(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2020 년 7 월 2 일 (02.07.2020)

WIPO | PCT

(10) 국제공개번호
WO 2020/138525 A1

(51) 국제특허분류:
H04L 29/06 (2006.01) *H04L 29/08* (2006.01)

(21) 국제출원번호: PCT/KR2018/016652

(22) 국제출원일: 2018 년 12 월 26 일 (26.12.2018)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2018-0169042 2018 년 12 월 26 일 (26.12.2018) KR

(71) 출원인: 서강대학교 산학협력단 (**SOGANG UNIVERSITY RESEARCH FOUNDATION**) [KR/KR]; 04107 서울시 마포구 백범로 35, 서강대학교 떼이야르관 306호, Seoul (KR).

(72) 발명자: **조수환 (CHO, Soo-Hwan)**; 10081 경기도 김포시 김포한강2로 362, 616동 1202호, Gyeonggi-do (KR). **박수용 (PARK, Soo-Yong)**; 04075 서울시 마포구 독막로 18길 5, 101동 1001호, Seoul (KR). **김순태 (KIM, Sun-Tae)**; 54896 전라북도 전주시 덕진구 백제대로 567, 공과대학 5호관, Jeollabuk-do (KR).

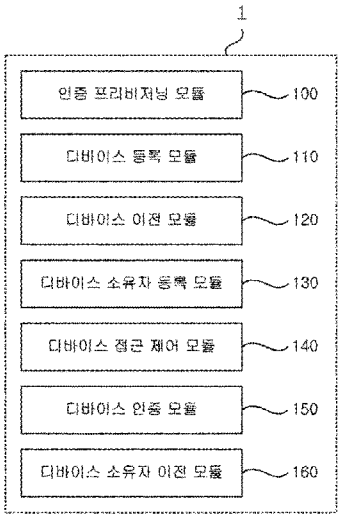
(74) 대리인: **이지연 (LEE, Ji-Yeon)**; 08793 서울시 관악구 남부순환로 1922, 청동빌딩 301, Seoul (KR).

(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, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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).

(54) **Title:** METHOD FOR DISTRIBUTED AUTHENTICATION OF DEVICE IN INTERNET-OF-THINGS BLOCKCHAIN ENVIRONMENT, AND SYSTEM FOR DISTRIBUTED AUTHENTICATION OF DEVICE USING SAME

(54) **발명의 명칭:** 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 방법 및 이를 이용한 디바이스 분산 인증 시스템



100 ... Authentication provisioning module
110 ... Device registration module
120 ... Device transfer module
130 ... Device owner registration module
140 ... Device access control module
150 ... Device authentication module
160 ... Device owner transfer module

(57) **Abstract:** The present invention relates to a system and method for distributed authentication of a device in an internet-of-things blockchain environment. In the system for distributed authentication of a device, each node: stores information and details about a device at each stage in a Distributed Hash Table (DHT) through blockchain consensus in order to perform authentication in an internet-of-things blockchain environment; requests, to a blockchain network, the control of user access or the authentication of a device, performs authentication by reaching a consensus on the basis of the stored details in the respective nodes, and multi-encrypts a message propagated by a manufacturer, a service provider, a user, and the like. Accordingly, the system for distributed authentication of a device according to the present invention can disallow the participation of counterfeit devices and devices having forged or falsified authentication information, prevent attacks utilizing stolen devices, prevent users from losing ownership, and prevent malicious users from accessing a device.

(57) **요약서:** 본 발명은 사물인터넷 블록체인 환경하에서의 디바이스 분산 인증 시스템 및 방법에 관한 것이다. 상기 디바이스 분산 인증 시스템은 사물인터넷 블록체인 환경에서 인증을 위해 각 단계별로 디바이스에 대한 정보 및 내역들을 블록체인 합의를 통해 각 노드가 분산 해쉬 테이블(Distributed Hash Table; 'DHT')에 저장하고, 사용자에 대한 접근 제어나 디바이스에 대한 인증은 블록체인 네트워크에 요청하며 각 노드들이 저장된 내역 기반으로 합의하여 승인을 하며, 제조사, 서비스 제공자, 사용자 등이 전파하는 메시지는 다중 암호화한다. 따라서, 본 발명에 따른 디바이스 분산 인증 시스템은 인증 정보의 위변조나 위조된 디바이스의 참여가 불가능하고, 기기의 탈취에 의한 공격을 방지할 수 있으며, 사용자의 소유권 탈취를 방지할 수 있으며, 악의적인 사용자가 디바이스에 접근하는 것을 방지할 수 있게 된다.

WO 2020/138525 A1

[다음 쪽 계속]

공개:
— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 방법 및 이를 이용한 디바이스 분산 인증 시스템

기술분야

[1] 본 발명은 사물인터넷 블록체인 환경에 관한 것으로서, 더욱 구체적으로는 사물 인터넷 블록체인 환경에 있어서 수많은 디바이스들에 대한 분산 인증을 위해 참여자들의 서명키 생성, 인증 정보 위변조를 막기 위한 블록체인 합의에 의한 분산 저장, 및 디바이스에 대한 인증 이력 데이터를 검증하기 위한 다중 서명 검증 기술을 사용하는 안정성을 갖는 디바이스 분산 인증 방법 및 이를 이용하여 구현한 디바이스 분산 인증 시스템에 관한 것이다.

[2] This work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2017-0-00325,blockchain based IoT reliability mangement system development)

배경기술

[3] 사물 인터넷(Internet of things; 'IoT')은 사물로 식별할 수 있는 시스템에 Bluetooth, Wi-Fi, LTE, Zigbee, NFC 등 다양한 센서와 통신 기능을 내장하여 실시간으로 데이터를 인터넷을 기반으로 연결하여 사물과 사물, 사람과 사물 간의 정보를 주고 받는 지능형 기술과 서비스를 의미한다. 현재 사물인터넷 환경은 수많은 디바이스의 연결제어, 확장성, 대용량의 데이터 처리, 보안등의 문제로 클라우드 기반의 중앙 집중형 환경에서 기기간의 연결을 이루는 분산형 환경인 포그, 엣지 컴퓨팅의 형태로 발전되고 있다.

[4] 분산된 사물인터넷 환경에서의 신뢰성 및 보안을 위한 프로토콜로서 블록체인(BlockChain)의 기술 적용 가능성이 제시되고 있다. 실제로 IBM은 사물인터넷 블록체인 환경을 제안한 바 있으며, 이는 사물 디바이스, 클라우드, 컴퓨터등이 블록체인 기반의 사물인터넷 피어 투 피어(Peer-to-peer)네트워크 환경으로 구성된다.

[5] 이러한 사물인터넷 블록체인 환경에서 새롭게 제시되는 문제는 기기인증이다. 비허가된 사물 디바이스의 인증 및 네트워크의 참여는 모방공격 (Imitation attacks), 개인 정보 공격(Privacy attacks), 차단 공격(Blocking attacks), 스푸핑 공격(Spoofing Attacks)등이 발생하게 될 우려가 있으며, 이로 인해 사물인터넷의 정상적인 서비스 제공 및 이용을 막는 보안 위협들이 나타나게 되는 문제가 발생하게 된다. 특히, 이러한 기기 인증 문제는 중앙 집중화된 인증서버에 대한(Certificate Authority, CA)의 보안 문제를 발생시키게 된다.

[6] 따라서, 기존의 사물인터넷 중앙 집중형 환경의 인증 문제를 해결하기 위해서 분산환경에서의 노드간의 합의를 통한 인증 체계가 필요하다. 본 발명에서는 사물인터넷의 CA기관에 의한 인증문제를 해결하기 위해, 분산화된 사물인터넷

블록체인 환경에서의 기기 분산 인증 프로토콜을 제시하고자 한다.

[7] 사물인터넷 블록체인 환경에서의 분산 기기인증의 해결해야 하는 문제점은 아래와 같다. 1. 중앙 집중형 CA기관에 의한 인증과 비교하여 분산 인증 시스템은 악의적인 노드의 공격이 발생하거나 시스템이 실패되는 경우에도 올바른 인증을 수행 하여야 한다. 2. 사전에 허가된 기기의 인증 정보(기기고유 식별값, 서명검증, 네트워크 맥주소)에 대한 올바른 인증을 수행할 수 있어야 한다. 공격자로부터 인증 정보가 위변조되거나 잘못된 정보에 의해 비 인가된 기기가 네트워크에 참여하는 것을 차단할 수 있어야 한다. 3. 모든 사물 디바이스는 사용자가 존재하며, 디바이스에 대한 소유권이 있다. 따라서, 해당 디바이스에 대한 소유권을 증명할 수 있어야 하며, 비 인가된 사용자의 소유권을 부인할 수 있어야 한다. 4. 사물 디바이스에 대한 소유권이 증명되면, 해당 디바이스의 리소스에 대한 접근 제어가 가능해야 하며, 악의적인 공격자에 의한 디바이스에 대한 접근 제어는 차단되어야 한다. 5. 사물인터넷 환경은 기기에 대한 교환이 빈번히 일어나게 되는데, 이러한 경우 이전 소유자로부터 새로운 소유자로의 올바른 기기 소유권 이전이 가능해야 한다.

발명의 상세한 설명

기술적 과제

[8] 전술한 문제점들을 해결하기 위한 본 발명에 따른 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 방법을 제공하는 것을 목적으로 한다.

[9] 본 발명의 다른 목적은 전술한 디바이스 분산 인증 방법으로 구현된 디바이스 분산 인증 시스템을 제공하는 것을 다른 목적으로 한다.

과제 해결 수단

[10] 본 발명의 제1 특징에 따른 디바이스 분산 인증 시스템은, 디바이스 제조사, 디바이스, 소유자, 서비스 제공자를 포함하는 참여자들이 블록체인 네트워크(PIBN)를 형성하는 사물 인터넷 블록체인 환경에서의 디바이스 분산 인증 시스템에 관한 것으로서, 상기 블록체인 네트워크의 참여자들의 각각에 대한 서명키와 검증키를 생성하고, 고유 식별값과 함께 블록체인 네트워크에 등록하는 인증 프리비저닝 모듈; 및 제조사에 의해 생성된 디바이스를 등록하는 디바이스 등록 모듈; 을 구비하고,

[11] 상기 디바이스 등록 모듈은, 제조사가 디바이스의 고유 식별값(UUID) 및 서명키와 검증키를 생성하고, 디바이스 등록 메시지(Md)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하고, 네트워크의 참여 노드들이 전파된 디바이스 등록 메시지를 사전 등록된 제조사의 검증키로 검증하여 유효하면, 사전 설정된 합의 알고리즘으로 메시지 내용에 대한 합의를 진행하고, 합의되면 분산 해쉬 테이블(DHT)에 저장하는 과정을 실행하는 것을 특징으로 하며,

[12] 상기 디바이스 등록 메시지(Md)는 디바이스의 고유 식별값과 검증키를 포함하며 디바이스의 서명키로 서명된 메시지이다.

[13] 전술한 제1 특징에 따른 디바이스 분산 인증 시스템은, 상기 제조사에 의해 등록된 디바이스를 서비스 제공자에게 이전하는 디바이스 이전 모듈을 더 구비하고,

[14] 상기 디바이스 이전 모듈은, 서비스 제공자가 제조사로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 기기 이전 등록 메시지(Sd)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하며, 네트워크의 참여 노드들이 전파받은 기기 이전 등록 메시지를 서비스 제공자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 DHT에 저장하는 과정을 실행하는 것을 특징으로 하며,

[15] 상기 기기 이전 등록 메시지(Sd)는 디바이스의 고유 식별값과 검증키를 포함하며, 디바이스의 서명키로 1차 암호화하고 다시 서비스 제공자의 서명키로 2차 암호화하여 다중 암호화된 메시지인 것이 바람직하다.

[16] 전술한 제1 특징에 따른 디바이스 분산 인증 시스템은, 소유자가 서비스 제공자로부터 상기 디바이스를 이전받는 소유자 등록 모듈을 더 구비하고,

[17] 상기 소유자 등록 모듈은, 소유자가 서비스 제공자로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 소유자 등록 메시지(Od)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하고, 네트워크의 참여 노드들이 상기 전파받은 소유자 등록 메시지를 소유자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 DHT에 저장하는 과정을 실행하는 것을 특징으로 하며,

[18] 상기 소유자 등록 메시지(Od)는 디바이스의 고유 식별값과 검증키, 상기 디바이스가 연결된 네트워크 맥 주소를 포함하며 디바이스의 서명키로 1차 암호화하고 다시 소유자의 서명키로 2차 암호화하여 다중 암호화된 메시지인 것이 바람직하다.

[19] 전술한 제1 특징에 따른 디바이스 분산 인증 시스템은, 서비스 제공자로부터 디바이스를 이전받은 소유자에게 디바이스에 대한 접근 제어를 하는 디바이스 접근 제어 모듈을 더 구비하고,

[20] 상기 디바이스 접근 제어 모듈은, 소유자가 소유자 등록 메시지(Od)를 생성하고, 소유자 등록 메시지를 포함하는 디바이스 접근 제어 요청 메시지(DAC)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하고, 네트워크의 참여 노드들이 상기 전파받은 디바이스 접근 제어 요청 메시지를 사용자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 소유자에게 디바이스에 대한 접근 토큰을 전달하는 과정을 실행하는 것을 특징으로 하며,

[21] 상기 소유자 등록 메시지(Od)는 디바이스의 고유 식별값과 검증키, 디바이스가

연결된 네트워크 맥 주소를 포함하며, 디바이스의 서명키로 1차 암호화시키고 다시 소유자의 서명키로 2차 암호화하여 다중 암호화한 메시지인 것이 바람직하다.

[22] 전술한 제1 특징에 따른 디바이스 분산 인증 시스템은, 디바이스 인증 모듈을 더 구비하고,

[23] 상기 디바이스 인증 모듈은, 디바이스가 디바이스에 대한 고유 식별값(UUID) 및 연결된 네트워크 맥 주소를 디바이스의 서명키로 서명한 인증 요청 메시지(DA)를 생성한 후 PIBN 네트워크에 전파하는 과정을 실행하고, 네트워크의 참여 노드들이 전파받은 인증 요청 메시지를 디바이스의 검증키로 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 인증 토큰을 전달하는 과정을 실행하는 것이 바람직하다.

[24] 전술한 제1 특징에 따른 디바이스 분산 인증 시스템은, 기기 소유자가 디바이스를 새로운 기기 소유자에게 이전하는 디바이스 소유권 이전 모듈을 더 구비하고,

[25] 상기 디바이스 소유권 이전 모듈은, 새로운 기기 소유자가 이전 기기 소유자로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 새로운 소유자 등록 메시지(New_Od)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하고, 네트워크의 참여 노드들이 전파받은 소유권 이전 요청 메시지를 새로운 기기 소유자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 DHT에 저장하는 과정을 실행하는 것을 특징으로 하며,

[26] 상기 새로운 소유자 등록 메시지(New_Od)는, 디바이스의 고유식별값과 검증키, 이전받은 디바이스가 연결된 네트워크 맥 주소를 포함하며, 디바이스의 서명키로 1차 암호화하고 다시 새로운 사용자의 서명키로 2차 암호화하여 다중 암호화된 메시지인 것이 바람직하다.

발명의 효과

[27] 전술한 본 발명에 따른 디바이스 분산 인증 방법에 있어서, 디바이스에 대한 인증은 분산 저장된 내역을 기반으로 하여 블록체인 네트워크에 있는 노드들에 의해 다중 서명을 검증받고 합의를 통해 이루어진다. 이는 블록체인의 과반수(51%이상) 이상의 노드가 공격을 당하지 않는 한 인증체계는 안전하다는 것을 증명한다. 인증 기관의 실패의 확률로 보게 된다면 기존의 단일 CA기관에 의한 인증 체계보다 안전하다고 할 수 있다.

[28] 또한, 본 발명의 디바이스 분산 인증 방법에 따라 디바이스가 네트워크에 참여를 하기 위해서는, 제조사 서명키 검증, 서비스 플랫폼 서명키 검증, 소유자 서명키 검증의 이력들이 분산 저장되어야 하며 이러한 분산 저장은 합의 알고리즘에 의한 합의에 의해 이루어져야 한다. 따라서, 비허가로 제조되어

위조된 디바이스나, 위변조된 인증 정보를 갖는 디바이스들은 각 단계별로의 서명검증과 디바이스에 이력 데이터를 위조할 수 없기 때문에 네트워크에 참여할 수 없게 된다.

[29] 또한, 본 발명의 디바이스 분산 인증 방법의 인증 프로토콜은 디바이스에 대한 사용 등록 정보 중 네트워크 맥주소를 등록해야 된다. 따라서, 악의적인 사용자가 디바이스를 물리적으로 탈취하더라도, 블록체인 네트워크내에 이미 분산 저장되어 있는 디바이스에 대한 네트워크 맥주소를 위변조하지 않는 한, 악의적인 사용자는 디바이스를 다른 곳에서 사용할 수 없으며 실제로 블록체인 네트워크에 분산 저장된 네트워크 맥주소의 위변조는 불가능하다. 따라서, 본 발명에 따른 디바이스 분산 인증 방법은 악의적인 사용자에 의한 기기 탈취에 대한 공격을 방지할 수 있게 된다.

[30] 또한, 본 발명의 디바이스 분산 인증 방법에 있어서, 디바이스의 소유권을 증명하거나 소유권 이전을 하기 위하여 안전 채널을 통해 디바이스의 서명키를 이전받고, 디바이스의 서명키와 소유자의 서명키로 다중 서명을 하고, 분산 저장된 내역을 기반으로 검증을 받고 합의 알고리즘에 의한 합의를 이루어야 한다. 따라서, 사용자의 소유권을 탈취하기 위해서는 블록체인 네트워크내에 분산 저장된 내역들을 위변조하고 디바이스의 서명키와 소유자의 서명키가 필요하지만, 본 발명에 따른 인증 방법은 실제로 블록체인 네트워크에 분산 저장된 내역들의 위변조가 불가능하고 디바이스의 서명키와 소유자의 서명키를 알 수 없기 때문에 소유권의 탈취가 불가능하다.

[31] 또한, 본 발명의 디바이스 분산 인증 방법에 있어서, 해당 디바이스에 대한 접근을 하기 위해서는 디바이스 등록 정보를 소유자의 서명키와 디바이스의 서명키로 다중 서명을 하고, 분산 저장된 내역을 기반으로 검증을 받고 합의를 통해 디바이스 접근 토근을 받아야만 한다. 따라서, 만약 악의적인 사용자가 디바이스에 대한 접근을 하고자 하는 경우, 블록체인 네트워크내에 분산 저장된 내역들을 위변조 하고 디바이스의 서명키와 소유자의 서명키를 탈취를 해야 된다. 하지만, 본 발명에 따른 인증 방법은 이러한 블록체인 네트워크의 분산 저장된 내역의 위변조와 서명키들의 탈취가 불가능하므로, 소유자가 아닌 사용자는 디바이스에 접근할 수 없게 된다.

[32] 이와 같이, 본 발명에 따른 사물인터넷 블록체인 환경에서의 분산 인증 방법은 종래의 중앙 집중형 사물인터넷에서의 인증 문제를 해결할 수 있게 된다.

도면의 간단한 설명

[33] 도 1은 본 발명의 바람직한 실시예에 따른 디바이스 분산 인증 방법을 구현한 디바이스 분산 인증 시스템을 도시한 블록도이다.

[34] 도 2는 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 분산 인증 프로토콜을 설명하기 위하여 사용되는 기호들에 대한 정의를 설명하는 도표이다.

[35] 도 3은 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 인증 프리비저닝 모듈에 의해 구현되는 인증 프리비저닝 프로토콜을 예시적으로 도시한 코드이다.

[36] 도 4는 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 등록 모듈에 의해 구현되는 디바이스 등록 프로토콜을 예시적으로 도시한 코드이다.

[37] 도 5는 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 이전 모듈에 의해 구현되는 디바이스 이전 프로토콜을 예시적으로 도시한 코드이다.

[38] 도 6은 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 소유자 등록 모듈에 의해 구현되는 디바이스 소유자 등록 프로토콜을 예시적으로 도시한 코드이다.

[39] 도 7은 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 접근 제어 모듈에 의해 구현되는 사용자에 대한 디바이스 접근 제어 프로토콜을 예시적으로 도시한 코드이다.

[40] 도 8은 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 인증 모듈에 의해 구현되는 디바이스 인증 프로토콜을 예시적으로 도시한 코드이다.

[41] 도 9는 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 소유권 이전 모듈에 의해 구현되는 디바이스 소유권 이전 프로토콜을 예시적으로 도시한 코드이다.

발명의 실시를 위한 최선의 형태

[42] 본 발명에 따른 디바이스 분산 인증 시스템은 사물인터넷 블록체인 환경에서 인증을 위해 각 단계별로 디바이스에 대한 정보 및 내역들을 블록체인 합의를 통해 각 노드가 분산 해쉬 테이블(Distributed Hash Table; 'DHT')에 저장하고, 사용자에 대한 접근 제어나 디바이스에 대한 인증은 블록체인 네트워크에 요청하며 각 노드들이 저장된 내역 기반으로 합의하여 승인을 하며, 제조사, 서비스 제공자, 사용자 등이 전파하는 메시지는 다중 암호화한다. 따라서, 본 발명에 따른 디바이스 분산 인증 시스템은 인증 정보의 위변조나 위조된 디바이스의 참여가 불가능하고, 기기의 탈취에 의한 공격을 방지할 수 있으며, 사용자의 소유권 탈취를 방지할 수 있으며, 악의적인 사용자가 디바이스에 접근하는 것을 방지할 수 있게 된다.

[43] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 따른 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 방법 및 이를 이용하여 구현된 디바이스 분산 인증 시스템에 대하여 구체적으로 설명한다.

[44] 도 1은 본 발명의 바람직한 실시예에 따른 디바이스 분산 인증 방법을 구현한 디바이스 분산 인증 시스템을 도시한 블록도이다.

[45] 도 1을 참조하면, 본 발명에 따른 디바이스 분산 인증 시스템(1)은, 디바이스 제조사, 디바이스, 소유자, IoT 플랫폼을 제공하는 서비스 제공자를 포함하는 참여자들이 노드로서 블록체인 네트워크(PIBN)를 형성하고, 디바이스들은 사물

인터넷을 형성하는 기기로서, 전체적으로 사물 인터넷 블록체인 환경을 이루게 된다. 전술한 본 발명에 따른 디바이스 분산 인증 시스템의 각 노드는, 인증 프리비저닝 모듈(100), 디바이스 등록 모듈(110), 디바이스 이전 모듈(120), 디바이스 소유자 등록 모듈(130), 디바이스 접근 제어 모듈(140), 디바이스 인증 모듈(150), 디바이스 소유자 이전 모듈(160)을 구비한다.

[46] 도 2는 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 분산 인증 프로토콜을 설명하기 위하여 사용되는 기호들에 대한 정의를 설명하는 도표이다.

[47] 상기 인증 프리비저닝(Authentication Privisioning) 모듈(100)은, 네트워크의 참여자들이 ECDSA(2561kl kurve) 알고리즘을 이용하여 각자의 키쌍인 서명키와 검증키를 생성하고, 고유 식별값과 함께 블록체인 네트워크에 등록한다. 인증 프리비저닝 모듈은 디바이스에 대한 각 내역들을 서명으로 검증하며 분산 합의를 위한 프리비저닝이다. 도 3은 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 인증 프리비저닝 프로토콜을 예시적으로 도시한 코드이다.

[48] 상기 디바이스 등록 모듈(110)은 제조사가 디바이스를 생성하여 사물인터넷 블록체인 네트워크에 등록하는 모듈이다. 상기 디바이스 등록 모듈은, 제조사가 디바이스의 고유 식별값(UUID) 및 서명키와 검증키를 생성하고, 디바이스의 메시지(md)를 생성한 후 PIBN에 전파하는 과정을 실행한다. 상기 디바이스 메시지(md)는 디바이스의 고유 식별값(UUID)와 디바이스의 서명키를 포함하며 제조사의 서명키로 서명한 메시지로서, 블록체인 네트워크에 전파된 후 각 노드들에 의하여 올바른 제조사로부터 제조된 디바이스인지 여부를 검증하기 위한 메시지이다.

[49] 또한, 상기 디바이스 등록 모듈은, 상기 네트워크의 참여 노드들이 상기 전파받은 디바이스 메시지를 사전 등록된 제조사의 검증키로 검증하여 유효하면, 사전 설정된 합의 알고리즘으로 메시지 내용에 대한 합의를 진행하고, 합의되면 분산 해쉬 테이블(DHT)에 저장하는 과정을 실행한다. 도 4는 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 등록 프로토콜을 예시적으로 도시한 코드이다.

[50] 상기 디바이스 이전 모듈(120)은, 상기 제조사에 의해 등록된 디바이스를 서비스 제공자에게 이전하는 모듈이다. 상기 디바이스 이전 모듈은, 서비스 제공자가 제조사로부터 안전 채널(Secure channel)을 통해 디바이스에 대한 서명키를 이전받고, 서비스 제공자가 기기 이전 등록을 위한 디바이스 이전 등록 메시지(Sd)를 생성하여 PIBN 네트워크에 전파하는 과정을 실행한다. 상기 서비스 제공자에 의한 기기 이전 등록 메시지(Sd)는 디바이스의 고유 식별값(UUID)과 검증키를 포함하며 상기 이전받은 디바이스의 서명키로 1차 암호화하고 다시 서비스 제공자의 서명키로 2차 암호화하여 다중 암호화한 메시지로서, 다중 암호화를 통해, 올바른 서비스 제공자에 대한 검증과 디바이스의 서명키의 검증을 통해 디바이스 이전을 검증을 하기 위한

메시지이다.

[51] 또한, 상기 디바이스 이전 모듈은, 네트워크의 참여 노드들이 상기 전파받은 기기 이전 등록 메시지를 서비스 제공자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 DHT에 저장하는 과정을 실행한다. 도 5는 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 이전 프로토콜을 예시적으로 도시한 코드이다.

[52] 상기 디바이스 소유자 등록 모듈(130)은 사용자가 소유자로서 서비스 제공자로부터 상기 디바이스를 이전받고 소유자로 등록하는 모듈이다. 상기 디바이스 소유자 등록 모듈은, 사용자가 소유자로서 서비스 제공자로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 소유자 등록 메시지(Od)를 생성한 후 PIBN 네트워크에 전파하는 과정을 실행한다. 상기 소유자 등록 메시지(Od)는 디바이스의 고유 식별값과 검증키, 디바이스가 연결된 네트워크 맥 주소를 포함하며, 디바이스의 서명키로 1차 암호화하고 다시 소유자의 서명키로 2차 암호화하여 다중 암호화한 메시지이다.

[53] 또한, 상기 디바이스 소유자 등록 모듈은, 네트워크의 참여 노드들이 상기 전파받은 메시지를 소유자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 DHT에 저장하는 과정을 실행한다. 도 6은 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 소유자 등록 프로토콜을 예시적으로 도시한 코드이다.

[54] 상기 디바이스 접근 제어 모듈(140)은 서비스 제공자로부터 디바이스를 이전받은 소유자에게 디바이스에 대한 접근 제어를 하는 모듈이다. 상기 디바이스 접근 제어 모듈은, 소유자가 소유자 등록 메시지(Od)를 포함하는 디바이스 접근 제어 요청 메시지(DAC)를 생성하여 PIBN 네트워크에 전파하는 과정을 실행한다. 상기 소유자 등록 메시지(Od)는 디바이스의 고유 식별값과 검증키, 디바이스가 연결된 네트워크 맥 주소를 포함하며 디바이스의 서명키로 1차 암호화하고 다시 소유자의 서명키로 2차 암호화하여 다중 암호화한 메시지이다.

[55] 또한, 상기 디바이스 접근 제어 모듈은, 네트워크의 참여 노드들이 상기 전파받은 메시지를 사용자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 노드들중 하나가 소유자에게 디바이스에 대한 접근 토큰을 전달하는 과정을 실행한다. 도 7은 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 사용자에 대한 디바이스 접근 제어 프로토콜을 예시적으로 도시한 코드이다.

[56] 상기 디바이스 인증 모듈(150)은, 디바이스가 디바이스에 대한 고유 식별값(UUID) 및 디바이스가 연결된 네트워크 맥 주소를 디바이스의 서명키로

서명한 디바이스 인증 요청 메시지(DA)를 생성한 후 PIBN 네트워크에 전파하는 과정을 실행하고, 네트워크의 참여 노드들은 전파받은 디바이스 인증 요청 메시지를 디바이스의 검증키로 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 노드들 중 하나가 인증 토큰을 전달하는 과정을 실행한다. 도 8은 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 인증 프로토콜을 예시적으로 도시한 코드이다.

[57] 상기 디바이스 소유권 이전 모듈(160)은 기기 소유자가 디바이스를 새로운 기기 소유자에게 이전하는 모듈이다. 상기 디바이스 소유권 이전 모듈은, 새로운 기기 소유자가 이전 기기 소유자로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받는 과정을 실행하고, 새로운 소유자 등록 메시지(New_Od)를 생성하여 PIBN 네트워크에 전파하는 과정을 실행한다. 상기 새로운 소유자 등록 메시지(New_Od)는 디바이스의 고유 식별값과 검증키, 이전받은 디바이스가 연결된 네트워크 맥 주소를 포함하며, 디바이스의 서명키로 1차 암호화하고 다시 새로운 소유자의 서명키로 2차 암호화하여 다중 암호화된 메시지이다.

[58] 또한, 상기 디바이스 소유권 이전 모듈은, 네트워크의 참여 노드들이 상기 전파받은 새로운 소유자 등록 메시지를 새로운 기기 소유자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 DHT에 저장하는 과정을 실행한다. 도 9는 본 발명에 따른 디바이스 분산 인증 시스템에 있어서, 디바이스 소유권 이전 프로토콜을 예시적으로 도시한 코드이다.

[59] 본 발명에 따른 디바이스 분산 인증 방법은 전술한 본 발명에 따른 디바이스 분산 인증 시스템을 구성하는 각 모듈들에 의해 구현되는 것으로서, 인증 프리비저닝 단계, 제조사로부터의 디바이스 등록 단계, 서비스 제공자로의 디바이스 이전 단계, 디바이스 소유자 등록 단계, 디바이스 접근 제어 단계, 디바이스 인증 단계, 디바이스 소유권 이전 단계를 구비하며, 이들은 각각 전술한 인증 프리비저닝 모듈, 디바이스 등록 모듈, 디바이스 이전 모듈, 디바이스 소유자 등록 모듈, 디바이스 접근 제어 모듈, 디바이스 인증 모듈, 디바이스 소유권 이전 모듈과 동일하게 수행된다.

[60] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나, 이는 단지 예시일 뿐 본 발명을 한정하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 그리고, 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어야 할 것이다.

[61]

[62]

청구범위

[청구항 1] 디바이스 제조사, 디바이스, 소유자, 서비스 제공자를 포함하는 참여자들이 블록체인 네트워크(PIBN)를 형성하는 사물 인터넷 블록체인 환경에서의 디바이스 분산 인증 시스템은,
상기 블록체인 네트워크의 참여자들의 각각에 대한 서명키와 검증키를 생성하고, 고유 식별값과 함께 블록체인 네트워크에 등록하는 인증 프리비저닝 모듈; 및
제조사에 의해 생성된 디바이스를 등록하는 디바이스 등록 모듈;
를 구비하고, 상기 디바이스 등록 모듈은,
제조사가 디바이스의 고유 식별값(UUID) 및 서명키와 검증키를 생성하고, 디바이스 등록 메시지(Md)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하고,
네트워크의 참여 노드들이 전파된 디바이스 등록 메시지를 사전 등록된 제조사의 검증키로 검증하여 유효하면, 사전 설정된 합의 알고리즘으로 메시지 내용에 대한 합의를 진행하고, 합의되면 분산 해쉬 테이블(DHT)에 저장하는 과정을 실행하는 것을 특징으로 하며,
상기 디바이스 등록 메시지(Md)는 디바이스의 고유 식별값과 검증키를 포함하며 디바이스의 서명키로 서명되어 생성된 메시지인 것을 특징으로 하는 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 시스템.

[청구항 2] 제1항에 있어서, 상기 디바이스 분산 인증 시스템은,
상기 제조사에 의해 등록된 디바이스를 서비스 제공자에게 이전하는 디바이스 이전 모듈을 더 구비하고,
상기 디바이스 이전 모듈은,
서비스 제공자가 제조사로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 기기 이전 등록 메시지(Sd)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하며,
네트워크의 참여 노드들이 전파받은 기기 이전 등록 메시지를 서비스 제공자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 DHT에 저장하는 과정을 실행하는 것을 특징으로 하며,
상기 기기 이전 등록 메시지(Sd)는 디바이스의 고유 식별값과 검증키를 포함하며, 디바이스의 서명키로 1차 암호화하고 다시 서비스 제공자의 서명키로 2차 암호화하여 다중 암호화된 메시지인 것을 특징으로 하는 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 시스템.

[청구항 3] 제1항에 있어서, 상기 디바이스 분산 인증 시스템은,
소유자가 서비스 제공자로부터 상기 디바이스를 이전받는 소유자 등록

모듈을 더 구비하고,
상기 소유자 등록 모듈은,
소유자가 서비스 제공자로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 소유자 등록 메시지(Od)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하고,
네트워크의 참여 노드들이 상기 전파받은 소유자 등록 메시지를 소유자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 DHT에 저장하는 과정을 실행하는 것을 특징으로 하며,
상기 소유자 등록 메시지(Od)는 디바이스의 고유 식별값과 검증키, 상기 디바이스가 연결된 네트워크 맥 주소를 포함하며 디바이스의 서명키로 1차 암호화하고 다시 소유자의 서명키로 2차 암호화하여 다중 암호화된 메시지인 것을 특징으로 하는 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 시스템.

[청구항 4] 제1항에 있어서, 상기 디바이스 분산 인증 시스템은,
서비스 제공자로부터 디바이스를 이전받은 소유자에게 디바이스에 대한 접근 제어를 하는 디바이스 접근 제어 모듈을 더 구비하고,
상기 디바이스 접근 제어 모듈은,
소유자가 소유자 등록 메시지(Od)를 생성하고, 소유자 등록 메시지를 포함하는 디바이스 접근 제어 요청 메시지(DAC)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하고,
네트워크의 참여 노드들이 상기 전파받은 디바이스 접근 제어 요청 메시지를 사용자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 소유자에게 디바이스에 대한 접근 토큰을 전달하는 과정을 실행하는 것을 특징으로 하며,
상기 소유자 등록 메시지(Od)는 디바이스의 고유 식별값과 검증키, 디바이스가 연결된 네트워크 맥 주소를 포함하며, 디바이스의 서명키로 1차 암호화시키고 다시 소유자의 서명키로 2차 암호화하여 다중 암호화한 메시지인 것을 특징으로 하는 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 시스템.

[청구항 5] 제1항에 있어서, 상기 디바이스 분산 인증 시스템은 디바이스 인증 모듈을 더 구비하고,
상기 디바이스 인증 모듈은,
디바이스가 디바이스에 대한 고유 식별값(UUID) 및 연결된 네트워크 맥 주소를 디바이스의 서명키로 서명한 인증 요청 메시지(DA)를 생성한 후 PIBN 네트워크에 전파하는 과정을 실행하고;

네트워크의 참여 노드들이 전파받은 인증 요청 메시지를 디바이스의 검증키로 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 인증 토큰을 전달하는 과정을 실행하는 것을 특징으로 하는 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 시스템.

[청구항 6] 제1항에 있어서, 상기 디바이스 분산 인증 시스템은,
기기 소유자가 디바이스를 새로운 기기 소유자에게 이전하는 디바이스 소유권 이전 모듈을 더 구비하고,
상기 디바이스 소유권 이전 모듈은,
새로운 기기 소유자가 이전 기기 소유자로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 새로운 소유자 등록 메시지(New_Od)를 생성하여 블록체인 네트워크에 전파하는 과정을 실행하고,
네트워크의 참여 노드들이 전파받은 소유권 이전 요청 메시지를 새로운 기기 소유자의 검증키로 1차 복호화하고 다시 디바이스의 검증키로 2차 복호화하여 유효하면, 합의 알고리즘을 통해 내용에 대한 합의를 진행하고, 합의되면 각 노드들은 DHT에 저장하는 과정을 실행하는 것을 특징으로 하며,
상기 새로운 소유자 등록 메시지(New_Od)는, 디바이스의 고유식별값과 검증키, 이전받은 디바이스가 연결된 네트워크 맥 주소를 포함하며,
디바이스의 서명키로 1차 암호화하고 다시 새로운 사용자의 서명키로 2차 암호화하여 다중 암호화된 메시지인 것을 특징으로 하는 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 시스템.

[청구항 7] 디바이스 제조사, 디바이스, 소유자, 서비스 제공자를 포함하는 참여자들이 블록체인 네트워크(PIBN)를 형성하는 사물 인터넷 블록체인 환경에서의 디바이스 분산 인증 방법은,
상기 블록체인 네트워크의 참여자들의 각각에 대한 서명키와 검증키를 생성하고, 고유 식별값과 함께 블록체인 네트워크에 등록하는 인증 프리비저닝 단계; 및
제조사에 의해 생성된 디바이스를 등록하는 디바이스 등록 단계;
를 구비하고, 상기 디바이스 등록 단계는,
제조사가 디바이스의 고유 식별값(UUID) 및 서명키와 검증키를 생성하고, 디바이스 등록 메시지(Md)를 생성하여 블록체인 네트워크에 전파하는 단계; 및
네트워크의 참여 노드들이 전파된 디바이스 등록 메시지를 사전 등록된 제조사의 검증키로 검증하여 유효하면, 사전 설정된 합의 알고리즘으로 메시지 내용에 대한 합의를 진행하고, 합의되면 분산 해쉬 테이블(DHT)에 저장하는 단계;를 구비하는 것을 특징으로 하며,

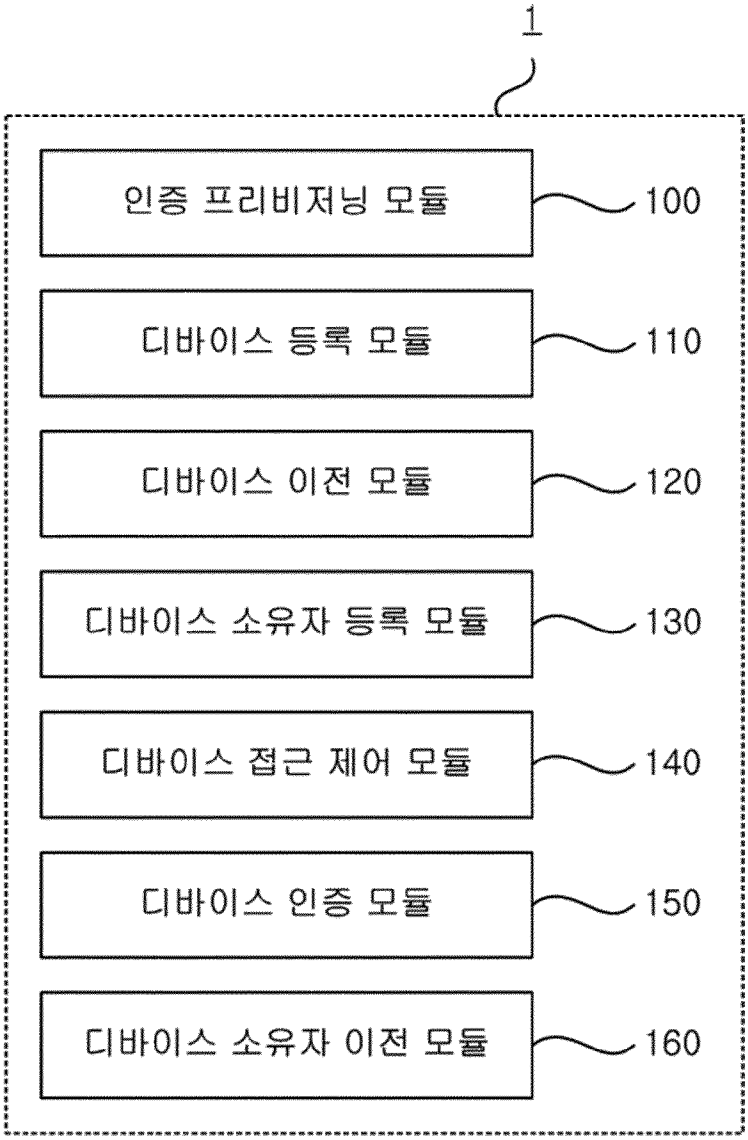
상기 디바이스 등록 메시지(Md)는 디바이스의 고유 식별값과 검증키를 포함하며 디바이스의 서명키로 서명되어 생성된 메시지인 것을 특징으로 하는 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 방법.

[청구항 8] 제7항에 있어서, 상기 디바이스 분산 인증 방법은,
서비스 제공자가 제조사로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 기기 이전 등록 메시지(Sd)를 생성하여 블록체인 네트워크에 전파하여, 상기 제조사에 의해 등록된 디바이스를 서비스 제공자에게 이전하는 디바이스 이전 단계;
소유자가 서비스 제공자로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 소유자 등록 메시지(Od)를 생성하여 블록체인 네트워크에 전파하여, 소유자가 서비스 제공자로부터 상기 디바이스를 이전받는 소유자 등록 단계; 및
새로운 기기 소유자가 이전 기기 소유자로부터 안전 채널을 통해 디바이스에 대한 서명키를 이전받고, 새로운 소유자 등록 메시지(New_Od)를 생성하여 블록체인 네트워크에 전파하여, 기기 소유자가 디바이스를 새로운 기기 소유자에게 이전하는 디바이스 소유권 이전 단계;
를 더 구비하는 것을 특징으로 하는 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 방법.

[청구항 9] 제7항에 있어서, 상기 디바이스 분산 인증 방법은,
소유자가 소유자 등록 메시지(Od)를 생성하고, 소유자 등록 메시지를 포함하는 디바이스 접근 제어 요청 메시지(DAC)를 생성하여 블록체인 네트워크에 전파하여, 서비스 제공자로부터 디바이스를 이전받은 소유자에게 디바이스에 대한 접근 제어를 하는 디바이스 접근 제어 단계; 및
디바이스가 디바이스에 대한 고유 식별값(UUID) 및 연결된 네트워크 맥 주소를 디바이스의 서명키로 서명한 인증 요청 메시지(DA)를 생성한 후 PIBN 네트워크에 전파하는 디바이스 인증 단계;
를 더 구비하는 것을 특징으로 하는 사물인터넷 블록체인 환경에서의 디바이스 분산 인증 방법.

WO 2020/138525 PCT/KR2018/016652

[도1]



[도2]

Notation	Description
$(G_{sig}, S_{sig}, v_{sig})$	Digital signature schems DSS described by the 3-tuple generator, signature, verification
PIBN	Private internet of thigns block chain network
DAC	Device access control
Pk^{n}_{sig} , Sk^{n}_{sig}	n's verify key , signing key
D_A	Device authentication message
o , new o	owner, New owner
s, s_d	Service Provider Device message of service provider
m, m_d	Device manufacturer Device message of manufacturer
$Info_n$	n's information for registered in the block-chain network

[도3]

PROTOCOL 1 Authentication Privisioing

1: **procedure** AuthenticationPrivisioning
2: o executes :
3: $(Pk^{O}_{sig}, , Sk^{O}_{sig})$ <- $G_{sig}()$
4: o participate in PIBN
5: $Info_o(Pk^{O}_{sig}, Id_o)$ enrollment in PIBN
6: s executes :
7: $(Pk^{s}_{sig}, , Sk^{s}_{sig})$ <- $G_{sig}()$
8: s participate in PIBN
9: $Info_S(Pk^{s}_{sig}, , Id_S)$ enrollment in PIBN
10: m executes:
11: $(Pk^{m}_{sig}, , Sk^{m}_{sig})$ <- $G_{sig}()$
12: m participate in PIBN
13: $Info_m(Pk^{m}_{sig}, , Id_m)$ enrollment in PIBN
14: **end procedure**

[도4]

PROTOCOL 2 Device Generation from manufacturer

1: **procedure** DeviceGeneration()
2: m excutes:
3: generate d with uuid
4: $(Pk^{d}_{sig,}, Sk^{d}_{sig}) \leftarrow G_{sig}()$
5: $m_d = (uuid, Pk^{d}_{sig}) \leftarrow S_{sig}(Sk^{m}_{sig})$ broadcast to PIBN
6: PIBN excutes:
7: **if** $m_d \leftarrow V_{sig}(Pk^{m}_{sig})$ is vaild :
8: **then** execute consensus rule :
9: insert m_d in DHT
10: **end procedure**

[도5]

PROTOCOL 3 Device transfer to service provider

1: **procedure**
2: s and m form a secure channel
3: transfer Sk^{d}_{sig} to s
4: s execute :
5: $s_d = \{(uuid, Pk^{d}_{sig}) \leftarrow S_{sig}(Sk^{d}_{sig})\} \leftarrow S_{sig}(Sk^{s}_{sig})$ broadcast to PIBN
6: PIBN excutes:
7: If $s_d \leftarrow V_{sig}(Pk^{s}_{sig}) \leftarrow V_{sig}(Pk^{d}_{sig})$ is valid:
8: **then** execute consensus rule :
9: insert s_d in DHT
10: **end procedure**

[도6]

PROTOCOL 4 Device owner registration

1: **procedure**
2: o and s form a secure channel
3: transfer Sk^{d}_{sig} to o
4: o execute :
5: o_d = {(uuid, Pk^{d}_{sig} ,Network mac address) <-S_{sig} (Sk^{d}_{sig}) } <- S_{sig} (Sk^{o}_{sig}) and broadcast to PIBN
6: PIBN excutes:
7: **If** o_d <- V_{sig} (Pk^{o}_{sig}) <- V_{sig} (Pk^{d}_{sig}) is valid:
8: **then** execute consensus rule **:**
9: insert o_d in DHT
10: **end procedure**

[도7]

PROTOCOL 5 Device access control

1: procedure
2: o execute :
3: o_d = {(uuid, Pk^{d}_{sig} ,Network mac address) <-S_{sig} (Sk^{d}_{sig}) } <- S_{sig} (Sk^{o}_{sig})
4: request DAC(o_d) to PIBN
5: PIBN execute:
6: if o_d <- V_{sig} (Pk^{o}_{sig}) <- V_{sig} (Pk^{d}_{sig}) is valid
7: then execute consensus rule :
8: return DAC token -
9: end procedure

[도8]

PROTOCOL 6 device authentication

1: procedure
2: d execute :
3: D_A = (uuid, Network mac address) <- S_{sig} (Sk^d_{sig})
4: request D_A to PIBN
5: PIBN execute:
6: if D_A <- V_{sig} (Pk^d_{sig}) is valid :
8: then execute consensus rule :
9: return authentication token
10:end procedure

[도9]

PROTOCOL 7 device transfer to other owner

1: procedure
2: o and new o form a secure channel
3: transfer Sk^d_{sig} to new o
4: new o execute :
5: new o_d = {(uuid, Pk^d_{sig} ,Network mac address) <- S_{sig} (Sk^d_{sig}) } <- S_{sig} ($Sk^{new\ o}_{sig}$)
6: and broadcast to PIBN
7: PIBN excutes:
8: If new o_d <- V_{sig} (Pk^o_{sig}) <- V_{sig} (Pk^d_{sig}) is valid:
9: **then** execute consensus rule :
10: insert new o_d in DHT

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2018/016652

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i, H04L 29/08(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)

H04L 29/06; H04L 12/28; H04L 9/06; H04L 9/08; H04L 9/32; H04L 29/08

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: internet of things, blockchain, device registration, verify key, signing key, unique ID, verify, consensus, distributed hash table

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2018-0183587 A1 (VMWARE, INC.) 28 June 2018 See paragraphs [0017]-[0045], [0073]-[0079]; claims 1, 6; and figures 1-2, 6.	1-9
A	US 2018-0254898 A1 (RIVETZ CORP.) 06 September 2018 See paragraphs [0052]-[0100]; and figures 2A-3A.	1-9
A	WO 2017-207314 A1 (GEMALTO SA.) 07 December 2017 See pages 13-18; and figures 4-7.	1-9
A	US 2018-0359095 A1 (CISCO TECHNOLOGY, INC.) 13 December 2018 See paragraphs [0026]-[0033]; and figure 2.	1-9
A	US 2017-0300901 A1 (PAYPAL, INC.) 19 October 2017 See paragraphs [0025]-[0027]; and figure 4.	1-9

☐ 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
19 SEPTEMBER 2019 (19.09.2019)	**20 SEPTEMBER 2019 (20.09.2019)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea Facsimile No. +82-42-481-8578	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2018/016652

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2018-0183587 A1	28/06/2018	None	
US 2018-0254898 A1	06/09/2018	WO 2018-164955 A1	13/09/2018
WO 2017-207314 A1	07/12/2017	CN 109196841 A	11/01/2019
		EP 3253020 A1	06/12/2017
		EP 3466020 A1	10/04/2019
		JP 2019-520752 A	18/07/2019
		KR 10-2019-0002598 A	08/01/2019
		US 2019-0124512 A1	25/04/2019
US 2018-0359095 A1	13/12/2018	None	
US 2017-0300901 A1	19/10/2017	US 2017-0300912 A1	19/10/2017
		US 2017-0300978 A1	19/10/2017

국 제 조 사 보 고 서

국제출원번호
PCT/KR2018/016652

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/06(2006.01)i, H04L 29/08(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 29/06; H04L 12/28; H04L 9/06; H04L 9/08; H04L 9/32; H04L 29/08

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:Internet Of Things, blockchain, device registration, verify key, signing key, unique ID, verify, consensus, distributed hash table

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 2018-0183587 A1 (VMWARE, INC.) 2018.06.28 단락 [0017]-[0045], [0073]-[0079]; 청구항 1, 6; 및 도면 1-2, 6 참조.	1-9
A	US 2018-0254898 A1 (RIVETZ CORP.) 2018.09.06 단락 [0052]-[0100]; 및 도면 2A-3A 참조.	1-9
A	WO 2017-207314 A1 (GEMALTO SA) 2017.12.07 페이지 13-18; 및 도면 4-7 참조.	1-9
A	US 2018-0359095 A1 (CISCO TECHNOLOGY, INC.) 2018.12.13 단락 [0026]-[0033]; 및 도면 2 참조.	1-9
A	US 2017-0300901 A1 (PAYPAL, INC.) 2017.10.19 단락 [0025]-[0027]; 및 도면 4 참조.	1-9

☐ 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
2019년 09월 19일 (19.09.2019)	2019년 09월 20일 (20.09.2019)

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

심사관
진상범
전화번호 +82-42-481-8398

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2018/016652

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2018-0183587 A1	2018/06/28	없음	
US 2018-0254898 A1	2018/09/06	WO 2018-164955 A1	2018/09/13
WO 2017-207314 A1	2017/12/07	CN 109196841 A	2019/01/11
		EP 3253020 A1	2017/12/06
		EP 3466020 A1	2019/04/10
		JP 2019-520752 A	2019/07/18
		KR 10-2019-0002598 A	2019/01/08
		US 2019-0124512 A1	2019/04/25
US 2018-0359095 A1	2018/12/13	없음	
US 2017-0300901 A1	2017/10/19	US 2017-0300912 A1	2017/10/19
		US 2017-0300978 A1	2017/10/19