(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2020 년 6 월 25 일 (25.06.2020)

WIPO | PCT

(10) 국제공개번호
WO 2020/130331 A1

(51) 국제특허분류:
H04L 29/08 (2006.01) *G06Q 10/10* (2012.01)
H04L 29/06 (2006.01) *G06F 21/62* (2013.01)
G06F 21/60 (2013.01) *H04L 9/06* (2006.01)

(21) 국제출원번호: PCT/KR2019/014749

(22) 국제출원일: 2019 년 11 월 1 일 (01.11.2019)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2018-0167815 2018 년 12 월 21 일 (21.12.2018) KR
10-2018-0168117 2018 년 12 월 24 일 (24.12.2018) KR

(71) 출원인: (주)소프트제국 (SWEMPIRE CO., LTD.) [KR/KR]; 10526 경기도 고양시 덕양구 용현로 9, 701호, Gyeonggi-do (KR).

(72) 발명자: 최명수 (CHOI, Myoung Soo); 10521 경기도 고양시 덕양구 무원로 41, 903동 1001호, Gyeonggi-do (KR).

(74) 대리인: 유철현 (YOO, Cheol Hyun); 06131 서울시 강남구 테헤란로25길 15-5, 5층 (역삼동, 아이티빌딩), 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.

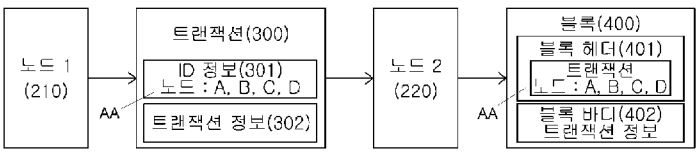
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:
— 국제조사보고서와 함께 (조약 제21조(3))

WO 2020/130331 A1

(54) Title: METHOD FOR SHARING AND VERIFYING BLOCKS AND ELECTRONIC DOCUMENTS BETWEEN NODES IN BLOCKCHAIN

(54) 발명의 명칭: 블록체인에서 노드들간 블록 및 전자 문서를 공유 및 검증하는 방법



210, 220 ...Node
300 ... Transaction
301 ... ID information
302 ... Transaction information
400 ... Block
401 ... Block header
402 ... Block body

AA ... Node: A, B, C, D

(57) Abstract: The present invention relates to a method for sharing and verifying blocks between specific nodes in a blockchain, wherein on the basis of identification information included in a block, specific nodes related to the block share blocks containing transaction information, and the remaining nodes not related to the block share blocks containing only a block header, such that the efficiency of management of all nodes in the blockchain can be increased.

(57) 요약서: 본 발명은 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법에 관한 것으로, 블록에 포함된 식별 정보에 기반하여, 블록과 관련된 특정 노드들은 트랜잭션 정보를 포함하는 블록을 공유하고 블록과 관련 없는 나머지 노드들은 블록 헤더만을 포함하는 블록을 공유함으로써, 블록체인 전체 노드들의 관리의 효율성을 증가시킬 수 있다.

명세서

발명의 명칭: 블록체인에서 노드들간 블록 및 전자 문서를 공유 및 검증하는 방법

기술분야

[1] 본 발명은 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법에 관한 것으로, 보다 자세하게는 블록체인에 포함된 복수의 노드들 중 블록을 공유할 특정 노드들을 그룹으로 지정하지 않으면서도 효율적으로 노드들간 블록을 공유하고 검증하는 방법에 관한 것이다.

[2] 또한, 본 발명은 블록체인에서 스마트 컨트랙트를 이용한 전자 문서 유통 방법에 관한 것으로, 보다 자세하게는 블록체인에서 전자 문서를 이용하는 시점에 전자 문서 서식과 전자 문서 정보를 자동으로 병합하는 방법에 관한 것이다.

배경기술

[3] 블록체인(blockchain)은 지속적으로 증가하는 데이터를 특정 단위의 블록에 기록하고, P2P(peer-to-peer) 네트워크를 구성하는 각각의 노드들이 블록을 체인 형태의 자료 구조로 관리하는 데이터 관리 기술 또는 체인 형태의 자료 구조로 구성된 데이터 그 자체를 의미한다. 이때, 체인 형태의 자료 구조로 구성된 블록체인 데이터는 중앙 시스템 없이 각각의 노드에서 분산 원장(distributed edger) 형태로 운영된다.

[4] 블록체인 기술은, 분산 데이터 관리 또는 데이터 위변조 방지를 위해 다양한 분야에 응용될 수 있다. 예를 들어, 블록체인 기술이 금융 분야에 응용되는 경우, 신뢰를 보증하는 중앙 금융기관이 없어도, 분산된 각각의 블록체인 노드가 관리하는 분산 원장을 통해 거래 당사자가 안전하게 거래를 수행할 수 있다.

[5] 한편, 블록체인은 퍼블릭(public) 블록체인과 프라이빗(privit) 블록체인으로 구분될 수 있는데, 특히 금융권 및 기업 등 특정 이해관계를 가진 단체들은 퍼블릭 블록체인 대신 허가된 기관만 열람이 가능한 프라이빗 블록체인을 선호하고 있다. 따라서, 프라이빗 블록체인은 퍼블릭 블록체인과 달리 블록체인에 참여한 노드들 중 이해관계에 따라 특정 노드들만 특정 블록을 공유하는 방법이 이루어지고 있다.

[6] 예를 들어, 특정 노드 간 블록을 공유하는 방법은 사전에 블록을 공유할 노드들을 그룹으로 지정하여 이루어졌다. 그러나 이렇게 사전에 블록을 공유할 노드들을 지정 할 경우, 블록체인을 활용 및 운용하는 측면에서 하기와 같이 3가지 문제점이 있다.

[7] 첫 번째 문제점으로서, 블록을 공유할 노드들의 그룹 지정이 동적으로 운용되지 못하여 기존에 지정 된 그룹에 새로운 노드를 추가하기 위해서는 신규 그룹을 지정해야 하므로 블록을 공유할 그룹이 불필요하게 증가하게 된다.

따라서, 그룹 증가에 따른 관리의 비효율성이 증가한다.

[8] 두 번째 문제점으로서, 블록을 공유하는 노드들의 그룹에서 저장 및 관리되는 블록은 노드들의 그룹이 해제 될 경우 삭제된다. 따라서, 그룹이 삭제된 이후 상기 관리되는 블록을 계속 조회하기 위해 별도로 저장을 해야하므로 블록체인 내의 복수의 노드들에 있어서 저장공간의 비효율성이 존재한다.

[9] 세 번째 문제점으로서, 그룹으로 지정 된 노드들만 공유하는 블록은 다른 노드들은 공유하지 못하여 블록체인에 참여한 모든 노드들에 의해 블록의 무결성이 검증될 수 없어 해당 블록체인의 전반적인 신뢰성이 낮아진다.

[10] 한편, 블록체인 기술은 앞서 설명한 바와 같이 신뢰성있는 데이터의 공유와 무결성을 보장하지만, 전자 문서를 유통하는데 있어서는 제한적인 부분이 있었다.

[11] 첫 번째 문제점으로서, 전자 문서를 파일형태 또는 전자 문서 서식과 데이터를 분리하여 유통하기에는 블록체인에서 분산 저장되는 블록의 크기가 제한적이다.

[12] 두 번째 문제점으로서, 전자 문서 파일이 블록체인에 저장될 경우 전체 블록체인의 용량이 매우 증가하여 관리의 효율성이 낮아진다.

[13] 세 번째 문제점으로서, 전자 문서의 데이터만 유통되는 경우, 문서 형태로 열람 및 조회하기 위해서는 전자 문서 서식을 외부 시스템에서 받아오거나 전자 문서의 데이터를 외부 시스템으로 전송해야 한다. 따라서, 전자 문서의 열람 및 조회의 편의성과 서식의 신뢰성을 보장하는 것이 어렵다. 또한, 증명서 같은 전자문서에는 다양한 개인정보가 존재하지만 이러한 개인 정보를 보호하기 어렵다.

발명의 상세한 설명

기술적 과제

[14] 본 발명은 상기와 같은 문제점을 해결하기 위해 안출된 것으로서, 사전에 미리 그룹을 지정하지 않고 모든 노드들이 블록을 공유하되, 블록에 포함된 식별 정보에 기반하여, 블록과 관련된 특정 노드들은 트랜잭션 정보를 포함하는 블록을 공유하고 블록과 관련 없는 나머지 노드들은 블록 헤더만을 포함하는 블록을 공유함으로써 블록체인 전체 노드들의 관리의 효율성을 증가시키는 방법을 제공하는 데 목적이 있다.

[15] 또한, 본 발명은 블록과 관련 있는 특정 노드들에게만 공유되는 블록의 헤더만을 블록과 관련 없는 나머지 노드들에게 공유함으로써 블록체인 전체 노드들의 저장 공간을 실질적으로 증가시키는 방법을 제공하는 데 목적이 있다.

[16] 또한, 본 발명은 블록과 관련 없는 나머지 노드들은 블록에 포함된 해시 값을 이용하여 블록의 무결성을 검증하고 블록에 포함되지 않은 트랜잭션 정보에 대한 무결성은 블록 생성 노드에서 제공하는 블록 해시 값을 이용하여 검증함으로써 블록체인에 참여한 모든 노드들이 블록의 무결성을 검증하는

방법을 제공하는 데 목적이 있다.

[17] 한편, 본 발명은 상기와 같은 문제점을 해결하기 위해 안출된 것으로서, 전자 문서를 분할하여 전자 문서 정보만 블록에 포함하여 유통하는 방법을 제공하는 데 목적이 있다.

[18] 또한, 본 발명은 전자 문서를 이용하는 시점에 전자 문서 서식과 데이터가 자동으로 연결되고 결합되는 방법을 제공하는 데 목적이 있다.

[19] 또한, 본 발명은 개인 정보가 포함된 전자 문서를 이용하는 시점에 열람 자격을 검증하는 방법을 제공하는 데 목적이 있다.

[20] 본 발명이 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

[21] 본 발명의 일 실시예에 따른 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법은 상기 복수의 노드들 중에서 적어도 하나의 제1 노드가 상기 특정 노드들의 식별 정보 및 트랜잭션 정보를 포함하는 적어도 하나의 트랜잭션을 생성하는 단계; 기 복수의 노드들 중에서 적어도 하나의 제2 노드가 상기 식별 정보 및 상기 트랜잭션 정보에 기반하여 적어도 하나의 블록을 생성하는 단계; 및 상기 적어도 하나의 제2 노드가 상기 생성된 적어도 하나의 블록을 상기 식별 정보에 기반하여 상기 특정 노드들에게 공유하는 단계를 포함할 수 있다.

[22] 본 발명의 일 실시예에 따른 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 시스템은 블록체인 네트워크를 구성하는 복수의 노드들을 포함하고, 기 복수의 노드들 중에서 적어도 하나의 제1 노드가 상기 특정 노드들의 식별 정보 및 트랜잭션 정보를 포함하는 적어도 하나의 트랜잭션을 생성하고, 상기 복수의 노드들 중에서 적어도 하나의 제2 노드가 상기 식별 정보 및 상기 트랜잭션 정보에 기반하여 적어도 하나의 블록을 생성하고, 상기 적어도 하나의 제2 노드가 상기 생성된 적어도 하나의 블록을 상기 식별 정보에 기반하여 상기 특정 노드들에게 공유할 수 있다.

[23] 본 발명의 일 실시예에 따른 복수의 노드들을 포함하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법은 상기 전자 문서를 전자 문서 서식 및 병합 조건을 포함하는 제1 분할 데이터 및 식별자와 전자 문서 정보를 포함하는 제2 분할 데이터로 분할하는 단계; 상기 제1 분할 데이터를 상기 복수의 노드들에 분산 저장하는 단계; 상기 제2 분할 데이터를 포함하는 블록을 생성하여 상기 복수의 노드들에 분산 저장하는 단계; 및 상기 복수의 노드들 중 어느 하나의 노드가, 상기 병합 조건 및 상기 식별자에 기반하여, 상기 제1 분할 데이터와 상기 제2 분할 데이터를 병합하는 단계를 포함할 수 있다.

[24] 본 발명의 일 실시예에 따른 복수의 노드들을 포함하는 블록체인에서 스마트

컨트랙트를 이용한 전자 문서를 유통하는 시스템은 상기 복수의 노드들은 전자 문서 관리 및 유통 모듈, 전자 문서 분할 모듈, 블록 생성 모듈 및 메모리를 포함하고, 상기 복수의 노드들 중 어느 하나의 노드가, 상기 전자 문서 분할 모듈을 이용하여, 상기 전자 문서를 전자 문서 서식 및 병합 조건을 포함하는 제1 분할 데이터 및 식별자와 전자 문서 정보를 포함하는 제2 분할 데이터로 분할하고, 상기 어느 하나의 노드가 상기 제1 분할 데이터를 상기 복수의 노드들에 분산 저장하고, 상기 어느 하나의 노드가, 상기 블록 생성 모듈을 이용하여, 상기 제2 분할 데이터를 포함하는 블록을 생성하여 상기 복수의 노드들에 분산 저장하고, 상기 복수의 노드들 중 어느 하나의 노드가, 상기 전자 문서 관리 및 유통 모듈을 이용하여, 상기 병합 조건 및 상기 식별자에 기반하여, 상기 제1 분할 데이터와 상기 제2 분할 데이터를 병합할 수 있다.

발명의 효과

[25] 상기와 같은 본 발명에 따르면, 아래와 같은 다양한 효과들을 가진다.

[26] 본 발명은 사전에 미리 그룹을 지정하지 않고 블록에 포함된 식별 정보를 통해 블록과 관련된 특정 노드들에게 트랜잭션이 포함된 블록을 공유시키고 블록과 관련 없는 나머지 노드들에게 블록 헤더만 포함된 서브 블록을 자동으로 공유시킬 수 있다.

[27] 또한, 본 발명은 블록의 헤더만 포함된 블록을 블록과 관련 없는 나머지 노드들에게 공유함으로써 블록체인 전체 노드들의 저장 공간을 실질적으로 증가시킬 수 있다.

[28] 또한, 본 발명은 나머지 노드들에게 공유된 블록의 헤더에 포함된 해시 값과 블록 생성 노드에서 제공하는 블록 해시 값을 이용함으로써 블록체인에 참여한 모든 노드들이 블록의 무결성을 검증할 수 있다.

[29] 또한, 본 발명은 프라이빗 블록체인에서 특정 노드들간 블록의 공유에 대한 자유도를 높일 수 있다.

[30] 한편, 본 발명은 전자 문서를 전자 문서 서식과 전자 문서 정보로 분할하여 유통함으로써 블록체인 상에서 블록에 저장되는 전자 문서와 관련된 데이터의 크기를 최소화할 수 있다.

[31] 또한, 본 발명은 전자 문서 관리 및 유통 모듈을 이용하여 문서를 이용하는 시점에 전자 문서 서식과 전자 문서 정보를 자동으로 병합하여 전자 문서를 제공할 수 있다.

[32] 또한, 본 발명은 개인정보가 포함된 전자 문서를 열람 및 검증 시 자격 조건을 검증하는 방법을 제공함으로써 블록체인에서 유통되는 전자 문서의 신뢰성을 높일 수 있다.

도면의 간단한 설명

[33] 도 1은 본 발명의 블록체인 시스템을 나타낸 블록도이다.

[34] 도 2는 본 발명의 일 실시 예에 따른 블록체인에서 특정 노드간 블록을

공유하는 방법을 나타낸 블록도이다.

[35] 도 3은 본 발명의 일 실시 예에 따른 블록체인에서 특정 노드간 블록을 공유하는 방법을 설명하기 위한 흐름도이다.

[36] 도 4는 본 발명의 일 실시 예에 따른 블록체인에서 특정 노드간 블록을 공유하는 방법을 설명하기 위한 예시도이다.

[37] 도 5는 본 발명의 일 실시 예에 따른 식별 정보를 이용하여 블록을 생성하고 특정 노드들에게 공유하는 방법을 설명하기 위한 흐름도이다.

[38] 도 6은 본 발명의 일 실시 예에 따른 서브 블록을 생성하고 공유하는 방법을 설명하기 위한 흐름도이다.

[39] 도 7은 본 발명의 일 실시 예에 따른 서브 블록을 생성하고 공유하는 방법을 설명하기 위한 예시도이다.

[40] 도 8은 본 발명의 일 실시 예에 따른 서브 블록 및 트랜잭션 정보의 무결성을 검증하는 방법을 설명하기 위한 흐름도이다.

[41] 도 9는 본 발명의 블록체인 시스템을 나타낸 블록도이다.

[42] 도 10은 본 발명의 블록체인 시스템의 복수의 노드들을 나타낸 블록도이다.

[43] 도 11은 본 발명의 일 실시 예에 따른 블록을 나타낸 예시도이다.

[44] 도 12는 본 발명의 일 실시 예에 따른 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법을 설명하기 위한 흐름도이다.

[45] 도 13은 본 발명의 일 실시 예에 따른 블록체인에서 분할된 전자 문서를 병합하는 방법을 설명하기 위한 예시도이다.

[46] 도 14는 본 발명의 일 실시 예에 따른 블록체인에서 개인 정보를 포함하는 전자 문서를 병합하는 방법을 설명하기 위한 흐름도이다.

발명의 실시를 위한 형태

[47] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명한다. 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 게시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 게시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[48] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[49] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다.

[50]

[51] <블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법>

[52]

[53] 도 1은 본 발명의 블록체인 시스템을 나타낸 블록도이다.

[54] 도 1을 참조하면, 블록체인 시스템은 복수의 노드들(200)로 이루어진 분권형 네트워크(decentralized network, 100) 시스템일 수 있다. 분권형 네트워크(100)를 구성하는 노드들(200)은 컴퓨터, 서버, 이동 단말기 등 연산 기능, 통신 기능, 저장 기능 등을 구비한 전자 장치일 수 있다.

[55] 일 실시 예에서, 분권형 네트워크(100)는 블록 체인(block chain)이라 불리는 블록(block)의 연결 묶음 내에 모든 참여 노드에 공통으로 알려진 정보를 저장하고 참조할 수 있다. 복수의 노드들(200)은 상호간 통신이 가능하며 블록 체인을 저장, 관리 및 전파를 담당하는 완전 노드(full node)와 단순하게 트랜잭션에만 참여할 수 있는 간이 노드(light node)로 구분될 수 있다. 본 명세서에서 별다른 설명 없이 노드에 대하여 언급되는 경우, 이는 분권형 네트워크(100)에 참여하며 블록 체인을 생성, 저장 또는 검증하는 동작을 수행하는 완전 노드를 지칭하는 경우가 많으나, 이에 국한되지 않는다.

[56] 일 실시 예에서, 블록 체인에 연결되어 있는 각 블록(block)들은 일정 기간 내의 거래 내역, 즉 트랜잭션(transaction)들을 포함한다. 노드들(200)은 각각 역할에 따라 블록 체인을 생성, 저장 또는 검증함으로써 트랜잭션들을 관리한다.

[57] 일 실시 예에서, 트랜잭션은 다양한 형태의 거래를 나타낼 수 있다. 예를 들어, 트랜잭션은 가상 화폐의 소유 상태 및 그 변동을 나타내기 위한 금융 거래에 해당할 수 있다. 또한, 다른 예에서 트랜잭션은 물건의 소유 상태 및 그 변동을 나타내기 위한 실물 거래에 해당할 수 있다. 분권형 네트워크(100)에서 거래를 수행하는 노드들은 각각의 암호학적 연관관계가 있는 개인키(private key) 및 공개키(public key) 쌍을 가질 수 있다.

[58] 일 실시 예에서, 본 발명은 앞서 설명한 바와 같은 퍼블릭 블록체인에서 적용될 수 있다.

[59] 다른 실시 예에서, 본 발명은 프라이빗 블록체인일 수 있다. 예를 들어, 프라이빗 블록체인은, 읽기 권한 측면에서 허가된 기관만 열람 가능할 수 있고, 거래 검증 및 승인 측면에서 승인된 기관과 감독 기관에 해당하는 노드만 거래 검증 및 승인을 수행할 수 있고, 트랜잭션 측면에서 법적 책임을 지는 기관만이 트랜잭션을 생성할 수 있다. 단, 본 발명에 적용되는 프라이빗 블록 체인은 앞서 설명한 내용에 국한되지 않고 특정 이해관계를 공유하는 특정 그룹들만 참여

가능한 블록체인을 모두 의미할 수 있다.

[60] 일 실시 예에서, 본 발명이 프라이빗 블록 체인에 적용될 경우, 거래 검증, 승인 및 관리 등을 수행하는 지정된 노드가 존재할 수 있다.

[61] 일 실시 예에서, 본 발명에 개시된 블록 체인은 순차적으로 연결된 하나 이상의 블록들의 분산 데이터베이스의 일종일 수 있다. 블록 체인은 블록 체인 시스템 내 사용자의 거래 내역을 저장하고 관리하기 위해 사용되며, 블록 체인 네트워크(100)에 참여하는 각 노드가 블록을 생성하여 블록 체인에 연결한다. 예컨대 후술할 도 4에 개시된 블록 1 내지 블록 3은 순차적으로 연결된 블록 체인의 블록 중 일부일 수 있다. 도 4에서 제한된 수의 블록들이 도시되어 있으나 블록 체인에 포함될 수 있는 블록의 수는 이에 제한되지 아니한다.

[62] 도 2는 본 발명의 일 실시 예에 따른 블록체인에서 특정 노드간 블록을 공유하는 방법을 나타낸 블록도이다.

[63] 도 2를 참조하면, 본 발명의 일 실시 예에 따른 블록체인에서 특정 노드간 블록을 공유하는 방법은 제1 노드(210)가 트랜잭션(300)을 생성할 수 있고, 제2 노드(220)가 트랜잭션(300)을 포함하는 블록(400)을 생성할 수 있다.

[64] 일 실시 예에서, 제1 노드(210)는 트랜잭션(300)을 제안하고 생성하는 노드일 수 있다. 제1 노드(210)는 복수의 노드들(200) 중 트랜잭션(300) 생성 권한을 가진 노드일 수 있고, 제1 노드(210)는 복수 개가 존재할 수 있다. 물론, 이와 달리 트랜잭션(300) 생성 권한이 별도로 존재하지 않고, 본 발명의 블록체인 네트워크(100)에 포함된 모든 노드들(200)이 트랜잭션(300)을 생성할 수 있다.

[65] 일 실시 예에서, 트랜잭션(300)은 특정 노드들의 식별 정보(ID Information, 301) 및 트랜잭션 정보(Transaction Information, 302)를 포함할 수 있다. 예를 들어, 식별 정보(301)는 해당 트랜잭션 정보(302)를 공유할 수 있는 노드를 확인할 수 있는 태그일 수 있다. 예를 들어, 도 2에 개시된 바와 같이, 식별 정보(301)에 A, B, C, D가 포함될 경우, 이는 트랜잭션 정보를 공유할 노드가 노드 A, 노드 B, 노드 C, 노드 D라는 것을 의미할 수 있다. 예를 들어, 트랜잭션 정보(302)는 다양한 형태의 거래와 관련된 정보일 수 있다.

[66] 일 실시 예에서, 제2 노드(220)는 블록(400)을 생성하는 노드일 수 있다. 제2 노드(220)는 복수의 노드들(200) 중 블록(400) 생성 권한을 가진 노드일 수 있고, 제2 노드(220)는 복수 개가 존재할 수 있다. 물론, 이와 달리 블록(400) 생성 권한이 별도로 존재하지 않고, 본 발명의 블록체인 네트워크(100)에 포함된 모든 노드들(200)이 거래를 생성할 수 있다.

[67] 일 실시 예에서, 블록 체인에 포함된 각 블록(Block, 400)은 블록 헤더(Block header, 401)와 블록 바디(Block body, 213)를 포함하도록 구성될 수 있다. 블록 헤더(401)는 각 블록들간의 연결 관계를 나타내기 위하여 이전 블록의 해시 값을 포함할 수 있다. 블록 체인이 유효한지 검증하는 과정에서 블록 헤더(401) 내의 연결 관계가 사용될 수 있다. 블록 바디(402)는 블록(400)에 저장되고 관리되는 데이터, 예를 들어 트랜잭션 정보(302), 트랜잭션 리스트 또는 트랜잭션 체인을

포함할 수 있다.

[68] 일 실시 예에서, 블록 헤더(401)는 블록(400)을 공유할 특정 노드들의 식별 정보(예: Node A, B, C, D), 이전 블록의 해시 값, 현재 블록의 해시 값, 넌스(Nonce)를 포함할 수 있다. 또한, 블록 헤더(401)는 블록(400) 내의 트랜잭션 정보(302)를 나타내는 해시 값을 포함할 수 있다.

[69] 일 실시 예에서, 블록 체인은 연결된 복수의 블록들을 포함할 수 있다. 복수의 블록들은 블록 헤더(401) 내의 해시 값에 기초하여 연결될 수 있다. 블록 헤더(401)에 포함된 이전 블록의 해시 값 직전 블록에 대한 해시 값으로서 직전 블록에 포함된 현재 해시 값과 동일한 값일 수 있다. 복수의 블록들은 각 블록 헤더 내의 이전 블록의 해시 값에 의하여 연쇄적으로 연결될 수 있다. 분권형 네트워크(100)에 참여하는 노드들(200)은 하나 이상의 블록들에 포함된 이전 블록의 해시 값에 기반하여 블록의 유효성을 검증하므로 악의적인 단일 노드가 이미 생성된 블록의 내용을 위조 또는 변조하는 행위가 불가능할 수 있다.

[70] 일 실시 예에서, 블록 바디(402)는 트랜잭션 정보(302), 트랜잭션 리스트, 또는 트랜잭션 체인을 포함할 수 있다. 트랜잭션 정보(302)는 트랜잭션(300)에서 생성된 거래와 관련된 정보일 수 있다. 트랜잭션 리스트는 블록 체인 기반의 거래의 목록일 수 있다. 예를 들면, 트랜잭션 리스트는 블록 체인 기반의 금융 시스템에서 이루어진 금융 거래에 대한 기록을 포함할 수 있다. 트랜잭션 리스트는 트리(tree) 형태로 표현될 수 있으며, 예를 들어, 사용자 A가 사용자 B에게 전송한 금액을 목록 형태로 기록하며, 블록 내의 저장 길이는 현재 블록에 포함된 트랜잭션의 수에 기초하여 증감될 수 있다.

[71] 발명의 한 실시 예에 따르면, 도 2에 개시된 바와 달리, 제1 노드(210)와 제2 노드(220)는 동일한 노드일 수 있다. 즉, 트랜잭션(300)을 생성하고 블록(400)을 생성하는 노드는 동일할 수 있다. 하기에서 설명의 편의를 위해 제1 노드(210)와 제2 노드(220)를 구분하여 기재하지만, 하기 도면 3 내지 도 8에 개시된 바와 달리 동일한 노드가 트랜잭션(300) 생성, 블록(400) 생성, 생성된 블록(400) 공유 및 블록(400) 검증을 모두 수행할 수 있다.

[72] 도 3은 본 발명의 일 실시 예에 따른 블록체인에서 특정 노드간 블록을 공유하는 방법을 설명하기 위한 흐름도이다. 도 4는 본 발명의 일 실시 예에 따른 블록체인에서 특정 노드간 블록을 공유하는 방법을 설명하기 위한 예시도이다. 도 3의 동작들은 도 2에 개시된 제1 노드(210)와 제2 노드(220)에 의해 수행될 수 있다. 한편, 도 4에 개시된 블록 1(410), 블록 2(420), 블록 3(430)은 순차적으로 연결된 블록 체인 구조일 수 있다.

[73] 한편, 설명의 편의를 위해 하기에서 설명할 특정 노드들은 생성된 블록과 관련 있는 노드들로써 블록 헤더와 블록 바디(트랜잭션 정보)를 모두 포함하는 블록을 공유하는 노드들로 이해될 수 있고, 나머지 노드들은 생성된 블록과 관련 없는 노드들로써 블록 헤더만을 포함하는 서브 블록을 공유하는 노드들로 이해될 수 있다.

[74] 도 3 및 도 4를 참조하면, 일 실시 예에서, 동작 31에서, 복수의 노드들(200) 중에서 적어도 하나의 제1 노드(210)가 특정 노드들의 식별 정보 및 트랜잭션 정보를 포함하는 적어도 하나의 트랜잭션을 생성할 수 있다. 여기서 적어도 하나의 제1 노드(210)는 단일 노드 또는 복수의 노드를 모두 포함하는 개념일 수 있다. 하기에서 "적어도 하나의"의 수식을 받는 구성은 모두 단일 또는 복수를 포함하는 개념으로 이해될 수 있다. 예를 들어, 도 4에 도시된 바와 같이, 적어도 하나의 제1 노드(210)는 트랜잭션 1(310), 트랜잭션 2(320), 트랜잭션 3(330), 트랜잭션 N(340)을 생성할 수 있다. 각각의 트랜잭션들은 하나의 제1 노드(210)가 생성하거나 또는 복수의 제1 노드(210)가 각각 생성할 수 있다. 트랜잭션 1(310)은 특정 노드들의 식별 정보(311, Node: A, B, C, D)와 트랜잭션 1 정보(312)를 포함할 수 있고, 트랜잭션 2(320)는 특정 노드들의 식별 정보(321, Node: B)와 트랜잭션 2 정보(322)를 포함할 수 있고, 트랜잭션 3(330)은 특정 노드들의 식별 정보(331, Node: A, B, C, D)와 트랜잭션 3 정보(332)를 포함할 수 있고, 트랜잭션 N(340)은 특정 노드들의 식별 정보(341, Node: B, D)와 트랜잭션 N 정보(342)를 포함할 수 있다. 여기서 도 4에 개시된 트랜잭션들의 개수는 설명의 편의를 위한 예시적인 것이고 트랜잭션들의 개수는 다양하게 변형될 수 있다.

[75] 일 실시 예에서, 동작 32에서, 복수의 노드들(200) 중에서 적어도 하나의 제2 노드(220)가 식별 정보 및 트랜잭션 정보에 기반하여 적어도 하나의 블록을 생성할 수 있다. 예를 들어, 적어도 하나의 제2 노드(200)는 블록 1(410), 블록 2(420), 블록 3(430)을 생성할 수 있다. 각각의 블록들은 하나의 제2 노드(220)가 생성하거나 또는 복수의 제2 노드(220)가 각각 생성할 수 있다. 예를 들어, 블록 2(420)는 트랜잭션 2(320)의 식별 정보(321, Node: B)와 트랜잭션 2 정보(322)에 기반하여 생성될 수 있고, 식별 정보(321, Node: B)를 포함하는 블록 헤더(421)와 트랜잭션 2 정보(322)를 포함하는 블록 바디(422)로 구성될 수 있다. 또한, 블록 3(430)는 트랜잭션 N(340)의 식별 정보(341, Node: B, D)와 트랜잭션 N 정보(342)에 기반하여 생성될 수 있고, 식별 정보(341, Node: B, D)를 포함하는 블록 헤더(431)와 트랜잭션 N 정보(342)를 포함하는 블록 바디(432)로 구성될 수 있다. 한편, 블록 1(410)의 생성에 관한 구체적인 설명은 도 5에서 후술한다. 여기서 도 4에 개시된 블록들의 개수는 설명의 편의를 위한 예시적인 것이고 블록들의 개수는 다양하게 변형될 수 있다.

[76] 일 실시 예에서, 동작 33에서, 적어도 하나의 제2 노드(220)가 생성된 적어도 하나의 블록을 식별 정보에 기반하여 특정 노드들에게 공유할 수 있다. 예를 들어, 적어도 하나의 제2 노드(220)는 블록 헤더(421)에 포함된 식별 정보(321, Node: B)에 기반해서 블록 2(420)를 노드 B(240)에게 공유할 수 있다. 또한, 적어도 하나의 제2 노드(220)는 블록 헤더(431)에 포함된 식별 정보(341, Node: B, D)에 기반해서 블록 3(430)을 노드 B(240)와 노드 D(260)에게 공유할 수 있다. 한편, 블록 1(410)의 공유에 관한 구체적인 설명은 도 5에서 후술한다.

[77] 일 실시 예에서, 블록 2(420)는 노드 A(230), 노드 C(250), 노드 D(260)에게도 공유될 수 있고, 블록 3(430)은 노드 A(230), 노드 C(250)에게도 공유될 수 있다. 특정 노드들을 제외한 나머지 노드들이 블록들을 공유하는 구체적인 내용은 도 6에서 후술한다.

[78] 일 실시 예에서, 동작 34에서, 적어도 하나의 제2 노드(220)가 생성된 적어도 하나의 블록을 저장 및 관리할 수 있다. 예를 들어, 블록(410, 420, 430)을 생성한 적어도 하나의 제2 노드(220)가 블록(410, 420, 430)을 저장하고 전반적으로 관리할 수 있다. 한편, 블록을 검증하는 방법에 관한 설명은 도 8에서 후술한다.

[79] 이와 같이 본 발명은 생성된 블록을 모든 노드들이 공유하되 식별 정보에 기반하여 블록과 관련 있는 특정노드들에게만 트랜잭션 정보를 포함하는 블록을 공유시킬 수 있다.

[80] 발명의 한 실시 예에 따르면, 도면에 도시된 바와 달리, 제1 노드(210)(210)와 제2 노드(220)(220)는 동일한 노드일 수 있다.

[81] 도 5는 본 발명의 일 실시 예에 따른 식별 정보를 이용하여 블록을 생성하고 특정 노드들에게 공유하는 방법을 설명하기 위한 흐름도이다. 도 5의 동작들은 도 3의 동작 32 및 동작 33을 구체화한 동작들일 수 있다. 도 5의 동작들은 도 2에 개시된 제1 노드(210)(210)와 제2 노드(220)(220)에 의해 수행될 수 있다. 한편, 도 4에 개시된 블록 1(410), 블록 2(420), 블록 3(430)은 순차적으로 연결된 블록 체인 구조일 수 있다.

[82] 도 4 및 도 5를 참조하면, 일 실시 예에서, 동작 51에서, 적어도 하나의 제2 노드(220)가 적어도 하나의 트랜잭션 중에서 동일한 식별 정보를 갖는 트랜잭션들을 확인할 수 있다. 예를 들어, 도 4에 도시된 바와 같이, 적어도 하나의 제2 노드(220)는 식별 정보(311, Node: A, B, C, D)를 갖는 트랜잭션 1(310)과 식별 정보(331, Node: A, B, C, D)를 갖는 트랜잭션 3(330)을 확인할 수 있다. 즉, 적어도 하나의 제2 노드(220)는 트랜잭션 1(310)과 트랜잭션 3(330)이 동일한 식별 정보로서 Node: A, B, C, D를 가짐을 확인할 수 있다.

[83] 일 실시 예에서, 동작 52에서, 적어도 하나의 제2 노드(220)가 동일한 식별 정보를 갖는 트랜잭션들만 포함되는 블록을 생성할 수 있다. 예를 들어, 적어도 하나의 제2 노드(220)는 블록 1(410)을 생성할 수 있다. 예를 들어, 블록 1(410)은 식별 정보(311, Node: A, B, C, D)와 식별 정보(331, Node: A, B, C, D)를 포함하는 블록 헤더(411)와 트랜잭션 1 정보(312)와 트랜잭션 3 정보(332)를 포함하는 블록 바디(412)로 구성될 수 있다.

[84] 일 실시 예에서, 동작 53에서, 적어도 하나의 제2 노드(220)가 동일한 식별 정보를 갖는 트랜잭션들만 포함되는 블록을 동일한 식별 정보에 대응하는 특정 노드들에게 공유할 수 있다. 예를 들어, 적어도 하나의 제2 노드(220)는 식별 정보(311, 331)에 따라 노드 A(230), 노드 B(240), 노드 C(250), 노드 D(260)에게 블록 1(410)을 공유할 수 있다.

[85] 발명의 한 실시 예에 따르면, 도면에 도시된 바와 달리, 제1 노드(210)(210)와

제2 노드(220)(220)는 동일한 노드일 수 있다.

[86] 도 6은 본 발명의 일 실시 예에 따른 서브 블록을 생성하고 공유하는 방법을 설명하기 위한 흐름도이다. 도 7은 본 발명의 일 실시 예에 따른 서브 블록을 생성하고 공유하는 방법을 설명하기 위한 예시도이다. 도 6의 동작들은 도 3의 동작 32 및 동작 33을 구체화한 동작들일 수 있다. 도 6의 동작들은 도 2에 개시된 제1 노드(210)(210)와 제2 노드(220)(220)에 의해 수행될 수 있다. 한편, 도 7에 개시된 블록 1(410), 블록 2(420), 블록 3(430)은 순차적으로 연결된 블록 체인 구조일 수 있다.

[87] 도 6 및 도 7을 참조하면, 일 실시 예에서, 동작 61에서, 적어도 하나의 블록의 생성이 완료된 이후, 적어도 하나의 제2 노드(220)가 생성한 적어도 하나의 블록의 헤더를 추출할 수 있다. 예를 들어, 도 7에 도시된 바와 같이, 적어도 하나의 제2 노드(220)는 블록 2(420)의 생성을 완료한 이후 블록 2(420)에서 블록 헤더(424)를 추출할 수 있다. 예를 들어, 블록 헤더(424)는 이전 블록의 해시 값(예: 블록 1 해시 값), 현재 블록의 해시 값, 트랜잭션 해시 값을 포함할 수 있다.

[88] 일 실시 예에서, 동작 62에서, 적어도 하나의 제2 노드(220)가 추출한 블록의 헤더만 포함되는 적어도 하나의 서브 블록을 생성할 수 있다. 여기서 서브 블록은 이미 생성한 블록과 동일성을 유지하되 블록의 헤더만을 포함하는 블록일 수 있다. 예를 들어, 적어도 하나의 제2 노드(220)는 블록 헤더(424)만 포함하는 서브 블록 2(423)을 생성할 수 있다. 여기서 블록 헤더(424)는 도 6에 개시된 바와 같이, 블록 헤더(421)에서 식별 정보(321)만 제외된 나머지 정보를 포함할 수 있다. 물론 이와 달리 블록 헤더(424)는 블록 2(420)의 블록 헤더(421)와 동일할 수 있다. 즉,서브 블록 2(423)은 블록2(420)와 동일성을 유지하되 블록 헤더(424)만 포함하는 블록일 수 있다.

[89] 일 실시 예에서, 동작 63에서, 적어도 하나의 제2 노드(220)가 생성한 적어도 하나의 서브 블록을 복수의 노드들(200) 중 특정 노드들을 제외한 나머지 노드들에게 공유할 수 있다. 예를 들어, 적어도 하나의 제2 노드(220)는 서브 블록 2(423)을 노드 A(230), 노드 C(250), 노드 D(260)에게 공유할 수 있다.

[90] 일 실시 예에서, 동작 64에서, 나머지 노드들이 블록 해시 값을 이용하여 적어도 하나의 서브 블록의 무결성을 검증할 수 있다. 서브 블록의 무결성을 검증하는 구체적인 설명은 도 8에서 후술한다.

[91] 일 실시 예에서, 도 4에 개시된 블록 3(430)도 도 6에 설명된 블록 2(420)의 서브 블록 2(423)의 공유 방법과 동일한 방법으로 나머지 노드들에게 공유될 수 있다. 즉, 블록 3(430)의 서브 블록 3은 블록 3(430)에서 추출된 블록 헤더만 가진 채 노드 A(230)와 노드 C(250)에게 공유될 수 있다.

[92] 이와 같이, 본 발명은 생성된 블록을 도 4에 도시된 바와 같이 모든 노드들이 공유하되, 특정 노드들은 트랜잭션 정보를 포함하는 완전한 블록을 공유시키고 나머지 노드들은 블록 헤더만 포함하는 서브 블록을 공유시킬 수 있다. 이와 같이 동작함으로써 본 발명은 별도의 그룹 지정 없이 블록의 관리 효율성을

증대시킬 수 있다.

[93] 발명의 한 실시 예에 따르면, 도면에 도시된 바와 달리, 제1 노드(210)(210)와 제2 노드(220)(220)는 동일한 노드일 수 있다.

[94] 도 8은 본 발명의 일 실시 예에 따른 서브 블록 및 트랜잭션 정보의 무결성을 검증하는 방법을 설명하기 위한 흐름도이다. 도 8의 동작들은 도 6의 동작 64를 구체화한 동작들일 수 있다. 도 8의 동작들은 도 2에 개시된 제1 노드(210)(210)와 제2 노드(220)(220)에 의해 수행될 수 있다.

[95] 일 실시 예에서, 나머지 노드들이 공유하는 블록 헤더가 없는 블록의 무결성 검증 방법은 두 단계로 이루어질 수 있다. 첫 번째 단계는 블록에 포함된 해시 값을 이용하여 검증하는 단계이고, 두 번째 단계는 블록에 포함되지 않은 트랜잭션의 무결성을 검증하는 단계이다.

[96] 도 7 및 도 8을 참조하면, 일 실시 예에서, 동작 81에서, 나머지 노드들이 블록 해쉬 값을 이용하여 서브 블록의 무결성을 검증할 수 있다. 예를 들어, 노드 A(230), 노드 C(250), 노드 D(260)는 서브 블록 2(423)에 포함된 블록 해시 값(이전 블록의 해시 값, 현재 블록의 해시 값)을 이용하여 서브 블록 2의 무결성을 검증할 수 있다.

[97] 일 실시 예에서, 동작 82에서, 나머지 노드들 중 적어도 하나의 노드가 적어도 하나의 제2 노드(220)에게 적어도 하나의 서브 블록에 대응하는 트랜잭션 해시 값을 요청할 수 있다. 예를 들어, 노드 A(230), 노드 C(250), 노드 D(260) 중 적어도 하나의 노드가 적어도 하나의 제2 노드(220)에게 서브 블록 2(423)에 대응하는 트랜잭션 해시 값을 요청할 수 있다. 여기서 제2 노드(220)는 블록 2(420)를 생성, 저장, 관리하는 노드일 수 있다.

[98] 일 실시 예에서, 동작 83에서, 적어도 하나의 제2 노드(220)가 요청한 트랜잭션 해시 값을 연산할 수 있다. 예를 들어, 적어도 하나의 제2 노드(220)는 블록 2(420)의 블록 헤어(421)에 저장된 트랜잭션 해시 값에 기반하여 요청한 트랜잭션 해시 값을 연산할 수 있다.

[99] 일 실시 예에서, 동작 84에서, 적어도 하나의 제2 노드(220)가 연산한 트랜잭션 해시 값을 적어도 하나의 노드에게 전송할 수 있다. 예를 들어, 적어도 하나의 제2 노드(220)는 연산한 트랜잭션 해시 값을 노드 A(230), 노드 C(250), 노드 D(260) 중 상기 요청을 한 노드에게 전송할 수 있다.

[100] 일 실시 예에서, 동작 85에서, 적어도 하나의 노드가 수신한 트랜잭션 해시 값과 기 저장된 트랜잭션 해시 값을 비교할 수 있다. 예를 들어, 노드 A(230), 노드 C(250), 노드 D(260) 중 적어도 하나의 노드는 수신한 트랜잭션 해시 값과 서브 블록 2(423)에 포함되어 기 저장된 트랜잭션 해시 값을 비교할 수 있다.

[101] 일 실시 예에서, 동작 86에서, 적어도 하나의 노드가 비교 결과에 기반하여 서브 블록에 포함된 트랜잭션 정보의 무결성을 검증할 수 있다. 예를 들어, 노드 A(230), 노드 C(250), 노드 D(260) 중 적어도 하나의 노드가 서브 블록 2(423)에 포함된 트랜잭션 정보의 무결성을 검증할 수 있다.

[102] 발명의 한 실시 예에 따르면, 복수의 노드들(200)은 적어도 하나의 블록과 적어도 하나의 서브 블록을 동일한 블록으로 저장 및 관리할 수 있다.

[103] 발명의 한 실시 예에 따르면, 도면에 도시된 바와 달리, 제1 노드(210)(210)와 제2 노드(220)(220)는 동일한 노드일 수 있다.

[104] 본 발명의 일 실시예에 따른 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법은 상기 복수의 노드들 중에서 적어도 하나의 제1 노드가 상기 특정 노드들의 식별 정보 및 트랜잭션 정보를 포함하는 적어도 하나의 트랜잭션을 생성하는 단계; 기 복수의 노드들 중에서 적어도 하나의 제2 노드가 상기 식별 정보 및 상기 트랜잭션 정보에 기반하여 적어도 하나의 블록을 생성하는 단계; 및 상기 적어도 하나의 제2 노드가 상기 생성된 적어도 하나의 블록을 상기 식별 정보에 기반하여 상기 특정 노드들에게 공유하는 단계를 포함할 수 있다.

[105] 다양한 실시 예에 따르면, 상기 적어도 하나의 블록을 생성하는 단계는, 상기 적어도 하나의 제2 노드가 상기 적어도 하나의 트랜잭션 중에서 동일한 식별 정보를 갖는 트랜잭션들을 확인하는 단계; 상기 적어도 하나의 제2 노드가 상기 동일한 식별 정보를 갖는 트랜잭션들만 포함되는 블록을 생성하는 단계; 및 상기 적어도 하나의 제2 노드가 상기 동일한 식별 정보를 갖는 트랜잭션들만 포함되는 상기 블록을 상기 동일한 식별 정보에 대응하는 특정 노드들에게 공유하는 단계를 포함할 수 있다.

[106] 다양한 실시 예에 따르면, 상기 적어도 하나의 제2 노드가 상기 생성된 적어도 하나의 블록을 저장 및 관리하는 단계를 더 포함할 수 있다.

[107] 다양한 실시 예에 따르면, 상기 적어도 하나의 블록을 생성하는 단계는, 상기 적어도 하나의 블록의 생성이 완료된 이후, 상기 적어도 하나의 제2 노드가 상기 생성한 적어도 하나의 블록의 헤더를 추출하는 단계; 및 상기 적어도 하나의 제2 노드가 상기 추출한 블록의 헤더만 포함되는 적어도 하나의 서브 블록을 생성하는 단계를 포함할 수 있다.

[108] 다양한 실시 예에 따르면, 상기 특정 노드들에게 공유하는 단계는, 상기 적어도 하나의 제2 노드가 상기 생성한 적어도 하나의 서브 블록을 상기 복수의 노드들 중 상기 특정 노드들을 제외한 나머지 노드들에게 공유하는 단계를 더 포함할 수 있다.

[109] 다양한 실시 예에 따르면, 상기 적어도 하나의 서브 블록은 블록 해시 값을 포함하고, 상기 나머지 노드들이 상기 블록 해시 값을 이용하여 상기 적어도 하나의 서브 블록의 무결성을 검증하는 단계를 더 포함할 수 있다.

[110] 다양한 실시 예에 따르면, 상기 나머지 노드들 중 적어도 하나의 노드가 상기 적어도 하나의 제2 노드에게 상기 적어도 하나의 서브 블록에 대응하는 트랜잭션 해시 값을 요청하는 단계; 상기 적어도 하나의 제2 노드가 상기 요청한 트랜잭션 해시 값을 연산하는 단계; 상기 적어도 하나의 제2 노드가 상기 연산한 트랜잭션 해시 값을 상기 적어도 하나의 노드에게 전송하는 단계; 및 상기

적어도 하나의 노드가 상기 수신한 트랜잭션 해시 값과 기 저장된 트랜잭션 해시 값을 비교하는 단계를 더 포함할 수 있다.

[111] 다양한 실시 예에 따르면, 상기 적어도 하나의 노드가 상기 비교 결과에 기반하여 상기 서브 블록에 포함된 상기 트랜잭션 정보의 무결성을 검증하는 단계를 더 포함할 수 있다.

[112] 다양한 실시 예에 따르면, 상기 복수의 노드들이 상기 적어도 하나의 블록과 상기 적어도 하나의 서브 블록을 동일한 블록으로 저장 및 관리하는 단계를 더 포함할 수 있다.

[113] 본 발명의 일 실시예에 따른 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 시스템은 블록체인 네트워크를 구성하는 복수의 노드들을 포함하고, 기 복수의 노드들 중에서 적어도 하나의 제1 노드가 상기 특정 노드들의 식별 정보 및 트랜잭션 정보를 포함하는 적어도 하나의 트랜잭션을 생성하고, 상기 복수의 노드들 중에서 적어도 하나의 제2 노드가 상기 식별 정보 및 상기 트랜잭션 정보에 기반하여 적어도 하나의 블록을 생성하고, 상기 적어도 하나의 제2 노드가 상기 생성된 적어도 하나의 블록을 상기 식별 정보에 기반하여 상기 특정 노드들에게 공유할 수 있다.

[114] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이 아닌 것으로 이해해야만 한다.

[115]

[116] <블록체인에서 스마트 컨트랙트를 이용한 전자 문서 유통 방법>

[117]

[118] 도 9는 본 발명의 블록체인 시스템을 나타낸 블록도이다.

[119] 도 9를 참조하면, 블록체인 시스템은 복수의 노드들(20)로 이루어진 분권형 네트워크(decentralized network, 10) 시스템일 수 있다. 분권형 네트워크(10)를 구성하는 노드들(20)은 컴퓨터, 서버, 이동 단말기 등 연산 기능, 통신 기능, 저장 기능 등을 구비한 전자 장치일 수 있다.

[120] 일 실시 예에서, 분권형 네트워크(10)는 블록체인(block chain)이라 불리는 블록(block)의 연결 묶음 내에 모든 참여 노드에 공통으로 알려진 정보를 저장하고 참조할 수 있다. 복수의 노드들(20)은 상호간 통신이 가능하며 블록체인을 저장, 관리 및 전파를 담당하는 완전 노드(full node)와 단순하게 트랜잭션에만 참여할 수 있는 간이 노드(light node)로 구분될 수 있다. 본 명세서에서 별다른 설명 없이 노드에 대하여 언급되는 경우, 이는 분권형 네트워크(10)에 참여하며 블록체인을 생성, 저장 또는 검증하는 동작을 수행하는 완전 노드를 지칭하는 경우가 많으나, 이에 국한되지 않는다.

[121] 도 10은 본 발명의 블록체인 시스템의 복수의 노드들을 나타낸 블록도이다. 도

11은 본 발명의 일 실시 예에 따른 블록을 나타낸 예시도이다. 한편, 도 11에 개시된 블록 1(310), 블록 2(320), 블록 3(330)은 순차적으로 연결된 블록체인 구조일 수 있다.

[122] 도 10 및 도 11을 참조하면, 본 발명의 일 실시 예에 따른 블록체인 시스템에 포함된 노드(200)는 제어 모듈(210), 전자 문서 관리 및 유통 모듈(220), 전자 문서 분할 모듈(230), 블록 생성 모듈(240), 통신 모듈(250), 메모리(260), 입력 및 출력 모듈(270)을 포함할 수 있다.

[123] 일 실시 예에서, 제어 모듈(210)은 노드(200)를 전반적으로 제어하기 위한 구성일 수 있다. 구체적으로, 제어 모듈(210)은 노드(200)의 메모리(260)에 저장된 각종 프로그램을 이용하여 노드(200)의 전반적인 동작을 제어할 수 있다. 제어 모듈(210)은 메모리(260)에 저장된 애플리케이션을 통해 데이터를 생성하도록 노드(200)를 제어할 수 있다.

[124] 일 실시 예에서, 전자 문서 관리 및 유통 모듈(220)은 블록체인 시스템(100)에서 합의 또는 서명이 이루어지거나, 또는 합의나 서명 없이 복수의 노드들(20)에게 배포될 수 있다.

[125] 일 실시 예에서, 전자 문서 관리 및 유통 모듈(220)은 스마트 컨트랙트 기반으로 동작할 수 있다. 스마트 컨트랙트는 블록체인에서 각 노드들이 자동으로 서로 거래를 할 수 있게 해주는 개념이다. 본 발명은 전자 문서 정보를 문서 파일 형태로 열람할 수 있게 해주는 전자 문서 서식을 분산화된 응용프로그램 형태로 각 노드들에 분산 저장할 수 있고, 여기서 분산화된 응용프로그램은 해당 응용프로그램의 기능을 정의하는 자체 실행 코드(스마트 컨트랙트)로 구성될 수 있다. 따라서, 전자 문서 서식과 관련된 분산화된 응용프로그램이 복수의 노드들에 분산저장됨으로써 전자 문서 정보가 자동으로 노드에서 서식과 결합될 수 있고, 이러한 자동 병합 동작이 스마트 컨트랙트를 의미할 수 있다.

[126] 일 실시 예에서, 전자 문서 관리 및 유통 모듈(220)은 블록체인 시스템(100)의 외부에서 전자 문서 서식과 관련된 분산화된 응용프로그램을 실행시킬 수 있는 인터페이스와 각종 전자 문서 서식을 포함할 수 있다. 또한, 전자 문서 관리 및 유통 모듈(220)은 전자 문서 서식과 전자 문서 정보를 병합하는 조건을 하기에서 설명할 제1 분할 데이터에서 추출하거나 자체적으로 미리 저장할 수 있다. 또한, 전자 문서 관리 및 유통 모듈(220)은 병합 조건에 따라 하기에서 설명할 전자 문서 서식에 대응하는 제1 분할 데이터와 전자 문서 정보에 대응하는 제2 분할 데이터를 병합할 수 있다. 전자 문서 서식과 전자 문서 정보의 병합하는 절차는 주어진 조건에 따라 전자 문서의 정보를 전자 문서 서식의 지정된 공간에 위치시키거나, 전자 문서 정보에 포함된 데이터의 연산 및 조합한 결과를 표시하거나, 전자 문서 정보의 크기 및 수량에 따라 전자 문서 서식을 추가하는 등의 다양한 방법을 포함할 수 있다.

[127] 일 실시 예에서, 전자 문서 분할 모듈(230)은 전자 문서를 제1 분할 데이터와 제2 분할 데이터로 분할할 수 있다. 여기서 제1 분할 데이터는 전자 문서 서식,

병합 조건, 기타 전자 문서의 이용과 관련된 각종 조건을 포함할 수 있다. 여기서 제2 분할 데이터는 전자 문서 정보와 식별자를 포함할 수 있다.

[128] 일 실시 예에서, 블록 생성 모듈(240)은 제2 분할 데이터를 포함하는 블록을 생성할 수 있다.

[129] 보다 구체적으로, 도 11을 참조하면, 일 실시 예에서, 블록체인에 연결되어 있는 각 블록(block)들은 일정 기간 내의 거래 내역, 즉 트랜잭션(transaction)들을 포함한다. 노드들(20)은 각각 역할에 따라 블록체인을 생성, 저장 또는 검증함으로써 트랜잭션들을 관리한다.

[130] 일 실시 예에서, 트랜잭션은 다양한 형태의 거래를 나타낼 수 있다. 예를 들어, 트랜잭션은 가상 화폐의 소유 상태 및 그 변동을 나타내기 위한 금융 거래에 해당할 수 있다. 또한, 다른 예에서 트랜잭션은 물건의 소유 상태 및 그 변동을 나타내기 위한 실물 거래에 해당할 수 있다. 분권형 네트워크(10)에서 거래를 수행하는 노드들은 각각의 암호학적 연관관계가 있는 개인키(private key) 및 공개키(public key) 쌍을 가질 수 있다.

[131] 일 실시 예에서, 본 발명에 개시된 블록체인은 순차적으로 연결된 하나 이상의 블록들의 분산 데이터베이스의 일종일 수 있다. 블록체인은 블록체인 시스템 내 사용자의 거래 내역을 저장하고 관리하기 위해 사용되며, 블록체인 네트워크(10)에 참여하는 각 노드가 블록을 생성하여 블록체인에 연결한다. 예컨대 도 11에 개시된 블록 1 내지 블록 3은 순차적으로 연결된 블록체인의 블록 중 일부일 수 있다. 도 11에서 제한된 수의 블록들이 도시되어 있으나 블록체인에 포함될 수 있는 블록의 수는 이에 제한되지 아니한다.

[132] 일 실시 예에서, 블록체인에 포함된 각 블록은 블록 헤더(Block header)와 블록 바디(Block body)를 포함하도록 구성될 수 있다. 블록 헤더는 각 블록들간의 연결 관계를 나타내기 위하여 이전 블록의 해시 값을 포함할 수 있다. 블록체인이 유효한지 검증하는 과정에서 블록 헤더 내의 연결 관계가 사용될 수 있다. 블록 바디는 블록에 저장되고 관리되는 데이터, 예를 들어 트랜잭션 정보, 트랜잭션 리스트 또는 트랜잭션 체인을 포함할 수 있다.

[133] 일 실시 예에서, 블록 헤더는 이전 블록의 해시 값, 현재 블록의 해시 값, 서브 블록의 해시 값, 트랜잭션 해시 값, 넌스(Nonce)를 포함할 수 있다.

[134] 일 실시 예에서, 블록체인은 연결된 복수의 블록들을 포함할 수 있다. 복수의 블록들은 블록 헤더 내의 해시 값에 기초하여 연결될 수 있다. 블록 헤더에 포함된 이전 블록의 해시 값 직전 블록에 대한 해시 값으로서 직전 블록에 포함된 현재 해시 값과 동일한 값일 수 있다. 복수의 블록들은 각 블록 헤더 내의 이전 블록의 해시 값에 의하여 연쇄적으로 연결될 수 있다. 분권형 네트워크(10)에 참여하는 노드들(20)은 하나 이상의 블록들에 포함된 이전 블록의 해시 값에 기반하여 블록의 유효성을 검증하므로 악의적인 단일 노드가 이미 생성된 블록의 내용을 위조 또는 변조하는 행위가 불가능할 수 있다.

[135] 일 실시 예에서, 블록 바디는 트랜잭션 정보, 트랜잭션 리스트, 또는 트랜잭션

체인을 포함할 수 있다. 트랜잭션 정보는 트랜잭션에서 생성된 다양한 형태의 거래와 관련된 정보일 수 있다. 트랜잭션 리스트는 블록체인 기반의 거래의 목록일 수 있다. 예를 들면, 트랜잭션 리스트는 블록체인 기반의 금융 시스템에서 이루어진 금융 거래에 대한 기록을 포함할 수 있다. 트랜잭션 리스트는 트리(tree) 형태로 표현될 수 있으며, 예를 들어, 사용자 A가 사용자 B에게 전송한 금액을 목록 형태로 기록하며, 블록 내의 저장 길이는 현재 블록에 포함된 트랜잭션의 수에 기초하여 증감될 수 있다.

[136] 일 실시 예에서, 예를 들어, 블록 1(310)은 블록 헤더(311)와 블록 바디(312)를 포함할 수 있다. 블록 헤더(311)는 이전 블록 해시 값(Block 0 hash), 현재 블록 해시 값(Block 1 hash) 및 트랜잭션 해시 값(Transaction hash)을 포함할 수 있다. 블록 바디(312)는 트랜잭션 1 정보와 보안 식별자(Security Identifier)를 포함할 수 있다. 여기서 트랜잭션 1 정보는 전자 문서의 제2 분할 데이터를 포함할 수 있다. 한편, 블록 2(320)와 블록 3(330)에 대한 설명은 블록 1(310)과 동일하므로 생략한다.

[137] 일 실시 예에서, 통신 모듈(250)은 노드(200)와 다른 노드들간 또는 외부 장치간의 통신 연결을 통해 데이터를 송수신할 수 있다. 한편, 통신 모듈(250)은 다양한 유형의 통신방식에 따라 다양한 유형의 외부 장치와 통신을 수행하는 구성일 수 있다. 예를 들어, 통신 모듈(250)은 근거리 통신 모듈(예: 블루투스, WiFi direct 또는 IrDA(infrared data association)) 또는 원거리 통신 모듈(예: 셀룰러 네트워크, 인터넷, 또는 컴퓨터 네트워크(예: LAN 또는 WAN))일 수 있다.

[138] 일 실시 예에서, 메모리(260)는 노드(200)의 각종 명령어 수행과 관련된 모든 데이터를 저장할 수 있다. 또한, 메모리(260)는 제어 모듈(210)의 처리 또는 제어를 위한 프로그램 등 노드(200)의 전반적인 동작을 위한 다양한 데이터를 저장할 수 있다.

[139] 일 실시 예에서, 입력 및 출력 모듈(270)은 사용자의 입력을 수신하기 위한 장치와 이미지 또는 음향을 출력하는 장치를 포함할 수 있다. 예를 들어, 입력 및 출력 모듈(270)은 터치스크린, 마우스, 키보드, 디스플레이, 스피커 등을 포함할 수 있다.

[140] 하기 도 12 내지 도 14에서 설명할 본 발명의 각 방법들은 블록체인 네트워크(10)에 포함된 복수의 노드들(20) 중 어느 하나의 노드가 수행할 수 있다. 또한, 전자 문서를 분할하는 동작, 블록을 생성하는 동작, 및 데이터를 병합하는 동작들은 어느 한 노드가 모두 수행하거나 각각 다른 노드가 수행할 수 있다.

[141] 도 12는 본 발명의 일 실시 예에 따른 블록체인에서 전자 문서를 유통하는 방법을 설명하기 위한 흐름도이다. 도 12의 동작들은 도 10에 개시된 노드(200)에 의해 수행될 수 있다.

[142] 도 12를 참조하면, 일 실시 예에서, 일 실시 예에서, 동작 41에서, 노드(200)는 전자 문서를 전자 문서 서식 및 병합 조건을 포함하는 제1 분할 데이터 및

식별자와 전자 문서 정보를 포함하는 제2 분할 데이터로 분할할 수 있다. 예를 들어, 제1 분할 데이터는 전자 문서 서식, 병합 조건, 기타 전자 문서의 이용과 관련된 각종 조건을 포함할 수 있다. 또한, 제2 분할 데이터는 전자 문서 정보, 식별자, 연결주소를 포함할 수 있다. 예컨대, 전자 문서 정보는 전자 문서에 포함된 각종 내용 등을 포함할 수 있고, 식별자는 제1 분할 데이터에 포함된 전자 문서 서식을 식별할 수 있는 태그일 수 있다.

[143] 일 실시 예에서, 동작 42에서, 노드(200)는 제1 분할 데이터를 복수의 노드들(20)에 분산 저장할 수 있다. 예를 들어, 복수의 노드들(20)은 제1 분할 데이터를 분산화된 응용프로그램 형태(스마트 컨트랙트)로 관리할 수 있다.

[144] 구체적으로, 스마트 컨트랙트는 블록체인에서 각 노드들이 자동으로 서로 거래를 할 수 있게 해주는 개념이다. 본 발명은 전자 문서 정보를 문서 파일 형태로 열람할 수 있게 해주는 전자 문서 서식을 분산화된 응용프로그램 형태로 각 노드들에 분산 저장할 수 있고, 여기서 분산화된 응용프로그램은 해당 응용프로그램의 기능을 정의하는 자체 실행 코드(스마트 컨트랙트)로 구성될 수 있다. 따라서, 전자 문서 서식과 관련된 분산화된 응용프로그램이 복수의 노드들에 분산저장됨으로써 전자 문서 정보가 자동으로 노드에서 서식과 결합될 수 있고, 이러한 자동 병합 동작이 스마트 컨트랙트를 의미할 수 있다.

[145] 일 실시 예에서, 동작 43에서, 노드(200)는 제2 분할 데이터를 포함하는 블록을 생성하여 복수의 노드들(20)에 분산 저장할 수 있다. 예를 들어, 블록은 도 11에 도시된 바와 같이 블록 바디에서 제2 분할 데이터를 포함할 수 있다. 또한, 전자 문서에 개인 정보가 포함될 경우, 블록은 보안 식별자를 더 포함할 수 있다. 보안 식별자는 전자 문서에 포함된 발급 번호, 전자 문서의 내용, 주민 번호, 주소 중 적어도 하나를 포함할 수 있다.

[146] 일 실시 예에서, 동작 44에서, 노드(200)는 병합 조건 및 식별자에 기반하여, 제1 분할 데이터와 제2 분할 데이터를 병합할 수 있다. 예컨대, 병합하는 방법은 전자 문서 서식의 지정된 공간에 전자 문서 정보를 위치시키거나, 전자 문서 정보에 기반한 연산 및 조합한 결과를 표시하거나, 전자 문서 정보의 크기와 수량에 따라 다른 전자 문서 서식을 추가하는 방법을 포함할 수 있다. 보다 구체적인 내용은 도 13 및 도 14에서 후술한다.

[147] 일 실시 예에서, 동작 45에서, 노드(200)는 병합 결과 생성된 전자 문서를 제공할 수 있다. 예를 들어, 노드(200)는 입력 및 출력 모듈(270)을 통해 전자 문서를 표시할 수 있다.

[148] 이와 같이 전자 문서를 블록체인에서 제공함에 따라 본 발명은 블록체인의 저장 공간을 효율적으로 관리할 수 있다.

[149] 도 13은 본 발명의 일 실시 예에 따른 블록체인에서 분할된 전자 문서를 병합하는 방법을 설명하기 위한 예시도이다. 도 5의 동작들은 도 12의 동작 44를 구체화한 동작들일 수 있다. 도 5의 동작들은 도 10에 개시된 노드(200)에 의해 수행될 수 있다.

[150] 도 13을 참조하면, 일 실시 예에서, 동작 51에서, 노드(200)는 입력 및 출력 모듈(270)을 이용하여 사용자로부터 전자 문서 이용 요청을 검출할 수 있다.

[151] 일 실시 예에서, 동작 52에서, 노드(200)는 전자 문서 관리 및 유통 모듈(220)을 이용하여 제1 분할 데이터에서 전자 문서 서식 및 병합 조건을 추출할 수 있다.

[152] 일 실시 예에서, 동작 53에서, 노드(200)는 전자 문서 관리 및 유통 모듈(220)을 이용하여 제2 분할 데이터에서 식별자와 전자 문서 정보를 추출할 수 있다.

[153] 일 실시 예에서, 동작 54에서, 노드(200)는 전자 문서 관리 및 유통 모듈(220)을 이용하여 식별자에 대응하는 전자 문서 서식을 확인할 수 있다.

[154] 일 실시 예에서, 동작 55에서, 노드(200)는 전자 문서 관리 및 유통 모듈(220)을 이용하여 확인한 전자 문서 서식에 전자 문서 정보를 자동으로 병합할 수 있다.

[155] 이와 같이 본 발명은 사용자의 전자 문서 이용 요청에 응답하여 자동으로 전자 문서 서식과 전자 문서 정보를 병합하여 전자 문서를 제공할 수 있다.

[156] 도 14는 본 발명의 일 실시 예에 따른 블록체인에서 개인 정보를 포함하는 전자 문서를 병합하는 방법을 설명하기 위한 흐름도이다. 도 14의 동작들은 도 12의 동작 44를 구체화한 동작들일 수 있다. 도 14의 동작들은 도 10에 개시된 노드(200)에 의해 수행될 수 있다.

[157] 도 14를 참조하면, 일 실시 예에서, 동작 61에서, 노드(200)는 입력 및 출력 모듈(270)을 이용하여 사용자로부터 개인 정보를 포함하는 전자 문서 이용 요청을 검출할 수 있다. 예를 들어, 개인 정보는 주민 번호, 주소, 개인 이력 등을 포함할 수 있다.

[158] 일 실시 예에서, 동작 62에서, 노드(200)는 전자 문서 관리 및 유통 모듈(220)을 이용하여 제1 분할 데이터에서 전자 문서 서식 및 합 조건을 추출할 수 있다.

[159] 일 실시 예에서, 동작 63에서, 노드(200)는 전자 문서 관리 및 유통 모듈(220)을 이용하여 제2 분할 데이터에서 식별자, 전자 문서 정보 및 보안 식별자를 추출할 수 있다. 예를 들어, 보안 식별자는 전자 문서에 포함된 발급 번호, 전자 문서의 내용, 주민 번호, 주소 중 적어도 하나를 포함할 수 있다.

[160] 일 실시 예에서, 동작 64에서, 노드(200)는 전자 문서 관리 및 유통 모듈(220)을 이용하여 개인 정보를 포함하는 전자 문서 이용 요청에 응답하여 보안 문자 입력을 요청할 수 있다. 예를 들어, 보안 문자는 전자 문서에 포함된 발급 번호 또는 주민 번호일 수 있다.

[161] 일 실시 예에서, 동작 65에서, 노드(200)는 전자 문서 관리 및 유통 모듈(220)을 이용하여 입력한 보안 문자와 보안 식별자를 비교할 수 있다.

[162] 일 실시 예에서, 동작 66에서, 노드(200)는 비교 결과 보안 문자와 보안 식별자가 동일할 경우, 전자 문서 관리 및 유통 모듈(220)을 이용하여 식별자에 대응하는 전자 문서 서식을 확인할 수 있다.

[163] 일 실시 예에서, 동작 67에서, 노드(200)는 전자 문서 관리 및 유통 모듈(220)을 이용하여 확인한 전자 문서 서식에 전자 문서 정보를 병합할 수 있다.

[164] 이와 같이 전자 문서를 블록체인에서 제공함에 따라 본 발명은 전자 문서 이용

신청 시점에 전자 문서 열람 자격을 검증함으로써 블록체인의 신뢰성을 높일 수 있다.

[165] 본 발명의 일 실시예에 따른 복수의 노드들을 포함하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법은 상기 전자 문서를 전자 문서 서식 및 병합 조건을 포함하는 제1 분할 데이터 및 식별자와 전자 문서 정보를 포함하는 제2 분할 데이터로 분할하는 단계; 상기 제1 분할 데이터를 상기 복수의 노드들에 분산 저장하는 단계; 상기 제2 분할 데이터를 포함하는 블록을 생성하여 상기 복수의 노드들에 분산 저장하는 단계; 및 상기 복수의 노드들 중 어느 하나의 노드가, 상기 병합 조건 및 상기 식별자에 기반하여, 상기 제1 분할 데이터와 상기 제2 분할 데이터를 병합하는 단계를 포함할 수 있다.

[166] 다양한 실시 예에 따르면, 상기 복수의 노드들은 상기 제1 분할 데이터를 분산화된 응용프로그램 형태로 관리하는 단계를 더 포함할 수 있다.

[167] 다양한 실시 예에 따르면, 상기 복수의 노드들은 전자 문서 관리 및 유통 모듈을 포함할 수 있다.

[168] 다양한 실시 예에 따르면, 상기 병합하는 단계는, 상기 복수의 노드들 중 어느 하나의 노드에서 전자 문서 이용 요청을 검출하는 단계; 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 제1 분할 데이터에서 상기 전자 문서 서식 및 상기 병합 조건을 추출하는 단계; 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 제2 분할 데이터에서 상기 식별자와 상기 전자 문서 정보를 추출하는 단계; 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 식별자에 대응하는 상기 전자 문서 서식을 확인하는 단계; 및 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 확인한 전자 문서 서식에 상기 전자 문서 정보를 병합하는 단계를 포함할 수 있다.

[169] 다양한 실시 예에 따르면, 상기 병합 결과 생성된 전자 문서를 제공하는 단계를 더 포함할 수 있다.

[170] 다양한 실시 예에 따르면, 상기 전자 문서에 개인 정보가 포함될 경우, 상기 제2 분할 데이터를 포함하는 블록에 보안 식별자를 추가하는 단계를 더 포함할 수 있다.

[171] 다양한 실시 예에 따르면, 상기 보안 식별자는 상기 전자 문서에 포함된 발급 번호, 전자 문서의 내용, 주민 번호, 주소 중 적어도 하나를 포함할 수 있다.

[172] 다양한 실시 예에 따르면, 상기 병합하는 단계는, 상기 복수의 노드들 중 어느 하나의 노드에서 개인 정보를 포함하는 전자 문서 이용 요청을 검출하는 단계; 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 제1 분할 데이터에서 상기 전자 문서 서식 및 상기 병합 조건을 추출하는 단계; 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 제2 분할 데이터에서 상기 식별자, 상기 전자 문서 정보 및 보안 식별자를 추출하는 단계; 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 개인 정보를 포함하는 전자 문서 이용 요청에 응답하여 보안 문자 입력을 요청하는 단계; 및 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 입력한

보안 문자와 상기 보안 식별자를 비교하는 단계를 더 포함할 수 있다.

[173] 다양한 실시 예에 따르면, 상기 비교 결과 상기 보안 문자와 상기 보안 식별자가 동일할 경우, 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 식별자에 대응하는 상기 전자 문서 서식을 확인하는 단계; 및 상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 확인한 전자 문서 서식에 상기 전자 문서 정보를 병합하는 단계를 더 포함할 수 있다.

[174] 본 발명의 일 실시예에 따른 복수의 노드들을 포함하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 시스템은 상기 복수의 노드들은 전자 문서 관리 및 유통 모듈, 전자 문서 분할 모듈, 블록 생성 모듈 및 메모리를 포함하고, 상기 복수의 노드들 중 어느 하나의 노드가, 상기 전자 문서 분할 모듈을 이용하여, 상기 전자 문서를 전자 문서 서식 및 병합 조건을 포함하는 제1 분할 데이터 및 식별자와 전자 문서 정보를 포함하는 제2 분할 데이터로 분할하고, 상기 어느 하나의 노드가 상기 제1 분할 데이터를 상기 복수의 노드들에 분산 저장하고, 상기 어느 하나의 노드가, 상기 블록 생성 모듈을 이용하여, 상기 제2 분할 데이터를 포함하는 블록을 생성하여 상기 복수의 노드들에 분산 저장하고, 상기 복수의 노드들 중 어느 하나의 노드가, 상기 전자 문서 관리 및 유통 모듈을 이용하여, 상기 병합 조건 및 상기 식별자에 기반하여, 상기 제1 분할 데이터와 상기 제2 분할 데이터를 병합할 수 있다.

[175] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이 아닌 것으로 이해해야만 한다.

청구범위

[청구항 1] 블록체인에 포함된 복수의 노드들 중에서 특정 노드들간 블록을 공유 및 검증하는 방법에 있어서,
상기 복수의 노드들 중에서 적어도 하나의 제1 노드가 상기 특정 노드들의 식별 정보 및 트랜잭션 정보를 포함하는 적어도 하나의 트랜잭션을 생성하는 단계;
상기 복수의 노드들 중에서 적어도 하나의 제2 노드가 상기 식별 정보 및 상기 트랜잭션 정보에 기반하여 적어도 하나의 블록을 생성하는 단계; 및
상기 적어도 하나의 제2 노드가 상기 생성된 적어도 하나의 블록을 상기 식별 정보에 기반하여 상기 특정 노드들에게 공유하는 단계를 포함하는 것을 특징으로 하는 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법.

[청구항 2] 제1 항에 있어서, 상기 적어도 하나의 블록을 생성하는 단계는,
상기 적어도 하나의 제2 노드가 상기 적어도 하나의 트랜잭션 중에서 동일한 식별 정보를 갖는 트랜잭션들을 확인하는 단계;
상기 적어도 하나의 제2 노드가 상기 동일한 식별 정보를 갖는 트랜잭션들만 포함되는 블록을 생성하는 단계; 및
상기 적어도 하나의 제2 노드가 상기 동일한 식별 정보를 갖는 트랜잭션들만 포함되는 상기 블록을 상기 동일한 식별 정보에 대응하는 특정 노드들에게 공유하는 단계를 포함하는 것을 특징으로 하는 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법.

[청구항 3] 제1 항에 있어서, 상기 적어도 하나의 제2 노드가 상기 생성된 적어도 하나의 블록을 저장 및 관리하는 단계를 더 포함하는 것을 특징으로 하는 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법.

[청구항 4] 제1 항에 있어서, 상기 적어도 하나의 블록을 생성하는 단계는,
상기 적어도 하나의 블록의 생성이 완료된 이후, 상기 적어도 하나의 제2 노드가 상기 생성한 적어도 하나의 블록의 헤더를 추출하는 단계; 및
상기 적어도 하나의 제2 노드가 상기 추출한 블록의 헤더만 포함되는 적어도 하나의 서브 블록을 생성하는 단계를 포함하는 것을 특징으로 하는 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법.

[청구항 5] 제4 항에 있어서, 상기 특정 노드들에게 공유하는 단계는, 상기 적어도 하나의 제2 노드가 상기 생성한 적어도 하나의 서브 블록을 상기 복수의 노드들 중 상기 특정 노드들을 제외한 나머지 노드들에게 공유하는 단계를 더 포함하는 것을 특징으로 하는 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법.

[청구항 6] 제5 항에 있어서, 상기 적어도 하나의 서브 블록은 블록 해시 값을 포함하고,

상기 나머지 노드들이 상기 블록 해시 값을 이용하여 상기 적어도 하나의 서브 블록의 무결성을 검증하는 단계를 더 포함하는 것을 특징으로 하는 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법.

[청구항 7] 제4 항에 있어서, 상기 복수의 노드들이 상기 적어도 하나의 블록과 상기 적어도 하나의 서브 블록을 동일한 블록으로 저장 및 관리하는 단계를 더 포함하는 것을 특징으로 하는 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 방법.

[청구항 8] 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 시스템에 있어서,
블록체인 네트워크를 구성하는 복수의 노드들을 포함하고,
상기 복수의 노드들 중에서 적어도 하나의 제1 노드가 상기 특정 노드들의 식별 정보 및 트랜잭션 정보를 포함하는 적어도 하나의 트랜잭션을 생성하고,
상기 복수의 노드들 중에서 적어도 하나의 제2 노드가 상기 식별 정보 및 상기 트랜잭션 정보에 기반하여 적어도 하나의 블록을 생성하고,
상기 적어도 하나의 제2 노드가 상기 생성된 적어도 하나의 블록을 상기 식별 정보에 기반하여 상기 특정 노드들에게 공유하는 것을 특징으로 하는 블록체인에서 특정 노드들간 블록을 공유 및 검증하는 시스템.

[청구항 9] 복수의 노드들을 포함하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법에 있어서,
상기 전자 문서를 전자 문서 서식 및 병합 조건을 포함하는 제1 분할 데이터 및 식별자와 전자 문서 정보를 포함하는 제2 분할 데이터로 분할하는 단계;
상기 제1 분할 데이터를 상기 복수의 노드들에 분산 저장하는 단계;
상기 제2 분할 데이터를 포함하는 블록을 생성하여 상기 복수의 노드들에 분산 저장하는 단계; 및
상기 복수의 노드들 중 어느 하나의 노드가, 상기 병합 조건 및 상기 식별자에 기반하여, 상기 제1 분할 데이터와 상기 제2 분할 데이터를 병합하는 단계를 포함하는 것을 특징으로 하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법.

[청구항 10] 제9 항에 있어서,
상기 복수의 노드들은 상기 제1 분할 데이터를 분산화된 응용프로그램 형태로 관리하는 단계를 더 포함하는 것을 특징으로 하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법.

[청구항 11] 제10 항에 있어서,
상기 복수의 노드들은 전자 문서 관리 및 유통 모듈을 포함하는 것을 특징으로 하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법.

[청구항 12] 제11 항에 있어서,

상기 병합하는 단계는,
상기 복수의 노드들 중 어느 하나의 노드에서 전자 문서 이용 요청을 검출하는 단계;
상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 제1 분할 데이터에서 상기 전자 문서 서식 및 상기 병합 조건을 추출하는 단계;
상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 제2 분할 데이터에서 상기 식별자와 상기 전자 문서 정보를 추출하는 단계;
상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 식별자에 대응하는 상기 전자 문서 서식을 확인하는 단계; 및
상기 전자 문서 관리 및 유통 모듈을 이용하여 상기 확인한 전자 문서 서식에 상기 전자 문서 정보를 병합하는 단계를 포함하는 것을 특징으로 하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법.

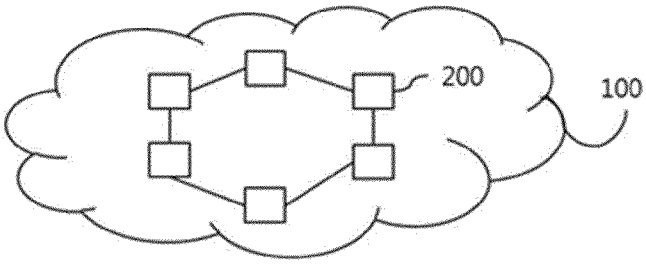
[청구항 13] 제9 항에 있어서,
상기 병합 결과 생성된 전자 문서를 제공하는 단계를 더 포함하는 것을 특징으로 하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법.

[청구항 14] 제11 항에 있어서,
상기 전자 문서에 개인 정보가 포함될 경우, 상기 제2 분할 데이터를 포함하는 블록에 보안 식별자를 추가하는 단계를 더 포함하는 것을 특징으로 하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법.

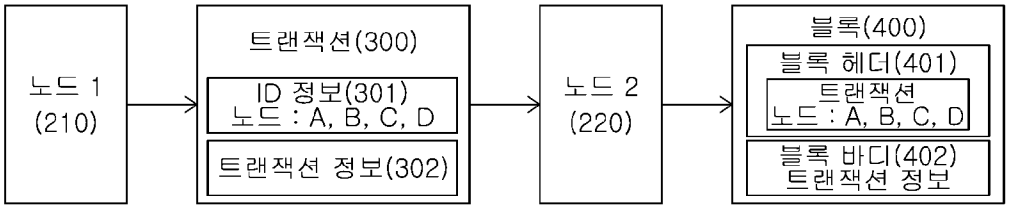
[청구항 15] 복수의 노드들을 포함하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 시스템에 있어서,
상기 복수의 노드들은 전자 문서 관리 및 유통 모듈, 전자 문서 분할 모듈, 블록 생성 모듈 및 메모리를 포함하고,
상기 복수의 노드들 중 어느 하나의 노드가, 상기 전자 문서 분할 모듈을 이용하여, 상기 전자 문서를 전자 문서 서식 및 병합 조건을 포함하는 제1 분할 데이터 및 식별자와 전자 문서 정보를 포함하는 제2 분할 데이터로 분할하고,
상기 어느 하나의 노드가 상기 제1 분할 데이터를 상기 복수의 노드들에 분산 저장하고,
상기 어느 하나의 노드가, 상기 블록 생성 모듈을 이용하여, 상기 제2 분할 데이터를 포함하는 블록을 생성하여 상기 복수의 노드들에 분산 저장하고,
상기 복수의 노드들 중 어느 하나의 노드가, 상기 전자 문서 관리 및 유통 모듈을 이용하여, 상기 병합 조건 및 상기 식별자에 기반하여, 상기 제1 분할 데이터와 상기 제2 분할 데이터를 병합하는 것을 특징으로 하는

블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 시스템.

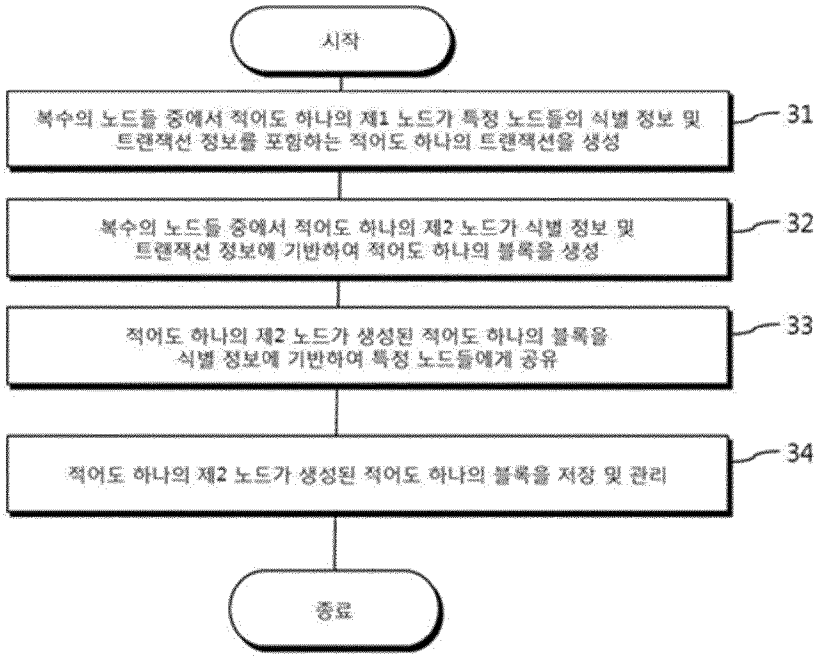
[도1]


200
100

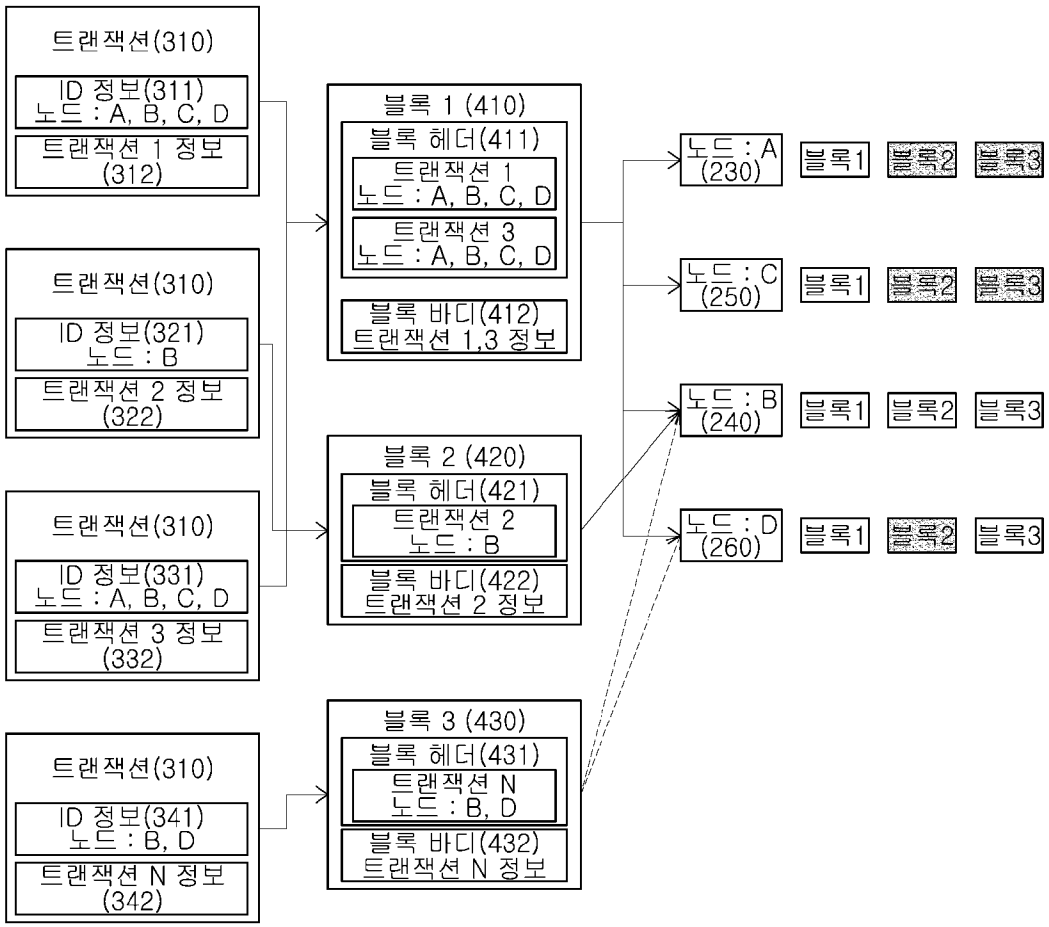
[도2]


노드 1
(210)
트랜잭션(300)
ID 정보(301)
노드 : A, B, C, D
트랜잭션 정보(302)
노드 2
(220)
블록(400)
블록 헤더(401)
트랜잭션
노드 : A, B, C, D
블록 바디(402)
트랜잭션 정보

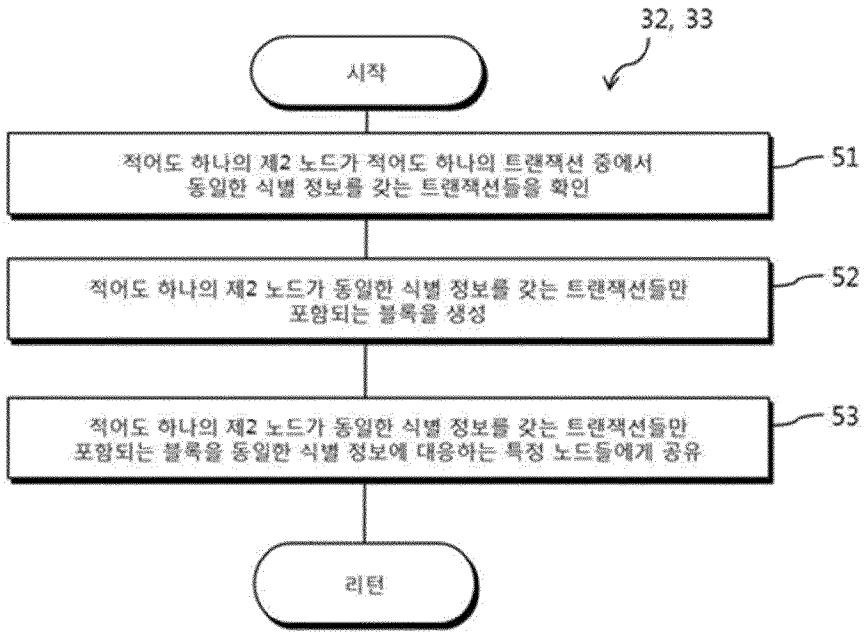
[도3]


시작
복수의 노드들 중에서 적어도 하나의 제1 노드가 특정 노드들의 식별 정보 및 트랜잭션 정보를 포함하는 적어도 하나의 트랜잭션을 생성
31
복수의 노드들 중에서 적어도 하나의 제2 노드가 식별 정보 및 트랜잭션 정보에 기반하여 적어도 하나의 블록을 생성
32
적어도 하나의 제2 노드가 생성된 적어도 하나의 블록을 식별 정보에 기반하여 특정 노드들에게 공유
33
적어도 하나의 제2 노드가 생성된 적어도 하나의 블록을 저장 및 관리
34
종료

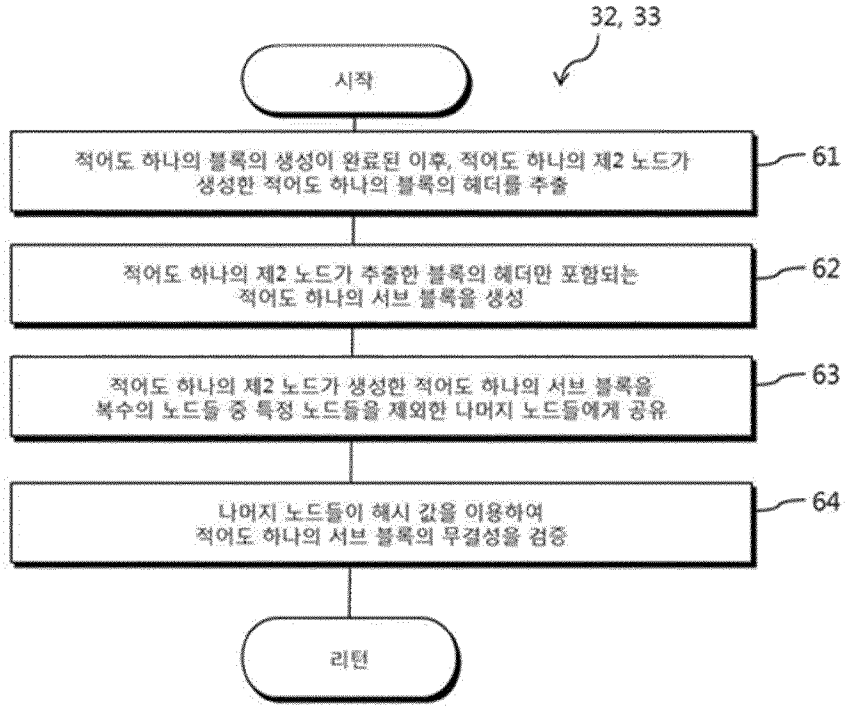
[도4]


트랜잭션(310)
ID 정보(311)
노드 : A, B, C, D
트랜잭션 1 정보
(312)
트랜잭션(310)
ID 정보(321)
노드 : B
트랜잭션 2 정보
(322)
트랜잭션(310)
ID 정보(331)
노드 : A, B, C, D
트랜잭션 3 정보
(332)
트랜잭션(310)
ID 정보(341)
노드 : B, D
트랜잭션 N 정보
(342)
블록 1 (410)
블록 헤더(411)
트랜잭션 1
노드 : A, B, C, D
트랜잭션 3
노드 : A, B, C, D
블록 바디(412)
트랜잭션 1,3 정보
블록 2 (420)
블록 헤더(421)
트랜잭션 2
노드 : B
블록 바디(422)
트랜잭션 2 정보
블록 3 (430)
블록 헤더(431)
트랜잭션 N
노드 : B, D
블록 바디(432)
트랜잭션 N 정보
노드 : A (230)
노드 : C (250)
노드 : B (240)
노드 : D (260)
블록1
블록2
블록3

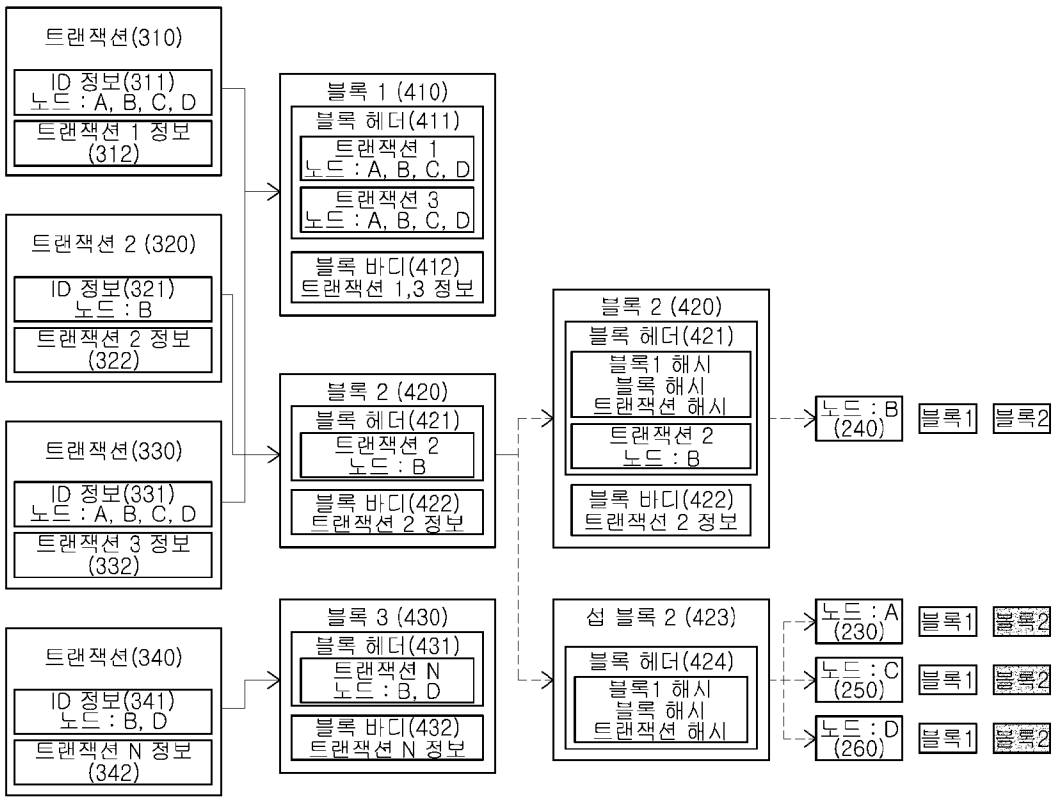
[도5]


32, 33
시작
적어도 하나의 제2 노드가 적어도 하나의 트랜잭션 중에서
동일한 식별 정보를 갖는 트랜잭션들을 확인
51
적어도 하나의 제2 노드가 동일한 식별 정보를 갖는 트랜잭션들만
포함되는 블록을 생성
52
적어도 하나의 제2 노드가 동일한 식별 정보를 갖는 트랜잭션들만
포함되는 블록을 동일한 식별 정보에 대응하는 특정 노드들에게 공유
53
리턴

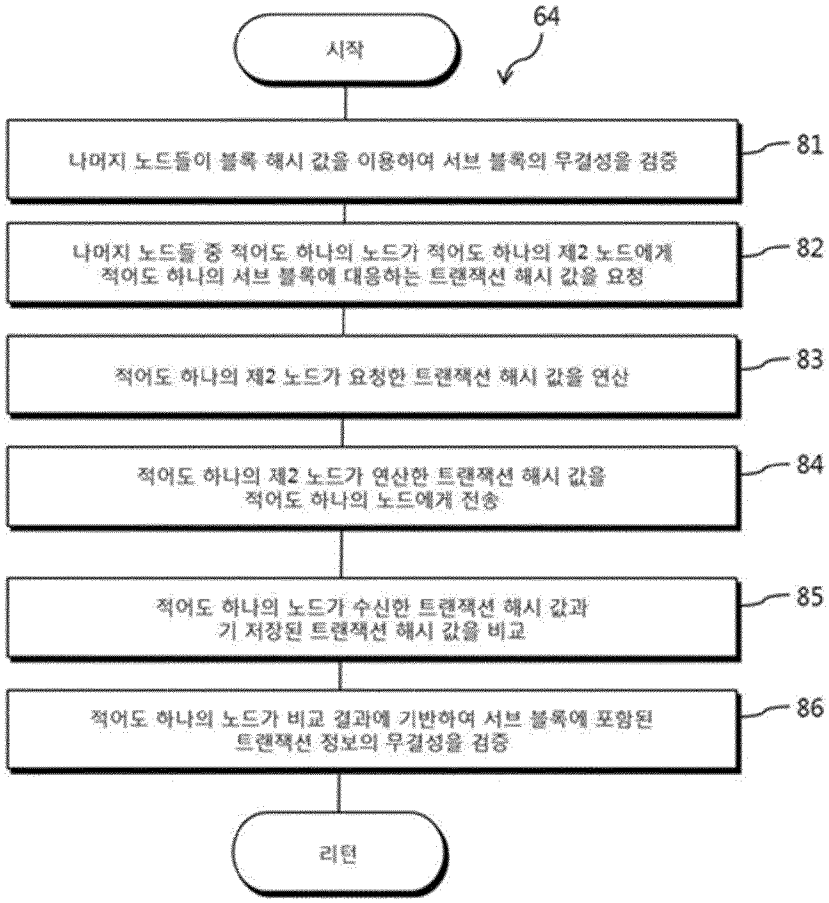
[도6]


32, 33
시작
적어도 하나의 블록의 생성이 완료된 이후, 적어도 하나의 제2 노드가 생성한 적어도 하나의 블록의 헤더를 추출
61
적어도 하나의 제2 노드가 추출한 블록의 헤더만 포함되는 적어도 하나의 서브 블록을 생성
62
적어도 하나의 제2 노드가 생성한 적어도 하나의 서브 블록을 복수의 노드들 중 특정 노드들을 제외한 나머지 노드들에게 공유
63
나머지 노드들이 해시 값을 이용하여 적어도 하나의 서브 블록의 무결성을 검증
64
리턴

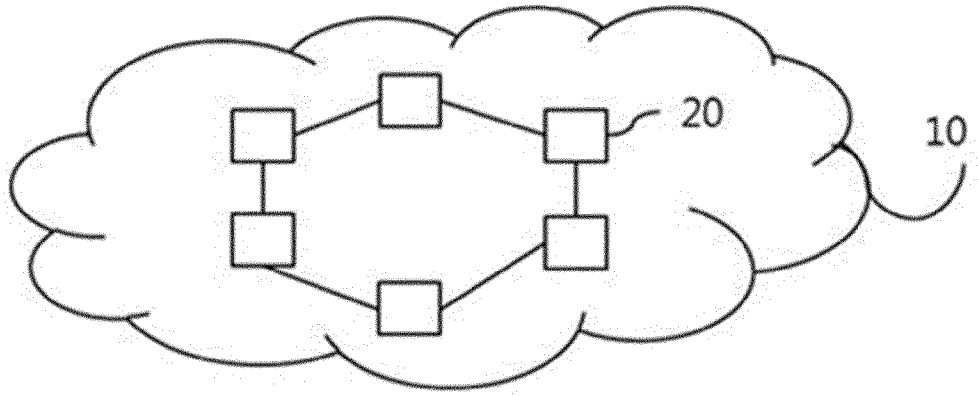
[도7]


트랜잭션(310)
ID 정보(311) 노드 : A, B, C, D
트랜잭션 1 정보 (312)
트랜잭션 2 (320)
ID 정보(321) 노드 : B
트랜잭션 2 정보 (322)
트랜잭션(330)
ID 정보(331) 노드 : A, B, C, D
트랜잭션 3 정보 (332)
트랜잭션(340)
ID 정보(341) 노드 : B, D
트랜잭션 N 정보 (342)
블록 1 (410)
블록 헤더(411)
트랜잭션 1 노드 : A, B, C, D
트랜잭션 3 노드 : A, B, C, D
블록 바디(412) 트랜잭션 1,3 정보
블록 2 (420)
블록 헤더(421)
트랜잭션 2 노드 : B
블록 바디(422) 트랜잭션 2 정보
블록 3 (430)
블록 헤더(431)
트랜잭션 N 노드 : B, D
블록 바디(432) 트랜잭션 N 정보
블록 2 (420)
블록 헤더(421)
블록1 해시 블록 해시 트랜잭션 해시
트랜잭션 2 노드 : B
블록 바디(422) 트랜잭션 2 정보
섭 블록 2 (423)
블록 헤더(424)
블록1 해시 블록 해시 트랜잭션 해시
노드 : B (240)
블록1
블록2
노드 : A (230)
블록1
블록2
노드 : C (250)
블록1
블록2
노드 : D (260)
블록1
블록2

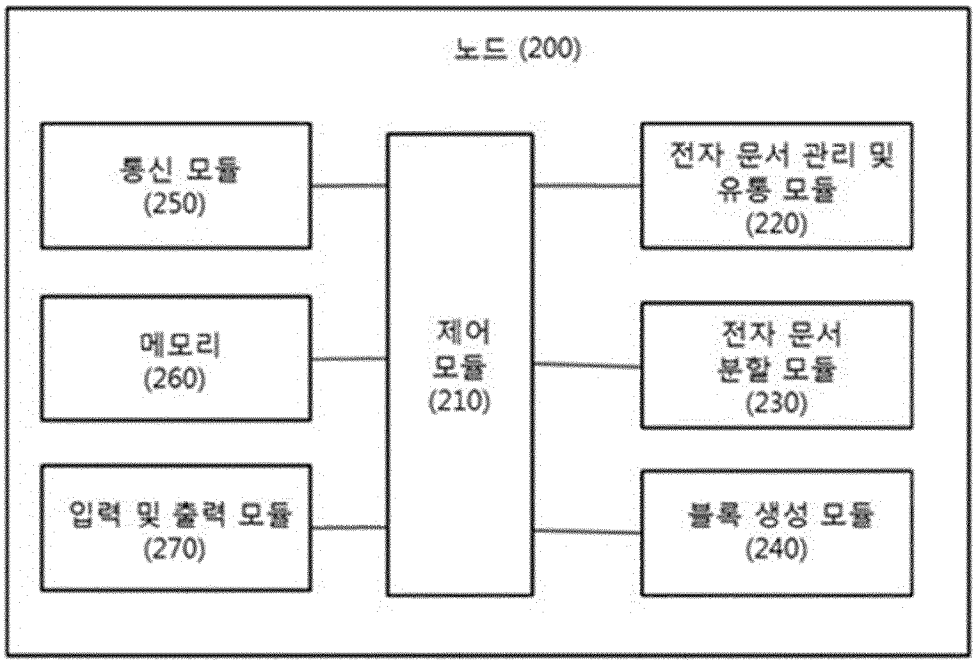
[도8]


64
시작
나머지 노드들이 블록 해시 값을 이용하여 서브 블록의 무결성을 검증
81
나머지 노드들 중 적어도 하나의 노드가 적어도 하나의 제2 노드에게
적어도 하나의 서브 블록에 대응하는 트랜잭션 해시 값을 요청
82
적어도 하나의 제2 노드가 요청한 트랜잭션 해시 값을 연산
83
적어도 하나의 제2 노드가 연산한 트랜잭션 해시 값을
적어도 하나의 노드에게 전송
84
적어도 하나의 노드가 수신한 트랜잭션 해시 값과
기 저장된 트랜잭션 해시 값을 비교
85
적어도 하나의 노드가 비교 결과에 기반하여 서브 블록에 포함된
트랜잭션 정보의 무결성을 검증
86
리턴

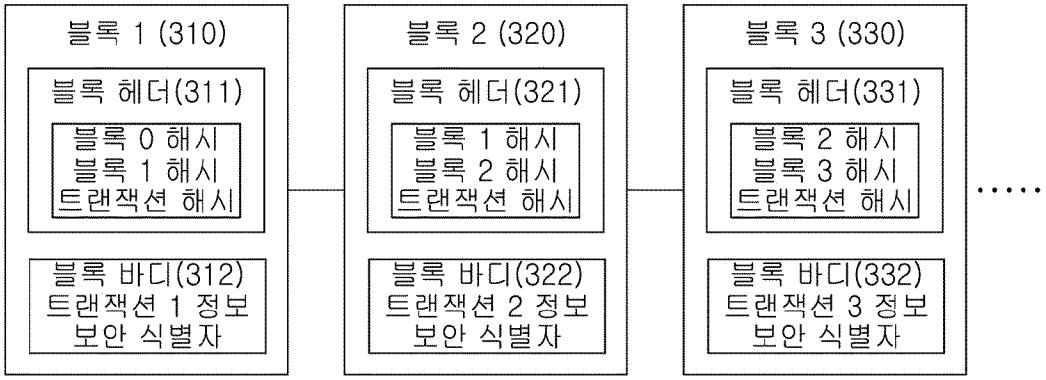
[도9]


20
10

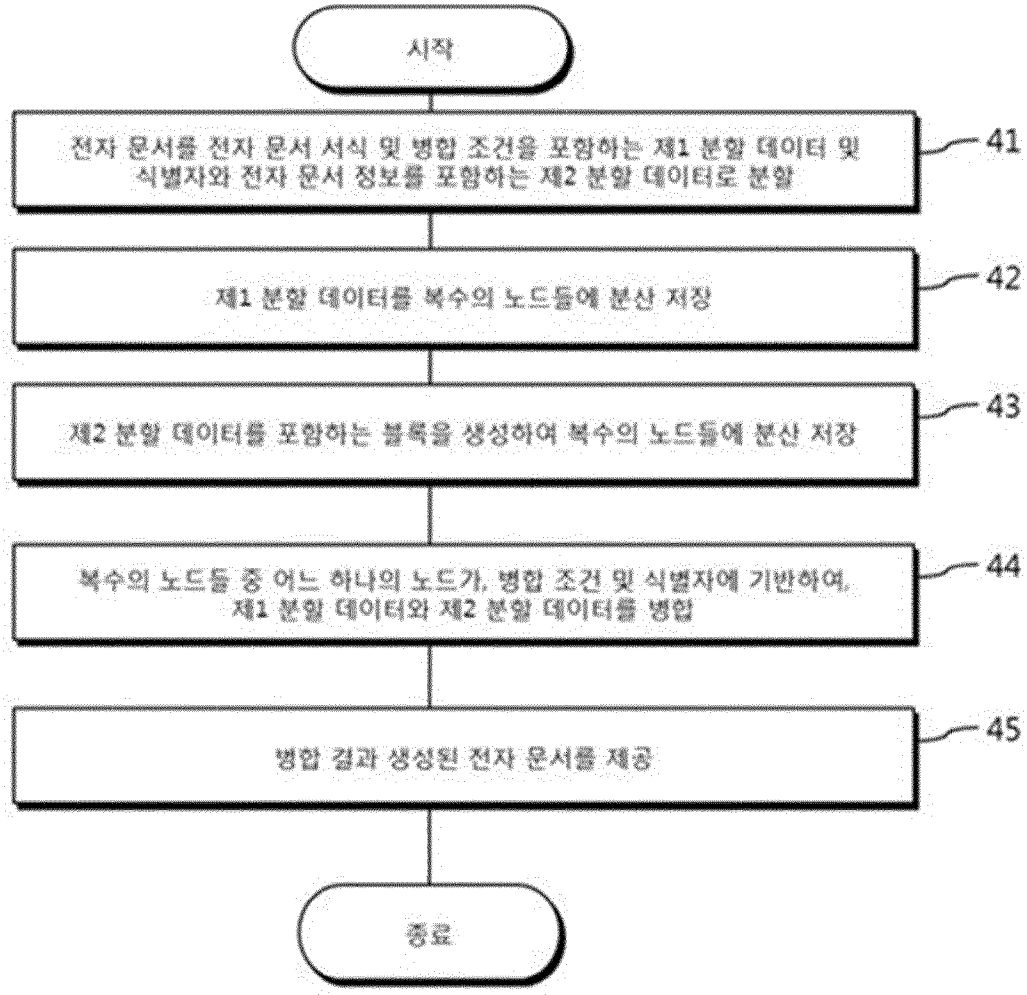
[도10]


노드 (200)
통신 모듈 (250)
메모리 (260)
입력 및 출력 모듈 (270)
제어 모듈 (210)
전자 문서 관리 및 유통 모듈 (220)
전자 문서 분할 모듈 (230)
블록 생성 모듈 (240)

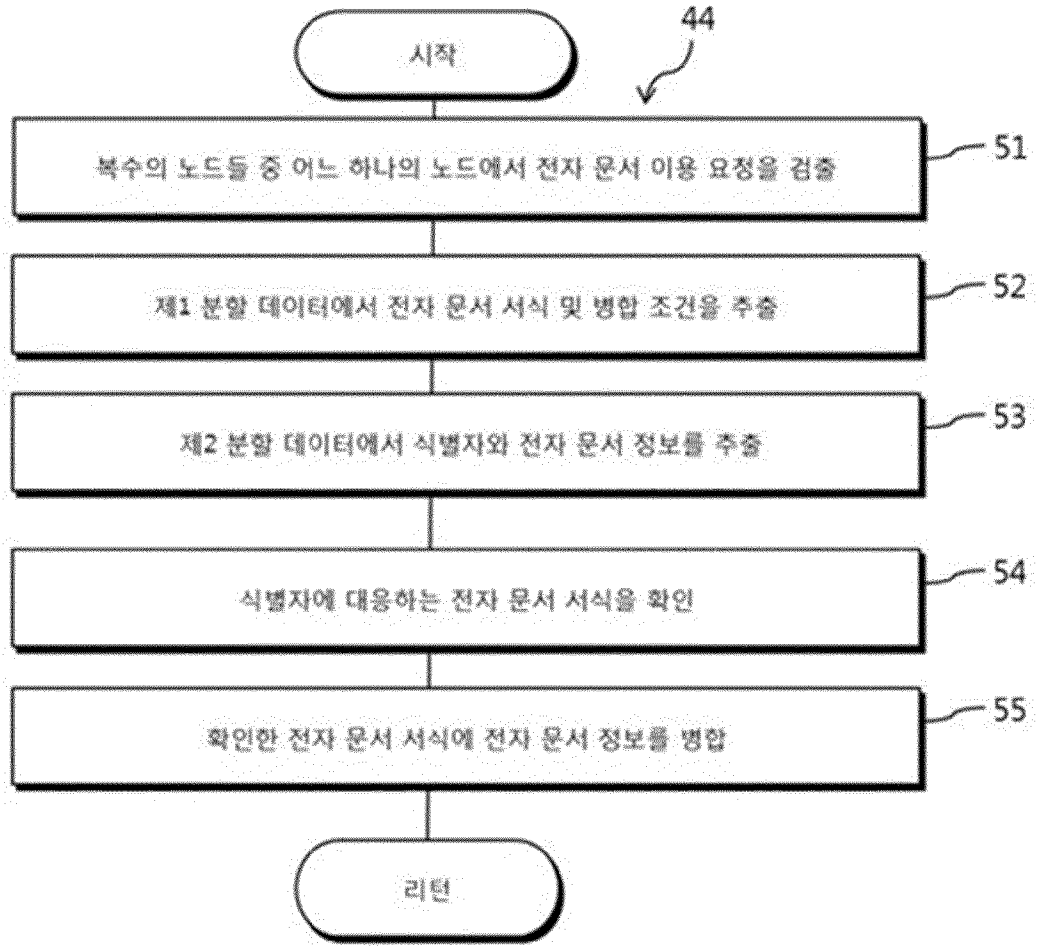
[도11]


블록 1 (310)
블록 헤더(311)
블록 0 해시
블록 1 해시
트랜잭션 해시
블록 바디(312)
트랜잭션 1 정보
보안 식별자
블록 2 (320)
블록 헤더(321)
블록 1 해시
블록 2 해시
트랜잭션 해시
블록 바디(322)
트랜잭션 2 정보
보안 식별자
블록 3 (330)
블록 헤더(331)
블록 2 해시
블록 3 해시
트랜잭션 해시
블록 바디(332)
트랜잭션 3 정보
보안 식별자
.....

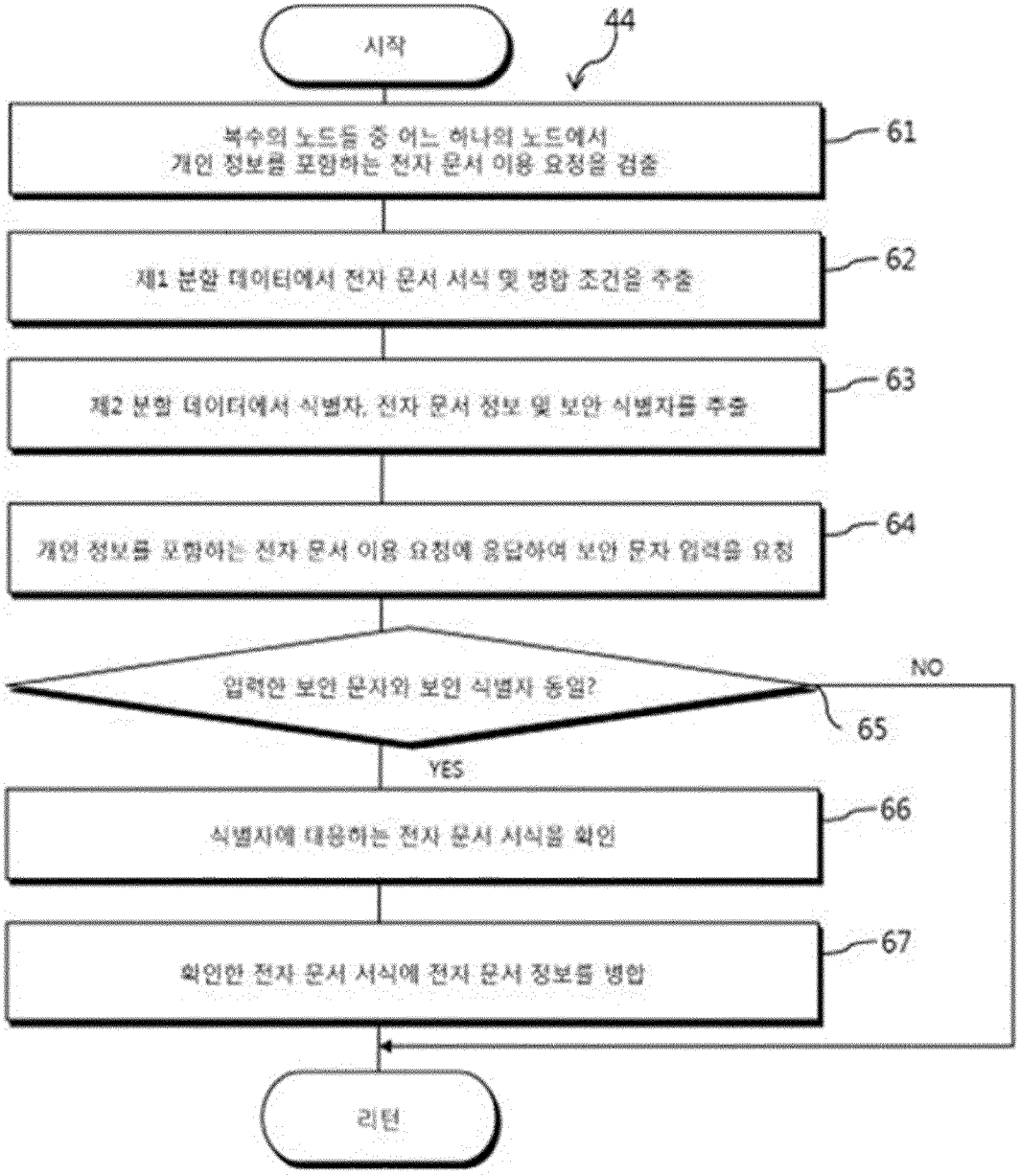
[도12]


시작
전자 문서를 전자 문서 서식 및 병합 조건을 포함하는 제1 분할 데이터 및 식별자와 전자 문서 정보를 포함하는 제2 분할 데이터로 분할
41
제1 분할 데이터를 복수의 노드들에 분산 저장
42
제2 분할 데이터를 포함하는 블록을 생성하여 복수의 노드들에 분산 저장
43
복수의 노드들 중 어느 하나의 노드가, 병합 조건 및 식별자에 기반하여, 제1 분할 데이터와 제2 분할 데이터를 병합
44
병합 결과 생성된 전자 문서를 제공
45
종료

[도13]


44
시작
복수의 노드들 중 어느 하나의 노드에서 전자 문서 이용 요청을 검출
51
제1 분할 데이터에서 전자 문서 서식 및 병합 조건을 추출
52
제2 분할 데이터에서 식별자와 전자 문서 정보를 추출
53
식별자에 대응하는 전자 문서 서식을 확인
54
확인한 전자 문서 서식에 전자 문서 정보를 병합
55
리턴

[도14]


시작
44
복수의 노드들 중 어느 하나의 노드에서
개인 정보를 포함하는 전자 문서 이용 요청을 검출
61
제1 분할 데이터에서 전자 문서 서식 및 병합 조건을 추출
62
제2 분할 데이터에서 식별자, 전자 문서 정보 및 보안 식별자를 추출
63
개인 정보를 포함하는 전자 문서 이용 요청에 응답하여 보안 문자 입력을 요청
64
입력한 보안 문자와 보안 식별자 동일?
NO
65
YES
식별자에 대응하는 전자 문서 서식을 확인
66
확인한 전자 문서 서식에 전자 문서 정보를 병합
67
리턴

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2019/014749

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08(2006.01)i, H04L 29/06(2006.01)i, G06F 21/60(2013.01)i, G06Q 10/10(2012.01)i, G06F 21/62(2013.01)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 20/06; G06Q 20/22; G06Q 20/36; G06Q 20/38; G06Q 40/02; H04L 29/06; G06F 21/60; G06Q 10/10; G06F 21/62; H04L 9/06

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, node, block

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-1701131 B1 (RAPI INC.) 13 February 2017 See paragraphs [0036], [0053], [0067]-[0068]; and figure 9.	1-8
Y	KR 10-2018-0124545 A (XBLOCKSYSTEMS CO., LTD.) 21 November 2018 See paragraphs [0058], [0072], [0075]; and figures 3, 5.	1-8
Y	CN 108200203 A (BEIJING QIHCO TECHNOLOGY COMPANY LIMITED) 22 June 2018 See paragraph [0026]; and figure 1.	4-7
Y	KR 10-1878869 B1 (METAPS PLUS INC.) 16 August 2018 See pages 10-11, 14; claim 2; and figure 12.	9-11,13-15
A		12
Y	KR 10-2015-0046941 A (NONG HYUP BANK) 04 May 2015 See paragraphs [0012], [0031], [0034]; and figure 1.	9-11,13-15
A	KR 10-2014-0049755 A (NONG HYUP BANK) 28 April 2014 See paragraphs [0030]-[0060]; and figure 1.	1-15

☐ 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
13 FEBRUARY 2020 (13.02.2020)	**13 FEBRUARY 2020 (13.02.2020)**

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2019/014749

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The invention of group 1: claims 1-8 pertain to a method for sharing and verifying a block among specific nodes in a plurality of nodes included in a blockchain,
The invention of group 2: claims 9-15 pertain to a method for distributing an electronic document by using a smart contract in a blockchain including a plurality of nodes.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2019/014749

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-1701131 B1	13/02/2017	None	
KR 10-2018-0124545 A	21/11/2018	KR 10-2017739 B1	03/09/2019
		KR 10-2019-0020721 A	04/03/2019
		SG 10201803839 A	28/12/2018
		TW 201901482 A	01/01/2019
		WO 2018-207975 A1	15/11/2018
CN108200203 A	22/06/2018	None	
KR 10-1878869 B1	16/08/2018	JP 2019-096272 A	20/06/2019
		JP 6532930 B1	31/05/2019
		KR 10-1878870 B1	16/08/2018
		KR 10-1962285 B1	26/03/2019
KR 10-2015-0046941 A	04/05/2015	None	
KR 10-2014-0049755 A	28/04/2014	KR 10-1456911 B1	31/10/2014

국 제 조 사 보 고 서

국제출원번호
PCT/KR2019/014749

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 29/08(2006.01)i, H04L 29/06(2006.01)i, G06F 21/60(2013.01)i, G06Q 10/10(2012.01)i, G06F 21/62(2013.01)i, H04L 9/06(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)
H04L 29/08; G06Q 20/06; G06Q 20/22; G06Q 20/36; G06Q 20/38; G06Q 40/02; H04L 29/06; G06F 21/60; G06Q 10/10; G06F 21/62; H04L 9/06

조사된 기술분야에 속하는 최소문헌 이외의 문헌
한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))
eKOMPASS(특허청 내부 검색시스템) & 키워드: 블록체인(blockchain), 노드(node), 블록(block)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-1701131 B1 (주식회사 라피) 2017.02.13 단락 [0036], [0053], [0067]-[0068]; 및 도면 9	1-8
Y	KR 10-2018-0124545 A (주식회사 엑스블록시스템즈) 2018.11.21 단락 [0058], [0072], [0075]; 및 도면 3, 5	1-8
Y	CN 108200203 A (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) 2018.06.22 단락 [0026]; 및 도면 1	4-7
Y	KR 10-1878869 B1 (주식회사 미텝스플러스) 2018.08.16 페이지 10-11, 14; 청구항 2; 및 도면 12	9-11,13-15
A		12
Y	KR 10-2015-0046941 A (농협은행(주)) 2015.05.04 단락 [0012], [0031], [0034]; 및 도면 1	9-11,13-15
A	KR 10-2014-0049755 A (농협은행(주)) 2014.04.28 단락 [0030]-[0060]; 및 도면 1	1-15

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"D" 본 국제출원에서 출원인이 인용한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2020년 02월 13일 (13.02.2020)	2020년 02월 13일 (13.02.2020)

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

심사관
김성희
전화번호 +82-42-481-3516

국 제 조 사 보 고 서

국제출원번호
PCT/KR2019/014749

제2기재란 일부 청구항을 조사할 수 없는 경우의 의견(첫 번째 용지의 2의 계속)

PCT 제17조(2)(a)의 규정에 따라 다음과 같은 이유로 일부 청구항에 대하여 본 국제조사보고서가 작성되지 아니하였습니다.

1. ☐ 청구항:
이 청구항은 본 기관이 조사할 필요가 없는 대상에 관련됩니다. 즉,

2. ☐ 청구항:
이 청구항은 유효한 국제조사를 수행할 수 없을 정도로 소정의 요건을 충족하지 아니하는 국제출원의 부분과 관련됩니다. 구체적으로는,

3. ☐ 청구항:
이 청구항은 종속청구항이나 PCT규칙 6.4(a)의 두 번째 및 세 번째 문장의 규정에 따라 작성되어 있지 않습니다.

제3기재란 발명의 단일성이 결여된 경우의 의견(첫 번째 용지의 3의 계속)

본 국제조사기관은 본 국제출원에 다음과 같이 다수의 발명이 있다고 봅니다.

제1군 발명: 청구항 1-8은 블록체인에 포함된 복수의 노드들 중에서 특정 노드들간 블록을 공유 및 검증하는 방법에 관한 것이고,
제2군 발명: 청구항 9-15는 복수의 노드들을 포함하는 블록체인에서 스마트 컨트랙트를 이용한 전자 문서를 유통하는 방법에 관한 것입니다.

1. ☐ 출원인이 모든 추가수수료를 기간 내에 납부하였으므로, 본 국제조사보고서는 모든 조사 가능한 청구항을 대상으로 합니다.

2. ☒ 추가수수료 납부를 요구하지 않고도 모든 조사 가능한 청구항을 조사할 수 있었으므로, 본 기관은 추가수수료 납부를 요구하지 아니하였습니다.

3. ☐ 출원인이 추가수수료의 일부만을 기간 내에 납부하였으므로, 본 국제조사보고서는 수수료가 납부된 청구항만을 대상으로 합니다. 구체적인 청구항은 아래와 같습니다.

4. ☐ 출원인이 기간 내에 추가수수료를 납부하지 아니하였습니다. 따라서 본 국제조사보고서는 청구범위에 처음 기재된 발명에 한정되어 있으며, 해당 청구항은 아래와 같습니다.

이의신청에 관한 기재

☐ 출원인의 이의신청 및 이의신청료 납부(해당하는 경우)와 함께 추가수수료가 납부되었습니다.

☐ 출원인의 이의신청과 함께 추가수수료가 납부되었으나 이의신청료가 보정요구서에 명시된 기간 내에 납부되지 아니하였습니다.

☐ 이의신청 없이 추가수수료가 납부되었습니다.

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2019/014749

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1701131 B1	2017/02/13	없음	
KR 10-2018-0124545 A	2018/11/21	KR 10-2017739 B1	2019/09/03
		KR 10-2019-0020721 A	2019/03/04
		SG 10201803839 A	2018/12/28
		TW 201901482 A	2019/01/01
		WO 2018-207975 A1	2018/11/15
CN108200203 A	2018/06/22	없음	
KR 10-1878869 B1	2018/08/16	JP 2019-096272 A	2019/06/20
		JP 6532930 B1	2019/05/31
		KR 10-1878870 B1	2018/08/16
		KR 10-1962285 B1	2019/03/26
KR 10-2015-0046941 A	2015/05/04	없음	
KR 10-2014-0049755 A	2014/04/28	KR 10-1456911 B1	2014/10/31