(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0014534
(43) 공개일자 2018년02월09일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 9/14* (2006.01)
(52) CPC특허분류
H04L 9/0637 (2013.01)
H04L 9/0643 (2013.01)
(21) 출원번호 10-2016-0097995
(22) 출원일자 2016년08월01일
심사청구일자 2016년08월01일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
박수용
서울특별시 마포구 독막로 98, 101동 1001호 (상수동, 상수두산위브아파트)
고동휘
인천광역시 계양구 계산로126번길 27, 101동 704호 (작전동, 한화아파트)
(뒷면에 계속)
(74) 대리인
특허법인충현

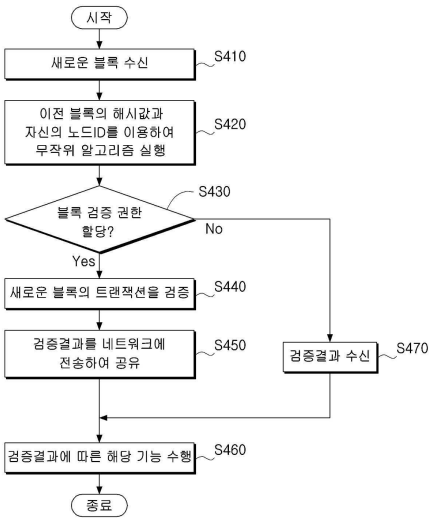
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 **블록체인 기반 트랜잭션 검증 시스템 및 그 방법**

(57) 요 약

본 발명은 블록 해시 기반의 알고리즘을 통하여 소수의 노드들에 블록 검증 권한을 무작위로 할당함으로써, 트랜잭션 검증의 무결성을 유지하면서 컴퓨팅 자원의 효율성을 높일 수 있는, 블록체인 기반 트랜잭션 검증 시스템에 관한 것으로, 트랜잭션이 모여 생성되는 블록 및 상기 블록을 수신 시 상기 블록에 대한 블록 검증 권한이 할당되었는지 여부를 판단하고, 상기 블록 검증 권한이 할당된 경우에 상기 블록의 트랜잭션을 검증하는 노드를 포함하여 구성되는 것을 특징으로 한다.

대 표 도 - 도4



(52) CPC특허분류
H04L 9/14 (2013.01)
(72) 발명자
고덕윤
서울특별시 영등포구 선유서로 67, 102동 601호 (양평동2가, 하이팰리스)
이우승
경기도 고양시 일산동구 산두로 26, 403동 105호 (마두동, 정발마을4단지건영빌라)
조수환
경기도 김포시 김포한강2로 11, 116동 1102호 (장기동, 수정마을 쌍용예가아파트)
최수진
서울특별시 마포구 백범로 35 서강대학교 (신수동)

명 세 서

청구범위

청구항 1

트랜잭션이 모여 생성되는 블록; 및

상기 블록을 수신 시 상기 블록에 대한 블록 검증 권한이 할당되었는지 여부를 판단하고, 상기 블록 검증 권한이 할당된 경우에 상기 블록의 트랜잭션을 검증하는 노드;를 포함하여 구성되는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 2

제1항에 있어서, 상기 노드는,

상기 블록 검증 권한이 할당되었는지 여부를 판단하기 위해 이전 블록의 해시값과 자신의 노드 아이디(ID)를 이용하는 알고리즘을 실행하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 3

제2항에 있어서, 상기 알고리즘은,

이전 블록의 해시값과 자신의 노드 아이디를 기반으로 임의의 수를 구하고 해시함수를 통해 해시값을 구하며, 상기 노드 아이디를 기반으로 해시 값을 구한 후, 상기 해당 해시 값들의 임의의 위치의 문자값이 같으면, 상기 수신된 블록은 해당 노드의 검증 대상인 것으로 구현된 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 4

제1항에 있어서,

상기 블록 검증 권한이 부여된 노드는 상기 수신된 블록에 포함된 트랜잭션 실행 결과값과 자신의 노드가 트랜잭션을 실행시킨 결과값의 일치 여부를 판단함으로써, 상기 트랜잭션을 검증하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 5

제1항에 있어서,

상기 블록 검증 권한이 부여된 노드는, 상기 트랜잭션 검증 결과를 네트워크에 전송하여 다른 모든 노드들에 공유하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 6

노드가 트랜잭션이 모여 생성된 블록을 수신하는 단계;

상기 노드가 상기 블록에 대한 블록 검증 권한이 할당되었는지 여부를 판단하는 단계; 및

상기 블록 검증 권한이 부여된 것으로 판단되면, 상기 수신된 블록의 트랜잭션을 검증하는 단계;를 포함하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 방법.

청구항 7

제6항에 있어서, 상기 블록 검증 권한이 할당되었는지 여부를 판단하는 단계는,

이전 블록의 해시값과 자신의 노드 ID를 이용하여 무작위 알고리즘을 실행하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 방법.

청구항 8

제7항에 있어서,

상기 무작위 알고리즘을 실행하는 단계는,

이전 블록의 해시값과 상기 자신의 노드 아이디를 기반으로 임의의 수를 구하며, 이를 해시함수로 해시값을 구하는 단계;

상기 노드 아이디를 기반으로 해시 값을 구하는 단계;

상기 노드 아이디를 기반으로 구한 해시값이 상기 해당 해시 값의 임의의 위치의 문자값이 같은지 동일여부를 판단하는 단계; 및

상기 동일여부 판단 단계에서 동일한 것으로 판단되면, 상기 수신된 블록은 상기 노드의 검증 대상인 것으로 설정하는 단계를 포함하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 방법.

청구항 9

제6항에 있어서, 상기 트랜잭션을 검증하는 단계는,

상기 수신된 블록에 포함된 트랜잭션 실행 결과값과 자신의 노드가 트랜잭션을 실행시킨 결과값의 일치 여부를 판단함으로써 수행하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 방법.

청구항 10

제9항에 있어서,

상기 트랜잭션 검증 결과를 네트워크에 전송하여 다른 모든 노드들에 공유하는 단계를 더 포함하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 방법.

청구항 11

전체 트랜잭션을 분할하여 생성된 다수의 블록들; 및

상기 다수의 블록들 각각에 대해 선택적으로 블록 검증 권한을 부여받은 노드들;을 포함하여 구성되는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 12

제11항에 있어서,

상기 블록들을 이루는 트랜잭션은 서로 간의 의존성이 없는 트랜잭션들인 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 13

제11항에 있어서,

상기 노드는,

상기 블록 검증 권한이 할당되었는지 여부를 판단하기 위해 이전 블록의 해시값과 자신의 노드 아이디(ID)를 이용하는 알고리즘을 실행하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 14

제11항에 있어서,

상기 알고리즘은,

이전 블록의 해시값과 자신의 노드 아이디를 기반으로 임의의 수를 구하고 해시함수를 통해 해시값을 구하며, 상기 노드 아이디를 기반으로 해시 값을 구한 후, 상기 해당 해시 값들의 임의의 위치의 문자값이 같으면, 상기 수신된 블록은 해당 노드의 검증 대상인 것으로 구현된 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 15

제11항에 있어서,

상기 블록 검증 권한이 부여된 노드는 상기 수신된 블록에 포함된 트랜잭션 실행 결과값과 자신의 노드가 트랜잭션을 실행시킨 결과값의 일치 여부를 판단함으로써, 상기 트랜잭션을 검증하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 16

제11항에 있어서,

상기 블록 검증 권한이 부여된 노드는 트랜잭션 검증 결과를 네트워크에 전송하여 다른 모든 노드들에 공유하는 것을 특징으로 하는, 블록체인 기반 트랜잭션 검증 시스템.

청구항 17

제6항 내지 제10항 중 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인 기반 트랜잭션 검증 시스템 및 그 방법에 관한 것으로, 더욱 상세하게는 블록 해시 기반의 알고리즘을 이용하여 소수의 노드들에 블록 검증 권한을 무작위로 할당함으로써, 트랜잭션 검증의 무결성을 유지하면서 컴퓨팅 자원의 효율성을 높일 수 있는, 블록체인 기반 트랜잭션 검증 시스템 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 2009년 최초의 블록체인에 기반을 둔 애플리케이션인 비트코인이 개발된 이후 블록체인은 비트코인과 같은 전자 화폐 시스템뿐 아니라 클라우드 저장소 서비스, 블록체인 컴퓨팅 서비스 등 다양한 분야에 적용되었다.

[0003] 비트코인은 정부나 은행과 같은 중앙화된 조직이 아닌 분산 네트워크 상에서 발행, 저장 및 유통되는 전자 화폐이다. 비트코인은 2009년 처음 발행되어 현재 시점까지 중앙화된 기관 없이 화폐의 가치를 유지하고 있으며, 사용자 수와 거래 규모 측면에서 급격하게 증가하고 있다.

[0004] 이러한 비트코인의 화폐 가치를 유지하는 배경에는 블록체인 기술이 있다. 블록체인은 중앙화된 서버 없이 탈중앙화된 네트워크 환경에서 보안성과 무결성을 유지하는 기술이다. 이러한 강점에 기반하여 다양한 컴퓨팅 데이터를 공유할 수 있게 되었고, 전자 화폐 이외의 다른 시스템에도 적용되기 시작하였다.

[0005] 예를 들어, 블록체인을 이용한 클라우드 스토리지 시스템으로 스토리지 제공자에게 자체 코인을 발급하여 다른 컴퓨터의 디스크 공간을 이용하고 분할 검증을 통하여 신뢰도를 유지하는 서비스가 있다.

[0006] 다른 예로, 이더리움은 전자화폐에 대한 스마트 계약(smart contract)을 수행하는 어플리케이션을 등록하여 실행할 수 있는 플랫폼이다. 비트코인은 단순히 전자 화폐의 송금을 제공하는데 반해 이더리움은 계약에 의한 거래를 제공해준다.

[0007] 그러나 블록체인은 컴퓨팅 자원 낭비가 심한 비효율적인 운영 구조를 갖고 있다. 구체적으로, 비트코인의 경우 거래 트랜잭션의 무결성을 검증하기 위해 최대한 시간이 소요되며, 각 참여 노드는 30Gbyte 크기의 장부를 저장해야 한다. 또한 거래를 승인하기 위하여서 모든 노드가 장부를 통해 트랜잭션을 검증하고, 검증 결과를 기반으로 거래를 승인해야 한다.

[0008] 즉, 블록체인에 참여한 모든 노드는 동일한 장부를 모두 저장하고 있어야 하고, 동일한 검증 작업을 모두 수행해야 한다. 이러한 사유로 인해 블록체인은 전체 네트워크 관점에서 자원 효율성이 매우 떨어진다.

[0009] 언급한 바와 같이, 블록체인이란 비트코인에서 탈 중앙화된 화폐관리를 위해 사용된 핵심기술이다. 블록체인은 중앙 관리 기관이 없이 임의의 사용자가 데이터를 위변조하는 것을 불가능하게 하여 거래의 무결성을 유지한다.

[0010] 블록체인은 무결성 유지를 위해 블록체인 네트워크에 참여한 모든 참여 노드는 거래 내역(장부)를 저장하고, 새롭게 생성되는 거래 트랜잭션을 저장된 장부를 통해 검사한다.

[0011] 예를 들어, 한 참여 노드가 거래를 조작하여 이중 결재를 감행하여도, 다른 모든 노드가 이중 결재 여부를 검증하여 합의를 부결함으로써, 거래의 승인이 거부된다. 따라서 전체 노드 중 51% 이상이 거짓으로 합의하여 주지 않는 이상, 데이터의 조작은 발생하지 않게 된다.

[0012] 그러나 블록체인은 컴퓨팅 자원 사용 측면에서 매우 비효율적이다. 앞에서도 언급한 바와 같이 블록체인 네트워크에 참여한 모든 노드는 한 거래 트랜잭션을 검증하기 위해 동일한 검증작업을 수행한다.

[0013] 이러한 문제점은 특히 트랜잭션 검증을 위해 복잡한 알고리즘을 수행해야 하는 이더리움의 경우 더욱 부각될 수 있다. 예를 들면, 이더리움 네트워크상에서 대출 계약을 수행하는 경우, 계약자의 거래 내역과 신용상태를 검증하고 이를 승인하는 검증 알고리즘을 수행하여야 한다. 이 때 모든 노드에서 검증 알고리즘을 수행하는 기존의 블록체인 합의 방식은 매우 비효율적이기 때문에 개선이 필요하다.

선행기술문헌

특허문헌

[0014] (특허문헌 0001) 대한민국 공개특허공보 제10-2015-0017723호 (2016년 02월 05일, "블록체인을 기반으로 하는 디지털 콘텐츠의 저작권리 위변조 감지시스템")

발명의 내용

해결하려는 과제

[0015] 본 발명은 상술한 종래 기술의 문제점을 극복하기 위한 것으로, 네트워크상의 모든 노드들이 블록을 검증하기 위해 블록 안에 있는 스마트 컨트랙트 실행 요청을 실행함으로 인해, 낭비된 컴퓨팅 자원을 효율적으로 개선할 수 있는 블록체인 기반 트랜잭션 검증 시스템 및 그 방법을 제공하는 것에 그 목적이 있다.

[0016] 또한, 본 발명은 모든 노드가 아니라 블록 검증 권한을 무작위로 할당받은 노드만 트랜잭션을 검증하게 함으로써, 컴퓨팅 자원 낭비를 줄일 뿐만 아니라, 동시에 소수의 노드가 트랜잭션을 검증하여도 무결성을 보증할 수 있는, 블록체인 기반 트랜잭션 검증 시스템 및 그 방법을 제공하는 것에 그 목적이 있다.

[0017] 아울러, 본 발명은 트랜잭션들 간의 의존성이 없는 경우에 한하여, 새로운 블록을 생성하는 과정에서 전체 트랜잭션을 분할하여 처리함으로써, 컴퓨팅 자원 효율성을 개선할 수 있는, 블록체인 기반 트랜잭션 검증 시스템 및 그 방법을 제공하는 것에 그 목적이 있다.

과제의 해결 수단

[0018] 상기 목적을 달성하기 위해 본 발명의 실시 예에 따른 블록체인 기반 트랜잭션 검증 시스템은, 트랜잭션이 모여 생성되는 블록 및 상기 블록을 수신 시 상기 블록에 대한 블록 검증 권한이 할당되었는지 여부를 판단하고, 상기 블록 검증 권한이 할당된 경우에 상기 블록의 트랜잭션을 검증하는 노드를 포함하여 구성되는 것을 특징으로 한다.

[0019] 여기서, 상기 노드는 상기 블록 검증 권한이 할당되었는지 여부를 판단하기 위해 이전 블록의 해시값과 자신의 노드 아이디(ID)를 이용하는 알고리즘을 실행하는 것을 특징으로 한다.

[0020] 여기서, 상기 알고리즘은 이전 블록의 해시값과 자신의 노드 아이디를 기반으로 임의의 수를 구하고 해시함수를 통해 해시값을 구하며, 상기 노드 아이디를 기반으로 해시 값을 구한 후, 상기 해당 해시 값들의 임의의 위치의 문자값이 같으면, 상기 수신된 블록은 해당 노드의 검증 대상인 것으로 구현된 것을 특징으로 한다.

[0021] 여기서, 상기 블록 검증 권한이 부여된 노드는 상기 수신된 블록에 포함된 트랜잭션 실행 결과값과 자신의 노드가 트랜잭션을 실행시킨 결과값의 일치 여부를 판단함으로써, 상기 트랜잭션을 검증하는 것을 특징으로 한다.

[0022] 여기서, 상기 블록 검증 권한이 부여된 노드는, 트랜잭션 검증 결과를 네트워크에 전송하여 다른 모든 노드들에 공유하는 것을 특징으로 한다.

[0023] 또한, 상기 목적을 달성하기 위해 본 발명의 실시 예에 따른 블록체인 기반 트랜잭션 검증 방법은, 노드가 트랜잭션이 모여 생성된 블록을 수신하는 단계;와, 상기 노드가 상기 블록에 대한 블록 검증 권한이 할당되었는지 여부를 판단하는 단계; 및 상기 블록 검증 권한이 부여된 것으로 판단되면, 상기 수신된 블록의 트랜잭션을 검증하는 단계;를 포함하는 것을 특징으로 한다.

[0024] 여기서, 상기 블록 검증 권한이 할당되었는지 여부를 판단하는 단계는, 이전 블록의 해시값과 자신의 노드 ID를 이용하여 무작위 알고리즘을 실행하는 것을 특징으로 한다.

[0025] 여기서, 상기 무작위 알고리즘을 실행하는 단계는, 이전 블록의 해시값과 상기 자신의 노드 아이디를 기반으로 임의의 수를 구하며, 이를 해시함수로 해시값을 구하는 단계;와, 상기 노드 아이디를 기반으로 해시 값을 구하는 단계;와, 상기 노드 아이디를 기반으로 구한 해시값이 상기 해당 해시 값의 임의의 위치의 문자값이 같은지 동일여부를 판단하는 단계; 및 상기 동일여부 판단 단계에서 동일한 것으로 판단되면 상기 수신된 블록은 상기 노드의 검증 대상인 것으로 설정하는 단계를 포함하는 것을 특징으로 한다.

[0026] 여기서, 상기 트랜잭션을 검증하는 단계는, 상기 수신된 블록에 포함된 트랜잭션 실행 결과값과 자신의 노드가 트랜잭션을 실행시킨 결과값의 일치 여부를 판단함으로써 수행하는 것을 특징으로 한다.

[0027] 상기 검증 결과를 네트워크에 전송하여 다른 모든 노드들에 공유하는 단계를 더 포함하는 것을 특징으로 한다.

[0028] 더불어, 상기 목적을 달성하기 위해 본 발명의 다른 실시 예에 따른 블록체인 기반 트랜잭션 검증 시스템은, 전체 트랜잭션을 분할하여 생성된 다수의 블록들; 및 상기 각 다수의 블록들에 대해 선택적으로 블록 검증 권한을 부여받은 노드들;을 포함하여 구성되는 것을 특징으로 한다.

[0029] 여기서, 상기 블록들을 이루는 트랜잭션은 서로 간의 의존성이 없는 트랜잭션들인 것을 특징으로 한다.

[0030] 여기서, 상기 노드는 상기 블록 검증 권한이 할당되었는지 여부를 판단하기 위해 이전 블록의 해시값과 자신의 노드 아이디(ID)를 이용하는 알고리즘을 실행하는 것을 특징으로 한다.

[0031] 여기서, 상기 알고리즘은 이전 블록의 해시값과 자신의 노드 아이디를 기반으로 임의의 수를 구하고 해시함수를 통해 해시값을 구하며, 상기 노드 아이디를 기반으로 해시 값을 구한 후, 상기 해당 해시 값들의 임의의 위치의 문자값이 같으면, 상기 수신된 블록은 해당 노드의 검증 대상인 것으로 구현된 것을 특징으로 한다.

[0032] 여기서, 상기 블록 검증 권한이 부여된 노드는 상기 수신된 블록에 포함된 트랜잭션 실행 결과값과 자신의 노드가 트랜잭션을 실행시킨 결과값의 일치 여부를 판단함으로써, 상기 트랜잭션을 검증하는 것을 특징으로 한다.

[0033] 여기서, 상기 블록 검증 권한이 부여된 노드는 트랜잭션 검증 결과를 네트워크에 전송하여 다른 모든 노드들에 공유하는 것을 특징으로 한다.

[0034] 더불어, 본 발명의 실시 예에 의한 기록매체는 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있다.

발명의 효과

[0035] 상기와 같이 구성된 본 발명에 따른 블록체인 기반 트랜잭션 검증 시스템 및 그 방법에 의하면, 모든 노드가 아니라 블록 검증 권한을 무작위로 할당받은 노드만 트랜잭션을 검증하게 함으로써, 컴퓨팅 자원 낭비를 줄일 뿐만 아니라, 동시에 소수의 노드가 트랜잭션을 검증하여도 무결성을 보증할 수 있는 효과가 있다.

[0036] 더불어, 본 발명에 따른 블록체인 기반 트랜잭션 검증 시스템 및 그 방법에 의하면, 트랜잭션들 간의 의존성이 없는 경우에 한하여, 전체 트랜잭션을 분할하여 블록을 생성하고, 각 블록에 대해 트랜잭션 검증을 담당할 노드를 할당함에 있어서, 노드들에 블록 검증 권한을 무작위로 부여함으로써, 트랜잭션 검증의 무결성을 유지하면서 컴퓨팅 자원의 효율성을 높일 수 있는 이점이 있다.

도면의 간단한 설명

[0037] 도 1은 블록체인상의 거래 기록 및 확정 메커니즘을 도시하는 도면이다.

도 2는 본 발명의 제1 실시 예에 따른 블록체인 기반 트랜잭션 검증 방법을 설명하기 위한 개괄적인 블록도이다.

도 3은 본 발명의 제1 실시 예에 따른 블록 검증 권한에 대한 할당 여부를 판단하는 알고리즘을 도시하는 도면

이다.

도 4는 본 발명의 제1 실시 예에 따른 블록체인 기반 트랜잭션 검증 방법을 설명하기 위한 순서도이다.

도 5는 본 발명의 제 2 실시 예에 따른 블록체인 기반 트랜잭션 검증 방법을 설명하기 위한 개괄적인 블록도이다.

도 6은 제안한 기법의 전체 노드의 트랜잭션 검증 횟수를 나타내는 그래프이다.

발명을 실시하기 위한 구체적인 내용

[0038] 본 발명은 다양한 변형 및 여러 가지 실시 예를 가질 수 있는바, 특정 실시 예들을 도면에 예시하고 상세한 설명에 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0040] 이하에서는 본 발명의 실시 예의 구성 및 작용에 대하여 참조한 도면을 참조하여 상세히 설명하기로 한다.

[0042] 도 1은 블록체인상의 거래 기록 및 확정 메커니즘을 도시하는 도면이고, 도 2는 본 발명의 제1 실시 예에 따른 블록체인 기반 트랜잭션 검증 방법을 설명하기 위한 개괄적인 블록도이다.

[0043] 도 2에 도시된 바와 같이, 본 발명의 블록체인 기반 트랜잭션 검증 시스템은 블록(Block)과 노드(node A ~ node F)를 포함하여 구성되고, 상기 블록은 도 1에 도시된 바와 같이 블록체인 형태로 구성된다.

[0045] 먼저, 발명의 이해를 돕기 위해 본 발명의 블록체인 기반 트랜잭션 검증 방법을 비트코인 시스템에 도입 및 적용한 예를 들어 설명하기로 하지만, 본 발명의 트랜잭션 검증 방안이 비트코인 시스템뿐만 아니라 컴퓨팅 자원을 이용한 각종 거래기록을 다루는 분야에 적용될 수 있음을 알린다.

[0047] 블록체인을 설명하자면, 채굴자(miner)가 네트워크상에 방송된 여러 거래들(여러 트랜잭션)을 모아서 하나의 블록을 형성한다. 이를 증명(proof)하고 이전 블록에 연결하기 위해 채굴자는 블록의 내용을 특정값(nonce)을 이용하여 SHA256(Secure Hash Algorithm 256) 해시값으로 만들어내는 과정을 거친다. 이때 만들어지는 해시값을 시스템이 허락할 정도로 작게 만들어내는 특정값(nonce)을 찾은 경우, 블록이 하나 생성되어 체인에 연결된다. 이 과정을 채굴(mining, 마이닝)이라 한다.

[0049] 비트코인(Bitcoin)은 현물에 대한 결제가 가능한 디지털 통화로, 통화를 발행하고 관리하는 중앙장치가 존재하지 않는 구조로 이루어진다. 대신에, 비트코인의 거래는 동등 계층간 통신망(P2P: Peer-to-peer network) 기반 분산 데이터베이스에 의해 이루어지며, 공개 키 암호 방식 기반으로 거래를 수행한다.

[0050] 이와 같은, 결제방식을 갖는 비트코인은 신용카드 결제 시에 필요한 카드번호나 유효기간 및 CVC번호 등의 정보 없이도 이용이 가능할 뿐만 아니라 사용수수료도 저렴한 이점이 있다. 또한, 비트코인은 파일의 형태인 전자지갑에 저장되고, 이 전자지갑에는 각각의 고유 주소(퍼블릭 어드레스)가 부여되며, 그 주소를 기반으로 비트코인의 거래가 이루어진다.

[0051] 이와 같은, 결제특성을 갖는 비트코인을 이용하기 위해서는 먼저, 비트코인 이용자는 비트코인 거래소(일예: www.coinplug.com)에 가입하여 전자지갑을 개설한 상태에서 원화에 해당하는 KRW를 충전한다.

[0052] 이후, 비트코인 거래소에서 매매되고 있는 비트코인의 현재 시세를 확인한 후 구매를 원하는 비트코인의 수량과 단가를 입력하여 구매주문을 하면, 거래조건에 맞는 판매주문을 통해 거래가 성립됨으로써, 이용자는 물품 구매 시 비트코인을 통해 결제를 수행할 수 있다.

[0054] 노드들에는 앞에서 언급한 바와 같이, 비트코인 거래소측이 운영하는 서버가 하나의 구성원으로 이루어질 수 있

다.

[0055] 이를 위해, 개개의 노드에는 블록체인이 탑재되어야 한다.(이하, 노드를 '블록체인 보유노드' 라고 지칭할 수 있음)

[0056] 노드는 비트코인 결제 시, 이 결제에 따라 생성되는 비트코인 결제용 트랜잭션 정보를 수신한다. 그러면, 노드는 이 수신된 비트코인 결제용 트랜잭션을 실행하고, 검증을 통해 비트코인 결제를 인증하며, 그 인증에 따라 비트코인 결제용 트랜잭션 정보를 기록함과 더불어, 지정된 다음 단의 노드들에게 비트코인 결제용 트랜잭션 정보를 전파한다.

[0057] 여기서, 특히 본 발명은 노드가 비트코인 결제용 트랜잭션 정보를 기록할 때, 트랜잭션을 실행한 결과값을 첨부하고, 결과값이 첨부된 비트코인 결제용 트랜잭션 정보를 다음 단의 노드들에게 전파한다.

[0058] 비트코인 결제용 트랜잭션 정보의 전파는 통신규약(protocol)에 의해 약속된 것으로 비트코인 결제용 트랜잭션 정보의 발생 시 1개의 노드(블록체인 보유 노드)가 지정된 n개의 노드로 전파시키며, 그 비트코인 결제용 트랜잭션 정보를 전송받은 n개의 노드마다 각각 지정된 m개의 노드로 반복 전파하는 피라미드식 전파를 통해 비트코인 결제를 수행하기 위해 필요한 블록체인이 탑재된 모든 블록체인 보유노드에게 전파됨으로써, 완료된다.

[0059] 블록체인 보유노드들에는 블록체인이 탑재된 것으로, 비트코인을 채굴하는 마이너가 운영하는 서버(또는 단말) 또는 비트코인 결제를 위한 사용자 단말(일 예로, PC나 스마트폰)도 블록체인을 갖는 전자지갑이 탑재된 경우 하나의 구성원으로 이루어질 수 있다.

[0060] 이와 더불어, 비트코인 결제의 경우 기본적으로 블록체인을 기반으로 결제가 수행되는데 이처럼, 블록체인을 기반으로 하는 결제에는 라이트 코인, 다크코인, 네임코인, 도기코인 및 리플 등이 있다.

[0062] 특히, 본 발명의 블록은 비트코인 결제를 위한 비트코인 결제용 트랜잭션 정보 및 트랜잭션 실행 결과값을 포함하고, 모든 노드는 새로운 블록을 수신 시 자신의 노드에 블록 검증 권한이 할당되었는지 판단할 수 있는 알고리즘을 실행한다.

[0063] 다시 말하면, 모든 노드는 수신된 블록에 대해 트랜잭션 검증을 수행할 권한이 있는 주체인지에 대한 여부를 판단하는 알고리즘을 실행하는데, 여기서 알고리즘은 이전 블록의 해시값과 자신의 노드 ID를 이용하는 이전 블록 해쉬 기반의 무작위 알고리즘이다. 이와 같은 이전 블록 해쉬 기반의 알고리즘은 블록이 생성될 때마다 노드들에 무작위로 즉, 랜덤으로 블록 검증 권한을 부여하기 위한 방안이라 할 수 있다.

[0065] 종래에 거래 트랜잭션 검증을 위해서 모든 블록체인 보유노드들이 같은 작업을 수행하는 비효율성을 해결하기 위해, 임의로 선정된 소수의 노드에서만 선택적으로 트랜잭션을 검증하는 방안을 제안할 수 있다. 그러나 거래 트랜잭션 검증이 소수의 노드에서 선택적으로 실행되면, 필연적으로 거래의 무결성 보장이 어려워진다. 왜냐하면, 검증하는 노드 수가 줄어들면, 데이터 조작을 위한 51%의 공유가 상대적으로 쉬워지기 때문이다.

[0066] 따라서, 본 발명에서는 이러한 문제를 해결하기 위해 거래 트랜잭션을 검증할 수 있는 권한이 무작위로 랜덤하게 할당된 노드, 즉 예측할 수 없는 노드에 할당되도록 한다. 이러한 블록 검증 권한은 트랜잭션이 모여 새로운 블록이 생성될 때마다 마지막 블록 해시에 따라 바뀌게 된다.

[0067]

[0068] 다시 요약하자면, 본 발명은 블록 검증 권한을 노드들에 무작위로 부여하기 위한 방안으로서, 예측 불가능한 이전 블록의 해시와 자신의 노드 ID를 이용해서 무작위 값을 추출하고, 추출된 값에 따라 노드들에게 블록 검증 권한을 부여한다.

[0069] 구체적인 방법으로서, 이전 블록의 해시 및 자신의 노드 ID를 이용한 무작위 값을 이용하여 노드에 블록 검증 권한을 할당하는 규칙은 도 3의 알고리즘과 같다.

[0071] 도 3을 참조하여, 이전 블록 해쉬 기반의 무작위 알고리즘을 설명하자면 먼저, 이전 블록의 해시값과 자신의 노드 아이디를 기반으로 임의의 수를 구하고, 이를 해시함수로 해시값을 구한다.(2~3라인). 이 알고리즘은 해시함수로 SHA256 알고리즘을 사용한다. 그리고 노드 아이디를 기반으로 해시 값을 구한 후(4라인), 해당 해시 값의

임의의 위치의 문자값(38번째 문자)이 같으면(5라인), 이 블록(prevHash)의 다음 블록은 해당 노드의 검증 대상이 된다(6라인).

[0072] 이와 같은 이전 블록 해쉬 기반의 무작위 알고리즘에 의하면, 이전 블록의 해시값을 이용하여 블록을 생성하기 때문에 블록 생성이 실시간으로 발생하므로, 실시간성이 확보되고, 데이터의 위변조를 위한 담합의 위험성이 줄어든다. 이러한 방법을 통해 모든 노드가 아니라 블록 검증 권한을 할당받은 소수의 노드가 트랜잭션을 검증하여도 무결성을 보장할 수 있다.

[0074] 이전 블록 해쉬 기반의 무작위 알고리즘은 암호화 해시 함수로서, 임의의 입력 메시지를 고정된 길이의 문자열로 출력하는 압축 함수를 이용한다. 이때, 출력 값은 입력 값에 의존한다. 즉, 입력 값의 데이터가 변하면 출력 값 또한 변경되어, 데이터의 무결성 검증 및 메시지 인증에 사용할 수 있다. 이러한 암호화 해시 함수는 일방향성과 충돌 회피성을 만족해야 한다. 먼저, 일방향성은 해시함수 H에서 주어진 출력 해시 값 h를 통해 H(x)=h를 만족하는 x값을 찾는 것이 계산적으로 불가능한 것을 말한다. 즉, 해시 함수 출력 값을 통해 원본 데이터를 추출할 수 없어야 한다. 강한 충돌 회피성이란, H(x)=H(y)를 만족하는 경우가 발생하지 않아야 함을 의미한다. 즉, 모든 입력 값에 대해 해시 함수의 입력 값이 다르다면 출력 값은 달라야 함을 의미한다.

[0076] 도 4는 본 발명의 제1 실시 예에 따른 블록체인 기반 트랜잭션 검증 방법을 설명하기 위한 순서도이다.

[0077] 도 4를 참조하면 먼저, 노드는 마이닝에 의해 생성된 새로운 블록을 수신한다(S410). 상기 블록은 트랜잭션 실행 결과값을 포함하고 있다.

[0078] 다음으로, 노드는 이전 블록의 해시값과 자신의 노드 ID를 이용하여 무작위 알고리즘을 실행한다(S420). 즉, 새로운 블록을 수신한 모든 노드는 자신에게 블록 검증 권한이 할당되었는지 여부를 판단하기 위해, 이전 블록의 해시값과 자신의 노드 ID를 이용하는, 이전 블록 해쉬 기반의 무작위 알고리즘을 실행한다.

[0079] 이전 블록 해쉬 기반의 무작위 알고리즘을 설명하기 위해 도 3을 참조하면 먼저, 이전 블록의 해시값과 자신의 노드 아이디를 기반으로 임의의 수를 구하고, 이를 해시함수로 해시값을 구한다(2~3라인). 이 알고리즘은 해시함수로 SHA256 알고리즘을 사용한다. 그리고 노드 아이디를 기반으로 해시 값을 구한 후(4라인), 해당 해시 값의 임의의 위치의 문자값(38번째 문자)이 같으면(5라인), 이 블록(prevHash)의 다음 블록은 해당 노드의 검증 대상이 된다(6라인).

[0080]

[0081] 다음으로, 상기 알고리즘 실행 결과, 자신의 노드에 블록 검증 권한이 할당되었는지에 대해 판단한다(S430). 즉, 앞선 S420 단계에서 해당 해시 값의 임의의 위치의 문자값(38번째 문자)이 자신의 노드 아이디를 기반으로 구한 해시 값과 동일한 경우, 이전 블록의 다음 블록, 즉 수신된 새로운 블록은 이 노드의 검증 대상이 된다. 반면, 앞선 S420 단계에서 해당 해시 값의 임의의 위치의 문자값(38번째 문자)이 자신의 노드 아이디를 기반으로 구한 해시 값과 동일하지 않은 경우, 이 노드는 블록 검증 권한을 할당받지 못한 것으로 간주된다.

[0083] 다음으로, 앞선 S430 단계에서 블록 검증 권한이 할당된 것으로 판단되면, 수신된 블록의 트랜잭션을 검증한다(S440). 여기서, 트랜잭션의 검증은 수신된 블록에 포함된 결과값과 자신의 노드가 트랜잭션을 실행시킨 결과값의 일치 여부를 판단함으로써 수행할 수 있다.

[0085] 다음으로, 트랜잭션 검증 결과를 네트워크에 전송하여 다른 모든 노드들에 공유한다(S450). 즉, 수신된 블록에 포함된 결과값과 자신의 노드가 트랜잭션을 실행시킨 결과값의 일치 여부에 대한 정보를 공유한다.

[0087] 다음으로, 검증 결과에 따른 해당 기능을 수행한다(S460). 예를 들어, 블록 검증 권한이 할당된 노드들 간에 트랜잭션 검증 결과를 공유하고, 이 검증 결과를 비교함으로써, 블록체인의 위변조 여부를 판단할 수 있다. 아울러, 트랜잭션 검증 결과나 이에 연관된 다른 정보들을 네트워크를 통해 다른 노드들에 공유할 수 있다.

[0089] 한편, 앞선 S430 단계에서 블록 검증 권한이 부여되지 않은 것으로 판단되면, 다른 노드에 의해 수행된 트랜잭션 검증 결과를 수신한다(S470).

[0091] 다음으로, 앞선 S470 단계에서 수신된 트랜잭션 검증 결과에 따른 해당 기능을 수행한다(S460). 예를 들어, 블록체인의 위변조 여부에 대해 판단한 결과에 따른 해당 기능을 수행할 수 있다.

[0093] 종래의 블록체인은 거래 트랜잭션의 검증을 위하여 모든 노드들이 검증에 참여한다. 이러한 기법은 전체 블록체인 네트워크의 컴퓨팅 자원 효율성을 현저하게 떨어뜨리는 주요 원인이 된다. 본 발명은 이를 해결하고자, 노드들에 블록 검증 권한을 무작위로 소수의 노드에 할당하여, 블록 검증 권한이 있는 소수의 노드들만 트랜잭션을 검증하게 함으로써, 자원 효율성을 높일 수 있다.

[0094] 더불어, 이전 블록의 해시값을 이용하여 블록 검증 권한을 할당하기 때문에, 할당이 실시간으로 발생하므로 실시간성을 확보하고, 데이터의 위변조를 위한 담합의 위험성을 줄일 수 있으며, 이러한 방법을 통해 무작위로 할당된 소수의 노드가 트랜잭션을 검증하여도 무결성을 보장할 수 있다.

[0096] 이하에서는 본 발명의 제2 실시 예에 따른 블록체인 기반 트랜잭션 검증 방법에 대해 설명하기로 한다.

[0097] 본 발명의 제2 실시 예에 대해서 먼저 개괄적으로 설명하자면, 새로운 블록이 수신될 시 모든 노드가 자신의 노드에 블록 검증 권한이 할당되었는지 판단하고, 상기 판단에 따라 블록 검증 권한이 할당된 노드만 트랜잭션을 검증하며, 트랜잭션 검증 결과를 공유하고, 트랜잭션 검증 결과에 따른 해당 기능을 수행하는 방법은 앞서 도 4의 순서도를 참고하여 설명한 제1 실시 예와 모두 동일하다.

[0098] 다만, 제 2 실시예는 트랜잭션들 간의 의존성이 없는 경우에 한하여, 새로운 블록을 생성하는 단계에서 전체 트랜잭션을 분할하여 블록을 생성함으로써, 컴퓨팅 자원 효율성을 개선하는 구성이 추가된다.

[0100] 도 5는 본 발명의 제2 실시 예에 따른 블록체인 기반 트랜잭션 검증 방법을 설명하기 위한 개괄적인 블록도이다. 우선, 본 발명의 제2 실시 예는 트랜잭션 간의 의존성이 없는 경우를 전제한 기법임을 알린다.

[0101] 도 5를 참조하면, 본 발명의 제2 실시 예에 따른 블록체인 기반 트랜잭션 검증 방법은 먼저, 특정 블록 분할 알고리즘(예를 들어, 공개키 범위 기반 분할)에 의해 트랜잭션을 분할하여 블록을 생성한다. 이 블록 생성 과정은 앞서 설명한 마이닝 과정을 기반으로 할 수 있다.

[0102] 도 5에서는 예를 들어 7개의 트랜잭션(T1~T7)을 세 개의 블록으로 분할하고, 각 블록에 대해서 두 개씩의 노드에 블록 검증 권한을 할당하는 구성을 개시하고 있으나, 이에 한정하지 않고 트랜잭션을 분할하는 방법이나 블록 검증 권한을 부여받는 노드의 개수 등은 다양하게 구현할 수 있다.

[0103] 노드에 블록 검증 권한을 할당하는 기술, 블록 검증 권한이 할당된 노드가 트랜잭션을 검증하는 기술 및 트랜잭션 검증 결과에 따라 해당 기능을 수행하는 기술에 대해서는 도 4를 참조하여 설명한 구성과 기술적으로 동일하므로, 이에 대한 상세한 설명은 생략하기로 한다.

[0105] 도 6은 제안한 기법의 전체 노드의 트랜잭션 검증 횟수를 나타내는 그래프이다.

[0106] 본 발명의 블록체인 기반 트랜잭션 검증방법의 유효성을 검증하기 위해, 1000개의 비트코인 지갑과 50개의 블록에서 약 2500개의 트랜잭션 데이터를 수집하였다. 1000개의 비트코인 지갑이 각각의 노드라고 가정하고, 이 중 20%가 악의적인 노드로 선정한다. 도 3에 도시된 알고리즘을 수행하여 50개의 블록을 50개에서 1000개의 노드에 할당하였다. 여기서 임의의 수를 추출하기 위한 알고리즘은 매르세네 트위스터(Mersenne Twister) 난수 생성 알고리즘을 채택하였다. 도 3의 알고리즘에 의해 한 노드는 여러 개의 블록을 검증할 수 있고, 한 블록은 여러 노드에서 검증받을 수 있다.

[0107] 도 6을 참조하면, 기존의 블록체인은 모든 노드에서 전체의 트랜잭션을 처리하는 데에 반해, 본 발명은 무작위

로 선택된 노드에서 분산하여 처리하므로, 전체 처리량이 현저하게 줄어듦을 알 수 있다. 실험에서는 모든 노드 수에서 평균 검증횟수가 약 6%로 줄어드는 효과를 보인다.

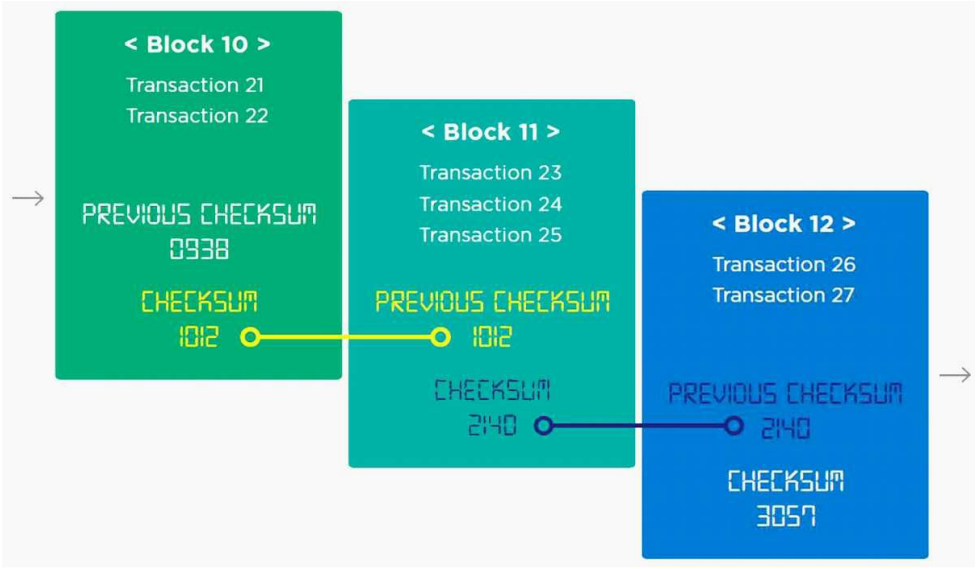
[0109] 본 명세서에 기재된 본 발명의 실시 예와 도면에 도시된 구성은 본 발명의 가장 바람직한 실시 예에 관한 것이고, 발명의 기술적 사상을 모두 포괄하는 것은 아니므로, 출원시점에 있어서 이들을 대체할 수 있는 다양한 균등물과 변형 예들이 있을 수 있음을 이해해야 한다. 따라서 본 발명은 상술한 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형실시가 가능한 것은 물론이고, 그와 같은 변경은 청구범위 기재의 권리범위 내에 있게 된다.

부호의 설명

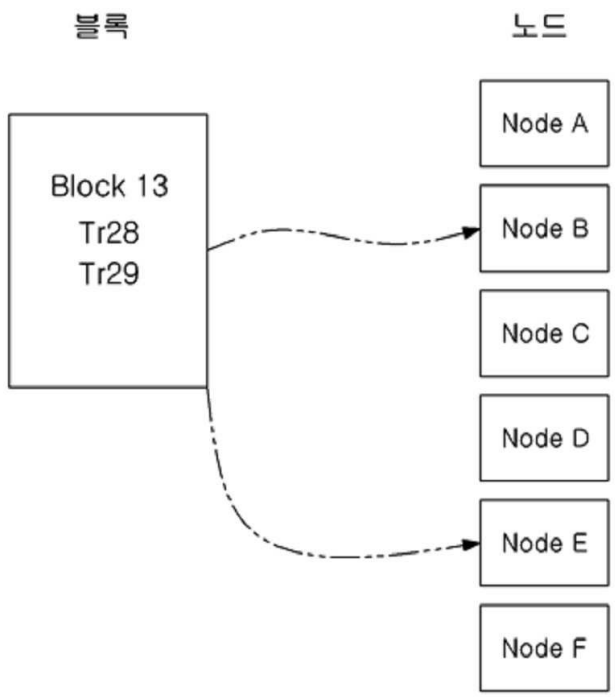
[0110] T1~T7: 트랜잭션 Noda A~Node F: 노드

도면

도면1



도면2

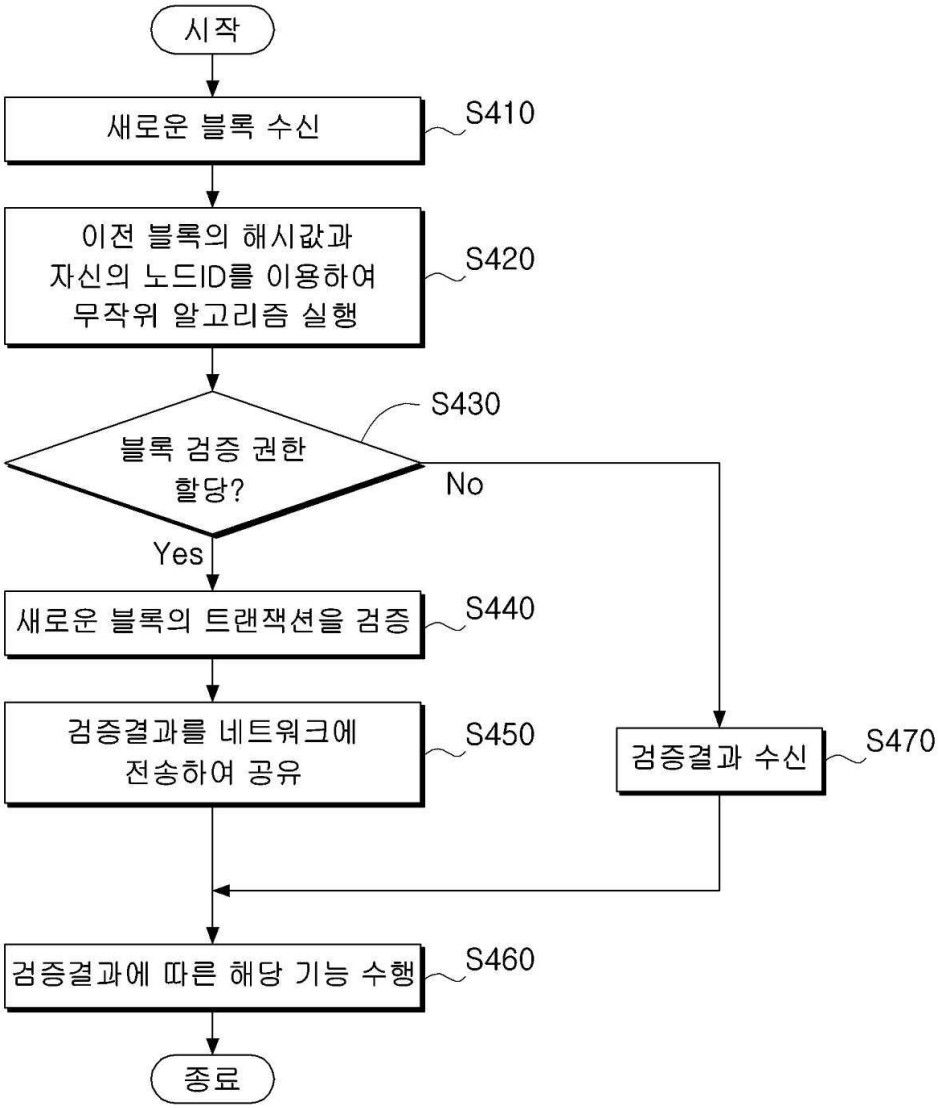


도면3

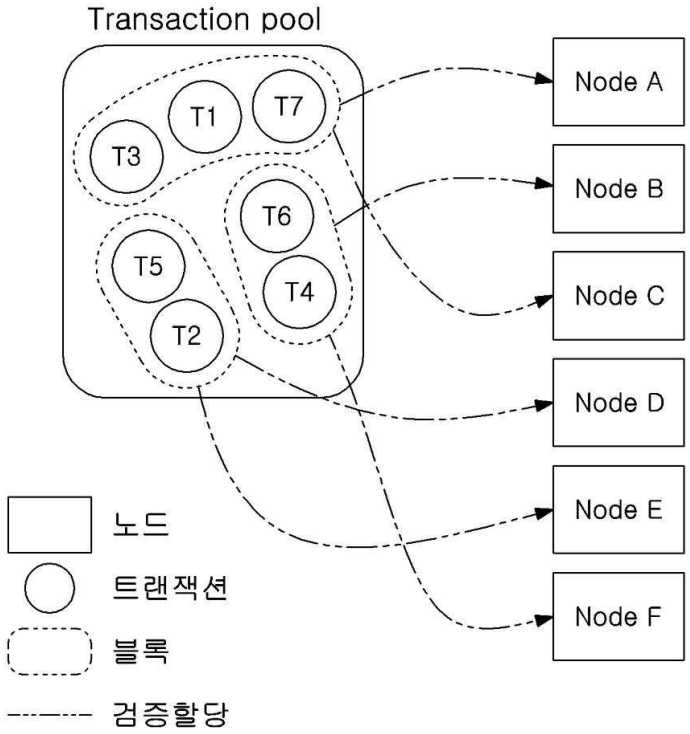
```
Input : prevHash (이전 블록 해시 값)
Output : 할당 블록 여부

1: procedure isAssignedBlock(prevHash)
2:    r1 = rand(prevHash + nodeId);
3:    r2 = SHA256(rand(r1));
4:    r3 = SHA256(nodeId);0
5:    if(r2.substr(38,1) == r3.substr(38,1))
6:       return true;
7:    return false;
```

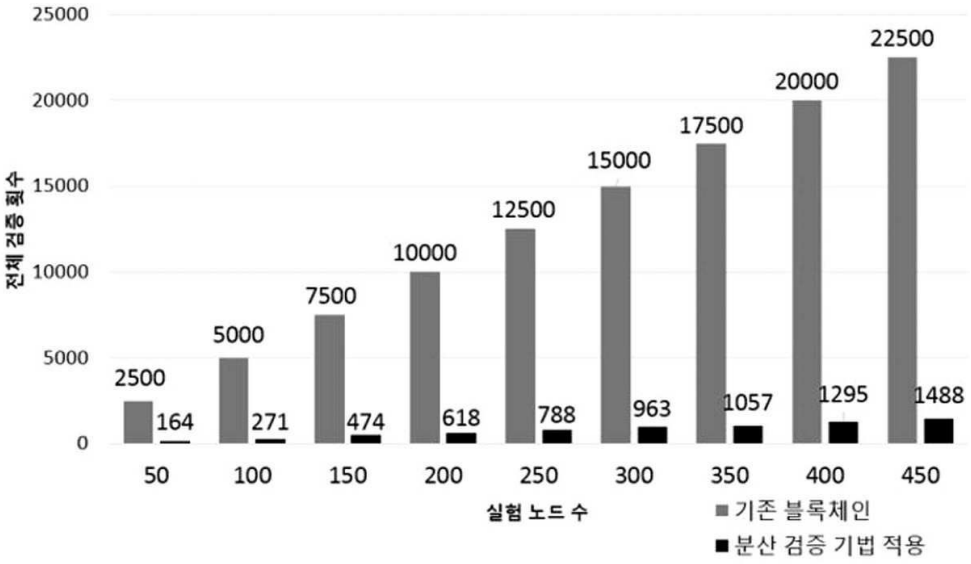
도면4


시작
새로운 블록 수신
S410
이전 블록의 해시값과
자신의 노드ID를 이용하여
무작위 알고리즘 실행
S420
S430
블록 검증 권한
할당?
No
Yes
새로운 블록의 트랜잭션을 검증
S440
검증결과를 네트워크에
전송하여 공유
S450
검증결과 수신
S470
검증결과에 따른 해당 기능 수행
S460
종료

도면5


Transaction pool
T1
T7
T3
T6
T5
T4
T2
Node A
Node B
Node C
Node D
Node E
Node F
노드
트랜잭션
블록
검증할당

도면6


25000
20000
15000
10000
5000
0
전체 검증 횟수
2500
164
5000
271
7500
474
10000
618
12500
788
15000
963
17500
1057
20000
1295
22500
1488
50
100
150
200
250
300
350
400
450
실험 노드 수
기존 블록체인
분산 검증 기법 적용