(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2019 년 8 월 29 일 (29.08.2019)

WIPO | PCT

(10) 국제공개번호
WO 2019/164260 A1

(51) 국제특허분류:
H04L 9/08 (2006.01) *H04L 29/12* (2006.01)
H04L 9/32 (2006.01)

(21) 국제출원번호: PCT/KR2019/002065

(22) 국제출원일: 2019 년 2 월 20 일 (20.02.2019)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2018-0021606 2018 년 2 월 23 일 (23.02.2018) KR

(71) 출원인: 에이치닥 테크놀로지 아게 (**HDAC TECHNOLOGY AG**) [CH/CH]; 6300 추크, 슈을리라인 4, Zug (CH).

(72) 발명자: 이재민 (**LEE, Jae Min**); 05813 서울시 송파구 송파대로8길 58 103동 901호, Seoul (KR). 김병철 (**KIM, Byung Chul**); 04180 서울시 마포구 새창로8길 72 206동 1402호, Seoul (KR).

(74) 대리인: 김함곤 (**KIM, Ham-Kon**); 06140 서울시 강남구 논현로 522, 2층, Seoul (KR).

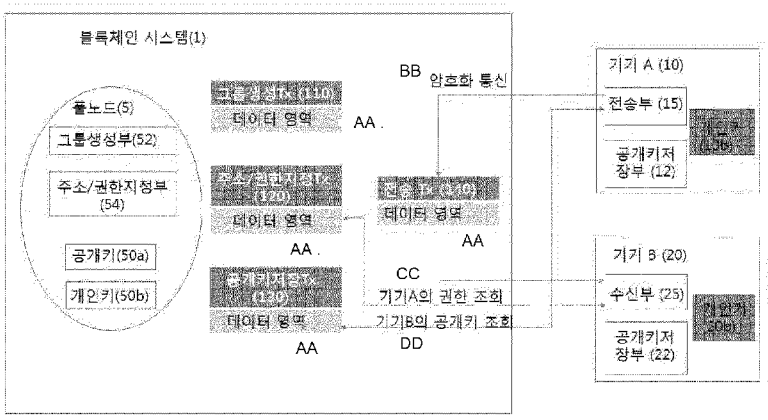
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR,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

WO 2019/164260 A1

(54) **Title:** METHOD AND SYSTEM FOR ENCRYPTED COMMUNICATION BETWEEN DEVICES BY USING BLOCK CHAIN SYSTEM

(54) **발명의 명칭:** 블록체인 시스템을 이용한 기기들간 암호화 통신 방법 및 시스템



1 ... Blockchain system
5 ... Pool node
10 ... Device A
10b, 20b, 50b ... Private key
12 ... Public key storage unit
15 ... Transmission unit
20 ... Device B
22 ... Public key storage unit
25 ... Reception unit
50a ... Public key

52 ... Group generation unit
54 ... Address/authority designation unit
110 ... Group generation Tx
120 ... Address/authority designation Tx
130 ... Public key storage Tx
140 ... Transmission Tx
AA ... Data area
BB ... Encrypted communication
CC ... View authority of device A
DD ... View public key of device B

(57) **Abstract:** The present invention relates to a method and system for encrypted communication between devices belonging to a group having been authenticated on the basis of stability provided by a block chain system. According to the present invention, P2P encrypted communication, encrypted communication between 1 and N, or encrypted communication between N and N is possible on a block chain system, in which all contents are disclosed, whereas an existing block chain enables only fully disclosed information to be shared.

(57) **요약서:** 본 발명은 블록체인 시스템이 제공하는 안정성을 기반으로 하여 인증이 이루어진 그룹에 속하는 기기들간의 암호화 통신 방법 및 시스템에 관한 것으로, 기존의 블록체인이 완전히 공개된 정보만 공유할 수 있음에 비하여, 본 발명에 의하면 모든 내용이 공개되는 블록체인 시스템 상에서 P2P 또는 1:N, N:N 사이의 암호화된 통신을 가능하게 해 준다.

[다음 쪽 계속]

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))

명세서

발명의 명칭: 블록체인 시스템을 이용한 기기들간 암호화 통신 방법 및 시스템

기술분야

[1] 본 발명은 기기들간 암호화 통신 방법 및 시스템에 관한 것으로, 특히 블록체인 시스템이 제공하는 안정성을 기반으로 하여 인증이 이루어진 그룹에 속하는 기기들간의 암호화 통신 방법 및 시스템에 관한 것이다.

배경기술

[2] 블록체인은 P2P 분산 원장(Distributed ledger) 형태의 데이터베이스 구조라 할 수 있다. 일정 크기의 거래 정보(데이터)들이 모여 블록이 형성되고, 이러한 블록들이 시간의 흐름상 순차적으로 체인으로 연결된 구조이다. 블록체인 형성을 위해서는 네트워크 참여자들의 거래 내역 검증과 승인 과정이 요구되고, 각 블록들은 바로 이전 블록의 존재를 정교하게 참조하고 있어 블록 순서를 바꾼다거나 블록 내 정보를 조작하는 것은 사실상 불가능하다. 이는 거래 관계에서 서로를 신뢰하지 못해 발생하는 비효율을 제거하는 결정적인 역할을 한다.

[3] 블록체인이 가져올 변화의 본질은 '거래 승인 권한과 정보의 민주화(Democratization)'로 요약할 수 있다. 이는 강력한 제3의 공인기관이나 중개자의 개입 없이 투명하고 안전한 직접 거래를 가능하게 한다. 안전한 시스템에 의한 자율적 권한 위임이 가능하므로 거의 실시간 승인이 가능해지고, 정보는 네트워크 참여자 모두에게 공개ㅇ보관ㅇ관리되므로 특정 거래 정보를 조작하려면 모든 참여자의 컴퓨터를 해킹해서 블록체인 전체를 조작해야 하는 비현실적 작업이 필요하다. 이렇듯 블록체인 기반의 거래 시스템은 신속성, 안전성, 투명성, 비용 절감 등의 사용자 편의를 제고시키는 효과를 가져다 준다.

[4] 그런데, 기존의 블록체인 시스템은 공개된 네트워크로 구성되어 있다. 따라서 블록체인 시스템에 접속된 모든 기기는 블록체인 상의 정보에 접근이 가능하기 때문에, 특정한 기기들 사이에서 기밀성이 보장된 트랜잭션을 만들기가 어렵다. 이에 비하여 기존의 블록체인 망이 아닌 SSL(Secure Socket Layer)을 이용하는 경우, 트랜잭션에 대한 무결성 보장이 달성되기 어렵다.

발명의 상세한 설명

기술적 과제

[5] 본 발명은 블록체인 시스템 상의 기기들 중 상호 인증된 기기들 사이에서만 암호화된 통신이 가능하도록 하는 블록체인 시스템을 이용한 기기들간 암호화 통신 방법 및 시스템을 제공함을 그 목적으로 한다.

과제 해결 수단

[6] 상기의 목적을 달성하기 위하여, 본 발명의 일측면에 의한 블록체인 시스템을

이용한 기기들간 암호화 통신 방법은, 블록체인 시스템에 접속된 기기들 상호간의 통신 방법으로, (a) 블록체인 시스템의 풀노드가 그룹(G)을 생성하는 그룹생성트랜잭션을 생성하는 단계; (b) 상기 풀노드가 상기 그룹(G)에 속하는 기기의 주소와 권한을 지정하는 주소/권한지정트랜잭션을 상기 그룹(G)과 관련하여 생성하는 단계; (c) 상기 그룹(G)에 속하는 기기(A,B)가 자신의 개인키를 사용하여 공개키를 생성하고, 생성된 공개키를 저장하는 공개키저장트랜잭션을 상기 그룹(G)과 관련하여 생성하는 단계; (d) 기기 A가 상기 공개키저장트랜잭션을 참조하여 얻은 기기 B의 공개키로 전송할 정보를 암호화 한 전송트랜잭션을 생성하여 기기 B로 전송하는 단계; 및 (e) 상기 전송트랜잭션을 수신한 기기 B가 기기 A에 할당된 권한을 상기 주소/권한지정트랜잭션을 참조하여 검증하고, 인증되면 상기 전송트랜잭션의 데이터 영역을 기기 B의 개인키로 복호화 하는 단계;를 포함하여 구성된다.

[7] 상기의 블록체인 시스템을 이용한 기기들간 암호화 통신 방법에서, 상기 그룹생성트랜잭션과 상기 주소/권한지정트랜잭션은 상기 풀노드의 개인키로 서명되는 것을 특징으로 한다.

[8] 상기의 블록체인 시스템을 이용한 기기들간 암호화 통신 방법에서, 상기 주소/권한지정트랜잭션에 지정되는 권한에는 상기 그룹(G)에 접근할 수 있는 권한과 기록할 수 있는 권한이 포함됨을 특징으로 한다.

[9] 상기의 목적을 달성하기 위하여, 본 발명의 다른 측면에 의한 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템은, 블록체인 풀노드; 및 상기 풀노드에 접속된 기기 A,B;를 포함하여 구성되고, 상기 풀노드는, 그룹(G)을 생성하는 그룹생성트랜잭션을 생성하는 그룹생성부; 상기 그룹(G)에 속하는 기기의 주소(A,B)와 권한을 지정하는 주소/권한지정트랜잭션을 상기 그룹(G)과 관련하여 생성하는 주소/권한지정부;를 구비하고, 기기 A,B는 각각 자신의 개인키를 사용하여 공개키를 생성하고, 생성된 공개키를 저장하는 공개키저장트랜잭션을 상기 그룹(G)과 관련하여 생성하는 공개키저장부;를 구비하고, 기기 A는 상기 공개키저장트랜잭션을 참조하여 얻은 기기 B의 공개키로 전송할 정보를 암호화 한 전송트랜잭션을 생성하여 기기 B로 전송하는 전송부;를 구비하고, 기기 B는 상기 전송트랜잭션을 수신하고, 기기 A에 할당된 권한을 상기 주소/권한지정트랜잭션을 참조하여 검증하고, 인증되면 상기 전송트랜잭션의 데이터 영역을 기기 B의 개인키로 복호화 하는 수신부;를 구비하는 것을 특징으로 한다.

[10] 상기의 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템에서, 상기 그룹생성트랜잭션과 상기 주소/권한지정트랜잭션은 상기 풀노드의 개인키로 서명되는 것을 특징으로 한다.

[11] 상기의 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템에서, 상기 주소/권한지정트랜잭션에 지정되는 권한에는 상기 그룹(G)에 접근할 수 있는 권한과 기록할 수 있는 권한이 포함됨을 특징으로 한다.

[12] 상기의 목적을 달성하기 위하여, 본 발명의 또 다른 측면에 의한 컴퓨터로 읽을 수 있는 기록 매체는 상기의 블록체인 시스템을 이용한 기기들간 암호화 통신 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한다.

발명의 효과

[13] 기존의 블록체인이 완전히 공개된 정보만 공유할 수 있음에 비하여, 본 발명에 의하면 모든 내용이 공개되는 블록체인 시스템 상에서 P2P 또는 1:N, N:N 사이의 암호화된 통신을 가능하게 해 준다. 또한 특정한 그룹에 속한 주소 사이에서만 암호화된 통신을 가능하게 해 준다.

[14] 예를 들어, 스마트홈에서 (해킹으로 내부 기기를 제어하는 등의) 보안문제가 많이 발생하는데, 본 발명에 의한 블록체인 그룹을 특정 아파트 11동 101호로 만들었다고 가정할 수 있다. 이때, 이 그룹에 속한 가족 구성원들과 월패트, 스마트 기기들이 그룹의 구성요소로 등록될 수 있다. 그러면, 이 그룹의 구성원은 안정하게 기기들을 보안의 안정성이 월등한 블록체인 기반의 인증을 통해서 제어할 수 있고, 옆집이나 다른 사람은 블록체인 상의 이 그룹에 등록되기 전에는 11동 101호의 기기들을 제어할 수가 없게 된다.

도면의 간단한 설명

[15] 도 1은 본 발명에 의한 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템에서 그룹생성트랜잭션과 주소/권한지정트랜잭션을 생성하는 과정을 설명하기 위한 도면이다.

[16] 도 2는 본 발명에 의한 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템에서 공개키저장트랜잭션을 생성하는 과정을 설명하기 위한 도면이다.

[17] 도 3은 본 발명에 의한 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템에서 전송트랜잭션(140)을 생성하는 과정을 설명하기 위한 도면이다.

발명의 실시를 위한 형태

[18] 이하에서 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 설명한다.

[19] 도 1 내지 3에 의하면, 본 발명에 의한 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템의 바람직한 일실시예는 블록체인 시스템(1)의 풀노드(5)와 여기에 연결된 기기들(A(10), B(20))로 구성된다.

[20] 블록체인은 퍼블릭 또는 프라이빗 P2P 네트워크에서 일어나는 트랜잭션의 정보가 네트워크 참여자간 공유된 디지털 원장으로, 네트워크의 모든 구성원 노드(블록체인 노드)에 분산되어있는 원장은 네트워크 피어 간에 이루어지는 자산 교환의 결과 블록 단위로 영구하게 저장된다. 네트워크 참여자에 의해 합의되고 유효성이 확인된 모든 거래의 블록은 체인의 시작 부분(Genesis block)에서부터 가장 최근의 블록으로 연결되어 블록체인이라는 이름으로 불려진다. 블록체인은 완전 무결한 원본데이터의 단일 접근경로로서의 역할을 하며, 블록체인 네트워크(5)의 구성원은 자신과 관련이 있는 트랜잭션만 볼 수 있다.

[21] 따라서 본 발명에 의한 블록체인 노드는 P2P 네트워크 상에서 블록체인 네트워크(3)의 구성원을 형성하는 것으로, 블록체인 시스템(1)은 블록체인 노드들의 집합체로 구성된다.

[22] 블록체인 노드에는 지갑(wallet)이 생성되며, 여기에는 최초의 주소(address)가 생성된다. 블록체인 노드에서 주소는 정보를 저장하거나 조회하거나 트랜잭션을 주고받는 키가 된다. 따라서, 블록체인 노드 상의 모든 정보 교환은 기본적으로 주소를 통해서 이루어진다. 각 블록체인 노드에는 1개 이상의 주소가 존재할 수 있고, 하나의 주소에는 시간별로 저장된 다수의 트랜잭션이 기록될 수 있다. 트랜잭션 ID는 하나의 트랜잭션마다 부여되는 고유의 해쉬값으로, 트랜잭션 ID를 알면 전체 블록체인 정보 중에서 해당하는 정보를 즉시 조회할 수 있다.

[23] 이와 같이 블록체인 노드는 라우팅, 블록체인 데이터베이스, 채굴, 지갑 서비스 등 기능의 집합체인데, 그 중 풀노드(5)는 이들 기능을 모두 가지고 가장 최신의 블록체인 복사본을 가지고 있어 외부의 참조 없이도 거래검증이 가능한 노드이다.

[24] 한편, 기기 A(10)와 기기 B(20)는 블록체인 풀노드(5)에 네트워크(도시되지 않음)를 통해 접속된 기기들로, 그 구체적인 대상은 제한되지 않는다.

[25] 본 발명에 의한 풀노드(5)는 그룹생성부(52)와 주소/권한지정부(54)를 구비하는데, 그룹생성부(52)는 그룹(G)을 생성하는 트랜잭션(그룹생성트랜잭션(110))을 생성하고, 주소/권한지정부(54)는 특정 그룹(G)에 속하는 기기의 주소(A,B)와 권한을 지정하는 트랜잭션(주소/권한지정트랜잭션(120))을 생성한다.

[26] 그룹생성트랜잭션(110)과 주소/권한지정트랜잭션(120)에 대한 상세한 설명은 후술하기로 한다.

[27] 또한, 본 발명에 의한 기기 A(10)에는 공개키저장부(12) 및 전송부(15)를 구비하고, 기기 B(20)에는 공개키저장부(22) 및 수신부(25)를 구비한다.

[28] 공개키저장부(12,22)는 공개키 암호화 방식에 따른 공개키를 생성하고, 생성된 공개키를 저장하는 트랜잭션(공개키저장트랜잭션(130))을 생성한다.

[29] 전송부(15)는 공개키저장트랜잭션(130)을 참조하여 얻은 기기 B(20)의 공개키(20a)로 전송할 정보를 암호화 한 전송트랜잭션(140)을 생성하여 기기 B(20)로 전송한다.

[30] 수신부(25)는 전송트랜잭션(140)을 수신하고, 기기 A(10)에 할당된 권한을 주소/권한지정트랜잭션(120)을 참조하여 검증하고, 인증되면 전송트랜잭션(140)의 데이터 영역을 기기 B(20)의 개인키(20b)로 복호화 한다.

[31] 공개키저장트랜잭션(130)과 전송트랜잭션(140)에 대한 상세한 설명은 후술하기로 한다.

[32] 이하에서, 도 1을 참조하여 본 발명에 의한 그룹생성트랜잭션(110)과 주소/권한지정트랜잭션(120)을 생성하는 과정에 대하여 상세히 설명하기로

한다.

[33] 블록체인 시스템(1)의 최초 서버인 풀노드(5)와 주소 A를 가진 기기 A(10)와 주소 B를 가진 기기 B(20)를 준비한다. 여기서, 주소 A와 주소 B는 각각 기기 A(10)와 B(20)의 ID(식별자)가 된다. 또한, 풀노드(5)의 공개키(5a)는 블록체인 시스템(1) 상에 공개되어 있다.

[34] 먼저, 풀노드(5)는 하나의 그룹(G)을 생성하는 트랜잭션(110)을 만든다. 그룹생성트랜잭션(110)의 데이터 영역에는 그룹(G)과 관련된 정보(예를 들어, 해당 그룹이 공개용인지 특정 사용자만 볼 수 있는 사설용인지에 대한 구분이 포함될 수 있다)가 저장되며, 풀노드(5)의 개인키(5b)로 서명되어 있다. 그룹생성트랜잭션(110)의 데이터 영역의 정보는 풀노드(5)의 개인키(5b)로 서명한 경우에만 유효하게 저장되고, 다른 노드로 확산된다.

[35] 따라서 블록체인 시스템(1) 상의 모든 노드는 그룹생성트랜잭션(110)에 첨부된 풀노드(5)의 공개키(5a)를 이용하여 그룹생성트랜잭션(110)의 데이터 영역에 접근할 수 있고, 그룹(G)가 생성되었다는 것을 알 수 있다.

[36] 이후, 풀노드(5)가 그룹(G)에 속하는 기기의 주소(A,B)와 권한을 지정하는 트랜잭션(주소/권한지정트랜잭션(120))을 생성한다. 이때 주소/권한지정트랜잭션(120)에는 그룹(G)의 ID(식별자)를 포함되어, 어느 그룹에 속하는 트랜잭션인지 알 수 있다.

[37] 주소/권한지정트랜잭션(120)의 데이터 영역에는 기기 A(10)와 기기 B(20)가 그룹(G)에 속한다는 내용이 풀노드(5)의 개인키(5b)로 서명되어 저장된다.

[38] 또한 주소/권한지정트랜잭션(120)의 데이터 영역에는 그룹(G)에 접근(Access)할 수 있는 권한 및 기록(Write)할 수 있는 권한이 풀노드(5)의 개인키(5b)로 서명되어 저장된다.

[39] 따라서 블록체인 시스템(1) 상의 모든 노드는 주소/권한지정트랜잭션(120)에 첨부된 풀노드(5)의 공개키(5a)를 이용하여 주소/권한지정트랜잭션(120)의 데이터 영역에 접근할 수 있고, 기기 A(10)와 기기 B(20)가 같은 그룹(G)에 속한다는 내용을 알 수 있다.

[40] 도 2를 참조하면, 기기 A(10)와 기기 B(20)는 각각 개인키(10b,20b)를 사용하여 공개키(10a,20a)를 생성하고, 생성된 공개키(10a,20a)를 저장하는 공개키저장트랜잭션(130)을 생성한다. 이때 공개키저장트랜잭션(130)에는 그룹(G)의 ID(식별자)를 포함되어, 어느 그룹에 속하는 트랜잭션인지 알 수 있다.

[41] 이하에서, 도 3을 참조하여 본 발명에 의한 전송트랜잭션(140)을 생성하는 과정을 통해 기기들간 암호화 통신이 이루어지는 과정에 대하여 상세히 설명하기로 한다.

[42] 기기 A(10)가 동일한 그룹(G)에 속하는 기기 B(20)에게 암호화된 정보를 전달하고자 하는 경우, 기기 A(10)가 공개키저장트랜잭션(130)을 참조하여 얻은 기기 B(20)의 공개키(20a)로 전송할 정보를 암호화 한 전송트랜잭션(140)을 생성하여 기기 B(20)로 전송한다.

[43] 그러면, 기기 B(20)는 전송트랜잭션(140)을 수신하고, 발송자가 수신자에게 발송이 가능한지 인증을 한다. 발송자 인증은 주소/권한지정트랜잭션(120)의 데이터 영역에 기기 A(10)에 할당된 권한에 기록할 수 있는 권한이 등록되어 있는지를 검증함으로써 확인이 가능하다. 기기 B(20)는 인증이 되면 전송트랜잭션(140)의 데이터 영역을 기기 B(20)의 개인키(20b)로 복호화 하고, 그렇지 않으면 전송된 내용을 무시한다.

[44] 이후, 복호화된 정보는 일반적인 처리 절차에 따라서 순차적으로 처리된다.

[45] 한편, 상술한 본 발명의 실시예는 개인용 컴퓨터를 포함한 범용 컴퓨터에서 사용되는 매체에 기록될 수 있다. 상기 매체는 마그네틱 기록매체(예를 들면, 롬, 플로피 디스크, 하드 디스크 등), 광학적 판독매체(예를 들면, 씨디롬, 디브이디 등) 및 전기적 기록매체(예를 들면, 플레쉬 메모리, 메모리 스틱 등)와 같은 기록매체를 포함한다.

[46] 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예는 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

청구범위

[청구항 1] 블록체인 시스템에 접속된 기기들 상호간의 통신 방법에 있어서,
(a) 블록체인 시스템의 풀노드가 그룹(G)을 생성하는
그룹생성트랜잭션을 생성하는 단계;
(b) 상기 풀노드가 상기 그룹(G)에 속하는 기기의 주소와 권한을 지정하는
주소/권한지정트랜잭션을 상기 그룹(G)과 관련하여 생성하는 단계;
(c) 상기 그룹(G)에 속하는 기기(A,B)가 자신의 개인키를 사용하여
공개키를 생성하고, 생성된 공개키를 저장하는 공개키저장트랜잭션을
상기 그룹(G)과 관련하여 생성하는 단계;
(d) 기기 A가 상기 공개키저장트랜잭션을 참조하여 얻은 기기 B의
공개키로 전송할 정보를 암호화 한 전송트랜잭션을 생성하여 기기 B로
전송하는 단계; 및
(e) 상기 전송트랜잭션을 수신한 기기 B가 기기 A에 할당된 권한을 상기
주소/권한지정트랜잭션을 참조하여 검증하고, 인증되면 상기
전송트랜잭션의 데이터 영역을 기기 B의 개인키로 복호화 하는 단계;를
포함함을 특징으로 하는 블록체인 시스템을 이용한 기기들간 암호화
통신 방법.

[청구항 2] 제1항에서, 상기 그룹생성트랜잭션과 상기 주소/권한지정트랜잭션은
상기 풀노드의 개인키로 서명되는 것을 특징으로 하는 블록체인
시스템을 이용한 기기들간 암호화 통신 방법.

[청구항 3] 제1항에서, 상기 주소/권한지정트랜잭션에 지정되는 권한에는
상기 그룹(G)에 접근할 수 있는 권한과 기록할 수 있는 권한이 포함됨을
특징으로 하는 블록체인 시스템을 이용한 기기들간 암호화 통신 방법.

[청구항 4] 블록체인 풀노드; 및
상기 풀노드에 접속된 기기 A,B;를 포함하여 구성되고,
상기 풀노드는,
그룹(G)을 생성하는 그룹생성트랜잭션을 생성하는 그룹생성부;
상기 그룹(G)에 속하는 기기의 주소(A,B)와 권한을 지정하는
주소/권한지정트랜잭션을 상기 그룹(G)과 관련하여 생성하는
주소/권한지정부;를 구비하고,
기기 A,B는 각각 자신의 개인키를 사용하여 공개키를 생성하고, 생성된
공개키를 저장하는 공개키저장트랜잭션을 상기 그룹(G)과 관련하여
생성하는 공개키저장부;를 구비하고,
기기 A는 상기 공개키저장트랜잭션을 참조하여 얻은 기기 B의 공개키로
전송할 정보를 암호화 한 전송트랜잭션을 생성하여 기기 B로 전송하는
전송부;를 구비하고,
기기 B는 상기 전송 트랜잭션을 수신하고, 기기 A에 할당된 권한을 상기

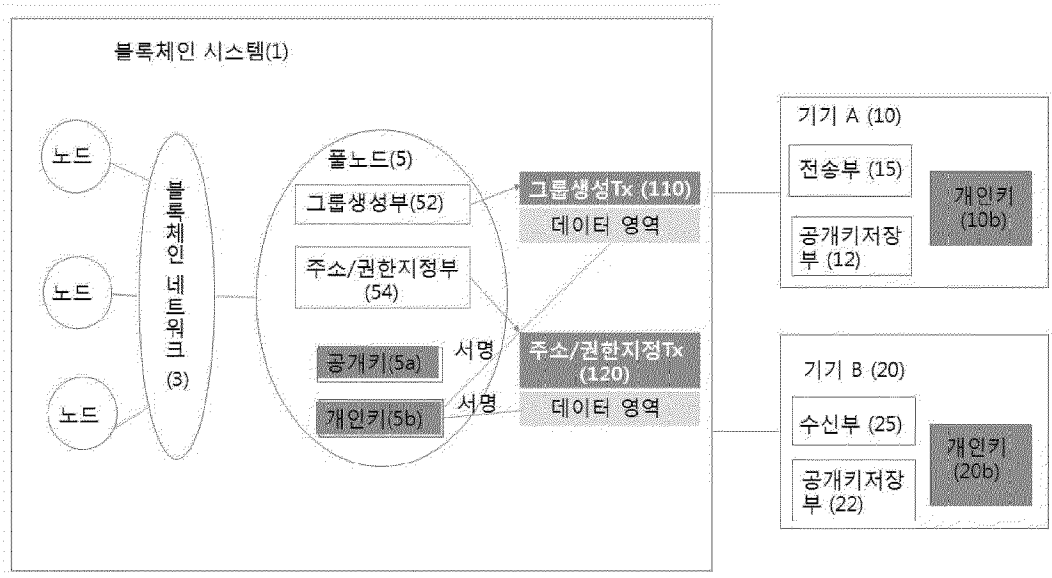
주소/권한지정트랜잭션을 참조하여 검증하고, 인증되면 상기 전송트랜잭션의 데이터 영역을 기기 B의 개인키로 복호화 하는 수신부;를 구비하는 것을 특징으로 하는 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템.

[청구항 5] 제4항에서, 상기 그룹생성트랜잭션과 상기 주소/권한지정트랜잭션은 상기 풀노드의 개인키로 서명되는 것을 특징으로 하는 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템.

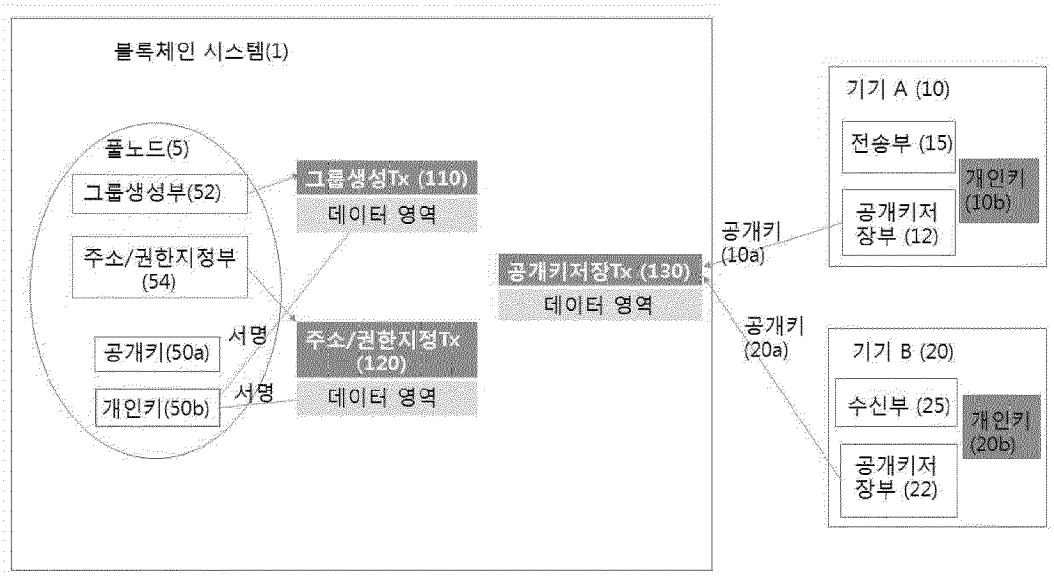
[청구항 6] 제4항에서, 상기 주소/권한지정트랜잭션에 지정되는 권한에는 상기 그룹(G)에 접근할 수 있는 권한과 기록할 수 있는 권한이 포함됨을 특징으로 하는 블록체인 시스템을 이용한 기기들간 암호화 통신 시스템.

[청구항 7] 제1항 내지 제3항 중 어느 한 항의 블록체인 시스템을 이용한 기기들간 암호화 통신 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

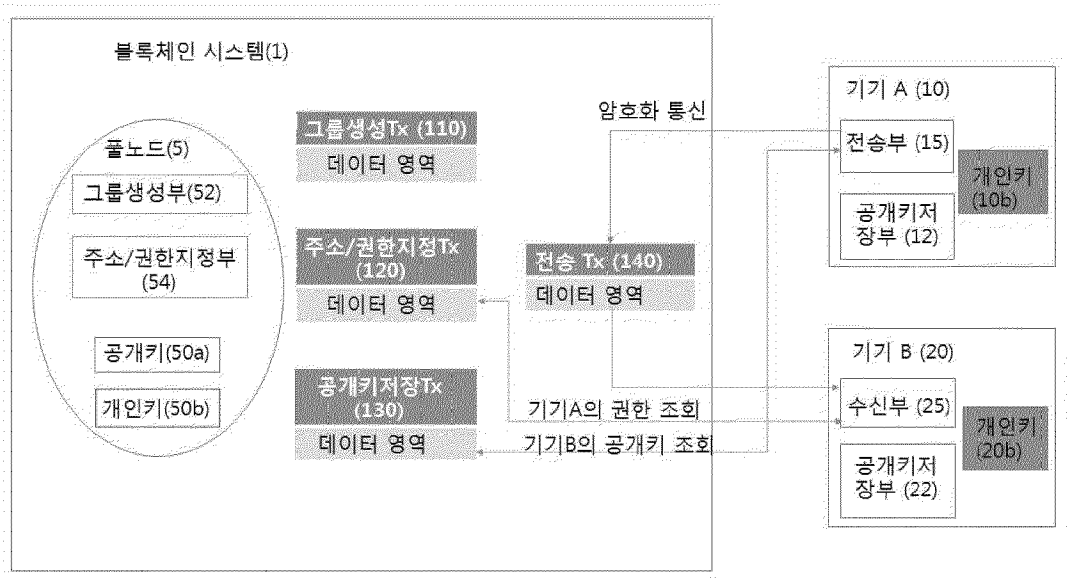
[도1]


블록체인 시스템(1)
노드
노드
노드
블록체인 네트워크 (3)
풀노드(5)
그룹생성부(52)
주소/권한지정부 (54)
공개키(5a)
개인키(5b)
서명
서명
그룹생성Tx (110)
데이터 영역
주소/권한지정Tx (120)
데이터 영역
기기 A (10)
전송부 (15)
공개키저장부 (12)
개인키 (10b)
기기 B (20)
수신부 (25)
공개키저장부 (22)
개인키 (20b)

[도2]


블록체인 시스템(1)
풀노드(5)
그룹생성부(52)
주소/권한지정부 (54)
공개키(50a)
개인키(50b)
서명
서명
그룹생성Tx (110)
데이터 영역
주소/권한지정Tx (120)
데이터 영역
공개키저장Tx (130)
데이터 영역
공개키 (10a)
공개키 (20a)
기기 A (10)
전송부 (15)
공개키저장부 (12)
개인키 (10b)
기기 B (20)
수신부 (25)
공개키저장부 (22)
개인키 (20b)

[도3]


블록체인 시스템(1)
풀노드(5)
그룹생성부(52)
주소/권한지정부 (54)
공개키(50a)
개인키(50b)
그룹생성Tx (110)
데이터 영역
주소/권한지정Tx (120)
데이터 영역
공개키저장Tx (130)
데이터 영역
전송 Tx (140)
데이터 영역
암호화 통신
기기A의 권한 조회
기기B의 공개키 조회
기기 A (10)
전송부 (15)
공개키저장부 (12)
개인키 (10b)
기기 B (20)
수신부 (25)
공개키저장부 (22)
개인키 (20b)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2019/002065

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i, H04L 9/32(2006.01)i, H04L 29/12(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 9/08; G06Q 20/06; G06Q 20/22; G06Q 50/00; H04L 9/06; H04L 9/14; H04L 9/32; H04L 29/12

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: blockchain, encryption, group

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-2018-0014534 A (SOGANG UNIVERSITY RESEARCH & BUSINESS DEVELOPMENT FOUNDATION) 09 February 2018 See paragraphs [0023]-[0024], [0101].	1-7
Y	KR 10-1590076 B1 (WAVESTRING CO., LTD.) 01 February 2016 See paragraphs [0013], [0039], [0045].	1-7
A	KR 10-1701131 B1 (RAPI INC.) 13 February 2017 See paragraphs [0035]-[0041]; and figure 1.	1-7
A	KR 10-2001-0078921 A (PARK, Joon Sang) 22 August 2001 See claims 1-6.	1-7
A	WO 2017-112469 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 29 June 2017 See page 19, line 7-page 20, line 11; and figure 4.	1-7

☐ 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
24 MAY 2019 (24.05.2019)	**27 MAY 2019 (27.05.2019)**

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/KR2019/002065

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2018-0014534 A	09/02/2018	KR 10-1950912 B1	21/02/2019
KR 10-1590076 B1	01/02/2016	None	
KR 10-1701131 B1	13/02/2017	None	
KR 10-2001-0078921 A	22/08/2001	None	
WO 2017-112469 A1	29/06/2017	AU 2016-378211 A1	07/06/2018
		BR 112018011775 A2	04/12/2018
		CA 3009326 A1	29/06/2017
		CN 108370318 A	03/08/2018
		EP 3395007 A1	31/10/2018
		JP 2019-505150 A	21/02/2019
		MX 2018007483 A	01/08/2018
		SG 11201804190 YA	28/06/2018
		US 10171248 B2	01/01/2019
		US 2017-0180134 A1	22/06/2017
		US 2018-0212783 A1	26/07/2018
		US 2019-0097813 A1	28/03/2019
		US 9948467 B2	17/04/2018

국 제 조 사 보 고 서

국제출원번호
PCT/KR2019/002065

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/08(2006.01)i, H04L 9/32(2006.01)i, H04L 29/12(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/08; G06Q 20/06; G06Q 20/22; G06Q 50/00; H04L 9/06; H04L 9/14; H04L 9/32; H04L 29/12

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: 블록체인(blockchain), 암호화(encryption), 그룹(group)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-2018-0014534 A (서강대학교산학협력단) 2018.02.09 단락 [0023]-[0024], [0101] 참조.	1-7
Y	KR 10-1590076 B1 (주식회사 웨이브스트링) 2016.02.01 단락 [0013], [0039], [0045] 참조.	1-7
A	KR 10-1701131 B1 (주식회사 라피) 2017.02.13 단락 [0035]-[0041]; 및 도면 1 참조.	1-7
A	KR 10-2001-0078921 A (박준상) 2001.08.22 청구항 1-6 참조.	1-7
A	WO 2017-112469 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 2017.06.29 페이지 19, 라인 7 - 페이지 20, 라인 11; 및 도면 4 참조.	1-7

☐ 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

"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 05월 24일 (24.05.2019)	2019년 05월 27일 (27.05.2019)

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

심사관
양정록
전화번호 +82-42-481-5709

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2019/002065

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2018-0014534 A	2018/02/09	KR 10-1950912 B1	2019/02/21
KR 10-1590076 B1	2016/02/01	없음	
KR 10-1701131 B1	2017/02/13	없음	
KR 10-2001-0078921 A	2001/08/22	없음	
WO 2017-112469 A1	2017/06/29	AU 2016-378211 A1	2018/06/07
		BR 112018011775 A2	2018/12/04
		CA 3009326 A1	2017/06/29
		CN 108370318 A	2018/08/03
		EP 3395007 A1	2018/10/31
		JP 2019-505150 A	2019/02/21
		MX 2018007483 A	2018/08/01
		SG 11201804190 YA	2018/06/28
		US 10171248 B2	2019/01/01
		US 2017-0180134 A1	2017/06/22
		US 2018-0212783 A1	2018/07/26
		US 2019-0097813 A1	2019/03/28
		US 9948467 B2	2018/04/17