

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국



(10) 국제공개번호

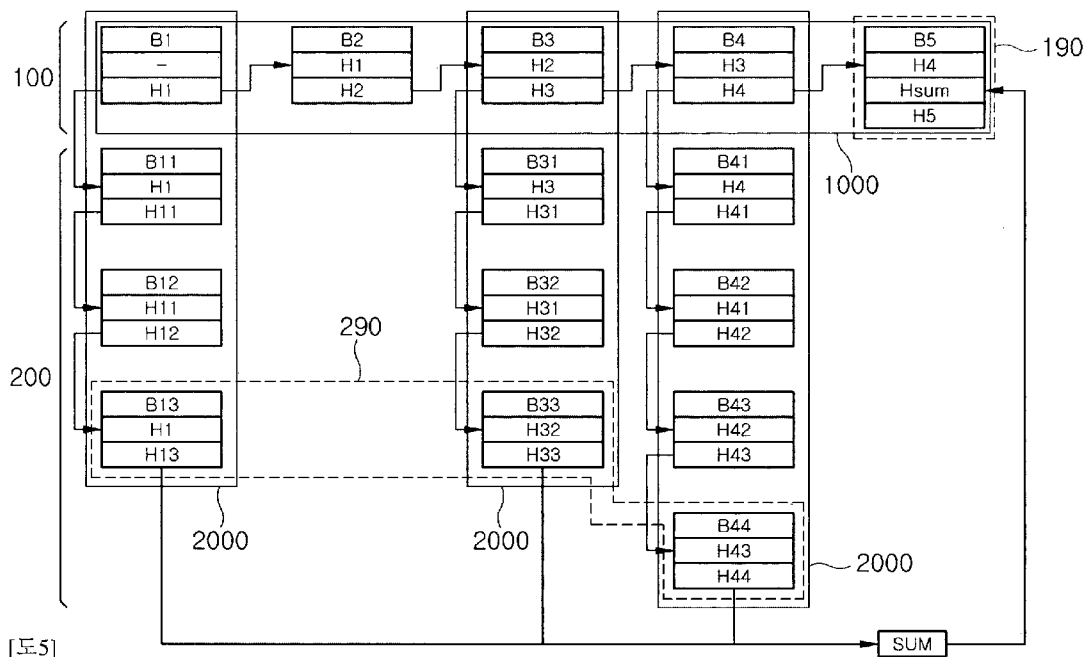
(43) 국제공개일
2018년 11월 15일 (15.11.2018) WIPO | PCT

WO 2018/207975 A1

- (51) 국제특허분류: G06Q 20/36 (2012.01) G06Q 20/38 (2012.01) (KIM, Byung Jin); 07042 서울시 동작구 국사봉1길 18 상진아파트 702호, Seoul (KR).
- (21) 국제출원번호: PCT/KR2017/010020 (74) 대리인: 신용현 등 (SHIN, Yong Hyun et al.); 06158 서울시 강남구 테헤란로 437 삼성빌딩 2층, Seoul (KR).
- (22) 국제출원일: 2017년 9월 13일 (13.09.2017)
- (25) 출원언어: 한국어 (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.
- (26) 공개언어: 한국어
- (30) 우선권정보: 10-2017-0059276 2017년 5월 12일 (12.05.2017) KR
- (71) 출원인: 주식회사 써트온 (CERTON CO., LTD.) [KR/KR]; 06026 서울시 강남구 도산대로 207 7층, Seoul (KR).
- (72) 발명자: 김승기 (KIM, Seung Ki); 12222 경기도 남양주시 평내로 113 1505-1703, Gyeonggi-do (KR). 김병진

(54) Title: BLOCKCHAIN SYSTEM AND METHOD FOR GENERATING BLOCKCHAIN

(54) 발명의 명칭: 블록체인 시스템 및 블록체인 생성 방법



(57) Abstract: The present invention relates to a blockchain system and a method for generating a blockchain, and more specifically, to a blockchain system including a main branch and a sub-branch, and a method for generating a blockchain. The blockchain system, according to the present invention, comprises at least one type one block. Each of the type one blocks include a main branch, one type one block, and at least one type two block, connected according to the order of generation of each block. The type two block includes at least one sub-branch connected using the type one block as a root block. The type two blocks of one sub-branch are connected according to the order of generation of each block, wherein the first type two block generated from the first sub-branch is connected to the root block. The last type one block of the main branch includes the hash value of at least a portion of the last type two block of the sub-branch.

[다음 쪽 계속]



WO 2018/207975 A1

(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).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

(57) 요약서: 본 발명은 블록체인 시스템 및 블록체인 생성 방법에 관한 것으로, 더욱 상세하게는 메인 브랜치와 서브 브랜치를 포함하는 블록체인 시스템과 이러한 블록체인의 생성 방법에 관한 것이다. 본 발명의 블록체인 시스템은, 적어도 하나의 제1 형 블록을 포함하고, 상기 제1 형 블록들은 각각 블록의 생성 순서에 따라 연결된 메인 브랜치 및 하나의 제1 형 블록 및 적어도 하나의 제2 형 블록을 포함하고, 상기 제2 형 블록은 상기 제1 형 블록을 루트 블록으로 하여 연결된 적어도 하나의 서브 브랜치를 포함하고, 하나의 서브 브랜치의 상기 제2 형 블록은 각각 블록의 생성 순서에 따라 연결되며, 상기 하나의 서브 브랜치에서 최초로 생성된 제2 형 블록은 상기 루트 블록에 연결되고, 상기 메인 브랜치의 마지막 제1 형 블록은, 상기 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함한다.

명세서

발명의 명칭: 블록체인 시스템 및 블록체인 생성 방법

기술분야

- [1] 본 발명은 블록체인 시스템 및 블록체인 생성 방법에 관한 것으로, 더욱 상세하게는 메인 브랜치와 서브 브랜치를 포함하는 블록체인 시스템과 이러한 블록체인의 생성 방법에 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.
- [4] 블록체인에 참여하는 노드들은 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 비트코인의 전체 블록체인 크기는 현재 수십 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.

발명의 상세한 설명

기술적 과제

- [6] 본 발명이 해결하려는 과제는, 블록들이 복수의 브랜치로 연결되도록 구성하여 데이터를 효율적이고 체계적으로 관리할 수 있는 블록체인 시스템을 제공하는 것이다.
- [7] 본 발명이 해결하려는 다른 과제는, 블록들이 복수의 브랜치로 연결되더라도 모든 블록의 위변조에 대한 안전성을 확보할 수 있는 블록체인 시스템 및 이러한 블록체인의 생성 방법을 제공하는 것이다.

과제 해결 수단

- [8] 상기 과제를 해결하기 위한 본 발명의 블록체인 시스템은, 적어도 하나의 제1 형 블록을 포함하고, 상기 제1 형 블록들은 각각 블록의 생성 순서에 따라 연결된 메인 브랜치 및 하나의 제1 형 블록 및 적어도 하나의 제2 형 블록을 포함하고, 상기 제2 형 블록은 상기 제1 형 블록을 루트 블록으로 하여 연결된 적어도 하나의 서브 브랜치를 포함하고, 하나의 서브 브랜치의 상기 제2 형 블록은 각각 블록의 생성 순서에 따라 연결되되, 상기 하나의 서브 브랜치에서 최초로 생성된 제2 형 블록은 상기 루트 블록에 연결되고, 상기 메인 브랜치의 마지막 제1 형 블록은, 상기 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함한다.
- [9] 본 발명의 일 실시예에 있어서, 상기 마지막 제1 형 블록은, 상기 메인 브랜치에 포함되고 상기 마지막 제1 형 블록보다 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 더 포함할 수 있다.
- [10] 본 발명의 일 실시예에 있어서, 상기 마지막 제1 형 블록은, 상기 마지막 제2 형 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 구분하여 포함할 수 있다.
- [11] 본 발명의 일 실시예에 있어서, 상기 마지막 제1 형 블록은, 상기 마지막 제2 형 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 블록헤더에 포함할 수 있다.
- [12] 본 발명의 일 실시예에 있어서, 상기 마지막 제1 형 블록은, 모든 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함할 수 있다.
- [13] 본 발명의 일 실시예에 있어서, 상기 마지막 제1 형 블록은, 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 마지막 제2 형 블록의 적어도 일부의 해시값을 포함할 수 있다.
- [14] 본 발명의 일 실시예에 있어서, 상기 마지막 제1 형 블록은, 둘 이상의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하고, 상기 해시값은, 각각의 마지막 제2 형 블록의 적어도 일부로부터 생성된 머클 트리의 루트에 대한 해시값일 수 있다.
- [15] 본 발명의 일 실시예에 있어서, 상기 마지막 제2 형 블록은, 상기 마지막 제1 형 블록보다 이전에 생성된 블록일 수 있다.
- [16] 또한, 상기 과제를 해결하기 위한 본 발명의 블록체인 시스템은, 적어도 하나의 제1 형 블록을 포함하고, 상기 제1 형 블록들은 각각 블록의 생성 순서에 따라 연결된 메인 브랜치 및 하나의 제1 형 블록 및 적어도 하나의 제2 형 블록을 포함하고, 상기 제2 형 블록은 상기 제1 형 블록을 루트 블록으로 하여 연결된 적어도 하나의 서브 브랜치를 포함하고, 하나의 서브 브랜치의 상기 제2 형 블록은 각각 블록의 생성 순서에 따라 연결되되, 상기 하나의 서브 브랜치에서 최초로 생성된 제2 형 블록은 상기 루트 블록에 연결되고, 상기 메인 브랜치의

- 임의의 제1 형 블록은, 상기 임의의 제1 형 블록보다 이전에 생성된 제2 형 블록 중 일부 블록의 적어도 일부의 해시값을 포함한다.
- [17] 본 발명의 일 실시예에 있어서, 상기 임의의 제1 형 블록은, 상기 메인 브랜치에 포함되고 상기 임의의 제1 형 블록보다 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 더 포함할 수 있다.
- [18] 본 발명의 일 실시예에 있어서, 상기 임의의 제1 형 블록은, 상기 일부 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 구분하여 포함할 수 있다.
- [19] 본 발명의 일 실시예에 있어서, 상기 임의의 제1 형 블록은, 상기 일부 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 블록헤더에 포함할 수 있다.
- [20] 본 발명의 일 실시예에 있어서, 상기 일부 블록은, 상기 임의의 제1 형 블록이 생성될 때, 상기 서브 브랜치의 마지막 블록일 수 있다.
- [21] 본 발명의 일 실시예에 있어서, 상기 일부 블록은, 상기 임의의 제1 형 블록이 생성될 때, 모든 서브 브랜치의 마지막 블록일 수 있다.
- [22] 본 발명의 일 실시예에 있어서, 상기 일부 블록은, 상기 임의의 제1 형 블록이 생성될 때, 상기 서브 브랜치의 마지막 블록이되, 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 블록일 수 있다.
- [23] 본 발명의 일 실시예에 있어서, 상기 일부 블록은 둘 이상의 블록이고, 상기 해시값은, 상기 일부 블록의 각각의 블록의 적어도 일부로부터 생성된 머클 트리의 루트에 대한 해시값일 수 있다.
- [24] 또한, 상기 과제를 해결하기 위한 본 발명의 블록체인 생성 방법은 적어도 하나의 제1 형 블록을 포함하고, 상기 제1 형 블록들은 각각 블록의 생성 순서에 따라 연결된 메인 브랜치 및 하나의 제1 형 블록 및 적어도 하나의 제2 형 블록을 포함하고, 상기 제2 형 블록은 상기 제1 형 블록을 루트 블록으로 하여 연결된 적어도 하나의 서브 브랜치를 포함하고, 하나의 서브 브랜치의 상기 제2 형 블록은 각각 블록의 생성 순서에 따라 연결되되, 상기 하나의 서브 브랜치에서 최초로 생성된 제2 형 블록은 상기 루트 블록에 연결되는 블록체인을 마련하는 단계 및 새로운 제1 형 블록을 상기 메인 브랜치의 마지막 제1 형 블록에 연결되도록 생성하는 단계를 포함하고, 상기 새로운 제1 형 블록은, 상기 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함한다.
- [25] 본 발명의 일 실시예에 있어서, 상기 새로운 제1 형 블록은, 상기 마지막 제1 형 블록의 적어도 일부의 해시값을 더 포함할 수 있다.
- [26] 본 발명의 일 실시예에 있어서, 상기 새로운 제1 형 블록은, 상기 마지막 제2 형 블록의 적어도 일부의 해시값과 상기 마지막 제1 형 블록의 적어도 일부의 해시값을 구분하여 포함할 수 있다.
- [27] 본 발명의 일 실시예에 있어서, 상기 새로운 제1 형 블록은, 상기 마지막 제2 형 블록의 적어도 일부의 해시값과 상기 마지막 제1 형 블록의 적어도 일부의

해시값을 블록헤더에 포함할 수 있다.

[28] 본 발명의 일 실시예에 있어서, 상기 새로운 제1 형 블록은, 모든 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함할 수 있다.

[29] 본 발명의 일 실시예에 있어서, 상기 새로운 제1 형 블록은, 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 마지막 제2 형 블록의 적어도 일부의 해시값을 포함할 수 있다.

[30] 본 발명의 일 실시예에 있어서, 상기 새로운 제1 형 블록은, 둘 이상의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하고, 상기 해시값은, 각각의 마지막 제2 형 블록의 적어도 일부로부터 생성된 머클 트리의 루트에 대한 해시값일 수 있다.

[31] 본 발명의 일 실시예에 있어서, 상기 마지막 제2 형 블록은, 상기 새로운 제1 형 블록보다 이전에 생성된 블록일 수 있다.

발명의 효과

[32] 본 발명의 일 실시예에 따른 블록체인 시스템은 블록들이 복수의 브랜치로 연결되도록 구성하여 데이터를 효율적이고 체계적으로 관리할 수 있다.

[33] 또한, 본 발명의 일 실시예에 따른 블록체인 시스템은 블록들이 복수의 브랜치로 연결되더라도 모든 블록의 위변조에 대한 안전성을 확보할 수 있다.

도면의 간단한 설명

[34] 도 1은 본 발명의 일 실시예에 따른 블록체인 시스템의 개별 블록의 구성을 도시한 것이다.

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

[36] 도 3은 본 발명의 일 실시예에 따른 블록체인 시스템의 데이터를 설명하기 위한 도면이다.

[37] 도 4는 블록체인에서 블록의 표시 방법을 설명하기 위한 도면이다.

[38] 도 5는 본 발명의 일 실시예에 따른 블록체인 시스템의 예시 도면이다.

[39] 도 6은 본 발명의 일 실시예에 따른 블록체인 시스템의 마지막 제1 형 블록을 설명하기 위한 도면이다.

[40] 도 7은 본 발명의 다른 일 실시예에 따른 블록체인 시스템의 예시 도면이다.

[41] 도 8 및 도 9는 본 발명의 또 다른 일 실시예에 따른 블록체인 시스템의 예시 도면이다.

[42] 도 10은 본 발명의 일 실시예에 따른 블록체인을 이용한 데이터 관리 방법을 설명하기 위한 순서도이다.

발명의 실시를 위한 최선의 형태

[43] 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.

[44]

[45] 이하, 첨부한 도 1 내지 도 5를 참조하여, 본 발명의 일 실시예에 따른 블록체인 시스템에 대해 설명한다.

[46] 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.

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

[48] 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.

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

[50] 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.

[51] 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.

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

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

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

[55] 블록헤더(110)에는 상술한 정보 중 일부가 제외될 수도 있고, 다른 정보가

추가로 포함될 수도 있다.

- [56] 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, 거래 정보, 인사 정보, 생산 이력 정보, 제품 또는 건축물의 설계 및 도면, 사운드 정보 등이 가능하며, 특정한 형태로 한정되는 것은 아니다.
- [57] 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.
- [58]
- [59] 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.
- [60] 도 2를 참조하면, 브랜치에서 임의의 하나의 블록(200)은 브랜치 내에서 직전에 생성된 블록(100)과 연결되게 된다. 블록(200)은 직전에 생성된 블록(100)의 해시값을 포함하는 것을 통해 연결된다. 구체적으로, 블록(200)은 블록헤더(210)에 직전에 생성된 블록(100)의 해시값을 포함하는 것을 통해 연결될 수 있다.
- [61] 직전에 생성된 블록(100)의 해시값은 상술한 것과 같이, 직전 블록(100)의 전체 또는 선택된 일부의 정보의 해시값일 수 있다. 예를 들어, 첨부한 도 2에 도시된 것과 같이 직전 블록(100)의 해시값은 직전 블록의 블록헤더(110)의 정보의 해시값인 것으로 정의될 수 있다. 직전 블록의 해시값은 블록을 설계하는 사람의 기호 및 판단에 따라 다양하게 변경될 수 있다.
- [62]
- [63] 도 3을 참조하여, 본 발명의 일 실시예에 따른 블록체인 시스템의 데이터에 대해 설명하도록 한다.
- [64] 본 발명의 블록체인 시스템은 복수의 블록을 포함한다. 하나의 블록은 하나의 데이터를 포함한다. 여기서 데이터는 하나의 블록에 포함되는 정보의 단위 집합을 의미한다. 구체적으로, 블록의 블록몸체는 데이터를 포함할 수 있다.
- [65] 블록체인 시스템의 블록이 포함하는 데이터는 제1 형 데이터 및 제2 형 데이터로 구분될 수 있다. 제1 형 데이터는 다른 데이터에 기반하지 않은 데이터에 해당한다. 제2 형 데이터는 제1 형 데이터에 기반한 데이터에 해당한다.
- [66] 도 3을 참조하면, 제1 형 데이터(10)는 신규 자료를 생성하는 것에 관한 데이터일 수 있다. 그리고 제2 형 데이터(20)는 기존 자료를 수정, 변경, 삭제, 폐기, 조회 및 전달 중 적어도 어느 하나를 수행하는 것에 관한 데이터일 수 있다.

여기서, 기존 자료란 제1 형 데이터(10)가 생성한 자료를 의미한다.

[67] 구체적으로, 데이터는 디지털 콘텐츠, 문서, 계좌, 거래, 인사, 생산 이력, 설계, 도면, 사운드, 프로그래밍 코드 등이 될 수 있다. 그리고 제1 형 데이터 및 제2 형 데이터도 이러한 다양한 종류에 따라 구분될 수 있다. 제1 형 데이터 및 제2 형 데이터는 상술한 것에 한정되지 않는다.

[68]

[69] 도 4를 참조하여, 도 5 내지 도 9에서 도시되는 블록체인을 구성하는 블록에 대해서 간략하게 설명하도록 한다.

[70] 블록은 도 1 및 도 2를 참조하여 설명한 것과 같이, 블록헤더와 블록몸체를 포함한다. 그러나 설명의 편의성을 위해 도 5 내지 도 9에서는 도 3에 도시된 방식으로 개별 블록을 표시하도록 한다.

[71] 도 3을 참조하면, 하나의 블록을 설명하는데 있어서, 블록의 타이틀, 직전 블록의 해시값 및 당해 블록의 해시값이 표시된다. 하나의 블록은 상하로 배열된 3칸의 표에서, 첫번째 칸에는 블록의 타이틀이 표시되고, 두번째 칸에는 직전 블록의 해시값이 표시되고, 세번째 칸에는 당해 블록의 해시값이 표시된다.

[72] 아래에서 설명할 마지막 제1 형 블록은 마지막 제2 형 노드의 해시값을 더 포함할 수 있다. 또한, 마지막 제1 형 블록을 설명하는데 있어서, 블록의 타이틀, 직전 블록의 해시값 및 당해 블록의 해시값에 더불어 마지막 제2 형 노드의 해시값이 추가로 표시될 수 있다. 마지막 제1 형 블록은 상하로 배열된 4칸의 표에서, 첫번째 칸에는 블록의 타이틀이 표시되고, 두번째 칸에는 직전 블록의 해시값이 표시되고, 세번째 칸에는 마지막 제2 형 노드의 해시값이 표시되고, 네번째 칸에는 당해 블록의 해시값이 표시된다. 마지막 제2 형 노드의 해시값에 대해서는 아래에서 상세하게 설명하도록 한다.

[73] 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 제2 형 블록이라는 것을 의미한다. 임의의 서브 브랜치의 m 번째 제2 형 블록은 상기 서브 브랜치의 $m+1$ 번째 블록에 해당한다.

[74] 어느 블록의 해시값은 H 라는 기호를 이용하여 표시된다. 예를 들어, 블록의 타이틀이 B_{nm} 인 블록의 해시값은 H_{nm} 으로 표시되게 된다. 도 4를 참조하면, 블록의 타이틀이 B_{nm} 인 블록의 직전 블록은 블록의 타이틀이 $B_{n(m-1)}$ 인 블록인 것이고, 직전 블록의 해시값은 $H_{n(m-1)}$ 인 것이다.

[75] 상기 블록의 타이틀, 해시값의 기호 등을 설명하면서 언급한 메인 브랜치, 서브 브랜치, 제2 형 블록 등에 대해서는 이하 도 5를 참조하여 상세하게 설명하도록 한다.

[76]

[77] 도 5를 참조하여, 본 발명의 일 실시예에 따른 블록체인 시스템에 대해서

설명하도록 한다. 도 5는 본 발명의 일 실시예에 따른 블록체인 시스템의 예시 도면이다.

- [78] 본 발명의 블록체인 시스템은 복수의 블록을 포함한다. 하나의 블록은 하나의 데이터를 포함한다. 상술한 것과 같이, 데이터는 제1 형 데이터(10) 및 제2 형 데이터(20)로 구분될 수 있다. 블록은 포함하는 데이터의 종류에 따라 제1 형 블록(100) 및 제2 형 블록(200)으로 구분될 수 있다. 제1 형 블록(100)은 제1 형 데이터(10)를 포함하는 블록에 해당한다. 또한, 제2 형 블록(200)은 제2 형 데이터(20)를 포함하는 블록에 해당한다.
- [79] 본 발명의 블록체인 시스템은 메인 브랜치(1000) 및 적어도 하나의 서브 브랜치(2000)를 포함한다. 여기서, 브랜치란 복수의 블록들이 서로 선형적으로 연결된 블록들의 집합을 의미한다.
- [80] 메인 브랜치(1000)는 최초로 생성된 블록(genesis block)과 이에 연결된 적어도 하나의 연결 블록을 포함한다. 메인 브랜치(1000)는 최초로 생성된 블록에서 연결 블록이 일 방향으로 분기되지 않고 연결된다. 메인 브랜치(1000)에서 분기되어 다른 브랜치가 형성될 수는 있지만 분기된 블록들은 메인 브랜치(1000)에 포함되는 것이 아니다. 분기된 블록들은 후술할 서브 브랜치(2000)에 포함될 수 있으며, 이에 대해서는 아래에서 설명하도록 한다.
- [81] 메인 브랜치(1000)는 제1 형 블록(100)들로 구성된다. 즉, 메인 브랜치(1000)가 포함하는 최초로 생성된 블록 및 연결 블록은 모두 제1 형 블록(100)에 해당한다. 메인 브랜치(1000)가 포함하는 블록들은 생성된 순서에 따라 순서대로 연결된다. 블록의 연결은 당해 블록이 직전에 생성된 블록의 적어도 일부의 해시값을 포함하는 것에 의해 달성된다. 이러한 연결 형태에 대해서는 도 5에 블록 사이의 화살표를 통해 표시되어 있다. 따라서 최초로 생성된 블록을 제외하고 하나의 제1 형 블록은 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 포함한다.
- [82] 서브 브랜치(2000)는 메인 브랜치(1000)로부터 분기되어 형성된 브랜치이다. 서브 브랜치(2000)는 루트 블록(root block)과 이에 연결된 적어도 하나의 연결 블록을 포함한다. 루트 블록은 메인 브랜치(1000)에도 포함되는 블록으로, 서브 브랜치(2000)의 분기가 시작되는 블록이다. 루트 블록은 당해 서브 브랜치(2000)에서 최초로 생성된 블록(genesis block)에 해당한다.
- [83] 여기서, 루트 블록은 제1 형 블록(100)에 해당한다. 그리고 서브 브랜치(2000)가 포함하는 연결 블록은 제2 형 블록(200)에 해당한다. 하나의 서브 브랜치(2000)가 포함하는 블록들은 생성된 순서에 따라 순서대로 연결된다. 블록의 연결은 당해 블록이 직전에 생성된 블록의 적어도 일부의 해시값을 포함하는 것에 의해 달성된다. 따라서 하나의 서브 브랜치(2000)에서 최초로 생성된 연결 블록(제2 형 블록)은 당해 서브 브랜치(2000)의 연결되는 루트 블록의 적어도 일부의 해시값을 포함한다. 또한, 하나의 서브 브랜치(2000)에서 최초로 생성되지 않은 연결 블록(제2 형 블록)은 당해 서브 브랜치(2000)에 포함되고 직전에 생성된 제2 형 블록의 적어도 일부의 해시값을 포함한다. 이러한 연결 형태에 대해서는 도

5에 블록 사이의 화살표를 통해 표시되어 있다.

- [84] 서브 브랜치(2000)는 적어도 하나의 연결 블록(제2 형 블록)을 포함하는 것을 조건으로 한다. 경우에 따라서, 연결 블록(제2 형 블록)이 없고 루트 블록(제1 형 블록)만이 존재하는 높이(길이)가 1개 블록인 서브 브랜치를 생각해볼 수도 있겠지만, 본 명세서에서는 이러한 경우 그러한 서브 브랜치가 존재하지 않는 것으로 정의한다. 즉, 설명의 편의성을 위해서 서브 브랜치(2000)는 하나의 루트 블록(제1 형 블록)과 이에 연결된 적어도 하나의 연결 블록(제2 형 블록)이 있는 것을 조건으로 정의한다.
- [85] 서브 브랜치(2000)는 하나 또는 둘 이상이 형성될 수 있다. 서브 브랜치(2000)는 하나의 루트 블록에서 하나 또는 둘 이상이 연장되는 형태로 형성될 수 있다. 그러나 첨부한 도면 및 이하에서는 설명의 편의성을 위해서 하나의 루트 블록에서 하나의 서브 브랜치(2000)만이 형성되는 것을 예를 들어 설명하도록 한다. 그러나 이러한 설명이 본 발명에서 하나의 루트 블록에서 둘 이상의 서브 브랜치(2000)가 연장되는 것을 제외하는 것은 아니다.
- [86] 하나의 루트 블록에서 하나의 서브 브랜치(2000)가 연장되어 형성되는 경우라면, 서브 브랜치(2000)는 최대 메인 브랜치(1000)의 블록의 개수까지 형성되는 것이 가능하다.
- [87] 도 5에서는 블록체인 시스템이 메인 브랜치(1000)와 서브 브랜치(2000)로 구성되고, 블록들이 제1 형 블록(100)과 제2 형 블록(200)으로 구성되는 것을 도시하였지만, 경우에 따라서는 메인 브랜치, 서브 브랜치 및 서브-서브 브랜치로 구성되고, 블록들도 제1 형 블록, 제2 형 블록 및 제3 형 블록으로 구성될 수도 있다. 여기서, 서브-서브 브랜치는 서브 브랜치를 메인 브랜치로 하고, 서브 브랜치에서 다시 분기된 브랜치를 의미한다. 서브-서브 브랜치의 루트 블록은 서브 브랜치에 포함되는 제2 형 블록이 될 수 있다. 그리고 서브-서브 브랜치의 연결 블록은 제3 형 블록이 될 수 있다. 이와 같이, 본 발명의 블록체인 시스템에서 메인 브랜치와 서브 브랜치는 상대적인 것으로, 서브 브랜치가 연쇄적으로 생성될 수 있다.
- [88] 이하, 도 5를 참조하여, 마지막 제1 형 블록(190)에 대해서 설명하도록 한다. 도 5에 도시된 블록체인 시스템은 본 발명의 블록체인 시스템의 일 예시에 불과하고, 이러한 블록체인 시스템의 마지막 제1 형 블록(190)도 본 발명의 설명을 위한 예시에 불과하다.
- [89] 도 5를 참조하면, 메인 브랜치(1000)에는 마지막 블록(190)이 존재한다. 마지막 블록(190)은 마지막 제1 형 블록에 해당한다. 구체적으로, 마지막 블록(190)은 메인 브랜치(1000)에서 최초로 생성된 블록을 시작으로 하여 연결된 브랜치의 마지막 제1 형 블록(190)에 해당한다. 도 5에서는 마지막 제1 형 블록(190)이 B_s 블록에 해당한다. 도 5에 있어서, 마지막 제1 형 블록(190)은 도 5에 도시된 다른 모든 블록보다 마지막에 생성된 블록에 해당한다.
- [90] 도 5에 도시된 마지막 제1 형 블록(B_s, 190)은 직전 블록의 해시값(H₄) 등 다른

블록의 해시값을 포함하지만, 마지막 제1 형 블록의 해시값(H_5)은 다른 블록에 포함되지 않는다. 이후에 메인 브랜치(1000)에 추가로 제1 형 블록이 연결되도록 생성된다면, 상기 마지막 제1 형 블록의 해시값(H_5)이 추가로 생성되는 블록에 포함될 수 있지만, 도 5를 참조하여 설명하는 시점에서는 마지막 제1 형 블록의 해시값(H_5)은 다른 블록에 포함되지 않는다.

- [91] 마지막 제1 형 블록($B_5, 190$)은 직전 블록의 해시값(H_4) 이외에 다른 블록의 해시값을 추가로 포함한다. 여기서, 직전 블록의 해시값(H_4)은 메인 브랜치(1000)에 포함되고 상기 마지막 제1 형 블록($B_5, 190$)보다 직전에 생성된 제1 형 블록(B_4)의 적어도 일부의 해시값에 해당한다. 그리고 다른 블록의 해시값이란 상기 직전 블록의 해시값과 구분되는 해시값이다. 이하, 상기 다른 블록의 해시값에 대해서 상세하게 설명한다.
- [92] 도 5를 참조하면, 마지막 제1 형 블록($B_5, 190$)은 서브 브랜치(2000)의 마지막 제2 형 블록(290)의 적어도 일부의 해시값(H_{sum})을 포함할 수 있다. 여기서, 마지막 제2 형 블록(290)의 범위는 마지막 제1 형 블록($B_5, 190$)이 생성되는 시점에서 결정된다. 구체적으로, 서브 브랜치(2000)는 마지막 제1 형 블록($B_5, 190$)보다 이전에 생성된 메인 브랜치(1000)의 제1 형 블록(B_1, B_2, B_3, B_4)을 루트 블록으로 하여 연결되는 브랜치이다. 그리고 마지막 제2 형 블록(290)은 이러한 서브 브랜치(2000)의 루트 블록을 시작으로 하여 연결된 브랜치의 마지막 제2 형 블록(290)에 해당한다. 이러한 마지막 제2 형 블록(290)은 상기 마지막 제1 형 블록($B_5, 190$)보다 이전에 생성된 블록이다. 즉, 여기서 마지막 제2 형 블록(290)이란 마지막 제1 형 블록($B_5, 190$)이 생성될 때, 서브 브랜치(2000)의 마지막 블록에 해당하는 블록을 의미한다.
- [93] 마지막 제1 형 블록($B_5, 190$)이 생성되는 시점에서 복수의 서브 브랜치(2000)가 존재할 수 있다. 그리고 마지막 제2 형 블록(290)도 복수로 존재할 수 있다. 구체적으로, 마지막 제2 형 블록(290)은 복수의 서브 브랜치에 각각 하나씩 존재한다. 도 5에서는 마지막 제2 형 블록(290)이 B_{13}, B_{33} 및 B_{44} 인 것으로 도시되어 있다. 상술한 것과 같이, 서브 브랜치(2000)는 적어도 하나의 제2 형 블록(290)을 포함하는 것을 조건으로 하기 때문에 서브 브랜치(2000)의 개수만큼 마지막 제2 형 블록(290)이 존재하게 된다.
- [94] 도 5에 도시된 것과는 다르지만, 마지막 제2 형 블록(290)이 하나가 존재하는 경우, 마지막 제1 형 블록(190)은 하나의 마지막 제2 형 블록(290)의 적어도 일부의 해시값을 포함할 수 있다.
- [95] 또한, 도 5에 도시된 것과 같이, 마지막 제2 형 블록(290)이 복수로 존재하는 경우, 마지막 제1 형 블록($B_5, 190$)은 모든 마지막 제2 형 블록(B_{13}, B_{33}, B_{44})의 적어도 일부의 해시값을 포함할 수 있다. 여기서, 마지막 제2 형 블록(B_{13}, B_{33}, B_{44})의 적어도 일부의 해시값은 마지막 제2 형 블록(B_{13}, B_{33}, B_{44})의 블록헤더의 해시값일 수 있다.
- [96] 이러한 마지막 제2 형 블록의 적어도 일부의 해시값(H_{sum})은 마지막 제1 형

블록(B₅, 190)의 블록헤더에 포함될 수 있다. 마지막 제1 형 블록(B₅, 190)의 블록헤더에는, 마지막 제2 형 블록의 적어도 일부의 해시값(H_{sum})과 메인 브랜치에 포함되고 마지막 제1 형 블록(B₅, 190)보다 직전에 생성된 제1 형 블록의 적어도 일부의 해시값(H₄)이 포함될 수 있다. 상기 마지막 제2 형 블록의 적어도 일부의 해시값(H_{sum})과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값(H₄)은 마지막 제1 형 블록(B₅, 190)의 블록헤더에서 구분되어 포함될 수 있다. 따라서 마지막 제2 형 블록(290) 및 메인 브랜치(1000)의 검증을 위해 상기 해시값들(H_{sum}, H₄) 이 사용될 수 있다. 이러한 해시값(H_{sum}, H₄)들이 포함된 마지막 제1 형 블록(190)의 블록헤더의 해시값(H₅)은 이후에 메인 브랜치(1000)에 추가로 제1 형 블록이 연결되도록 생성된다면, 추가로 생성되는 블록에 포함되어 연쇄적으로 연결되게 된다.

[97]

[98] 도 6을 참조하여, 마지막 제1 형 블록(B₅, 190)이 복수의 마지막 제2 형 블록의 적어도 일부의 해시값(H_{sum})을 포함하는 경우에 대해서 설명하도록 한다. 마지막 제2 형 블록(290)이 복수인 경우, 마지막 제1 형 블록(190)이 포함하는 해시값은 각각의 마지막 제2 형 블록(290)의 적어도 일부로부터 생성된 머클 트리의 루트에 대한 해시값(H_{sum})일 수 있다. 구체적으로, 마지막 제1 형 블록(190)은 각각의 마지막 제2 형 블록의 블록헤더의 해시값(H₁₃, H₃₃, H₄₄)으로부터 생성된 머클 트리의 루트에 대한 해시값(H_{sum})을 포함할 수 있다.

[99]

[100] 도 5 및 도 6을 참조하여 설명한 블록체인 시스템은 특정 블록의 검증을 위해서 전체 블록체인 데이터를 저장하고 이용하지 않을 수 있다. 구체적으로, 특정 블록이 제1 형 블록(100)일 경우, 노드는 메인 브랜치(1000)의 블록체인 데이터만을 이용하여 상기 특정 블록의 검증이 가능하다. 또한, 특정 블록이 제2 형 블록(200)일 경우, 노드는 상기 특정 블록이 포함된 서브 브랜치(2000)와 메인 브랜치(1000)의 블록체인 데이터만을 이용하여 상기 특정 블록의 검증이 가능하다. 이에 따라 노드가 저장하고 검증해야 하는 블록의 크기를 줄일 수 있다.

[101] 또한, 상술한 마지막 제1 형 블록(190)이 마지막 제2 형 블록(290)의 적어도 일부의 해시값(H_{sum})을 포함하는 것에 의해서, 마지막 제2 형 블록(290)의 안전성이 강화될 수 있다.

[102] 통상적인 블록체인 시스템에서는 마지막 블록의 안전성이 상대적으로 취약하다는 단점이 있다. 이는 마지막 블록은 그것의 해시값이 다른 블록에 다시 포함되지 않기 때문이다. 상술한 메인 브랜치 및 적어도 하나의 서브 브랜치를 포함하는 블록체인 시스템은 브랜치의 개수만큼 마지막 블록이 존재하여, 상대적으로 안전성이 취약한 마지막 블록이 많을 수 있다.

[103] 그러나 상술한 것과 같이 마지막 제1 형 블록(190)이 마지막 제2 형 블록(290)의 적어도 일부의 해시값(H_{sum})을 포함하여, 마지막 제2 형 블록(290)의 안전성을

확보할 수 있다. 구체적으로, 마지막 제2 형 블록(290)은 개별 서브 브랜치(2000)의 마지막 블록이지만, 그것의 해시값이 마지막 제1 형 블록(190)에 포함되게 되어 상술한 취약성이 극복될 수 있다. 결과적으로, 본 발명의 블록체인 시스템에서 실질적인 마지막 블록은 통상적인 블록체인 시스템과 마찬가지로 하나만 존재하게 된다.

[104]

[105] 도 7을 참조하여 본 발명의 다른 일 실시예에 따른 블록체인 시스템에 대해서 설명하도록 한다.

[106] 도 7을 참조하여 설명하는 블록체인 시스템은 도 5 및 도 6을 참조하여 상술한 블록체인 시스템과 마지막 제1 형 블록(190)이 포함하는 마지막 제2 형 블록의 적어도 일부의 해시값에서 차이가 있다. 따라서 설명의 편의성을 위해서 본 실시예의 블록체인 시스템을 설명하는데 있어서, 도 5 및 도 6을 참조하여 상술한 것과 다른 점을 중심으로 설명하도록 한다.

[107] 도 7에 있어서, 마지막 제1 형 블록(190)은 도 7에 도시된 다른 모든 블록보다 마지막에 생성된 블록에 해당한다.

[108] 도 7을 참조하면, 마지막 제1 형 블록(190)은 서브 브랜치의 마지막 제2 형 블록(290)의 적어도 일부의 해시값(H_{sum})을 포함할 수 있다. 여기서, 마지막 제1 형 블록(190)은 마지막 제2 형 블록(290) 중 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 마지막 제2 형 블록의 적어도 일부의 해시값을 포함할 수 있다. 즉, 상기 마지막 제1 형 블록(190)이 생성되기 전에, 다른 제1 형 블록이 생성되면서 적어도 일부의 해시값이 상기 다른 제1 형 블록에 포함된 제2 형 블록은 상기 마지막 제1 형 블록(190)이 포함하는 해시값의 마지막 제2 형 블록에 해당하지 않게 된다.

[109] 도 7에 도시된 예시의 블록체인 시스템을 참고로 하여 설명하면, 마지막 제1 형 블록($B_5, 190$)이 생성되는 시점에 마지막 제2 형 블록(290)은 B_{13}, B_{33} 및 B_{44} 이 존재한다. 그러나 B_{13} 이 생성되고, B_{33} 및 B_{44} 이 생성되기 전에 B_2 가 생성되게 된다. B_2 가 생성되는 시점에서, B_{13} 의 적어도 일부의 해시값(H_{13})이 B_2 에 포함되게 된다.

[110] 따라서 마지막 제1 형 블록($B_5, 190$)이 생성되는 시점의 마지막 제2 형 블록(290) 중 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 마지막 제2 형 블록은 B_{33} 및 B_{44} 만 해당한다. 따라서 마지막 제1 형 블록($B_5, 190$)은 B_{33} 및 B_{44} 의 적어도 일부의 해시값을 포함한다. 구체적으로, 마지막 제1 형 블록($B_5, 190$)은 B_{33} 및 B_{44} 의 블록헤더의 해시값(H_{33}, H_{44})으로부터 생성된 머클 트리의 루트에 대한 해시값(H_{sum})을 포함할 수 있다.

[111] 이러한 경우, 마지막 제1 형 블록이 생성되는 시점에, 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 마지막 제2 형 블록이 존재하지 않을 수 있다. 도 7에 도시된 예시의 블록체인 시스템에서 B_3 및 B_4 는 이러한 경우에 해당한다. 이런 경우, 마지막 제1 형 블록은 메인 브랜치에 포함되고 마지막 제1 형

블록보다 직전에 생성된 제1 형 블록의 적어도 일부의 해시값만을 포함하고, 마지막 제2 형 블록의 적어도 일부의 해시값은 포함하지 않을 수 있다.

[112] 이러한 방식에 따르면, 마지막 제2 형 블록은 한 번만 그것의 적어도 일부의 해시값이 마지막 제1 형 블록에 포함되게 된다. 따라서 마지막 제1 형 블록이 생성되면서 포함해야 하는 마지막 제2 형 블록의 개수가 도 5를 참조하여 상술한 실시예의 경우보다 감소하게 된다. 도 5를 참조하여 상술한 실시예의 경우, 마지막 제2 형 블록의 안전성을 향상시킬 수 있지만 블록체인의 규모가 커지면 새로운 마지막 제1 형 블록이 참조해야 할 마지막 제2 형 블록의 개수가 점차 증가하게 된다. 이는 블록체인의 효율성을 떨어뜨리는 요인이 될 수 있다. 따라서 도 7을 참조하여 설명한 실시예에 따르면 마지막 제2 형 블록의 안전성도 향상시키면서, 블록체인의 효율성을 확보할 수 있다는 장점이 있다.

[113] 도 5 내지 도 7을 참조하여, 본 발명의 다양한 실시예들에 따른 블록체인 시스템과 마지막 제1 형 블록에 대해서 상세하게 설명하였다.

[114] 그러나 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하는 마지막 제1 형 블록은 메인 브랜치에 다른 제1 형 블록이 생성되어 연결됨에 따라 마지막 제1 형 블록에는 해당하지 않게 된다. 따라서 제2 형 블록의 적어도 일부의 해시값을 포함하는 제1 형 블록이 메인 브랜치의 마지막 블록이 아닌 경우를 포함하는 블록체인 시스템에 대해서 추가로 설명하도록 한다.

[115]

[116] 도 8은 본 발명의 일 실시예에 따른 블록체인 시스템의 예시 도면이다. 도 8을 참조하여, 본 발명의 또 다른 일 실시예에 따른 블록체인 시스템에 대해서 설명하도록 한다.

[117] 도 8에는 각 블록의 생성 순서가 빨간색의 글자로 표시되어 있다. 이러한 생성 순서를 참조하여 블록체인 시스템에 대해서 설명하도록 한다.

[118] 도 8의 실시예에서, 메인 브랜치의 임의의 제1 형 블록은 임의의 제1 형 블록보다 이전에 생성된 제2 형 블록 중 일부 블록의 적어도 일부의 해시값을 포함한다. 구체적으로, 상기 일부 블록은 상기 임의의 제1 형 블록이 생성될 때, 서브 브랜치의 마지막 블록일 수 있다. 더욱 구체적으로, 상기 일부 블록은 상기 임의의 제1 형 블록이 생성될 때, 모든 서브 브랜치의 마지막 블록일 수 있다. 이러한 내용에 대해서 도 8에 도시된 예시의 블록체인 시스템을 참조하여 설명하도록 한다.

[119] B_2 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록은 B_{11} 블록이다. 따라서 B_2 블록은 B_{11} 블록의 적어도 일부의 해시값(H_{11})을 포함한다. 그리고 B_2 블록은 해시값(H_{11})과 구분되도록 메인 브랜치에 포함되고 B_2 블록보다 직전에 생성된 제1 형 블록(B_1 블록)의 적어도 일부의 해시값(H_1)을 포함한다.

[120] B_3 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록도 B_{11} 블록이다. B_3 블록이 생성될 때 B_2 블록을 루트블록으로 하는 서브 브랜치가 없으므로, B_3 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록은 B_{11} 블록이 유일하다.

따라서 B_3 블록은 B_{11} 블록의 적어도 일부의 해시값(H_{11})을 포함한다. 그리고 B_3 블록은 해시값(H_{11})과 구분되도록 메인 브랜치에 포함되고 B_3 블록보다 직전에 생성된 제1 형 블록(B_2 블록)의 적어도 일부의 해시값(H_2)을 포함한다.

[121] B_4 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록은 B_{13} 및 B_{32} 블록이다. 따라서 B_4 블록은 B_{13} 및 B_{32} 블록의 적어도 일부의 해시값(H_{sum})을 포함한다. 그리고 B_4 블록은 해시값(H_{sum})과 구분되도록 메인 브랜치에 포함되고 B_4 블록보다 직전에 생성된 제1 형 블록(B_3 블록)의 적어도 일부의 해시값(H_3)을 포함한다.

[122] B_5 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록은 B_{13} , B_{33} 및 B_{43} 블록이다. 따라서 B_5 블록은 B_{13} , B_{33} 및 B_{44} 블록의 적어도 일부의 해시값(H_{sum})을 포함한다. 그리고 B_5 블록은 해시값(H_{sum})과 구분되도록 메인 브랜치에 포함되고 B_5 블록보다 직전에 생성된 제1 형 블록(B_4 블록)의 적어도 일부의 해시값(H_4)을 포함한다.

[123] B_5 블록이 생성된 이후에 B_{44} 블록이 생성된다. B_{44} 블록까지 생성된 것이 도 8에 도시된 블록체인 시스템의 상태이다. 이후에 다른 제2 형 블록이 생성되지 않고, 추가로 제1 형 블록이 생성된다면, 이 때 존재하는 서브 브랜치의 마지막 블록은 B_{13} , B_{33} 및 B_{44} 블록이다. 따라서 새롭게 생성되는 마지막 제1 형 블록은 B_{13} , B_{33} 및 B_{44} 블록의 적어도 일부의 해시값을 포함하게 된다.

[124]

[125] 도 9를 참조하여, 본 발명의 또 다른 일 실시예에 따른 블록체인 시스템에 대해서 설명하도록 한다. 도 9는 본 발명의 일 실시예에 따른 블록체인 시스템의 예시 도면이다.

[126] 도 9에는 각 블록의 생성 순서가 빨간색의 글자로 표시되어 있다. 이러한 생성 순서를 참조하여 블록체인 시스템에 대해서 설명하도록 한다. 도 9는 도 8에 도시된 블록체인 시스템과 각각의 블록의 연결 및 생성 순서가 동일한 것을 도시한 것이다.

[127] 도 9의 실시예에서, 메인 브랜치의 임의의 제1 형 블록은 임의의 제1 형 블록보다 이전에 생성된 제2 형 블록 중 일부 블록의 적어도 일부의 해시값을 포함한다. 구체적으로, 상기 일부 블록은 임의의 제1 형 블록이 생성될 때, 서브 브랜치의 마지막 블록일 수 있다. 더욱 구체적으로, 상기 일부 블록은 임의의 제1 형 블록이 생성될 때, 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 블록일 수 있다. 이러한 내용에 대해서 도 9에 도시된 예시의 블록체인 시스템을 참조하여 설명하도록 한다.

[128] B_2 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록은 B_{11} 블록이다. B_{11} 블록은 그것의 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 블록이다. 따라서 B_2 블록은 B_{11} 블록의 적어도 일부의 해시값(H_{11})을 포함한다. 그리고 B_2 블록은 해시값(H_{11})과 구분되도록 메인 브랜치에 포함되고 B_2 블록보다 직전에 생성된 제1 형 블록(B_1 블록)의 적어도 일부의 해시값(H_1)을 포함한다.

- [129] B_3 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록도 B_{11} 블록이다. B_3 블록이 생성될 때 B_2 블록을 루트블록으로 하는 서브 브랜치가 없으므로, B_3 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록은 B_{11} 블록이 유일하다. 그러나 B_{11} 블록은 그것의 적어도 일부의 해시값이 이미 B_2 블록에 포함되어 있다. 따라서 B_3 블록은 메인 브랜치에 포함되고 B_3 블록보다 직전에 생성된 제1 형 블록(B_2 블록)의 적어도 일부의 해시값(H_2)만을 포함하고, 제2 형 블록의 적어도 일부의 해시값은 포함하지 않는다.
- [130] B_4 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록은 B_{13} 및 B_{32} 블록이다. B_{13} 및 B_{32} 블록은 그것의 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 블록이다. 따라서 B_4 블록은 B_{13} 및 B_{32} 블록의 적어도 일부의 해시값(H_{sum})을 포함한다. 그리고 B_4 블록은 해시값(H_{sum})과 구분되도록 메인 브랜치에 포함되고 B_4 블록보다 직전에 생성된 제1 형 블록(B_3 블록)의 적어도 일부의 해시값(H_3)을 포함한다.
- [131] B_5 블록이 생성될 때 존재하는 서브 브랜치의 마지막 블록은 B_{13} , B_{33} 및 B_{43} 블록이다. 이 중, B_{13} 블록은 그것의 적어도 일부의 해시값이 이미 B_4 블록에 포함되어 있다. 또한, B_{33} 및 B_{43} 블록은 그것의 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 블록이다. 따라서 B_5 블록은 B_{33} 및 B_{44} 블록의 적어도 일부의 해시값(H_{sum})을 포함한다. 그리고 B_5 블록은 해시값(H_{sum})과 구분되도록 메인 브랜치에 포함되고 B_5 블록보다 직전에 생성된 제1 형 블록(B_4 블록)의 적어도 일부의 해시값(H_4)을 포함한다.
- [132] B_5 블록이 생성된 이후에 B_{44} 블록이 생성된다. B_{44} 블록까지 생성된 것이 도 9에 도시된 블록체인 시스템의 상태이다. 이후에 다른 제2 형 블록이 생성되지 않고, 추가로 제1 형 블록이 생성된다면, 이 때 존재하는 서브 브랜치의 마지막 블록은 B_{13} , B_{33} 및 B_{44} 블록이다. 이 중, B_{13} 및 B_{33} 블록은 그것의 적어도 일부의 해시값이 이미 B_5 블록에 포함되어 있다. 또한, B_{44} 블록은 그것의 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 블록이다. 따라서 새롭게 생성되는 마지막 제1 형 블록은 B_{44} 블록의 적어도 일부의 해시값을 포함하게 된다.
- [133]
- [134] 도 10은 본 발명의 일 실시예에 따른 블록체인을 이용한 데이터 관리 방법을 설명하기 위한 순서도이다. 이하, 도 10을 참조하여 본 발명의 일 실시예에 따른 블록체인 생성 방법에 대해 설명하도록 한다.
- [135] 도 10을 참조하여 설명할 블록체인 생성 방법은 도 1 내지 도 9를 참조하여 설명한 블록체인 시스템의 블록체인을 생성하는 방법에 관한 것이다. 따라서 설명의 편의성을 위해 도 1 내지 도 9를 참조하여 상술한 내용과 중복되는 내용 중 일부는 생략하도록 한다.
- [136] 도 10을 참조하면, 블록체인 생성 방법은 블록체인을 마련하는 단계(S100) 및 새로운 제1 형 블록을 생성하는 단계(S200)를 포함한다.
- [137] 이하, 상술한 각 단계에 대해서 상세하게 설명하도록 한다.

- [138] 블록체인을 마련하는 단계(S100)는 메인 브랜치 및 적어도 하나의 서브 브랜치를 포함하는 블록체인을 마련하는 단계이다. 이에 대해서는 도 5를 참조하여 상세하게 설명하였다.
- [139] 새로운 제1 형 블록을 생성하는 단계(S200)는 새로운 제1 형 블록을 메인 브랜치의 마지막 제1 형 블록에 연결되도록 생성하는 단계이다. 여기서, 새로운 제1 형 블록은 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함한다. 또한, 새로운 제1 형 블록은 마지막 제1 형 블록의 적어도 일부의 해시값을 더 포함할 수 있다. 새로운 제1 형 블록은 마지막 제2 형 블록의 적어도 일부의 해시값과 마지막 제1 형 블록의 적어도 일부의 해시값을 블록헤더에 구분하여 포함할 수 있다.
- [140] 구체적으로, 새로운 제1 형 블록은 모든 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함할 수 있다. 이에 대해서는 도 5 및 도 8을 참조하여 상세하게 설명하였다.
- [141] 또한, 경우에 따라서 새로운 제1 형 블록은 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 마지막 제2 형 블록의 적어도 일부의 해시값을 포함할 수 있다. 이에 대해서는 도 7 및 도 9를 참조하여 상세하게 설명하였다.
- [142] 새로운 제1 형 블록은 둘 이상의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하고, 상기 해시값은 각각의 마지막 제2 형 블록의 적어도 일부로부터 생성된 머클 트리의 루트에 대한 해시값일 수 있다. 이에 대해서는 도 6을 참조하여 상세하게 설명하였다.
- [143]
- [144] 이상, 본 발명의 블록체인 시스템 및 블록체인 생성 방법의 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 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.
- [145] 10: 제1 형 데이터 20: 제2 형 데이터
- [146] 100: 제1 형 블록 200: 제2 형 블록
- [147] 110, 210: 블록헤더 120, 220: 블록몸체
- [148] 190: 마지막 제1 형 블록 290: 마지막 제2 형 블록
- [149] 1000: 메인 브랜치 2000: 서브 브랜치
- [150]

청구범위

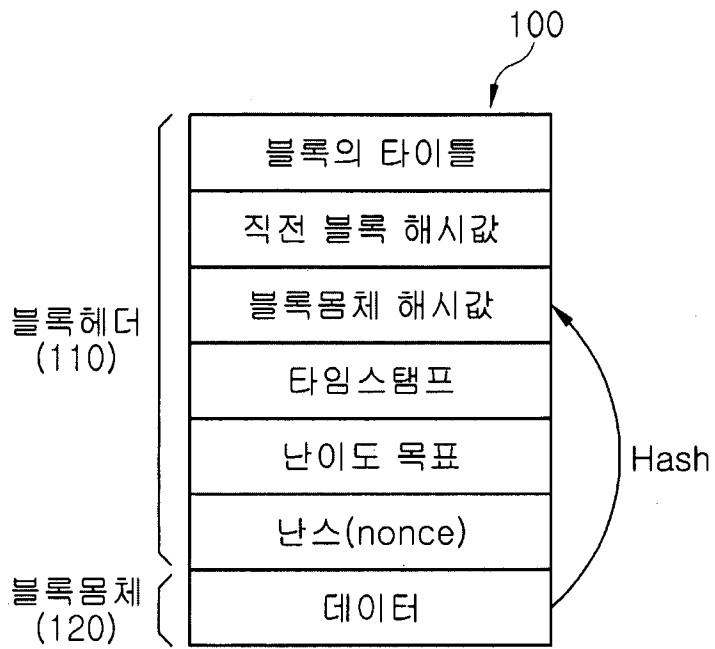
- [청구항 1] 적어도 하나의 제1 형 블록을 포함하고, 상기 제1 형 블록들은 각각 블록의 생성 순서에 따라 연결된 메인 브랜치; 및 하나의 제1 형 블록 및 적어도 하나의 제2 형 블록을 포함하고, 상기 제2 형 블록은 상기 제1 형 블록을 루트 블록으로 하여 연결된 적어도 하나의 서브 브랜치를 포함하고, 하나의 서브 브랜치의 상기 제2 형 블록은 각각 블록의 생성 순서에 따라 연결되며, 상기 하나의 서브 브랜치에서 최초로 생성된 제2 형 블록은 상기 루트 블록에 연결되고, 상기 메인 브랜치의 마지막 제1 형 블록은, 상기 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하는 블록체인 시스템.
- [청구항 2] 제1 항에 있어서, 상기 마지막 제1 형 블록은, 상기 메인 브랜치에 포함되고 상기 마지막 제1 형 블록보다 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 더 포함하는 블록체인 시스템.
- [청구항 3] 제2 항에 있어서, 상기 마지막 제1 형 블록은, 상기 마지막 제2 형 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 구분하여 포함하는 블록체인 시스템.
- [청구항 4] 제2 항에 있어서, 상기 마지막 제1 형 블록은, 상기 마지막 제2 형 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형 블록의 적어도 일부의 해시값을 블록헤더에 포함하는 블록체인 시스템.
- [청구항 5] 제1 항에 있어서, 상기 마지막 제1 형 블록은, 모든 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하는 블록체인 시스템.
- [청구항 6] 제1 항에 있어서, 상기 마지막 제1 형 블록은, 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하는 블록체인 시스템.
- [청구항 7] 제1 항에 있어서, 상기 마지막 제1 형 블록은, 둘 이상의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하고,

- 상기 해시값은,
 각각의 마지막 제2 형 블록의 적어도 일부로부터 생성된 머클 트리의
 루트에 대한 해시값인 블록체인 시스템.
- [청구항 8] 제1 항에 있어서,
 상기 마지막 제2 형 블록은,
 상기 마지막 제1 형 블록보다 이전에 생성된 블록인 블록체인 시스템.
- [청구항 9] 적어도 하나의 제1 형 블록을 포함하고, 상기 제1 형 블록들은 각각
 블록의 생성 순서에 따라 연결된 메인 브랜치; 및
 하나의 제1 형 블록 및 적어도 하나의 제2 형 블록을 포함하고, 상기 제2
 형 블록은 상기 제1 형 블록을 루트 블록으로 하여 연결된 적어도 하나의
 서브 브랜치를 포함하고,
 하나의 서브 브랜치의 상기 제2 형 블록은 각각 블록의 생성 순서에 따라
 연결되며, 상기 하나의 서브 브랜치에서 최초로 생성된 제2 형 블록은
 상기 루트 블록에 연결되고,
 상기 메인 브랜치의 임의의 제1 형 블록은, 상기 임의의 제1 형 블록보다
 이전에 생성된 제2 형 블록 중 일부 블록의 적어도 일부의 해시값을
 포함하는 블록체인 시스템.
- [청구항 10] 제9 항에 있어서,
 상기 임의의 제1 형 블록은,
 상기 메인 브랜치에 포함되고 상기 임의의 제1 형 블록보다 직전에
 생성된 제1 형 블록의 적어도 일부의 해시값을 더 포함하는 블록체인
 시스템.
- [청구항 11] 제10 항에 있어서,
 상기 임의의 제1 형 블록은,
 상기 일부 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형
 블록의 적어도 일부의 해시값을 구분하여 포함하는 블록체인 시스템.
- [청구항 12] 제10 항에 있어서,
 상기 임의의 제1 형 블록은,
 상기 일부 블록의 적어도 일부의 해시값과 상기 직전에 생성된 제1 형
 블록의 적어도 일부의 해시값을 블록헤더에 포함하는 블록체인 시스템.
- [청구항 13] 제9 항에 있어서,
 상기 일부 블록은,
 상기 임의의 제1 형 블록이 생성될 때, 상기 서브 브랜치의 마지막 블록인
 블록체인 시스템.
- [청구항 14] 제9 항에 있어서,
 상기 일부 블록은,
 상기 임의의 제1 형 블록이 생성될 때, 모든 서브 브랜치의 마지막 블록인
 블록체인 시스템.

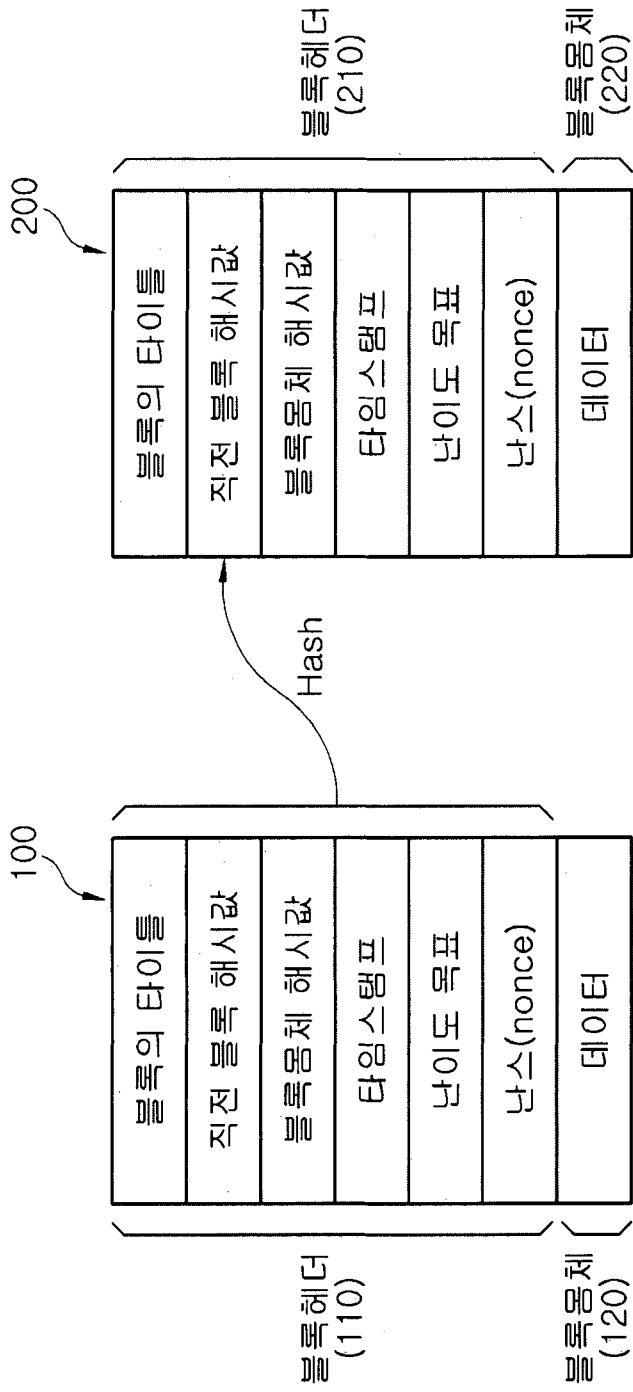
- [청구항 15] 제9 항에 있어서,
상기 일부 블록은,
상기 임의의 제1 형 블록이 생성될 때, 상기 서브 브랜치의 마지막 블록이 되, 적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 블록인 블록체인 시스템.
- [청구항 16] 제9 항에 있어서,
상기 일부 블록은 둘 이상의 블록이고,
상기 해시값은,
상기 일부 블록의 각각의 블록의 적어도 일부로부터 생성된 머클 트리의 루트에 대한 해시값인 블록체인 시스템.
- [청구항 17] 적어도 하나의 제1 형 블록을 포함하고, 상기 제1 형 블록들은 각각 블록의 생성 순서에 따라 연결된 메인 브랜치 및 하나의 제1 형 블록 및 적어도 하나의 제2 형 블록을 포함하고, 상기 제2 형 블록은 상기 제1 형 블록을 루트 블록으로 하여 연결된 적어도 하나의 서브 브랜치를 포함하고, 하나의 서브 브랜치의 상기 제2 형 블록은 각각 블록의 생성 순서에 따라 연결되, 상기 하나의 서브 브랜치에서 최초로 생성된 제2 형 블록은 상기 루트 블록에 연결되는 블록체인을 마련하는 단계; 및 새로운 제1 형 블록을 상기 메인 브랜치의 마지막 제1 형 블록에 연결되도록 생성하는 단계를 포함하고,
상기 새로운 제1 형 블록은,
상기 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하는 블록체인 생성 방법.
- [청구항 18] 제17 항에 있어서,
상기 새로운 제1 형 블록은,
상기 마지막 제1 형 블록의 적어도 일부의 해시값을 더 포함하는 블록체인 생성 방법.
- [청구항 19] 제18 항에 있어서,
상기 새로운 제1 형 블록은,
상기 마지막 제2 형 블록의 적어도 일부의 해시값과 상기 마지막 제1 형 블록의 적어도 일부의 해시값을 구분하여 포함하는 블록체인 생성 방법.
- [청구항 20] 제18 항에 있어서,
상기 새로운 제1 형 블록은,
상기 마지막 제2 형 블록의 적어도 일부의 해시값과 상기 마지막 제1 형 블록의 적어도 일부의 해시값을 블록헤더에 포함하는 블록체인 생성 방법.
- [청구항 21] 제17 항에 있어서,
상기 새로운 제1 형 블록은,
모든 서브 브랜치의 마지막 제2 형 블록의 적어도 일부의 해시값을

- 포함하는 블록체인 생성 방법.
- [청구항 22] 제17 항에 있어서,
상기 새로운 제1 형 블록은,
적어도 일부의 해시값이 다른 제1 형 블록에 포함되지 않은 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하는 블록체인 생성 방법.
- [청구항 23] 제17 항에 있어서,
상기 새로운 제1 형 블록은,
둘 이상의 마지막 제2 형 블록의 적어도 일부의 해시값을 포함하고,
상기 해시값은,
각각의 마지막 제2 형 블록의 적어도 일부로부터 생성된 머클 트리의 루트에 대한 해시값인 블록체인 생성 방법.
- [청구항 24] 제17 항에 있어서,
상기 마지막 제2 형 블록은,
상기 새로운 제1 형 블록보다 이전에 생성된 블록인 블록체인 생성 방법.

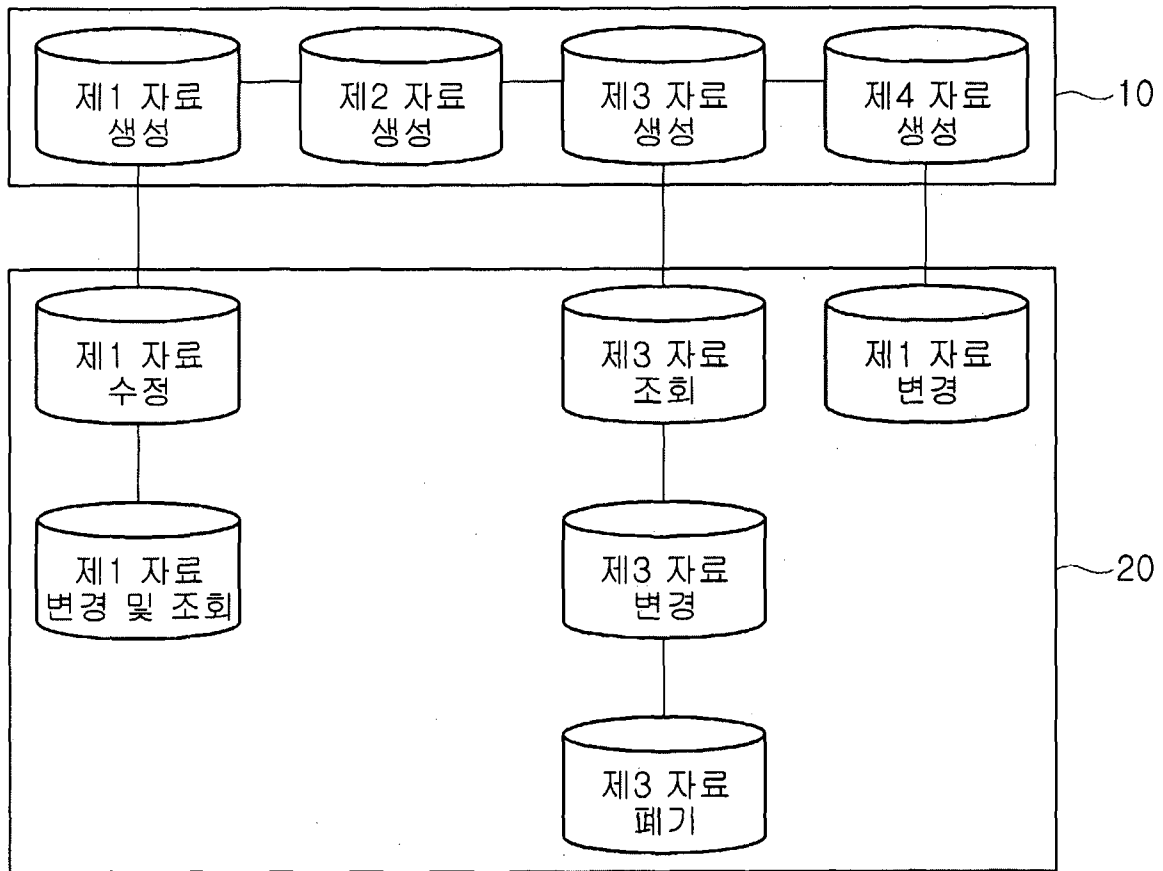
[도1]



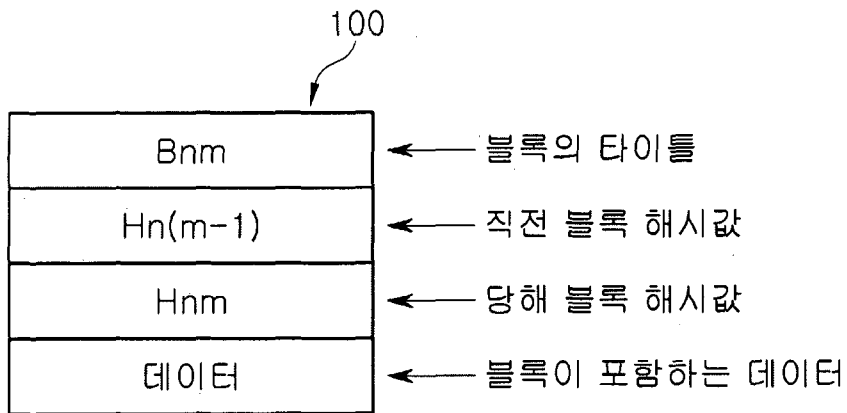
[도2]



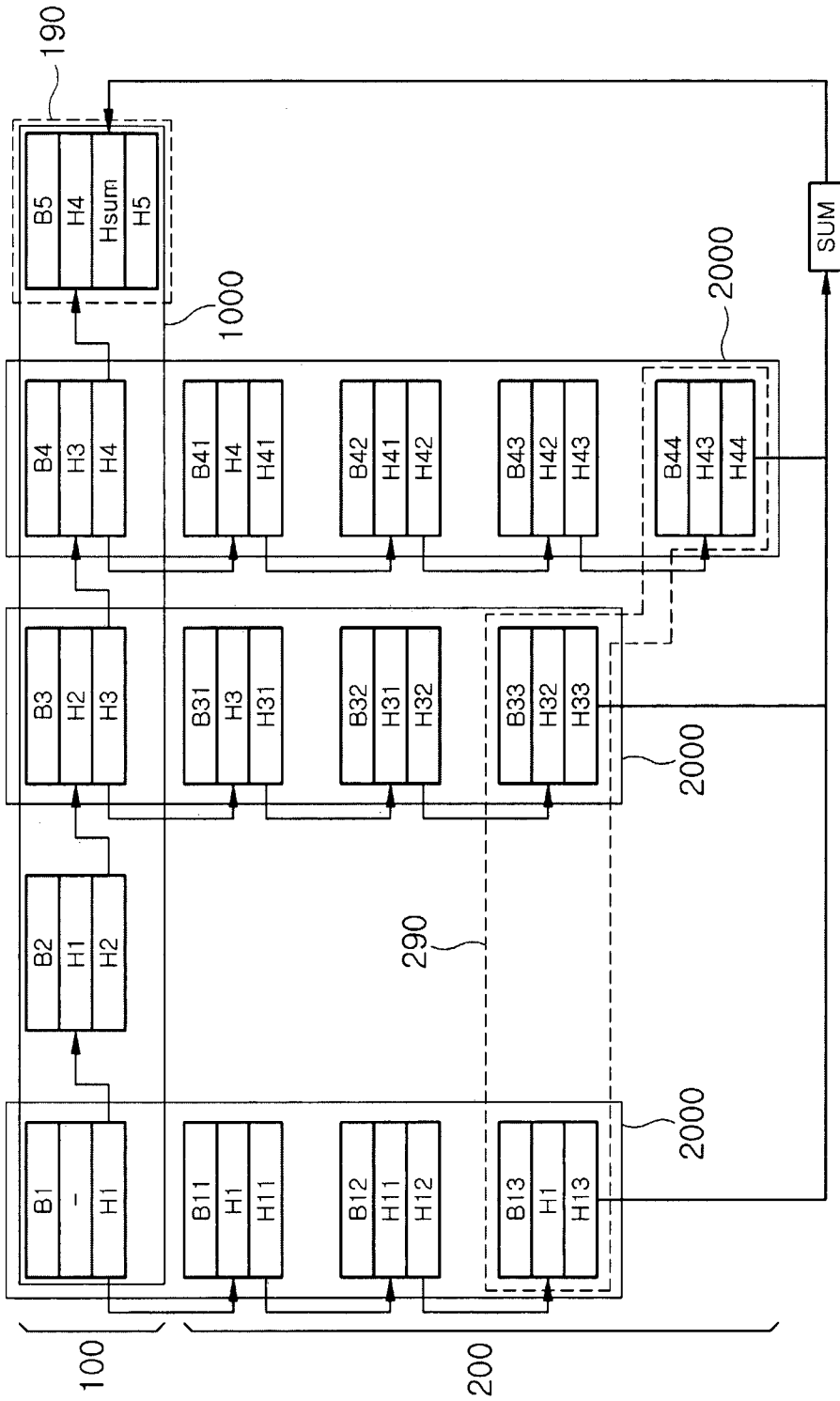
[도3]



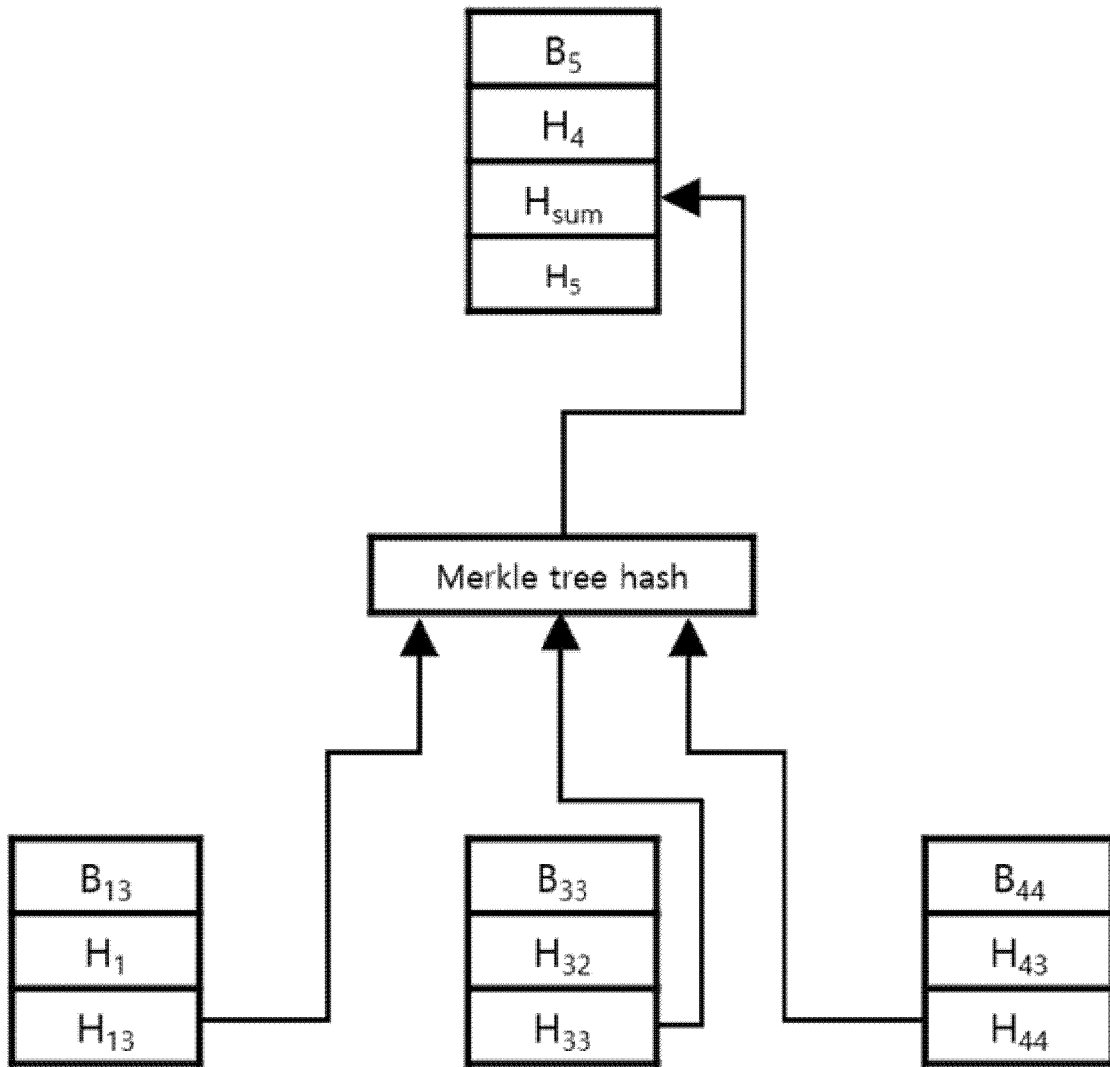
[도4]



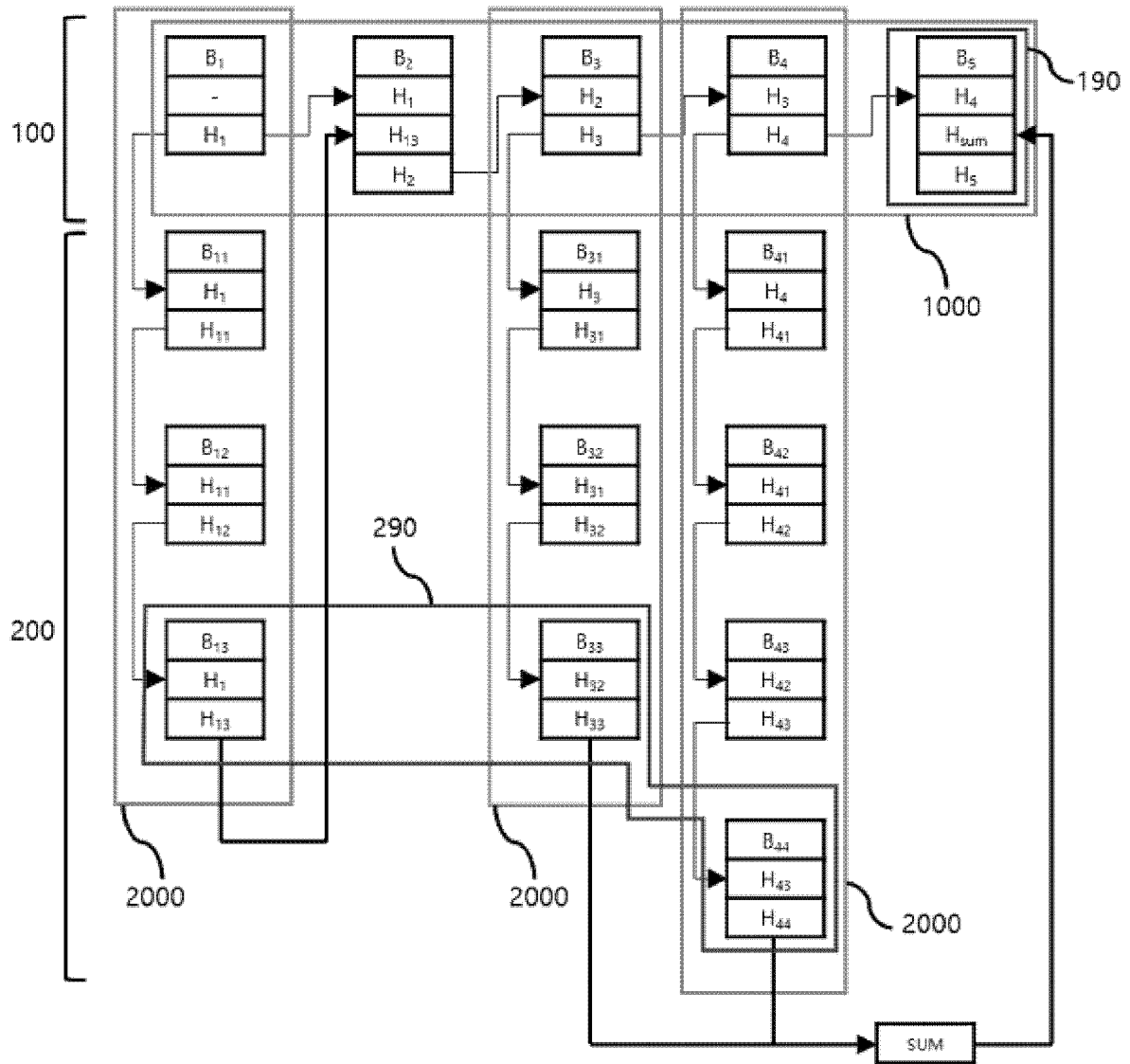
[도5]



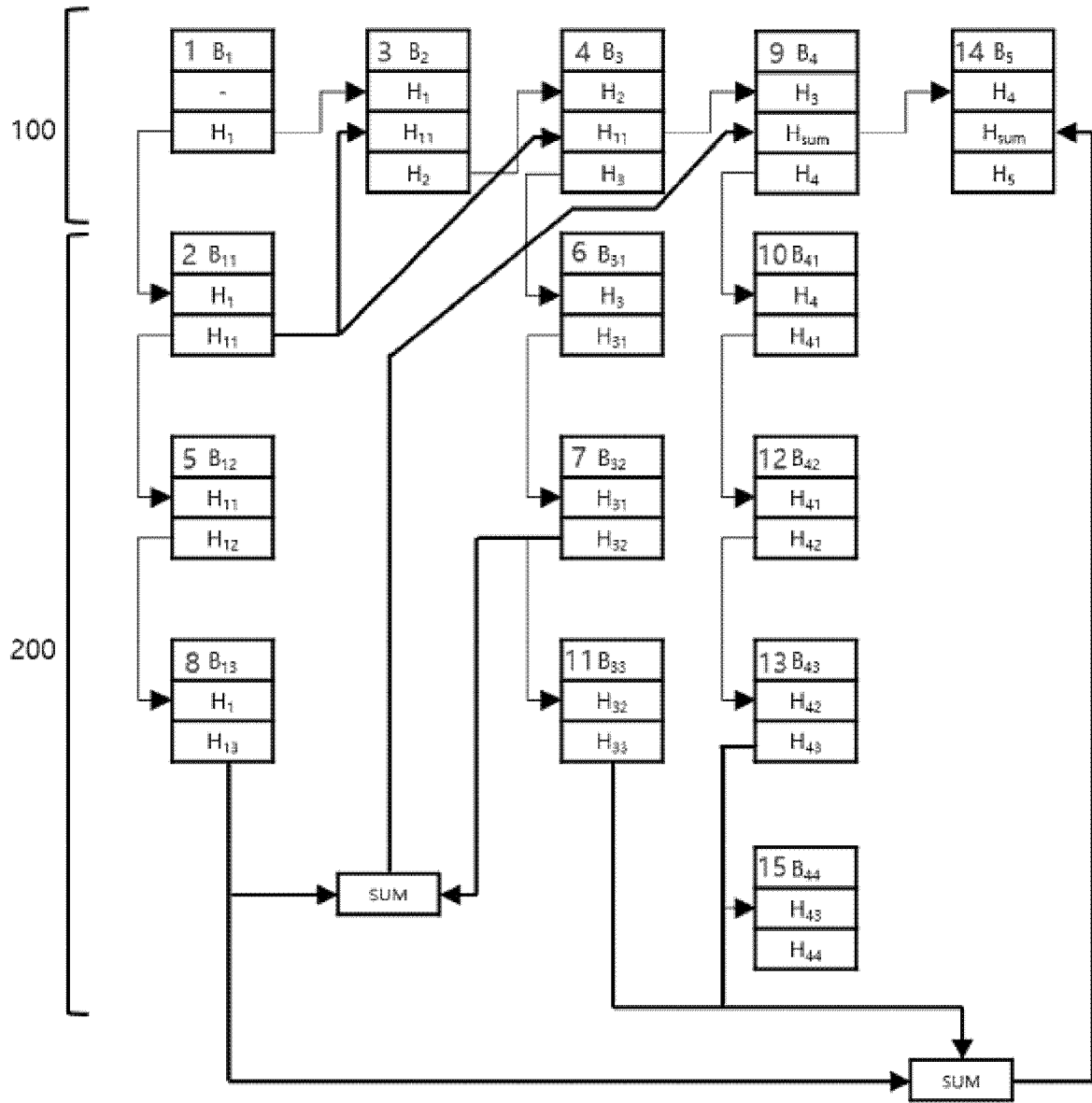
[도6]



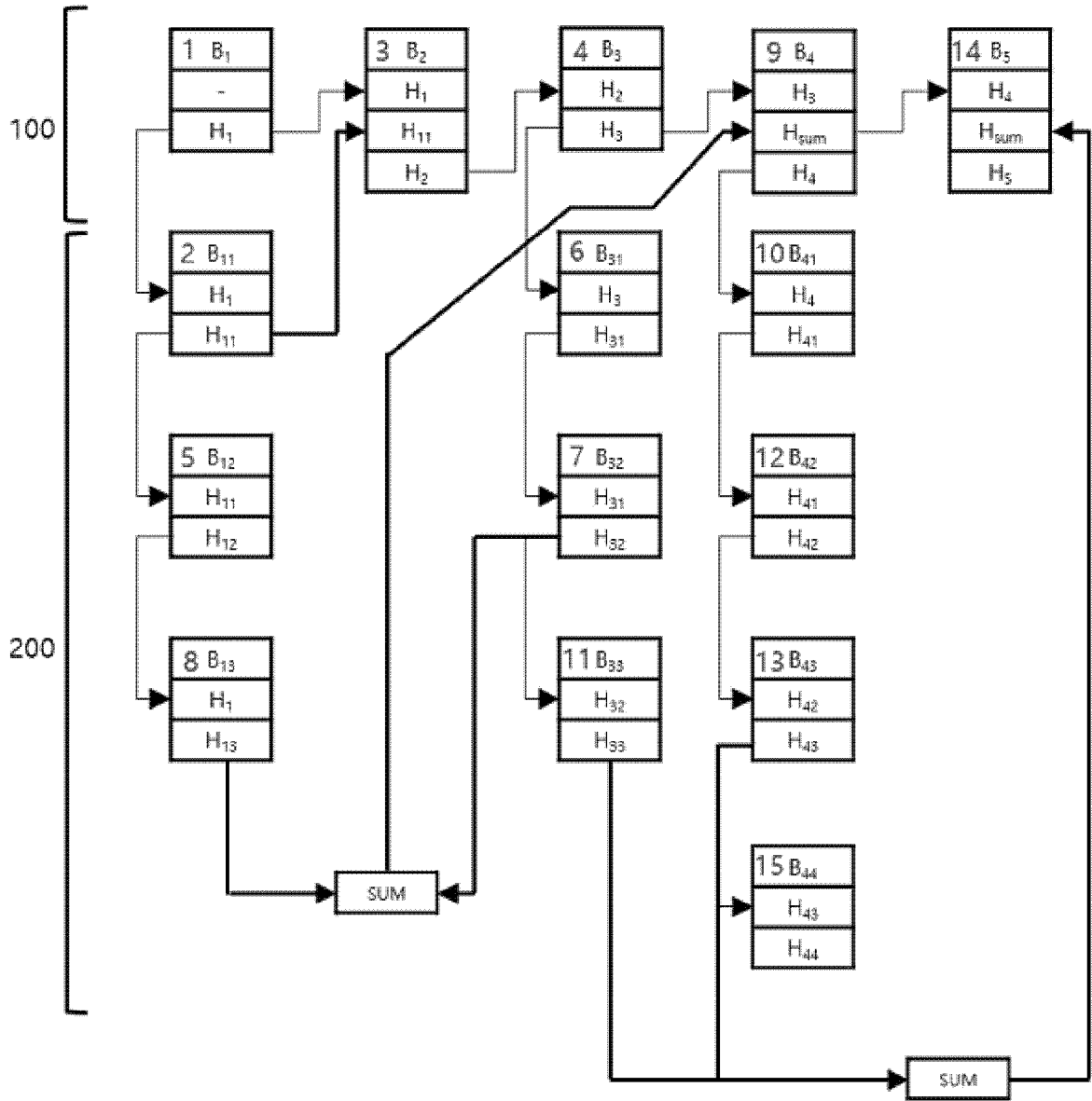
[도7]



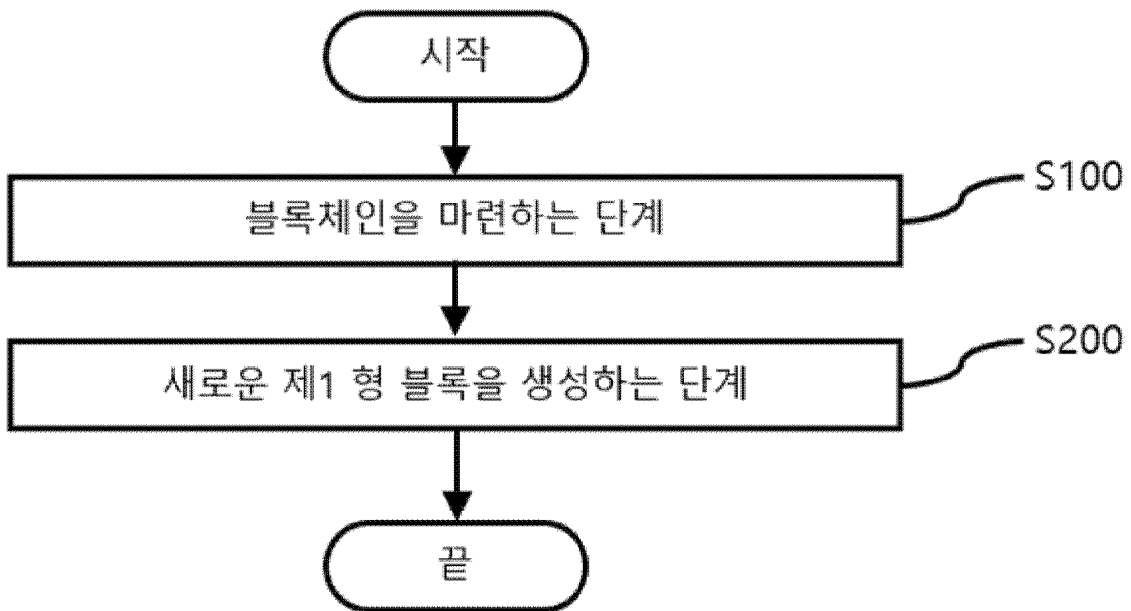
[도8]



[도9]



[도10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2017/010020

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/36(2012.01)i, G06Q 20/38(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q 20/36; G06F 12/02; G06Q 20/06; H04W 84/18; H04L 9/32; G06Q 20/38; G06Q 20/22; H04W 12/00

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, branch, hash, root

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016-0028552 A1 (SPANOS, Nikolaos et al.) 28 January 2016 See paragraph [0038] and figure 2.	1-24
A	Say Security, "Easy-to-Understand Blockchain, the Core of Bitcoin", Tistory, 25 January 2016, Internet:<URL: http://saysecurity.tistory.com/5 >, pages 1-12. See pages 4-5.	1-24
A	KR 10-1701131 B1 (RAPI INC.) 13 February 2017 See claims 1-3 and figures 11-12.	1-24
A	KR 10-1048509 B1 (PUSAN NATIONAL UNIVERSITY INDUSTRY-UNIVERSITY COOPERATION FOUNDATION) 11 July 2011 See claims 1, 3 and figure 1.	1-24
A	KR 10-2016-0106570 A (SUNRISE TECH GROUP LLC.) 12 September 2016 See claims 1, 3-4 and figure 17.	1-24



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

22 JANUARY 2018 (22.01.2018)

Date of mailing of the international search report

22 JANUARY 2018 (22.01.2018)

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/KR2017/010020

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2016-0028552 A1	28/01/2016	US 9608829 B2 WO 2016-015041 A1	28/03/2017 28/01/2016
KR 10-1701131 B1	13/02/2017	NONE	
KR 10-1048509 B1	11/07/2011	KR 10-2011-0031752 A	29/03/2011
KR 10-2016-0106570 A	12/09/2016	CN 106415530 A EP 3095044 A1 EP 3095044 A4 US 2017-243176 A1 WO 2015-077378 A1	15/02/2017 23/11/2016 06/09/2017 24/08/2017 28/05/2015

A. 발명이 속하는 기술분류(국제특허분류(IPC)) G06Q 20/36(2012.01)i, G06Q 20/38(2012.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) G06Q 20/36; G06F 12/02; G06Q 20/06; H04W 84/18; H04L 9/32; G06Q 20/38; G06Q 20/22; H04W 12/00 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, 브랜치, 해시, 루트		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 2016-0028552 A1 (NIKOLAOS SPANOS 등) 2016.01.28 단락 [0038] 및 도면 2 참조.	1-24
A	쎄이 시큐리티, `비트코인의 핵심, 블록체인 쉽게 이해하기`, 티스토리, 2016.01.25, 인터넷:<URL: http://saysecurity.tistory.com/5>, 페이지 1-12, 페이지 4-5 참조.	1-24
A	KR 10-1701131 B1 (주식회사 라피) 2017.02.13 청구항 1-3 및 도면 11-12 참조.	1-24
A	KR 10-1048509 B1 (부산대학교 산학협력단) 2011.07.11 청구항 1, 3 및 도면 1 참조.	1-24
A	KR 10-2016-0106570 A (썬라이즈 테크 그룹, 엘엘씨) 2016.09.12 청구항 1, 3-4 및 도면 17 참조.	1-24
<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 2018년 01월 22일 (22.01.2018)	국제조사보고서 발송일 2018년 01월 22일 (22.01.2018)	
ISA/KR의 명칭 및 우편주소  대한민국 특허청 (35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-481-8578	심사관 김연경 전화번호 +82-42-481-3325	

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2016-0028552 A1	2016/01/28	US 9608829 B2 WO 2016-015041 A1	2017/03/28 2016/01/28
KR 10-1701131 B1	2017/02/13	없음	
KR 10-1048509 B1	2011/07/11	KR 10-2011-0031752 A	2011/03/29
KR 10-2016-0106570 A	2016/09/12	CN 106415530 A EP 3095044 A1 EP 3095044 A4 US 2017-243176 A1 WO 2015-077378 A1	2017/02/15 2016/11/23 2017/09/06 2017/08/24 2015/05/28