

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구  
국제사무국

(43) 국제공개일  
2023년 6월 15일 (15.06.2023) WIPO PCT



(10) 국제공개번호  
WO 2023/106629 A1

- (51) 국제특허분류:  
G06Q 50/26 (2012.01) H04L 9/00 (2006.01)  
H04L 9/06 (2006.01)
- (21) 국제출원번호: PCT/KR2022/016801
- (22) 국제출원일: 2022년 10월 31일 (31.10.2022)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:  
10-2021-0175172 2021년 12월 8일 (08.12.2021) KR
- (71) 출원인: 고려대학교 산학협력단 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) [KR/KR]: 02841 서울특별시 성북구 안암로 145, Seoul (KR). 최지혁 (CHOI, Jihyok) [KR/KR]: 05348 서울특별시 강동구 천호대로 1239, 110동 803호, Seoul (KR).
- (72) 발명자: 인호 피터 (IN, Hoh Peter); 04385 서울특별시 용산구 서빙고로 35, 102동 1705호, Seoul (KR).
- (74) 대리인: 윤귀상 (YUN, Kuisang); 08511 서울특별시 금천구 디지털로 9길 47 804호(가산동, 한신IT 타워2차), Seoul (KR).

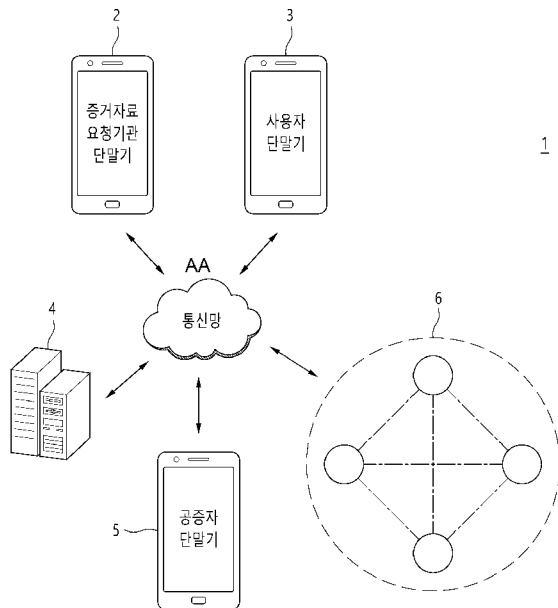
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, 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, CV, 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, ME, 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))

(54) Title: CONTROL METHOD FOR BLOCKCHAIN-BASED EVIDENCE DATA NOTARIZATION SYSTEM, AND RECORDING MEDIUM AND SYSTEM FOR PERFORMING SAME

(54) 발명의 명칭: 블록체인 기반 증거자료 공증 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 시스템



- 2 ... Evidence data request agency terminal  
3 ... User terminal  
5 ... Notary terminal  
AA ... Communication network

(57) Abstract: Provided is a blockchain-based evidence data notarization system comprising: a user terminal that, if receiving a notarization request, transmits evidence data; a notarization server that receives the evidence data, generates a hash value for the evidence data, and transmits the generated hash value to each of the user terminal and a notary terminal; and a blockchain server that receives signatures written on the hash value from the user terminal and the notary terminal, respectively, and generates a smart contract block.

(57) 요약서: 공증요청을 수신하면 증거자료를 전송하는 사용자 단말기; 증거자료를 수신하고 증거자료에 대한 해시값을 생성하고, 생성된 해시값을 각각 사용자 단말기와 공증자 단말기 측에 전송하는 공증서버; 및 사용자 단말기와 공증자 단말기 측으로부터 각각 해시값에 작성한 서명을 수신하고, 스마트컨트랙트 블록을 생성하는 블록체인 서버; 를 포함하는 블록체인 기반 증거자료 공증 시스템을 제공한다.

## 명세서

### 발명의 명칭: 블록체인 기반 증거자료 공증 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 시스템

#### 기술분야

- [1] 본 발명은 블록체인 기반 증거자료 공증 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 시스템에 관한 것으로, 보다 상세하게는, 증거자료를 공증하는 블록체인 기반 증거자료 공증 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 시스템에 관한 것이다.

#### 배경기술

- [2] 최근 공판중심주의 재판으로의 변화로 인해 수사 기관에서 수집하는 디지털 증거의 증거 능력은 사건 판결의 중요한 부분을 차지하고 있으며, 디지털 증거자료가 수사 과정의 핵심적인 역할을 수행함에 따라 신뢰성 확보의 문제가 대두되고 있다. 또한, 디지털 증거는 비가시적이기 때문에 증거의 동일성과 무결성이 중요하다는 특징이 있다.
- [3] 2009년 블록체인(blockchain)에 기반을 둔 비트코인(bitcoin)이 공개된 이후, 블록체인은 비트코인과 같은 전자 화폐 시스템뿐만 아니라 스마트 계약을 위한 플랫폼 제공 서비스, 클라우드 저장 서비스, 블록체인 컴퓨팅 서비스 등 다양한 분야에서 적용되고 있다.
- [4] 이러한 블록체인을 구성하는 가장 중요한 요소인 분산원장(Distributed Ledger)는 블록체인을 탈중앙화된 시스템으로 만들어 주는 핵심 기술로서, 거래 기록 등의 데이터를 저장하는 데이터베이스를 중앙화된 서버가 소유하는 것이 아닌 블록체인 네트워크에 참여하는 모든 노드가 동일한 원장을 소유하고 관리하는 형태를 가리킨다.
- [5] 블록체인 기술은 사물인터넷 기술과 결합하여 전 과정에 대한 모니터링을 통해 투명성을 확보하고 중간에 문제가 발생할 경우 책임소재를 명확히 가려낼 수 있다는 장점이 있다.
- [6] 따라서, 공증기관과의 연계를 통해 공증한 증거자료를 블록체인 상에 저장해 증거의 신뢰성과 무결성을 확보하는 블록체인 기반 증거자료 공증 시스템이 요구되는 실정이다.
- [7] [선행기술문헌]
- [8] [특허문헌] KR 10-2016-0123752A
- [9]

#### 발명의 상세한 설명

##### 기술적 과제

- [10] 본 발명이 해결하고자 하는 기술적 과제는 공증기관 서버에서 증거자료를 공증하여 증거자료의 신뢰성을 확보하고, 블록체인 서버에 저장함으로써

증거자료의 위조가 불가능하도록 하는 블록체인 기반 증거자료 공증 시스템의 제어방법, 이를 수행하기 위한 기록매체 및 장치를 제공하는 것이다.

- [11] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

### 과제 해결 수단

- [12] 본 발명의 일측면은, 사용자로부터의 증거자료에 대한 공증요청에 응답하여 상기 증거자료를 블록체인 기반으로 공증하기 위한 블록체인 기반 증거자료 공증 시스템에 있어서, 상기 공증요청에 따라 상기 증거자료를 전송하는 사용자 단말기; 상기 증거자료를 수신하고 이를 암호화하여 상기 증거자료에 대한 해시값을 생성하고, 상기 생성된 해시값을 각각 상기 사용자 단말기와 상기 증거자료에 대한 공증을 수행하는 공증자 단말기 측에 전송하는 공증서버; 및 상기 사용자 단말기와 공증자 단말기 측으로부터 각각 상기 해시값에 작성한 서명을 수신하고, 상기 서명이 작성된 해시값을 기초로 스마트컨트랙트 블록을 생성하는 블록체인 서버;를 포함할 수 있다.
- [13] 또한, 상기 공증 서버는, 상기 사용자 단말기로부터 상기 증거자료를 수신하는 통신부; 상기 사용자의 정보를 관리하는 회원 관리부; 상기 증거자료를 암호화하여 해시값을 생성하는 암호화부; 및 상기 증거자료와 해시값이 매칭되어 클라우드 저장소에 저장되도록 상기 클라우드 저장소와 연동되는 클라우드 연동부;를 포함할 수 있다.
- [14] 또한, 상기 블록체인 서버는, 상기 사용자 단말기로부터 상기 사용자의 트랜잭션 서명을 수신하고, 상기 공증자 단말기로부터 상기 공증자의 트랜잭션 서명을 수신하는 통신부; 상기 수신한 사용자의 트랜잭션 서명과 상기 공증자의 트랜잭션 서명을 검증하고, 검증된 상기 트랜잭션 서명을 저장하는 서명관리부;
- [15] 상기 트랜잭션이 실행되어 스마트 컨트랙트 블록을 생성하는 스마트 컨트랙트 블록 관리부; 상기 스마트 컨트랙트 블록을 기초로 토큰을 생성하는 토큰 생성부; 및 상기 토큰 생성부가 생성한 토큰이 저장되도록 통합 API를 통해 전자지갑과 연동되는 지갑 연동부;를 포함할 수 있다.
- [16] 또한, 상기 공증 서버는, 상기 사용자 단말기로부터 증거자료 검색을 요청받으면, 상기 블록체인 서버에 상기 사용자 서명이 포함된 상기 스마트 컨트랙트 블록의 존재여부 확인을 요청할 수 있다.
- [17] 또한, 상기 공증서버는, 상기 블록체인 서버로부터 상기 사용자 서명이 포함된 상기 스마트 컨트랙트 블록이 존재한다는 신호를 수신하면, 상기 클라우드 연동부로부터 상기 클라우드에 저장된 사용자의 공증된 증거자료의 해시값을 상기 사용자 단말기에 전송할 수 있다.
- [18] 또한, 상기 사용자 단말기는, 증거자료 요청기관 단말기에 상기 공증된 증거자료의 해시값을 전송할 수 있다.
- [19] 본 발명의 다른 일측면은, 사용자로부터의 증거자료에 대한 공증요청에

응답하여 상기 증거자료를 블록체인 기반으로 공증하기 위한 블록체인 기반 증거자료 공증 시스템의 제어방법에 있어서, 사용자 단말기가 상기 공증요청에 따라 상기 증거자료를 전송하고, 공증서버가 상기 증거자료를 수신하고 이를 암호화하여 상기 증거자료에 대한 해시값을 생성하고, 상기 생성된 해시값을 각각 상기 사용자 단말기와 상기 증거자료에 대한 공증을 수행하는 공증자 단말기 측에 전송하며, 블록체인 서버가 상기 사용자 단말기와 공증자 단말기 측으로부터 각각 상기 해시값에 작성한 서명을 수신하고, 상기 서명이 작성된 해시값을 기초로 스마트컨트랙트 블록을 생성하는 것을 포함할 수 있다.

[20] 또한, 상기 공증서버는 상기 사용자 단말기로부터 상기 증거자료를 수신하고, 상기 사용자의 정보를 관리하며, 상기 증거자료를 암호화하여 해시값을 생성하고, 상기 증거자료와 해시값이 매칭되어 클라우드 저장소에 저장되도록 상기 클라우드 저장소와 연동되는 것을 포함할 수 있다.

[21] 또한, 상기 블록체인 서버는 상기 사용자 단말기로부터 사용자의 트랜잭션 서명을 수신하고, 상기 공증자 단말기로부터 상기 공증자의 트랜잭션 서명을 수신하며, 상기 수신한 사용자의 트랜잭션 서명과 상기 공증자의 트랜잭션 서명을 검증하고, 검증된 상기 트랜잭션 서명을 저장하며, 상기 트랜잭션이 실행되어 스마트 컨트랙트 블록을 생성하고, 상기 스마트 컨트랙트 블록을 기초로 토큰을 생성하되, 생성된 토큰이 통합 API를 통해 연동되는 전자지갑에 저장되는 것을 포함할 수 있다.

[22] 본 발명의 또 다른 일측면은, 컴퓨터로 관독 가능한 저장 매체에는 블록체인 기반 증거자료 공증 시스템의 제어방법을 수행하기 위한 컴퓨터 프로그램이 기록될 수 있다.

### **발명의 효과**

[23] 상술한 본 발명의 일측면에 따르면, 블록체인 서버의 노드에 참여하는 공증기관 서버를 제공함으로써, 증거자료를 공증하고, 블록체인 서버에 저장함으로써 증거자료의 위조 방지 및 무결성을 증명할 수 있는 효과가 있다.

### **도면의 간단한 설명**

[24] 도1은 본 발명의 일 실시예에 따른 블록체인 기반 증거자료 공증 시스템을 나타내는 개념도이다.

[25] 도2는 공증 서버를 나타내는 개념도이다.

[26] 도3은 블록체인 서버를 나타내는 개념도이다.

[27] 도4는 스마트 컨트랙트 블록을 나타내는 도면이다.

[28] 도5 내지 도6은 본 발명의 일 실시예에 따른 블록체인 기반 증거자료 공증 시스템의 제어방법을 나타내는 전체적인 흐름도이다.

### **발명의 실시를 위한 최선의 형태**

[29] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본

발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[30] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[31]

[32] 도1은 본 발명의 일 실시예에 따른 블록체인 기반 증거자료 공증 시스템을 나타내는 개념도이다.

[33] 블록체인 기반 증거자료 공증 시스템(1)은 증거자료 요청기관 단말기(2), 사용자 단말기(3), 공증 서버(4), 공증자 단말기(5) 및 블록체인 서버(6)를 포함할 수 있다.

[34] 블록체인 기반 증거자료 공증 시스템(1)은 사용자로부터 수신한 증거자료를 공증하는 시스템일 수 있다.

[35] 사용자는 증거자료 요청기관 단말기(2)로부터 증거자료의 제출을 요청받을 수 있다. 증거자료 요청기관 단말기(2)는 증거자료를 수집하는 수사기관, 법원일 수 있다. 다만, 이에 한정되는 것은 아니다.

[36] 사용자는 사용자 단말기(3)를 통해 해당 증거자료를 공증 서버(4)에 전송할 수 있다. 이 때, 증거자료는 범죄의 유무를 판단하는 사진, 영상, 텍스트 파일로 구성된 증거자료일 수 있다.

[37] 공증자 단말기(5), 사용자 단말기(3) 및 증거자료 요청기관 단말기(2)는 PCS(Personal Communication System), GSM(Global System for Mobile communications), PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)- 2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet) 단말, 스마트폰 (smartphone), 스마트 패드(smartpad), 태블릿 PC(Tablet PC) 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치 및 거치형 PC, 노트북과 같은 컴퓨팅 장치가 이용될 수 있다.

[38] 이 때, 공증 서버(4)는 블록체인 기반 증거자료 공증 시스템(1)을 구현하기 위해 마련된 플랫폼일 수 있다. 공증 서버(4)를 통해, 사용자가 증거자료의 공증을 요청할 수 있다. 공증 서버(4)는 사용자 단말기(3)를 통해 수신한 파일을

- 공증하도록 공증자 단말기(5)에 전송할 수 있다.
- [39] 사용자는 공증 서버(4)에서 공증이 완료된 증거자료를 검색할 수 있고, 증거자료를 발급받아 증거자료 요청기관 단말기(2)에 전송할 수 있다.
- [40] 블록체인 기반 증거자료 공증 시스템(1)을 구성하는 각 구성요소들은 네트워크(network)를 통해 연결될 수 있다. 네트워크는 단말들 및 서버들과 같은 각각의 노드 상호 간에 정보 교환이 가능한 연결 구조를 의미하는 것으로, 이러한 네트워크(network)의 일 예에는 3GPP(3rd Generation Partnership Project) 네트워크, LTE(Long Term Evolution) 네트워크, WIMAX(World Interoperability for Microwave Access) 네트워크, 인터넷 (Internet), LAN(Local Area Network), Wireless LAN(Wireless Local Area Network), WAN(Wide Area Network), PAN(Personal Area Network), 블루투스(Bluetooth) 네트워크, 위성 방송 네트워크, 아날로그 방송 네트워크, DMB(Digital Multimedia Broadcasting) 네트워크, WiFi 등이 포함되나 이에 한정되지는 않는다.
- [41] 블록체인 서버(6)는 복수개의 노드로 마련될 수 있다. 블록체인 서버(6)는 하나 이상의 분산원장과 체인코드가 저장되는 소수의 피어(peer)로 구성되어 있고, 체인코드는 CLI 명령어로 실행되며 QSCC(Query System ChainCode), ESCC(Endorsement System ChainCode), VSCC(Validation System ChainCode), CSCC(Configuration System ChainCode) 및 LSCC(Lifecycle System ChainCode) 등이 있다. QSCC는 블록체인의 저장된 데이터를 읽어올 때 사용되는 체인코드이고, ESCC는 보증 정책을 담당하는 체인코드이고, VSCC는 블록을 검증할 때 사용되는 체인코드이다. 또한, CSCC는 채널 설정 시 사용되는 체인코드이고, LSCC는 체인코드의 설치부터 인스턴스화까지 모든 일련의 과정을 수행하는 데 사용되는 체인코드이다.
- [42] 이러한 블록체인 서버(6)는 신뢰할 수 있는 기관에 의한 서버가 패브릭 네트워크를 구성하고, 네트워크 설정을 변경할 수 있는 관리자 권한에 의해, 채널에 참여하길 원하는 소수의 노드와 공증 서버(4)가 피어(peer)를 생성하게 된다. 여기서, 각각의 피어는 원장을 저장하고 있고, 각 피어에 체인코드를 설치 및 설치하고 그 인터페이스를 다른 피어들에게 알리는 인스턴스 과정 이후 체인코드의 쿼리함수의 호출(invok)이 가능하게 된다. 이러한 구조에 따라, 블록체인 서버(6)는 신뢰할 수 있는 공증 서버(4)가 노드로 참여함으로써 소수의 피어들의 원장을 증명해주는 역할을 할 수 있다.
- [43] 공증자 단말기(5), 공증서버(4), 증거자료 요청기관 단말기(2) 및 사용자 단말기(3)는 블록체인 서버(6)의 복수개의 노드 중 하나로 참여하여, 데이터를 송수신할 수 있다.
- [44]
- [45] 도2는 공증 서버를 나타내는 개념도이다.
- [46] 공증 서버(4)는 통신부(10), 제어부(20)를 포함할 수 있고, 제어부(20)는 회원 관리부(21), 암호화부(22) 및 클라우드 연동부(23)를 포함할 수 있다.

- [47] 사용자는 사용자 단말기(3)를 이용하여 공증 서버(4)에 접속할 수 있다. 사용자는 공증 서버(4)에서 회원가입절차를 수행하여 고유한 ID를 생성할 수 있다. 사용자 단말기(3)에 탑재되는 인증장치로부터 사용자의 인증을 수행하여 회원가입절차를 수행할 수 있다. 이 때, 사용자의 인증은 사용자의 개인정보, ID정보, 안면인식 정보, 홍채정보 또는 지문정보일 수 있다. 다만, 이에 한정되는 것은 아니다.
- [48] 회원 관리부(21)는 사용자의 정보를 저장하여 관리할 수 있다. 사용자의 정보는 사용자의 개인정보, ID정보, 안면인식 정보, 홍채정보 또는 지문정보일 수 있다.
- [49] 통신부(10)는 사용자 단말기(3)로부터 증거자료를 수신할 수 있다. 이 때, 증거자료는 사용자 단말기(3)로부터 촬영된 이미지 파일, 오디오 파일, 텍스트 파일, 영상 파일일 수 있으나, 다만 이에 한정되는 것은 아니다.
- [50] 암호화부(22)는 사용자 단말기(3)로부터 수신한 증거자료의 파일을 암호화하여 파일 소스코드에 대한 해시값을 생성할 수 있다.
- [51] 클라우드 연동부(23)는 증거자료의 파일과 생성된 해시값을 매칭시켜 클라우드 저장소에 저장되도록 클라우드와 공증 서버(4)간 통신을 통해 연동시킬 수 있다.
- [52] 클라우드는 데이터, 소프트웨어 및 다양한 컴퓨터 자원 등을 사용자가 소유하고 있는 하드웨어에 두지 않고 인터넷을 통해 접근할 수 있도록 저장되는 저장소를 의미한다.
- [53] 이 때, 공증 서버(4)는 해당 증거자료가 진실한 것인지 여부를 공증하기 위해서, 공증자 단말기(5)에 증거자료의 해시값을 전송할 수 있다.
- [54]
- [55] 도3은 블록체인 서버를 나타내는 개념도이다.
- [56] 블록체인 서버(6)는 복수개의 노드로 마련되며, 해당 노드에는 통신부(30), 서명 관리부(41), 스마트 컨트랙트 블록 관리부(42) 및 지갑 연동부(44)를 포함할 수 있다.
- [57] 통신부(30)는 사용자 단말기(3)로부터 사용자의 트랜잭션 서명 원본, 공개키, 전자 서명을 수신할 수 있다.
- [58] 이 때, 서명 관리부(41)는 수신한 사용자의 트랜잭션 서명과 공증자의 트랜잭션 서명 원본을 검증하고, 검증된 트랜잭션 서명 원본을 저장할 수 있다. 서명 관리부(41)는 공개키를 이용하여 트랜잭션 서명 원본을 검증할 수 있다. 즉, 사용자 단말기(3)로부터 수신한 사용자의 공개키로 전자 서명을 복호화하고, 트랜잭션 서명 원본을 해싱하여 얻은 해시 값과 비교하여 해당 전자 서명이 위조된 것이 아님을 확인하여 트랜잭션 서명 원본을 검증할 수 있는 것이다.
- [59] 만약, 복호화된 전자 서명과 해시 값이 일치하지 않는 경우에는 트랜잭션 서명 원본이 위조된 것으로 판단하여, 통신부(30)는 사용자 단말기(3)로 전자 서명을 요청할 수 있다.
- [60] 통신부(30)는 공증자 단말기(5)로부터 공증자의 트랜잭션 서명 원본, 공개키,

전자 서명을 수신할 수 있다. 이 때, 공개키를 이용하여 트랜잭션 서명 원본을 검증할 수 있다. 즉, 공증자 단말기(5)로부터 수신한 공증자의 공개키로 전자 서명을 복호화하고, 트랜잭션 서명 원본을 해싱하여 얻은 해시 값과 비교하여 해당 전자 서명이 위조된 것이 아님을 확인하여 트랜잭션 서명 원본을 검증할 수 있는 것이다.

- [61] 만약, 복호화된 전자 서명과 해시 값이 일치하지 않는 경우에는 트랜잭션 서명 원본이 위조된 것으로 판단하여, 통신부(30)는 공증자 단말기(5)로 전자 서명을 요청할 수 있다.
- [62] 스마트 컨트랙트 블록 관리부(42)는 사용자와 공증자의 트랜잭션 서명 원본 이 위조된 것이 아닌 것으로 검증되면, 트랜잭션이 수행되어 스마트 컨트랙트 블록을 생성할 수 있다. 스마트 컨트랙트 블록에 저장된 정보는 도4에서 상세히 후술하도록 한다.
- [63] 토큰 생성부(43)는 스마트 컨트랙트 블록을 기초로 토큰을 생성할 수 있다. 이 때, 토큰은 대체가능(Fungible)토큰과 대체불가능(Non-Fungible) 토큰으로 분류될 수 있다. 대체가능 토큰은 동일한 타입의 다른 토큰과 교환이 가능하지만 대체불가능 토큰은 동일한 타입의 다른 토큰과 교환이 불가능하다는 특징이 있다. 본 발명의 토큰은 블록체인 네트워크의 ERC-721, ERC-1155 표준의 대체불가능 토큰(NFT: Non Fungible Token)으로 이루어질 수 있으나, 이에 한정하는 것은 아니다.
- [64] 지갑 연동부(44)는 토큰 생성부(43)가 생성한 토큰이 저장되도록 통합 API를 통해 전자지갑과 연동될 수 있다. 전자지갑은 스마트컨트랙트 블록에 판매자의 서명이 기록되어 있으면, 판매자의 고유한 트랜잭션에 해당되는 하나의 개인 온라인 전자지갑이 자동으로 생성될 수 있다. 전자지갑은 토큰을 저장하고 인출할 수 있도록 판매자의 고유의 개인 은행 계좌 역할로서 전자 은행 계좌처럼 작동될 수 있는 것이다. 이 때, 전자지갑은 통합 API가 제공되어 METAMASK, Klay, MyCrypto 등의 웹 지갑 어플리케이션과 연동되는 것일 수 있다.
- [65]
- [66] 도4는 스마트 컨트랙트 블록을 나타내는 도면이다.
- [67] 스마트 컨트랙트 블록은 공증 서버(4)에 가입된 사용자의 ID, 해시값인 URL주소, 파일의 생성일시, 파일의 크기, 파일의 확장자, 사용자의 지갑 주소 및 사용자와 공증자의 트랜잭션 서명 원본 정보를 포함할 수 있다.
- [68] 스마트 컨트랙트 블록은 복수개로 마련되어 블록체인 서버(6)에 생성될 수 있다. 사용자가 사용자 단말기(3)를 통해 공증을 요청한 증거자료가 복수개인 경우, 각각의 증거자료에 대한 스마트 컨트랙트 블록이 생성될 수 있는 것이다.
- [69]
- [70] 도5는 본 발명의 일 실시예에 따른 블록체인 기반 증거자료 공증 시스템의 제어방법을 나타내는 전체적인 흐름도이다.
- [71] 본 발명의 일 실시예에 따른 블록체인 기반 증거자료 공증 시스템의

제어방법은 도 1에 도시된 블록체인 기반 증거자료 공증 시스템(1)과 실질적으로 동일한 구성 상에서 진행되므로, 도 1의 블록체인 기반 증거자료 공증 시스템(1)과 동일한 구성요소에 대해 동일한 도면 부호를 부여하고, 반복되는 설명은 생략하기로 한다.

[72] 사용자 단말기(3)는 공증 서버(4)에 회원가입을 요청할 수 있고, 회원가입을 위한 인증절차가 수행되면 공증 서버(4)에 사용자의 정보가 저장될 수 있다.

[73] 사용자 단말기(3)는 단말기에 마련된 카메라 장치를 통해 사진을 촬영하고, 사진파일을 공증 서버(4)에 전송할 수 있다. 이 때, 도5에서 도시하지는 않았으나, 동영상 파일, 오디오 파일 및 텍스트 파일일 수도 있으며, 파일 종류는 제한하지 않는다.

[74] 공증 서버(4)는 사용자 단말기(3)로부터 수신한 파일을 암호화하여 해시값을 생성할 수 있고, 클라우드와 연동되어 클라우드에 파일과 해시값을 매칭하여 저장할 수 있다.

[75] 공증 서버(4)는 사용자 단말기(3)와 공증자 단말기(5)에 해시값을 전송할 수 있다. 공증자 단말기(5)는 해시값을 수신하여 해당 증거자료를 공증할 수 있다.

[76] 공증자 단말기(5)는 트랜잭션에 대한 서명 원본, 공개키, 전자 서명을 블록체인 서버(6)에 전송하고, 사용자 단말기(3)는 트랜잭션에 대한 서명 원본, 공개키, 전자 서명을 블록체인 서버(6)에 전송할 수 있다.

[77] 이 때, 블록체인 서버(6)는 수신한 사용자의 트랜잭션 서명과 공증자의 트랜잭션 서명 원본을 검증하고, 검증된 트랜잭션 서명 원본을 저장할 수 있다. 트랜잭션 서명을 검증하는 것은 공개키를 이용하여 트랜잭션 서명 원본을 검증하는 것을 의미할 수 있다. 즉, 사용자 단말기(3)로부터 수신한 사용자의 공개키와 공증자 단말기(5)로부터 수신한 공증자의 공개키로 사용자와 공증자 각각의 전자 서명을 복호화하고, 트랜잭션 서명 원본을 해싱하여 얻은 해시 값과 비교하여 해당 전자 서명이 위조된 것이 아님을 확인하여 트랜잭션 서명 원본을 검증할 수 있는 것이다.

[78] 트랜잭션 서명 원본이 유효한 것으로 검증되는 경우에는 블록체인 서버(6)에 사용자의 트랜잭션 서명 원본, 공증자의 트랜잭션 서명 원본이 저장될 수 있다.

[79] 블록체인 서버(6)는 사용자와 공증자의 트랜잭션 서명 원본 이 위조된 것이 아닌 것으로 검증되면, 트랜잭션이 수행되어 스마트 컨트랙트 블록을 생성할 수 있다. 또한, 블록체인 서버(6)는 스마트 컨트랙트 블록을 기초로 토큰을 생성할 수 있으며, 블록체인 서버(6)와 연동되는 지갑에 해당 토큰이 저장될 수 있다.

[80]

[81] 도6은 본 발명의 일 실시예에 따른 블록체인 기반 증거자료 공증 시스템의 제어방법을 나타내는 전체적인 흐름도이다.

[82] 공증자에 의해 이미 공증되어 공증 서버(4)와 연동되는 클라우드 저장소에 저장된 사용자의 증거자료를 증거자료 요청기관 단말기(2)에 제출할 수 있다.

[83] 도6을 참조하면, 증거자료 요청기관 단말기(2)로부터 사용자 단말기(3)는

증거자료 제출 요청 신호를 수신할 수 있다. 이 때, 사용자는 회원 가입된 공증 서버(4)에 사용자 인증 정보를 통해 로그인할 수 있다.

- [84]     사용자가 공증 서버(4)에 로그인하면, 회원 관리부(21)에 저장된 사용자 정보와 사용자 인증 정보가 일치하는지 여부를 확인하고, 일치하는 경우 사용자의 로그인을 수락할 수 있다.
- [85]     사용자는 공증 서버(4)에 공증된 증거자료의 검색을 요청할 수 있다. 이 때, 공증 서버(4)는 사용자의 트랜잭션 서명 원본이 포함된 스마트 컨트랙트 블록의 존재여부를 블록체인 서버(6)에 조회를 요청할 수 있고, 블록체인 서버(6)로부터 조회 결과를 수신할 수 있다. 해당 스마트 컨트랙트 블록에 사용자의 트랜잭션 서명 원본이 포함된 스마트 컨트랙트 블록이 존재한다는 결과를 수신하면, 공증 서버(4)는 클라우드 저장소에 저장된 사용자의 공증된 증거자료 목록을 검색할 수 있다.
- [86]     이 때, 사용자가 공증받은 증거자료가 복수개인 경우에는, 공증 서버(4)는 사용자 단말기(3)에 증거자료를 선택하도록 요청하는 신호를 전송할 수 있고, 사용자는 사용자 단말기(3)를 통해 증거자료를 선택할 수 있다. 이 때, 사용자는 복수개의 증거자료를 선택할 수도 있을 것이다.
- [87]     공증 서버(4)는 사용자 단말기(3)에 해당 증거자료의 해시값을 전송할 수 있으며, 사용자 단말기(3)는 증거자료 요청기관 단말기(2)에 해당 증거자료의 해시값을 전송하여 증거자료를 제출할 수 있다.
- [88]     도6에서는 도시하지 않았으나, 공증 서버(4)는 사용자 단말기(3)에 증거자료 발급 방식을 선택하는 신호를 전송할 수 있다. 증거자료 발급 방식은 블록체인 서버(6)가 생성한 토큰 또는 공증된 파일의 해시값일 수 있다.
- [89]     사용자가 토큰으로 증거자료를 발급하는 방식을 선택하면, 공증 서버(4)의 통신부(10)는 블록체인 서버(6)의 통신부(30)에 해당 신호를 전송할 수 있다.
- [90]     이 때, 사용자의 전자지갑에 저장된 토큰이 증거자료 요청기관 단말기(2)의 전자 지갑 주소로 전송될 수 있다.
- [91]     이와 같은, 블록체인 기반 증거자료 공증 시스템의 제어방법은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나와 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.
- [92]     컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히

구성된 하드웨어 장치가 포함된다.

[93] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[94] 이상에서 본 발명의 실시예들에 대하여 설명하였으나, 본 발명의 사상은 본 명세서에 제시되는 실시 예에 제한되지 아니하며, 본 발명의 사상을 이해하는 당업자는 동일한 사상의 범위 내에서, 구성요소의 부가, 변경, 삭제, 추가 등에 의해서 다른 실시 예를 용이하게 제안할 수 있을 것이나, 이 또한 본 발명의 사상범위 내에 든다고 할 것이다.

[95] [부호의 설명]

[96] 1: 블록체인 기반 증거자료 공증 시스템

[97] 2: 증거자료 요청기관 단말기

[98] 3: 사용자 단말기

[99] 4: 공증 서버

[100] 5: 공증자 단말기

[101] 6: 블록체인 서버

[102] 10: 공증서버의 통신부

[103] 20: 공증서버의 제어부

[104] 21: 회원 관리부

[105] 22: 암호화부

[106] 23: 클라우드 연동부

[107] 30: 블록체인 서버의 통신부

[108] 40: 블록체인 서버의 제어부

[109] 41: 서명 관리부

[110] 42: 스마트 컨트랙트 블록 관리부

[111] 43: 토큰 생성부

[112] 44: 지갑 연동부

## 청구범위

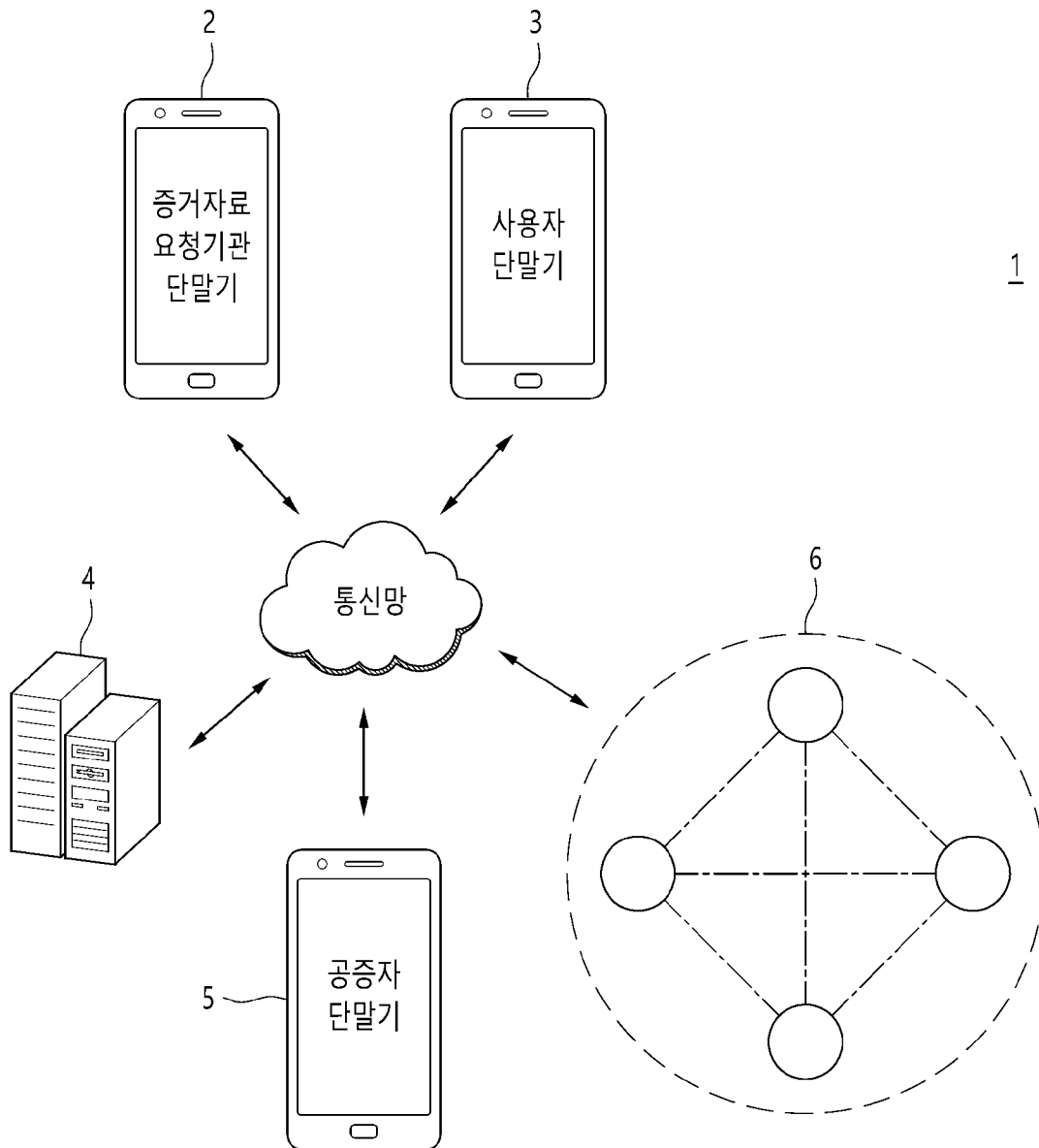
- [청구항 1]     사용자로부터의 증거자료에 대한 공증요청에 응답하여 상기 증거자료를  
블록체인 기반으로 공증하기 위한 블록체인 기반 증거자료 공증  
시스템에 있어서,  
상기 공증요청에 따라 상기 증거자료를 전송하는 사용자 단말기;  
상기 증거자료를 수신하고 이를 암호화하여 상기 증거자료에 대한  
해시값을 생성하고, 상기 생성된 해시값을 각각 상기 사용자 단말기와  
상기 증거자료에 대한 공증을 수행하는 공증자 단말기 측에 전송하는  
공증서버; 및  
상기 사용자 단말기와 공증자 단말기 측으로부터 각각 상기 해시값에  
작성한 서명을 수신하고, 상기 서명이 작성된 해시값을 기초로  
스마트컨트랙트 블록을 생성하는 블록체인 서버;를 포함하는 블록체인  
기반 증거자료 공증 시스템.
- [청구항 2]     제 1항에 있어서,  
상기 공증 서버는,  
상기 사용자 단말기로부터 상기 증거자료를 수신하는 통신부;  
상기 사용자의 정보를 관리하는 회원 관리부;  
상기 증거자료를 암호화하여 해시값을 생성하는 암호화부; 및  
상기 증거자료와 해시값이 매칭되어 클라우드 저장소에 저장되도록 상기  
클라우드 저장소와 연동되는 클라우드 연동부;를 포함하는 블록체인  
기반 증거자료 공증 시스템.
- [청구항 3]     제 2항에 있어서,  
상기 블록체인 서버는,  
상기 사용자 단말기로부터 상기 사용자의 트랜잭션 서명을 수신하고,  
상기 공증자 단말기로부터 상기 공증자의 트랜잭션 서명을 수신하는  
통신부;  
상기 수신한 사용자의 트랜잭션 서명과 상기 공증자의 트랜잭션 서명을  
검증하고, 검증된 상기 트랜잭션 서명을 저장하는 서명관리부;  
상기 트랜잭션이 실행되어 스마트 컨트랙트 블록을 생성하는 스마트  
컨트랙트 블록 관리부;  
상기 스마트 컨트랙트 블록을 기초로 토큰을 생성하는 토큰 생성부; 및  
상기 토큰 생성부가 생성한 토큰이 저장되도록 통합 API를 통해  
전자지갑과 연동되는 지갑 연동부;를 포함하는 블록체인 기반 증거자료  
공증 시스템.
- [청구항 4]     제 3항에 있어서,  
상기 공증 서버는,  
상기 사용자 단말기로부터 증거자료 검색을 요청받으면, 상기 블록체인

- 서버에 상기 사용자 서명이 포함된 상기 스마트 컨트랙트 블록의 존재여부 확인을 요청하는 블록체인 기반 증거자료 공증 시스템.
- [청구항 5] 제 4항에 있어서,  
상기 공증서버는,  
상기 블록체인 서버로부터 상기 사용자 서명이 포함된 상기 스마트 컨트랙트 블록이 존재한다는 신호를 수신하면, 상기 클라우드 연동부로부터 상기 클라우드에 저장된 사용자의 공증된 증거자료의 해시값을 상기 사용자 단말기에 전송하는 블록체인 기반 증거자료 공증 시스템.
- [청구항 6] 제 5항에 있어서,  
상기 사용자 단말기는,  
증거자료 요청기관 단말기에 상기 공증된 증거자료의 해시값을 전송하는 블록체인 기반 증거자료 공증 시스템.
- [청구항 7] 사용자로부터의 증거자료에 대한 공증요청에 응답하여 상기 증거자료를 블록체인 기반으로 공증하기 위한 블록체인 기반 증거자료 공증 시스템의 제어방법에 있어서,  
사용자 단말기가 상기 공증요청에 따라 상기 증거자료를 전송하고,  
공증서버가 상기 증거자료를 수신하고 이를 암호화하여 상기 증거자료에 대한 해시값을 생성하고, 상기 생성된 해시값을 각각 상기 사용자 단말기와 상기 증거자료에 대한 공증을 수행하는 공증자 단말기 측에 전송하며,  
블록체인 서버가 상기 사용자 단말기와 공증자 단말기 측으로부터 각각 상기 해시값에 작성한 서명을 수신하고, 상기 서명이 작성된 해시값을 기초로 스마트컨트랙트 블록을 생성하는 것을 포함하는 블록체인 기반 증거자료 공증 시스템의 제어방법.
- [청구항 8] 제 7항에 있어서,  
상기 공증서버는 상기 사용자 단말기로부터 상기 증거자료를 수신하고, 상기 사용자의 정보를 관리하며, 상기 증거자료를 암호화하여 해시값을 생성하고, 상기 증거자료와 해시값이 매칭되어 클라우드 저장소에 저장되도록 상기 클라우드 저장소와 연동되는 블록체인 기반 증거자료 공증 시스템의 제어방법.
- [청구항 9] 제 8항에 있어서,  
상기 블록체인 서버는 상기 사용자 단말기로부터 사용자의 트랜잭션 서명을 수신하고, 상기 공증자 단말기로부터 상기 공증자의 트랜잭션 서명을 수신하며, 상기 수신한 사용자의 트랜잭션 서명과 상기 공증자의 트랜잭션 서명을 검증하고, 검증된 상기 트랜잭션 서명을 저장하며, 상기 트랜잭션이 실행되어 스마트 컨트랙트 블록을 생성하고, 상기 스마트 컨트랙트 블록을 기초로 토큰을 생성하되, 생성된 토큰이 통합 API를

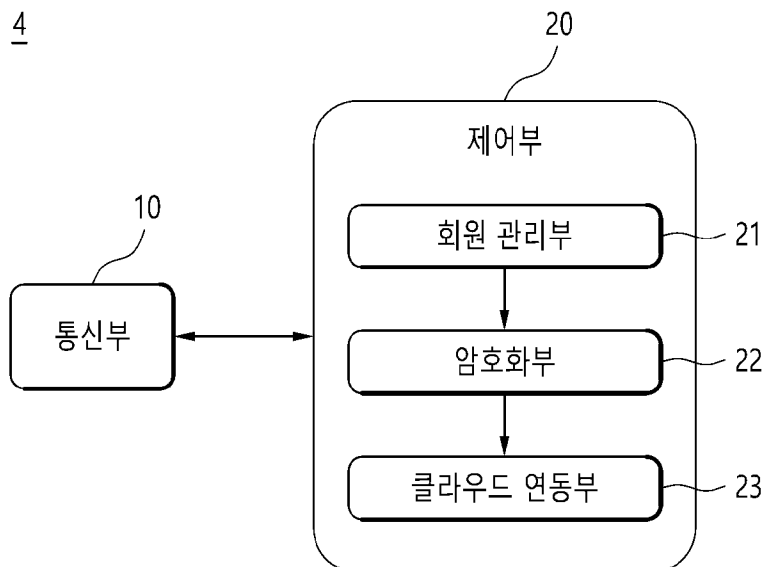
통해 연동되는 전자지갑에 저장되는 블록체인 기반 증거자료 공증 시스템의 제어방법.

- [청구항 10] 제 7항에 따른 상기 블록체인 기반 증거자료 공증 시스템의 제어방법을 수행하기 위한 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 저장 매체.

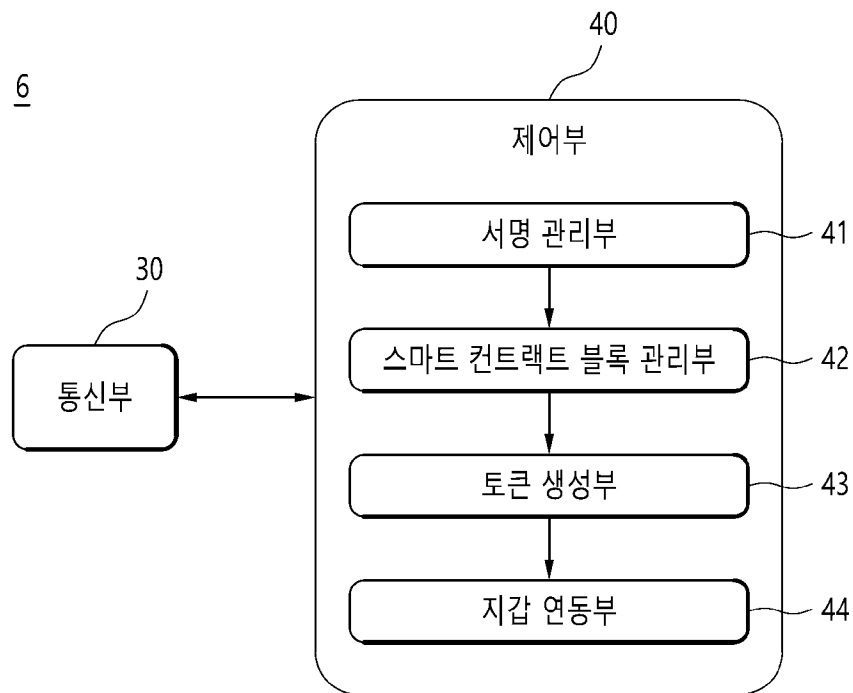
[도1]



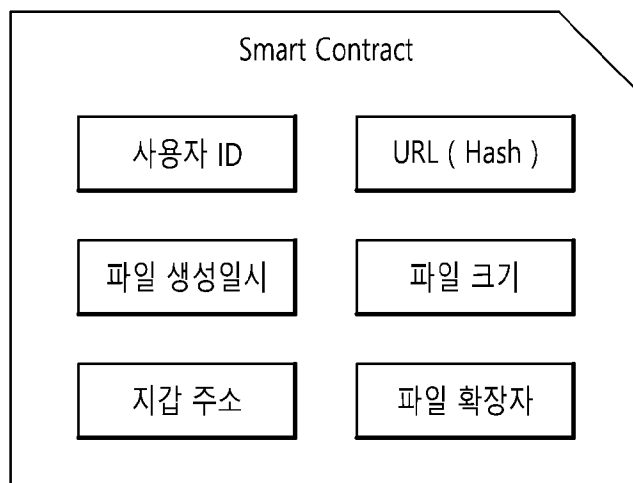
[도2]



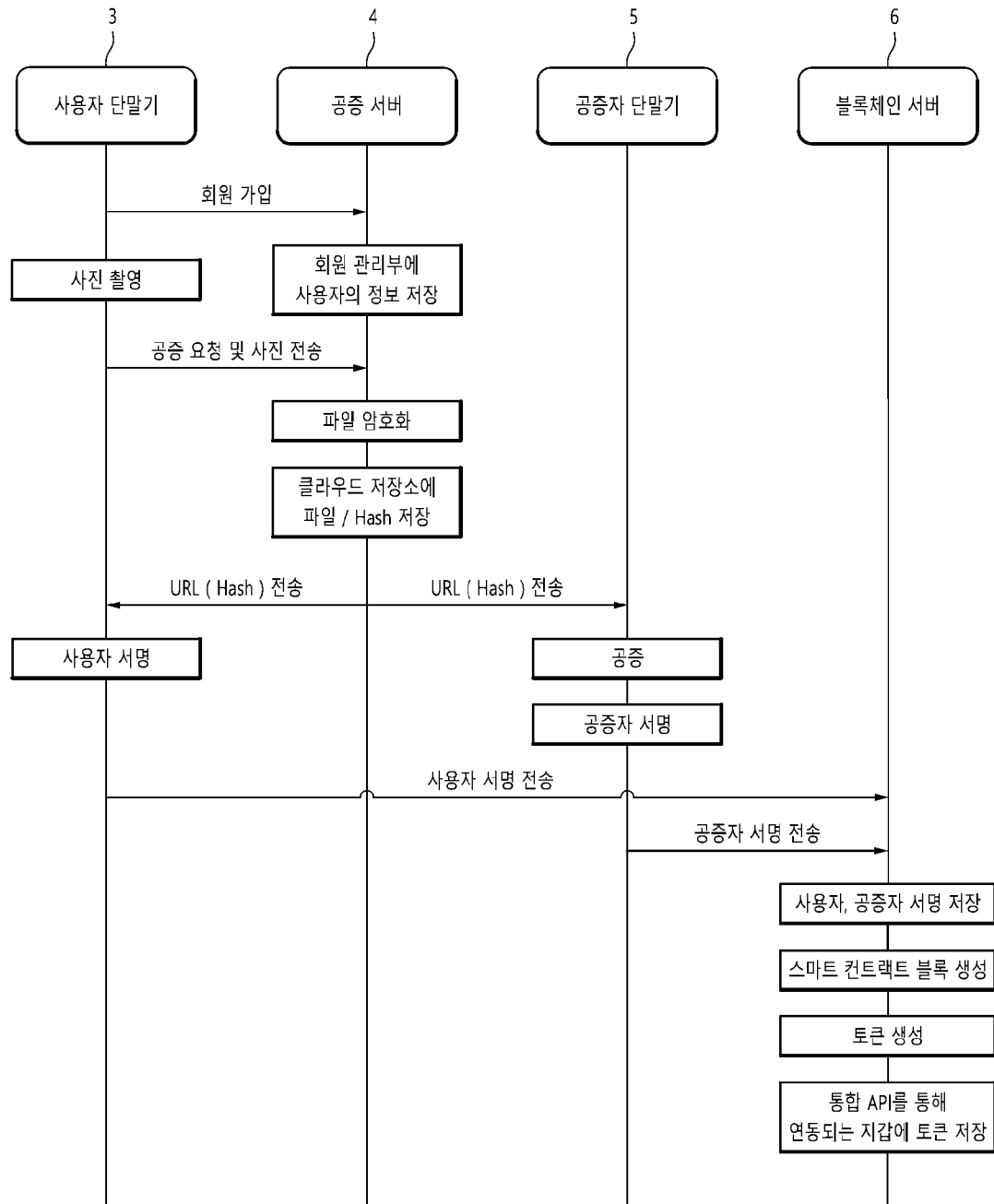
[도3]



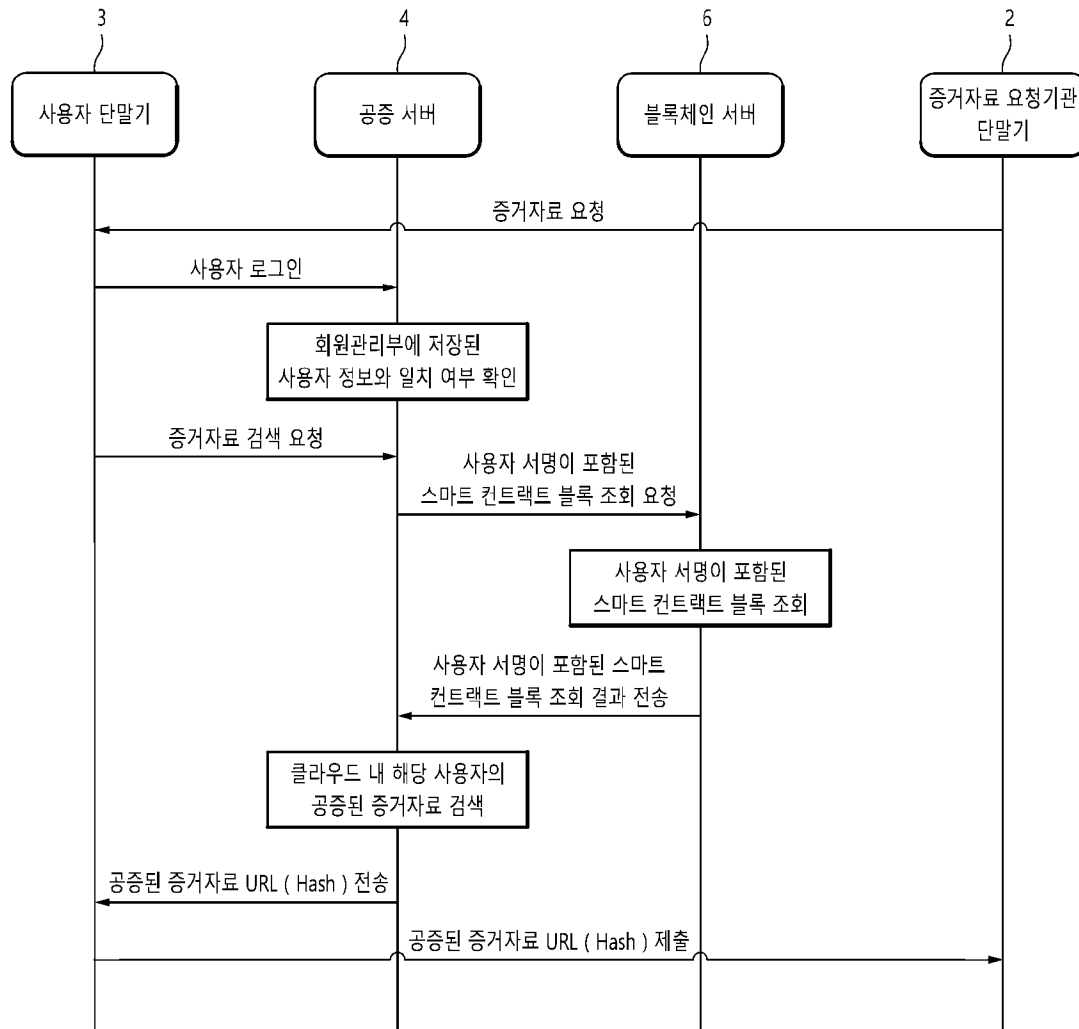
[도4]



[도5]



[도6]



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2022/016801

**A. CLASSIFICATION OF SUBJECT MATTER****G06Q 50/26**(2012.01)i; **H04L 9/06**(2006.01)i; **H04L 9/00**(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 50/26(2012.01); G06F 16/901(2019.01); G06F 16/904(2019.01); G06F 21/10(2013.01); G06F 21/60(2013.01);  
G06F 21/64(2013.01); G06Q 20/38(2012.01); G06Q 30/06(2012.01); G06Q 40/02(2012.01)

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) &amp; keywords: 블록체인(blockchain), 증거(evidence), 공증(notarization), 서명(signature)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages                                                                        | Relevant to claim No. |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Y         | CN 112035894 A (JIANGSU WORLD AALLWELL HOLDINGS CO., LTD.) 04 December 2020 (2020-12-04)<br>See paragraphs [0047] and [0060]-[0062] and claims 1-2 and 5. | 1-10                  |
| Y         | JP 2021-149904 A (BACOR DAPPS CO., LTD. et al.) 27 September 2021 (2021-09-27)<br>See paragraphs [0065]-[0066], [0071] and [0073] and claim 1.            | 1-10                  |
| Y         | KR 10-2244185 B1 (KIM, Tae Heon) 23 April 2021 (2021-04-23)<br>See paragraphs [0016], [0060]-[0061] and [0081]-[0084] and claim 1.                        | 1,7,10                |
| Y         | KR 10-2008001 B1 (MOFAS CO., LTD. et al.) 06 August 2019 (2019-08-06)<br>See paragraphs [0029] and [0041]-[0042] and claim 1.                             | 1,7,10                |
| A         | KR 10-2259851 B1 (ICERTI CO., LTD.) 03 June 2021 (2021-06-03)<br>See entire document.                                                                     | 1-10                  |



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

“D” document cited by the applicant in the international application

“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

13 February 2023

Date of mailing of the international search report

13 February 2023

Name and mailing address of the ISA/KR

**Korean Intellectual Property Office**  
**Government Complex-Daejeon Building 4, 189 Cheongsaro, 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/KR2022/016801**

| Patent document<br>cited in search report |             |    | Publication date<br>(day/month/year) | Patent family member(s) |             |    | Publication date<br>(day/month/year) |
|-------------------------------------------|-------------|----|--------------------------------------|-------------------------|-------------|----|--------------------------------------|
| CN                                        | 112035894   | A  | 04 December 2020                     | FR                      | 3112627     | A1 | 21 January 2022                      |
|                                           |             |    |                                      | JP                      | 2022-020595 | A  | 01 February 2022                     |
| JP                                        | 2021-149904 | A  | 27 September 2021                    | CN                      | 113841174   | A  | 24 December 2021                     |
|                                           |             |    |                                      | JP                      | 6804073     | B1 | 23 December 2020                     |
|                                           |             |    |                                      | WO                      | 2021-186814 | A1 | 23 September 2021                    |
| KR                                        | 10-2244185  | B1 | 23 April 2021                        | KR 10-2020-0129879      |             | A  | 18 November 2020                     |
| KR                                        | 10-2008001  | B1 | 06 August 2019                       | None                    |             |    |                                      |
| KR                                        | 10-2259851  | B1 | 03 June 2021                         | KR 10-2020-0145400      |             | A  | 30 December 2020                     |

| <b>A. 발명이 속하는 기술분류(국제특허분류(IPC))</b><br><b>G06Q 50/26(2012.01)i; H04L 9/06(2006.01)i; H04L 9/00(2006.01)i</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                      |                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| <b>B. 조사된 분야</b><br>조사된 최소문헌(국제특허분류를 기재)<br>G06Q 50/26(2012.01); G06F 16/901(2019.01); G06F 16/904(2019.01); G06F 21/10(2013.01); G06F 21/60(2013.01);<br>G06F 21/64(2013.01); G06Q 20/38(2012.01); G06Q 30/06(2012.01); G06Q 40/02(2012.01)<br>조사된 기술분야에 속하는 최소문헌 이외의 문헌<br>한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC<br>일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC<br>국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))<br>eKOMPASS(특허청 내부 검색시스템) & 키워드: 블록체인(blockchain), 증거(evidence), 공증(notarization), 서명(signature)                                                                         |                                                                                                      |                                               |
| <b>C. 관련 문헌</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                      |                                               |
| 카테고리*                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 인용문헌명 및 관련 구절(해당하는 경우)의 기재                                                                           | 관련 청구항                                        |
| Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | CN 112035894 A (JIANGSU WORLDALLWELL HOLDINGS CO., LTD.) 2020.12.04<br>단락 47, 60-62 및 청구항 1-2, 5 참조. | 1-10                                          |
| Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | JP 2021-149904 A (BACOR DAPPS CO., LTD. 등) 2021.09.27<br>단락 65-66, 71, 73 및 청구항 1 참조.                | 1-10                                          |
| Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | KR 10-2244185 B1 (김태현) 2021.04.23<br>단락 16, 60-61, 81-84 및 청구항 1 참조.                                 | 1,7,10                                        |
| Y                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | KR 10-2008001 B1 (주식회사 모파스 등) 2019.08.06<br>단락 29, 41-42 및 청구항 1 참조.                                 | 1,7,10                                        |
| A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | KR 10-2259851 B1 (주식회사 아이서티) 2021.06.03<br>전체 문서 참조.                                                 | 1-10                                          |
| <input type="checkbox"/> 추가 문헌이 C(계속)에 기재되어 있습니다. <input checked="" type="checkbox"/> 대응특허에 관한 별지를 참조하십시오.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                      |                                               |
| * 인용된 문헌의 특별 카테고리:<br>“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌<br>“D” 본 국제출원에서 출원인이 인용한 문헌<br>“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌<br>“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌<br>“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌<br>“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌<br>“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌<br>“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.<br>“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.<br>“&” 동일한 대응특허문헌에 속하는 문헌 |                                                                                                      |                                               |
| 국제조사의 실제 완료일<br><b>2023년02월13일(13.02.2023)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                      | 국제조사보고서 발송일<br><b>2023년02월13일(13.02.2023)</b> |
| ISA/KR의 명칭 및 우편주소<br>대한민국 특허청<br>(35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)<br>팩스 번호 +82-42-481-8578                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                      | 심사관<br>홍기완<br>전화번호 +82-42-481-5003            |

| 국제조사보고서에서<br>인용된 특허문헌 | 공개일        | 대응특허문헌               | 공개일        |
|-----------------------|------------|----------------------|------------|
| CN 112035894 A        | 2020/12/04 | FR 3112627 A1        | 2022/01/21 |
|                       |            | JP 2022-020595 A     | 2022/02/01 |
| JP 2021-149904 A      | 2021/09/27 | CN 113841174 A       | 2021/12/24 |
|                       |            | JP 6804073 B1        | 2020/12/23 |
|                       |            | WO 2021-186814 A1    | 2021/09/23 |
| KR 10-2244185 B1      | 2021/04/23 | KR 10-2020-0129879 A | 2020/11/18 |
| KR 10-2008001 B1      | 2019/08/06 | 없음                   |            |
| KR 10-2259851 B1      | 2021/06/03 | KR 10-2020-0145400 A | 2020/12/30 |