(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0081533
(43) 공개일자 2020년07월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 29/08* (2006.01)
H04L 9/06 (2006.01)
(52) CPC특허분류
H04L 9/0836 (2013.01)
H04L 67/1097 (2013.01)
(21) 출원번호 10-2018-0170020
(22) 출원일자 2018년12월27일
심사청구일자 2018년12월27일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
조수환
경기도 김포시 김포한강2로 362 616동 1202호 (장기동,청송마을6단지중흥S클래스아파트)
박수용
서울특별시 마포구 독막로 18길 5, 101동 1001호 (상수동, 두산위브아파트)
(74) 대리인
이지연

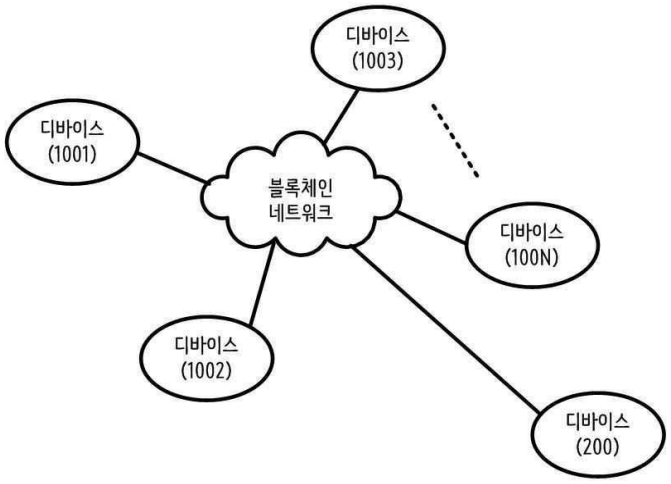
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 **사물 인터넷 환경을 위한 동적 블라인드 투표기반의 블록체인 합의방법**

(57) 요 약

본 발명에 따르는 사물 인터넷 환경을 위한 동적 블라인드 투표기반의 블록체인 합의방법은, 사물 인터넷 환경의 블록체인 네트워크를 구성하는 디바이스들 각각이 트랜잭션 리스트를 이용하여 투표노드를 선출하고, 상기 투표노드인 디바이스로 투표정보를 전송하는 제1단계; 상기 투표정보를 수신받은 디바이스는 블록을 생성하여 상기 블록체인 네트워크를 구성하는 디바이스들로 전파하는 제2단계; 및 상기 전파되는 블록을 수신받은 디바이스들 각각은 상기 블록을 검증하고, 상기 블록이 유효하면 블록체인 저장소에 블록을 연결하여 저장하고, 상기 블록이 유효하지 않으면 상기 블록을 무시하는 제3단계;를 구비함을 특징으로 한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0643 (2013.01)
H04L 2209/38 (2013.01)
H04L 2209/463 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2017-0-00325
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술 진흥 센터
연구사업명 정보통신방송 기술개발 사업
연구과제명 블록체인 기반 IoT 신뢰성 제어 및 관리 기술 개발
기 여 율 1/1
주관기관 달리웍스
연구기간 2017.04.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

사물 인터넷 환경을 위한 동적 블라인드 투표기반의 블록체인 합의방법에 있어서,

사물 인터넷 환경의 블록체인 네트워크를 구성하는 디바이스들 각각이 트랜잭션 리스트를 이용하여 투표노드를 선출하고, 상기 투표노드인 디바이스로 투표정보를 전송하는 제1단계;

상기 투표정보를 수신받은 디바이스는 블록을 생성하여 상기 블록체인 네트워크를 구성하는 디바이스들로 전파하는 제2단계; 및

상기 전파되는 블록을 수신받은 디바이스들 각각은 상기 블록을 검증하고, 상기 블록이 유효하면 블록체인 저장소에 블록을 연결하여 저장하고, 상기 블록이 유효하지 않으면 상기 블록을 무시하는 제3단계;를 구비함을 특징으로 하는 사물 인터넷 환경을 위한 동적 블라인드 투표기반 블록체인 합의 방법.

청구항 2

제1항에 있어서,

상기 투표정보를 수신받은 디바이스로부터 블록을 수신받지 못하거나, 상기 블록이 유효하지 않으면, 상기 디바이스를 실패로 처리하는 단계;를 더 구비함을 특징으로 하는 사물 인터넷 환경을 위한 동적 블라인드 투표기반 블록체인 합의 방법.

청구항 3

제1항에 있어서,

상기 투표정보를 수신받은 디바이스로부터 블록을 수신받지 못하거나, 상기 블록이 유효하지 않으면, 상기 디바이스를 실패로 처리하고, 사물 인터넷 환경의 블록체인 네트워크를 구성하는 디바이스들 각각이 트랜잭션 리스트를 이용하여 투표노드를 선출하고, 상기 투표노드인 디바이스로 재투표정보를 전송하는 단계;

상기 재투표정보를 수신받은 디바이스는 블록을 생성하여 상기 블록체인 네트워크를 구성하는 디바이스들로 전파하는 단계; 및

상기 전파되는 블록을 수신받은 디바이스들 각각은 상기 블록을 검증하고, 상기 블록이 유효하면 블록체인 저장소에 블록을 연결하여 저장하고, 상기 블록이 유효하지 않으면 상기 블록을 무시하는 단계;를 더 구비함을 특징으로 하는 사물 인터넷 환경을 위한 동적 블라인드 투표기반 블록체인 합의 방법.

청구항 4

제1항에 있어서,

상기 디바이스들 각각은 미리 저장된 트랜잭션 리스트를 독출하고,

상기 트랜잭션 리스트를 미리 정해진 수로 쌍을 이루어 SHA 256으로 해쉬화를 하며, 반복적인 해쉬를 통해 머클트리를 생성하고,

상기 머클트리를 이용하여 투표노드를 선정함을 특징으로 하는 사물 인터넷 환경을 위한 동적 블라인드 투표기반 블록체인 합의 방법.

청구항 5

제4항에 있어서,

상기 디바이스들 각각은 미리 저장된 트랜잭션 리스트를 독출하고,

상기 트랜잭션 리스트를 미리 정해진 수로 쌍을 이루어 SHA 256으로 해쉬화를 하며, 반복적인 해쉬를 통해 머클

트리를 생성하고,

상기 머클 트리 루트 해쉬값에 이전 블록해쉬값을 더하여 $Voting_f$(최종 투표 블록 해쉬값)을 생성하고,

상기 $Voting_f$에 모듈러(modular) 연산을 한 후에 1을 더한 후 그 값에 따르는 디바이스를 투표노드로 선정함을 특징으로 하는 사물 인터넷 환경을 위한 동적 블라인드 투표기반 블록체인 합의 방법.

청구항 6

제1항에 있어서,

상기 제2단계가,

상기 투표정보를 수신받은 디바이스는 상기 투표정보를 수신받은 개수에 대응되게 블록 생성 난이도를 결정하고,

상기 블록 생성 난이도에 따라 블록을 생성함을 특징으로 하는 동적 블라인드 투표기반 블록체인 합의 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 사물 인터넷 기술에 관한 것으로, 더욱 상세하게는 네트워크와의 연결 및 해제가 유연하며 저성능의 디바이스들로 구성된 사물 인터넷 환경에서 데이터 무결성을 유지하여 무결성 침해 발생을 일으키는 보안 위협들로부터 신뢰성을 보장할 수 있도록 동적 블라인드 투표기반의 블록체인 합의를 이행하는 사물 인터넷 환경을 위한 동적 블라인드 투표기반의 블록체인 합의방법에 관한 것이다.

배 경 기 술

[0002] 사물 인터넷(Internet of Things)은 사물로 식별할 수 있는 디바이스에 블루투스(bluetooth), Wi-Fi, LTE, Zigbee, NFC 등 다양한 센서와 통신 기능을 내장하여 실시간으로 연결하여 사물과 사물, 사람과 사물 사이의 정보를 주고받는 지능형 기술과 서비스를 의미한다.

[0003] 현재의 사물 인터넷 환경은 수많은 디바이스의 연결 제어, 확장성, 대용량의 데이터 처리, 보안 등의 문제로 클라우드 기반의 중앙 집중형 환경에서 디바이스사이의 연결을 이루는 분산형 환경인 포그, 엣지 컴퓨팅의 형태로 발전하고 있다.

[0004] 그리고 분산된 사물 인터넷 환경에서의 신뢰성 및 보안을 위한 프로토콜로서 블록체인(blockchain)의 기술 적용 가능성도 제시되고 있다. 실제로 IBM에서는 ADET라는 프로젝트로 사물 인터넷 블록체인 개념을 제시하였다. 즉, 인터넷 블록체인 환경으로 사물 디바이스, 클라우드, 컴퓨터 등으로 구성한 블록체인 기반의 사물 인터넷 피어 투 피어(Peer To Peer) 네트워크 환경을 제시하였다.

[0005] 이러한 사물 인터넷 블록체인 환경에서 새롭게 이슈되는 사항은 합의 알고리즘이다. 블록체인 합의 알고리즘은 분산된 환경에서 노드들이 위변조되지 않는 동일한 거래내역(블록)을 유지할 수 있도록 한다. 그러나 종래의 합의 알고리즘들은 전자화폐 시스템을 기반으로 개발되어 있어 사물 인터넷 환경에 적용시 많은 문제들이 내재되어 있었다.

[0006] 좀더 설명하면, 사물 인터넷 환경에서의 합의 알고리즘의 문제는 다음과 같다.

[0007] <디바이스의 네트워크 연결실패>

[0008] 먼저, 사물 인터넷 환경은 무선 네트워크의 환경, 디바이스의 교체, 이동형 환경으로 인해 디바이스의 네트워크 연결이 끊어지는 경우가 있으며, 이와같이 디바이스의 네트워크의 연결이 끊어지는 경우에도 합의 알고리즘은 수행되어야 하는 문제가 있었다.

[0009] <저성능 디바이스에서의 가용성>

[0010] 그리고 사물 인터넷 환경은 저성능의 디바이스로 이루어져 있다. 이러한 저성능의 디바이스는 합의 알고리즘을 수행하기 위해 높은 연산을 수행하는 데에는 한계가 있었다.

[0011] <트랜잭션 처리속도>

[0012] 또한 사물 인터넷 환경은 많은 양의 데이터 처리와 측정된 데이터를 기반으로 디바이스의 제어를 이행하므로 높은 트랜잭션 처리율이 요구되었다.

[0013] <데이터의 무결성>

[0014] 또한 사물 인터넷으로 구성된 블록체인 네트워크 환경에서 합의 알고리즘은 악의적인 공격자로부터의 데이터 위변조 시도에도 데이터 무결성을 유지할 수 있어야 한다.

[0015] 이와 같이 종래에는 네트워크와의 연결 및 해제가 유연하며 저성능의 디바이스들로 구성된 사물 인터넷 환경에서 데이터 무결성을 유지하여 무결성 침해 발생을 일으키는 보안 위협들로부터 신뢰성을 보장할 수 있는 합의 알고리즘의 개발이 절실하게 요망되었다.

선행기술문헌

특허문헌

[0016] (특허문헌 0001) 한국특허등록 제10-1887894호

(특허문헌 0002) 한국특허공개 제10-2018-0095260호

(특허문헌 0003) 한국특허등록 제10-1678795호

발명의 내용

해결하려는 과제

[0017] 본 발명은 네트워크와의 연결 및 해제가 유연하며 저성능의 디바이스들로 구성된 사물 인터넷 환경에서 데이터 무결성을 유지하여 무결성 침해 발생을 일으키는 보안 위협들로부터 신뢰성을 보장할 수 있도록 동적 블라인드 투표기반의 블록체인 합의를 이행하는 사물 인터넷 환경을 위한 동적 블라인드 투표기반의 블록체인 합의방법을 제공하는 것을 그 목적으로 한다.

과제의 해결 수단

[0018] 상기한 목적을 달성하기 위한 본 발명에 따르는 사물 인터넷 환경을 위한 동적 블라인드 투표기반의 블록체인 합의방법은, 사물 인터넷 환경의 블록체인 네트워크를 구성하는 디바이스들 각각이 트랜잭션 리스트를 이용하여 투표노드를 선출하고, 상기 투표노드인 디바이스로 투표정보를 전송하는 제1단계; 상기 투표정보를 수신받은 디바이스는 블록을 생성하여 상기 블록체인 네트워크를 구성하는 디바이스들로 전파하는 제2단계; 및 상기 전파되는 블록을 수신받은 디바이스들 각각은 상기 블록을 검증하고, 상기 블록이 유효하면 블록체인 저장소에 블록을 연결하여 저장하고, 상기 블록이 유효하지 않으면 상기 블록을 무시하는 제3단계;를 구비함을 특징으로 한다.

발명의 효과

[0019] 본 발명은 네트워크와의 연결 및 해제가 유연하며 저성능의 디바이스들로 구성된 사물 인터넷 환경에서 디바이스들이 동적 블라인드 투표기반의 블록체인 합의를 이행하여 네트워크에 참여한 디바이스들의 블록기록을 가능하게 하여 데이터 무결성을 유지하여 무결성 침해 발생을 일으키는 보안 위협들로부터 신뢰성을 보장할 수 있게 하는 효과를 야기한다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들을 도시한 도면.

도 2는 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스 참여과정을 도시한 도면.

도 3은 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스 참여를 위한 알고리즘을 예시한 도면.

도 4는 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들의 투표 협의 과정을 도시한 도면.

도 5는 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들의 투표 협의를 위한 알고리즘을 예시한 도면.

도 6은 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들의 재투표 협의 과정을 도시한 도면.

도 7은 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들의 재투표 협의를 위한 알고리즘을 예시한 도면.

발명을 실시하기 위한 구체적인 내용

[0021] 본 발명의 설명에 앞서 몇가지 관련 기술에 대해 설명한다.

[0022] 먼저, 작업 증명(POW:Proof of work)은 블록생성을 하고자 하는 노드들이 특정한 해쉬값(Nonce)값을 찾는 연산을 수행하여 작업을 수행했음을 증명하는 합의 방법이다. 이는 높은 연산을 통해 악의적인 공격자에게 기회 비용을 들이고, 가장 긴 블록체인(longest blockchain)을 채택한다.

[0023] 그리고 지분 증명(Proof of stake) 방식은 참여자의 소유 지분(stake)이 블록생성 권한에 반영되는 알고리즘을 말한다. 상기 지분증명 방식은 블록생성 및 검증의 역할을 하는 검증자(Validator)가 되기 위해 자신이 보유하고 있는 암호화폐를 보증금의 형태로 락업하는 특별한 거래(Special Transaction)를 한다. 그 이후에는 새로운 블록을 생성하고 검증하는 절차는 모든 검증자(Validator)가 참여할 수 있도록 하는 특정 '합의 알고리즘(Consensus Algorithm)'에 의해 이루어진다. 여기서 특정 합의 알고리즘은 'Chain-based proof of stake','BFT Style poof of stake' 등이 있다.

[0024] 그리고 PBFT(Practical Byzantine fault tolerance)는 비잔틴 장군문제를 해결하기 위한 실질적인 프로토콜이다. 이는 시스템의 실패, 악의적인 노드가 있음에도 불구하고 전체 시스템이 안정적으로 동작하도록 하는 프로토콜로서, 리플리카 중 의사결정의 리더 역할을 하는 프라이머리 노드(Primary node)가 있으며 두번의 메시지 브로드캐스팅을 통해 다수의 의결을 모은다.

[0025] 본 발명은 저성능의 디바이스 환경을 고려한 투표 기반의 알고리즘을 제안한다. 이는 다수의 의결을 모으기 위해 블록체인 내역기반의 해쉬값과 트랜잭션들을 사용하며, 선출된 디바이스의 추적을 방지하기 위해 동적 블라인드 투표 방식을 제안한다.

[0026] 또한 본 발명은 네트워크 지연 및 연결 실패에 의한 블록 합의 실패가 일어났을 때를 위해 피기백(piggy-back) 형식의 재투표 블라인트 블록 합의 기능을 포함한다.

[0027] 또한 본 발명에서는 서명 검증을 위한 ECDSA(secp 2561 kl kurve), 해쉬화를 위한 SHA 256, 머클트리(Merkle tree)를 이용한다.

[0028] 본 발명에 따르는 알고리즘을 설명하기 위한 표기법은 아래의 표 1과 같다.

표 1

Notation	Description
Pk^{n}_{sig} ,Sk^{n}_{sig}	n's verify key , n's signing key / n 의 검증키, n 의 서명키
PIBN	Private internet of thigns block chain network /사물 인터넷 디바이스로 구성되는 사설 블록 체인 네트워크
$(G_{sig},S_{sig},V_{sig})$	Digital signature schems DSS described by the 3-tuple generator, signature, verification / 생성자, 서명, 검증으로 구성되는 디지털 서명 스킴(DSS)
bn	block chain nodes / 블록체인 노드들
$D_{Info}{}^{n}$	n's device info / 디바이스 n 의 정보
NMP	Node mapping table-node index number, device info (uuid, mac address, pk_{sig}), network status / 노드 맵핑 테이블 - 노드 인덱스 번호, 디바이스정보, 네트워크 상태
$Block_{GC}$	BlockGenerateCondition / 블록 생성 조건
$Voting_{f}$	final voting block hash / 최종 투표 블록 해쉬
$Voting_{n}$	voting number / 투표 수
$Voting_{m}$	voting message / 투표 메시지
$Voting_{v}$	voting validation / 투표 확인
bgn	block generate node / 블록 생성 노드

[0029]

[0030] 이제 상기한 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경을 위한 동적 블라인드 투표기반의 블록체인 합의방법을 도면을 참조하여 상세히 설명한다.

[0031] <사물 인터넷 환경의 디바이스들의 구성>

[0032] 도 1은 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들을 도시한 도면이다. 상기 사물 인터넷 환경의 디바이스들(1001~100N)은 블록체인 네트워크를 구성하며, 상기한 블록체인 네트워크에는 새로운 디바이스(200)가 참여할 수도 있다.

[0033] 상기 디바이스들(1001~100N,200)은 동작 블라인드 투표 방식으로 어느 한 디바이스를 선출하고, 선출된 디바이스는 투표결과에 따라 블록생성 난이도를 설정하고, 블록생성 난이도에 따라 블록을 생성하여 다른 디바이스들로 전파한다. 상기 블록을 수신한 디바이스는 블록에 대한 검증을 이행하고 해당 블록을 내부의 블록체인 저장소에 저장한다.

[0034] 또한 상기 디바이스들(1001~100N,200)은 선출된 디바이스가 블록을 전파하지 않거나, 수신된 블록이 유효하지 않은 블록이면 해당 디바이스를 실패노드로 처리하고 재투표를 이행한다.

[0035] <사물 인터넷 환경의 디바이스 참여과정>

[0036] 이제 사물 인터넷 환경의 디바이스들(1001~100N)이 구성하는 블록체인 네트워크에 새로운 디바이스가 참여하는 네트워크 프리비저닝 과정을 설명한다. 도 2는 블록체인 네트워크에 새로운 디바이스가 참여하는 네트워크 프리비저닝 과정을 나타낸 것이고, 도 3은 블록체인 네트워크에 새로운 디바이스가 참여하는 네트워크 프리비저닝 알고리즘을 예시한 것이다.

[0037] 먼저, 상기 사물 인터넷 환경의 디바이스들은 합의 검증과 커뮤니케이션을 위한 노드 매핑 테이블을 저장하고 이를 관리한다. 상기 노드 매핑 테이블은 표 2에 도시한 바와 같이 노드의 인덱스 숫자와 디바이스에 대한 식별정보, 맥주소, 검증키, 해당 노드의 네트워크 연결 상태로 구성된다.

표 2

[0038]

Key	Value
Index	Node index number
Device info	uuid, mac address, pk_{sig}
Network Status	Normal or Falut

[0039] 상기 도 2 및 도 3을 참조하면, 상기 네트워크에 참여하는 디바이스(200)는 ECDSA(2561kl kurve)를 사용하여 키쌍(서명키, 검증키)를 생성하고(300단계), 고유 식별값 및 맥주소, 노드의 검증키로 구성되는 네트워크 참여정보를 상기 네트워크에 전파한다(302단계). 상기 네트워크의 디바이스들은 수신받은 네트워크 참여정보를 노드 매핑 테이블에 기록하여 저장한다(304,306단계). 이로서 합의를 위한 네트워크 프리비저닝이 완료된다.

[0040] <사물 인터넷 환경을 위한 동적 블라인드 투표기반의 블록체인 합의과정>

[0041] 이제 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경을 위한 동적 블라인드 투표기반의 블록체인 합의과정을 설명한다. 도 4는 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들의 투표 협의 과정을 도시한 도면이고, 도 5는 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들의 투표 협의를 위한 알고리즘을 예시한 도면이다.

[0042] 상기 도 4 및 도 5를 참조하면, 상기 네트워크를 구성하는 디바이스들 각각은 블록생성 조건을 확인하며, 이는 트랜잭션의 개수, 블록의 크기(일정 트랜잭션의 용량)에 의해 블록생성 조건이 만족되는지 확인한다(400단계).

[0043] 이후 상기 디바이스들 각각은 미리 저장된 트랜잭션 리스트를 독출하고, 상기 트랜잭션 리스트를 짝수개의 쌍을 이루어 SHA 256으로 해쉬화를 하며, 반복적인 해쉬를 통해 머클트리를 완성한다(402,404단계). 여기서, 머클트리의 특징에 따르면 모든 노드가 똑같은 트랜잭션을 가지고 있다면, 머클트리 루트 값은 모든 노드가 같다. 이에 악의적인 공격자가 트랜잭션을 위변조하게 되면, 머클트리 루트 해쉬값이 틀려지게 된다.

[0044] 이후 상기 디바이스들 각각은 상기 머클 트리 루트 해쉬값에 이전 블록해쉬값을 더하여 $Voting_f$(최종 투표 블록 해쉬값)을 생성한다(406단계).

[0045] 상기한 $Voting_f$에 모듈러(modular) 연산을 하여 1을 더한 후 그 값에 따르는 디바이스를 $Voting_n$, 즉 투표노드로 설정한다(408단계). 이후 상기 디바이스들 각각은 $Voting_n$에 해당하는 디바이스에게 개인키로 서명한 후 투표정보를 전송한다(410단계).

[0046] 상기 투표노드인 디바이스는 다른 디바이스들로부터의 투표정보를 제공받아 투표결과가 유효한지를 체크하고, 상기 투표결과에 따라 블록 생성 난이도를 결정한다(412,414단계). 여기서, 다른 노드로부터 한표라도 받게 되면, 블록을 생성하며, 유효성 검증은 표를 받았는지 해당 투표의 서명검증을 했는지 여부에 따라 결정된다.

[0047] 상기 블록 생성 난이도는 투표결과에 대응되게 결정되며 다수의 투표를 받은 디바이스는 빠른 블록을 생성하고 적게 투표를 받은 디바이스는 느리게 블록을 생성할 수 있게 한다. 악의적인 노드가 데이터의 위변조를 시도할 때에는 전체 네트워크의 51%이상을 위변조해야 가능하다.

[0048] 상기의 블록 생성 난이도가 결정되면, 상기 디바이스는 상기 블록 생성 난이도에 따라 블록을 생성하고, 생성된 블록을 네트워크의 디바이스들로 전파한다(416,418단계).

[0049] 상기 네트워크의 나머지 디바이스들은 블록이 수신되면(420단계), 수신된 블록을 검증하여 블록이 유효하면 수신된 블록을 이전 블록에 연결하여 블록체인 저장소에 저장한다(422,424,426단계). 이와 달리 블록이 유효하지 않으면 상기 네트워크의 나머지 디바이스들은 수신된 블록을 무시하고(428단계) 재투표 절차를 이행한다(430단계). 또한 미리 정해둔 시간이상 블록이 수신되지 않는다면 상기 네트워크의 나머지 디바이스들은 재투표 절차를 수행한다(430단계).

[0050] <사물 인터넷 환경을 위한 동적 블라인드 재투표기반의 블록체인 합의과정>

[0051] 이제 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경을 위한 동적 블라인드 재투표기반의 블록체인 합의과정을 설명한다. 여기서, 본 발명에서 합의 실패에 대한 경우는 블록 전파 실패(노드의 충돌, 네트워크 연결 문제)와 블록 생성 노드가 악의적인 공격자인 경우이므로, 합의 실패에 대한 재투표 합의를 수행하며, 상기 재투표 합의 방식에는 피기백(Piggy-back) 흐름 제어 방식을 사용한다.

[0052] 도 6은 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들의 재투표 협의 과정을 도시한 도면이며, 도 7은 본 발명의 바람직한 실시예에 따르는 사물 인터넷 환경의 디바이스들의 재투표 협의를 위한 알고리즘을 예시한 도면이다.

[0053] 상기 도 6 및 도 7을 참조하면, 상기 네트워크를 구성하는 디바이스들 각각은 블라인드 재투표가 요청되면 블록생성 조건을 확인하며, 이는 트랜잭션의 개수, 블록의 크기(일정 트랜잭션의 용량)에 의해 블록생성 조건이 만족되는지 확인한다(500,502단계).

[0054] 이후 상기 디바이스들 각각은 이전에 선출했던 투표노드인 디바이스를 실패로 변환하고 새로운 디바이스를 선출한다(504단계). 상기 디바이스들 각각은 미리 저장된 트랜잭션 리스트를 독출하고, 상기 트랜잭션 리스트를 짝수개의 쌍을 이루어 SHA 256으로 해쉬화를 하며, 반복적인 해쉬를 통해 머클트리를 완성한다(506,508단계). 여기서, 머클트리의 특징에 따르면 모든 노드가 똑같은 트랜잭션을 가지고 있다면, 머클트리 루트 값은 모든 노드가 같다. 이에 악의적인 공격자가 트랜잭션을 위변조하게 되면, 머클트리 루트 해쉬값이 틀려지게 된다.

[0055] 이후 상기 디바이스들 각각은 상기 머클 트리 루트 해쉬값에 이전 블록해쉬값을 더하여 $Voting_f$(최종 투표 블록 해쉬값)을 생성한다(510단계).

[0056] 상기한 $Voting_f$ 에 모듈러(modular) 연산을 한 후에 1을 더한 후 그 값에 따르는 디바이스를 $Voting_n$, 즉 투표노드로 설정한다(512단계). 이후 상기 디바이스들 각각은 $Voting_n$에 해당하는 디바이스에게 개인키로 서명한 후 투표정보를 전송한다(514단계).

[0057] 상기 투표노드인 디바이스는 다른 디바이스들로부터의 투표정보를 제공받아 투표결과가 유효한지를 체크하고, 상기 투표결과에 따라 블록 생성 난이도를 결정한다(516,518단계). 상기 블록 생성 난이도는 투표결과에 대응되게 결정되며 다수의 투표를 받은 디바이스는 빠른 블록을 생성하고 적게 투표를 받은 디바이스는 느리게 블록을 생성할 수 있게 한다. 악의적인 노드가 데이터의 위변조를 시도할 때에는 전체 네트워크의 51%이상을 위변조해야 가능하다. 또한 블록체인 네트워크에서의 51% 이상의 다수의 정직한 노드가 존재할 때에 무결성은 유지되며,

악의적인 공격자(malicious node) 데이터 위변조시 머클트리를 이용한 투표결과가 다르게 나타낸다. 51% 이상의 정직한 노드가 존재한다고 했을 때에 악의적인 노드(소수)가 적은 투표를 받게 되고 적은 투표는 블록 생성 난이도가 올라가게 되어 위변조된 블록 생성을 억제한다.

[0058] 상기의 블록 생성 난이도가 결정되면, 상기 디바이스는 상기 블록 생성 난이도에 따라 블록을 생성하고, 생성된 블록을 네트워크의 디바이스들로 전파한다(520,522단계).

[0059] 상기 네트워크의 나머지 디바이스들은 블록이 수신되면(524단계), 수신된 블록을 검증하여 블록이 유효하면 수신된 블록을 이전 블록에 연결하여 블록체인 저장소에 저장한다(526,528,530단계). 이와 달리 블록이 유효하지 않으면 상기 네트워크의 나머지 디바이스들은 수신된 블록을 무시하고(532단계) 재투표 절차를 이행한다(534단계). 또한 미리 정해둔 시간이상 블록이 수신되지 않는다면 상기 네트워크의 나머지 디바이스들은 재투표 절차를 수행한다(534단계).

[0060] 이제 본 발명의 바람직한 실시예에 따르는 합의 알고리즘에 대한 안정성과 성능 분석을 이행한 결과를 설명한다.

[0061] <디바이스의 네트워크 연결실패>

[0062] 본 발명은 노드 매핑 테이블을 통한 디바이스들의 상태 체크와 피기백 흐름 제어 방식을 통하여, 사물 인터넷 환경에서 디바이스가 네트워크 연결 실패에 대해 제어한다. 또한 디바이스가 네트워크 연결에 실패하여도 네트워크 전체의 블록 합의는 최종적으로 이루어질 수 있게 한다.

[0063] <저성능 디바이스에서의 가용성>

[0064] 또한 본 발명은 사물 인터넷 환경의 디바이스들 각각이 블록의 분산원장내역과 트랜잭션 내용을 기반으로 투표를 하고 투표 결과에 따라 블록을 생성하여 합의를 이행한다. 또한 투표의 메시지 교환 방식과 선의적인 노드는 블록의 생성 난이도가 낮게 주어지게 때문 저성능 디바이스에서의 가용성은 높다.

[0065] <비잔틴 장군문제와 데이터의 무결성>

[0066] 또한 사물 인터넷 환경의 블록체인 네트워크 상태에서 비잔틴 장군문제는 블록체인 네트워크내 악의적인 노드가 있을 때 올바른 다수의 의결을 모을 수 있게 한다.

[0067] 또한 본 발명은 각 노드가 독립적으로 투표를 진행한다. 이는 어떤 노드가 선출될지 모르는 블라인드 방식이기 때문에 악의적인 노드로부터 추적성에 의한 공격을 막을 수 있다. 또한 투표로부터 선출된 노드는 다수의 의결을 받는 노드이고, 블록 생성의 조건 또한 쉽게 주어진다. 악의적인 노드는 표를 받지 못하거나, 소수의 표를 얻기 때문에 블록 생성을 억제받게 된다. 이는 결국 다수의 의결은 받은 블록으로 합의가 이루어진다. 또한 악의적인 노드가 선출된 경우에도 재투표를 통하여 의결이 무시된다.

[0068] 또한 본 발명에 따르는 합의 알고리즘은 악의적인 노드가 F개일때 F+1(51%이상의)개의 노드가 존재한다면 데이터의 무결성이 유지된다.

[0069] <트랜잭션 처리속도>

[0070] 본 발명의 트랜잭션 처리속도를 특정하기 위해 다음과 같은 환경에서의 실험을 진행하였다. 즉, "블록체인 기반의 IoT 신뢰성 제어 시스템 제어개발 프로젝트"에서 개발한 블록체인 플랫폼인 Logchain에 본 발명의 합의 알고리즘을 적용하였다. 상기 Logchain은 사물인터넷 환경에 고도화된 블록체인 플랫폼이다. 실험환경은 사물 인터넷 환경의 블록체인 네트워크로 구성된, 사물 디바이스 5대(라즈베리 파이 5대), 클라우드 노드 2대(윈도우 하이퍼v 2대), PC노드 10대로 구성하였다. 그리고 처리속도를 측정하기 위하여 한블록당 트랜잭션 30건에 대하여 트랜잭션 처리건수와 블록 생성 속도를 측정하였다. 상기한 실험환경을 구성한 후에, 블록생성 조건을 트랜잭션 30건에 대하여 총 10번의 블록생성을 실험했을시, 평균 트랜잭션 처리건수 초당 3155건, 평균 블록 생성기간 0.02900 Sec이었다. 이는 다른 블록체인 합의를 적용한 속도보다 높은 수치이며, 블록 생성 조건의 트랜잭션 건수를 늘리게 되면 더 높은 수치를 보여줄 것으로 기대된다.

[0071] 이와 같이 본 발명은 사물 인터넷 환경을 고려한 블록체인 합의 알고리즘을 제시하였다. 종래의 전자 화폐 합의 알고리즘과 달리 사물 인터넷 환경에서는 디바이스의 네트워크 연결 실패, 저성능 디바이스에서의 가용성, 높은 트랜잭션 처리속도를 만족하면서도 비잔틴 장군 문제 해결과 사물인터넷 데이터 무결성 보장을 해야 한다. 본 발명은 분산 원장 내역 기반으로 투표를 하여 블라인드 투표 방식을 제안하였고, 선출된 디바이스는 투표결과에 따라 블록생성 조건을 다르게 한다. 이는 악의적인 디바이스의 추적성을 없애고, 블록 생성을 억제시킨다. 또

한 디바이스의 실패를 고려하여 노드 매핑 테이블을 통해 네트워크 상태를 체크하고, 재투표를 통한 합의를 가능하게 했다.

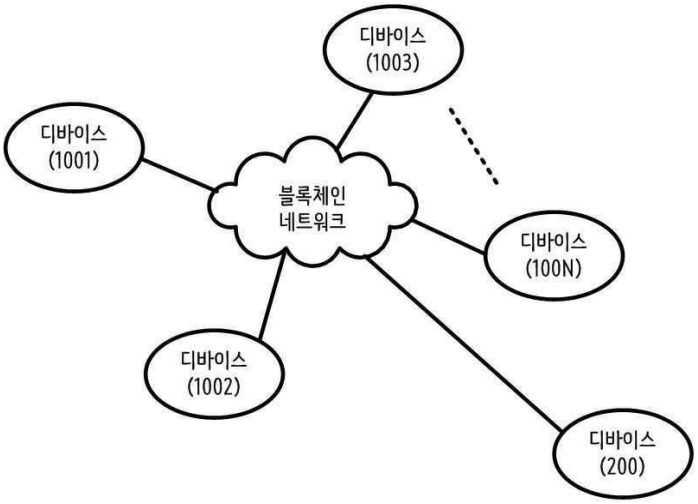
[0072] 이러한 본 발명은 합의 알고리즘을 바탕으로 사물 인터넷 환경에서 데이터 무결성을 유지하여 무결성 침해 발생을 일으키는 보안 위협들로부터 신뢰성을 보장할 것이다.

부호의 설명

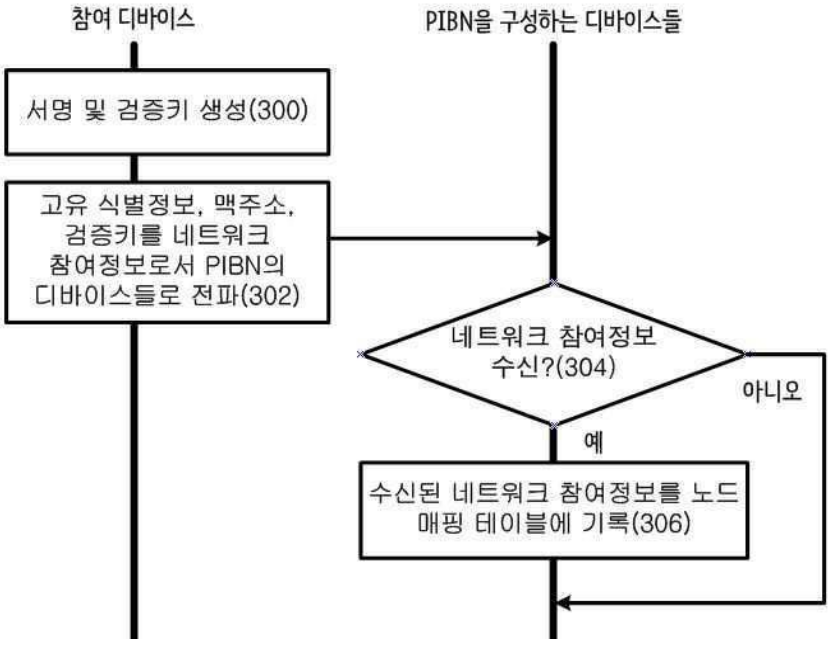
[0073] 1001~100N, 200 : 디바이스들

도면

도면1



도면2

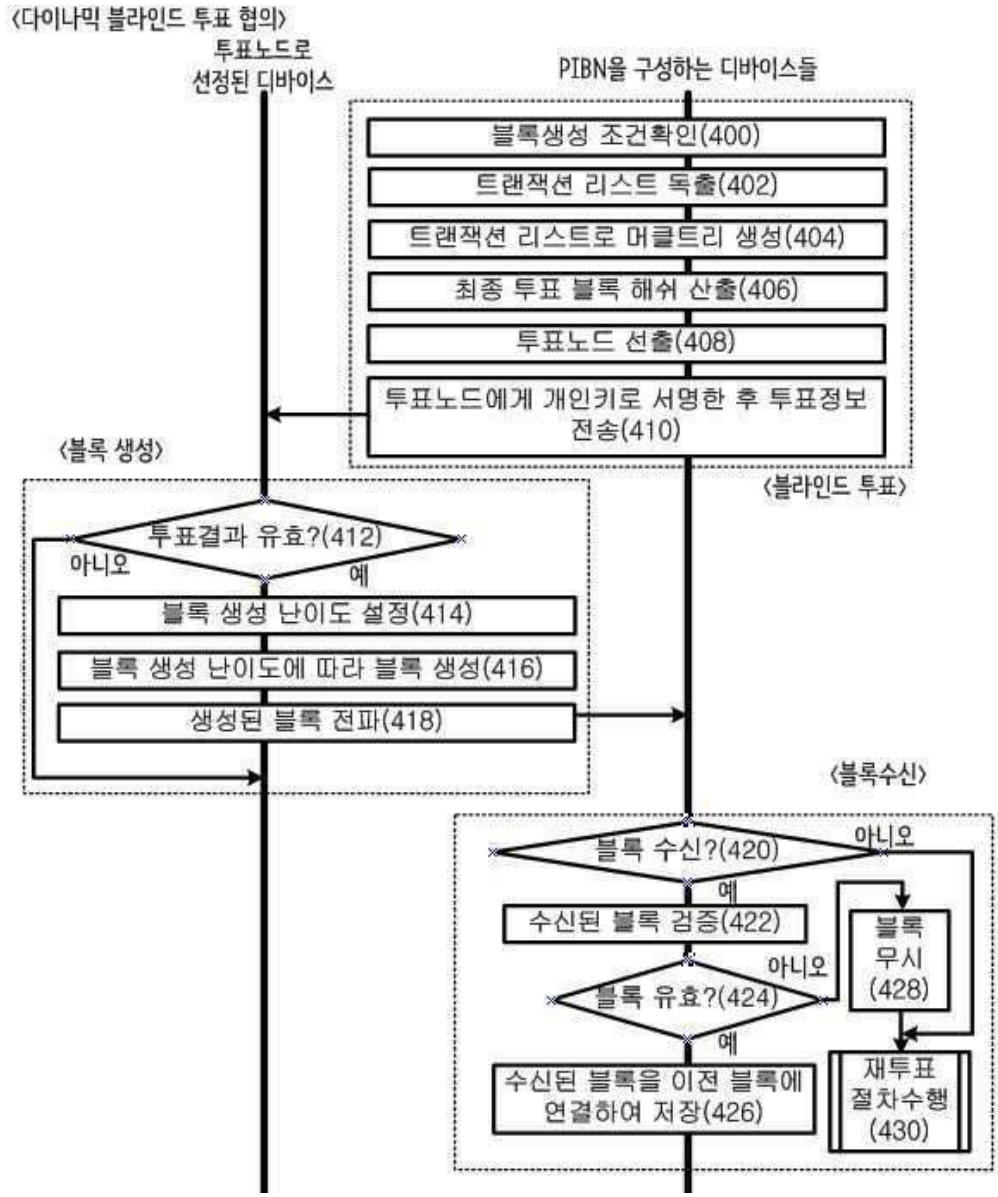


도면3

Consensus Algorithm 1 NetworkPrivisioing

1: **procedure** NetworkPrivisioning
2: bn executes :
3: $(Pk^{bn}_{sig,}, Sk^{bn}_{sig}) \leftarrow G_{sig}()$
4: $D_{info}{}^{n} = (uuid, mac\ address, Pk^{bn}_{sig})$
broadcast to PIBN
5: update to NMP($D_{info}{}^{n}$)
6: **end procedure**

도면4



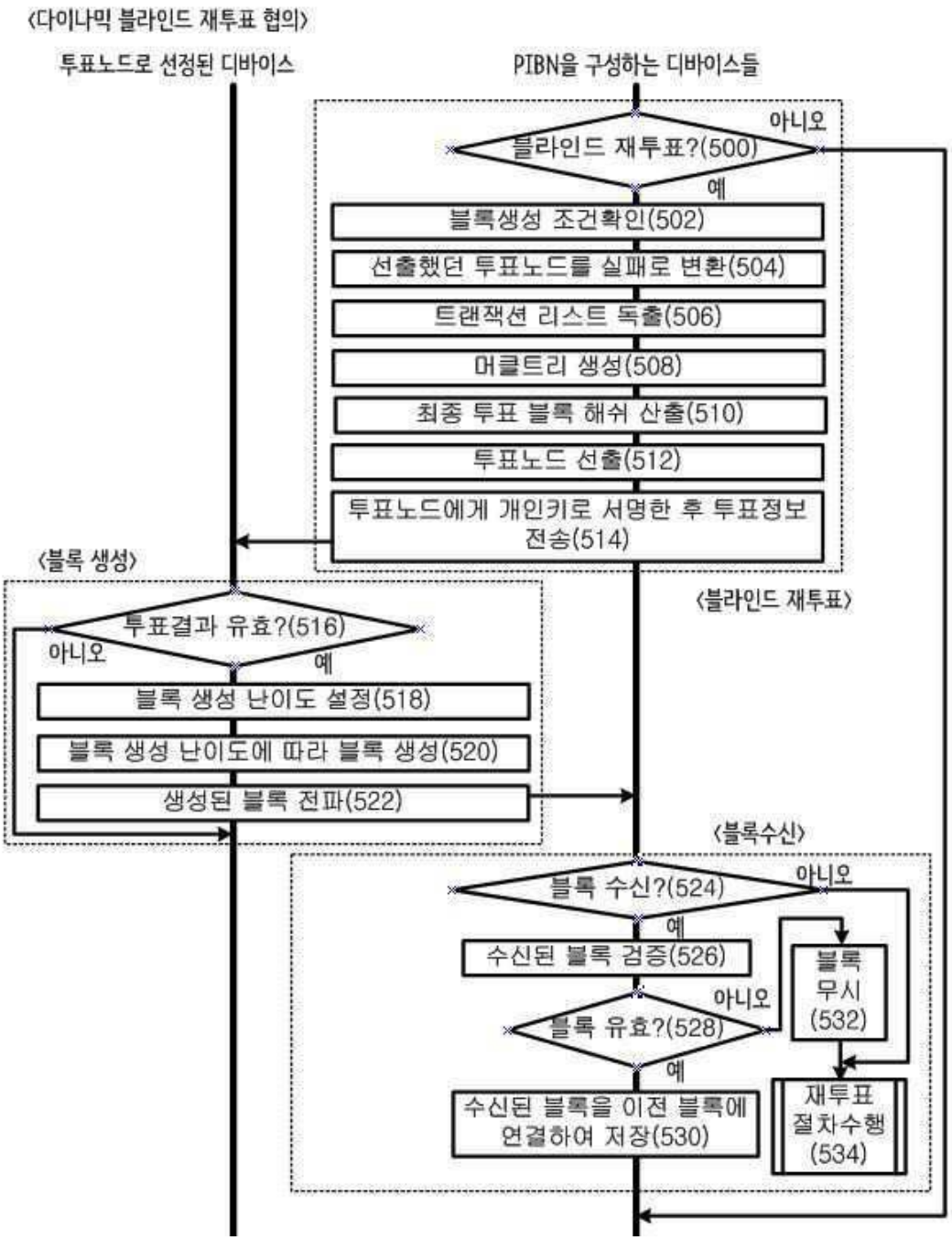
도면5

<DynamicBlindVotingConsensus>

Consensus Algorithm2 DynamicBlindVotingConsensus

```
1: procedure DynamicBlindVotingConsensus
2: bn executes:
4:   if Block_GC is valid:
3:     open := transaction list
4:     call module Merkleroothash[transactionlist]
5:     Voting_f = SHA 256 (Merkle root hash +
                  last block hash)
6:     Voting_n  =  (Voting_f Modular PeerNum) + 1
7:     Send  Voting_n <-S_sig(Sk^n_sig) to peer[Voting_n]
8:       if Voting_v is valid:
9:                    then  difficulty  =  call  module
SetDifficulty(Voting_v)
10:        target value = 2**(difficulty)
11:         while find nonce :
12:          if new block receive from other peer then
13:            Call module VerifyBlock(block)
14:                        break;
15:          else SHA 256 (block info + nonce) < targe
                          value then
16:              block hash = SHA256(block info + nonce)
17:                        return block
18: end procedure
```

도면6


〈다이나믹 블라인드 재투표 협의〉
투표노드로 선정된 디바이스
PIBN을 구성하는 디바이스들
아니오
블라인드 재투표?(500)
예
블록생성 조건확인(502)
선출했던 투표노드를 실패로 변환(504)
트랜잭션 리스트 독출(506)
머클트리 생성(508)
최종 투표 블록 해쉬 산출(510)
투표노드 선출(512)
투표노드에게 개인키로 서명한 후 투표정보 전송(514)
〈블라인드 재투표〉
〈블록 생성〉
투표결과 유효?(516)
아니오
예
블록 생성 난이도 설정(518)
블록 생성 난이도에 따라 블록 생성(520)
생성된 블록 전파(522)
〈블록수신〉
블록 수신?(524)
아니오
예
수신된 블록 검증(526)
블록 유효?(528)
아니오
예
블록 무시 (532)
수신된 블록을 이전 블록에 연결하여 저장(530)
재투표 절차수행 (534)

도면7

<Re-voting for Consensus Failure>

Consensus Algorithm3 Re-voting for Consensus Failure

```
1: procedure Re-voting for Consensus Failure
2: bn executes :
3:   if Block_CC is valid:
4:    if block is not received or block is not valid :
5:          set network status is fault where index by
              previous bgn
6:    open := transaction list +previous transaction list
7:    call module Merkleroothash[transaction list
                +previous transaction list ]
8:    Voting_r = SHA 256 (Merkle root hash + last block
                hash)
9:    Voting_n = (Voting_r Modular PeerNum) + 1
10:   if peer[Voting_n] = network status is fault :
11:       Voting_n = Voting_n where network status is
normal
12:    Send Voting_n <-S_sig(Sk^n_sig) to peer[Voting_n]
13:      if Voting_v is valid:
14:        then difficulty = call module
                              SetDifficulty(Voting_v)
15:       target value = 2**(difficulty)
16:        while find nonce :
17:         if new block receive from other peer then
18:              Call module VerifyBlock(block)
19:                  break;
20:         else SHA 256 (block info + nonce) < target
                  value then
21:              block hash = SHA256(block info + nonce)
22:                  return block
```