(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2019 년 5 월 16 일 (16.05.2019)

WIPO | PCT

(10) 국제공개번호
WO 2019/093574 A1

(51) 국제특허분류:
H04L 9/32 (2006.01) *H04L 9/06* (2006.01)

(21) 국제출원번호: PCT/KR2017/014684

(22) 국제출원일: 2017 년 12 월 14 일 (14.12.2017)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2017-0149091 2017 년 11 월 10 일 (10.11.2017) KR

(71) 출원인: 부산대학교 산학협력단 (**PUSAN NATIONAL UNIVERSITY INDUSTRY-UNIVERSITY COOPERATION FOUNDATION**) [KR/KR]; 46241 부산시 금정구 부산대학로63번길 2 (장전동, 부산대학교), Busan (KR).

(72) 발명자: 김호원 (**KIM, Ho Won**); 49497 부산시 사하구 다대낙조2길 100, 218동 1603호, Busan (KR). 배봉진 (**BAE, Bong Jin**); 46288 부산시 금정구 부산대학로63번길 45, 201호, Busan (KR). 박태환 (**PARK, Tae Hwan**); 48091 부산시 해운대구 해운대해변로 117, 106동 104호, Busan (KR). 이가람 (**LEE, Ga Ram**); 46288 부산시 금정구 금강로279번길 9-2, 101호, Busan (KR).

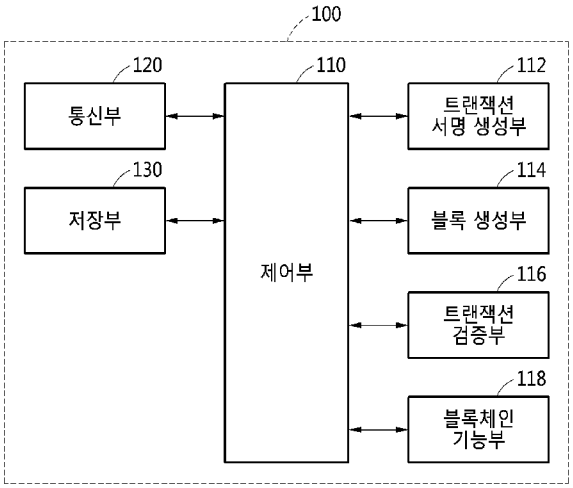
(74) 대리인: 특허법인 무한 (**MUHANN PATENT & LAW FIRM**); 06144 서울시 강남구 언주로 560, 8층 (역삼동, 진영빌딩), Seoul (KR).

(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:** BLOCK CHAIN SYSTEM AND METHOD EMPLOYING HASH-BASED SIGNATURE SCHEME

(54) **발명의 명칭:** 해시 기반 서명 기법을 적용한 블록체인 시스템 및 방법



110 ... Control unit
112 ... Transaction signature generation unit
114 ... Block generation unit
116 ... Transaction verification unit
118 ... Block chain function unit
120 ... Communication unit
130 ... Storing unit

(57) **Abstract:** The present invention relates to a block chain system and method employing a hash-based signature scheme, wherein each node of the block chain system may provide a block chain service by comprising: a transaction signature generation unit for generating a transaction signature that is a signature for a transaction using a hash-based signature scheme, and storing the transaction signature in the transaction; a block generation unit for generating a Merkle signature corresponding to each transaction to be included in a block, and generating a block including transactions in which the Merkle signature is stored; and a transaction verification unit for verifying the transaction signature of the transaction to be verified and verifying the transaction through verification of the Merkle signature of the transaction to be verified.

(57) **요약서:** 본 발명은 해시 기반 서명 기법을 적용한 블록체인 시스템 및 방법에 관한 것으로, 블록체인 시스템의 각 노드는 해시 기반 서명 기법을 이용해 트랜잭션에 대한 서명인 트랜잭션 서명을 생성하고, 트랜잭션 서명을 트랜잭션에 저장하는 트랜잭션 서명 생성부와, 블록에 포함될 트랜잭션 각각에 대응하는 머클 서명을 생성하고, 머클 서명이 저장된 트랜잭션들을 포함하는 블록을 생성하는 블록 생성부와 검증하고자 하는 트랜잭션의 트랜잭션 서명을 검증하고, 검증하고자 하는 트랜잭션의 머클 서명의 검증을 통해서 트랜잭션을 검증하는 트랜잭션 검증부를 포함하여 블록체인 서비스를 제공할 수 있다.

WO 2019/093574 A1

[다음 쪽 계속]

규칙 4.17에 의한 선언서:

— 신규성을 해치지 아니하는 개시 또는 신규성 상실의 예외에 관한 선언 (규칙 4.17(v))

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 해시 기반 서명 기법을 적용한 블록체인 시스템 및 방법

기술분야

[1] 이하의 일 실시 예들은 기존의 블록체인 구조에 비해 보다 강인한 양자 내성 특성을 갖는 구조를 제공하기 위한 것이다.

배경기술

[2] 블록체인은 최근 비트코인, 이더리움과 같은 암호화 화폐가 주목을 받으면서 암호화 화폐의 보안 기술인 블록체인에 대한 관심도가 높아지고 있다. 기존의 금융 거래 방식의 경우, 신뢰할 수 있는 제3자 기관(TTP, Trusted Third Party)를 중개자로 두고 거래의 유효성을 검증하는 반면, 블록체인의 경우, 거래 장부를 네트워크 참여자 모두에게 공유를 함으로써, 분산된 공공 거래 장부 형태로 서로의 거래에 대해 유효성을 검증해줌으로써 거래의 신뢰성을 유지하게 된다. 블록체인은 블록의 연결된 형태로 각 블록은 특정 시간 동안의 트랜잭션들(거래 내역들)과 합의 알고리즘 관련 필드, 블록에 대한 정보 필드 등으로 구성되어있다. 이러한 블록을 만드는 권한은 합의 알고리즘(PoW, PoS, DpoS 등)을 통해 특정 참여 노드(네트워크 참여자)를 선정하여 블록을 생성하게 되며 이러한 합의 알고리즘을 통해 특정 참여자의 독점에 인한 악의적인 블록 생성을 예방할 수 있다.

[3] 현재 비트코인 기준 블록체인에서는 트랜잭션별 서명 알고리즘으로 ECDSA를 사용하고 있다. 하지만 ECDSA(Elliptic Curve Digital Signature Algorithm) 전자 서명 알고리즘은 타원곡선 기반의 암호 알고리즘으로 이산대수 문제인 DLP(Discrete Logarithm Problem)에 기반을 두고 있으며, 이산대수 문제는 양자 컴퓨터 알고리즘 중 쇼어 알고리즘(Shor's algorithm)에 의해 효율적인 시간 내에 공격이 가능하다는 문제점을 가지고 있다. 이러한 문제로 인해 기존 블록체인 시스템은 양자 컴퓨팅 환경에서 취약점을 가지게 된다.

[4] 따라서, 양자 컴퓨팅 환경에서도 강인한 내성을 가진 트랜잭션 서명 알고리즘이 요구된다.

발명의 상세한 설명

기술적 과제

[5] 본 발명은 상기와 같은 종래 기술의 문제점을 해결하고자 도출된 것으로서, 양자 컴퓨팅 환경에서도 강인한 내성을 가진 해시 기반 OTS(One Time Signature) 알고리즘을 기반한 트랜잭션 서명을 생성하는 방법을 제공하는 것을 목적으로 한다.

[6] 구체적으로, 본 발명은 해시 기반 OTS 알고리즘으로 트랜잭션 서명을 생성하고, 트랜잭션의 검증키를 이용해서 머클 트리를 구성하고 트랜잭션

각각의 머클 서명을 생성함으로써, 트랜잭션 서명과 머클 루트 값의 2단계 검증을 통해서 트랜잭션을 검증할 수 있는 방법을 제공하는 것을 목적으로 하다.

과제 해결 수단

[7] 상기와 같은 목적을 달성하기 위하여, 본 발명의 일 실시 예에 따른 해시 기반 서명 기법을 적용한 블록체인 시스템의 노드는, 해시 기반 서명 기법을 이용해 트랜잭션에 대한 서명인 트랜잭션 서명을 생성하고, 상기 트랜잭션 서명을 상기 트랜잭션에 저장하는 트랜잭션 서명 생성부; 블록에 포함될 트랜잭션 각각에 대응하는 머클 서명을 생성하고, 상기 머클 서명이 저장된 트랜잭션들을 포함하는 블록을 생성하는 블록 생성부; 및 검증하고자 하는 트랜잭션의 트랜잭션 서명을 검증하고, 상기 검증하고자 하는 트랜잭션의 머클 서명의 검증을 통해서 트랜잭션을 검증하는 트랜잭션 검증부를 포함한다.

[8] 이때, 노드는 합의 알고리즘에 따른 처리와, 생성된 블록을 블록체인에 연결하고, 블록 헤더를 구성하는 기능을 수행하는 블록체인 기능부; 및 블록체인 시스템의 다른 노드들과 트랜잭션을 송수신하고, 블록을 공유하기 위해 통신을 하는 통신부를 더 포함할 수 있다.

[9] 이때, 상기 트랜잭션 서명 생성부는, 서명키와 검증키로 이루어진 한쌍의 키를 생성하고, 해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 상기 트랜잭션과 상기 서명키를 이용해서 상기 트랜잭션 서명을 생성하고, 상기 트랜잭션 서명과 상기 검증키를 상기 트랜잭션에 저장할 수 있다.

[10] 이때, 상기 블록 생성부는, 상기 블록에 포함될 트랜잭션 각각의 검증키를 트리의 리프노드에 배치하여 머클 트리를 생성하고, 상기 머클 트리의 머클 루트 값을 상기 블록의 헤더에 저장하고, 상기 블록에 포함될 트랜잭션 각각의 상기 머클 서명을 생성하고, 상기 블록에 포함될 트랜잭션 각각에 상기 머클 서명을 저장할 수 있다.

[11] 이때, 상기 머클 서명은, 트랜잭션 서명, 검증키 및 인증 경로를 포함하고, 상기 인증 경로는 상기 머클 트리 없이도 상기 머클 루트 값을 계산하는데 필요한 값일 수 있다.

[12] 이때, 상기 트랜잭션 검증부는, 상기 검증하고자 하는 트랜잭션에 저장된 검증키를 이용해서 해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 상기 검증하고자 하는 트랜잭션에 저장된 트랜잭션 서명을 검증하고, 상기 트랜잭션 서명의 검증에 성공하면, 상기 검증하고자 하는 트랜잭션에 저장된 머클 서명을 확인하고, 상기 머클 서명에 포함된 상기 검증키와 인증 경로를 이용하여 머클 루트 값을 계산하고, 상기 검증하고자 하는 트랜잭션을 포함하는 해당 블록의 블록 헤더에 저장된 머클 루트 값을 확인하고, 상기 계산된 머클 루트 값과 상기 저장된 머클 루트 값을 비교해서 동일하면 상기 머클 서명에 대한 검증에 성공했다고 판단할 수 있다.

[13] 이때, 상기 트랜잭션 검증부는, 상기 머클 서명에 대한 검증에 성공하면, 상기

검증하고자 하는 트랜잭션에 관한 검증에 성공했음을 네트워크로 송신할 수 있다.

[14] 이때, 상기 트랜잭션 검증부는, 상기 트랜잭션 서명에 관한 검증에 실패하거나 상기 머클 서명에 관한 검증에 실패하면, 상기 검증하고자 하는 트랜잭션에 관한 검증에 실패했음을 네트워크로 송신할 수 있다.

[15] 본 발명의 일 실시 예에 따른 해시 기반 서명 기법을 적용한 블록체인 시스템에서 트랜잭션을 검증하는 방법은, 해시 기반 서명 기법을 이용해 트랜잭션에 대한 서명인 트랜잭션 서명을 생성하고, 상기 트랜잭션 서명을 상기 트랜잭션에 저장하는 단계; 블록에 포함될 트랜잭션 각각에 대응하는 머클 서명을 생성하고, 상기 머클 서명이 저장된 트랜잭션들을 포함하는 블록을 생성하는 단계: 및 상기 블록에 포함된 트랜잭션들 중에서 검증하고자 하는 트랜잭션의 트랜잭션 서명을 검증하고, 상기 검증하고자 하는 트랜잭션의 머클 서명의 검증을 통해서 트랜잭션을 검증하는 단계를 포함한다.

[16] 이때, 상기 트랜잭션 서명을 생성하고, 상기 트랜잭션 서명을 상기 트랜잭션에 저장하는 단계는, 서명키와 검증키로 이루어진 한쌍의 키를 생성하는 단계; 해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 상기 트랜잭션과 상기 서명키를 이용해서 상기 트랜잭션 서명을 생성하는 단계; 및 상기 트랜잭션 서명과 상기 검증키를 상기 트랜잭션에 저장하는 단계를 포함할 수 있다.

[17] 이때, 상기 블록을 생성하는 단계는, 상기 블록에 포함될 트랜잭션 각각의 검증키를 트리의 리프노드에 배치하여 머클 트리를 생성하는 단계; 상기 머클 트리의 머클 루트 값을 상기 블록의 헤더에 저장하는 단계; 상기 블록에 포함될 트랜잭션 각각의 상기 머클 서명을 생성하는 단계; 및 상기 블록에 포함될 트랜잭션 각각에 상기 머클 서명을 저장하는 단계를 포함할 수 있다.

[18] 이때, 상기 머클 서명은, 트랜잭션 서명, 검증키 및 인증 경로를 포함하고, 상기 인증 경로는 상기 머클 트리 없이도 상기 머클 루트 값을 계산하는데 필요한 값일 수 있다.

[19] 이때, 상기 트랜잭션을 검증하는 단계는, 상기 검증하고자 하는 트랜잭션에 저장된 검증키를 이용해서 해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 상기 검증하고자 하는 트랜잭션에 저장된 트랜잭션 서명을 검증하는 단계; 상기 트랜잭션 서명의 검증에 성공하면, 상기 검증하고자 하는 트랜잭션에 저장된 머클 서명을 확인하는 단계; 상기 머클 서명에 포함된 상기 검증키와 인증 경로를 이용하여 머클 루트 값을 계산하는 단계; 상기 검증하고자 하는 트랜잭션을 포함하는 해당 블록의 블록 헤더에 저장된 머클 루트 값을 확인하는 단계; 및 상기 계산된 머클 루트 값과 상기 저장된 머클 루트 값을 비교해서 동일하면 상기 머클 서명에 대한 검증에 성공했다고 판단하는 단계를 포함할 수 있다.

[20] 이때, 상기 트랜잭션을 검증하는 단계는, 상기 머클 서명에 대한 검증에 성공하면, 상기 검증하고자 하는 트랜잭션에 관한 검증에 성공했음을

네트워크로 송신하는 단계를 더 포함할 수 있다.

[21] 이때, 상기 트랜잭션을 검증하는 단계는, 상기 트랜잭션 서명에 관한 검증에 실패하거나 상기 머클 서명에 관한 검증에 실패하면, 상기 검증하고자 하는 트랜잭션에 관한 검증에 실패했음을 네트워크로 송신하는 단계를 더 포함할 수 있다.

발명의 효과

[22] 본 발명은 해시 기반 서명 기법을 적용한 블록체인 시스템 및 방법에 관한 것으로, 양자 알고리즘에 내성을 가지는 해시 기반 서명 기법을 사용함으로써 양자 알고리즘에 강인한 효과를 가지고, 머클 서명을 이용한 트랜잭션 서명 검증을 통해 트랜잭션 검증뿐만 아니라 블록에 포함된 트랜잭션 전체에 대한 무결성 검증 및 트랜잭션에 대한 블록 포함 여부도 함께 확인이 가능하고, 기존에 사용되는 ECDSA에 비해 해시 기반 서명 기법의 서명 생성 및 검증 속도가 빠르기 때문에 전반적인 블록체인 성능 향상을 기대할 수 있고, 해시 함수(SHA-256)을 이용해 해시 기반 서명 기법을 적용했을 때 기존 전자 서명 알고리즘(ECDSA)와 뒤쳐지지 않는 보안강도를 가질 수 있다.

도면의 간단한 설명

[23] 도 1은 본 발명의 일 실시 예에 따른 해시 기반 서명 기법을 적용한 블록체인 시스템의 노드의 구성을 도시한 도면이다.

[24] 도 2는 본 발명의 일 실시 예에 따른 블록체인 시스템에서 블록 헤더에 포함되는 머클 루트 값을 계산하는 방법을 도시한 도면이다.

[25] 도 3은 본 발명의 일 실시 예에 따른 블록체인 시스템에서 블록을 생성할 때, 각 트랜잭션에 머클 서명 정보를 포함함을 도시한 도면이다.

[26] 도 4는 본 발명의 일 실시 예에 따른 블록체인 시스템에서 트랜잭션을 2단계로 검증하는 과정을 도시한 도면이다.

[27] 도 5는 본 발명의 일 실시 예에 따른 블록체인 시스템의 노드에서 블록을 생성하고 트랜잭션을 검증하는 과정을 도시한 흐름도이다.

[28] 도 6은 본 발명의 일 실시 예에 따른 블록체인 시스템의 노드에서 트랜잭션 서명을 생성하는 과정을 도시한 흐름도이다.

[29] 도 7은 본 발명의 일 실시 예에 따른 블록체인 시스템의 노드에서 블록을 생성하는 과정을 도시한 흐름도이다.

[30] 도 8은 본 발명의 일 실시 예에 따른 블록체인 시스템의 노드에서 트랜잭션을 검증하는 과정을 도시한 흐름도이다.

발명의 실시를 위한 최선의 형태

[31] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[32] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 변경, 균등물, 또는 대체물을 포함한다.

[33] 제1 또는 제2 등의 용어를 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만, 예를 들어 본 발명의 개념에 따른 권리 범위로부터 이탈되지 않은 채, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소는 제1 구성요소로도 명명될 수 있다.

[34] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성요소들 간의 관계를 설명하는 표현들, 예를 들어 "~사이에"와 "바로~사이에" 또는 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다.

[35] 본 명세서에서 사용한 용어는 단지 특정한 실시 예들을 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함으로 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[36] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[37] 이하, 실시 예들을 첨부된 도면을 참조하여 상세하게 설명한다. 그러나, 특허출원의 범위가 이러한 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[38] 이하에서는, 본 발명의 일 실시 예에 따른 해시 기반 서명 기법을 적용한 블록체인 시스템 및 방법을 첨부된 도 1 내지 도 8을 참조하여 상세히 설명한다.

[39] 도 1은 본 발명의 일 실시 예에 따른 해시 기반 서명 기법을 적용한 블록체인

시스템의 노드의 구성을 도시한 도면이다.

[40] 도 1을 참조하면, 블록체인 시스템의 노드(100)는 제어부(110), 트랜잭션 서명 생성부(112), 블록 생성부(114), 트랜잭션 검증부(116), 블록체인 기능부(118), 통신부(120) 및 저장부(130)를 이용해서 해시 기반 서명 기법을 적용한 트랜잭션 서명을 생성하여 양자 컴퓨팅 환경에서도 블록체인에 포함되는 블록의 보안을 유지할 수 있도록 할 수 있다.

[41] 통신부(120)는 수신기(Receiver)와 송신기(transmitter)를 포함하는 통신 인터페이스 장치로서 유선 또는 무선으로 데이터를 송수신한다. 통신부(120)는 블록체인 시스템의 네트워크에 포함된 다른 노드들과 트랜잭션을 송수신하고, 블록을 공유하기 위해 통신을 한다.

[42] 저장부(130)는 노드(100)의 전반적인 동작을 제어하기 위한 운영체제, 응용 프로그램 등을 저장한다. 또한, 저장부(130)는 블록 생성부(114)에서 생성한 블록과 블록체인 시스템에서 관리하는 블록체인을 저장할 수 있다.

[43] 트랜잭션 서명 생성부(112)는 해시 기반 서명 기법을 이용해 트랜잭션에 대한 서명인 트랜잭션 서명을 생성하고, 트랜잭션 서명을 트랜잭션에 저장한다.

[44] 보다 구체적으로, 트랜잭션 서명 생성부(112)는 서명키와 검증키로 이루어진 한쌍의 키를 생성하고, 해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 트랜잭션과 서명키를 이용해서 트랜잭션 서명을 생성하고, 트랜잭션 서명과 검증키를 트랜잭션에 저장한다.

[45] 블록 생성부(114)는 블록에 포함될 트랜잭션 각각에 대응하는 머클 서명을 생성하고, 머클 서명이 저장된 트랜잭션들을 포함하는 블록을 생성한다.

[46] 보다 구체적으로 블록 생성부(114)는 아래의 도 2의 예와 같이 블록에 포함될 트랜잭션 각각의 검증키를 트리의 리프노드에 배치하여 머클 트리를 생성하고, 머클 트리의 머클 루트 값을 블록의 헤더에 저장한다.

[47]

[48] 도 2는 본 발명의 일 실시 예에 따른 블록체인 시스템에서 블록 헤더에 포함되는 머클 루트 값을 계산하는 방법을 도시한 도면이다.

[49] 도 2를 참조하면, 블록 생성부(114)는 블록에 포함될 트랜잭션(211, 212, 213, 214) 각각의 검증키(Y_A, Y_B, Y_C, Y_D)를 트리의 리프노드(221, 222, 223, 224)에 배치하여 해시한다. 리프노드(221, 222, 223, 224)들을 2개씩 연접한 데이터에 대해 해쉬하여 새로운 부모 노드(231, 232)를 생성하고, 이를 반복하여 머클 루트 값(204)를 계산하여 블록의 헤더에 저장한다.

[50]

[51] 블록 생성부(114)에서 생성하는 블록의 구조를 살펴보면 블록은 크게 4가지로 구성되어있다. 전체 블록 크기를 나타내는 4 bytes의 블록 크기 필드(201), 총 80 bytes의 블록 헤더 필드, 블록에 저장된 트랜잭션의 개수를 나타내고 1~9bytes의 가변 크기를 가진 트랜잭션 개수 필드(208), 그리고 블록에 저장된 트랜잭션(211, 212, 213, 214)들을 저장하는 트랜잭션 필드로 구성되어있다.

[52] 블록 헤더의 구성에 대해 자세히 알아보면, 먼저 4 bytes로 구성된 버전 필드(202)는 블록체인 소프트웨어나 사용하는 프로토콜에 대한 업그레이드 버전을 나타낸다.

[53] 32 bytes로 구성된 이전 블록 헤더 크기 필드(203)는 블록체인에서 현재 블록 이전의 블록 헤더(80bytes) 부분을 해시한 값이 저장된다. 이때, 비트코인의 블록체인 기준으로 SHA-256 해시 함수를 사용하여 이전 블록 헤더를 해싱하게 된다.

[54] 32 bytes로 구성된 머클 루트 필드(204)는 해당 블록에 저장된 모든 트랜잭션을 이용하여 머클 트리를 구성하고 그 트리의 루트 값을 저장한 것으로 블록이 가지고 있는 모든 트랜잭션에 대한 무결성을 검증하거나, 특정 거래가 해당 블록에 포함이 되는지 아닌지를 확인할 수 있다.

[55] 4 bytes로 구성된 타임스탬프 필드(205)는 블록의 생성 시간을 나타내는 필드로 유닉스 기준일로부터 초 단위로 계산한 값이 저장된다.

[56] 각각 4 bytes로 구성된 난이도 목표 필드(206)와 논스 필드(207)는 채굴(Mining)이라는 과정에서 사용된다.

[57] 채굴에 관해 설명하면, 채굴은 전자 화폐를 생산하며, 블록에 대한 트랜잭션의 유효성을 검증하고, 블록을 블록체인에 연결하는 것이다. 채굴을 수행하기 위해 수많은 채굴자가 참가하게 되고, 수많은 채굴자 중 합의 메커니즘을 통해 보상으로 코인을 얻고, 블록을 생성하여 블록체인에 연결하는 채굴자를 선정하게 된다. 이러한 합의 메커니즘은 비트코인에서 작업의 증명(Proof Of Work)을 통해 이루어지며, 작 업의 증명 문제로 hash cash 문제를 사용하게 된다. 컴퓨팅 성능이 향상됨에 따라 hash cash 문제를 빨리 풀게 되는데, 이러한 경우 난이도 목표 필드값을 수정하여 hash cash 문제 푸는 시간을 조정할 수 있다.

[58]

[59] 그리고, 블록 생성부(114)는 아래 도 3의 예와 같이 블록에 포함될 트랜잭션 각각의 머클 서명을 생성하고, 블록에 포함될 트랜잭션 각각에 머클 서명을 저장한다.

[60]

[61] 도 3은 본 발명의 일 실시 예에 따른 블록체인 시스템에서 블록을 생성할 때, 각 트랜잭션에 머클 서명 정보를 포함함을 도시한 도면이다.

[62] 도 3을 참조하면, 블록 생성부(114)는 트랜잭션들 별로 머클 서명을 생성하여 저장한다. 예를 들어, 트랜잭션(T_XA)의 경우 트랜잭션 서명($T_XA\ \sigma_{OTS}$), 검증키(Y_A) 및 인증 경로($Hash(Y_B)$, H_{CD})를 포함하는 머클 서명을 생성하여 트랜잭션(T_XA)에 저장한다.

[63] 이때, 인증 경로(AP; Authentication Path)($A_s = \{a_0, ..., a_{H-1}\}$)는 머클 트리 없이도 머클 루트 값(204)을 계산하는데 필요한 값으로, 인증 경로 상의 노드 h는 인증 경로상에서 높이가 h인 노드의 형제 노드를 나타내며, 인증 경로 인덱스 계산 공식은 아래와 <수학식 1>과 같다.

[64] [수학식 1]

$$a_h = v_h[\lceil (s/2^h) - 1 \rceil], if \lfloor s/2^h \rfloor \equiv 1 \mod 2, h = 0, ..., H-1$$

$$a_h = v_h[\lceil (s/2^h) + 1 \rceil], if \lfloor s/2^h \rfloor \equiv 0 \mod 2, h = 0, ..., H-1$$

[65] 트랜잭션 검증부(116)는 아래 도 4의 예와 같이 검증하고자 하는 트랜잭션의 트랜잭션 서명을 검증(검증 1단계)하고, 검증하고자 하는 트랜잭션의 머클 서명의 검증(검증 2단계)을 통해서 트랜잭션을 검증한다.

[66]

[67] 도 4는 본 발명의 일 실시 예에 따른 블록체인 시스템에서 트랜잭션을 2단계로 검증하는 과정을 도시한 도면이다.

[68] 도 4를 참조하면, 트랜잭션 검증부(116)는 트랜잭션 서명을 검증하는 검증 1단계와 트랜잭션의 머클 서명의 검증 2단계의 2번의 검증을 통해서 최종적으로 트랜잭션을 검증할 수 있다.

[69] 검증 1단계에서 트랜잭션 검증부(116)는 검증하고자 하는 트랜잭션에 저장된 검증키(410)를 이용해서 해시 기반 OTS(One Time Signature) 알고리즘(414)을 기반으로 검증하고자 하는 트랜잭션(411)에 저장된 트랜잭션 서명(413)을 검증할 수 있다.

[70] 보다 구체적으로, 트랜잭션(411)을 해시(412)한 값과 트랜잭션 서명(413)을 해시 기반 OTS(One Time Signature) 알고리즘(414)을 기반을 트랜잭션(411)의 검증키를 생성하고, 생성한 검증키와 트랜잭션(411)에 저장된 검증키(410)을 비교하여 동일하면 트랜잭션 서명(413)이 검증에 성공했다고 판단할 수 있다.

[71] 검증 2단계에서 트랜잭션 검증부(116)는 검증 1단계의 검증에 성공하면, 검증하고자 하는 트랜잭션에 저장된 머클 서명을 확인하고, 머클 서명에 포함된 검증키(421)와 인증 경로(423, 423)를 이용하여 머클 루트 값(426)을 계산하고, 검증하고자 하는 트랜잭션을 포함하는 해당 블록의 블록 헤더에 저장된 머클 루트 값(420)을 확인하고, 계산된 머클 루트 값(426)과 저장된 머클 루트 값(420)을 비교해서 동일하면 머클 서명에 대한 검증에 성공했다고 판단할 수 있다. 보다 구체적으로, 트랜잭션 검증부(116)는 머클 루트 값(426)을 계산하기 위해서 검증키(421)를 해시(422)한 값과 인증 경로(423)를 해시(424)하고, 해시값(424)와 인증 경로(425)를 해시해서 머클 루트 값(426)을 계산할 수 있다.

[72] 이때, 트랜잭션 검증부(116)는 머클 서명에 대한 검증에 성공하면, 검증하고자 하는 트랜잭션에 관한 검증에 성공했음을 네트워크로 송신할 수 있다.

[73] 트랜잭션 검증부(116)는 트랜잭션 서명에 관한 검증에 실패하거나 머클 서명에 관한 검증에 실패하면, 검증하고자 하는 트랜잭션에 관한 검증에 실패했음을 네트워크로 송신할 수 있다.

[74]

[75] 블록체인 기능부(118)는 합의 알고리즘에 따른 처리와, 생성된 블록을 블록체인에 연결하고, 블록 헤더를 구성하는 기능을 수행한다.

[76] 제어부(110)는 노드(100)의 전반적인 동작을 제어할 수 있다. 그리고, 제어부(110)는 트랜잭션 서명 생성부(112), 블록 생성부(114), 트랜잭션 검증부(116) 및 블록체인 기능부(118)의 기능을 수행할 수 있다. 제어부(110), 트랜잭션 서명 생성부(112), 블록 생성부(114), 트랜잭션 검증부(116) 및 블록체인 기능부(118)를 구분하여 도시한 것은 각 기능들을 구별하여 설명하기 위함이다. 따라서 제어부(110)는 트랜잭션 서명 생성부(112), 블록 생성부(114), 트랜잭션 검증부(116) 및 블록체인 기능부(118) 각각의 기능을 수행하도록 구성된(configured) 적어도 하나의 프로세서를 포함할 수 있다. 또한, 제어부(110)는 트랜잭션 서명 생성부(112), 블록 생성부(114), 트랜잭션 검증부(116) 및 블록체인 기능부(118) 각각의 기능 중 일부를 수행하도록 구성된(configured) 적어도 하나의 프로세서를 포함할 수 있다.

[77]

[78] 이하, 상기와 같이 구성된 본 발명에 따른 블록체인 시스템의 노드에서 블록을 생성하고 트랜잭션을 검증하는 방법을 아래에서 도면을 참조하여 설명한다.

[79] 도 5는 본 발명의 일 실시 예에 따른 블록체인 시스템의 노드에서 블록을 생성하고 트랜잭션을 검증하는 과정을 도시한 흐름도이다.

[80] 도 5를 참조하면, 본 발명의 노드(100)는 해시 기반 서명 기법을 이용해 트랜잭션에 대한 서명인 트랜잭션 서명을 생성하고, 트랜잭션 서명을 트랜잭션에 저장한다(510). 해시 기반 서명 기법이 적용된 트랜잭션 서명을 생성하는 보다 구체적인 과정은 이후 도 6을 참조하여 후술한다.

[81] 그리고, 노드(100)는 블록에 포함될 트랜잭션 각각에 대응하는 머클 서명을 생성하고, 머클 서명이 저장된 트랜잭션들을 포함하는 블록을 생성할 수 있다(520). 해시 기반 서명 기법이 적용된 블록을 생성하는 보다 구체적인 과정은 이후 도 7을 참조하여 후술한다.

[82] 그리고, 노드(100)는 블록에 포함된 트랜잭션들 중에서 검증하고자 하는 트랜잭션의 트랜잭션 서명을 검증하고, 검증하고자 하는 트랜잭션의 머클 서명의 검증을 통해서 트랜잭션을 검증할 수 있다(530). 해시 기반 서명 기법이 적용된 트랜잭션을 검증하는 보다 구체적인 과정은 이후 도 8을 참조하여 후술한다.

[83]

[84] 도 6은 본 발명의 일 실시 예에 따른 블록체인 시스템의 노드에서 트랜잭션 서명을 생성하는 과정을 도시한 흐름도이다.

[85] 도 6을 참조하면, 노드(100)는 트랜잭션 서명을 생성하기 위해서 서명키와 검증키로 이루어진 한쌍의 키를 생성한다(610).

[86] 그리고, 노드(100)는 해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 트랜잭션과 서명키를 이용해서 트랜잭션 서명을 생성한다(612).

[87] 그리고, 노드(100)는 트랜잭션 서명과 검증키를 트랜잭션에 저장한다(614).

[88]

[89] 도 7은 본 발명의 일 실시 예에 따른 블록체인 시스템의 노드에서 블록을 생성하는 과정을 도시한 흐름도이다.

[90] 도 7을 참조하면, 노드(100)는 블록을 생성하기 위해서 블록에 포함될 트랜잭션 각각의 검증키를 트리의 리프노드에 배치하여 머클 트리를 생성한다(710).

[91] 그리고, 노드(100)는 머클 트리의 루트(root)에 위치하는 머클 루트 값을 계산한다(712).

[92] 그리고, 노드(100)는 머클 트리의 머클 루트 값을 블록의 헤더에 저장한다(714).

[93] 그리고, 노드(100)는 블록에 포함될 트랜잭션 각각의 머클 서명을 생성한다 그리고, 노드(100)는 머클 트리의 머클 루트 값을 블록의 헤더에 저장한다(716). 이때, 머클 서명은 트랜잭션 서명, 검증키 및 인증 경로를 포함하고, 여기서, 인증 경로는 머클 트리 없이도 머클 루트 값을 계산하는데 필요한 값을 나타낸다.

[94] 그리고, 노드(100)는 블록에 포함될 트랜잭션 각각에 머클 서명을 저장한다(718).

[95] 그리고, 노드(100)는 블록 헤더에 저장되는 그 외 다른 정보들(버전, 이전 블록 헤더 해시, 타임 스탬프, 난이도 목표, 난스 등)을 확인 또는 생성한다(720).

[96] 그리고, 노드(100)는 720단계에서 확인 또는 생성된 정보와 머클 루트 값을 이용해서 블록 헤더를 생성하고, 블록의 페이로드에 머클 서명을 포함하는 트랜잭션들을 저장하여 블록을 생성한다(722).

[97]

[98] 도 8은 본 발명의 일 실시 예에 따른 블록체인 시스템의 노드에서 트랜잭션을 검증하는 과정을 도시한 흐름도이다.

[99] 도 8을 참조하면, 노드(100)는 블록에 포함된 트랜잭션을 검증하는 이벤트가 발생하는 경우, 검증하고자 하는 트랜잭션에 저장된 검증키를 이용해서 해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 검증하고자 하는 트랜잭션에 저장된 트랜잭션 서명을 검증한다(810).

[100] 그리고, 노드(100)는 810단계에서 트랜잭션 노드의 검증을 수행한 결과 트랜잭션 서명의 검증에 성공하였는지 확인한다(812).

[101] 812단계의 확인결과 트랜잭션 서명의 검증에 성공하면, 노드(100)는 검증하고자 하는 트랜잭션에 저장된 머클 서명을 확인한다(814).

[102] 그리고, 노드(100)는 머클 서명에 포함된 검증키와 인증 경로를 이용하여 머클 루트 값을 계산한다(816).

[103] 그리고, 노드(100)는 검증하고자 하는 트랜잭션을 포함하는 해당 블록의 블록 헤더에 저장된 머클 루트 값을 확인한다(818).

[104] 그리고, 노드(100)는 계산된 머클 루트 값과 저장된 머클 루트 값을 비교해서 머클 서명을 검증한다(820).

[105] 그리고, 노드(100)는 계산된 머클 루트 값과 저장된 머클 루트 값이 동일하지

여부로 머클 서명에 대한 검증의 성공 유무를 확인한다(822).

[106] 822단계의 확인결과 계산된 머클 루트 값과 저장된 머클 루트 값이 동일하여 검증에 성공으로 확인되면, 노드(100)는 검증하고자 하는 트랜잭션에 관한 검증에 성공했음을 블록체인 시스템의 노드들이 포함된 네트워크로 송신한다(824).

[107] 812단계의 확인결과 트랜잭션 서명의 검증에 실패하거나, 822단계의 확인결과 머클 서명의 검증에 실패하면, 노드(100)는 검증하고자 하는 트랜잭션에 관한 검증에 실패했음을 블록체인 시스템의 노드들이 포함된 네트워크로 송신한다(826).

[108]

[109] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[110] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[111] 실시 예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시 예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[112] 이상과 같이 실시 예들이 비록 한정된 실시 예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[113] 그러므로, 다른 구현들, 다른 실시 예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

청구범위

[청구항 1] 해시 기반 서명 기법을 이용해 트랜잭션에 대한 서명인 트랜잭션 서명을 생성하고, 상기 트랜잭션 서명을 상기 트랜잭션에 저장하는 트랜잭션 서명 생성부;
블록에 포함될 트랜잭션 각각에 대응하는 머클 서명을 생성하고, 상기 머클 서명이 저장된 트랜잭션들을 포함하는 블록을 생성하는 블록 생성부; 및
검증하고자 하는 트랜잭션의 트랜잭션 서명을 검증하고, 상기 검증하고자 하는 트랜잭션의 머클 서명의 검증을 통해서 트랜잭션을 검증하는 트랜잭션 검증부
를 포함하는 해시 기반 서명 기법을 적용한 블록체인 시스템의 노드.

[청구항 2] 제1항에 있어서,
합의 알고리즘에 따른 처리와, 생성된 블록을 블록체인에 연결하고, 블록 헤더를 구성하는 기능을 수행하는 블록체인 기능부; 및
블록체인 시스템의 다른 노드들과 트랜잭션을 송수신하고, 블록을 공유하기 위해 통신을 하는 통신부
를 더 포함하는 해시 기반 서명 기법을 적용한 블록체인 시스템의 노드.

[청구항 3] 제1항에 있어서,
상기 트랜잭션 서명 생성부는,
서명키와 검증키로 이루어진 한쌍의 키를 생성하고, 해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 상기 트랜잭션과 상기 서명키를 이용해서 상기 트랜잭션 서명을 생성하고, 상기 트랜잭션 서명과 상기 검증키를 상기 트랜잭션에 저장하는
해시 기반 서명 기법을 적용한 블록체인 시스템의 노드.

[청구항 4] 제1항에 있어서,
상기 블록 생성부는,
상기 블록에 포함될 트랜잭션 각각의 검증키를 트리의 리프노드에 배치하여 머클 트리를 생성하고, 상기 머클 트리의 머클 루트 값을 상기 블록의 헤더에 저장하고, 상기 블록에 포함될 트랜잭션 각각의 상기 머클 서명을 생성하고, 상기 블록에 포함될 트랜잭션 각각에 상기 머클 서명을 저장하는
해시 기반 서명 기법을 적용한 블록체인 시스템의 노드.

[청구항 5] 제4항에 있어서,
상기 머클 서명은,
트랜잭션 서명, 검증키 및 인증 경로를 포함하고, 상기 인증 경로는 상기 머클 트리 없이도 상기 머클 루트 값을 계산하는데 필요한 것을 특징으로 하는

해시 기반 서명 기법을 적용한 블록체인 시스템의 노드.

[청구항 6] 제1항에 있어서,
상기 트랜잭션 검증부는,
상기 검증하고자 하는 트랜잭션에 저장된 검증키를 이용해서 해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 상기 검증하고자 하는 트랜잭션에 저장된 트랜잭션 서명을 검증하고, 상기 트랜잭션 서명의 검증에 성공하면, 상기 검증하고자 하는 트랜잭션에 저장된 머클 서명을 확인하고, 상기 머클 서명에 포함된 상기 검증키와 인증 경로를 이용하여 머클 루트 값을 계산하고, 상기 검증하고자 하는 트랜잭션을 포함하는 해당 블록의 블록 헤더에 저장된 머클 루트 값을 확인하고, 상기 계산된 머클 루트 값과 상기 저장된 머클 루트 값을 비교해서 동일하면 상기 머클 서명에 대한 검증에 성공했다고 판단하는
해시 기반 서명 기법을 적용한 블록체인 시스템의 노드.

[청구항 7] 제6항에 있어서,
상기 트랜잭션 검증부는,
상기 머클 서명에 대한 검증에 성공하면, 상기 검증하고자 하는 트랜잭션에 관한 검증에 성공했음을 네트워크로 송신하는
해시 기반 서명 기법을 적용한 블록체인 시스템의 노드.

[청구항 8] 제6항에 있어서,
상기 트랜잭션 검증부는,
상기 트랜잭션 서명에 관한 검증에 실패하거나 상기 머클 서명에 관한 검증에 실패하면, 상기 검증하고자 하는 트랜잭션에 관한 검증에 실패했음을 네트워크로 송신하는
해시 기반 서명 기법을 적용한 블록체인 시스템의 노드.

[청구항 9] 해시 기반 서명 기법을 이용해 트랜잭션에 대한 서명인 트랜잭션 서명을 생성하고, 상기 트랜잭션 서명을 상기 트랜잭션에 저장하는 단계;
블록에 포함될 트랜잭션 각각에 대응하는 머클 서명을 생성하고, 상기 머클 서명이 저장된 트랜잭션들을 포함하는 블록을 생성하는 단계: 및
상기 블록에 포함된 트랜잭션들 중에서 검증하고자 하는 트랜잭션의 트랜잭션 서명을 검증하고, 상기 검증하고자 하는 트랜잭션의 머클 서명의 검증을 통해서 트랜잭션을 검증하는 단계
를 포함하는 해시 기반 서명 기법을 적용한 블록체인 시스템에서 트랜잭션을 검증하는 방법.

[청구항 10] 제9항에 있어서,
상기 트랜잭션 서명을 생성하고, 상기 트랜잭션 서명을 상기 트랜잭션에 저장하는 단계는,
서명키와 검증키로 이루어진 한쌍의 키를 생성하는 단계;
해시 기반 OTS(One Time Signature) 알고리즘을 기반으로 상기

트랜잭션과 상기 서명키를 이용해서 상기 트랜잭션 서명을 생성하는 단계; 및
상기 트랜잭션 서명과 상기 검증키를 상기 트랜잭션에 저장하는 단계
를 포함하는 해시 기반 서명 기법을 적용한 블록체인 시스템에서
트랜잭션을 검증하는 방법.

[청구항 11] 제9항에 있어서,
상기 블록을 생성하는 단계는,
상기 블록에 포함될 트랜잭션 각각의 검증키를 트리의 리프노드에
배치하여 머클 트리를 생성하는 단계;
상기 머클 트리의 머클 루트 값을 상기 블록의 헤더에 저장하는 단계;
상기 블록에 포함될 트랜잭션 각각의 상기 머클 서명을 생성하는 단계; 및
상기 블록에 포함될 트랜잭션 각각에 상기 머클 서명을 저장하는 단계
를 포함하는 해시 기반 서명 기법을 적용한 블록체인 시스템에서
트랜잭션을 검증하는 방법.

[청구항 12] 제11항에 있어서,
상기 머클 서명은,
트랜잭션 서명, 검증키 및 인증 경로를 포함하고,
상기 인증 경로는 상기 머클 트리 없이도 상기 머클 루트 값을 계산하는데
필요한 것을 특징으로 하는
해시 기반 서명 기법을 적용한 블록체인 시스템에서 트랜잭션을
검증하는 방법.

[청구항 13] 제9항에 있어서,
상기 트랜잭션을 검증하는 단계는,
상기 검증하고자 하는 트랜잭션에 저장된 검증키를 이용해서 해시 기반
OTS(One Time Signature) 알고리즘을 기반으로 상기 검증하고자 하는
트랜잭션에 저장된 트랜잭션 서명을 검증하는 단계;
상기 트랜잭션 서명의 검증에 성공하면, 상기 검증하고자 하는
트랜잭션에 저장된 머클 서명을 확인하는 단계;
상기 머클 서명에 포함된 상기 검증키와 인증 경로를 이용하여 머클 루트
값을 계산하는 단계;
상기 검증하고자 하는 트랜잭션을 포함하는 해당 블록의 블록 헤더에
저장된 머클 루트 값을 확인하는 단계; 및
상기 계산된 머클 루트 값과 상기 저장된 머클 루트 값을 비교해서
동일하면 상기 머클 서명에 대한 검증에 성공했다고 판단하는 단계
를 포함하는 해시 기반 서명 기법을 적용한 블록체인 시스템에서
트랜잭션을 검증하는 방법.

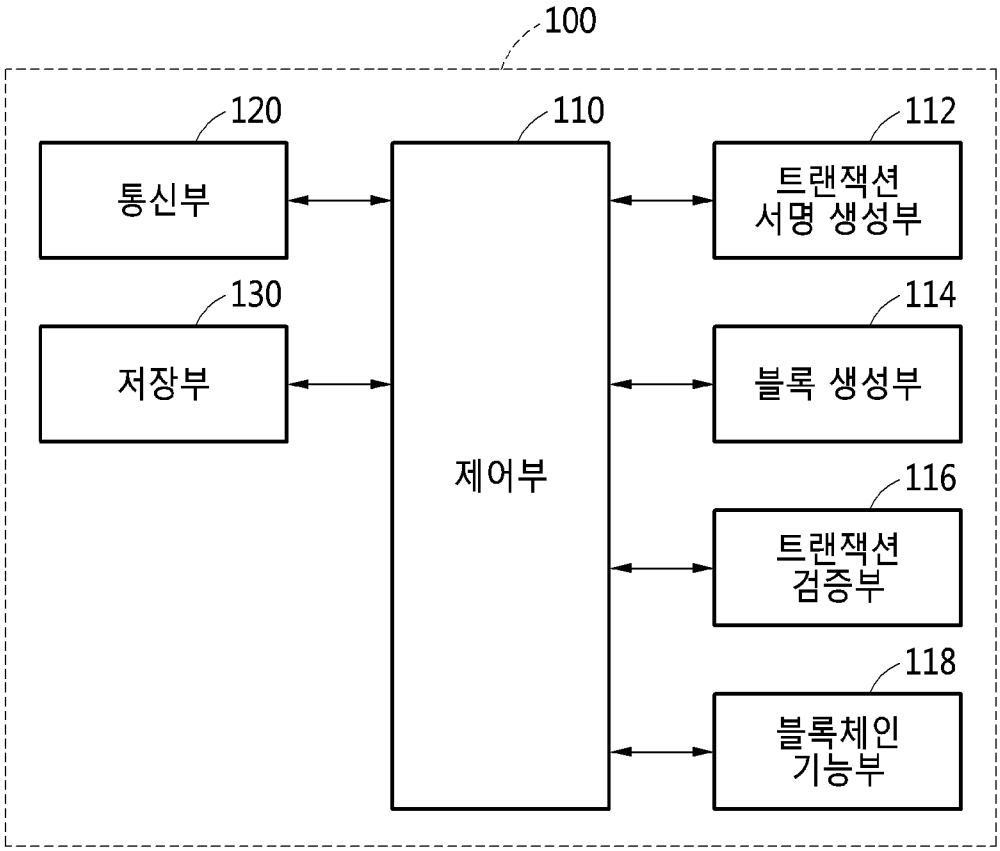
[청구항 14] 제13항에 있어서,
상기 트랜잭션을 검증하는 단계는,

상기 머클 서명에 대한 검증에 성공하면, 상기 검증하고자 하는 트랜잭션에 관한 검증에 성공했음을 네트워크로 송신하는 단계
를 더 포함하는 해시 기반 서명 기법을 적용한 블록체인 시스템에서 트랜잭션을 검증하는 방법.

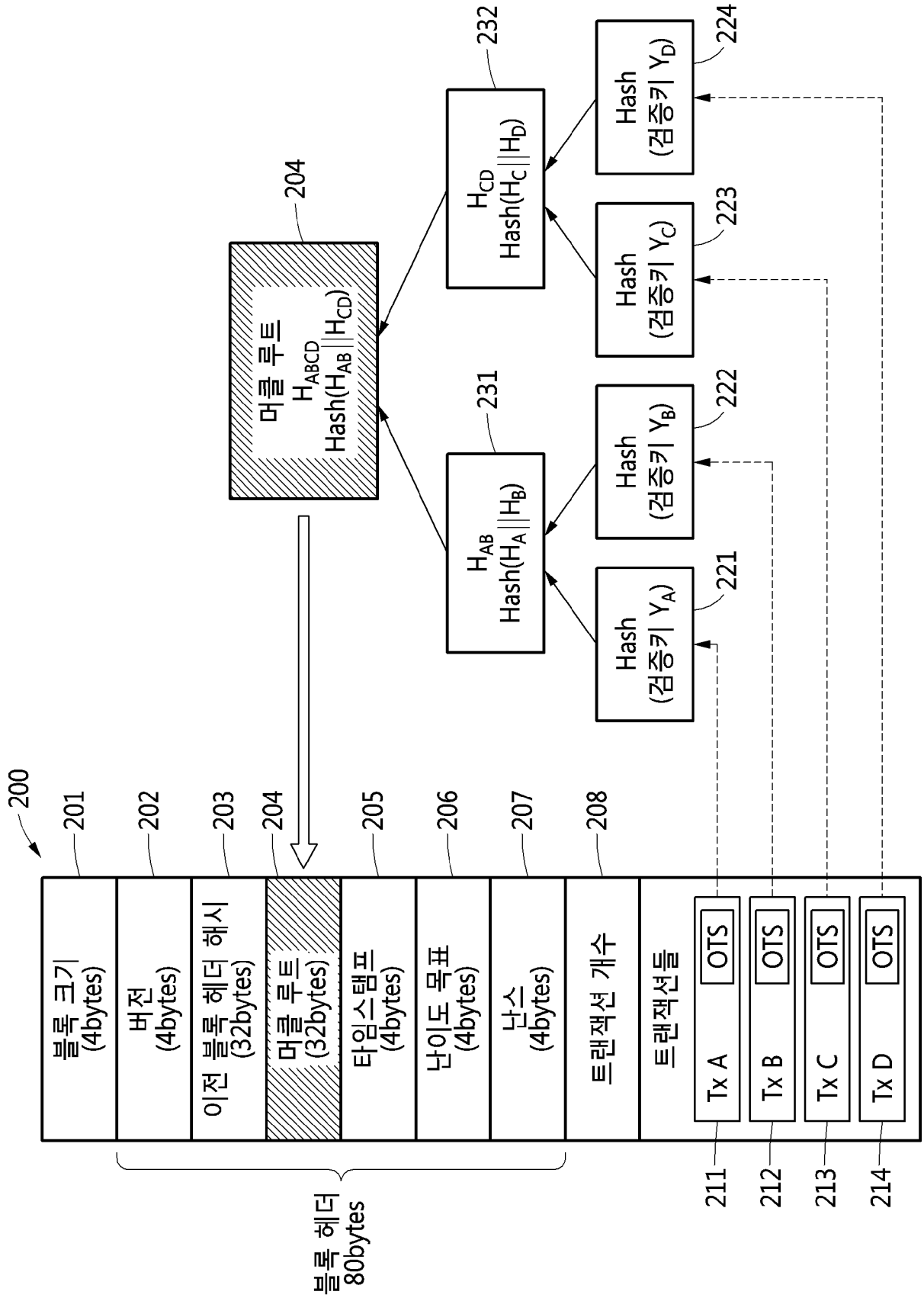
[청구항 15] 제13항에 있어서,
상기 트랜잭션을 검증하는 단계는,
상기 트랜잭션 서명에 관한 검증에 실패하거나 상기 머클 서명에 관한 검증에 실패하면, 상기 검증하고자 하는 트랜잭션에 관한 검증에 실패했음을 네트워크로 송신하는 단계
를 더 포함하는 해시 기반 서명 기법을 적용한 블록체인 시스템에서 트랜잭션을 검증하는 방법.

[청구항 16] 제9항의 방법을 실행하기 위한 프로그램이 기록되어 있는 것을 특징으로 하는 컴퓨터에서 판독 가능한 기록 매체.

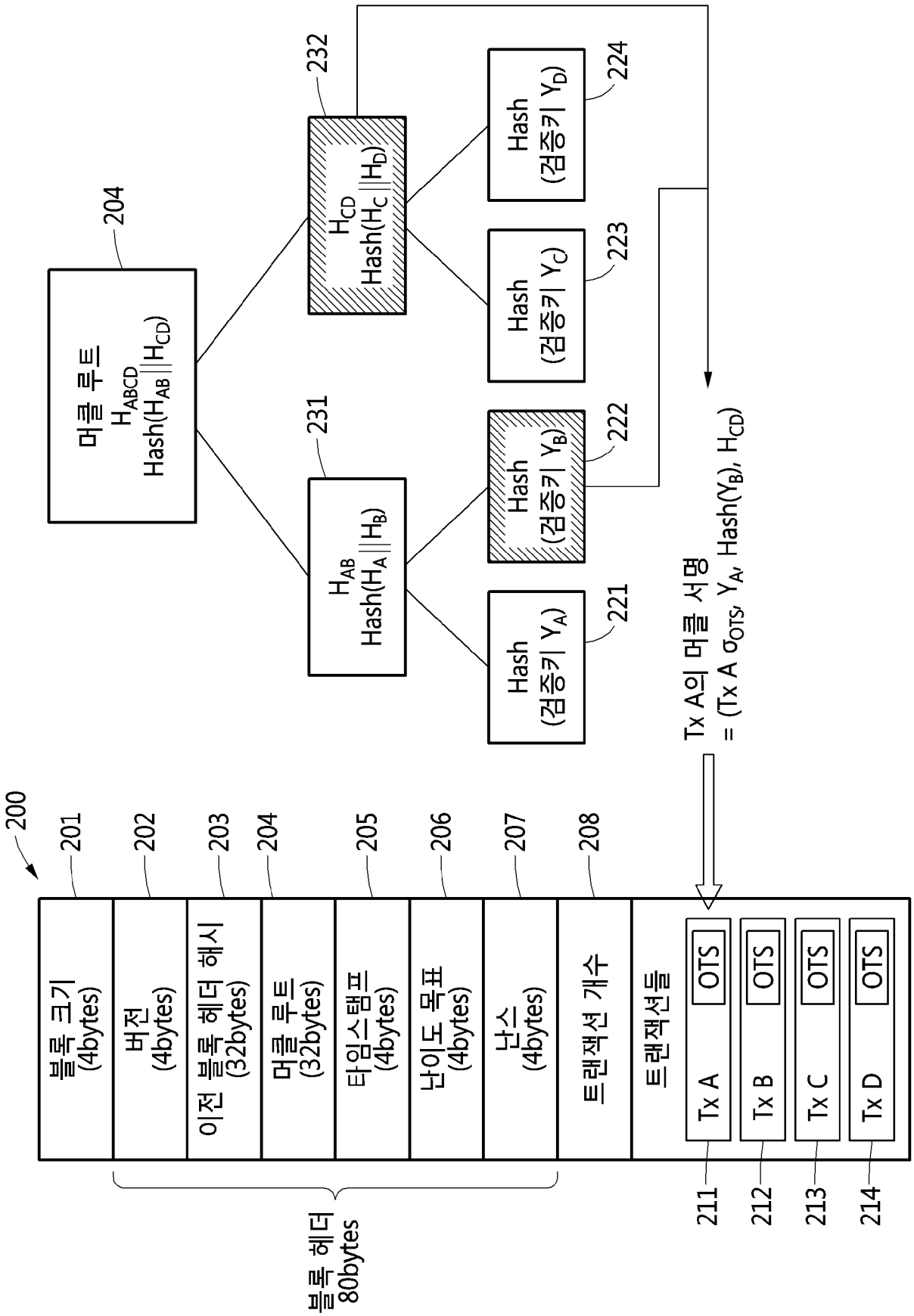
[도1]


100
120
통신부
130
저장부
110
제어부
112
트랜잭션
서명 생성부
114
블록 생성부
116
트랜잭션
검증부
118
블록체인
기능부

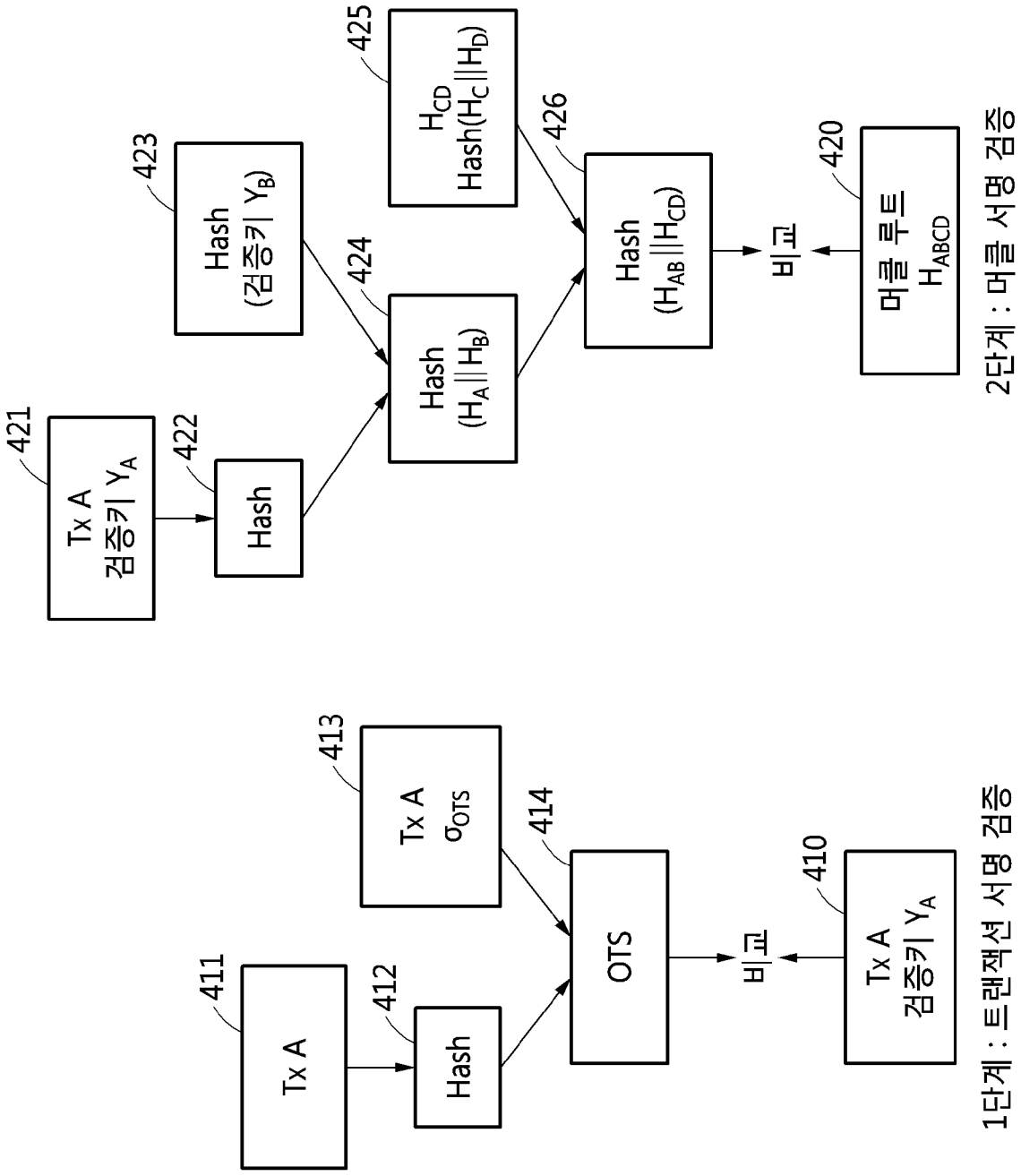
[도2]


200
201
블록 크기 (4bytes)
202
버전 (4bytes)
203
이전 블록 헤더 해시 (32bytes)
204
머클 루트 (32bytes)
205
타임스탬프 (4bytes)
206
난이도 목표 (4bytes)
207
난스 (4bytes)
208
트랜잭션 개수
트랜잭션들
Tx A
OTS
Tx B
OTS
Tx C
OTS
Tx D
OTS
211
212
213
214
블록 헤더 80bytes
204
머클 루트
H_{ABCD}
Hash($H_{AB}||H_{CD}$)
231
H_{AB}
Hash($H_A||H_B$)
232
H_{CD}
Hash($H_C||H_D$)
Hash (검증키 Y_A)
221
Hash (검증키 Y_B)
222
Hash (검증키 Y_C)
223
Hash (검증키 Y_D)
224

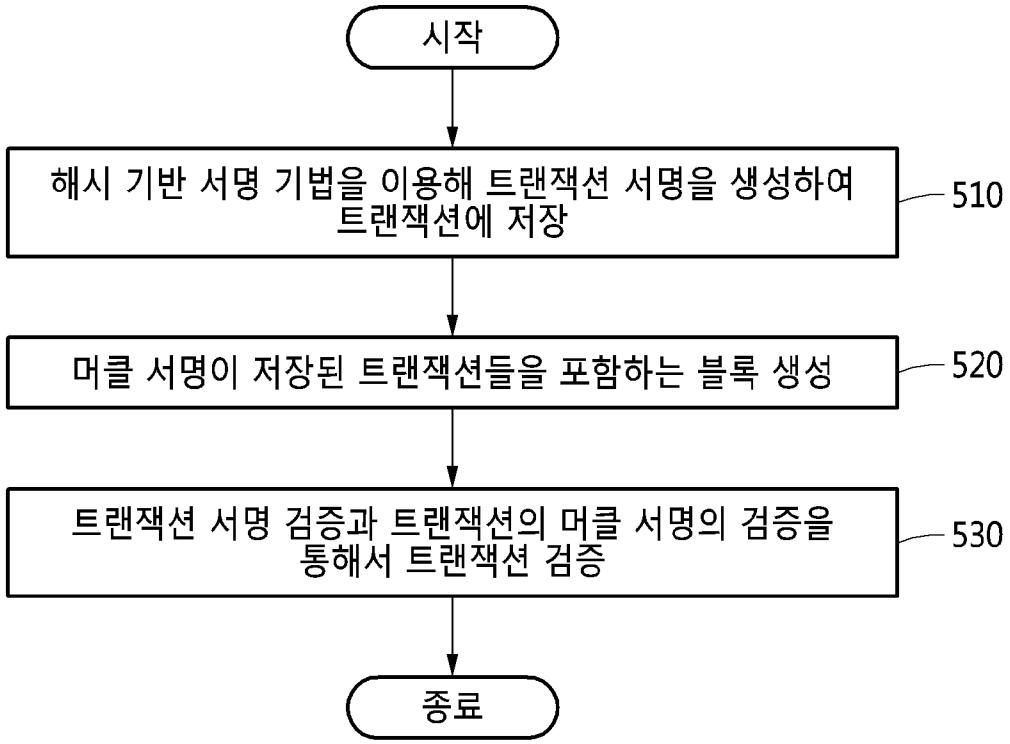
[도3]


200
201
202
203
204
205
206
207
208
블록 크기 (4bytes)
버전 (4bytes)
이전 블록 헤더 해시 (32bytes)
머클 루트 (32bytes)
타임스탬프 (4bytes)
난이도 목표 (4bytes)
난스 (4bytes)
트랜잭션 개수
트랜잭션들
Tx A
OTS
Tx B
OTS
Tx C
OTS
Tx D
OTS
211
212
213
214
블록 헤더 80bytes
Tx A의 머클 서명
= (Tx A σOTS, YA, Hash(YB), HCD)
머클 루트
HABCD
Hash(HAB||HCD)
204
HAB
Hash(HA||HB)
231
HCD
Hash(HC||HD)
232
Hash (검증키 YA)
221
Hash (검증키 YB)
222
Hash (검증키 YC)
223
Hash (검증키 YD)
224

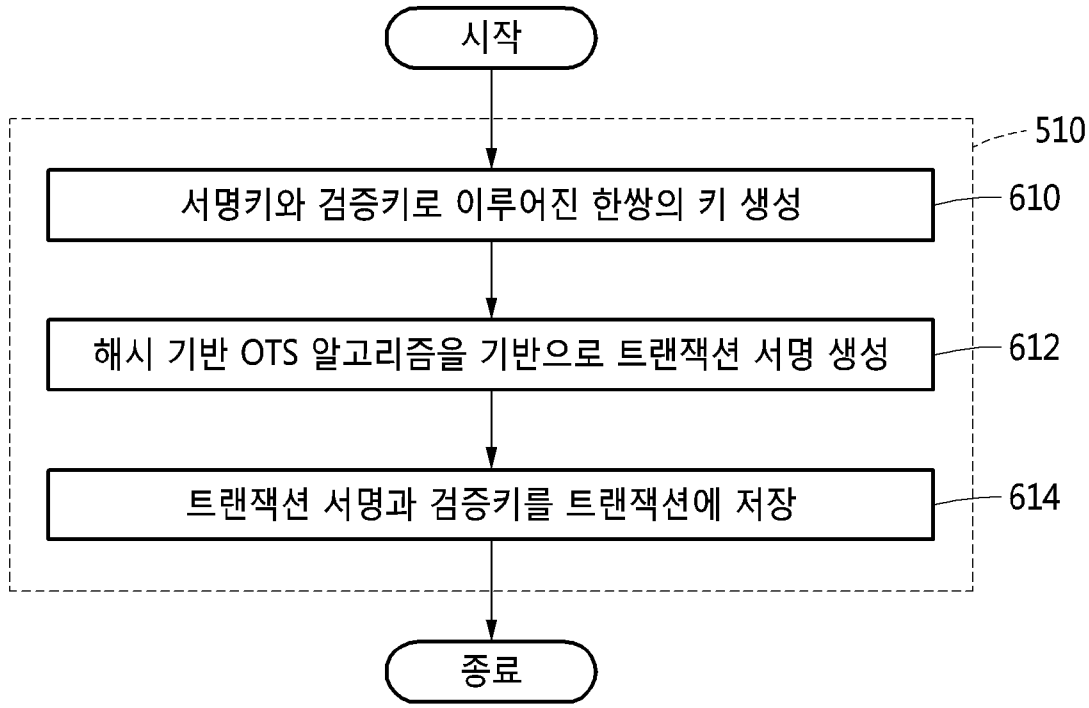
[도4]


421
Tx A
검증키 Y_A
422
Hash
423
Hash
(검증키 Y_B)
424
Hash
($H_A||H_B$)
425
H_{CD}
Hash($H_C||H_D$)
426
Hash
($H_{AB}||H_{CD}$)
비교
420
머클 루트
H_{ABCD}
2단계 : 머클 서명 검증
411
Tx A
412
Hash
413
Tx A
σ_{OTS}
414
OTS
비교
410
Tx A
검증키 Y_A
1단계 : 트랜잭션 서명 검증

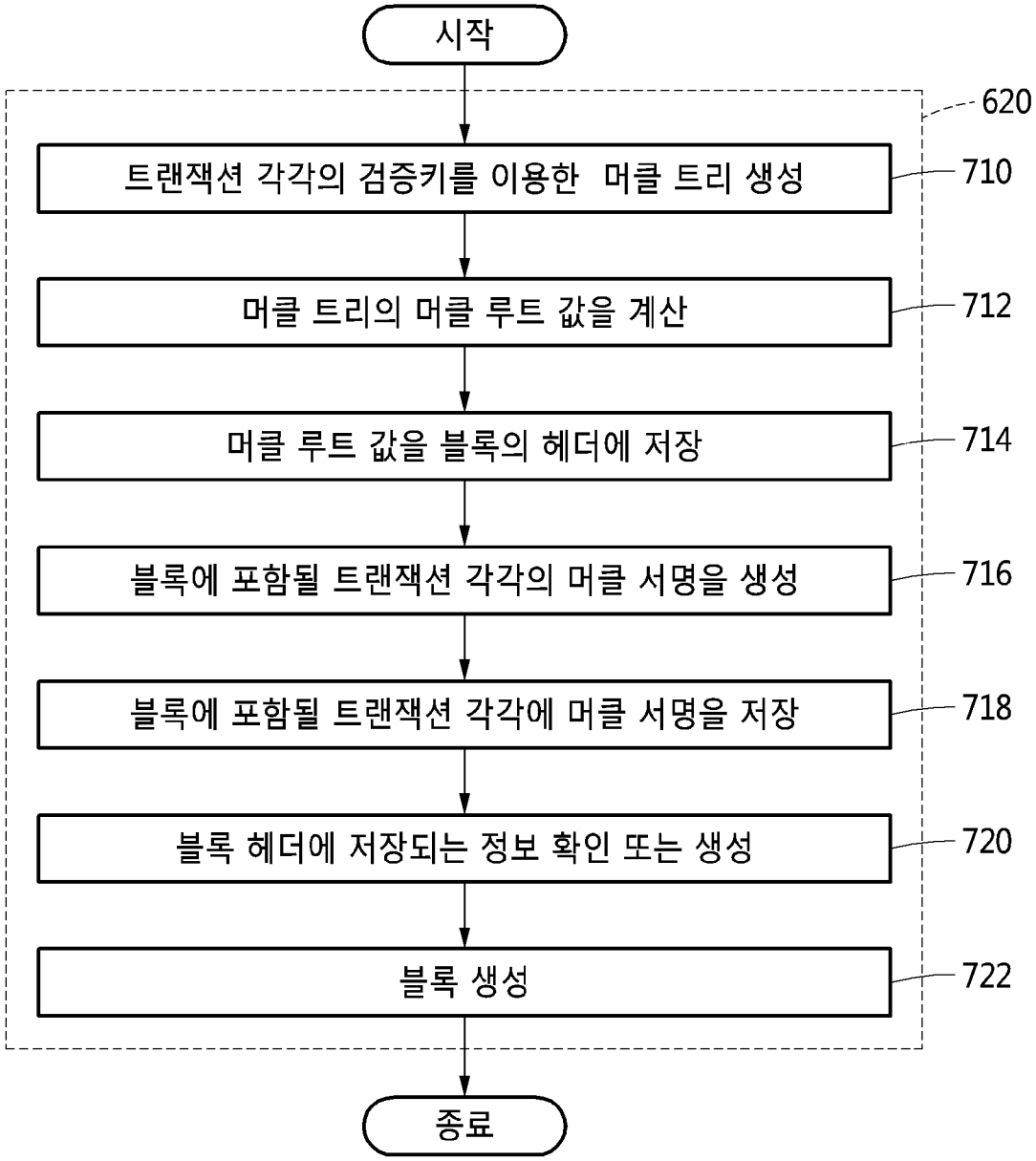
[도5]


시작
해시 기반 서명 기법을 이용해 트랜잭션 서명을 생성하여 트랜잭션에 저장
510
머클 서명이 저장된 트랜잭션들을 포함하는 블록 생성
520
트랜잭션 서명 검증과 트랜잭션의 머클 서명의 검증을 통해서 트랜잭션 검증
530
종료

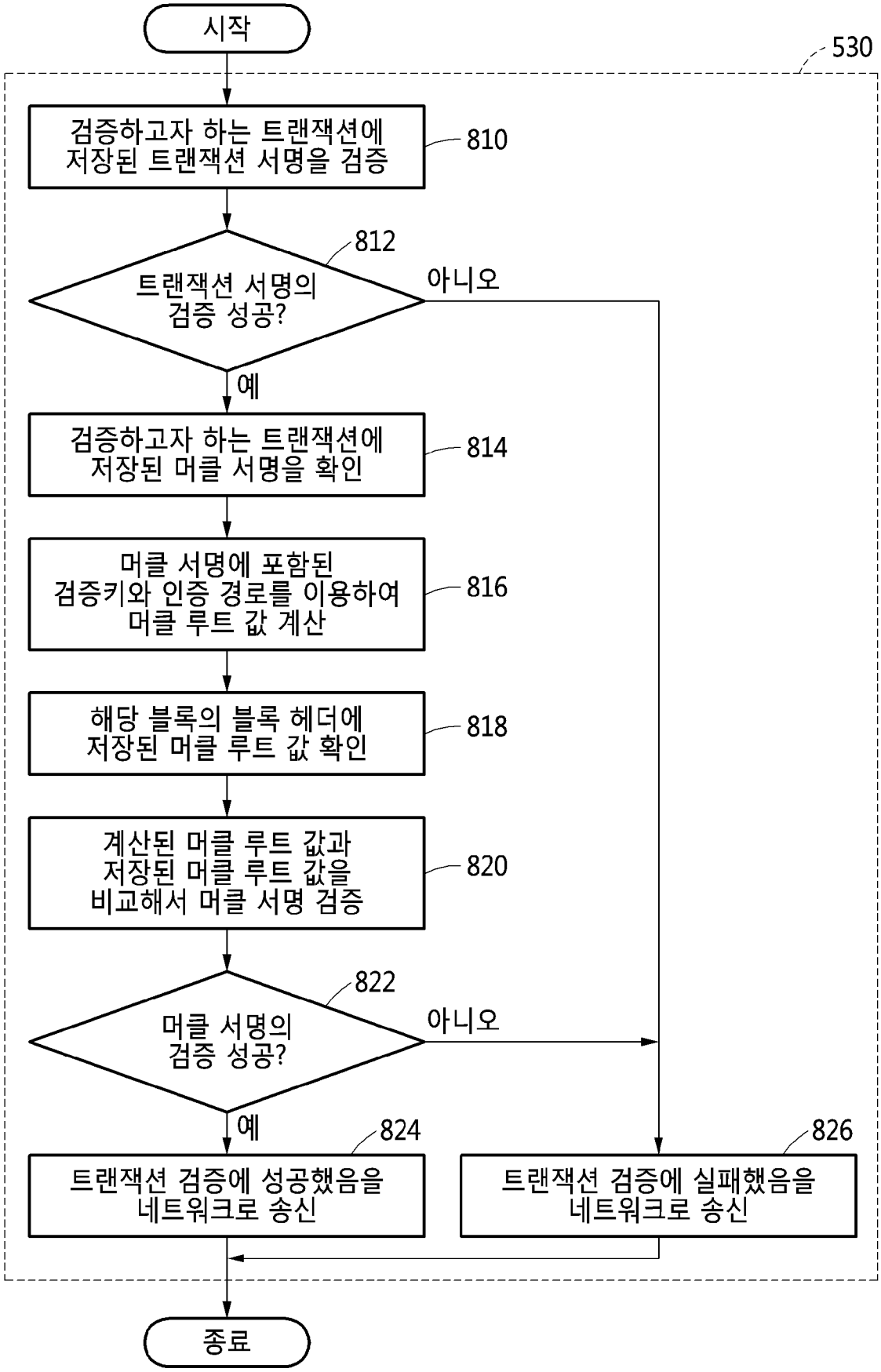
[도6]


시작
510
서명키와 검증키로 이루어진 한쌍의 키 생성
610
해시 기반 OTS 알고리즘을 기반으로 트랜잭션 서명 생성
612
트랜잭션 서명과 검증키를 트랜잭션에 저장
614
종료

[도7]


시작
620
트랜잭션 각각의 검증키를 이용한 머클 트리 생성
710
머클 트리의 머클 루트 값을 계산
712
머클 루트 값을 블록의 헤더에 저장
714
블록에 포함될 트랜잭션 각각의 머클 서명을 생성
716
블록에 포함될 트랜잭션 각각에 머클 서명을 저장
718
블록 헤더에 저장되는 정보 확인 또는 생성
720
블록 생성
722
종료

[도8]


시작
530
검증하고자 하는 트랜잭션에 저장된 트랜잭션 서명을 검증
810
812
트랜잭션 서명의 검증 성공?
아니오
예
검증하고자 하는 트랜잭션에 저장된 머클 서명을 확인
814
머클 서명에 포함된 검증키와 인증 경로를 이용하여 머클 루트 값 계산
816
해당 블록의 블록 헤더에 저장된 머클 루트 값 확인
818
계산된 머클 루트 값과 저장된 머클 루트 값을 비교해서 머클 서명 검증
820
822
머클 서명의 검증 성공?
아니오
예
824
826
트랜잭션 검증에 성공했음을 네트워크로 송신
트랜잭션 검증에 실패했음을 네트워크로 송신
종료

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2017/014684

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)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)
H04L 9/32; G06Q 20/06; H04L 9/12; H04L 9/06; G06Q 20/38; H04L 29/06; H04L 9/30

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: block chain, hash, signature, merkle, one time

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2017-0040079 A (AHN, Kyu Tae et al.) 12 April 2017 See claims 1-11 and figure 4.	1-16
A	US 2017-0132621 A1 (SWFL, INC., D/B/A "FILAMENT") 11 May 2017 See claim 1 and figure 5.	1-16
A	WO 2017-079652 A1 (PULSIFER, Allen) 11 May 2017 See claims 4-7 and figure 9.	1-16
A	US 2017-0033932 A1 (GUARDTIME IP HOLDINGS LIMITED) 02 February 2017 See claims 1-13 and figure1.	1-16
A	US 2016-0283920 A1 (FISHER, Justin et al.) 29 September 2016 See claims 1-19 and figure1.	1-16
X	BAE, Bong Jin, Hash-based Signature Scheme for Blockchain, 20 June 2017, Master's Thesis, Pusan National University See pages 30-34. * The above document is a known document declaring exceptions to lack of novelty by the applicant.	1-16

☐ 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
02 AUGUST 2018 (02.08.2018)	**02 AUGUST 2018 (02.08.2018)**
Name and mailing address of the ISA/KR 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	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2017/014684

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2017-0040079 A	12/04/2017	WO 2017-192007 A2	09/11/2017
		WO 2017-192007 A3	04/01/2018
US 2017-0132621 A1	11/05/2017	US 2017-0132619 A1	11/05/2017
		US 2017-0132620 A1	11/05/2017
		US 2017-0134937 A1	11/05/2017
WO 2017-079652 A1	11/05/2017	NONE	
US 2017-0033932 A1	02/02/2017	EP 3031169 A1	15/06/2016
		US 2015-0039893 A1	05/02/2015
		US 9473306 B2	18/10/2016
		US 9853819 B2	26/12/2017
		WO 2015-018516 A1	12/02/2015
US 2016-0283920 A1	29/09/2016	NONE	

국 제 조 사 보 고 서

국제출원번호
PCT/KR2017/014684

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 9/32(2006.01)i, H04L 9/06(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 9/32; G06Q 20/06; H04L 9/12; H04L 9/06; G06Q 20/38; H04L 29/06; H04L 9/30

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: block chain, hash, signature, merkle, one time

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	KR 10-2017-0040079 A (안규태 등) 2017.04.12 청구항 1-11과 도4 참조.	1-16
A	US 2017-0132621 A1 (SWFL, INC., D/B/A "FILAMENT") 2017.05.11 청구항 1과 도5 참조.	1-16
A	WO 2017-079652 A1 (PULSIFER, ALLEN) 2017.05.11 청구항 4-7과 도9 참조.	1-16
A	US 2017-0033932 A1 (GUARDTIME IP HOLDINGS LIMITED) 2017.02.02 청구항 1-13과 도1 참조.	1-16
A	US 2016-0283920 A1 (JUSTIN FISHER 등) 2016.09.29 청구항 1-19와 도1 참조.	1-16
X	배봉진, 블록체인에 대한 해시 기반 서명 기법 적용방안, 2017.6.20., 부산대학교 석사학위청구논문 페이지 30-34 참조. * 위 문헌은 출원인이 신규성 상실의 예외로서 선언한 공지문헌임.	1-16

☐ 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
2018년 08월 02일 (02.08.2018)	2018년 08월 02일 (02.08.2018)

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

심사관
김성우
전화번호 +82-42-481-3348

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2017/014684

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2017-0040079 A	2017/04/12	WO 2017-192007 A2	2017/11/09
		WO 2017-192007 A3	2018/01/04
US 2017-0132621 A1	2017/05/11	US 2017-0132619 A1	2017/05/11
		US 2017-0132620 A1	2017/05/11
		US 2017-0134937 A1	2017/05/11
WO 2017-079652 A1	2017/05/11	없음	
US 2017-0033932 A1	2017/02/02	EP 3031169 A1	2016/06/15
		US 2015-0039893 A1	2015/02/05
		US 9473306 B2	2016/10/18
		US 9853819 B2	2017/12/26
		WO 2015-018516 A1	2015/02/12
US 2016-0283920 A1	2016/09/29	없음	