



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년09월09일
(11) 등록번호 10-2154354
(24) 등록일자 2020년09월03일

(51) 국제특허분류(Int. Cl.)
G06F 11/30 (2006.01) G06Q 20/06 (2012.01)
G06Q 20/36 (2012.01)
(52) CPC특허분류
G06F 11/3006 (2013.01)
G06Q 20/065 (2013.01)
(21) 출원번호 10-2019-0097144
(22) 출원일자 2019년08월09일
심사청구일자 2019년08월09일
(56) 선행기술조사문헌
KR101758870 B1*
KR1020180113145 A*
KR101796690 B1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김승주
서울특별시 강남구 도곡로57길 12, 103동 503호 (역삼동, 역삼2차아이파크)
이수현
서울특별시 노원구 공릉로34길 28, 나동 403호 (공릉동, 공릉아파트)
(74) 대리인
이기성

전체 청구항 수 : 총 14 항

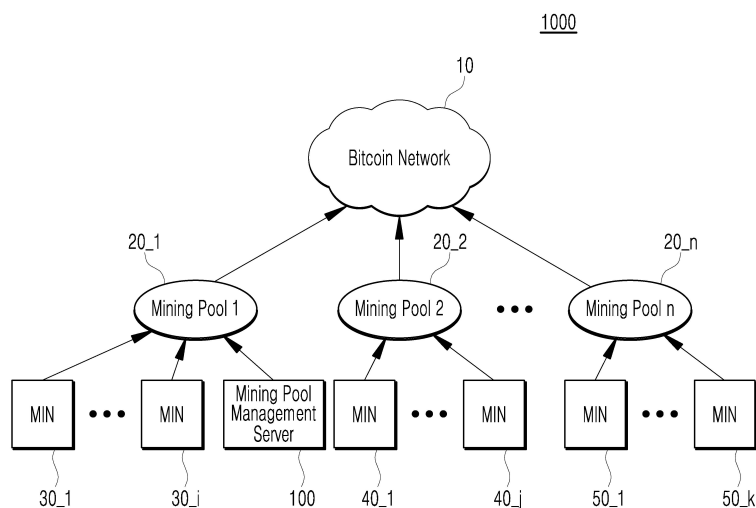
심사관 : 김계준

(54) 발명의 명칭 경쟁 마이닝 풀의 이기적 채굴 전략을 억제할 수 있는 마이닝 풀 관리 서버 및 그 동작 방법

(57) 요약

본 출원은 암호화폐에 대한 것으로, 좀 더 자세하게는 암호화폐 채굴 방법에 대한 것이다. 본 출원의 실시 예에 따른 마이닝 풀 관리 서버는 경쟁 마이닝 풀에 대한 모니터링 동작을 수행하고, 상기 경쟁 마이닝 풀의 이전 블록에 대한 데이터를 획득하는 모니터부, 상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터에 기초하여, 프라이빗 블록의 존재 여부를 탐지하는 프라이빗 블록 탐지부, 및 상기 프라이빗 블록이 존재한다고 판단되는 경우, 상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터에 기초하여 상기 프라이빗 블록의 다음 블록에 대응하는 작업을 재구성하는 작업 재구성부를 포함한다. 본 출원의 실시 예에 따른 마이닝 풀 관리 서버는 경쟁 마이닝 풀의 이기적 채굴에 의한 연산 낭비를 억제시킴으로써 효율적인 채굴 동작을 수행할 수 있다.

대표도 - 도1



(52) CPC특허분류

G06Q 20/3678 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711074104
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기술진흥센터
연구사업명	정보보호핵심원천기술개발(R&D)
연구과제명	고등급(EAL6 이상) 보안 마이크로커널 개발
기 여 율	1/1
과제수행기관명	고려대학교산학협력단
연구기간	2018.04.01 ~ 2018.12.31

공지예외적용 : 있음

명세서

청구범위

청구항 1

경쟁 마이닝 풀에 대한 모니터링 동작을 수행하고, 상기 경쟁 마이닝 풀의 이전 블록에 대한 데이터를 획득하는 모니터부;

상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터에 기초하여, 프라이빗 블록의 존재 여부를 탐지하는 프라이빗 블록 탐지부; 및

상기 프라이빗 블록이 존재한다고 판단되는 경우, 상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터에 기초하여 상기 프라이빗 블록의 다음 블록에 대응하는 작업을 재구성하는 작업 재구성부를 포함하고,

상기 프라이빗 블록 탐지부에 의하여 상기 프라이빗 블록이 존재한다고 판단되는 경우, 상기 작업 재구성부는 상기 프라이빗 블록에 대응하는 작업을 노출된 작업으로 설정하는, 마이닝 풀 관리 서버.

청구항 2

제1 항에 있어서,

상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터는 상기 경쟁 마이닝 풀의 이전 블록 해시 값인, 마이닝 풀 관리 서버.

청구항 3

제1 항에 있어서,

상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터는 상기 경쟁 마이닝 풀의 머클루트 해시 값인, 마이닝 풀 관리 서버.

청구항 4

제1 항에 있어서,

상기 프라이빗 블록 탐지부는 상기 이전 블록에 대한 데이터를 기 공개된 적어도 하나의 퍼블릭 블록과 비교하고, 상기 이전 블록에 대한 데이터와 매칭되는 퍼블릭 블록이 존재하지 않을 때에 상기 프라이빗 블록이 존재하는 것으로 판단하는, 마이닝 풀 관리 서버.

청구항 5

삭제

청구항 6

제1 항에 있어서,

상기 작업 재구성부는 상기 노출된 작업에 대한 채굴 동작을 스킵하도록 자기 마이닝 풀의 마이닝 노드들을 제어하는, 마이닝 풀 관리 서버.

청구항 7

제6 항에 있어서,

상기 작업 재구성부는 상기 프라이빗 블록의 다음 블록에 대한 채굴 작업을 수행하도록 작업을 재구성하는, 마이닝 풀 관리 서버.

청구항 8

제1 항에 있어서,

상기 경쟁 마이닝 풀과 데이터를 송수신하는 통신부를 더 포함하는, 마이닝 풀 관리 서버.

청구항 9

제8 항에 있어서,

상기 프라이빗 블록의 다음 블록에 대한 채굴 작업을 완료한 경우에, 상기 프라이빗 블록의 다음 블록에 대한 채굴 완료 정보를 상기 통신부를 통하여 상기 경쟁 마이닝 풀에 전송하는 제어부를 더 포함하는, 마이닝 풀 관리 서버.

청구항 10

제1 항에 있어서,

상기 프라이빗 블록은 상기 경쟁 마이닝 풀에 의하여 채굴 완료되었으나, 기 공개된 퍼블릭 블록과 매칭되지 않는 블록인, 마이닝 풀 관리 서버.

청구항 11

모니터부에 의하여, 경쟁 마이닝 풀로부터 이전 블록에 대한 데이터를 획득하는 단계;

프라이빗 블록 탐지부에 의하여, 상기 경쟁 마이닝 풀로부터 획득한 상기 이전 블록에 대한 데이터에 기초하여, 프라이빗 블록의 존재 여부를 탐지하는 단계; 및

작업 재구성부에 의하여, 상기 프라이빗 블록이 존재한다고 판단되는 경우, 상기 프라이빗 블록에 대응하는 작업을 스킵하도록 작업을 재구성하는 단계를 포함하고,

상기 프라이빗 블록 탐지부에 의하여 상기 프라이빗 블록이 존재한다고 판단되는 경우, 상기 작업 재구성부는 상기 프라이빗 블록에 대응하는 작업을 노출된 작업으로 설정하는, 마이닝 풀 관리 서버의 동작 방법.

청구항 12

제11 항에 있어서,

상기 프라이빗 블록의 존재 여부를 탐지하는 단계는, 상기 경쟁 마이닝 풀로부터 획득한 상기 이전 블록에 대한 데이터를 기 공개된 적어도 하나의 퍼블릭 블록과 비교하는 단계를 포함하는, 마이닝 풀 관리 서버의 동작 방법.

청구항 13

제12 항에 있어서,

상기 프라이빗 블록의 존재 여부를 탐지하는 단계는,

상기 경쟁 마이닝 풀로부터 획득한 상기 이전 블록에 대한 데이터가 상기 적어도 하나의 퍼블릭 블록과 매칭되지 않는 경우에, 상기 프라이빗 블록이 존재하는 것으로 판단하는 단계를 더 포함하는, 마이닝 풀 관리 서버의 동작 방법.

청구항 14

제13 항에 있어서,

상기 경쟁 마이닝 풀로부터 획득한 상기 이전 블록에 대한 데이터는 상기 경쟁 마이닝 풀의 이전 블록 해시 값인, 마이닝 풀 관리 서버의 동작 방법.

청구항 15

제13 항에 있어서,

상기 경쟁 마이닝 풀로부터 획득한 상기 이전 블록에 대한 데이터는 상기 경쟁 마이닝 풀의 머클루트 해시 값인, 마이닝 풀 관리 서버의 동작 방법.

발명의 설명

기술 분야

[0001] 본 출원은 암호화폐에 대한 것으로, 좀 더 자세하게는 암호화폐 채굴 방법에 대한 것이다.

배경 기술

[0002] 작업증명(PoW, Proof of Work)이란 목표 값 이하의 해시를 찾는 과정을 무수히 반복함으로써 해당 작업에 참여했음을 증명하는 방식의 합의 알고리즘이다. 일반적으로 채굴(mining)을 통해 작업증명을 하며, 비트코인, 이더리움, 라이트코인, 비트코인캐시, 비트코인골드, 모네로, 지캐시 등의 암호화폐에서 작업증명 방식을 사용하고 있다. 작업증명 방식의 합의 알고리즘을 사용하는 블록체인은 어떤 트랜잭션이 발생했을 경우 해당 트랜잭션이 유효한 트랜잭션인지에 대한 합의 방법 및 새로운 블록이 진짜인지 혹은 가짜인지 여부에 대한 검증 동작을 수행한다.

[0003] 마이닝(Mining, 채굴)은 암호화폐의 거래내역을 기록한 블록을 생성하고, 그 대가로 암호화폐를 얻는 행위를 말한다. 채굴은 임의의 논스(Nonce) 값을 대입하여 얻은 결과 값이 제시된 타겟보다 작은 결과 값이 나올 때까지 무한 반복 작업이 실행된다. 이러한 수학 문제를 풀이하는 과정을 1초에 몇 번이나 수행할 수 있는지에 대한 수치 정보를 해시 파워라 한다. 해시 파워가 높다는 것은 주어진 시간당 더 많은 문제를 풀어낼 수 있다는 의미이며, 이에 따라 새로운 블록을 찾을 확률이 더 높아진다. 결국, 높은 해시 파워를 가진 채굴자는 확률적으로 더 많은 보상을 받게 된다.

[0004] 블록체인은 롱 체인 룰(long chain rule)에 따라, 일반적으로 긴 체인이 정당한 체인으로 인정된다. 이에 따라, 복수의 채굴자들은 동일한 블록을 서로 먼저 발견하기 위하여 서로 경쟁할 수 있다. 만약 어느 채굴자가 블록을 발견하더라도 이를 제출하지 않고 숨긴다면, 다른 채굴자들이 자신이 이미 발견했으나 숨겨놓은 블록을 발견하기 위한 채굴 동작을 계속 수행하게 된다. 이후, 다른 채굴자가 해당 블록을 발견했을 때에 자신이 숨겨서 채굴했던 블록들을 제출한다면, 자신의 블록은 인정되고 다른 채굴자가 발견한 블록은 인정되지 않기에, 경쟁자인 다른 채굴자의 채굴 자원을 낭비시킬 수 있다. 이와 같이, 고의적으로 자신이 발견한 블록을 숨김으로써, 상대방의 채굴 자원을 낭비시키는 채굴 전략은 이기적 채굴(selfish mining)이라 칭해질 수 있다.

발명의 내용

해결하려는 과제

[0005] 본 출원은 경쟁 마이닝 풀의 이기적 채굴(selfish mining) 여부를 탐지하고, 경쟁 마이닝 풀의 이기적 채굴에 의한 연산 낭비를 억제할 수 있는 마이닝 풀 관리 서버를 제공하는데 그 목적이 있다.

과제의 해결 수단

[0006] 본 출원의 실시 예에 따른 마이닝 풀 관리 서버는 경쟁 마이닝 풀에 대한 모니터링 동작을 수행하고, 상기 경쟁 마이닝 풀의 이전 블록에 대한 데이터를 획득하는 모니터링부; 상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터에 기초하여, 프라이빗 블록의 존재 여부를 탐지하는 프라이빗 블록 탐지부; 및 상기 프라이빗 블록이 존재한다고 판단되는 경우, 상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터에 기초하여 상기 프라이빗 블록의 다음 블록에 대응하는 작업을 재구성하는 작업 재구성부를 포함한다.

[0007] 일 실시 예에 있어서, 상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터는 상기 경쟁 마이닝 풀의 이전 블록 해시 값이다.

[0008] 일 실시 예에 있어서, 상기 경쟁 마이닝 풀의 상기 이전 블록에 대한 데이터는 상기 경쟁 마이닝 풀의 머클루트 해시 값이다.

[0009] 일 실시 예에 있어서, 상기 프라이빗 블록 탐지부는 상기 이전 블록에 대한 데이터를 기 공개된 적어도 하나의 퍼블릭 블록과 비교하고, 상기 이전 블록에 대한 데이터와 매칭되는 퍼블릭 블록이 존재하지 않을 때에 상기 프라이빗 블록이 존재하는 것으로 판단한다.

[0010] 일 실시 예에 있어서, 상기 프라이빗 블록 탐지부에 의하여 상기 프라이빗 블록이 존재한다고 판단되는 경우,

상기 작업 재구성부는 상기 프라이빗 블록에 대응하는 작업을 노출된 작업으로 설정한다.

- [0011] 일 실시 예에 있어서, 상기 작업 재구성부는 상기 노출된 작업에 대한 채굴 동작을 스킵하도록 자기 마이닝 풀의 마이닝 노드들을 제어한다.
- [0012] 일 실시 예에 있어서, 상기 작업 재구성부는 상기 프라이빗 블록의 다음 블록에 대한 채굴 작업을 수행하도록 작업을 재구성한다.
- [0013] 일 실시 예에 있어서, 상기 경쟁 마이닝 풀과 데이터를 송수신하는 통신부를 더 포함한다.
- [0014] 일 실시 예에 있어서, 상기 프라이빗 블록의 다음 블록에 대한 채굴 작업을 완료한 경우에, 상기 프라이빗 블록의 다음 블록에 대한 채굴 완료 정보를 상기 통신부를 통하여 상기 경쟁 마이닝 풀에 전송하는 제어부를 더 포함한다.
- [0015] 일 실시 예에 있어서, 상기 프라이빗 블록은 상기 경쟁 마이닝 풀에 의하여 채굴 완료되었으나, 기 공개된 퍼블릭 블록과 매칭되지 않는 블록이다.
- [0016] 본 출원의 실시 예에 따른 마이닝 풀 관리 서버의 동작 방법은 모니터부에 의하여, 경쟁 마이닝 풀로부터 이전 블록에 대한 데이터를 획득하는 단계; 프라이빗 블록 탐지부에 의하여, 상기 경쟁 마이닝 풀로부터 획득한 상기 이전 블록에 대한 데이터에 기초하여, 프라이빗 블록의 존재 여부를 탐지하는 단계; 및 작업 재구성부에 의하여, 상기 프라이빗 블록이 존재한다고 판단되는 경우, 상기 프라이빗 블록에 대응하는 작업을 스킵하도록 작업을 재구성하는 단계를 포함한다.
- [0017] 일 실시 예에 있어서, 상기 프라이빗 블록의 존재 여부를 탐지하는 단계는, 상기 경쟁 마이닝 풀로부터 획득한 상기 이전 블록에 대한 데이터를 기 공개된 적어도 하나의 퍼블릭 블록과 비교하는 단계를 포함한다.
- [0018] 일 실시 예에 있어서, 상기 프라이빗 블록의 존재 여부를 탐지하는 단계는, 상기 경쟁 마이닝 풀로부터 획득한 상기 이전 블록에 대한 데이터가 상기 적어도 하나의 퍼블릭 블록과 매칭되지 않는 경우에, 상기 프라이빗 블록이 존재하는 것으로 판단하는 단계를 더 포함한다.

발명의 효과

- [0019] 본 출원의 실시 예에 따른 마이닝 풀 관리 서버는 경쟁 마이닝 풀의 이기적 채굴에 의한 연산 낭비를 억제시킴으로써 효율적인 채굴 동작을 수행할 수 있다.

도면의 간단한 설명

- [0020] 도 1은 본 출원의 일 실시 예에 따른 암호화폐 시스템(1000)을 보여주는 도면이다.
- 도 2는 도 1의 마이닝 풀 관리 서버(100)를 좀 더 자세히 보여주는 블록도이다.
- 도 3은 본 출원의 일 실시 예에 따른 비트코인의 블록 구조의 일 예를 보여주는 도면이다.
- 도 4는 본 출원의 실시 예에 따른 마이닝 풀 관리 서버(100)의 동작을 보여주는 도면들이다.
- 도 5는 본 출원의 다른 실시 예에 따른 암호화폐 시스템(2000)을 보여주는 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0021] 이하에서는, 본 출원의 기술분야에서 통상의 지식을 가진 자가 본 출원의 기술적 사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 출원의 실시 예들이 첨부된 도면을 참조하여 설명될 것이다.
- [0022] 도 1은 본 출원의 일 실시 예에 따른 암호화폐 시스템(1000)을 보여주는 도면이다.
- [0023] 도 1에서는, 암호화폐의 일 예로, 비트코인이 도시되어 있다. 도 1을 참조하면, 암호화폐 시스템(1000)은 비트코인 네트워크(10), 복수의 마이닝 풀들(20_1~20_n), 복수의 마이닝 노드들(30_1~30_i, 40_1~40_j, 50_1~50_k) 및 마이닝 풀 관리 서버(100)를 포함한다.
- [0024] 비트코인 네트워크(10)는 암호화폐 시스템(1000) 내에서의 통신망 기능을 제공한다. 예를 들어, 비트코인 네트워크(10)는 P2P 또는 간접통신을 수행하는 기능을 구비하는 통신망일 수 있다. 예를 들어, 비트코인 네트워크(10)는 이동통신망, 인터넷, 블루투스, 전용선 또는 LPWAN(Low Power Wide Area Network)(75) 등을 통하여 구현될 수 있다. 예를 들어, 비트코인 네트워크(10)는 미국의 LoRaWAN, 유럽의 Sigfox, Weightless, 차세대 LTE

통신망일 수도 있다. 또한, 비트코인 네트워크(10)는 무선 또는 유선 방식으로 마이닝 노드들(30_1~30_i, 40_1~40_j, 50_1~50_k)과 마이닝 풀 관리 서버(100) 사이의 통신을 지원할 수 있다.

- [0025] 복수의 마이닝 풀들(20_1~20_n) 각각은 적어도 하나의 마이닝 노드에 대응한다. 여기서, 마이닝 풀(mining pool)이란 비트코인, 이더리움 등 암호화폐를 채굴하기 위해서 복수의 채굴자들이 협력하는 네트워크를 의미한다. 예를 들어, 마이닝 풀은 전 세계의 채굴자들이 채굴 성공률을 높이기 위해 자발적으로 결성한 채굴 조합일 수 있다. 마이닝 풀에 가입하여 채굴에 성공한 경우, 해당 마이닝 풀의 참가자들은 각자의 해시 연산력 비율, 즉 해시 파워(hash power) 비율에 따라 채굴 보상을 받을 수 있다.
- [0026] 복수의 마이닝 풀들(20_1~20_n) 각각에는 복수의 마이닝 노드들이 대응될 수 있다. 다시 말하면, 각 마이닝 풀에는 복수의 마이닝 노드들이 참가하여 채굴 동작을 수행할 수 있다. 예를 들어, 제1 마이닝 풀(20_1)에는 마이닝 노드들(30_1~30_i)이 채굴자로 참여할 수 있고, 제2 마이닝 풀(20_2)에는 마이닝 노드들(40_1~40_j)이 채굴자로 참여할 수 있으며, 제3 마이닝 풀(20_n)에는 마이닝 노드들(50_1~50_k)이 채굴자로 참여할 수 있다.
- [0027] 본 출원의 기술적 사상에 따른 실시 예에 있어서, 제1 마이닝 풀(20_1)은 마이닝 풀 관리 서버(100)를 포함할 수 있다. 마이닝 풀 관리 서버(100)는 경쟁 마이닝 풀(competitive mining pool)에서 이기적 채굴 전략(selfish mining strategy)을 수행하는 지의 여부를 탐지한다. 예를 들어, 도 1과 같이 마이닝 풀 관리 서버(100)가 제1 마이닝 풀(20_1)에 속하는 경우, 제2 내지 제n 마이닝 풀들(20_2~20_n)이 경쟁 마이닝 풀로 설정될 수 있다. 이 경우, 마이닝 풀 관리 서버(100)는 경쟁 마이닝 풀들인 제2 내지 n 마이닝 풀들(20_2~20_n)에 대한 모니터링을 통하여 경쟁 마이닝 풀의 이전 블록 해시(PrevBlockHash)를 획득하고, 획득된 경쟁 마이닝 풀의 이전 블록 해시를 공개된 퍼블릭 블록(public block)과 비교함으로써, 경쟁 마이닝 풀이 이기적 채굴 전략을 수행하는 지의 여부를 탐지할 수 있다.
- [0028] 경쟁 마이닝 풀이 이기적 채굴 전략을 수행하는 것으로 탐지된 경우, 본 출원의 기술적 사상의 실시 예에 따른 마이닝 풀 관리 서버(100)는 경쟁 마이닝 풀이 채굴에 성공하였으나 숨겨둔 블록을 프라이빗 블록(private block)으로 설정할 수 있다. 이후, 마이닝 풀 관리 서버(100)는 프라이빗 블록을 채굴하기 위한 작업(이하, 노출된 작업(leaked task))을 스킵하고, 프라이빗 블록에 연결될 새로운 블록을 채굴하기 위한 작업을 재구성할 수 있다. 이후, 새로운 블록에 대한 채굴에 성공하면, 마이닝 풀 관리 서버(100)는 경쟁 마이닝 풀에 새로운 블록의 채굴 사실을 알림으로써, 경쟁 마이닝 풀이 이기적 채굴 전략을 포기하도록 유도할 수 있다.
- [0029] 상술한 바와 같이, 본 출원의 실시 예에 따른 마이닝 풀 관리 서버(100)는 경쟁 마이닝 풀의 이기적 채굴 전략을 탐지하고, 이기적 채굴 전략에 의한 연산 낭비를 억제시킴으로써, 효율적인 채굴 동작을 수행할 수 있다.
- [0030] 한편, 본 출원의 일 실시 예에 따른 시스템에서 사용하는 각 구성요소들은 설명의 편의상 제시된 것으로서, 그 구성요소들의 개수에 특별히 제한을 두는 것은 아니다. 또한, 마이닝 노드와 마이닝 풀 관리 서버는 설명의 편의상 분리한 것으로서, 마이닝 노드도 마이닝 풀 관리 서버의 기능을 가질 수 있고, 마이닝 풀 관리 서버도 채굴 기능을 수행할 수 있다.
- [0031] 또한, 본 출원에서 지칭하는 노드는 필요에 따라서, 서버들 각각을 나타내거나, 노드들의 그룹을 지칭할 수도 있다. 즉, 독립된 단위 개체로서 기능하면, 모두 노드로 표현될 수 있다. 따라서, 마이닝 노드는 개인 PC나 랩탑 컴퓨터는 물론, 스마트폰, 이동단말기와 같이 개체로서 시스템에 접속할 수 있는 것이면 어떠한 것도 포함할 수 있다.
- [0032] 도 2는 도 1의 마이닝 풀 관리 서버(100)를 좀 더 자세히 보여주는 블록도이다.
- [0033] 도 2를 참조하면, 마이닝 풀 관리 서버(100)는 통신부(110), 모니터부(120), 프라이빗 블록 탐지부(130), 작업 재구성부(140) 및 제어부(150)를 포함한다.
- [0034] 통신부(110)는 수신기 또는 송신기를 포함하는, 통신 인터페이스 장치로서 유선 또는 무선으로 데이터를 송수신할 수 있다.
- [0035] 예를 들어, 통신부(110)는 암호화폐 시스템(1000)의 네트워크에 포함된 마이닝 풀들(20_1~20_n) 중 마이닝 풀 관리 서버(100)가 속하는 마이닝 풀(20_1)(이하, "자기 마이닝 풀")의 마이닝 노드들과 유선 또는 무선으로 데이터를 송수신할 수 있다. 다른 예로, 통신부(110)는 암호화폐 시스템(1000)의 네트워크에 포함된 마이닝 풀들(20_1~20_n) 중 경쟁 마이닝 풀들 및 이에 참가하는 마이닝 노드들과 유선 또는 무선으로 데이터를 송수신할 수 있다.
- [0036] 모니터부(120)는 경쟁 마이닝 풀의 작업에 대한 모니터링 동작을 수행한다. 특히, 모니터부(120)는 경쟁 마이닝

풀의 이전 블록의 데이터에 대한 모니터링 동작을 수행할 수 있다. 여기서, 이전 블록의 데이터는, 경쟁 마이닝 풀이 현재 채굴 작업을 진행하고 있는 블록의 이전 블록에 대한 데이터를 의미한다.

- [0037] 예를 들어, 마이닝 풀은 보통 스트라텀 프로토콜(stratum protocol)에 기반한 프로토콜을 사용하며, 이 경우에 작업에 필수적인 요소로 이전 블록 해시(previous block hash)가 주어진다. 이전 블록 해시는 블록체인에서 채굴하고자 하는 블록의 이전 블록의 값을 지정해 줄 수 있다. 이 경우, 이전 블록의 데이터는 이전 블록 해시 값을 의미할 수 있으며, 모니터부(120)는 경쟁 마이닝 풀의 이전 블록 해시에 대한 모니터링 동작을 수행할 수 있다.
- [0038] 프라이빗 블록 탐지부(130)는 모니터부(120)로부터 경쟁 마이닝 풀의 이전 블록에 대한 데이터를 수신한다. 프라이빗 블록 탐지부(130)는 경쟁 마이닝 풀의 이전 블록의 데이터에 기초하여, 프라이빗 블록이 존재하는지의 여부를 탐지할 수 있다. 여기서, 프라이빗 블록은 경쟁 마이닝 풀이 채굴에 성공하였으나 숨겨놓은 블록을 의미할 수 있다.
- [0039] 좀 더 자세히 설명하면, 프라이빗 블록 탐지부(130)는 모니터부(120)로부터 경쟁 마이닝 풀의 이전 블록 해시 값을 수신할 수 있다. 이후, 프라이빗 블록 탐지부(130)는 경쟁 마이닝 풀의 이전 블록 해시를 공개된 퍼블릭 블록(public block)과 비교할 수 있다.
- [0040] 만약 이전 블록 해시 값이 퍼블릭 블록들 중 어느 것과 매칭되지 않는다면, 프라이빗 블록 탐지부(130)는 해당 경쟁 마이닝 풀이 이기적 채굴 전략을 수행한다고 판단할 수 있다. 또한, 프라이빗 블록 탐지부(130)는 이전 블록 해시에 대응하는 블록이 이미 채굴되었다고 판단하고, 해당 블록을 프라이빗 블록으로 설정할 수 있다.
- [0041] 작업 재구성부(140)는 프라이빗 블록 탐지부(130)로부터 프라이빗 블록에 대한 데이터를 수신할 수 있다. 작업 재구성부(140)는 프라이빗 블록을 채굴하기 위한 작업이 아닌, 프라이빗 블록에 연결될 새로운 블록을 채굴하기 위한 작업을 재구성할 수 있다.
- [0042] 예를 들어, 작업 재구성부(140)는 프라이빗 블록에 대한 데이터에 기초하여, 프라이빗 블록을 채굴하기 위한 작업을 노출된 작업(leaked task)으로 설정하고, 해당 노출된 작업을 스킵할 수 있다. 이후, 작업 재구성부(140)는 프라이빗 블록에 대한 데이터 및/또는 이전 블록 해시 값에 기초하여, 프라이빗 블록에 연결될 새로운 블록을 채굴하기 위한 작업을 재구성할 수 있다. 예를 들어, 새로운 블록에 대한 작업은 경쟁 마이닝 풀의 이기적 채굴 전략을 발견한 시점 이후의 거래를 포함할 수 있다.
- [0043] 제어부(150)는 마이닝 풀 관리 서버(100)의 전반적인 동작을 제어할 수 있다. 또한, 프라이빗 블록에 연결될 새로운 블록에 대한 채굴 작업이 수행될 수 있도록, 제어부(150)는 해당 새로운 블록에 대한 작업 정보를 통신부(110)를 통하여 자기 마이닝 풀의 마이닝 노드들에 알려줄 수 있다. 이에 따라, 마이닝 풀 관리 서버(100)가 속한 자기 마이닝 풀의 마이닝 노드들은 새로운 블록을 채굴하기 위한 작업을 수행할 수 있다.
- [0044] 또한, 새로운 블록에 대한 채굴이 성공한 경우, 제어부(150)는 해당 사실을 통신부(110)를 통하여 경쟁 마이닝 풀에 알려줄 수 있다. 이에 따라, 이기적 채굴 전략을 수행하고 있는 다른 경쟁 마이닝 풀에 대하여, 해당 전략을 포기하도록 유도할 수 있다.
- [0045] 도 3은 본 출원의 일 실시 예에 다른 비트코인의 블록 구조의 일 예를 보여주는 도면이다.
- [0046] 도 3에 도시된 바와 같이, 비트코인 블록은 헤더(header) 정보와 트랜잭션(transaction) 정보를 포함할 수 있다. 헤더 정보는 트랜잭션 정보를 암호화하여 출력한 머클루트 해시 값(merkleRootHash)을 포함할 수 있다. 헤더 정보는, 또한, 이전 블록 해시 값(prevBlockHash)을 포함할 수 있다. 트랜잭션 정보는 암호화된 블록을 생성한 채굴자의 계좌정보에 해당하는 Coinbase 트랜잭션을 포함할 수 있다.
- [0047] 도 4는 본 출원의 실시 예에 따른 마이닝 풀 관리 서버(100)의 동작을 보여주는 도면들이다. 설명의 편의상, 블록 A는 퍼블릭 블록이고, 블록 B는 프라이빗 블록이며, 블록 C는 새로운 블록이라고 가정된다.
- [0048] 먼저, 도 4a를 참조하면, 마이닝 풀 관리 서버(100)는 경쟁 마이닝 풀들을 모니터링하고, 경쟁 마이닝 풀의 이전 블록 해시 값(1)을 획득할 수 있다.
- [0049] 도 4b를 참조하면, 마이닝 풀 관리 서버(100)는 경쟁 마이닝 풀의 이전 블록 해시 값(1)이 퍼블릭 블록(A)을 가리키는지의 여부를 확인한다. 예를 들어,
- [0050] 도 4c를 참조하면, 경쟁 마이닝 풀의 이전 블록 해시 값(1)이 퍼블릭 블록(A)에 매칭되지 않는 경우, 마이닝 풀 관리 서버(100)는 경쟁 마이닝 풀에 의하여 숨겨진 프라이빗 블록(B)이 존재한다고 판단한다. 즉, 마이닝 풀 관

리 서버(100)는 경쟁 마이닝 풀이 이기적 채굴 전략을 수행한다고 판단한다.

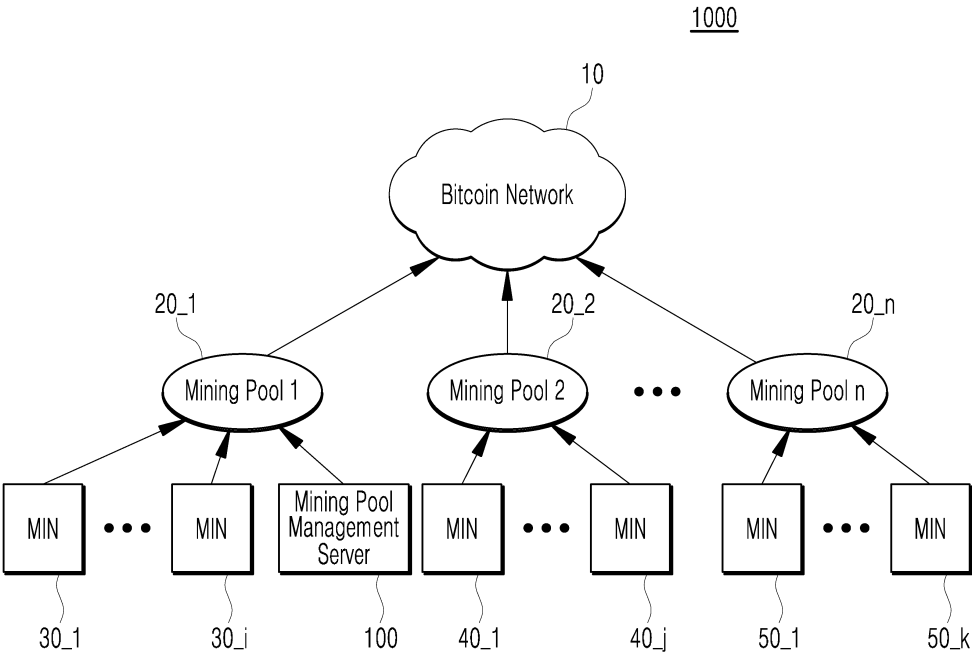
- [0051] 도 4d를 참조하면, 경쟁 마이닝 풀이 이기적 채굴 전략을 수행하는 경우, 마이닝 풀 관리 서버(100)는 프라이빗 블록(B)을 채굴하기 위한 작업을 노출된 작업(leaked task)으로 설정하고, 해당 노출된 작업에 대응하는 채굴 동작을 스킵한다. 그 대신, 마이닝 풀 관리 서버(100)는 이전 블록 해시 값(1)에 기초하여, 새로운 블록(C)을 채굴하기 위한 작업을 재구성할 수 있다.
- [0052] 또한, 마이닝 풀 관리 서버(100)는 자기 마이닝 풀에 속한 마이닝 노드들이 새로운 블록(C)에 대한 채굴 동작을 수행하도록 해당 정보를 제공할 수 있다.
- [0053] 새로운 블록(C)에 대한 채굴에 성공하는 경우, 마이닝 풀 관리 서버(100)는 새로운 블록(C)의 발견 사실을 경쟁 마이닝 풀에 알릴 수 있다. 이에 따라, 경쟁 마이닝 풀이 얻을 수 있는 보상이 줄어들게 되며, 경쟁 마이닝 풀이 이기적 채굴 전략을 포기하도록 유도할 수 있다.
- [0054] 상술한 바와 같이, 본 출원의 실시 예에 따른 마이닝 풀 관리 서버(100)는 경쟁 마이닝 풀의 이기적 채굴 전략을 탐지하고, 이기적 채굴 전략에 의한 연산 낭비를 억제함으로써, 효율적인 채굴 동작을 수행할 수 있다. 또한, 경쟁 마이닝 풀이 이기적 채굴 전략을 포기하게끔 유도함으로써, 건전한 블록체인 생태계를 구축하도록 할 수 있다.
- [0055] 한편, 상술한 설명은 예시적인 것이며, 본 출원의 기술적 사상은 이에 한정되지 않음이 이해될 것이다. 본 출원의 기술적 사상은 당업자에 의하여 다양하게 응용 및 적용될 수 있을 것이다.
- [0056] 예를 들어, 도 1에서, 마이닝 풀 관리 서버(100)가 마이닝 풀에 참여하는 것으로 도시되어 있다. 그러나 본 출원의 기술적 사상은 이에 한정되지 않으며, 마이닝 풀 관리 서버는 별도의 독립적인 개체로 시스템에 참여할 수 있다. 예를 들어, 도 5에 도시된 바와 같이, 마이닝 풀 관리 서버(200)는 비트코인 네트워크(10)에 직접 연결될 수 있으며, 복수의 마이닝 풀들 중 이기적 채굴 전략을 수행하는 마이닝 풀을 탐지하고 억제하도록 구현될 수도 있다.
- [0057] 또한, 도 1 내지 도 4에서, 이전 블록 해시 값에 의하여 프라이빗 블록을 탐지하는 것으로 설명되었다. 다만, 이는 예시적인 것이며, 본 출원의 실시 예에 따른 마이닝 풀 관리 서버는 머클루트 해시 값을 이용하여 프라이빗 블록을 탐지할 수도 있다.
- [0058] 본 출원은 도면에 도시된 일 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 따라서, 본 출원의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

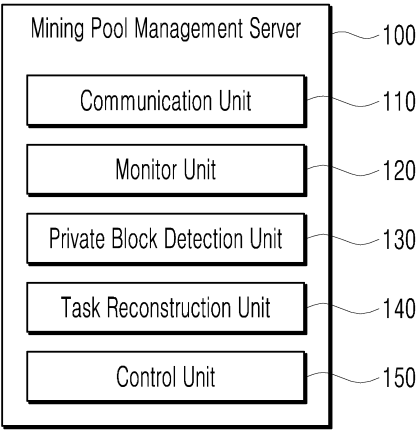
- [0059] 1000, 2000: 암호화폐 시스템
- 10: 비트코인 네트워크
- 20: 마이닝 풀
- 30, 40, 50: 마이닝 노드
- 100: 마이닝 풀 관리 서버
- 110: 통신부
- 120: 모니터부
- 130: 프라이빗 블록 탐지부
- 140: 작업 재구성부
- 150: 제어부

도면

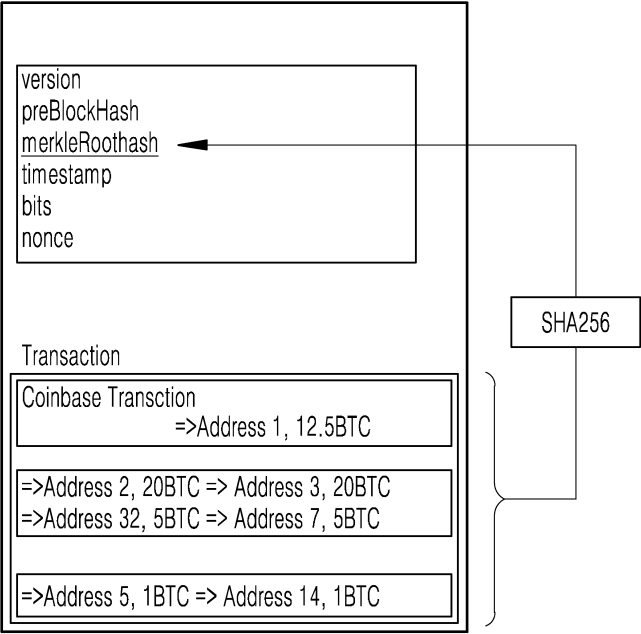
도면1



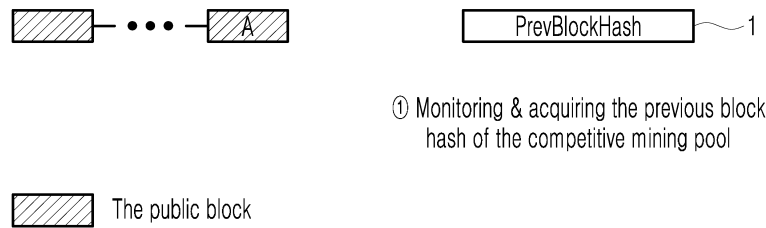
도면2



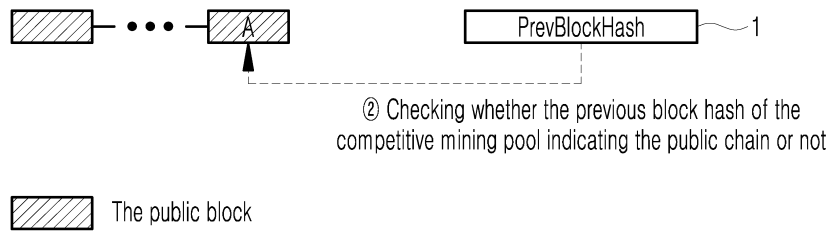
도면3



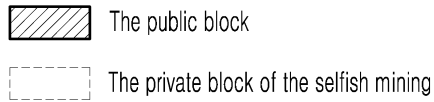
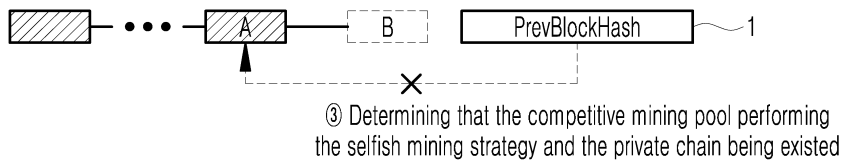
도면4a



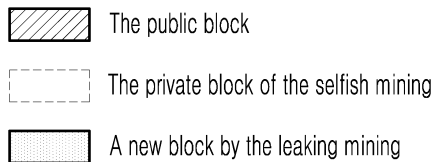
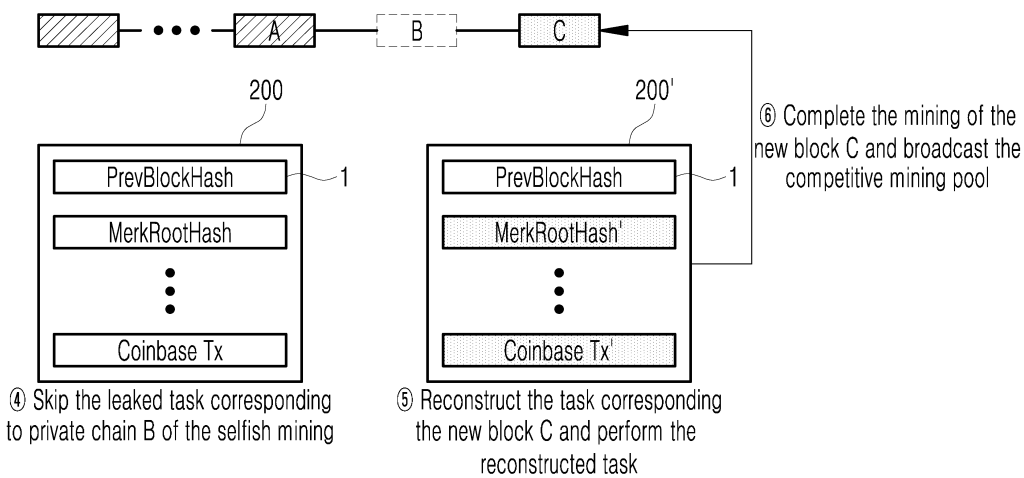
도면4b



도면4c



도면4d



도면5

