



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0115476
(43) 공개일자 2024년07월26일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2022.01)

(52) CPC특허분류
H04L 9/50 (2022.05)
H04L 2209/08 (2013.01)

(21) 출원번호 10-2023-0007845

(22) 출원일자 2023년01월19일

심사청구일자 2023년01월19일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

주식회사 소테리아

서울특별시 강남구 테헤란로33길 5, 8층(역삼동, 제이엘케이타워)

(72) 발명자

전기석

인천광역시 서구 솔빛로 13, 546동 1503호

이중희

서울특별시 성북구 길음로9길 50, 907동 202호

(뒷면에 계속)

(74) 대리인

김준석, 박민욱

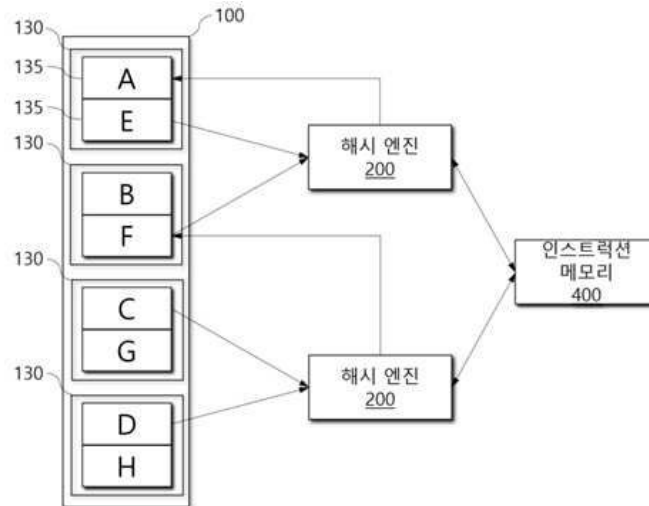
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 재사용 가능한 머클트리를 포함하는 블록체인 마이닝 방법 및 시스템

(57) 요약

본 발명의 블록체인 마이닝 방법은 머클트리를 활용하는 블록체인 마이닝 방법에 관한 것으로, 인스트럭션을 생성하는 단계, 인스트럭션에 따라 해시엔진을 통해 계산된 해시값을 뱅크 메모리에 오버라이트하며 머클루트를 산출하는 단계 및 코인베이스를 변경하고, 뱅크 메모리에 오버라이트된 해시값을 해시 연산에 재사용하여 머클루트를 재산출하는 단계를 포함할 수 있다.

대표도 - 도4



(72) 발명자

김범수

서울특별시 관악구 호암로24길 6, 205호

김 제임스 제이

서울특별시 관악구 호암로24길 6, 205호

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152771
과제번호	2021-0-00532-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	데이터경제를위한블록체인기술개발
연구과제명	고성능/대용량 트랜잭션 확장성 보장 기술개발
기 여 율	40/100
과제수행기관명	고려대학교산학협력단
연구기간	2023.01.01 ~ 2023.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152852
과제번호	2021-0-00528-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(정진기금)
연구과제명	하드웨어 중심 신뢰계산기반과 분산 데이터보호박스를 위한 표준 프로토콜 개발
기 여 율	40/100
과제수행기관명	고려대학교산학협력단
연구기간	2023.01.01 ~ 2023.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152985
과제번호	2021-0-00518-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	데이터경제를위한블록체인기술개발
연구과제명	블록체인 데이터 암호화 기반의 프라이버시 보호 기술개발
기 여 율	20/100
과제수행기관명	한양대학교산학협력단
연구기간	2023.01.01 ~ 2023.12.31

명세서

청구범위

청구항 1

머클트리를 활용하는 블록체인 마이닝 방법에 관한 것으로,

인스트럭션을 생성하는 단계;

상기 인스트럭션에 따라 해시엔진을 통해 계산된 해시값을 뱅크 메모리에 오버라이트하며 머클루트를 산출하는 단계; 및

코인베이스를 변경하고, 상기 뱅크 메모리에 오버라이트된 해시값을 해시 연산에 재사용하여 머클루트를 재산출하는 단계; 를 포함하는 블록체인 마이닝 방법.

청구항 2

제1항에 있어서,

상기 인스트럭션을 생성하는 단계는,

상기 뱅크 메모리내에 저장된 데이터의 라이프타임을 분석하는 단계;

분석된 라이프타임에 기초하여 라이프타임을 새로 설정하는 단계; 및

설정된 라이프타임에 기초하여 데이터 저장 위치를 설정하는 단계; 를 포함하는 블록체인 마이닝 방법.

청구항 3

제2항에 있어서,

상기 라이프타임을 분석하는 단계는,

머클루트의 재산출을 위해 필요하다고 판단되는 데이터를 식별하는 것을 특징으로 하는 블록체인 마이닝 방법.

청구항 4

제3항에 있어서,

상기 라이프타임을 새로 설정하는 단계는,

상기 머클루트의 재산출을 위해 필요하다고 판단되는 데이터의 라이프타임을 머클루트 산출이 종료될 때까지로 설정하는 것을 특징으로 하는 블록체인 마이닝 방법.

청구항 5

제4항에 있어서,

상기 데이터 저장 위치를 설정하는 단계는,

라이프타임이 머클루트 산출이 종료될 때까지로 설정된 데이터는 오버라이트되지 않도록 저장 위치를 설정하는 것을 특징으로 하는 블록체인 마이닝 방법.

청구항 6

제2항에 있어서,

상기 인스트럭션을 생성하는 단계는,

뱅크를 해시엔진에 할당하는 단계를 더 포함하여,

상기 해시엔진은, 미리 할당된 뱅크에서만 데이터를 읽어오도록 하는 것을 특징으로 하는 블록체인 마이닝 방법.

청구항 7

제6항에 있어서,

상기 뱅크를 해시엔진에 할당하는 단계는,

복수의 해시엔진에 뱅크가 중복되지 않도록, 해시엔진 하나당 한쌍의 뱅크를 할당하는 것을 특징으로 하는 블록체인 마이닝 방법.

청구항 8

제7항에 있어서,

상기 데이터 저장 위치를 설정하는 단계는,

하나의 사이클에 산출된 복수의 해시값은 하나의 해시엔진에 할당된 한쌍의 뱅크에 나뉘어 저장되도록 저장 위치를 설정하는 것을 특징으로 하는 블록체인 마이닝 방법.

청구항 9

제1항에 있어서,

상기 머클루트를 재산출하는 단계는,

코인베이스를 산출된 상기 머클루트 값으로 변경하는 것을 특징으로 하는 블록체인 마이닝 방법.

청구항 10

머클트리를 활용하는 블록체인 마이닝 시스템에 관한 것으로,

뱅크 메모리를 포함하는 데이터 메모리;

해시엔진;

인스트럭션 생성부 및

인스트럭션이 저장되는 인스트럭션 메모리; 를 포함하여,

인스트럭션을 생성하고,

상기 인스트럭션에 따라 상기 해시엔진을 통해 계산된 해시값을 상기 뱅크 메모리에 오버라이트하며 머클루트를 산출하고,

코인베이스를 변경하고, 상기 뱅크 메모리에 오버라이트된 해시값을 해시 연산에 재사용하여 머클루트를 재산출하는 블록체인 마이닝 시스템.

청구항 11

제10항에 있어서,
상기 인스트럭션 생성부는,
상기 बैं크 메모리내에 저장된 데이터의 라이프타임을 분석하는 분석부;
분석된 라이프타임에 기초하여 라이프타임을 새로 설정하는 라이프타임 설정부; 및
설정된 라이프타임에 기초하여 데이터 저장 위치를 설정하는 저장 위치 설정부; 를 더 포함하는 블록체인 마이닝 시스템.

청구항 12

제11항에 있어서,
상기 분석부는,
머클루트의 재산출을 위해 필요하다고 판단되는 데이터를 식별하는 것을 특징으로 하는 블록체인 마이닝 시스템.

청구항 13

제12항에 있어서,
상기 라이프타임 설정부는,
상기 머클루트의 재산출을 위해 필요하다고 판단되는 데이터의 라이프타임을 머클루트 산출이 종료될 때까지로 설정하는 것을 특징으로 하는 블록체인 마이닝 시스템.

청구항 14

제13항에 있어서,
상기 저장 위치 설정부는,
라이프타임이 머클루트 산출이 종료될 때까지로 설정된 데이터는 오버라이트되지 않도록 저장 위치를 설정하는 것을 특징으로 하는 블록체인 마이닝 시스템.

청구항 15

제11항에 있어서,
상기 인스트럭션 생성부는,
뱅크를 해시엔진에 할당하여,
상기 해시엔진은 미리 할당된 뱅크에서만 데이터를 읽어오도록 하는 것을 특징으로 하는 블록체인 마이닝 시스템.

청구항 16

제15항에 있어서,
상기 뱅크를 해시엔진에 할당하는 과정은,

복수의 해시엔진에 뱅크가 중복되지 않도록, 해시엔진 하나당 한쌍의 뱅크를 할당하는 것을 특징으로 하는 블록체인 마이닝 시스템.

청구항 17

제16항에 있어서,

상기 저장 위치 설정부는,

하나의 사이클에 산출된 복수의 해시값은 하나의 해시엔진에 할당된 한쌍의 뱅크에 나뉘어 저장되도록 저장 위치를 설정하는 것을 특징으로 하는 블록체인 마이닝 시스템.

청구항 18

제10항에 있어서,

코인베이스를 산출된 상기 머클루트 값으로 변경하는 것을 특징으로 하는 블록체인 마이닝 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 블록체인 마이닝 방법 및 시스템에 관한 것이다.

배경 기술

[0002] 블록체인(Blockchain) 마이닝(mining) 혹은 채굴이라 불리는 과정은 발생한 거래기록(transaction records)을 공개원장(public ledger)에 추가하는 것을 의미한다. 비트코인과 같은 개개인의 노드가 거미줄처럼 얹여있어 서로간의 감시를 통해 장부를 기록하는 탈중앙화 방식의 퍼블릭 블록체인에서, 전력유지 및 실행시간 등을 감수하며 노드를 유지하는 것은 사용자에게 큰 부담이 될 수 있다. 따라서, 노드를 유지하는 사용자에게 보상을 주는 것이 필요하다. 여기서 보상은 사용자에게 코인을 주거나, 블록을 생성할 권한을 주는 방식으로 이루어질 수 있다.

[0003] 블록체인 마이닝을 통해 사용자는 노드를 유지하며 문제를 푸는 작업을 수행하여 보상(예로, 코인 등)을 받거나 생성하는 권한을 얻을 수 있다. 문제를 푸는 작업은 무작위 문자열을 해시함수의 연산을 통해 해시값을 생성하고, 논스(nonce)값을 변경하며 조건에 맞는 해시값을 찾는 과정을 의미하며, 적절한 해시값을 찾으면 사용자는 보상을 얻을 수 있다.

[0004] 블록체인 마이닝 과정에서 머클트리(Merkle tree)가 사용될 수 있다. 머클트리는 적은 컴퓨팅 파워로 데이터의 무결성을 효율적으로 검증할 수 있는 바이너리 해시트리(Binary hash tree)로, 처음 트랜잭션(transaction) 값이 입력되면 2개의 자식노드(leaf node)가 1개의 부모 노드(non-leaf node)로 합쳐져 해시 컴퓨팅(hash computing)된다. 머클트리 구조는 한 개의 자식 노드가 변경이 되면, 모든 전체 노드(root node) 해시 결과값이 변경되어, 노드 값의 위변조를 알아낼 수 있는 트리구조이다.

[0005] 블록체인 마이닝에서 머클트리를 사용하는 경우, 적절한 논스값을 찾지 못하여 새로운 블록후보(block candidate)의 재탐색시, 후보 트랜잭션의 선택 및 검증부터 다시하는 과정을 거치며 오버헤드(overhead)가 커지게 된다. 특히, 최근 비트코인 등 블록체인의 가치가 높아짐에 따라 마이닝 작업의 난이도가 상승하는 가운데, 이러한 오버헤드의 증가는 마이닝 과정의 전력소모 및 실행시간의 증가를 불러일으켜 환경오염을 발생시키는 문제가 있다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 일 실시예에 따른 블록체인 마이닝 방법 및 시스템의 목적은, 머클트리의 일부 해시값 재사용을 통해 새로운 블록후보를 재탐색하는데 필요한 전력소모를 줄이고, 실행시간을 단축시키고자 하는데 있다.

과제의 해결 수단

[0007] 블록체인 마이닝 방법의 일 실시예는 머클트리를 활용하는 블록체인 마이닝 방법에 관한 것으로, 인스트럭션을 생성하는 단계, 인스트럭션에 따라 해시엔진을 통해 계산된 해시값을 뱅크 메모리에 오버라이트하며 머클루트를 산출하는 단계 및 코인베이스를 변경하고, 뱅크 메모리에 오버라이트된 해시값을 해시 연산에 재사용하여 머클루트를 재산출하는 단계를 포함할 수 있다.

[0008] 또한, 일 실시예에 따라서, 인스트럭션을 생성하는 단계는, 뱅크 메모리내에 저장된 데이터의 라이프타임을 분석하는 단계, 분석된 라이프타임에 기초하여 라이프타임을 새로 설정하는 단계 및 설정된 라이프타임에 기초하여 데이터 저장 위치를 설정하는 단계를 포함할 수 있다.

[0009] 또한, 일 실시예에 따라서, 라이프타임을 분석하는 단계는, 머클루트의 재산출을 위해 필요하다고 판단되는 데이터를 식별하는 것을 특징으로 할 수 있다.

[0010] 또한, 일 실시예에 따라서 라이프타임을 새로 설정하는 단계는, 머클루트의 재산출을 위해 필요하다고 판단되는 데이터의 라이프타임을 머클루트 산출이 종료될 때까지로 설정하는 것을 특징으로 할 수 있다.

[0011] 또한, 일 실시예에 따라서, 데이터 저장 위치를 설정하는 단계는, 라이프타임이 머클루트 산출이 종료될 때까지로 설정된 데이터는 오버라이트되지 않도록 저장 위치를 설정하는 것을 특징으로 할 수 있다.

[0012] 또한, 일 실시예에 따라서, 인스트럭션을 생성하는 단계는, 뱅크를 해시엔진에 할당하는 단계를 더 포함하여, 해시엔진은, 미리 할당된 뱅크에서만 데이터를 읽어오도록 하는 것을 특징으로 할 수 있다.

[0013] 또한, 일 실시예에 따라서, 뱅크를 해시엔진에 할당하는 단계는, 해시엔진에 뱅크가 중복되지 않도록, 해시엔진 하나당 한쌍의 뱅크를 할당하는 것을 특징으로 할 수 있다.

[0014] 또한, 일 실시예에 따라서, 데이터 저장 위치를 설정하는 단계는, 하나의 사이클에 산출된 복수의 해시값은 하나의 해시엔진에 할당된 한쌍의 뱅크에 나뉘어 저장되도록 저장 위치를 설정하는 것을 특징으로 할 수 있다.

[0015] 또한, 일 실시예에 따라서, 머클루트를 재산출하는 단계는, 코인베이스를 산출된 머클루트 값으로 변경하는 것을 특징으로 할 수 있다.

[0016] 블록체인 마이닝 시스템의 일 실시예는 머클트리를 활용하는 블록체인 마이닝 시스템에 관한 것으로, 뱅크 메모리를 포함하는 데이터 메모리, 해시엔진, 인스트럭션 생성부 및 인스트럭션이 저장되는 인스트럭션 메모리를 포함하여, 인스트럭션을 생성하고, 인스트럭션에 따라 해시엔진을 통해 계산된 해시값을 뱅크 메모리에 오버라이트하며 머클루트를 산출하고, 코인베이스를 변경하고, 뱅크 메모리에 오버라이트된 해시값을 해시 연산에 재사용하여 머클루트를 재산출할 수 있다.

[0017] 또한, 일 실시예에 따라서, 인스트럭션 생성부는, 뱅크 메모리내에 저장된 데이터의 라이프타임을 분석하는 분석부, 분석된 라이프타임에 기초하여 라이프타임을 새로 설정하는 라이프타임 설정부 및 설정된 라이프타임에 기초하여 데이터 저장 위치를 설정하는 저장 위치 설정부를 더 포함할 수 있다.

[0018] 또한, 일 실시예에 따라서, 분석부는, 머클루트의 재산출을 위해 필요하다고 판단되는 데이터를 식별하는 것을 특징으로 할 수 있다.

[0019] 또한, 일 실시예에 따라서, 라이프타임 설정부는, 머클루트의 재산출을 위해 필요하다고 판단되는 데이터의 라이프타임을 머클루트 산출이 종료될 때까지로 설정하는 것을 특징으로 할 수 있다.

[0020] 또한, 일 실시예에 따라서, 저장 위치 설정부는, 라이프타임이 머클루트 산출이 종료될 때까지로 설정된 데이터는 오버라이트되지 않도록 저장 위치를 설정하는 것을 특징으로 할 수 있다.

[0021] 또한, 일 실시예에 따라서, 인스트럭션 생성부는, 뱅크를 해시엔진에 할당하여, 해시엔진은, 미리 할당된 뱅크에서만 데이터를 읽어오도록 하는 것을 특징으로 할 수 있다.

[0022] 또한, 일 실시예에 따라서, 뱅크를 해시엔진에 할당하는 것은, 복수의 해시엔진에 뱅크가 중복되지 않도록, 해시엔진 하나당 한쌍의 뱅크를 할당하는 것을 특징으로 할 수 있다.

[0023] 또한, 일 실시예에 따라서, 저장 위치 설정부는, 하나의 사이클에 산출된 복수의 해시값은 하나의 해시엔진에

할당된 한쌍의 बैं크에 나뉘어 저장되도록 저장 위치를 설정하는 것을 특징으로 할 수 있다.

[0024] 또한, 일 실시예에 따라서, 코인베이스를 산출된 머클루트 값으로 변경하는 것을 특징으로 할 수 있다.

발명의 효과

[0025] 본 발명의 일 실시예에 의한 블록체인 마이닝 방법에 따르면, 중간 해시값의 재사용을 통해 기존의 방법에 비하여 일부 트랜잭션의 선택 및 검증의 생략으로, 작업 수행 시간 및 전력 소비를 줄일 수 있는 효과가 있다.

도면의 간단한 설명

[0026] 도 1은 일 실시예에 따른 일반적인 블록해시 산출 과정을 나타낸 도면이다.

도 2는 일 실시예에 따른 본 발명의 블록체인 마이닝 시스템의 블록도이다.

도 3은 일 실시예에 따른 데이터 메모리의 블록도이다.

도 4는 일 실시예에 따른 블록체인 마이닝 시스템의 블록도이다.

도 5는 일 실시예에 따라 인스트럭션을 생성하는 과정을 나타낸 순서도이다.

도 6은 일 실시예에 따른 인스트럭션 생성부의 블록도이다.

도 7은 일 실시예에 따른 블록체인 마이닝 시스템의 블록도이다.

도 8은 일 실시예에 따라 머클루트를 산출하는 과정을 나타낸 도면이다.

도 9는 일 실시예에 따라 बैं크 메모리에 저장된 데이터의 변화를 사이클 별로 나타낸 도면이다.

도 10은 일 실시예에 따라 머클루트 재산출을 결정하는 과정을 나타낸 순서도이다.

도 11은 일 실시예에 따라 머클루트를 재산출하는 과정을 나타낸 도면이다.

도 12는 일 실시예에 따라 बैं크 메모리에 저장된 데이터의 변화를 사이클 별로 나타낸 도면이다.

도 13은 본 발명의 블록체인 마이닝 시스템의 트랜잭션 및 해시엔진에 따른 소요시간 및 소모전력을 비교하여 나타낸 테이블이다.

도 14는 일 실시예에 따른 본 발명의 블록체인 마이닝 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0027] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

[0028] 본 명세서에서 사용되는 용어에 대해 간략히 설명하고, 본 발명에 대해 구체적으로 설명하기로 한다.

[0029] 본 발명에서 사용되는 용어는 본 발명에서의 기능을 고려하면서 가능한 현재 널리 사용되는 일반적인 용어들을 선택하였으나, 이는 당 분야에 종사하는 기술자의 의도 또는 관례, 새로운 기술의 출현 등에 따라 달라질 수 있다. 또한, 특정한 경우는 출원인이 임의로 선정한 용어도 있으며, 이 경우 해당되는 발명의 설명 부분에서 상세히 그 의미를 기재할 것이다. 따라서 본 발명에서 사용되는 용어는 단순한 용어의 명칭이 아닌, 그 용어가 가지는 의미와 본 발명의 전반에 걸친 내용을 토대로 정의되어야 한다.

[0030] 명세서 전체에서 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있음을 의미한다. 또한, 명세서에서 사용되는 "부", "모듈", "유닛" 등의 용어는 적어도 하나의 기능 또는 동작을 처리하는 단위를 의미하며, 소프트웨어, FPGA 또는 ASIC과 같은 하드웨어 구성요소, 또는 소프트웨어와 하드웨어의 결합으로 구현될 수 있다. 그렇지만 "부", "모듈", "유닛" 등의 용어가 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. "부", "모듈", "유닛" 등은 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 "부", "모듈", "유닛" 등의 용어는 소프트웨어 구성요소들, 객

체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로 코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들 및 변수들을 포함한다.

[0031] 아래에서는 첨부한 도면을 참고하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략한다. “제1”, “제2” 등과 같이 서수를 포함하는 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 구성 요소들은 용어들에 의해 한정되지는 않는다. 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. “및/또는”이라는 용어는 복수의 관련된 항목들의 조합 또는 복수의 관련된 항목들 중의 어느 하나의 항목을 포함한다.

[0032] 본 명세서에 설명된 다양한 시스템, 장치, 저장 매체, 모듈 및 기구는 전용 연산 디바이스, 또는 하나 이상의 전용 연산 디바이스의 하나 이상의 연산 칩에서 구현될 수도 있다.

[0033] 이하, 본 발명의 블록체인 마이닝 시스템 및 방법에 관하여 설명하도록 한다.

[0034] 도 1은 일반적인 블록체인 마이닝 시스템의 실시예를 도시한 도면이다.

[0035] 도 1의 일 실시예에 따른 블록체인 마이닝 시스템에 의하면, 복수의 노드는 댄풀(mempool)과 같은 트랜잭션 저장소에서 복수의 트랜잭션을 가져올 수 있고, 해시엔진을 이용하여 각 트랜잭션의 해시값을 계산할 수 있다. 블록체인 마이닝 시스템은 계산된 복수의 해시값을 머클트리를 이용하여 머클트리 최종해시값(이하, 머클루트(MR))을 산출할 수 있다. 여기서 머클트리는 앞서 설명된 바와 같이 2개의 자식 노드(leaf node)가 1개의 부모 노드(non-leaf node)로 합쳐져 해시값을 계산하는 구조이다. 머클트리는 계산된 해시값을 두개씩 합쳐 하나의 해시값을 산출하는 해시 계산을 반복하여 최종적으로 머클루트(MR)를 산출할 수 있다. 블록체인 마이닝 시스템은 산출된 머클루트(MR)를 블록헤더에 포함시킬 수 있다. 여기서 블록헤더는 소프트웨어 버전, 이전 블록해시, 블록 생성시간, 난이도, 논스값(NC)을 더 포함할 수 있다. 블록체인 마이닝 시스템은 산출된 머클루트(MR)를 포함한 블록헤더의 해시값(이하, 블록해시(BH))을 산출할 수 있다. 블록체인 마이닝 시스템은 산출한 블록해시(BH)가 일정 조건(예로, 앞자리의 0이 n개 이상)을 충족하는 경우, 블록을 생성할 수 있다. 블록해시(BH)가 조건을 만족하지 않는 경우, 블록체인 마이닝 시스템은 블록해시(BH)가 조건을 만족할 때까지 논스값(NC)을 변경하며 블록해시(BH)를 산출하는 과정을 반복할 수 있다. 만약 논스값(NC)을 가능한 만큼 반복하여 변경하여도 조건을 만족하는 블록해시(BH)를 찾지 못한 경우, 새로운 블록후보를 생성하기 위하여 머클루트(MR)를 변경할 수 있다. 머클루트(MR) 변경을 위해 머클루트(MR)를 재산출하려 하는 경우, 트랜잭션 저장소에서 복수의 트랜잭션을 선택 및 검증하는 과정과 이를 이용하여 해시값을 모두 새로 계산하는 과정을 반복해야 할 수 있다. 이는 블록체인 마이닝의 소모전력 및 실행시간을 크게 증가시키는 원인이 될 수 있다.

[0036] 본 발명의 블록체인 마이닝 시스템(1)은 머클루트(MR)를 재산출하는 과정에 있어서, 초기 머클루트(MR)를 산출하는 데 사용된 일부 해시값을 해시 연산에 재사용함으로써, 복수의 새로운 트랜잭션을 선택하고 검증하는 과정 및 이들의 해시값을 계산하는 과정을 생략하여 전력소모를 감소시키고, 실행시간을 단축시키는 효과를 가질 수 있다.

[0037] 도 2는 일 실시예에 의한 본 발명의 블록체인 마이닝 시스템(1)의 구성을 나타낸 도면이다.

[0038] 본 발명의 블록체인 마이닝 시스템(1)은 각 적어도 하나 이상의 데이터 메모리(100), 해시엔진(200), 인스트럭션 생성부(300) 및 인스트럭션 메모리(400)를 포함할 수 있다.

[0039] 본 발명의 블록체인 마이닝 시스템(1)을 구성하는 각 요소는 서로 연결되어 정보를 전달하고 받을 수 있도록 하나 이상의 통신 메커니즘 및 하드웨어 프로세서를 포함할 수 있다. 또한, 각 구성요소는 블록체인 마이닝을 위해 다양한 단계를 수행하게 하도록 프로세서에 의해 실행 가능한 명령어로 구성된 비일시적 판독가능 저장 매체를 포함할 수도 있다.

[0040] 해시엔진(200)은 데이터 메모리(100)에 데이터(트랜잭션 및/혹은 해시값 등)를 저장하거나 데이터 메모리(100)로부터 데이터를 전달받을 수 있다. 또한, 인스트럭션 생성부(300)는 데이터 메모리에 저장된 데이터를 분석하여 복수의 인스트럭션을 생성할 수 있다.

[0041] 인스트럭션 메모리(400)는 인스트럭션 생성부(300)에서 생성된 복수의 인스트럭션을 저장할 수 있고, 인스트럭

선 메모리(400)는 저장된 인스트럭션을 통해 해시엔진(200)의 계산 과정을 통제 및 컨트롤할 수 있다.

[0042] 도 3을 참조하여 데이터 메모리(100)에 관하여 설명하도록 한다.

[0043] 도 3은 일 실시예에 따른 데이터 메모리(100)의 블록도이다.

[0044] 데이터 메모리(100)는 데이터를 저장할 수 있는 공간으로 정의될 수 있다. 즉, 데이터는 데이터 메모리(100)에 저장될 수 있으며, 이는 데이터를 쓰는(write) 것으로 표현될 수 있다.

[0045] 또한, 데이터 메모리(100)는 저장된 데이터를 해시엔진(200)으로 전달할 수도 있다. 즉, 해시엔진(200) 등은 데이터 메모리(100)로부터 데이터를 불러올 수 있으며, 이는 데이터를 읽는(read) 것으로 표현될 수 있다.

[0046] 데이터 메모리(100)는 복수의 बैं크(130)로 구분될 수 있다. 즉, 데이터 메모리(100)는 서로 다른 복수의 बैं크(130)들로 이루어진 집합을 의미할 수 있다.

[0047] 서로 다른 बैं크(130)는 동시에 접근이 가능할 수 있다. 따라서, 해시엔진(200)이 데이터 메모리(100)로부터 데이터를 읽거나, 데이터 메모리(100)에 데이터를 쓰는 과정이 한 사이클(cycle)내에서 동시에 이루어지는 것이 가능할 수 있다. 여기서 사이클은 하나의 동작이 행해지는 시간 단위를 의미할 수 있다.

[0048] 예로, 도 3의 बैं크(130) (A,E) 및 (B,F)는 서로 다른 बैं크(130)로, 한 사이클 내에서 각각 해시엔진(200)에 의한 접근(예로, 읽는 행위)이 가능하여, A 데이터와 B 데이터를 한 사이클 내에 동시에 읽는 것이 가능할 수 있다.

[0049] 각 बैं크(130)는 적어도 하나의 해시엔진(200)에 미리 할당(pre-assign)될 수 있다.

[0050] 해시엔진(200)은 미리 할당된 बैं크(130)에서만 데이터를 읽어올 수 있다. 반면, 해시엔진(200)이 계산된 해시값을 बैं크(130)에 저장하려는 경우, 어떤 बैं크(130)에도 제한없이 저장할 수 있다. 즉, 해시엔진(200)이 데이터를 저장하려는 경우, 미리 할당된 बैं크(130)뿐만 아니라 할당되지 않은 बैं크(130)에도 저장할 수 있다.

[0051] 일 실시예에 의하면, 블록체인 마이닝 시스템(1) 내에 존재하는 बैं크(130)의 개수는 해시엔진(200) 개수의 2배가 되도록 할 수 있다. 또한, 각 해시엔진(200)에 서로 다른 2개의 बैं크(130)가 중복되지 않도록 할당되도록 할 수 있다. 따라서, 각 해시엔진(200)은 각각 미리 할당된 2개의 बैं크(130)에서만 데이터를 읽도록 설정될 수 있고, 각 बैं크(130)는 하나의 해시엔진(200)으로만 데이터를 전달하도록 설정될 수 있다. 여기서 하나의 해시엔진(200)에 할당된 서로 다른 2개의 बैं크(130)를 서로 짝이되는 한쌍의 बैं크(130)로 표현할 수 있다. 도 3의 실시예를 예시로 들면, बैं크(130) (A,E) 및 (B,F)가 같은 일 해시엔진(200)에 할당되는 경우, बैं크(130) (A,E) 및 (B,F)는 동일한 하나의 해시엔진에 할당된 한쌍의 बैं크(130)로 표현할 수 있다.

[0052] 각 बैं크(130)를 각 해시엔진(200)에 미리 할당함으로써, 블록체인 마이닝 시스템(1)의 하드웨어 및/혹은 소프트웨어 구현시 라우팅 복잡성(routing complexity)을 낮출 수 있다.

[0053] 하나의 बैं크(130)는 2개의 बैं크 메모리(135)로 구성될 수 있다.

[0054] 하나의 बैं크 메모리(135)는 하나의 데이터를 저장할 수 있다. 따라서, 하나의 बैं크(130)는 서로 다른 2개의 데이터를 저장할 수 있다.

[0055] 또한, बैं크 메모리(135)에 데이터를 저장하려 할 때, 해당 बैं크 메모리(135)에 이미 다른 데이터가 저장되어 있는 경우, 원래 저장되어 있던 데이터를 지우고 새롭게 저장하려는 데이터를 저장할 수 있다. 이는 데이터를 덮어쓰는 것 혹은 오버라이트(overwrite)하는 것으로 표현될 수 있다.

[0056] 도 4를 참조하여 해시엔진(200)에 관하여 설명하도록 한다.

[0057] 해시엔진(200)은 데이터 메모리(100)로부터 데이터를 읽어올 수 있고, 데이터 메모리(100)에 데이터를 저장할 수도 있다.

[0058] 또한, 해시엔진(200)은 해시 함수를 이용하여 데이터에서 해시값을 산출할 수 있다. 여기서 해시 함수는 임의의 데이터를 임의의 고정된 길이를 갖는 데이터로 맵핑하는 단방향 함수를 의미한다. 즉, 해시엔진(200)은 데이터를 임의의 고정된 길이를 갖는 다른 데이터로 변경할 수 있다. 여기서 변경된 임의의 다른 데이터를 해시값으로 정의할 수 있다.

[0059] 해시엔진(200)은 두개의 데이터에서 하나의 해시값을 산출할 수도 있다. 이 과정은 위와 동일하게 해시 함수를 이용하여 계산될 수 있다.

- [0060] 따라서, 도 4에 예시된 것과 같이, 해시엔진(200)은 데이터 메모리(100)에서 데이터를 읽어 해시값을 산출할 수 있고, 산출한 해시값을 다시 데이터 메모리(100)에 저장할 수 있다. 더 바람직하게는 해시엔진(200)은 각 बैं크 메모리(135)에서 데이터를 읽을 수 있고, बैं크 메모리(135)에 데이터를 저장할 수 있다. 여기서 बैं크 메모리(135)에 데이터를 저장하는 것은 데이터를 쓰거나 덮어쓰는 것을 포함할 수 있다.
- [0061] 해시엔진(200)은 앞서 언급된 것과 같이 미리 할당된 बैं크(130)에서만 데이터를 읽어올 수 있고, 어떤 बैं크(130)에도 데이터를 저장할 수 있다.
- [0062] 본 발명의 블록체인 마이닝 시스템(1)은 복수의 해시엔진(200)을 포함할 수 있다.
- [0063] 하나의 해시엔진(200)은 한 사이클내에 한번의 해시 연산만을 수행할 수 있다. 즉, 한 사이클내에 수행 가능한 해시 연산의 수는 블록체인 마이닝 시스템(1)에 포함된 해시엔진(200)의 개수에 기초할 수 있다. 예로, 일 실시예에 의한 블록체인 마이닝 시스템(1)이 2개의 해시엔진(200)을 포함하는 경우, 해당 블록체인 마이닝 시스템(1)은 한 사이클내에 최대 2번의 해시 연산을 수행할 수 있다.
- [0064] 도 4 내지 도 7을 참조하여 인스트럭션 생성부(300) 및 인스트럭션 메모리(400)에 관하여 설명하도록 한다.
- [0065] 인스트럭션 생성부(300)는 머클루트(MR) 산출에 필요한 인스트럭션을 생성할 수 있다. 인스트럭션은 본 발명의 머클트리 해시값의 재사용을 통한 머클루트(MR) 재산출에 필요한 명령을 포함할 수 있다.
- [0066] 인스트럭션은 머클루트(MR)를 산출하려 하는 경우마다 생성될 수 있다. 따라서, 머클루트(MR)를 재산출하는 경우, 인스트럭션 생성부(300)는 머클루트(MR) 재산출에 필요한 또 다른 인스트럭션을 생성할 수 있다.
- [0067] 인스트럭션 생성부(300)는 일 알고리즘에 의해 인스트럭션을 생성할 수 있다.
- [0068] 본 발명의 블록체인 마이닝 시스템의 인스트럭션 생성부(300)에서 사용되는 일 알고리즘은 기존의 블록체인 마이닝에서 사용되는 알고리즘과 일부 차이가 존재한다.
- [0069] 기존의 알고리즘에 비해 본 발명의 알고리즘이 갖는 추가적 제약 조건은, बैं크(130)에 저장되는 일부 해시값은 재사용을 위하여 머클루트(MR)를 산출할 때까지 오버라이트되지 않고 남아있어야 할 것 및 해시엔진(200)은 오직 미리 할당된 बैं크(130)에서만 데이터를 읽어올 수 있을 것을 포함할 수 있다.
- [0070] 도 5는 인스트럭션 생성부(300)에서 인스트럭션을 생성하는 과정을 나타낸 순서도이다.
- [0071] 인스트럭션 생성부(300)에서 인스트럭션을 생성하는 방법은 데이터 라이프타임을 분석하는 단계(S501)를 포함할 수 있다. 여기서 라이프타임은, 각 데이터가 बैं크 메모리(135)에 저장되어 있는 시간을 의미할 수 있다. 즉, 일 데이터가 어느 하나의 बैं크 메모리(135)에 저장되고, 다른 데이터가 해당 बैं크 메모리(135)에 저장되어 오버라이트됨으로써 원래의 일 데이터가 지워지기까지의 기간을 일 데이터의 라이프타임으로 정의할 수 있다. 또한, 인스트럭션을 생성하는 방법은 데이터 라이프타임을 설정하는 단계(S502)를 포함할 수 있다. 또한, 인스트럭션을 생성하는 방법은 데이터 저장 위치를 설정하는 단계(S503)를 포함할 수 있다.
- [0072] 한편, 도시하지는 않았으나, 인스트럭션을 생성하는 방법은 बैं크(130)를 해시엔진(200)에 할당하는 단계를 더 포함할 수 있다.
- [0073] 인스트럭션 생성부(300)는 각 단계를 거쳐 인스트럭션을 생성할 수 있다. 즉 생성된 인스트럭션은 어떤 데이터를 언제 읽어올지, 어떤 해시엔진으로 언제 계산을 할지 및 어떤 데이터를 언제 덮어쓸지 등에 관한 명령 정보를 포함하고 있을 수 있다.
- [0074] 도 6은 일 실시예에 따른 인스트럭션 생성부(300)의 블록도를 도시한 도면이다.
- [0075] 인스트럭션 생성부(300)는 분석부(310), 라이프타임 설정부(320), 저장 위치 설정부(330)를 포함할 수 있다.
- [0076] 인스트럭션 생성부(300)에 포함되는 각 구성부는 전술한 각 단계를 수행할 수 있도록 구현될 수 있다.
- [0077] 분석부(310)는 데이터 라이프타임 분석 단계를 수행할 수 있다.
- [0078] 분석부(310)는, 각 데이터별 라이프타임을 분석할 수 있다. 즉, 분석부(310)는 블록체인 마이닝 시스템(1)에서 활용되는 각 데이터가 언제까지 저장되어 있을지를 판단할 수 있다.
- [0079] 분석부(310)는, 각 데이터별 라이프타임을 분석할 때, 머클루트(MR)의 재산출을 위해 필요하다고 판단되는 데이터를 식별할 수 있다.

- [0080] 일 실시예에 따르면, 분석부(310)는, 각 데이터별 라이프타임 분석을 통해, 머클루트(MR) 재산출시 변경되는 데이터에 영향을 받지 않는 데이터를 머클루트(MR)의 재산출을 위해 필요한 데이터로 판단할 수 있다.
- [0081] 라이프타임 설정부(320)는 라이프타임 설정 단계를 수행할 수 있다.
- [0082] 라이프타임 설정부(320)는, 앞선 분석부(310)에서 분석된 데이터별 라이프타임에 기초하여, 각 데이터별로 다시 라이프타임을 설정할 수 있다.
- [0083] 이에 따라, 라이프타임 설정부(320)는 머클루트(MR)의 재산출을 위해 필요하다고 판단하여 식별한 데이터가 오버라이트되지 않도록 라이프타임을 머클루트(MR)의 산출이 종료될 때까지로 설정할 수 있다.
- [0084] 도시하지는 않았지만, 일 실시예에 의하면, 인스트럭션 생성부(300)는 추가적인 구성요소를 포함하여 बैं크(130)를 해시엔진(200)에 할당하는 단계를 수행할 수 있다.
- [0085] बैं크(130)를 해시엔진(200)에 할당하는 단계는 앞서 기술한 것과 같이 각 बैं크(130)가 일 해시엔진(200)에 할당되도록 할 수 있다. 위와 같은 단계를 통해 각 해시엔진(200)은 해당 해시엔진(200)에 미리 할당된 बैं크(130)에서만 데이터를 읽어오도록 할 수 있다.
- [0086] 또한, बैं크(130)를 해시엔진(200)에 할당하는 단계는, 복수의 해시엔진(200)에 बैं크(130)가 중복되지 않도록, 해시엔진(200) 하나당 한쌍의 बैं크(130)를 할당하도록 할 수 있다.
- [0087] 저장 위치 설정부(330)는 데이터 저장 위치 설정 단계를 수행할 수 있다.
- [0088] 저장 위치 설정부(330)는, 앞서 설정된 데이터별 라이프타임에 기초하여, 각 해시엔진(200)이 어떤 बैं크 메모리(135)에 데이터를 저장할지 결정하고, 인스트럭션이 결정된 저장 위치 내용을 포함하도록 설정할 수 있다.
- [0089] 일 실시예에 의하면, 저장 위치 설정부(330)는 인스트럭션이 앞서 라이프타임이 머클루트(MR) 산출이 종료될 때까지로 설정된 데이터는 오버라이트하지 않도록 저장 위치를 결정할 수 있다.
- [0090] 일 실시예에 의하면, 저장 위치 설정부(330)는, 하나의 사이클에서 산출된 해시값은 동일한 하나의 해시엔진(200)에 할당된 한쌍의 बैं크(130)에 나뉘어 각각 저장되도록 저장 위치를 결정할 수 있다.
- [0091] 다시 도 4의 예시를 참조하면, 각 बैं크(130) (A,E) 및 (B,F)는 동일한 하나의 해시엔진(200)에 할당된 짝이되는 한쌍의 बैं크(130)이며, बैं크(130) (C,G) 및 (D,H)도 동일한 하나의 해시엔진(200)에 할당된 짝이되는 한쌍의 बैं크(130)이다. 여기서 각 해시엔진(200)의 결과값은 일 실시예에 따라 짝이되는 한쌍의 बैं크(130) (A,E) 및 (B,F)에 나뉘어 각각 저장될 수 있다.
- [0092] 인스트럭션 생성부(300)에서 생성된 복수의 인스트럭션은 인스트럭션 메모리(400)에 저장될 수 있다.
- [0093] 인스트럭션 메모리(400)는 인스트럭션 생성부(300)에서 생성된 인스트럭션을 전달받아 저장하고, 인스트럭션을 수행하여 머클루트(MR)를 산출하도록 할 수 있다.
- [0094] 도 7은 인스트럭션 메모리(400)에 저장된 인스트럭션에 의해 해시엔진(200)이 제어되는 일 실시예를 도시한 도면이다.
- [0095] 인스트럭션 메모리(400)는 인스트럭션을 통해 해시엔진(200)을 통제하고 컨트롤 할 수 있다.
- [0096] 인스트럭션 메모리(400)는 인스트럭션을 통해 해시엔진(200)이 어떤 बैं크 메모리(135)에서 데이터를 읽어올지 결정하고 명령할 수 있다. 또한, 인스트럭션 메모리(400)는 인스트럭션을 통해 해시엔진(200)이 계산된 해시값을 어떤 बैं크 메모리(135)에 저장할지 결정하고 명령할 수 있다.
- [0097] 도 7의 실시예에 따르면, 인스트럭션 메모리(400)는 인스트럭션을 통해 일 해시엔진(200)이 0,0 बैं크 메모리(135) 및 1,0 बैं크 메모리(135)에서 데이터를 읽어오도록 하고, 계산된 해시값을 2,0 बैं크 메모리(135)에 저장하도록 할 수 있다. 또한, 다른 해시엔진(200)이 2,0 बैं크 메모리(135) 및 3,0 बैं크 메모리(135)에서 데이터를 읽어오도록 하고, 계산된 해시값을 3.0 बैं크 메모리(135)에 저장하도록 할 수 있다. 400앞서 언급된 바와 같이, 해시엔진(200)은 한 사이클 내에 한번의 해시 연산만을 수행 할 수 있기 때문에, 위의 인스트럭션을 통한 해시엔진(200)의 연산 수행 방식 결정 및 명령은 머클루트(MR) 산출을 더욱 효율적으로 하도록 할 수 있다.
- [0098] 정리하자면, 인스트럭션 메모리(400)는 인스트럭션 생성부(300)에서 각 단계를 거쳐 생성된 인스트럭션을 저장하고, 인스트럭션을 통해 해시엔진(200)을 제어할 수 있다. 인스트럭션 메모리(400)는 인스트럭션을 통해 해시엔진(200)이 어느 बैं크 메모리(135)에서 데이터를 읽어올 것인지 및 어느 बैं크 메모리(135)에 해시값을 저장할

것인지를 결정하고 명령할 수 있다. 블록체인 마이닝 시스템은 본 발명의 각 단계를 거쳐 생성된 인스트럭션을 수행하여 머클루트(MR)를 산출할 수 있다.

- [0099] 본 발명의 블록체인 마이닝 시스템(1)은 초기 머클루트(MR) 산출시 해시값을 이용해 데이터를 오버라이트하는 것을 특징으로 한다. 또한, 일부 데이터는 오버라이트되지 않도록 제어하여, 머클루트(MR) 재산출시 일부 해시값을 재사용하여 빠르게 머클루트(MR)를 재산출하는 것에 특징이 있다.
- [0100] 이하 도 8 내지 도 12을 참조하여 일 실시예에 따른 본 발명의 해시값 재사용을 통한 머클루트(MR) 산출 방법을 자세하게 설명하도록 한다.
- [0101] 도 8 내지 도 12은 4개의 뱅크(130)(8개의 뱅크 메모리(135)) 및 2개의 해시엔진(200)(제1 해시엔진 및 제2 해시엔진)으로 머클루트(MR)를 산출하는 과정의 일 실시예이다.
- [0102] 여기서 사용된 뱅크(130) 및 이에 저장된 데이터는 도 7에 예시된 것과 같이 (A,E), (B,F), (C,G) 및 (D,H)로 구성된 것일 수 있다.
- [0103] 도 8은 일 실시예에 따라, 복수의 트랜잭션으로부터 머클트리를 통해 머클루트(MR)를 산출하는 과정을 나타낸 도면이다.
- [0104] 8개의 뱅크 메모리(135)는 트랜잭션 및/혹은 해시값을 각각 저장할 수 있다.
- [0105] 각 해시엔진(200)의 데이터를 읽고 쓰는 작업은 인스트럭션 메모리(400) 및 인스트럭션을 통해 제어될 수 있다.
- [0106] 도 8의 실시예에 따르면, Cycle 0에서 각 뱅크 메모리(135)는 A 내지 H에 해당하는 트랜잭션(혹은 각 트랜잭션을 해시 계산을 통해 변환시킨 해시값)을 저장할 수 있다.
- [0107] Cycle 1에서, 인스트럭션에 따라, 제1 해시엔진(200)은 뱅크 메모리(135)에서 A 및 B 데이터를 읽고, A 및 B 데이터를 이용하여 해시 연산을 수행하여 해시값 AB를 산출할 수 있다. 제1 해시엔진(200)은 산출한 AB 해시값을 C 데이터가 저장된 뱅크 메모리(135)에 오버라이트할 수 있다.
- [0108] 또한, 인스트럭션에 따라, 제2 해시엔진(200)은 뱅크 메모리(135)에서 C 및 D 데이터를 읽고, C 및 D 데이터를 이용하여 해시 연산을 수행하여 해시값 CD를 산출할 수 있다. 제2 해시엔진(200)은 산출한 CD 해시값을 D 데이터가 저장된 뱅크 메모리(135)에 오버라이트할 수 있다.
- [0109] 여기서 각 해시엔진(200)의 계산은 동시에 이루어지기 때문에, 해시값 AB가 오버라이트되어 저장되기 전에 C를 이용한 해시 연산이 이루어질 수 있다.
- [0110] Cycle 2에서, 인스트럭션에 따라, 제1 해시엔진(200)은 뱅크 메모리(135)에서 E 및 F 데이터를 읽고, E 및 F 데이터를 이용하여 해시 연산을 수행하여 해시값 EF를 산출할 수 있다. 제1 해시엔진(200)은 산출한 EF 해시값을 E 데이터가 저장된 뱅크 메모리(135)에 오버라이트할 수 있다.
- [0111] 또한, 인스트럭션에 따라, 제2 해시엔진(200)은 뱅크 메모리(135)에서 G 및 H 데이터를 읽고, G 및 H 데이터를 이용하여 해시 연산을 수행하여 해시값 GH를 산출할 수 있다. 제2 해시엔진(200)은 산출한 GH 해시값을 F 데이터가 저장된 뱅크 메모리(135)에 오버라이트할 수 있다.
- [0112] Cycle 3에서, 인스트럭션에 따라, 제1 해시엔진(200)은 뱅크 메모리(135)에서 해시값 AB 및 CD를 읽고, AB 및 CD를 이용하여 해시 연산을 수행하여 해시값 ABCD를 산출할 수 있다. 제1 해시엔진(200)은 산출한 ABCD 해시값을 EF가 저장된 뱅크 메모리(135)에 오버라이트할 수 있다.
- [0113] 또한, 인스트럭션에 따라, 제2 해시엔진(200)은 뱅크 메모리(135)에서 EF 및 GH 데이터를 읽고, EF 및 GH 데이터를 이용하여 해시 연산을 수행하여 해시값 EFGH를 산출할 수 있다. 제2 해시엔진(200)은 산출한 EFGH 해시값을 GH 데이터가 저장된 뱅크 메모리(135)에 오버라이트할 수 있다.
- [0114] 마찬가지로, 각 해시엔진(200)의 계산은 동시에 이루어지기 때문에, 해시값 ABCD가 오버라이트되어 저장되기 전에 EF를 이용한 해시 계산이 이루어질 수 있다.
- [0115] Cycle 4에서, 인스트럭션에 따라, 제1 해시엔진(200)은 뱅크 메모리(135)에서 해시값 ABCD 및 EFGH를 읽고, ABCD 및 EFGH를 이용하여 해시 연산을 수행하여 해시값 ABCDEFGH를 산출할 수 있다. 계산된 해시값 ABCDEFGH는 머클트리의 최종 해시값으로, 머클루트(MR)일 수 있다.
- [0116] 도 9는 앞선 실시예의 전술한 과정에 따라 뱅크 메모리(135)에 저장된 데이터의 변화를 사이클 별로 나타낸 도

면이다.

- [0117] 도 9를 참조하여 설명하면, 초기에는 각 बैं크 메모리(135)에 데이터 A 내지 H가 저장되어 있을 수 있다.
- [0118] Cycle 1에서, 데이터 C 및 D가 저장되어 있던 बैं크 메모리(135) 2,0 및 3,0에 각각 AB및 CD의 해시값이 오버라이트되었으므로, Cycle 1 이후 बैं크 메모리(135) 2,0 및 3,0에 각각 AB 및 CD가 저장된 것을 확인할 수 있다.
- [0119] 또한, Cycle 2에서, 데이터 E 및 F가 저장되어 있던 बैं크 메모리(135) 0,1 및 1,1에 각각 EF및 GH의 해시값이 오버라이트되었으므로, Cycle 2 이후 बैं크 메모리(135) 0,1 및 1,1에 각각 EF 및 GH가 저장된 것을 확인할 수 있다.
- [0120] 또한, Cycle 3에서, 데이터 EF 및 GH가 저장되어 있던 बैं크 메모리(135) 0,1 및 1,1에 각각 ABCD및 EFGH의 해시값이 오버라이트되었으므로, Cycle 2 이후 बैं크 메모리(135) 0,1 및 1,1에 각각 ABCD 및 EFGH가 저장된 것을 확인할 수 있다.
- [0121] 도 10은 일 실시예에 따라 초기 머클루트(MR) 산출 이후 머클루트(MR) 재산출을 결정하는 과정을 나타낸 순서도이다.
- [0122] 블록체인 마이닝 시스템(1)은 초기 머클루트(MR)를 산출할 수 있다(S1001). 또한, 블록체인 마이닝 시스템(1)은 산출된 초기 머클루트(MR)를 포함한 블록헤더의 블록해시(BH)를 산출할 수 있다(S1002). 또한, 블록체인 마이닝 시스템(1)은 논스값(NC)을 변경하는 과정을 반복하여 블록해시가 조건에 맞도록 하는 논스값(NC)을 탐색할 수 있다(S1003). 블록체인 마이닝 시스템(1)은 더 이상 논스값(NC) 변경이 불가능하여, 블록해시(BH)가 조건에 맞도록 하는 논스값(NC) 발견하지 못한 경우, 머클루트(MR) 재산출을 결정할 수 있다(S1004).
- [0123] 머클루트(MR)를 재산출하는 경우, 인스트럭션 생성부(300)는 전술한 과정을 다시 거쳐 인스트럭션을 다시 생성할 수 있다. 또한, 생성된 인스트럭션은 인스트럭션 메모리(400)로 전달되어 새로운 머클루트(MR)를 산출하는데 이용될 수 있다.
- [0124] 도 9, 도 11 및 도 12를 참조하여 일 실시예에 따라 머클루트(MR)를 재산출하는 과정을 자세히 설명하도록 한다.
- [0125] 도 9의 실시예에 따르면, cycle 4 이후 각 बैं크 메모리(135)에는 A, ABCD, B, EFGH, AB, G, CD, H의 데이터가 저장되어 있을 수 있다.
- [0126] A는 코인베이스(coinbase)로, 머클루트(MR)를 재산출하기 위해 A를 A'로 변경할 수 있다. 여기서 코인베이스는 첫번째 बैं크 메모리(135)에 저장된 트랜잭션을 말하며, 블록상에 존재하는 마이너가 임의로 변경이 가능한 약 100Byte의 공간을 의미할 수 있다.
- [0127] 일 실시예에 따르면, 코인베이스를 산출된 상기 머클루트(MR) 값으로 변경할 수 있다. 즉, 위의 실시예를 참조하면, A'는 초기 산출된 머클루트(MR) 값인 ABCDEFGH일 수 있다. 이러한 경우, 블록체인 마이닝 시스템(1)은 산출된 머클루트(MR)를 코인베이스가 존재하는 बैं크 메모리(135)에 오버라이트할 수 있다.
- [0128] 나머지 데이터 B, CD, EFGH는 머클루트(MR)를 재산출하기 위해 그대로 재사용된다. 따라서, 각 बैं크 메모리(135)에는 A', ABCD, B, EFGH, AB, G, CD, H의 데이터가 저장되어 있을 수 있다.
- [0129] 여기서 재사용을 위해 필요하다고 판단되는 데이터는 인스트럭션 생성부(300)에서 판단되고 결정될 수 있다.
- [0130] 일 실시예에 의하면, 인스트럭션 생성부(300)(는 데이터의 라이프타임 분석을 통해, 코인베이스의 영향을 받지 않는 데이터를 판별할 수 있다. 또한, 인스트럭션 생성부(300)는 각 बैं크 메모리(135)에 저장된 데이터 중, 코인베이스가 되는 데이터 A의 영향을 받지 않는 B, CD, EFGH 데이터의 라이프타임을 머클루트(MR) 산출이 종료될 때까지로 설정할 수 있다. 또한, 인스트럭션 생성부(300)는 코인베이스가 되는 데이터에 영향을 받지 않는 B, CD, EFGH 데이터가 다른 데이터에 의해 오버라이트되지 않도록, 이들 데이터를 제외한 다른 데이터에 오버라이트되게끔 데이터의 저장 위치를 설정할 수 있다.
- [0131] 도 11은 복수의 데이터로부터 머클루트를 통해 머클루트(MR)를 재산출하는 과정을 나타낸 도면이다.
- [0132] 도 11의 실시예에 따르면, Cycle 1에서, 인스트럭션에 따라, 제1 해시엔진(200)은 बैं크 메모리(135)에서 A' 및 B 데이터를 읽고, A' 및 B 데이터를 이용하여 해시 연산을 수행하여 해시값 A'B를 산출할 수 있다. 제1 해시엔진(200)은 산출한 A'B 해시값을 AB 데이터가 저장된 बैं크 메모리(135)에 오버라이트할 수 있다.
- [0133] Cycle 2에서, 인스트럭션에 따라, 제1 해시엔진(200)은 बैं크 메모리(135)에서 A'B 및 CD 데이터를 읽고, A'B 및

CD 데이터를 이용하여 해시 연산을 수행하여 해시값 A'BCD를 산출할 수 있다. 제2 해시엔진(200)은 산출한 A'BCD 해시값을 ABCD 데이터가 저장된 뱅크 메모리(135)에 오버라이트할 수 있다.

- [0134] Cycle 3에서, 인스트럭션에 따라, 제1 해시엔진(200)은 뱅크 메모리(135)에서 A'BCD 및 EFGH 데이터를 읽고, A'BCD 및 EFGH 데이터를 이용하여 해시 연산을 수행하여 해시값 A'BCDEFGH를 산출할 수 있다. 계산된 해시값 A'BCDEFGH는 머클트리의 최종 해시값으로, 재산출된 머클루트(MR)일 수 있다.
- [0135] 도 12는 앞선 실시예의 전술한 과정에 따라 뱅크 메모리(135)에 저장된 데이터의 변화를 사이클 별로 나타낸 도면이다.
- [0136] 도 12를 참조하여 설명하면, 초기에는 각 뱅크 메모리(135)에 데이터 A', ABCD, B, EFGH, AB, G, CD, H가 저장되어 있을 수 있다.
- [0137] Cycle 1에서, 데이터 AB가 저장되어 있던 뱅크 메모리(135) 2,0에 A'B 해시값이 오버라이트되었으므로, Cycle 1 이후 뱅크 메모리(135) 2,0에 A'B가 저장된 것을 확인할 수 있다.
- [0138] 또한, Cycle 2에서, 데이터 ABCD가 저장되어 있던 뱅크 메모리(135) 0,1에 A'BCD의 해시값이 오버라이트되었으므로, Cycle 2 이후 뱅크 메모리(135) 0,1에 A'BCD가 저장된 것을 확인할 수 있다.
- [0139] 전술한 과정과 같이, 본 발명의 블록체인 마이닝 방법의 머클트리는 변경된 코인베이스 A'를 제외한, B, CD, EFGH를 새롭게 계산하지 않고 재사용하여 머클루트(MR)를 재산출하는데 필요한 계산과정을 단축할 수 있다. 또한, 본 발명의 블록체인 마이닝 방법은 해시값 재사용을 통한 계산과정의 단축으로 전력소모를 줄이고 실행시간을 단축시킬 수 있다.
- [0140] 이하, 복수의 실시예 별로 본 발명의 블록체인 마이닝 시스템(1)의 성능을 비교하도록 한다.
- [0141] 본 발명의 블록체인 마이닝 시스템(1)의 초기 머클루트(MR) 산출에 소모되는 전력 및 소요되는 시간 대비 머클루트(MR) 재산출시 소모되는 전력 및 소요되는 시간 값을 구하여 성능을 비교하였다.
- [0142] 또한, 블록체인 마이닝 시스템(1)에 포함되는 트랜잭션의 수와 해시엔진(200)의 수를 변경하며 각 트랜잭션 및 해시엔진(200)의 수에 따른 성능을 비교하였다.
- [0143] 첫 머클루트(MR) 산출에 소요되는 시간은 수학적 식 1과 같은 식으로 계산될 수 있다.

수학적 식 1

$$E_{init} = E_h \left[\frac{2T - 1}{H} \right]$$

- [0144]
- [0145] 여기서 E_h 는 하나의 해시엔진(200)이 해시값을 계산하는데 소요되는 시간이며, T는 트랜잭션의 수, H는 해시엔진(200)의 수이다.
- [0146] 또한, 첫 머클루트(MR) 산출에 소모되는 전력은 수학적 식 2와 같은 식으로 계산될 수 있다.

수학적 식 2

$$P_{init} = P_h(2T - 1)$$

- [0147]
- [0148] 여기서 P_h 는 하나의 해시엔진(200)이 해시값을 계산하는데 소모되는 전력이다.
- [0149] 본 발명의 블록체인 마이닝 시스템에 따라 코인베이스만 변경하고, 다른 해시값 재사용을 통해 머클루트(MR)를 산출하는 경우 소요되는 시간은 수학적 식 3과 같은 식으로 계산될 수 있다.

수학식 3

[0150] $E_{reuse} = E_h[\log_2 T]$

[0151] 또한, 본 발명의 블록체인 마이닝 시스템에 따라 코인베이스만 변경하고, 다른 해시값 재사용을 통해 머클루트(MR)를 산출하는 경우 소모되는 전력은 수학식 4와 같은 식으로 계산될 수 있다.

수학식 4

[0152] $P_{reuse} = P_h[\log_2 T]$

[0153] 도 13은 위와 같은 계산식들을 활용하여 트랜잭션 및 해시엔진(200)에 따른 소요시간 및 소모전력을 비교하여 나타낸 테이블이다.

[0154] 도 13의 결과값을 비교하여 설명하면, 트랜잭션이 512개이고, 해시엔진(200)의 수가 16개인 경우, 머클루트(MR) 재산출에 필요한 시간은 초기 머클루트(MR) 산출에 필요한 시간의 14.08%이며, 머클루트(MR) 재산출에 필요한 전력은 초기 머클루트(MR) 산출에 필요한 전력의 0.88%이다.

[0155] 또한, 트랜잭션이 512개이고, 해시엔진(200)의 수가 8개인 경우, 머클루트(MR) 재산출에 필요한 시간은 초기 머클루트(MR) 산출에 필요한 시간의 7.04%이며, 머클루트(MR) 재산출에 필요한 전력은 초기 머클루트(MR) 산출에 필요한 전력의 0.88%이다.

[0156] 또한, 트랜잭션이 512개이고, 해시엔진(200)의 수가 4개인 경우, 머클루트(MR) 재산출에 필요한 시간은 초기 머클루트(MR) 산출에 필요한 시간의 3.52%이며, 머클루트(MR) 재산출에 필요한 전력은 초기 머클루트(MR) 산출에 필요한 전력의 0.88%이다.

[0157] 또한, 트랜잭션이 1024개이고, 해시엔진(200)의 수가 16개인 경우, 머클루트(MR) 재산출에 필요한 시간은 초기 머클루트(MR) 산출에 필요한 시간의 7.82%이며, 머클루트(MR) 재산출에 필요한 전력은 초기 머클루트(MR) 산출에 필요한 전력의 0.49%이다.

[0158] 또한, 트랜잭션이 1024개이고, 해시엔진(200)의 수가 8개인 경우, 머클루트(MR) 재산출에 필요한 시간은 초기 머클루트(MR) 산출에 필요한 시간의 3.91%이며, 머클루트(MR) 재산출에 필요한 전력은 초기 머클루트(MR) 산출에 필요한 전력의 0.49%이다.

[0159] 또한, 트랜잭션이 1024개이고, 해시엔진(200)의 수가 4개인 경우, 머클루트(MR) 재산출에 필요한 시간은 초기 머클루트(MR) 산출에 필요한 시간의 1.96%이며, 머클루트(MR) 재산출에 필요한 전력은 초기 머클루트(MR) 산출에 필요한 전력의 0.88%이다.

[0160] 또한, 트랜잭션이 2048개이고, 해시엔진(200)의 수가 16개인 경우, 머클루트(MR) 재산출에 필요한 시간은 초기 머클루트(MR) 산출에 필요한 시간의 4.30%이며, 머클루트(MR) 재산출에 필요한 전력은 초기 머클루트(MR) 산출에 필요한 전력의 0.27%이다.

[0161] 또한, 트랜잭션이 2048개이고, 해시엔진(200)의 수가 8개인 경우, 머클루트(MR) 재산출에 필요한 시간은 초기 머클루트(MR) 산출에 필요한 시간의 2.15%이며, 머클루트(MR) 재산출에 필요한 전력은 초기 머클루트(MR) 산출에 필요한 전력의 0.27%이다.

[0162] 또한, 트랜잭션이 2048개이고, 해시엔진(200)의 수가 4개인 경우, 머클루트(MR) 재산출에 필요한 시간은 초기 머클루트(MR) 산출에 필요한 시간의 1.08%이며, 머클루트(MR) 재산출에 필요한 전력은 초기 머클루트(MR) 산출에 필요한 전력의 0.27%이다.

[0163] 도 14를 참조하여 본 발명의 블록체인 방법에 관하여 설명하도록 한다.

[0164] 도 14는 일 실시예에 따른 본 발명의 블록체인 마이닝 방법의 순서도이다.

[0165] 일 실시예에 따르면, 블록체인 마이닝 방법은 인스트럭션을 생성하는 단계(S1401)를 포함할 수 있다. 또한, 블록체인 마이닝 방법은 머클트리(MR)를 이용하여 생성된 인스트럭션에 따라 초기 머클루트(MR)를 산출하는 단계

(S1402)를 포함할 수 있다. 이 단계에서, 머클트리 중간에 산출되는 해시값을 다시 데이터 메모리(100)에 저장할 수 있다. 또한, 블록체인 마이닝 방법은 산출된 머클루트(MR)를 포함한 블록헤드의 블록해시(BH)를 산출하는 단계(S1403)를 포함할 수 있다. 블록체인 마이닝 방법은 산출된 블록해시(BH)가 조건을 만족하는지 판단하는 단계(S1404)를 포함할 수 있다. 블록해시(BH)가 조건을 만족하지 않는 경우(S1405의 N), 블록체인 마이닝 방법은 논스값(NC)이 변경이 가능하면(S1406의 Y) 논스값(NC)을 변경하는 단계(S1407)를 포함할 수 있다. 또한, 블록체인 마이닝 방법은 변경된 논스값(NC)을 포함하여 블록해시(BH)를 재산출하는 단계(S1408)를 포함하여, 다시 블록해시(BH)가 조건을 만족하는지 판단할 수 있다. 블록체인 마이닝 방법은 논스값(NC)이 변경이 불가능하면(S1406의 N) 코인베이스를 변경하는 단계(S1409)를 포함할 수 있다. 블록체인 마이닝 방법은 인스트럭션을 재생성하는 단계(S1410)를 포함하여, 변경된 코인베이스 및 인스트럭션에 따라 머클루트(MR)를 재산출할 수 있다. 블록체인 마이닝 방법은 재산출된 머클루트(MR)를 포함한 블록헤드의 블록해시(BH)를 산출하고, 블록해시(BH)가 조건을 만족하는지 판단하는 과정을 반복할 수 있다. 블록체인 마이닝 방법은 블록해시(BH)가 조건을 만족한다면(S1405의 Y) 블록을 생성하는 단계(S1411)를 포함할 수 있다.

[0166]

본원 발명의 실시예 등과 관련된 기술 분야에서 통상의 지식을 가진 자는 상기 기재의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로, 개시된 방법들은 한정적인 관점이 아닌 설명적 관점에서 고려되어야 한다. 본 발명의 범위는 발명의 상세한 설명이 아닌 특허청구 범위에 나타나며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0167]

1: 블록체인 마이닝 시스템

100: 데이터 메모리

130: 뱅크

135: 뱅크 메모리

200: 해시엔진

300: 인스트럭션 생성부

310: 분석부

320: 라이프타임 설정부

330: 저장 위치 설정부

400: 인스트럭션 메모리

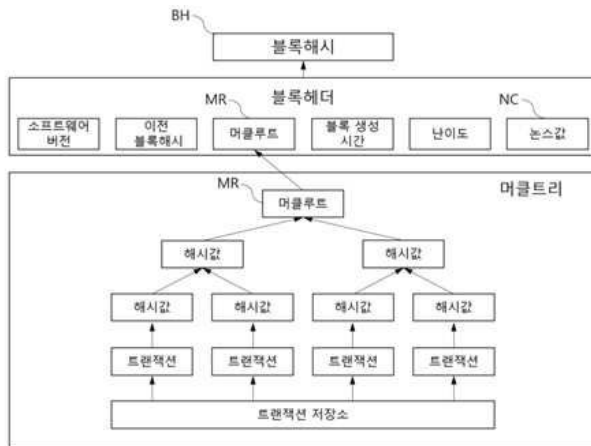
MR: 머클루트

NC: 논스값

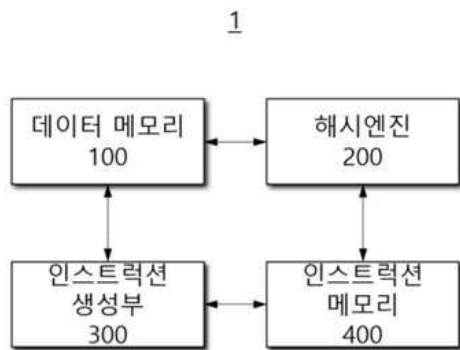
BH: 블록해시

도면

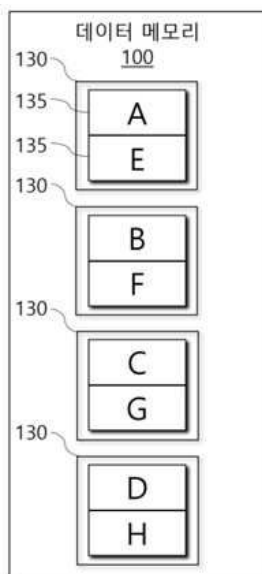
도면1



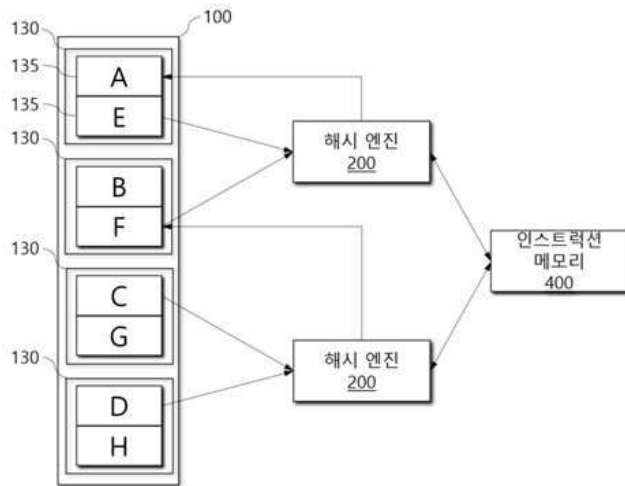
도면2



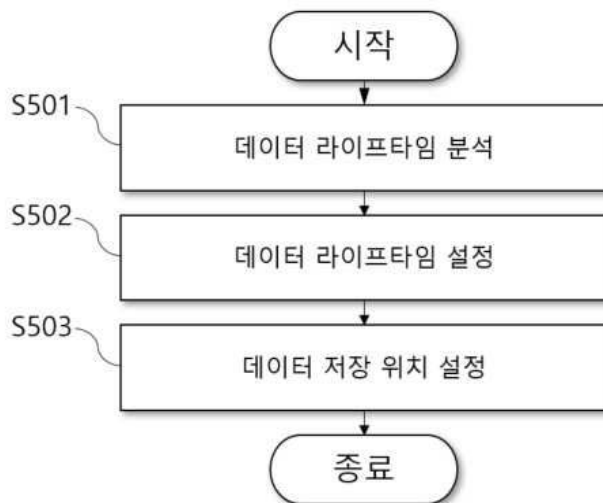
도면3



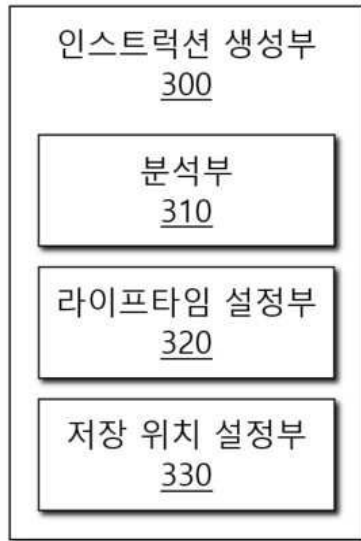
도면4



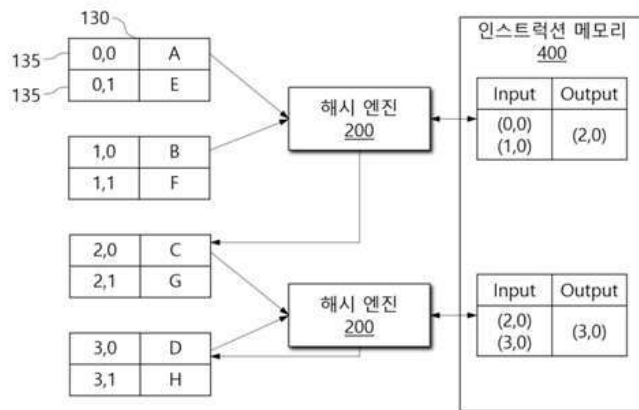
도면5



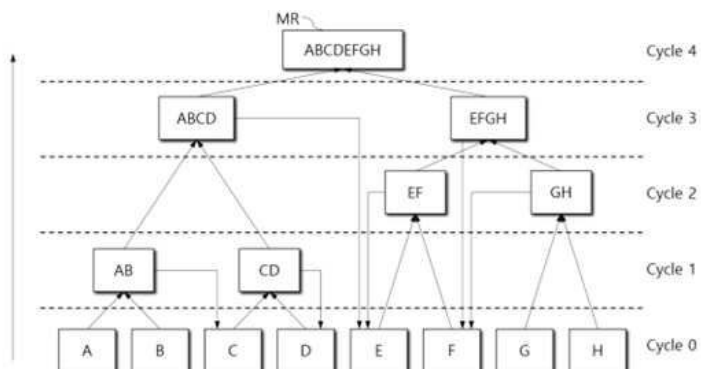
도면6



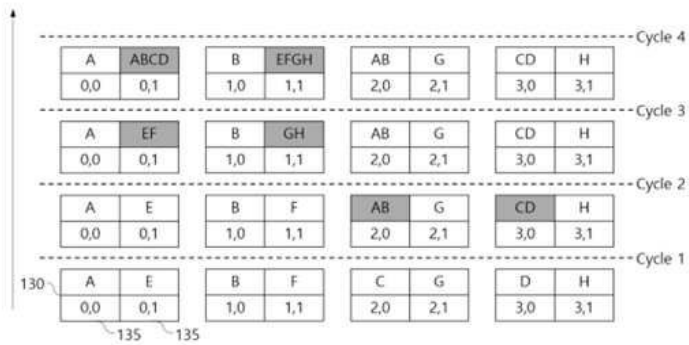
도면7



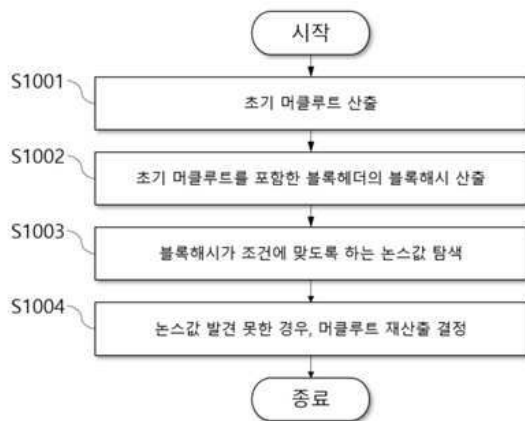
도면8



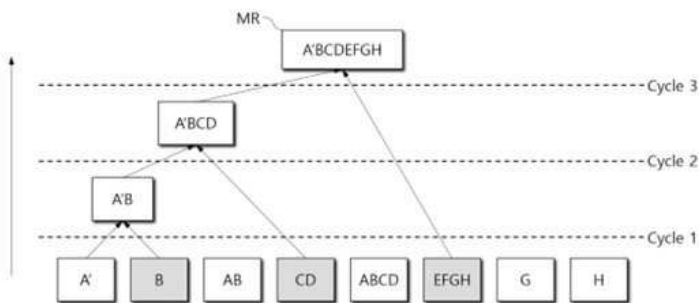
도면9



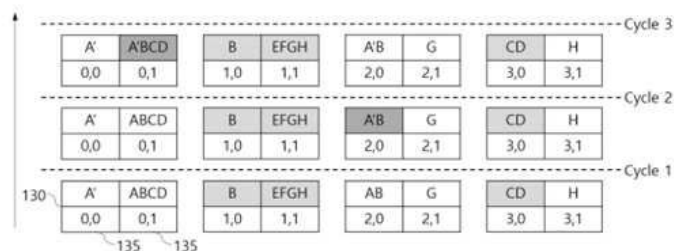
도면10



도면11



도면12



도면13

T	H	Reuse/Init percentage(%)	
		Time $\frac{(E_{reuse})}{(E_{init})}$	Power $\frac{(P_{reuse})}{(P_{init})}$
512	16	14.08	0.88
	8	7.04	0.88
	4	3.52	0.88
1024	16	7.82	0.49
	8	3.91	0.49
	4	1.96	0.49
2048	16	4.30	0.27
	8	2.15	0.27
	4	1.08	0.27

도면14

