하며, 본 발명에서는 일 실시예로 두 벡터 a와 b의 내적을 계산하는, 즉, f(a,b) = <a,b>인 내적 함수 암호를 이용하나, 내적 함수 이외의 함수암호 또한 이용할 수 있다. 또한, 본 발명의 일 실시예로 P2P 전력 거래를 고려하나, 본 발명은 데이터의 크기 비교에 기반하는 임의의 거래 방법에 적용될 수 있다.

[55] 내적 함수 암호는 키 파라미터 설정, 키 생성, 암호화 및 함수 복호화로 구성될 수 있다. 키 파라미터 설정은 주어진 안전성 요구조건을 만족하는 public parameter pp, master secret key msk를 생성하는 것을 의미할 수 있다. 키 생성은 x벡터에 대해 msk로 비밀키(secret key, sk_x)를 생성하는 것을 의미할 수 있다. 암호화는 y벡터에 대해 msk로 암호문(ciphertext, ct_y)를 생성하는 것을 의미할 수 있다. 함수 복호화는 Dec(sk_x, ct_y)라고 표기하며, 특정 함수에 비밀키(sk_x)와 암호문(ct_y)를 제공하면 두 벡터 x와 y의 내적값을 돌려주는 것을 의미할 수 있다.

[56] 블록체인(400)의 예로는 이더리움, 비트코인, 퀀텀 등이 있으며, 본 발명의 한 실시예에서는 이더리움을 예로 하여 설명하기로 한다.

[57] 본 발명의 일 실시예로, 이더리움 블록체인(400)에서 제공되는 Smart Contract를 이용하여 전력 거래에 대한 암호화를 구현할 수 있다. 판매자와 구매자들이 각각 희망하는 전력 거래량과 거래 희망 금액을 제안하면, 암호화된 정보를 블록체인(400) 상에서 최적 매칭을 수행하여 매매가 이루어지도록 할 수 있다.

[58]

[59] 도 2는 본 발명의 일 실시예에 따른 전력 거래 서버를 개략적으로 나타낸 블록도이다.

[60] 도 2를 참조하면, 본 발명의 일 실시예에 따른 전력 거래 서버(300)는 인터페이스부(310), 인코딩부(320), 암호화부(330) 및 제어부(340)를 포함한다.

[61] 인터페이스부(310)는 사용자 장치(100)로부터 거래 방식, 거래량 및 거래 희망 금액을 포함하는 전력 거래 정보를 통신망을 통해 수신한다.

[62] 인코딩부(320)는 전력 거래 정보를 인코딩하여 제1 벡터 및 제2 벡터를 생성한다. 이때, 인코딩부(320)는 전력 거래 정보의 거래 희망 금액을 인코딩할 수 있다. 또한, 인코딩부(320)는 인터페이스부(310)로부터 전달받은 전력 거래 정보들을 내적 결과값으로 크기를 비교할 수 있도록 인코딩할 수 있다.

[63] 즉, 인코딩부(320)는 인코딩이 가능한 단위 전력당 거래 금액 값의 범위(P)를 확인할 수 있다. 여기서, 단위 전력당 거래 금액 값의 범위는 미리 설정된 범위일 수 있다. 그런 후, 인코딩부(320)는 거래 희망 금액을 단위 전력당 거래 금액 범위와 비교하고, 그 비교결과에 기초하여 제1 벡터를 생성한다. 예컨대, 인코딩부(320)는 거래 희망 금액보다 작은 인덱스는 0, 이외의 인덱스는 1의 형태를 가지는 제1 벡터를 생성할 수 있다. 또한, 인코딩부(320)는 거래 희망 금액을 one-hot 인코딩하여 제2 벡터를 생성할 수 있다.

[64] 예를 들어, 단위 전력당 거래 금액 값의 범위(P)가 P={1, ..., 10}이고, 거래 희망 금액으로 '5'를 넣었다면, 인코딩부(320)는 5보다 작은 인덱스는 0, 그 외의 인덱스는 1의 형태를 가지는 제1 벡터(U_a, U_a = {0, 0, 0, 0, 1, 1, 1, 1, 1, 1}를 생성할 수 있다. 또한, 인코딩부(320)는 거래 희망 금액을 one-hot 인코딩하여 제2 벡터(U_b, U_b = {0, 0, 0, 0, 1, 0, 0, 0, 0, 0}를 생성할 수 있다.

[65] 암호화부(330)는 제1 벡터에 대한 비밀키를 생성하고, 제2 벡터에 대한 암호문을 생성하며, 생성된 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인(400)에 전송한다. 즉, 암호화부(330)는 키 생성 알고리즘을 이용하여 제1 벡터에 대한 비밀키를 생성하고, 암호화 알고리즘을 이용하여 제2 벡터에 대한 암호문을 생성한 후, 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인(400)으로 전송한다. 여기서, 키 생성 알고리즘 및 암호화 알고리즘은 종래의 알고리즘을 이용할 수 있다.

[66] 예를 들면, 암호화부(330)는 키 생성 알고리즘을 이용하여 제1 벡터(U_a)에 대한 비밀키(secret key, sk_U)를 생성하고, 암호화 알고리즘을 이용하여 제2 벡터(U_b)에 대한 암호문(ct_U)를 생성한 후 암호문 쌍(sk_U, ct_U) 을 블록체인(400)에 전달할 수 있다.

[67] 암호화부(330)는 거래 방식, 사용자 식별정보 등을 암호문 쌍과 함께 블록체인(400)으로 전송할 수 있다.

[68] 한편, 인코딩부(320) 및 암호화부(330)는 컴퓨팅 장치상에서 프로그램을 실행하기 위해 필요한 프로세서 등에 의해 각각 구현될 수 있다. 이처럼 인코딩부(320) 및 암호화부(330)는 물리적으로 독립된 각각의 구성에 의해

구현될 수도 있고, 하나의 프로세서 내에서 기능적으로 구분되는 형태로 구현될 수도 있다.

[69] 제어부(340)는 인터페이스부(310), 인코딩부(320) 및 암호화부(330)를 포함하는 전력 거래 서버(300)의 다양한 구성부들의 동작을 제어하는 구성으로, 적어도 하나의 연산 장치를 포함할 수 있는데, 여기서 상기 연산 장치는 범용적인 중앙연산장치(CPU), 특정 목적에 적합하게 구현된 프로그래머블 디바이스 소자(CPLD, FPGA), 주문형 반도체 연산장치(ASIC) 또는 마이크로 컨트롤러 칩일 수 있다.

[70]

[71] 도 3은 본 발명의 일 실시예에 따른 스마트 컨트랙트를 실행하는 블록체인을 설명하기 위한 블록도이다.

[72] 도 3을 참조하면, 본 발명의 일 실시예에 따른 스마트 컨트랙트를 실행하는 블록체인(400)은 기록 처리부(410), 비교부(420), 및 거래 처리부(430)를 포함한다.

[73] 기록 처리부(410)는 전력 거래 서버(300)로부터 암호문 쌍을 수신하면, 암호문 쌍의 요청자를 확인하여, 암호문 쌍을 판매자 목록 또는 구매자 목록에 기록한다.

[74] 즉, 기록 처리부(410)는 암호문 쌍과 함께 수신받은 거래 방식을 이용하여 요청자가 구매자 또는 판매자인지 확인할 수 있다. 기록 처리부(410)는 요청자가 판매자인 경우 암호문 쌍을 판매자 목록에 기록하고, 구매자인 경우 암호문 쌍을 구매자 목록에 기록할 수 있다.

[75] 비교부(420)는 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 판매자 암호문 쌍에 인코딩된 판매 희망 금액들 간의 대소를 비교함으로써 판매자 목록 중 최솟값에 대한 판매자 암호문 쌍을 찾고, 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 구매자 암호문 쌍에 인코딩된 구매 희망 금액들 간의 대소를 비교함으로써 구매자 목록 중 최댓값에 대한 구매자 암호문 쌍을 찾는다. 즉, 비교부(420)는 판매자 목록에서의 최솟값에 대한 암호문 쌍, 구매자 목록에서의 최댓값에 대한 암호문 쌍을 식별하기 위한 함수 복호화를 수행할 수 있다. 구체적으로, 비교부(420)는 판매자 A의 비밀키와 판매자 B의 암호문을 함수 복호화하여 내적 1 또는 0을 얻고 이를 이용하여 대소 관계를 판별하는 일을, 여러 판매자 쌍에 대해 반복함으로써, 판매자 목록에서 판매 희망 금액이 최소인 판매자의 암호문 쌍을 획득할 수 있다. 또한, 비교부(420)는 구매자 A의 비밀키와 구매자 B의 암호문을 함수 복호화하여 내적 1 또는 0을 얻고 이를 이용하여 대소 관계 판별하는 일을, 여러 구매자 쌍에 대해 반복함으로써, 구매자 목록에서 구매 희망 금액이 최대인 구매자의 암호문 쌍을 획득할 수 있다.

[76] 상술한 바와 같이 비교부(420)는 판매자 목록에서 판매 희망 금액이 최소인 판매자의 암호문 쌍을 획득할 수 있고, 구매자 목록에서 구매 희망 금액이

최대인 구매자의 암호문 쌍을 획득할 수 있다.

[77] 예를 들어, 판매자 목록 또는 구매자 목록에서 비교하고자 하는 두 사용자 U, N의 암호문 쌍을 각각 (sk_U, ct_U), (sk_N, ct_N)라 하면, 비교부(420)는 $Dec(sk_U, ct_N)$를 이용하여 암호문 쌍 (sk_U, ct_U), (sk_N, ct_N)에 대한 함수 복호화를 진행함으로써 U가 제시한 값과 N이 제시한 값을 모르는 상태로 이들에 대한 대소 비교를 할 수 있다. 만약 U의 거래 희망 금액이 5이면, $U_a = \{0, 0, 0, 0, 1, 1, 1, 1, 1, 1\}$이고, N의 거래 희망 금액이 6이면, $N_b = \{0, 0, 0, 0, 0, 1, 0, 0, 0\}$일 것이므로 $Dec(sk_U, ct_N)$의 결과, 즉 U_a와 N_b의 내적이 1이 되어 N의 거래 희망 금액이 더 큰 것을 확인할 수 있다. 또한, N의 거래 희망 금액이 4이면, $N_b = \{0, 0, 0, 1, 0, 0, 0, 0, 0\}$이므로 $Dec(sk_U, ct_N)$의 결과가 0이 되어 N의 거래 희망 금액이 더 적은 것을 확인할 수 있다. 이러한 방식을 이용하여 스마트 컨트랙트 실행자는 다수 사용자의 요청들을 비교함으로써 각각 판매자 목록 중 최솟값에 대한 암호문 쌍, 구매자 목록 중 최댓값에 대한 암호문 쌍을 확인할 수 있다. 이때, 최솟값과 최댓값이 무엇인지는 알 수 없을 수 있다.

[78] 거래 처리부(430)는 판매자 목록에서의 최솟값에 대한 암호문 쌍, 및 구매자 목록에서의 최댓값에 대한 암호문 쌍을 함수 복호화하여, 판매자 목록에서의 최솟값이 무엇인지, 구매자 목록에서의 최댓값이 무엇인지 모르는 상태로 이들에 대한 대소 비교만 함으로써 거래 성공 여부를 결정하고, 거래 성공 여부 정보를 전력 거래 서버(300)로 전송한다.

[79] 거래 처리부(430)가 수행하는 대소 비교 연산은 비교부(420)가 수행하는 대소 비교 연산과 유사한 방식으로 수행될 수 있다. 즉, 거래 처리부(430)는 판매자 목록에서의 최솟값에 대한 암호문 쌍 및 구매자 목록에서의 최댓값에 대한 암호문 쌍을 함수 복호화하여 내적을 산출하고, 산출된 내적에 기초하여 해당 판매자와 구매자 간의 거래 성공 여부를 결정할 수 있다. 이때, 거래 처리부(430)는 판매자 목록 중 최솟값에 대한 암호문 쌍의 비밀키와 구매자 목록 중 최댓값에 대한 구매자 암호문 쌍의 암호문에 대해 함수 복호화 연산을 적용함으로써 판매자 목록 중 최솟값에 대해 인코딩된 제1 벡터 및 구매자 목록 중 최댓값에 대해 인코딩된 제2 벡터 간의 내적 결과를 산출하고, 산출된 내적이 '1'인 경우 구매자 목록에서의 최댓값이 판매자 목록에서의 최솟값보다 크거나 같아 판매자와 구매자 간의 거래 성공으로 결정할 수 있고, 내적이 '0'인 경우 판매자와 구매자 간의 거래 실패로 결정할 수 있다.

[80] 거래 처리부(430)는 판매자와 구매자 간의 거래 성공으로 결정한 경우, 판매자의 주소 및 전력 거래 정보, 구매자의 주소 및 전력 거래 정보를 전력 거래 서버(300)로 전송할 수 있다.

[81] 상기의 모든 과정은 블록체인(400) 상의 smart contract에 의해 이루어지므로 조작이 불가능하며, 따라서 거래 결정 과정의 무결성이 보장될 수 있다. 그러나 모든 거래 금액은 암호화되어 있으므로, 거래 희망 금액이나 매칭된 금액 등의 정보를 보호할 수 있다.

[82]

[83] 도 4는 본 발명의 일 실시예에 따른 블록체인 기반 전력 거래 방법을 설명하기 위한 도면이다.

[84] 도 4를 참조하면, 사용자 장치(100)는 거래 방식, 거래량 및 거래 희망 금액을 포함하는 전력 거래 정보를 입력받으면(S410), 입력받은 전력 거래 정보를 전력 거래 서버(300)로 전송한다(S420).

[85] S420 단계가 수행되면, 전력 거래 서버(300)는 전력 거래 정보를 인코딩하여 제1 벡터 및 제2 벡터를 생성한다(S430). 즉, 전력 거래 서버(300)는 거래 희망 금액을 단위 전력당 거래 금액 범위와 비교하고, 그 비교결과에 기초하여 제1 벡터를 생성할 수 있다. 또한, 전력 거래 서버(300)는 거래 희망 금액을 one-hot 인코딩하여 제2 벡터를 생성할 수 있다.

[86] S430 단계가 수행되면, 전력 거래 서버(300)는 제1 벡터에 대한 비밀키를 생성하고, 제2 벡터에 대한 암호문을 생성하며(S440), 생성된 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인(400)에 전송하여 기록한다(S450). 즉, 전력 거래 서버(300)는 키 생성 알고리즘을 이용하여 제1 벡터에 대한 비밀키를 생성하고, 암호화 알고리즘을 이용하여 제2 벡터에 대한 암호문을 생성한 후, 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인(400)으로 전송할 수 있다. 그러면, 블록체인(400)은 암호문 쌍과 함께 수신받은 거래 방식을 이용하여 요청자가 구매자 또는 판매자인지 확인하고, 요청자가 판매자인 경우 암호문 쌍을 판매자 목록에 기록하고, 구매자인 경우 암호문 쌍을 구매자 목록에 기록할 수 있다.

[87] S450 단계가 수행되면, 블록체인(400)은 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 판매자 목록 중 최솟값에 대한 판매자 암호문 쌍을 찾고, 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 구매자 목록 중 최댓값에 대한 구매자 암호문 쌍을 찾는다(S460). 즉, 블록체인(400)은 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 판매자 암호문 쌍에 인코딩된 판매 희망 금액들 간의 대소를 비교함으로써 판매자 목록 중 최솟값에 대한 판매자 암호문 쌍을 찾고, 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 구매자 암호문 쌍에 인코딩된 구매 희망 금액들 간의 대소를 비교함으로써 구매자 목록 중 최댓값에 대한 구매자 암호문 쌍을 찾을 수 있다.

[88] S460 단계가 수행되면, 블록체인(400)은 최솟값에 대한 판매자 암호문 쌍 및 최댓값에 대한 구매자 암호문 쌍을 함수 복호화하여 내적을 산출하고(S470), 산출된 내적에 기초하여 거래 성공 여부를 결정하며(S480), 거래 성공 여부 정보를 전력 거래 서버(300)로 전송한다(S490). 즉, 블록체인(400)은 판매자 목록 중 최솟값에 대해 인코딩된 제1 벡터 및 구매자 목록 중 최댓값에 대해 인코딩된 제2 벡터 간의 내적 결과를 산출하고, 산출된 내적이 '1'인 경우 구매자 목록에서의 최댓값이 판매자 목록에서의 최솟값보다 크거나 같아 판매자와

구매자 간의 거래 성공으로 결정할 수 있고, 내적이 '0'인 경우 판매자와 구매자 간의 거래 실패로 결정할 수 있다.

[89] 상술한 바와 같이 본 발명의 일 실시예에 따른 블록체인 기반 전력 거래 시스템 및 방법은, 블록체인 기반의 함수암호 기법을 이용하여 거래 데이터를 암호화하여 보호함과 동시에, 거래 당사자 이외의 제3자는 거래 내용을 모르면서도 결과의 무결성 증명에 기여할 수 있다. 즉, 암호화된 상태에서 크기 비교가 가능하기 때문에 거래 내용을 제3자가 확인하지 못하더라도 크기 비교의 결과는 알 수 있고, 이로 인해 블록체인의 기밀성 문제를 해결할 수 있다.

[90] 본 발명은 도면에 도시된 실시예를 참고로 하여 설명되었으나, 이는 예시적인 것에 불과하며, 당해 기술이 속하는 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서 본 발명의 진정한 기술적 보호범위는 아래의 특허청구범위에 의해서 정하여져야 할 것이다.

[91]

[92] [부호의 설명

[93] 100 : 사용자 장치

[94] 300 : 전력 거래 서버

[95] 310 : 인터페이스부

[96] 320 : 인코딩부

[97] 330 : 암호화부

[98] 340 : 제어부

[99] 400 : 블록체인

[100] 410 : 기록 처리부

[101] 420 : 비교부

[102] 430 : 거래 처리부

청구범위

[청구항 1] 전력 거래 정보를 입력받는 사용자 장치;
상기 사용자 장치로부터 전력 거래 정보를 수신하고, 상기 전력 거래 정보를 인코딩하며, 상기 인코딩된 정보를 암호화하는 전력 거래 서버; 및
상기 전력 거래 서버로부터 암호문 쌍을 수신하면, 상기 암호문 쌍을 판매자 목록 또는 구매자 목록에 입력하고, 상기 판매자 목록 및 구매자 목록에 있는 판매자 암호문 쌍들 및 구매자 암호문 쌍들을 이용하여 거래 성공 여부를 결정하며, 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 블록체인
을 포함하는 블록체인 기반 전력 거래 시스템.

[청구항 2] 제1항에 있어서,
상기 전력 거래 서버는,
상기 전력 거래 정보의 거래 희망 금액을 인코딩하여 제1 벡터 및 제2 벡터를 생성하는 인코딩부; 및
상기 제1 벡터에 대한 비밀키를 생성하고, 상기 제2 벡터에 대한 암호문을 생성하며, 상기 생성된 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인에 전송하는 암호화부를 포함하는 것을 특징으로 하는 블록체인 기반 전력 거래 시스템.

[청구항 3] 제2항에 있어서,
상기 인코딩부는,
상기 거래 희망 금액을 기 설정된 단위 전력당 거래 금액 범위와 비교하고, 그 비교결과를 기초로 상기 거래 희망 금액을 인코딩하여 제1 벡터 및 제2 벡터를 생성하는 것을 특징으로 하는 블록체인 기반 전력 거래 시스템.

[청구항 4] 제3항에 있어서,
상기 암호화부는,
키 생성 알고리즘을 이용하여 상기 제1 벡터에 대한 비밀키를 생성하고, 암호화 알고리즘을 이용하여 상기 제2 벡터에 대한 암호문을 생성한 후, 상기 비밀키 및 암호문을 포함하는 암호문 쌍을 상기 블록체인으로 전송하는 것을 특징으로 하는 블록체인 기반 전력 거래 시스템.

[청구항 5] 제1항에 있어서,
상기 블록체인은,
상기 전력 거래 서버로부터 암호문 쌍을 수신하면, 상기 암호문 쌍의 요청자를 확인하여, 판매자 목록 또는 구매자 목록에 기록하는 기록 처리부;
상기 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 최솟값에 대한 판매자 암호문 쌍을 찾고, 상기 구매자 목록의

구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 최댓값에 대한 구매자 암호문 쌍을 찾는 비교부; 및
상기 최솟값에 대한 판매자 암호문 쌍 및 상기 최댓값에 대한 구매자 암호문 쌍을 함수 복호화 연산하여, 거래 성공 여부를 결정하고, 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 거래 처리부를 포함하는 것을 특징으로 하는 블록체인 기반 전력 거래 시스템.

[청구항 6] 제5항에 있어서,
상기 비교부는,
상기 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 판매자 암호문 쌍에 인코딩된 판매 희망 금액들 간의 대소를 비교함으로써 상기 판매자 목록 중 최솟값에 대한 판매자 암호문 쌍을 찾고, 상기 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 구매자 암호문 쌍에 인코딩된 구매 희망 금액들 간의 대소를 비교함으로써 상기 구매자 목록 중 최댓값에 대한 구매자 암호문 쌍을 찾는 것을 특징으로 하는 블록체인 기반 전력 거래 시스템.

[청구항 7] 제5항에 있어서,
상기 거래 처리부는,
상기 최솟값에 대한 판매자 암호문 쌍 및 상기 최댓값에 대한 구매자 암호문 쌍을 함수 복호화하여 내적을 산출하고, 상기 산출된 내적에 기초하여 해당 판매자와 구매자 간의 거래 성공 여부를 결정하는 것을 특징으로 하는 블록체인 기반 전력 거래 시스템.

[청구항 8] 제7항에 있어서,
상기 거래 처리부는,
상기 최솟값에 대한 판매자 암호문 쌍의 비밀키와 상기 최댓값에 대한 구매자 암호문 쌍의 암호문에 대해 함수 복호화 연산을 적용함으로써 상기 판매자 목록 중 최솟값에 대해 인코딩된 제1 벡터 및 상기 구매자 목록 중 최댓값에 대해 인코딩된 제2 벡터의 내적 결과를 산출하고, 상기 산출된 내적이 '1'인 경우 상기 판매자와 구매자 간의 거래 성공으로 결정하며, 상기 내적이 '0'인 상기 판매자와 구매자 간의 거래 실패로 결정하는 것을 특징으로 하는 블록체인 기반 전력 거래 시스템.

[청구항 9] 제8항에 있어서,
상기 거래 처리부는,
상기 판매자와 구매자 간의 거래 성공으로 결정한 경우, 상기 판매자의 주소 및 전력 거래 정보, 상기 구매자의 주소 및 전력 거래 정보를 상기 전력 거래 서버로 전송하는 것을 특징으로 하는 블록체인 기반 전력 거래 시스템.

[청구항 10] 전력 거래 서버가 사용자 장치로부터 전력 거래 정보를 수신하면, 상기 전력 거래 정보를 인코딩하고, 상기 인코딩된 정보를 암호화하는 단계; 및

블록체인이 상기 전력 거래 서버로부터 암호문 쌍을 수신하면, 상기 암호문 쌍을 판매자 목록 또는 구매자 목록에 입력하고, 상기 판매자 목록 및 구매자 목록에 있는 판매자 암호문 쌍들 및 구매자 암호문 쌍들을 이용하여 거래 성공 여부를 결정하며, 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 단계

를 포함하는 블록체인 기반 전력 거래 방법.

[청구항 11] 제10항에 있어서,

상기 전력 거래 정보를 인코딩하고, 상기 인코딩된 정보를 암호화하는 단계는,

상기 전력 거래 서버가 상기 전력 거래 정보의 거래 희망 금액을 인코딩하여 제1 벡터 및 제2 벡터를 생성하는 단계; 및

상기 전력 거래 서버가 상기 제1 벡터에 대한 비밀키를 생성하고, 상기 제2 벡터에 대한 암호문을 생성하며, 상기 생성된 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인에 전송하는 단계를 포함하는 것을 특징으로 하는 블록체인 기반 전력 거래 방법.

[청구항 12] 제11항에 있어서,

상기 제1 벡터 및 제2 벡터를 생성하는 단계에서,

상기 전력 거래 서버는, 상기 거래 희망 금액을 기 설정된 단위 전력당 거래 금액 범위와 비교하고, 그 비교결과를 기초로 상기 거래 희망 금액을 인코딩하여 제1 벡터 및 제2 벡터를 생성하는 것을 특징으로 하는 블록체인 기반 전력 거래 방법.

[청구항 13] 제11항에 있어서,

상기 생성된 비밀키 및 암호문을 포함하는 암호문 쌍을 블록체인에 전송하는 단계에서,

상기 전력 거래 서버는 키 생성 알고리즘을 이용하여 상기 제1 벡터에 대한 비밀키를 생성하고, 암호화 알고리즘을 이용하여 상기 제2 벡터에 대한 암호문을 생성한 후, 상기 비밀키 및 암호문을 포함하는 암호문 쌍을 상기 블록체인으로 전송하는 것을 특징으로 하는 블록체인 기반 전력 거래 방법.

[청구항 14] 제10항에 있어서,

상기 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 단계는,

상기 블록체인이 상기 전력 거래 서버로부터 암호문 쌍을 수신하면, 상기 암호문 쌍의 요청자를 확인하여, 판매자 목록 또는 구매자 목록에 기록하는 단계;

상기 블록체인이 상기 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 최솟값에 대한 판매자 암호문 쌍을 찾고, 상기 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 최댓값에 대한 구매자 암호문 쌍을 찾는 단계; 및

상기 블록체인이 상기 최솟값에 대한 판매자 암호문 쌍 및 상기 최댓값에 대한 구매자 암호문 쌍을 함수 복호화 연산하여, 거래 성공 여부를 결정하고, 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 단계를 포함하는 것을 특징으로 하는 블록체인 기반 전력 거래 시스템.

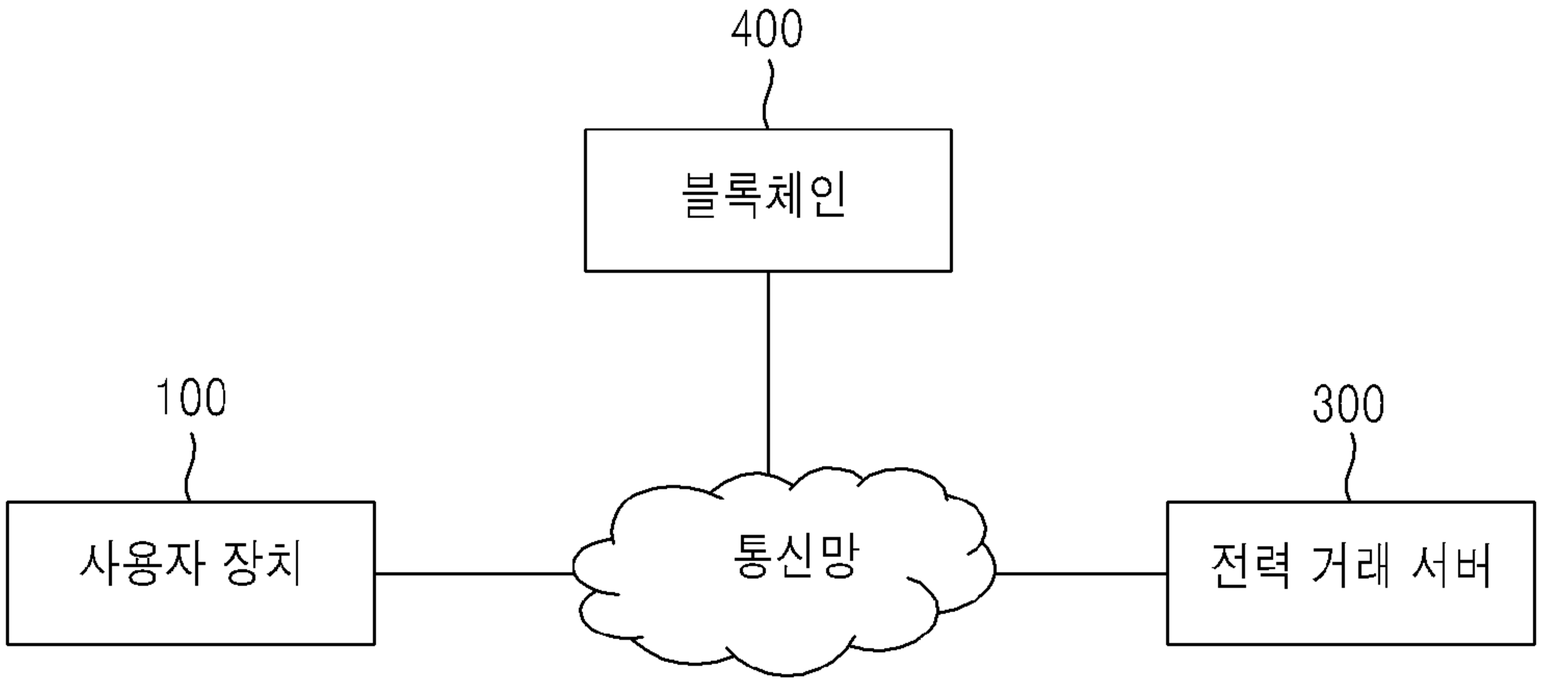
[청구항 15] 제14항에 있어서,
상기 최댓값에 대한 구매자 암호문 쌍을 찾는 단계에서,
상기 블록체인은, 상기 판매자 목록의 판매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 판매자 암호문 쌍에 인코딩된 판매 희망 금액들 간의 대소를 비교함으로써 상기 판매자 목록 중 최솟값에 대한 판매자 암호문 쌍을 찾고, 상기 구매자 목록의 구매자 암호문 쌍들에 대한 함수 복호화 연산을 적용하여 구매자 암호문 쌍에 인코딩된 구매 희망 금액들 간의 대소를 비교함으로써 상기 구매자 목록 중 최댓값에 대한 구매자 암호문 쌍을 찾는 것을 특징으로 하는 블록체인 기반 전력 거래 방법.

[청구항 16] 제14항에 있어서,
상기 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 단계에서,
상기 블록체인은 상기 최솟값에 대한 판매자 암호문 쌍 및 상기 최댓값에 대한 구매자 암호문 쌍을 함수 복호화하여 내적을 산출하고, 상기 산출된 내적에 기초하여 해당 판매자와 구매자 간의 거래 성공 여부를 결정하는 것을 특징으로 하는 블록체인 기반 전력 거래 방법.

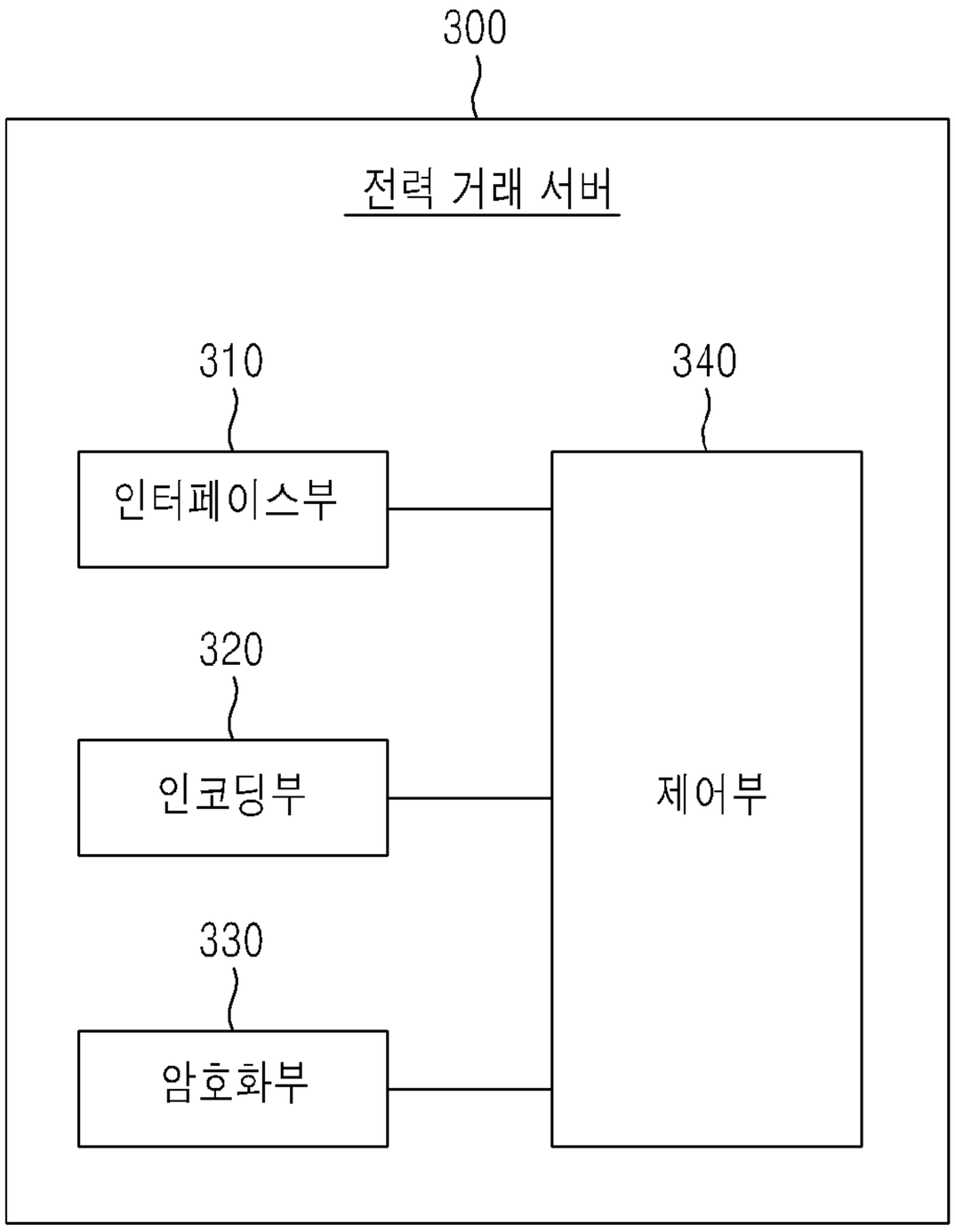
[청구항 17] 제16항에 있어서,
상기 거래 성공 여부 정보를 상기 전력 거래 서버로 전송하는 단계에서,
상기 블록체인은 상기 최솟값에 대한 판매자 암호문 쌍의 비밀키와 상기 최댓값에 대한 구매자 암호문 쌍의 암호문에 대해 함수 복호화 연산을 적용함으로써 상기 판매자 목록 중 최솟값에 대해 인코딩된 제1 벡터 및 상기 구매자 목록 중 최댓값에 대해 인코딩된 제2 벡터의 내적 결과를 산출하고, 상기 산출된 내적이 '1'인 경우 상기 판매자와 구매자 간의 거래 성공으로 결정하며, 상기 내적이 '0'인 상기 판매자와 구매자 간의 거래 실패로 결정하는 것을 특징으로 하는 블록체인 기반 전력 거래 방법.

[청구항 18] 제17항에 있어서,
상기 판매자와 구매자 간의 거래 성공으로 결정한 경우, 상기 판매자의 주소 및 전력 거래 정보, 상기 구매자의 주소 및 전력 거래 정보를 상기 전력 거래 서버로 전송하는 것을 특징으로 하는 블록체인 기반 전력 거래 방법.

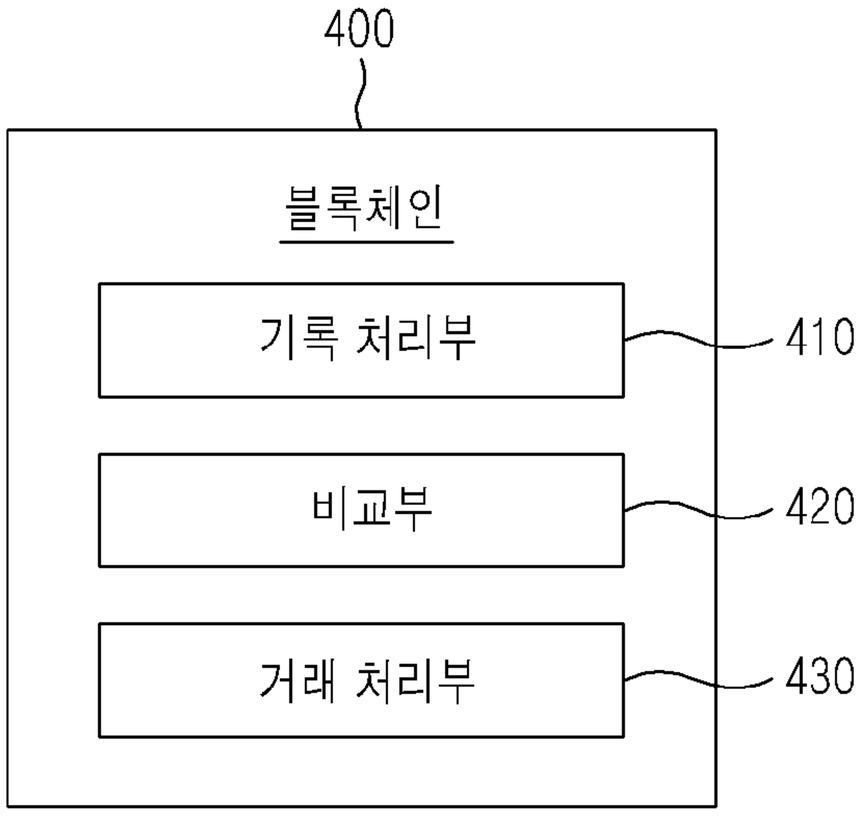
[도1]


400
블록체인
100
사용자 장치
통신망
300
전력 거래 서버

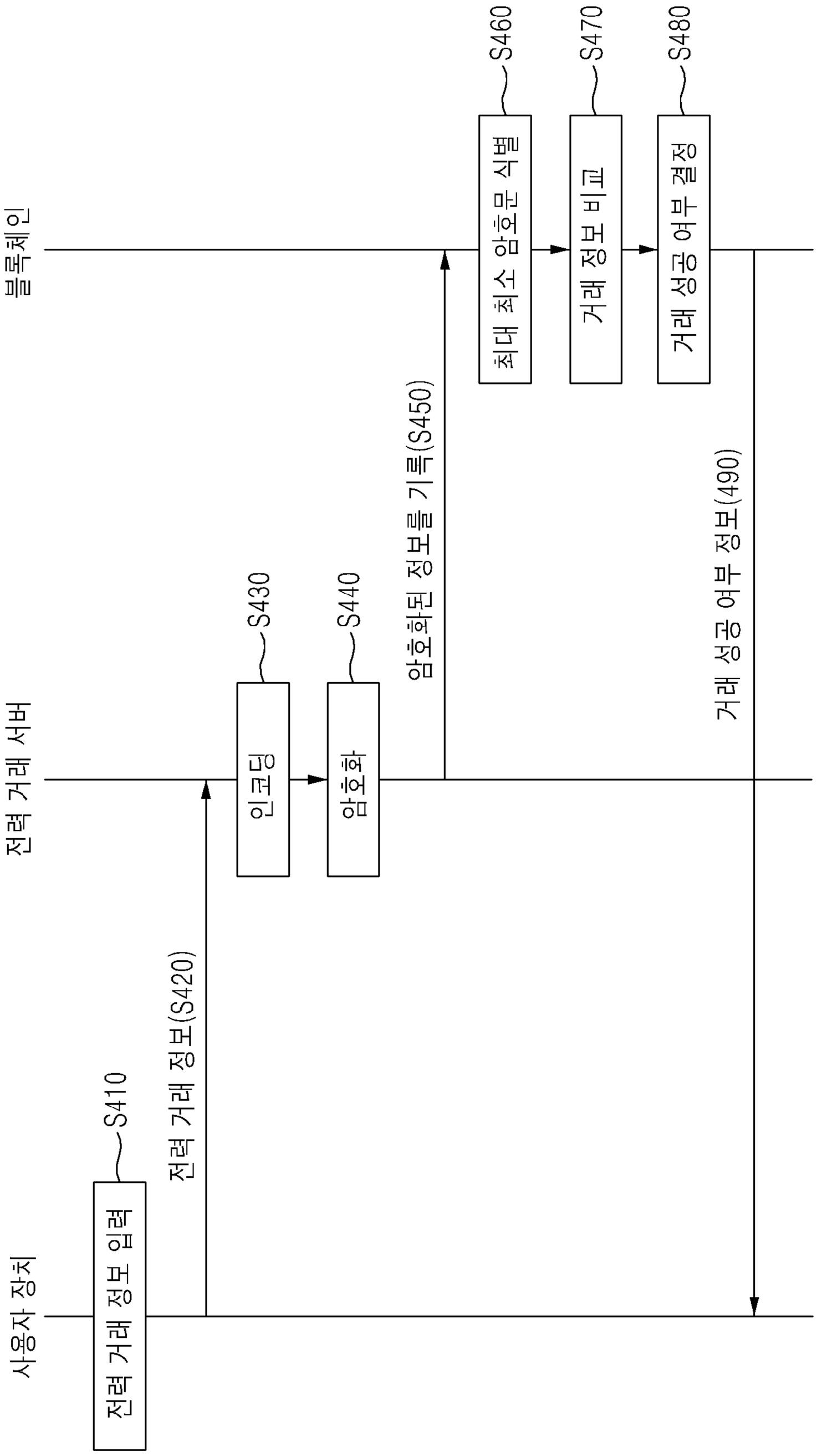
[도2]


300
전력 거래 서버
310
인터페이스부
340
320
인코딩부
제어부
330
암호화부

[도3]



[도4]


블록체인
전력 거래 서버
사용자 장치
전력 거래 정보 입력
S410
전력 거래 정보(S420)
인코딩
S430
암호화
S440
암호화된 정보를 기록(S450)
최대 최소 암호문 식별
S460
거래 정보 비교
S470
거래 성공 여부 결정
S480
거래 성공 여부 정보(490)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2020/007773

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 50/06(2012.01)i; **H04L 9/06**(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q 50/06; G06Q 20/36; H04L 9/00; H04L 9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: 전력 거래(energy transaction), 블록체인(blockchain), 보안(security), 함수암호(functional encryption), 매칭(matching), 벡터(vector), 내적(inner product)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-1976401 B1 (KOREA ELECTRIC POWER CORPORATION) 09 May 2019. See claims 1-4, 7-13 and 16-20.	1,10
A		2-9,11-18
Y	WO 2017-090041 A1 (BEN-ARI, Adi) 01 June 2017. See page 17; and claims 1-9.	1,10
A	ANDONI, Merlinda et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. ELSEVIER. Renewable and Sustainable Energy Reviews. vol. 100, 28 February 2019, pp. 143-174. See pages 144-167.	1-18
A	WANG, Naiyu et al. When Energy Trading Meets Blockchain in Electrical Power System: The State of the Art. MDPI. applied sciences. Article. 15 April 2019, pp. 1-31. See pages 1-24.	1-18
PX	SON, Ye-Byoul et al. Privacy-Preserving Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids Using Functional Encryption. MDPI. energies. Article. 12 March 2020, pp. 1-22. See pages 1-19.	1-18

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 September 2020	**25 September 2020**
Name and mailing address of the ISA/KR **Korean Intellectual Property Office** **Government Complex-Daejeon Building 4, 189 Cheongsa-ro, Seo-gu, Daejeon 35208** Facsimile No. **+82-42-481-8578**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2020/007773

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
KR 10-1976401 B1	09 May 2019	KR 10-2019-0019422 A	27 February 2019
		WO 2019-035527 A1	21 February 2019
WO 2017-090041 A1	01 June 2017	EP 3380984 A1	03 October 2018
		EP 3380984 A4	31 July 2019
		US 2018-0343114 A1	29 November 2018

국 제 조 사 보 고 서

국제출원번호
PCT/KR2020/007773

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06Q 50/06(2012.01)i, H04L 9/06(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
G06Q 50/06; G06Q 20/36; H04L 9/00; H04L 9/06

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 전력 거래(energy transaction), 블록체인(blockchain), 보안(security), 함수암호(functional encryption), 매칭(matching), 벡터(vector), 내적(inner product)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y A	KR 10-1976401 B1 (한국전력공사) 2019.05.09 청구항 1-4, 7-13, 16-20.	1,10 2-9,11-18
Y	WO 2017-090041 A1 (BEN-ARI, ADI) 2017.06.01 페이지 17; 및 청구항 1-9.	1,10
A	MERLINDA ANDONI 등. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. ELSEVIER, Renewable and Sustainable Energy Reviews, 100부, 2019.02.28, 페이지 143-174. 페이지 144-167.	1-18
A	NAIYU WANG 등. When Energy Trading Meets Blockchain in Electrical Power System: The State of the Art. MDPI, applied sciences, Article, 2019.04.15, 페이지 1-31. 페이지 1-24.	1-18
PX	YE-BYOUL SON 등. Privacy-Preserving Peer-to-Peer Energy Trading in Blockchain-Enabled Smart Grids Using Functional Encryption. MDPI, energies, Article, 2020.03.12, 페이지 1-22. 페이지 1-19.	1-18

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"D" 본 국제출원에서 출원인이 인용한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2020년 09월 25일 (25.09.2020)	2020년 09월 25일 (25.09.2020)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-481-8578

심사관
강민정
전화번호 +82-42-481-8131

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2020/007773

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1976401 B1	2019/05/09	KR 10-2019-0019422 A	2019/02/27
		WO 2019-035527 A1	2019/02/21
WO 2017-090041 A1	2017/06/01	EP 3380984 A1	2018/10/03
		EP 3380984 A4	2019/07/31
		US 2018-0343114 A1	2018/11/29