

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국



(10) 국제공개번호

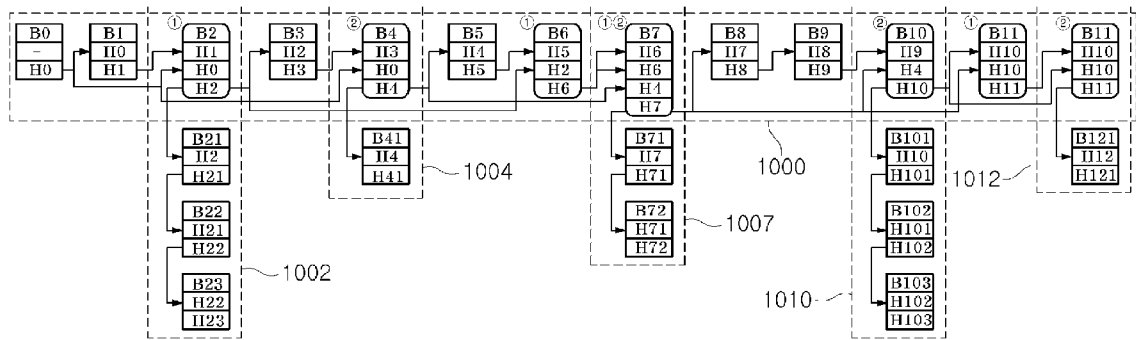
(43) 국제공개일
2019년 10월 3일 (03.10.2019) WIPO | PCT

WO 2019/190234 A1

- (51) 국제특허분류: H04L 29/08 (2006.01) H04L 9/06 (2006.01)
- (21) 국제출원번호: PCT/KR2019/003656
- (22) 국제출원일: 2019년 3월 28일 (28.03.2019)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보: 10-2018-0035587 2018년 3월 28일 (28.03.2018) KR
- (71) 출원인: 주식회사 엑스블록시스템즈 (XBLOCK-SYSTEMS CO., LTD.) [KR/KR]; 06026 서울시 강남구 도산대로207 성도빌딩 7층, Seoul (KR).
- (72) 발명자: 김승기 (KIM, Seung Ki); 12222 경기도 남양주시 평내로 113, 1505-1703, Gyeonggi-do (KR). 박경옥 (PARK, Kyeong Ok); 13483 경기도 성남시 분당구 판교원로 237, 703동 902호, Gyeonggi-do (KR). 권용석 (KWON, Yong Seok); 12141 경기도 남양주시 천마산로 65, 116동 903호, Gyeonggi-do (KR).
- (74) 대리인: 이버드특허법인 (E-BIRD INTERNATIONAL IP LAW FIRM); 06158 서울시 강남구 테헤란로 437 삼영빌딩 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 국내 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,

(54) Title: BLOCKCHAIN SYSTEM

(54) 발명의 명칭: 블록체인 시스템



(57) Abstract: A blockchain system is disclosed. A blockchain system of the present invention comprises a main branch including a genesis block, at least one first-type block, and at least one second-type block, wherein: the blocks included in the main branch are respectively connected according to the generation order of blocks, starting from the genesis block; a block included in the main branch, excluding the genesis block, includes a hash value of at least a portion of a block generated immediately before the corresponding block in the main branch; at least a portion of the first-type block includes a hash value of at least a portion of a first-type block generated immediately before the corresponding first-type block in the main branch; at least a portion of the second-type block includes a hash value of at least a portion of a second-type block generated immediately before the corresponding second-type block in the main branch; and the main branch includes at least one overlapping block, which is the first-type block while also being the second-type block.

(57) 요약서: 블록체인 시스템이 개시된다. 본 발명의 블록체인 시스템은, 블록체인 시스템에 있어서, 최초(genesis) 블록, 적어도 하나의 제1형 블록 및 적어도 하나의 제2형 블록을 포함하는 메인 브랜치를 포함하고, 상기 메인 브랜치에 포함된 블록은 상기 최초 블록을 시작으로 각각 블록의 생성 순서에 따라 연결되고, 상기 최초 블록을 제외한 상기 메인 브랜치에 포함된 블록은 상기 메인 브랜치에서 해당 블록 직전에 생성된 블록의 적어도 일부의 해시값을 포함하고, 상기 제1형 블록 중 적어도 일부는 상기 메인 브랜치에서 해당 제1형 블록 직전에 생성된 제1형 블록의 적어도 일부의 해시값을 포함하고, 상기 제2형 블록 중 적어도 일부는 상기 메인 브랜치에서 해당 제2형 블록 직전에 생성된 제2형 블록의 적어도 일부의 해시값을 포함하고, 상기 메인 브랜치는 상기 제1형 블록이면서 동시에 상기 제2형 블록인 적어도 하나의 중첩 블록을 포함한다.

WO 2019/190234 A1

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 시스템

기술분야

- [1] 본 발명은 블록체인 시스템에 관한 것으로, 더욱 상세하게는 적어도 일부의 블록들이 이중으로 연결되면서, 또한 이중으로 연결된 것 중에서 중첩된 블록을 포함하는 블록체인 시스템에 관한 것이다.

배경기술

- [2] 블록체인은 분산 데이터베이스의 일종으로 암호화된 가상화폐인 비트코인에서 도입된 개념으로 알려져 있다. 기존에 거래장부, 문서 등의 디지털 콘텐츠를 중앙집중형 서버에 보관하고 관리하던 것과 달리, 블록체인 시스템에서는 누적된 디지털 콘텐츠를 네트워크를 통해 연결된 복수의 참여자의 장치(노드)에 저장하여 관리한다. 이러한 블록체인 시스템은 디지털 콘텐츠 자체가 인터넷을 통해 공개되어 있고, 다수의 참여자에 의해 수시로 검증이 진행되므로 위조 또는 변조가 매우 어렵다는 장점이 있다.
- [3] 이러한 블록체인 시스템은 비트코인 등의 가상화폐 시스템 또는 금융기관의 거래기록 보관 등에 사용되고 있다. 또한, 최근에는 이러한 블록체인 시스템을 전자화된 문서관리 및 원본확인 등을 위해 사용되기도 한다. 대한민국 등록특허공보 제10-1763827호(2017년 7월 26일 등록) 및 대한민국 등록특허공보 제10-1751025호(2017년 6월 20일 등록)에는 이러한 블록체인 시스템을 이용한 의료데이터전송시스템 및 증권업무 처리 시스템에 대해서 개시되어 있다.
- [4] 블록체인에 참여하는 노드들은 데이터의 진위여부를 확인하기 위해서 전체 블록체인의 데이터를 장치에 저장하고 유지관리 해야 한다. 누적된 거래 등이 적어 전체 블록체인의 크기가 크지 않은 경우에는 문제되지 않으나, 거래 등 신규 이벤트 발생이 누적되면서 블록의 개수가 증가할수록 전체 블록체인의 크기는 점차 증가하게 된다. 대표적인 블록체인 시스템인 비트코인 및 이더리움 등의 전체 블록체인 크기는 현재 수백 Gbyte에 달하고 있다.
- [5] 따라서 블록체인에 참여하는 노드들은 이러한 대용량의 데이터를 저장하고 유지관리할 수 있는 높은 수준의 저장 장치 및 컴퓨팅 장치가 필요하다. 그러나 일반적인 개인용 컴퓨터는 이러한 수준의 성능에 도달하지 못할 수 있다. 특히, 스마트폰, 태블릿 컴퓨터 등 개인용 모바일 장치는 더욱 이러한 수준의 성능에 도달하지 못하는 실정이다.
- [6] 선행기술문헌
- [7] 대한민국 등록특허공보 제10-1763827호(2017년 7월 26일 등록)
- [8] 대한민국 등록특허공보 제10-1751025호(2017년 6월 20일 등록)

발명의 상세한 설명

기술적 과제

- [9] 본 발명이 해결하려는 과제는, 블록체인 시스템에 참여하는 노드가 필요한 블록들만을 선택적으로 저장하는 것만으로도 데이터의 진위여부를 확인할 수 있는 블록체인 시스템 및 이러한 블록체인을 이용한 데이터 관리 방법을 제공하는 것이다.
- [10] 본 발명이 해결하려는 다른 과제는, 블록의 유형에 따라 블록 간의 연결관계를 다르게 형성하여 체계적인 효율적인 블록체인 시스템을 제공하는 것이다.

과제 해결 수단

- [11] 상기 과제를 해결하기 위한 본 발명의 블록체인 시스템은, 블록체인 시스템에 있어서, 최초(genesis) 블록, 적어도 하나의 제1 형 블록 및 적어도 하나의 제2 형 블록을 포함하는 메인 브랜치를 포함하고, 상기 메인 브랜치에 포함된 블록은 상기 최초 블록을 시작으로 각각 블록의 생성 순서에 따라 연결되고, 상기 최초 블록을 제외한 상기 메인 브랜치에 포함된 블록은 상기 메인 브랜치에서 해당 블록 직전에 생성된 블록의 적어도 일부의 해시값을 포함하고, 상기 제1 형 블록 중 적어도 일부는 상기 메인 브랜치에서 해당 제1 형 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 포함하고, 상기 제2 형 블록 중 적어도 일부는 상기 메인 브랜치에서 해당 제2 형 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 포함하고, 상기 메인 브랜치는 상기 제1 형 블록이면서 동시에 상기 제2 형 블록인 적어도 하나의 중첩 블록을 포함한다.
- [12] 본 발명의 일 실시예에 있어서, 상기 중첩 블록은, 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 블록의 적어도 일부의 해시값, 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값 및 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 포함할 수 있다.
- [13] 본 발명의 일 실시예에 있어서, 상기 중첩 블록은, 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 블록의 적어도 일부의 해시값, 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값 및 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 각각 구분하여 포함할 수 있다.
- [14] 본 발명의 일 실시예에 있어서, 상기 메인 브랜치에서 상기 중첩 블록 직후에 생성된 제1 형 블록은, 상기 메인 브랜치에서 해당 제1 형 블록 직전에 생성된 블록의 적어도 일부의 해시값과 상기 중첩 블록의 적어도 일부의 해시값을 포함할 수 있다.
- [15] 본 발명의 일 실시예에 있어서, 상기 메인 브랜치에서 상기 중첩 블록 직후에 생성된 제2 형 블록은, 상기 메인 브랜치에서 해당 제2 형 블록 직전에 생성된 블록의 적어도 일부의 해시값과 상기 중첩 블록의 적어도 일부의 해시값을 포함할 수 있다.
- [16] 본 발명의 일 실시예에 있어서, 상기 적어도 일부의 제1 형 블록은 상기 직전에

- 생성된 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 구분하여 포함할 수 있다.
- [17] 본 발명의 일 실시예에 있어서, 상기 적어도 일부의 제2 형 블록은 상기 직전에 생성된 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 구분하여 포함할 수 있다.
- [18] 본 발명의 일 실시예에 있어서, 상기 적어도 일부의 제1 형 블록이 포함하는 상기 직전에 생성된 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값이 동일한 경우, 하나의 해시값만을 포함할 수 있다.
- [19] 본 발명의 일 실시예에 있어서, 상기 적어도 일부의 제2 형 블록이 포함하는 상기 직전에 생성된 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제2 형 블록의 적어도 일부의 해시값이 동일한 경우, 하나의 해시값만을 포함할 수 있다.
- [20] 본 발명의 일 실시예에 있어서, 상기 제1 형 블록은 제1 형 블록 중 가장 먼저 생성된 최초 제1 형 블록 및 상기 최초 제1 형 블록 이후에 생성된 후속 제1 형 블록을 포함하고, 상기 후속 제1 형 블록은 상기 메인 브랜치에서 해당 후속 제1 형 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 포함할 수 있다.
- [21] 본 발명의 일 실시예에 있어서, 상기 최초 제1 형 블록은 상기 최초 블록의 적어도 일부의 해시값을 포함할 수 있다.
- [22] 본 발명의 일 실시예에 있어서, 상기 최초 제1 형 블록은 상기 최초 제1 형 블록 직전 블록의 적어도 일부의 해시값을 포함하고, 다른 블록의 적어도 일부의 해시값은 포함하지 않을 수 있다.
- [23] 본 발명의 일 실시예에 있어서, 상기 제2 형 블록은 제2 형 블록 중 가장 먼저 생성된 최초 제2 형 블록 및 상기 최초 제2 형 블록 이후에 생성된 후속 제2 형 블록을 포함하고, 상기 후속 제2 형 블록은 상기 메인 브랜치에서 해당 후속 제2 형 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 포함할 수 있다.
- [24] 본 발명의 일 실시예에 있어서, 상기 최초 제2 형 블록은 상기 최초 블록의 적어도 일부의 해시값을 포함할 수 있다.
- [25] 본 발명의 일 실시예에 있어서, 상기 최초 제2 형 블록은 상기 최초 제2 형 블록 직전 블록의 적어도 일부의 해시값을 포함하고, 다른 블록의 적어도 일부의 해시값은 포함하지 않을 수 있다.
- [26] 본 발명의 일 실시예에 있어서, 상기 제1 형 블록 및 상기 제2 형 블록은 해당 제1 형 블록 및 제2 형 블록을 루트 블록으로 하는 포킹을 허용할 수 있다.
- [27] 본 발명의 일 실시예에 있어서, 상기 제1 형 블록 및 상기 제2 형 블록 중 적어도 일부를 루트 블록으로 하여 서브 블록이 연결되는 것을 허용할 수 있다.
- [28] 본 발명의 일 실시예에 있어서, 상기 제1 형 블록 및 상기 제2 형 블록 중 적어도 일부를 루트 블록으로 하여 포킹된 서브 브랜치를 더 포함할 수 있다.
- [29] 본 발명의 일 실시예에 있어서, 상기 제1 형 블록 및 상기 제2 형 블록 중 적어도

일부를 루트 블록으로 하여 연결된 적어도 하나의 서브 블록을 포함하는 서브 브랜치를 더 포함할 수 있다.

발명의 효과

- [30] 본 발명의 일 실시예에 따른 블록체인 시스템 및 블록체인을 이용한 데이터 관리 방법은 블록체인 시스템에 참여하는 노드가 필요한 블록들만을 선택적으로 저장하는 것만으로도 데이터의 진위여부를 확인할 수 있는 장점이 있다.
- [31] 또한, 본 발명의 일 실시예에 따른 블록체인 시스템은 블록의 유형에 따라 블록 간의 연결관계를 다르게 형성하여 체계적인 효율적이라는 장점이 있다.

도면의 간단한 설명

- [32] 도 1은 본 발명의 일 실시예에 따른 블록체인 시스템의 개별 블록의 구성을 도시한 것이다.
- [33] 도 2는 본 발명의 일 실시예에 따른 블록체인 시스템의 두 개의 블록이 연결된 것을 도시한 것이다.
- [34] 도 3 및 도 4는 블록체인에서 블록의 표시 방법을 설명하기 위한 도면이다.
- [35] 도 5는 본 발명의 일 실시예에 따른 블록체인 시스템의 예시적인 블록도이다.
- [36] 도 6은 본 발명의 다른 일 실시예에 따른 블록체인 시스템의 예시적인 블록도이다.

발명의 실시를 위한 최선의 형태

- [37] 이하, 첨부된 도면을 참조하여 본 발명의 실시예들을 상세히 설명한다. 본 발명을 설명하는데 있어서, 해당 분야에 이미 공지된 기술 또는 구성에 대한 구체적인 설명을 부가하는 것이 본 발명의 요지를 불분명하게 할 수 있다고 판단되는 경우에는 상세한 설명에서 이를 일부 생략하도록 한다. 또한, 본 명세서에서 사용되는 용어들은 본 발명의 실시예들을 적절히 표현하기 위해 사용된 용어들로서, 이는 해당 분야의 관련된 사람 또는 관례 등에 따라 달라질 수 있다. 따라서, 본 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [38] 여기서 사용되는 전문용어는 단지 특정 실시예를 언급하기 위한 것이며, 본 발명을 한정하는 것을 의도하지 않는다. 여기서 사용되는 단수 형태들은 문구들이 이와 명백히 반대의 의미를 나타내지 않는 한 복수 형태들도 포함한다. 명세서에서 사용되는 '포함하는'의 의미는 특정 특성, 영역, 정수, 단계, 동작, 요소 및/또는 성분을 구체화하며, 다른 특정 특성, 영역, 정수, 단계, 동작, 요소, 성분 및/또는 군의 존재나 부가를 제외시키는 것은 아니다.
- [39]
- [40] 이하, 첨부된 도 1 내지 도 5를 참조하여 본 발명의 일 실시예에 따른 블록체인 시스템에 대해서 설명하도록 한다.
- [41] 도 1은 본 발명의 일 실시예에 따른 블록체인 시스템의 개별 블록의 구성을

도시한 것이다. 도 2는 본 발명의 일 실시예에 따른 블록체인 시스템의 두 개의 블록이 연결된 것을 도시한 것이다.

[42] 도 1을 참조하면, 하나의 블록(100)은 블록헤더(110) 및 블록몸체(120)를 포함한다.

[43] 블록헤더(110)는 블록의 타이틀, 직전 블록의 해시값, 블록몸체의 해시값, 타임스탬프, 난이도 목표 및 난스 등을 포함할 수 있다. 블록헤더(110)가 포함하는 정보는 다양하게 변경되어 구성될 수 있다.

[44] 블록의 타이틀은 블록(100)을 다른 블록과 구분할 수 있는 식별 정보를 의미한다. 블록의 타이틀은 다른 블록과의 연결 관계에 따라 정해질 수 있다.

[45] 직전 블록의 해시값은 브랜치에서 해당 블록 이전에 생성되어 해당 블록과 연결되는 블록의 해시값이다. 직전 블록의 해시값은 직전 블록의 전체 또는 선택된 일부의 정보의 해시값일 수 있다. 예를 들어, 직전 블록의 해시값은 직전 블록의 블록헤더의 정보의 해시값인 것으로 정의될 수 있다. 블록헤더에 직전 블록의 해시값이 포함됨으로서, 블록 간의 연결성이 강화될 수 있다. 블록 간의 연결성이 강화되는 것은 블록체인 시스템 전체의 보안성이 향상되는 것을 의미한다.

[46] 블록몸체의 해시값은 해당 블록의 블록몸체(120)가 포함하는 데이터의 해시값이다. 후술하는 것과 같이, 블록몸체(120)는 데이터를 포함한다. 블록몸체의 해시값은 블록몸체가 포함하는 데이터의 전체 또는 선택된 일부의 해시값일 수 있다. 블록몸체의 해시값은 다양한 방식으로 결정될 수 있다. 예를 들어, 블록몸체의 해시값은 블록몸체(120)의 데이터로부터 생성된 머클 트리의 루트에 대한 해시값일 수 있다. 블록몸체의 해시값은 블록몸체(120)의 데이터의 요약본에 해당하는 것으로, 상대적으로 크기가 큰 블록몸체(120)의 데이터를 효율적으로 관리하고 검증할 수 있게 한다.

[47] 타임스탬프(time stamp)는 해당 블록의 생성시간에 관한 정보이다.

[48] 난이도 목표는 해당 블록의 작업증명 알고리즘에 대한 난이도 목표이다. 이는 해당 블록의 난스를 찾는 데 필요한 해싱과워를 결정하는 것에 관한 정보이다.

[49] 난스(nonce)는 해당 블록의 작업증명 알고리즘에 사용되는 카운터 정보이다.

[50] 블록헤더(110)에는 상술한 정보 중 일부가 제외될 수도 있고, 다른 정보가 추가로 포함될 수도 있다.

[51] 블록몸체(120)는 블록(100)이 저장하고 관리하는 데이터를 포함한다. 데이터는 디지털 데이터에 해당한다. 데이터는 다양한 형태의 자료일 수 있다. 예를 들어, 데이터는 디지털 콘텐츠, 문서 정보, 계좌 정보, 의료 정보, 진료 정보, 행정 정보, 등기부 정보, 코인의 발생 정보, 거래 정보, 인사 정보, 생산 이력 정보, 제품 또는 건축물의 설계 및 도면, 사운드 정보 등이 가능하며, 특정한 형태로 한정되는 것은 아니다.

[52] 블록몸체(120)가 포함하는 데이터는 블록에 따라서 종류 또는 크기 등이 제한될 수 있다. 이러한 데이터의 제한은 모든 블록에 공통으로 적용될 수도

있고, 특정한 몇몇 블록에만 선택적으로 적용될 수도 있다. 또한, 이러한 데이터의 제한은 필요에 따라 변경될 수 있다.

[53]

[54] 도 2를 참조하면, 두 개의 블록은 서로 연결될 수 있다. 구체적으로, 복수의 블록은 순차적으로 연결되어 브랜치를 형성할 수 있다. 여기서, 브랜치란 복수의 블록들이 서로 선형적으로 연결된 블록들의 집합을 의미한다. 도 2에는 이러한 브랜치에서 임의의 두 개의 블록이 연결된 상태가 도시되어 있다.

[55]

도 2를 참조하면, 브랜치에서 임의의 하나의 블록(200)은 브랜치 내에서 이전에 생성된 블록(100)과 연결되게 된다. 여기서, 연결된다는 것은 해당 블록(200)이 이전에 생성된 블록(100)의 적어도 일부의 해시값을 포함하는 것을 의미한다. 구체적으로, 블록(200)은 블록헤더(210)에 이전에 생성된 블록(100)의 적어도 일부의 해시값을 포함하는 것을 통해 연결될 수 있다.

[56]

이전에 생성된 블록(100)이란 해당 블록(200) 직전에 생성된 것일 수 있다. 아래에서 상세하게 설명하겠지만, 경우에 따라서 이전에 생성된 블록(100)이란 이전에 생성된 블록들 중 해당 블록(200)과 동일한 유형의 마지막 블록일 수도 있다.

[57]

이전에 생성된 블록(100)의 해시값은 상술한 것과 같이, 이전 블록(100)의 전체 또는 선택된 일부의 정보의 해시값일 수 있다. 예를 들어, 첨부한 도 2에 도시된 것과 같이 이전 블록(100)의 해시값은 이전 블록의 블록헤더(110)의 정보의 해시값인 것으로 정의될 수 있다. 이전 블록의 해시값은 블록을 설계하는 사람의 기호 및 판단에 따라 다양하게 변경될 수 있다.

[58]

[59]

도 3 및 도 4를 참조하여, 도 5에서 도시되는 블록체인 시스템을 구성하는 블록에 대해서 간략하게 설명하도록 한다.

[60]

블록은 도 1 및 도 2를 참조하여 설명한 것과 같이, 블록헤더와 블록몸체를 포함한다. 그러나 설명의 편의성을 위해 도 5에서는 도 3 및 도 4에 도시된 방식으로 개별 블록을 표시하도록 한다.

[61]

먼저 도 3을 참조하면, 하나의 블록(100)에는 블록의 타이틀, 이전 연결 블록의 해시값 및 해당 블록의 해시값이 표시된다. 하나의 블록(100)은 상하로 배열된 3칸의 표에서, 첫번째 칸에는 블록의 타이틀이 표시되고, 두번째 칸에는 이전 연결 블록의 해시값이 표시되고, 세번째 칸에는 해당 블록의 해시값이 표시된다.

[62]

도 4를 참조하면, 하나의 블록(101)에는 이전 연결 블록의 해시값이 둘 이상 포함될 수 있다. 복수의 이전 연결 블록의 해시값은 가장 아래 칸의 해당 블록의 해시값의 위에 순차적으로 표시된다. 도 4를 참조하면, 하나의 블록(101)에는 2개의 이전 연결 블록의 해시값이 포함된다. 이는 각각 세번째 칸 및 네번째 칸에 표시되고, 마지막 칸에는 해당 블록의 해시값이 표시되어 있다.

[63]

도면에는 도시되지 않았지만 경우에 따라서 하나의 블록은 둘 이상의 추가 블록의 해시값을 포함할 수도 있다. 이러한 경우, 추가 블록의 해시값은 해당

블록의 해시값 위의 칸에 표시되는 것이 바람직할 것이다. 그리고 블록의 마지막 칸에는 해당 블록의 해시값이 표시되는 것이 바람직할 것이다.

[64] 추가 블록의 해시값에 대해서는 아래에서 더욱 상세하게 설명하도록 한다.

[65] 도 3 및 도 4에서, 블록의 타이틀은 B_n 또는 B_{nm} 과 같은 형태로 표시된다. 블록의 타이틀이 B_n 이라는 것은 상기 블록이 메인 브랜치의 n 번째 블록이라는 것을 의미한다. 그리고 블록의 타이틀이 B_{nm} 이라는 것은 상기 블록이 메인 브랜치의 n 번째 블록에서 분기되는 서브 브랜치의 m 번째 서브 블록이라는 것을 의미한다. 임의의 서브 브랜치의 m 번째 서브 블록은 상기 서브 브랜치의 $m+1$ 번째 블록에 해당한다.

[66] 어느 블록의 해시값은 H 라는 기호를 이용하여 표시된다. 예를 들어, 블록의 타이틀이 B_{nm} 인 블록의 해시값은 H_{nm} 으로 표시되게 된다.

[67] 상기 블록의 타이틀, 해시값의 기호 등을 설명하면서 언급한 메인 브랜치, 서브 브랜치 및 서브 블록 등에 대해서는 이하 도 5를 참조하여 상세하게 설명하도록 한다.

[68]

[69] 도 5를 참조하여, 본 발명의 일 실시예에 따른 블록체인 시스템에 대해서 설명하도록 한다. 도 5는 본 발명의 일 실시예에 따른 블록체인 시스템의 예시적인 블록도이다.

[70] 본 발명의 블록체인 시스템은 메인 브랜치(1000)를 포함한다. 여기서, 메인 브랜치(1000)는 이후에 설명할 서브 브랜치(1002, 1004, 1007, 1010, 1012)와 구분되는 것으로, 이들의 차이점은 이하에서 설명하도록 한다.

[71] 메인 브랜치(1000)는 최초 블록(genesis block), 제1 형 블록, 제2 형 블록 및 제3 형 블록을 포함한다. 제1 형 블록, 제2 형 블록 및 제3 형 블록이 어떻게 구분되는지 여부는 이후에서 상세하게 설명하도록 한다.

[72] 도 5에서 최초 블록은 두꺼운 테두리의 사각형으로 표시했고, 제1 형 블록과 제2 형 블록은 코너 부분이 라운드진 사각형으로 표시하였고, 제3 형 블록은 일반적인 사각형으로 표시하였다. 그리고 제1 형 블록과 제2 형 블록은 블록의 좌측 상단에 각각 ① 및 ②를 표시하여 구분하였다.

[73] 최초 블록(genesis block)은 블록체인 시스템에서 최초로 생성된 블록이다. 최초 블록은 블록체인 시스템의 다른 블록과 달리 예외적으로 이전 연결 블록이 없을 수 있다. 블록체인 시스템에서 최초 블록이 생성된 이후에 후속적으로 생성된 블록은 최초 블록과 직접적으로 또는 간접적으로 연결되게 된다. 도 5를 참조하면, B_0 가 최초 블록에 해당한다.

[74] 이하, 제1 형 블록, 제2 형 블록 및 제3 형 블록에 대해 설명하도록 한다. 설명의 편의성을 위해, 제3 형 블록에 대해서 먼저 설명하도록 한다.

[75] 제3 형 블록은 제1 형 블록 및 제2 형 블록과 달리, 해당 블록을 루트 블록으로 한 분기를 허용하지 않는 블록이다. 분기에 대해서는 아래에서 제1 형 블록 및 제2 형 블록을 설명하면서 상술하도록 한다. 따라서 제3 형 블록은 메인

브랜치(1000)에서 직전의 블록과 직후의 블록과만 연결되게 된다. 도 5를 참조하면, B_1 , B_3 , B_5 , B_8 및 B_9 가 제3 형 블록에 해당한다.

- [76] 제1 형 블록 및 제2 형 블록은 해당 제1 형 블록 및 제2 형 블록을 루트 블록(root block)으로 하여 분기를 허용하는 블록이다. 분기란 메인 브랜치(1000)의 임의의 블록을 루트 블록으로 하여 메인 브랜치(1000)와 분기되도록 연결된 서브 브랜치를 생성하는 것을 의미한다. 이러한 분기란 포킹(forking)이라는 용어로 설명되기도 한다. 따라서 제1 형 블록 및 제2 형 블록은 포킹된 블록(forked block)으로 설명될 수 있다. 또한, 제1 형 블록 및 제2 형 블록은 메인 브랜치(1000)와 서브 브랜치가 결합(joint)되는 결합 블록(joint block)으로 설명될 수도 있다.
- [77] 서브 브랜치에서 루트 블록을 제외한 나머지 루트 블록에 연결된 블록을 서브 블록으로 지칭하도록 한다. 따라서 제1 형 블록 및 제2 형 블록은 해당 제1 형 블록 및 제2 형 블록을 루트 블록으로 하여 서브 블록이 연결되는 것을 허용하는 블록을 의미한다.
- [78] 여기서 제1 형 블록 및 제2 형 블록은 분기를 허용만 하는 것으로, 제1 형 블록 및 제2 형 블록에는 해당 제1 형 블록 제2 형 블록을 루트 블록으로 하는 서브 브랜치가 연결되어 있을 수도 있고, 그렇지 않을 수도 있다. 서브 브랜치가 연결되어 있지 않는 제1 형 블록 및 제2 형 블록은 이후에 이벤트의 생성에 따라 해당 제1 형 블록 및 제2 형 블록을 루트 블록으로 하는 서브 브랜치가 연결될 수도 있다.
- [79] 도 5를 참조하면, B_2 , B_6 , B_7 및 B_{11} 이 제1 형 블록에 해당한다. 그리고 B_2 및 B_7 은 이에 연결된 서브 브랜치(1002, 1007)가 존재한다. 그러나 B_6 및 B_{11} 의 경우, 제1 형 블록임에도 불구하고 이에 연결된 서브 브랜치가 존재하지 않는다.
- [80] 현재 상태에서는 B_6 및 B_{11} 에 연결되는 서브 브랜치가 존재하지 않지만 이후에 B_{61} 및 B_{111} 에 해당하는 새로운 서브 블록이 생성되어 B_6 및 B_{11} 에 연결될 수 있다. 이러한 경우, B_6 및 B_{11} 에 연결된 서브 브랜치가 새롭게 생성될 수 있다. 또한, 이후에 B_{62} 및 B_{112} 에 해당하는 새로운 서브 블록이 생성되어 B_{61} 및 B_{111} 에 연결될 수 있다. 이러한 경우, B_6 및 B_{11} 에 연결된 서브 브랜치가 연장될 수 있다.
- [81] 그리고 B_4 , B_7 , B_{10} 및 B_{12} 이 제2 형 블록에 해당한다. 그리고 B_4 , B_7 , B_{10} 및 B_{12} 는 이에 연결된 서브 브랜치(1004, 1010)가 존재한다. 현재까지의 제2 형 블록에서는 서브 브랜치가 존재하지 않는 제2 형 블록이 존재하지 않는다. 그러나 이후 새롭게 생성되어 메인 브랜치(1000)에 연결되는 제2 형 블록에는 서브 브랜치가 존재하지 않을 수 있다.
- [82] 앞서 설명한 것에서, B_7 은 제1 형 블록면서 동시에 제2 형 블록인 중첩 블록에 해당한다. 중첩 블록에 대해서는 이하에서 더욱 상세하게 설명한다.
- [83]
- [84] 최초 블록이 생성된 이후에는 제1 형 블록, 제2 형 블록 및 제3 형 블록이 생성되어 메인 브랜치(1000)에 연결되게 된다. 제1 형 블록, 제2 형 블록 및 제3 형

블록은 각 블록의 생성 순서에 따라 연결된다.

- [85] 블록체인 시스템에서는 제1 형 블록, 제2 형 블록 및 서브 블록이 생성될 수 있다. 여기서 어떠한 종류의 블록이 생성될지는 블록이 포함하는 데이터가 기반한 이벤트에 따라 결정될 수 있다.
- [86] 예를 들어, 발생한 이벤트가 제1 형 이벤트인 경우, 발생한 제1 형 이벤트의 데이터를 포함하는 블록이 제1 형 블록으로 생성되어 연결될 수 있다. 또한, 발생한 이벤트가 제2 형 이벤트인 경우, 발생한 제2 형 이벤트의 데이터를 포함하는 블록이 제2 형 블록으로 생성되어 연결될 수 있다. 또한, 발생한 이벤트가 제3 형 이벤트인 경우, 발생한 제3 형 이벤트의 데이터를 포함하는 블록이 서브 블록으로 생성되어 연결될 수 있다.
- [87] 경우에 따라서, 발생한 이벤트가 제1 형 이벤트이면서 동시에 제2 형 이벤트일 수도 있다. 이러한 이벤트의 데이터를 포함하는 블록은 제1 형 블록이면서 동시에 제2 형 블록인 중첩 블록으로 생성되어 연결될 수 있다.
- [88] 제1 형 이벤트, 제2 형 이벤트 및 제3 형 이벤트를 구분하는 기준은 블록을 설계하는 사람의 기호 및 판단에 따라 다양하게 변경될 수 있다.
- [89]
- [90] 메인 브랜치(1000)에 포함된 블록 중 최초 블록을 제외한 블록은 메인 브랜치(1000)에서 해당 블록 직전에 생성된 블록의 적어도 일부의 해시값을 포함한다. 구체적으로, 블록은 블록헤더에 직전에 생성된 블록의 적어도 일부의 해시값을 포함하는 것을 통해 연결될 수 있다.
- [91] 이는 해당 블록이 제1 형 블록이든 제2 형 블록이든 제3 형 블록이든 중첩 블록이든 구분하지 않고 적용된다.
- [92] 도 5를 참조하면, 제1 형 블록인 B_2 의 경우 메인 브랜치(1000)에서 B_2 직전에 생성된 블록은 B_1 에 해당한다. B_2 는 B_1 의 적어도 일부의 해시값(H_1)을 포함한다.
- [93] 또한, 제2 형 블록인 B_4 의 경우 메인 브랜치(1000)에서 B_4 직전에 생성된 블록은 B_3 에 해당한다. B_4 는 B_3 의 적어도 일부의 해시값(H_3)을 포함한다.
- [94] 또한, 제3 형 블록인 B_1 의 경우 메인 브랜치(1000)에서 B_1 직전에 생성된 블록은 최초 블록인 B_0 에 해당한다. B_1 는 B_0 의 적어도 일부의 해시값(H_0)을 포함한다.
- [95] 또한, 중첩 블록인 B_7 의 경우 메인 브랜치(1000)에서 B_7 직전에 생성된 블록은 B_6 에 해당한다. B_7 은 B_6 의 적어도 일부의 해시값(H_6)을 포함한다.
- [96]
- [97] 제1 형 블록은 최초 제1 형 블록과 후속 제1 형 블록을 포함한다. 최초 제1 형 블록은 제1 형 블록 중 가장 먼저 생성된 블록을 의미한다. 그리고 후속 제1 형 블록은 최초 제1 형 블록 이후에 생성된 블록을 의미한다.
- [98] 그리고, 제2 형 블록은 최초 제2 형 블록과 후속 제2 형 블록을 포함한다. 최초 제2 형 블록은 제2 형 블록 중 가장 먼저 생성된 블록을 의미한다. 그리고 후속 제2 형 블록은 최초 제2 형 블록 이후에 생성된 블록을 의미한다.
- [99] 도 5를 참조하면, 최초 제1 형 블록 및 최초 제2 형 블록은 두꺼운 테두리의

라운드진 사각형으로 표시했고, 후속 제1 형 블록 및 후속 제2 형 블록은 일반 테두리의 라운드진 사각형으로 표시하여 구분하였다.

[100] 도 5를 참조하면, B_2 가 최초 제1 형 블록에 해당하고, B_6 및 B_7 이 후속 제1 형 블록에 해당한다. 또한, B_4 가 최초 제2 형 블록에 해당하고, B_{10} 및 B_{11} 이 후속 제2 형 블록에 해당한다

[101] 먼저, 제1 형 블록에 대해서 설명하도록 한다.

[102] 후속 제1 형 블록은 메인 브랜치(1000)에서 해당 후속 제1 형 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 포함한다. 구체적으로, 후속 제1 형 블록은 블록헤더에 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 포함하는 것을 통해 연결될 수 있다. 여기서, 직전 제1 형 블록이란 최초 제1 형 블록일 수도 있고, 후속 제1 형 블록일 수도 있다.

[103] 구체적으로, B_6 을 기준으로 설명하면, B_6 직전에 생성된 제1 형 블록은 B_2 에 해당한다. B_6 은 B_2 의 적어도 일부의 해시값(H_2)을 포함한다.

[104] 위에서 설명한 것과 같이, 제1 형 블록 중 두번째로 생성된 제1 형 블록(B_6)은 최초 제1 형 블록(B_2)의 적어도 일부의 해시값(H_2)을 포함하게 된다.

[105] 이하, 제2 형 블록에 대해서 설명하도록 한다.

[106] 제2 형 블록도 제1 형 블록과 마찬가지로, 후속 제2 형 블록은 메인 브랜치(1000)에서 해당 후속 제2 형 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 포함한다.

[107] 구체적으로, B_{12} 를 기준으로 설명하면, B_{12} 직전에 생성된 제2 형 블록은 B_{10} 에 해당한다. B_{12} 는 B_{10} 의 적어도 일부의 해시값(H_{10})을 포함한다.

[108] 이에 따라, 후속 제1 형 블록 및 후속 제2 형 블록은 2개의 해시값을 포함하게 된다. 구체적으로, B_6 의 경우, 직전 블록의 적어도 일부의 해시값으로 B_5 의 적어도 일부의 해시값(H_5)을 포함하고, 직전 제1 형 블록의 적어도 일부의 해시값으로 B_2 의 적어도 일부의 해시값(H_2)을 포함한다. 후속 제1 형 블록 및 후속 제2 형 블록은 2개의 해시값을 구분하여 포함할 수 있다.

[109]

[110] 최초 제1 형 블록 및 최초 제2 형 블록은 최초 블록의 적어도 일부의 해시값을 포함한다. 구체적으로, 최초 제1 형 블록인 B_2 은 B_0 의 적어도 일부의 해시값을 포함한다. 그리고 최초 제2 형 블록인 B_4 는 B_0 의 적어도 일부의 해시값을 포함한다.

[111]

[112] 중첩 블록은 제1 형 블록이면서 동시에 제2 형 블록인 것이다. 따라서 중첩 블록은 메인 브랜치에서 중첩 블록 직전에 생성된 블록의 적어도 일부의 해시값, 메인 브랜치에서 중첩 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값 및 메인 브랜치에서 중첩 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 포함한다.

[113] 중첩 블록은 제1 형 블록이면서 동시에 제2 형 블록이므로 중첩 블록을 루트

블록으로 하는 서브 브랜치가 연결될 수 있다.

- [114] 도 5를 참조하면, B_7 이 중첩 블록에 해당한다. B_7 에는 B_7 을 루트 블록으로 하는 서브 브랜치(1007)가 연결되어 있다.
- [115] B_7 을 기준으로 설명하면, B_7 직전에 생성된 제1 형 블록은 B_6 에 해당한다. B_7 은 B_6 의 적어도 일부의 해시값(H_6)을 포함한다. 또한, B_7 직전에 생성된 제2 형 블록은 B_4 에 해당한다. B_7 은 B_4 의 적어도 일부의 해시값(H_4)을 포함한다.
- [116] 도 5에 도시된 것과 같이, 중첩 블록은 메인 브랜치에서 중첩 블록 직전에 생성된 블록의 적어도 일부의 해시값, 메인 브랜치에서 중첩 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값 및 메인 브랜치에서 중첩 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 각각 구분하여 포함할 수 있다.
- [117] 경우에 따라서 2개의 해시값이 동일할 수 있다. 구체적으로, B_7 의 경우, 직전 블록의 적어도 일부의 해시값으로 B_6 의 적어도 일부의 해시값(H_6)을 포함하고, 직전 제1 형 블록의 적어도 일부의 해시값으로도 B_6 의 적어도 일부의 해시값(H_6)을 포함한다. 이러한 경우, 도 5에 도시된 것과 같이, 2개의 해시값을 구분하여 각각 포함할 수도 있다. 그러나 경우에 따라서 중복되는 해시값을 하나만 포함할 수도 있다.
- [118] 경우에 따라서, B_7 이 직전 블록의 적어도 일부의 해시값으로 포함하는 B_6 의 적어도 일부의 해시값과 직전 제1 형 블록의 적어도 일부의 해시값으로 포함하는 B_6 의 적어도 일부의 해시값이 상이할 수도 있다. 이는 B_6 의 데이터에서 해시값을 어떻게 산출하는지 여부에 따라 결정될 수 있다.
- [119]
- [120] 메인 브랜치에서 중첩 블록 직후에 생성된 제1 형 블록은, 메인 브랜치에서 해당 제1 형 블록 직전에 생성된 블록의 적어도 일부의 해시값과 중첩 블록의 적어도 일부의 해시값을 포함한다.
- [121] 도 5를 참조하면, B_{11} 이 중첩 블록 직후에 생성된 제1 형 블록에 해당한다. B_{11} 을 기준으로 설명하면, B_{11} 직전에 생성된 블록은 B_{10} 에 해당한다. 따라서 B_{11} 은 B_{10} 의 적어도 일부의 해시값(H_{10})을 포함한다. 또한, B_{11} 직전에 생성된 중첩 블록은 B_7 에 해당한다. 따라서 B_{11} 은 B_7 의 적어도 일부의 해시값(H_7)을 포함한다.
- [122] 메인 브랜치에서 중첩 블록 직후에 생성된 제2 형 블록은, 메인 브랜치에서 해당 제2 형 블록 직전에 생성된 블록의 적어도 일부의 해시값과 중첩 블록의 적어도 일부의 해시값을 포함한다.
- [123] 도 5를 참조하면, B_{10} 이 중첩 블록 직후에 생성된 제2 형 블록에 해당한다. B_{10} 을 기준으로 설명하면, B_{10} 직전에 생성된 블록은 B_9 에 해당한다. 따라서 B_{10} 은 B_9 의 적어도 일부의 해시값(H_9)을 포함한다. 또한, B_{10} 직전에 생성된 중첩 블록은 B_7 에 해당한다. 따라서 B_{10} 은 B_7 의 적어도 일부의 해시값(H_7)을 포함한다.
- [124]
- [125] 이러한 블록체인 시스템을 이용하면, 발생한 이벤트가 제1 형 이벤트이면서 동시에 제2 형 이벤트인 경우, 중첩 블록에 데이터를 포함하여 관리할 수 있다.

- [126] 또한, 이러한 블록체인 시스템을 이용하면, 특정 노드가 진위여부를 검증하려는 데이터의 종류에 따라 일부의 블록만을 저장하고 사용하는 것이 가능하다.
- [127] 예를 들어, 특정 노드가 제1 형 이벤트의 데이터만의 검증을 원할 경우를 가정하여 설명한다. 상술한 것과 같이, 제1 형 이벤트의 데이터는 제1 형 블록에 포함되게 된다. 따라서 상기 특정 노드는 최초 블록과 제1 형 블록만을 저장하고, 이를 활용하여 데이터를 검증하는 것이 가능하다.
- [128] 구체적으로 도 5에서, 특정 노드가 B₇에 저장된 제1 형 이벤트의 데이터의 검증을 원할 경우, 상기 특정 노드는 메인 브랜치(1000)의 최초 블록과 제1 형 블록만을 저장하고 있으면 된다. 즉, 상기 특정 노드는 총 5개의 블록만을 저장하고 있는 것이다. 이는 총 23개로 구성된 모든 블록체인의 모든 블록을 저장하는 것보다 작은 개수의 블록을 저장하는 것이다.
- [129] 또한, 도 5에서, 특정 노드가 B₇에 저장된 제2 형 이벤트의 데이터의 검증을 원할 경우, 상기 특정 노드는 메인 브랜치(1000)의 최초 블록과 제2 형 블록만을 저장하고 있으면 된다. 즉, 상기 특정 노드는 총 5개의 블록만을 저장하고 있는 것이다. 이는 총 23개로 구성된 모든 블록체인의 모든 블록을 저장하는 것보다 작은 개수의 블록을 저장하는 것이다.
- [130] 또한 도 5에서, 특정 노드가 B₁₀₁에 저장된 데이터의 검증을 원할 경우, 상기 특정 노드는 메인 브랜치(1000)의 최초 블록과 제2 형 블록 및 B₁₀₂가 포함된 서브 브랜치의 서브 블록만을 저장하고 있으면 된다. 즉, 상기 특정 노드는 총 8개의 블록만을 저장하고 있는 것이다. 이는 총 23개로 구성된 모든 블록체인의 모든 블록을 저장하는 것보다 작은 개수의 블록을 저장하는 것이다.
- [131] 이와 같이, 본 발명의 블록체인 시스템은 모든 노드가 블록체인의 모든 블록을 저장할 필요가 없다는 장점이 있다. 이는 노드가 부담해야 하는 컴퓨팅 작업 및 노드가 확보해야 하는 저장 공간을 감소시킬 수 있다는 장점이 있다. 이는 컴퓨팅 능력과 저장 공간이 상대적으로 제한된 모바일 장치 및 웨어러블 장치 등도 용이하게 블록체인 시스템의 노드로 참여할 수 있게 한다.
- [132]
- [133] 도 6을 참조하여, 본 발명의 다른 일 실시예에 따른 블록체인 시스템에 대해서 설명하도록 한다. 도 6은 본 발명의 다른 일 실시예에 따른 블록체인 시스템의 예시적인 블록도이다.
- [134] 설명의 편의를 위해서, 도 6을 참조하여 본 발명의 실시예를 설명하면서 도 5를 참조하여 이미 설명한 것과 동일한 내용 중 일부는 생략하도록 한다.
- [135] 본 발명의 블록체인 시스템은 메인 브랜치(1000) 및 서브 브랜치(1002, 1004, 1007, 1010, 1012)를 포함한다.
- [136] 최초 제1 형 블록은 해당 최초 제1 형 블록 직전 블록의 적어도 일부의 해시값을

포함한다. 즉, 도 5를 참조하여 설명한 것과 달리, 최초 제1 형 블록은 최초 블록(B_0)의 해시값(H_0)을 포함하는 것이 아니라 해당 최초 제1 형 블록 직전 블록의 적어도 일부의 해시값을 포함하는 것이다.

- [137] 구체적으로, 도 6을 참조하면 최초 제1 형 블록은 B_2 에 해당한다. B_2 를 기준으로 직전 블록은 B_1 에 해당한다. 따라서 B_2 는 B_1 의 적어도 일부의 해시값(H_1)을 포함한다.
- [138] 최초 제1 형 블록은 직전 블록의 적어도 일부의 해시값을 2개로 구분하여 포함할 수도 있고, 하나로 포함할 수도 있다. 도 6을 참조하면, 최초 제1 형 블록은 B_2 는 B_1 의 적어도 일부의 해시값(H_1)을 구분하여 포함하는 것으로 도시하였지만 이에 한정되는 것은 아니다.
- [139] 이와 마찬가지로, 최초 제2 형 블록도 해당 최초 제2 형 블록 직전 블록의 적어도 일부의 해시값을 포함한다. 즉, 도 5를 참조하여 설명한 것과 달리, 최초 제2 형 블록은 최초 블록(B_0)의 해시값(H_0)을 포함하는 것이 아니라 해당 최초 제2 형 블록 직전 블록의 적어도 일부의 해시값을 포함하는 것이다.
- [140] 구체적으로, 도 6을 참조하면 최초 제2 형 블록은 B_4 에 해당한다. B_4 를 기준으로 직전 블록은 B_3 에 해당한다. 따라서 B_4 는 B_3 의 적어도 일부의 해시값(H_3)을 포함한다.
- [141] 최초 제2 형 블록은 직전 블록의 적어도 일부의 해시값을 2개로 구분하여 포함할 수도 있고, 하나로 포함할 수도 있다. 도 6을 참조하면, 최초 제2 형 블록은 B_4 는 B_3 의 적어도 일부의 해시값(H_3)을 구분하여 포함하는 것으로 도시하였지만 이에 한정되는 것은 아니다.
- [142]
- [143] 이상, 본 발명의 블록체인 시스템의 실시예들에 대해 설명하였다. 본 발명은 상술한 실시예 및 첨부한 도면에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자의 관점에서 다양한 수정 및 변형이 가능할 것이다. 따라서 본 발명의 범위는 본 명세서의 청구범위뿐만 아니라 이 청구범위와 균등한 것들에 의해 정해져야 한다.
- [144] 100, 200: 블록
- [145] 110, 210: 블록 헤더
- [146] 120, 220: 블록 몸체
- [147] 1000: 메인 브랜치
- [148] 1002, 1004, 1007, 1010, 1212: 서브 브랜치

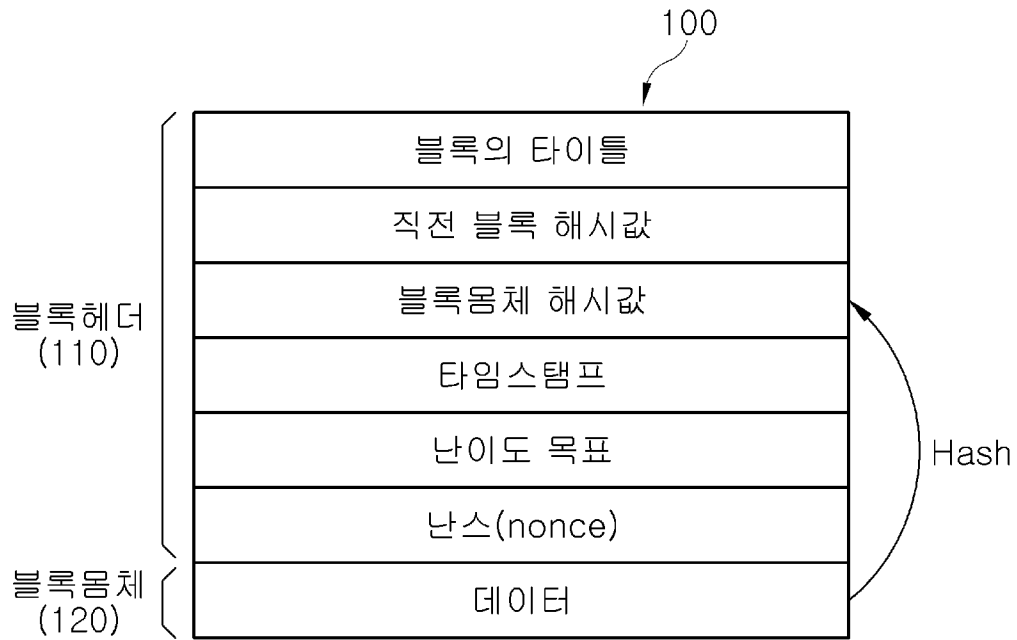
청구범위

- [청구항 1] 블록체인 시스템에 있어서,
 최초(genesis) 블록, 적어도 하나의 제1 형 블록 및 적어도 하나의 제2 형 블록을 포함하는 메인 브랜치를 포함하고,
 상기 메인 브랜치에 포함된 블록은 상기 최초 블록을 시작으로 각각 블록의 생성 순서에 따라 연결되고,
 상기 최초 블록을 제외한 상기 메인 브랜치에 포함된 블록은 상기 메인 브랜치에서 해당 블록 직전에 생성된 블록의 적어도 일부의 해시값을 포함하고,
 상기 제1 형 블록 중 적어도 일부는 상기 메인 브랜치에서 해당 제1 형 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 포함하고,
 상기 제2 형 블록 중 적어도 일부는 상기 메인 브랜치에서 해당 제2 형 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 포함하고,
 상기 메인 브랜치는 상기 제1 형 블록이면서 동시에 상기 제2 형 블록인 적어도 하나의 중첩 블록을 포함하는 블록체인 시스템.
- [청구항 2] 제1 항에 있어서,
 상기 중첩 블록은,
 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 블록의 적어도 일부의 해시값, 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값 및 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 포함하는 블록체인 시스템.
- [청구항 3] 제2 항에 있어서,
 상기 중첩 블록은,
 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 블록의 적어도 일부의 해시값, 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값 및 상기 메인 브랜치에서 상기 중첩 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 각각 구분하여 포함하는 블록체인 시스템.
- [청구항 4] 제1 항에 있어서,
 상기 메인 브랜치에서 상기 중첩 블록 직후에 생성된 제1 형 블록은,
 상기 메인 브랜치에서 해당 제1 형 블록 직전에 생성된 블록의 적어도 일부의 해시값과 상기 중첩 블록의 적어도 일부의 해시값을 포함하는 블록체인 시스템.
- [청구항 5] 제4 항에 있어서,
 상기 메인 브랜치에서 상기 중첩 블록 직후에 생성된 제2 형 블록은,
 상기 메인 브랜치에서 해당 제2 형 블록 직전에 생성된 블록의 적어도

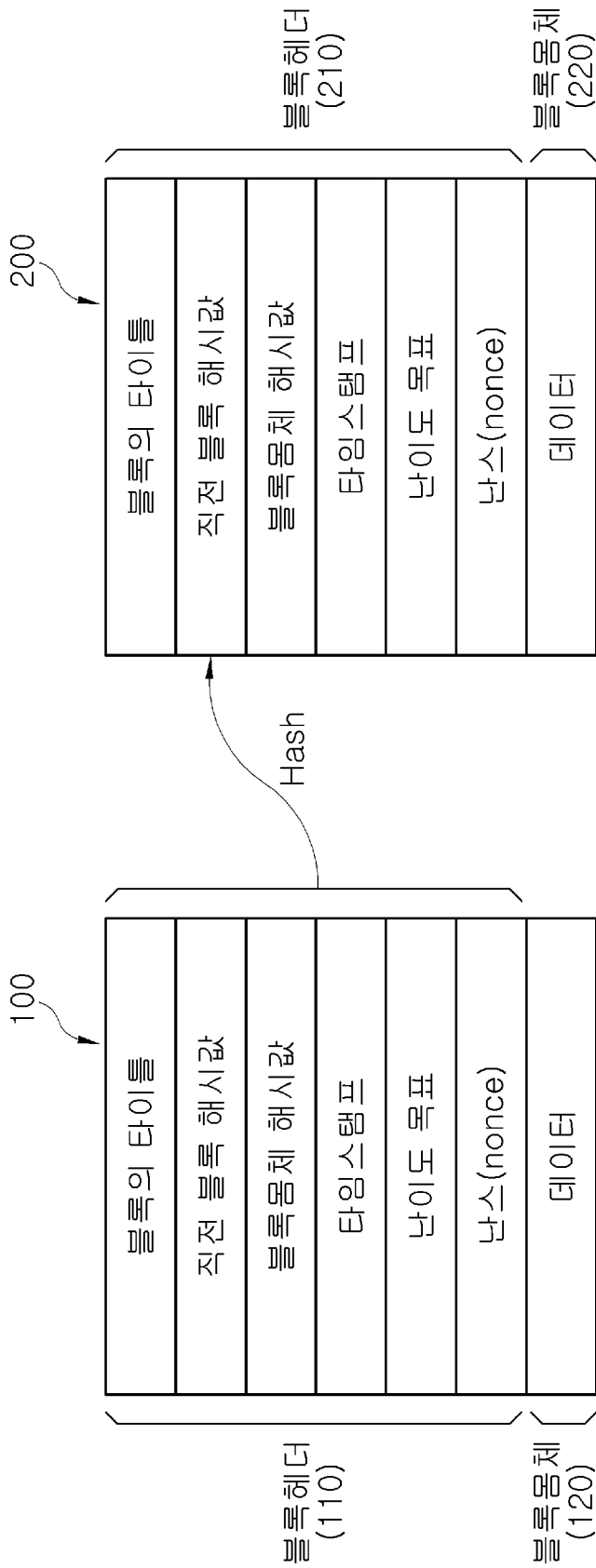
- 일부의 해시값과 상기 중첩 블록의 적어도 일부의 해시값을 포함하는 블록체인 시스템.
- [청구항 6] 제1 항에 있어서,
상기 적어도 일부의 제1 형 블록은 상기 직전에 생성된 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 구분하여 포함하는 블록체인 시스템.
- [청구항 7] 제6 항에 있어서,
상기 적어도 일부의 제2 형 블록은 상기 직전에 생성된 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 구분하여 포함하는 블록체인 시스템.
- [청구항 8] 제1 항에 있어서,
상기 적어도 일부의 제1 형 블록이 포함하는 상기 직전에 생성된 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값이 동일한 경우, 하나의 해시값만을 포함하는 블록체인 시스템.
- [청구항 9] 제8 항에 있어서,
상기 적어도 일부의 제2 형 블록이 포함하는 상기 직전에 생성된 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제2 형 블록의 적어도 일부의 해시값이 동일한 경우, 하나의 해시값만을 포함하는 블록체인 시스템.
- [청구항 10] 제1 항에 있어서,
상기 제1 형 블록은 제1 형 블록 중 가장 먼저 생성된 최초 제1 형 블록 및 상기 최초 제1 형 블록 이후에 생성된 후속 제1 형 블록을 포함하고, 상기 후속 제1 형 블록은 상기 메인 브랜치에서 해당 후속 제1 형 블록 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 포함하는 블록체인 시스템.
- [청구항 11] 제10 항에 있어서,
상기 최초 제1 형 블록은 상기 최초 블록의 적어도 일부의 해시값을 포함하는 블록체인 시스템.
- [청구항 12] 제10 항에 있어서,
상기 최초 제1 형 블록은 상기 최초 제1 형 블록 직전 블록의 적어도 일부의 해시값을 포함하고, 다른 블록의 적어도 일부의 해시값은 포함하지 않는 블록체인 시스템.
- [청구항 13] 제10 항에 있어서,
상기 제2 형 블록은 제2 형 블록 중 가장 먼저 생성된 최초 제2 형 블록 및 상기 최초 제2 형 블록 이후에 생성된 후속 제2 형 블록을 포함하고, 상기 후속 제2 형 블록은 상기 메인 브랜치에서 해당 후속 제2 형 블록 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 포함하는 블록체인

- 시스템.
- [청구항 14] 제13 항에 있어서,
상기 최초 제2 형 블록은 상기 최초 블록의 적어도 일부의 해시값을 포함하는 블록체인 시스템.
- [청구항 15] 제13 항에 있어서,
상기 최초 제2 형 블록은 상기 최초 제2 형 블록 직전 블록의 적어도 일부의 해시값을 포함하고, 다른 블록의 적어도 일부의 해시값은 포함하지 않는 블록체인 시스템.
- [청구항 16] 제1 항에 있어서,
상기 제1 형 블록 및 상기 제2 형 블록은 해당 제1 형 블록 및 제2 형 블록을 루트 블록으로 하는 포킹을 허용하는 블록체인 시스템.
- [청구항 17] 제1 항에 있어서,
상기 제1 형 블록 및 상기 제2 형 블록 중 적어도 일부를 루트 블록으로 하여 서브 블록이 연결되는 것을 허용하는 블록체인 시스템.
- [청구항 18] 제1 항에 있어서,
상기 제1 형 블록 및 상기 제2 형 블록 중 적어도 일부를 루트 블록으로 하여 포킹된 서브 브랜치를 더 포함하는 블록체인 시스템.
- [청구항 19] 제1 항에 있어서,
상기 제1 형 블록 및 상기 제2 형 블록 중 적어도 일부를 루트 블록으로 하여 연결된 적어도 하나의 서브 블록을 포함하는 서브 브랜치를 더 포함하는 블록체인 시스템.

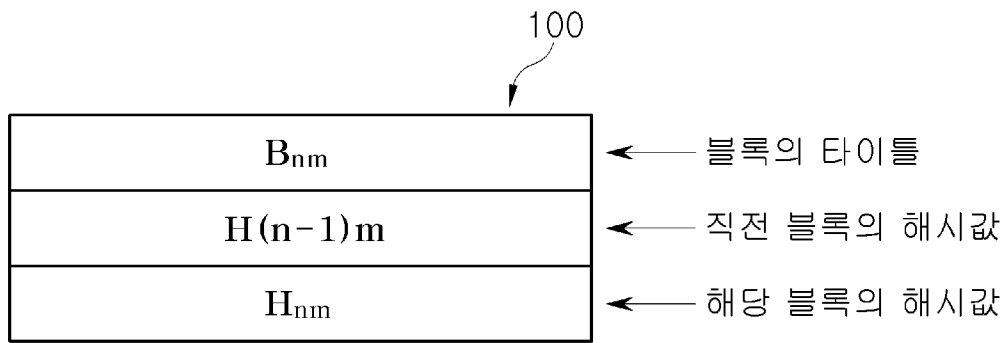
[도1]



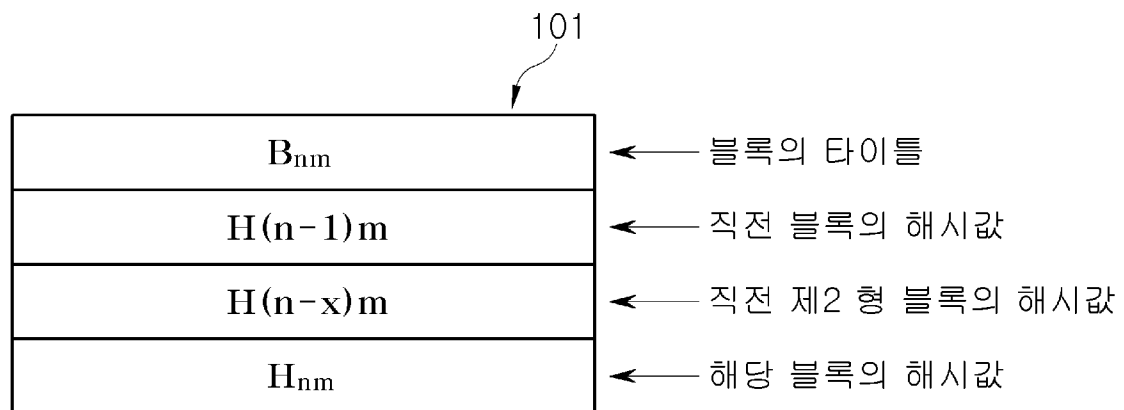
[도2]



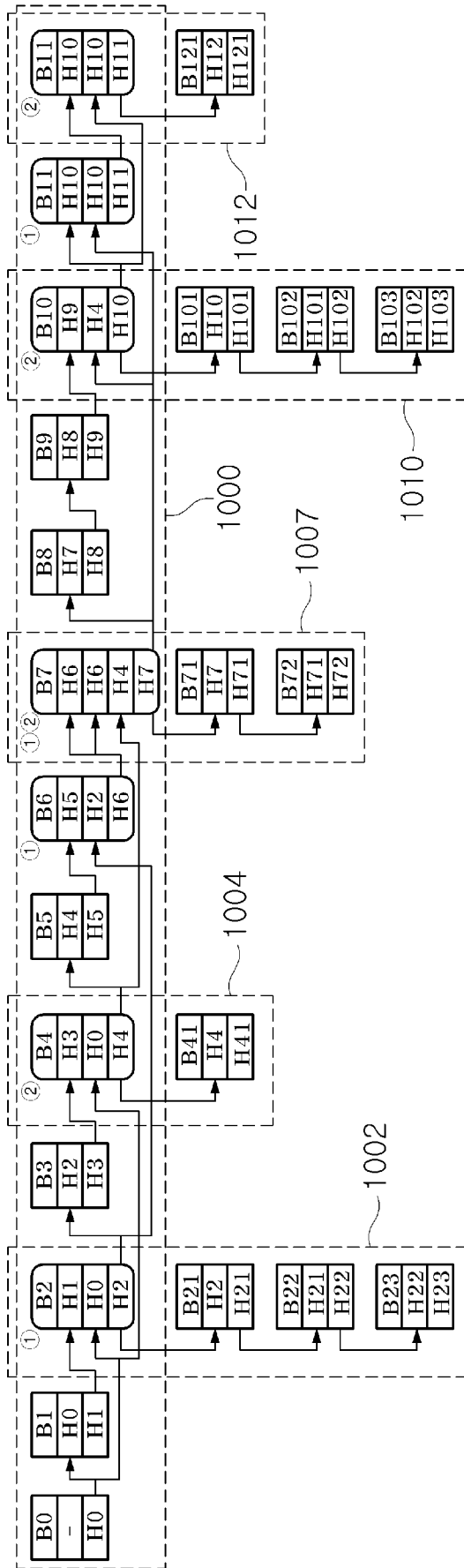
[도3]



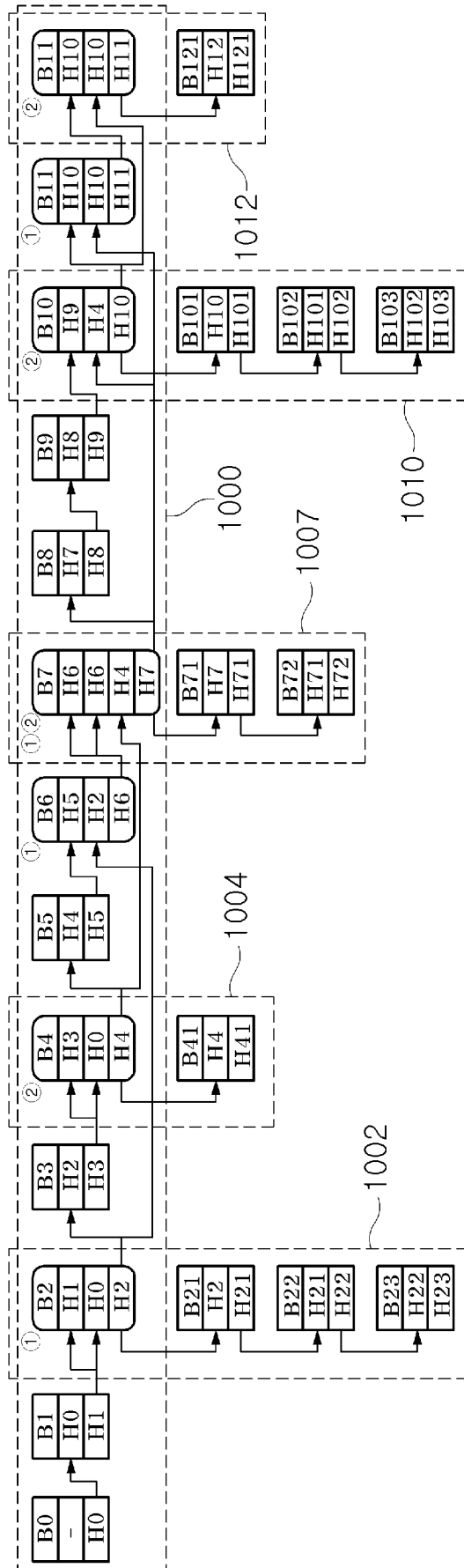
[도4]



[Fig. 5]



[圖 6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2019/003656

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08(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 29/08; G06Q 20/40; H04L 29/06; H04L 9/06; H04L 9/12; H04L 9/32

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, genesis branch, hash value, fork

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 9608829 B2 (BLOCKCHAIN TECHNOLOGIES CORPORATION) 28 March 2017 See column 6, line 53-column 8, line 41; and figures 2-5.	1-19
A	김형건 등. 블록체인 기반 최신 플랫폼에 대한 조사. 한국정보과학회 2017년 한국컴퓨터종합학술대회 논문집. June 2017, pages 1048-1050 (KIM, Hyeong-geon et al. A survey on platforms of blockchain. Korean Institute of Information Scientists and Engineers. Proceedings of Korea Computer Congress 2017.) See section 2.	1-19
A	KR 10-2017-0040079 A (AHN, Kyu Tae et al.) 12 April 2017 See paragraphs [0026]-[0060]; and figures 2a-4.	1-19
A	US 2017-0236123 A1 (BLOCKSTACK INC.) 17 August 2017 See paragraphs [0093]-[0124]; and figures 7-9.	1-19
A	US 2017-0359374 A1 (INTEL CORPORATION) 14 December 2017 See paragraphs [0052]-[0098]; and figures 2-8.	1-19

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

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	


Date of the actual completion of the international search

21 JUNE 2019 (21.06.2019)

Date of mailing of the international search report

02 JULY 2019 (02.07.2019)

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/KR2019/003656

Patent document cited in search report	Publication date	Patent family member	Publication date
US 9608829 B2	28/03/2017	US 2016-0027229 A1	28/01/2016
		US 2016-0028552 A1	28/01/2016
		US 2017-0352219 A1	07/12/2017
		US 2018-0102013 A1	12/04/2018
		US 9836908 B2	05/12/2017
		WO 2016-015041 A1	28/01/2016
		WO 2016-022864 A2	11/02/2016
		WO 2016-022864 A3	07/04/2016
KR 10-2017-0040079 A	12/04/2017	CN 109075964 A	21/12/2018
		WO 2017-192007 A2	09/11/2017
		WO 2017-192007 A3	04/01/2018
US 2017-0236123 A1	17/08/2017	None	
US 2017-0359374 A1	14/12/2017	None	

A. 발명이 속하는 기술분류(국제특허분류(IPC)) H04L 29/08(2006.01)i, H04L 9/06(2006.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04L 29/08; G06Q 20/40; H04L 29/06; H04L 9/06; H04L 9/12; H04L 9/32 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(block-chain), 메인 브랜치(genesis branch), 해시값(hash value), 분기(fork)		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 9608829 B2 (BLOCKCHAIN TECHNOLOGIES CORPORATION) 2017.03.28 컬럼 6, 라인 53 - 컬럼 8, 라인 41; 및 도면 2-5 참조.	1-19
A	김형건 등, '블록체인 기반 최신 플랫폼에 대한 조사', 한국정보과학회 2017년 한국컴퓨터종합학술대회 논문집, 2017.06, 페이지 1048-1050 섹션 2 참조.	1-19
A	KR 10-2017-0040079 A (안규태 등) 2017.04.12 단락 [0026]-[0060]; 및 도면 2a-4 참조.	1-19
A	US 2017-0236123 A1 (BLOCKSTACK INC.) 2017.08.17 단락 [0093]-[0124]; 및 도면 7-9 참조.	1-19
A	US 2017-0359374 A1 (INTEL CORPORATION) 2017.12.14 단락 [0052]-[0098]; 및 도면 2-8 참조.	1-19
<input type="checkbox"/> 추가 문헌이 C(계속)에 기재되어 있습니다. <input checked="" type="checkbox"/> 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 2019년 06월 21일 (21.06.2019)	국제조사보고서 발송일 2019년 07월 02일 (02.07.2019)	
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	

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 9608829 B2	2017/03/28	US 2016-0027229 A1 US 2016-0028552 A1 US 2017-0352219 A1 US 2018-0102013 A1 US 9836908 B2 WO 2016-015041 A1 WO 2016-022864 A2 WO 2016-022864 A3	2016/01/28 2016/01/28 2017/12/07 2018/04/12 2017/12/05 2016/01/28 2016/02/11 2016/04/07
KR 10-2017-0040079 A	2017/04/12	CN 109075964 A WO 2017-192007 A2 WO 2017-192007 A3	2018/12/21 2017/11/09 2018/01/04
US 2017-0236123 A1	2017/08/17	없음	
US 2017-0359374 A1	2017/12/14	없음	