(19) 대한민국 지식재산처(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2025년11월28일
(11) 등록번호 10-2891812
(24) 등록일자 2025년11월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2022.01)
(52) CPC특허분류
H04L 9/50 (2022.05)
(21) 출원번호 10-2023-0001142
(22) 출원일자 2023년01월04일
심사청구일자 2023년01월04일
(65) 공개번호 10-2024-0031858
(43) 공개일자 2024년03월08일
(30) 우선권주장
1020220110964 2022년09월01일 대한민국(KR)
(56) 선행기술조사문헌
[Arthur Gervais 외 5명. "On the Security and Performance of Proof of Work Blockchains." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016.](2016.10.24)*
[Lin Liu 외 6명. "A recursive reinforced blockchain performance evaluation and improvement architecture: maximising diversity to improve scalability." International Journal of Communication Systems (2022): e5315.](2022.08.22)*
[Xiaoliang Wu 외 2명. "Virtual-Time-Accelerated Emulation for Blockchain Network and Application Evaluation." Proceedings of the 2019 ACM SIGSIM Conference on Principles of Advanced Discrete Simulation. 2019.](2019.06.05)*
KR1020200059234 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
경기대학교 산학협력단
경기도 수원시 영통구 광교산로 154-42 (이의동, 경기대학교)
(72) 발명자
김도훈
대전광역시 유성구 지족북로 33, 106동 304호(지족동, 한화꿈에그린 1블럭)
김희상
경기도 용인시 수지구 신봉2로 115-20(신봉동)
(74) 대리인
특허법인 신지

전체 청구항 수 : 총 20 항 심사관 : 홍기완

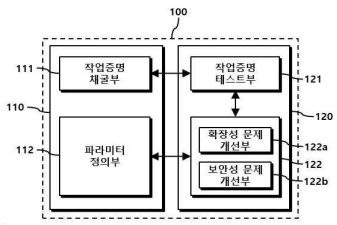
(54) 발명의 명칭 **작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치 및 방법**

(57) 요 약

본 발명은 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치 및 방법에 관한 것으로, 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 퍼블릭 블록체인 메인넷의 태생적으로 낮은 확장성

(뒷면에 계속)

대 표 도 - 도1



(Scalability) 문제를 개선함으로써 블록 생성 속도와 블록 전파 비율의 관계와 보안성을 유지하면서도 확장성(Scalability)을 높일 수 있도록 한 것이다.

이 발명을 지원한 국가연구개발사업

과제고유번호	1415177456
과제번호	P0008691
부처명	산업통상자원부
과제관리(전문)기관명	한국산업기술진흥원
연구사업명	산업혁신인재성장지원(R&D)
연구과제명	산업인공지능 전문인력 양성
기 여 율	1/1
과제수행기관명	한국전자기술연구원
연구기간	2021.03.01 ~ 2021.12.31

공지예외적용 : 있음

명 세 서

청구범위

청구항 1

탈중앙화(Decentralization)에 장점이 있는 퍼블릭 블록체인 메인넷(Public Blockchain Main Net)과 유사한 테스트넷(Test Net)을 구성하는 테스트넷 처리부와;

테스트넷 처리부에 의해 구성된 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 퍼블릭 블록체인 메인넷의 태생적으로 낮은 확장성(Scalability) 문제를 개선할 수 있는 최적의 합의 조건을 도출하는 최적 합의 분석부를;

포함하되,

최적 합의 분석부가:

최적의 합의 조건 도출에 필요한 파라미터(Parameter)들을 정의하고, 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 정의된 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들의 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 2

제 1 항에 있어서,

테스트넷 처리부가:

테스트넷 상에서 블록 생성 속도(Block Interval)로 블록(Block)들을 반복 채굴(Mining)하여, 블록(Block)들이 체인(Chain) 형태로 연결되는 합의(Consensus) 과정을 수행하는 작업증명 채굴부를;

포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 3

제 2 항에 있어서,

테스트넷은:

높은 탈중앙화의 전제조건으로 충분히 많은 노드가 뒷받침되어, 유효한 블록이 채굴된 후에도 채굴되는 스테일 블록(Stale Block) 비율이 다소 증가하더라도 보안성(Security) 문제가 발생하지 않도록 구현되는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 4

제 2 항에 있어서,

테스트넷 처리부가:

최적의 합의 조건 도출에 필요한 파라미터(Parameter)들을 정의하는 파라미터 정의부를;

더 포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 5

제 4 항에 있어서,

최적의 합의 조건 도출에 필요한 파라미터(Parameter)가:

확장성(Scalability) 문제 개선을 위한 성능 파라미터(Performance Parameter)와;

보안성(Security) 문제 개선을 위한 보안성 파라미터(Security Parameter)를;

포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 6

제 5 항에 있어서,

성능 파라미터가:

블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 7

제 5 항에 있어서,

보안성 파라미터가:

네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 8

제 4 항 내지 제 6 항 중의 어느 한 항에 있어서,

최적 합의 분석부가:

테스트넷의 작업증명 채굴부를 통해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하는 작업증명 테스트부와;

작업증명 테스트부에 의한 시뮬레이팅 결과를 분석하여 파라미터 정의부에 의해 정의된 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들의 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출하는 합의 조건 도출부를;

포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 9

제 8 항에 있어서,

합의 조건 도출부가:

블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 확장성(Scalability) 문제를 개선하는 확장성 문제 개선부를;

포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 10

제 9 항에 있어서,

합의 조건 도출부가:

네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 보안성(Security) 문제를 개선하는 보안성 문제 개선부를;

더 포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치.

청구항 11

탈중앙화(Decentralization)에 장점이 있는 퍼블릭 블록체인 메인넷(Public Blockchain Main Net)과 유사한 테스트넷(Test Net)을 구성하는 테스트넷 처리단계와;

테스트넷 처리단계에 의해 구성된 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 퍼블릭 블록체인 메인넷의 태생적으로 낮은 확장성(Scalability) 문제를 개선할 수 있는 최적의 합의 조건을 도출하는 최적 합의 분석단계를;

포함하되,

최적 합의 분석단계에서:

최적의 합의 조건 도출에 필요한 파라미터(Parameter)들을 정의하고, 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 정의된 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들의 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

청구항 12

제 11 항에 있어서,

테스트넷이:

블록 생성 속도(Block Interval)로 블록(Block)들을 반복 채굴(Mining)하여, 블록(Block)들이 체인(Chain) 형태로 연결되는 합의(Consensus) 과정을 수행하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

청구항 13

제 12 항에 있어서,

테스트넷은:

높은 탈중앙화의 전제조건으로 충분히 많은 노드가 뒷받침되어, 유효한 블록이 채굴된 후에도 채굴되는 스테일 블록(Stale Block) 비율이 다소 증가하더라도 보안성(Security) 문제가 발생하지 않도록 구현되는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

청구항 14

제 12 항에 있어서,

테스트넷 처리단계에서:

최적의 합의 조건 도출에 필요한 파라미터(Parameter)들을 정의하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

청구항 15

제 14 항에 있어서,

최적의 합의 조건 도출에 필요한 파라미터(Parameter)가:

확장성(Scalability) 문제 개선을 위한 성능 파라미터(Performance Parameter)와;

보안성(Security) 문제 개선을 위한 보안성 파라미터(Security Parameter)를;

포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

청구항 16

제 15 항에 있어서,

성능 파라미터가:

블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

청구항 17

제 15 항에 있어서,

보안성 파라미터가:

네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

청구항 18

제 14 항 내지 제 16 항 중의 어느 한 항에 있어서,

최적 합의 분석단계가:

테스트넷을 통해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하는 작업증명 테스트단계와;

작업증명 테스트단계에 의한 시뮬레이팅 결과를 분석하여 정의된 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들의 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출하는 합의 조건 도출단계를;

포함하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

청구항 19

제 18 항에 있어서,

합의 조건 도출단계에서:

블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 확장성(Scalability) 문제를 개선하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

청구항 20

제 19 항에 있어서,

합의 조건 도출단계에서:

네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 보안성(Security) 문제를 개선하는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인(Blockchain) 기술에 관련한 것으로, 특히 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 블록체인(Blockchain)은 분산 원장 기술(DLT : Distributed Ledger Technology)의 일종으로, 데이터 분산처리 기술이다. 네트워크 상에 존재하는 노드의 수가 기하급수적으로 증가하고 노드 간 통신 속도가 증가하면서 과거에는 불가능했던 Peer-to-Peer(P2P) 통신이 다소 자유로워졌다. 이로써 네트워크에 참여하는 모든 노드가 모든 거래 내역 등의 데이터를 분산, 저장할 수 있는 환경이 되었다.

[0003] 개인과 개인의 거래(P2P)에서 발생하는 모든 거래 내역의 데이터가 기록되는 장부를 블록에 저장하여서 궁극적인 체인 형태로 결합하기 때문에 블록체인이 되었다. 따라서, 블록들은 채굴(Mining)된 후 시간의 흐름(Time-

stamping)에 따라 순차적으로 연결된 체인의 구조가 되며 'liveness'와 확률적인 'safety'를 보장한다.

[0004] 여기서, 'liveness'는 합의 대상에 문제가 없다면, 네트워크 내에서 반드시 합의가 이루어진다는 것을 의미하고, 'safety'는 노드 간 합의가 발생했다면, 어느 노드가 접근하든 그 값은 동일해야 한다는 것을 의미한다.

[0005] 그러나, 현재의 블록체인은 실제 서비스에 이용되기에 너무 느리다. 블록체인은 시간의 흐름 그대로 기록되어 변조가 매우 어렵다는 성질에서 암호화폐부터, 전자 문서 기록, 인공지능 학습 데이터 저장, 응용 보안 서비스, 금융 산업, 게임, SNS에까지 적용되는 추세이다.

[0006] 그렇지만, 블록체인이 안정적으로 적용되려면 블록체인 네트워크 자체의 성능, 블록체인 트릴레마(Trilemma) 중 확장성(Scalability) 문제 해결이 요구된다. 블록체인 트릴레마의 탈중앙화(Decentralization), 확장성(Scalability), 보안성(Security) 세 가지를 모두 만족할 수 없다.

[0007] 퍼블릭(Public) 블록체인 네트워크 환경은 특히 탈중앙화(Decentralization)에 장점이 있으며, 프라이빗(Private) 블록체인은 확장성(Scalability)의 장점이 있다. 블록 채굴(Mining) 시의 합의(Consensus) 과정에서 참여 노드, 그리고 네트워크 구조에 따라 블록체인 트릴레마 상의 트라이앵귤러 포인트(triangular point)가 변경되며 각 포인트(point)의 트레이드 오프(trade-off)가 생긴다.

[0008] 퍼블릭 블록체인의 낮은 확장성(Scalability) 문제는 블록에 거래가 담길 시 또는 노드 간 합의 과정 시에 발생한다. 특히 작업증명 합의(Proof-of-Work consensus)의 낮은 확장성(Scalability) 문제 개선을 위해 H/W 개선, 세그윗(Segwit), 하드포크(Hardfork), 샤딩(Sharding), 합의 알고리즘(consensus algorithm) 변경 등으로 TPS(Transaction Per Second) 개선에 있어 다양한 시도가 진행중이다.

[0009] 그러나, 블록의 크기를 키워 TPS를 높이는 하드포크(hardfork) 방식의 예인 비트코인 캐시(Bitcoin Cash)는 기존의 비트코인과는 다른 새로운 블록체인이기 때문에 근본적인 확장성(Scalability)을 해결해 주었다고 할 수 없다. 그리고, 블록체인은 비구조화 오버레이 네트워크(overlay network)이기 때문에 이미 전파된 노드에게 다시 전파하는 문제가 발생하는데, 이는 블록체인 기본 특성이기 때문에 개선할 수 없다.

[0010] 인터넷과 H/W를 개선하여 전파 및 검증을 빠르게 할 수 있으나, H/W의 혁신적인 성능 발전을 기다리는 것은 요원하며, 채굴과정의 전기소비량도 무시할 수 없다. 각 개선 방법은 한계점이 존재하며, 이 때문에 근본적인 퍼블릭 블록체인의 확장성(Scalability) 개선을 위해서는 이들 중에서 합의 알고리즘(Consensus Algorithm)에 대한 개선이 요구된다.

[0011] 이 과정에서 현재 블록체인보다 적절한 난이도(Difficulty)와 블록 생성 속도(Block Interval)를 줄여 확장성(Scalability) 문제를 해결하는 것이 중요하다. 난이도(Difficulty)가 낮아져 새로운 블록이 채굴(Mining)되는 간격(Interval)이 짧아지고 총 해시(hash) 비율이 바뀌어도 블록체인 트릴레마(Trilemma)를 해결하기 위해서는 기존의 메인넷과 비교해도 거의 동등한 보안성이 요구된다.

[0012] 따라서, 본 발명자는 블록 생성 속도와 블록 전파 비율의 관계와 보안성을 유지하면서도 확장성(Scalability)을 높일 수 있는 기술에 대한 연구를 하였다. 이 과정에서 퍼블릭(Public) 블록체인의 확장성(Scalability) 문제를 어느 정도 해소함에 따라 난이도(Difficulty)가 지속적으로 높아지며 작업증명(Proof-of-Work)의 단점으로 꼽히는 H/W 리소스(resources) 증가량을 낮출 수 있을 것이다.

선행기술문헌

특허문헌

[0013] (특허문헌 0001) 대한민국 등록특허 제10-2135403호(2020.07.17 공고)

발명의 내용

해결하려는 과제

[0014] 본 발명은 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 퍼블릭 블록체인 메인넷의 태생적으로 낮은 확장성(Scalability) 문제를 개선함으로써 블록 생성 속도와 블록 전파 비율의 관계와 보안성을 유지하면서도 확장성

(Scalability)을 높일 수 있는 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치 및 방법을 제공함을 그 목적으로 한다.

과제의 해결 수단

[0015] 상기한 목적을 달성하기 위한 본 발명의 일 양상에 따르면, 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 탈중앙화(Decentralization)에 장점이 있는 퍼블릭 블록체인 메인넷(Public Blockchain Main Net)과 유사한 테스트넷(Test Net)을 구성하는 테스트넷 처리부와; 테스트넷 처리부에 의해 구성된 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 퍼블릭 블록체인 메인넷의 태생적으로 낮은 확장성(Scalability) 문제를 개선할 수 있는 최적의 합의 조건을 도출하는 최적 합의 분석부를 포함한다.

[0016] 본 발명의 부가적인 양상에 따르면, 테스트넷 처리부가 테스트넷 상에서 블록 생성 속도(Block Interval)로 블록(Block)들을 반복 채굴(Mining)하여, 블록(Block)들이 체인(Chain) 형태로 연결되는 합의(Consensus) 과정을 수행하는 작업증명 채굴부를 포함할 수 있다.

[0017] 본 발명의 부가적인 양상에 따르면, 테스트넷은 높은 탈중앙화의 전제조건으로 충분히 많은 노드가 뒷받침되어, 유효한 블록이 채굴된 후에도 채굴되는 스테일 블록(Stale Block) 비율이 다소 증가하더라도 보안성(Security) 문제가 발생하지 않도록 구현될 수 있다.

[0018] 본 발명의 부가적인 양상에 따르면, 테스트넷 처리부가 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들을 정의하는 파라미터 정의부를 더 포함할 수 있다.

[0019] 본 발명의 부가적인 양상에 따르면, 최적의 합의 조건 도출에 필요한 파라미터(Parameter)가 확장성(Scalability) 문제 개선을 위한 성능 파라미터(Performance Parameter)와; 보안성(Security) 문제 개선을 위한 보안성 파라미터(Security Parameter)를 포함할 수 있다.

[0020] 본 발명의 부가적인 양상에 따르면, 성능 파라미터가 블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 포함할 수 있다.

[0021] 본 발명의 부가적인 양상에 따르면, 보안성 파라미터가 네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 포함할 수 있다.

[0022] 본 발명의 부가적인 양상에 따르면, 최적 합의 분석부가 테스트넷의 작업증명 채굴부를 통해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하는 작업증명 테스트부와; 작업증명 테스트부에 의한 시뮬레이팅 결과를 분석하여 파라미터 정의부에 의해 정의된 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들의 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출하는 합의 조건 도출부를 포함할 수 있다.

[0023] 본 발명의 부가적인 양상에 따르면, 합의 조건 도출부가 블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 확장성(Scalability) 문제를 개선하는 확장성 문제 개선부를 포함할 수 있다.

[0024] 본 발명의 부가적인 양상에 따르면, 합의 조건 도출부가 네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 보안성(Security) 문제를 개선하는 보안성 문제 개선부를 더 포함할 수 있다.

[0025] 한편, 본 발명의 또 다른 양상에 따르면, 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법이 탈중앙화(Decentralization)에 장점이 있는 퍼블릭 블록체인 메인넷(Public Blockchain Main Net)과 유사한 테스트넷(Test Net)을 구성하는 테스트넷 처리단계와; 테스트넷 처리단계에 의해 구성된 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 퍼블릭 블록체인 메인넷의 태생적으로 낮은 확장성(Scalability) 문제를 개선할 수 있는 최적의 합의 조건을 도출하는 최적 합의 분석단계를 포함한다.

[0026] 본 발명의 부가적인 양상에 따르면, 테스트넷이 블록 생성 속도(Block Interval)로 블록(Block)들을 반복 채굴

(Mining)하여, 블록(Block)들이 체인(Chain) 형태로 연결되는 합의(Consensus) 과정을 수행한다.

[0027] 본 발명의 부가적인 양상에 따르면, 테스트넷 처리단계에서 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들을 정의할 수 있다.

[0028] 본 발명의 부가적인 양상에 따르면, 최적 합의 분석단계가 테스트넷을 통해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하는 작업증명 테스트단계와; 작업증명 테스트단계에 의한 시뮬레이팅 결과를 분석하여 정의된 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들의 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출하는 합의 조건 도출단계를 포함할 수 있다.

[0029] 본 발명의 부가적인 양상에 따르면, 합의 조건 도출단계에서 블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 확장성(Scalability) 문제를 개선하도록 구현될 수 있다.

[0030] 본 발명의 부가적인 양상에 따르면, 합의 조건 도출단계에서 네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 보안성(Security) 문제를 개선하도록 구현될 수 있다.

발명의 효과

[0031] 본 발명은 블록 생성 속도와 블록 전파 비율의 관계와 보안성을 유지하면서도 확장성(Scalability)을 높일 수 있으므로, 퍼블릭(Public) 블록체인의 확장성(Scalability) 문제를 어느 정도 해소함에 따라 난이도(Difficulty)가 지속적으로 높아지며 작업증명(Proof-of-Work)의 단점으로 꼽히는 H/W 리소스(resources) 증가량을 낮출 수 있는 효과가 있다.

도면의 간단한 설명

[0032] 도 1 은 본 발명에 따른 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치의 일 실시예의 구성을 도시한 블록도이다.

도 2 는 본 발명에 따른 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법의 일 실시예의 구성을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0033] 이하, 첨부된 도면을 참조하여 기술되는 바람직한 실시예를 통하여 본 발명을 당업자가 용이하게 이해하고 재현할 수 있도록 상세히 기술하기로 한다. 특정 실시예들이 도면에 예시되고 관련된 상세한 설명이 기재되어 있으나, 이는 본 발명의 다양한 실시예들을 특정한 형태로 한정하려는 것은 아니다.

[0034] 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명 실시예들의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다.

[0035] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다.

[0036] 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해될 수 있어야 할 것이다.

[0037] 도 1 은 본 발명에 따른 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치의 일 실시예의 구성을 도시한 블록도이다. 도 1 에 도시한 바와 같이, 이 실시예에 따른 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치(100)는 테스트넷 처리부(110)와, 최적 합의 분석부(120)를 포함한다.

[0038] 테스트넷 처리부(110)는 탈중앙화(Decentralization)에 장점이 있는 퍼블릭 블록체인 메인넷(Public Blockchain Main Net)과 유사한 테스트넷(Test Net)을 구성한다. 예컨대, 테스트넷은 높은 탈중앙화의 전제조건으로 충분히 많은 노드가 뒷받침되어, 유효한 블록이 채굴된 후에도 채굴되는 스테일 블록(Stale Block) 비율이 다소 증가하더라도 보안성(Security) 문제가 발생하지 않도록 구현될 수 있다.

[0039] 이 때, 테스트넷 처리부(110)가 작업증명 채굴부(111)를 포함할 수 있다. 작업증명 채굴부(111)는 테스트넷 상에서 블록 생성 속도(Block Interval)로 블록(Block)들을 반복 채굴(Mining)하여, 블록(Block)들이 체인(Chain) 형태로 연결되는 합의(Consensus) 과정을 수행한다.

[0040] 작업증명 채굴부(111)는 작업증명(PoW : Proof-of-Work) 채굴(Mining) 과정을 블록 생성(Block Generation), 블록 전파(Block Propagation), 블록 검증(Block Verification) 3부분으로 나누어 실제 구축하기 원하는 퍼블릭 블록체인 메인넷과 유사하게 디자인된 테스트넷을 통해 작업증명(PoW : Proof-of-Work) 채굴(Mining)을 수행한다.

[0041] 작업증명(PoW : Proof-of-Work) 채굴(Mining)에 참여하는 채굴 노드(Mining Node)를 구성할 때 해시(Hash) 비율별로 애드버서리(adversary)하게 구성하고, 새로운 블록을 채굴하고 난 뒤에는 작업증명 알고리즘(Proof-of-Work Algorithm)과 'Deepeest subtree process'대로 블록체인을 구성한다.

[0042] 한편, 작업증명 알고리즘(Proof-of-Work Algorithm)에서 블록 크기, 네트워크 속도 등 다른 변수를 고려하지 않고, 오직 난이도(Difficulty)를 낮춰 'hash Proof-of-Worker'에 대한 변화를 매집하도록 구현하여, 채굴(Mining) 경쟁에서 'Hash Proof-of-Worker'가 낮아져도 큰 보안 문제가 발생하지 않도록 한다.

[0043] 한편, 테스트넷 처리부(110)가 파라미터 정의부(112)를 더 포함할 수 있다. 파라미터 정의부(112)는 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들을 정의한다. 이 때, 최적의 합의 조건 도출에 필요한 파라미터(Parameter)가 확장성(Scalability) 문제 개선을 위한 성능 파라미터(Performance Parameter)와, 보안성(Security) 문제 개선을 위한 보안성 파라미터(Security Parameter)를 포함할 수 있다.

[0044] 예컨대, 성능 파라미터는 블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 포함할 수 있고, 보안성 파라미터는 네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 포함할 수 있다.

[0045] 최적 합의 분석부(120)는 테스트넷 처리부(110)에 의해 구성된 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 퍼블릭 블록체인 메인넷의 태생적으로 낮은 확장성(Scalability) 문제를 개선할 수 있는 최적의 합의 조건을 도출한다. 예컨대, 최적 합의 분석부(120)가 작업증명 테스트부(121)와, 합의 조건 도출부(122)를 포함할 수 있다.

[0046] 작업증명 테스트부(121)는 테스트넷의 작업증명 채굴부(111)를 통해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)한다.

[0047] 예컨대, 작업증명 테스트부(121)가 블록 생성 속도(Block Interval)를 25초부터 0.5초까지 균일 또는 비균일한 간격으로 줄이면서 작업증명 채굴부(111)를 통해 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하도록 구현될 수 있다.

[0048] 합의 조건 도출부(122)는 작업증명 테스트부(121)에 의한 시뮬레이팅 결과를 분석하여 파라미터 정의부(112)에 의해 정의된 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들의 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출한다.

[0049] 이 때, 합의 조건 도출부(122)가 파라미터(Parameter)들에 대한 트레이드 오프(Trade-off) 분석을 통해 특정 파라미터에 정의된 파라미터 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출하도록 구현될 수 있다. 한편, 합의 조건 도출부(122)가 인공 지능 러닝 머신 학습 기반으로 최적의 합의 조건을 도출하도록 구현될 수도 있다.

[0050] 예컨대, 합의 조건 도출부(122)가 확장성 문제 개선부(122a)를 포함할 수 있다. 확장성 문제 개선부(122a)는 블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 확장성(Scalability) 문제를 개선한다.

[0051] 난이도(Difficulty)는 채굴자(Miner)가 새로운 블록을 생성하기 위해 암호를 풀게 되는데, 이 암호의 어려움 또는 쉬움을 나타내는 정도를 말한다. 채굴 난이도가 높다는 것은 암호를 풀기 어렵다는 뜻이고, 채굴 난이도가 낮다는 것은 상대적으로 암호를 풀기 쉽다.

[0052] 블록체인 채굴 경쟁이 심화돼 채굴 속도가 빨라질 것 같으면, 채굴자가 풀어야 하는 암호 문제의 난이도를 자동으로 높이고, 반대로 채굴 경쟁이 완화되면 블록 생성 함수 문제의 난이도를 낮도록 설계가 되어있다.

[0053] 난이도가 높아지면 이전과 동일한 블록을 만들기 위해 더 많은 해시레이트(hashrate)를 필요로 하고, 반대로 난이도가 낮아지면 이전과 동일한 블록을 만들기 위해 더 적은 해시레이트(hashrate)를 필요로 하므로, 난이도(Difficulty)는 블록 생성 속도(Block Interval)에 영향을 준다.

[0054] 따라서, 합의 조건 도출부(122)를 통해 성능 파라미터에 정의된 난이도(Difficulty) 값에 맞도록 블록 생성 속도(Block Interval)를 조정하면 확장성(Scalability) 문제를 개선할 수 있게 된다.

[0055] 채굴(Mining) 과정에서 비중이 대다수를 차지하는 채굴 풀 즉 채굴력(Mining Power)이 51%가 넘는 풀이 채굴에 성공하여 보상을 가져가므로, 채굴력(Mining Power)의 비율은 채굴 경쟁과 관련되어 블록 생성 속도(Block Interval)에 영향을 준다.

[0056] 또한, 채굴력의 비율에 따라 'Selfish Mining Attacks'을 방지할 수 있기 때문에 채굴력(Mining Power)은 성능 파라미터에 속하는 동시에 보안성과도 관련된다.

[0057] 따라서, 합의 조건 도출부(122)를 통해 성능 파라미터에 정의된 채굴력(Mining Power) 값에 맞도록 블록 생성 속도(Block Interval)를 조정하면 확장성(Scalability) 문제를 개선하는 동시에 보안성(Security) 문제도 개선할 수 있게 된다.

[0058] 한편, 합의 조건 도출부(122)가 보안성 문제 개선부(122b)를 더 포함할 수 있다. 보안성 문제 개선부(122b)는 네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 보안성(Security) 문제를 개선한다.

[0059] 유효 처리량은 평균 블록 생성 속도(Block Interval) 내에 블록을 전파하는 노드의 비율(평균 블록 생성 속도라는 시간 단위 안에서 전체 네트워크상에서 가장 최신 블록을 전파받고 검증하는 노드의 비율)로, 전파 비율(Propagation Rate)에 영향을 준다. 만일 유효 처리량이 90%라 한다면 해당 대역폭에서 네트워크의 노드 중 10%는 지체된다는 말이며, 잠재적으로 서비스 거부가 발생하여 네트워크의 유효 채굴력(Mining Power)이 줄어들 수 있다.

[0060] 채굴이 끝난 블록을 전체 블록체인 네트워크에 전파하는 블록 전파(Block Propagation) 과정에서 전파 비율(Propagation Rate)이 최대한 100%에 수렴할 수 있도록 해야 하기 때문에, 전파 비율(Propagation Rate)은 'Double-Spending Attacks'을 방지하기 위한 보안성 파라미터이다.

[0061] 따라서, 합의 조건 도출부(122)를 통해 보안성 파라미터에 정의된 전파 비율(Propagation Rate) 값에 맞도록 블록 생성 속도(Block Interval)를 조정하면 보안성(Security) 문제를 개선할 수 있게 된다.

[0062] 스테일 블록 비율(Stale Block Rate)은 메인 체인블록에 포함되지 않는 채굴 보상을 받지 못하는 블록으로, 두 명의 채굴자들이 비슷한 시기에 블록을 생성할 때, 혹은 해커가 거래를 교란시키기 위한 공격을 시도할 때 생성되므로, 보안성(Security)에 반비례한다.

[0063] 따라서, 합의 조건 도출부(122)를 통해 보안성 파라미터에 정의된 스테일 블록 비율(Stale Block Rate) 값에 맞도록 블록 생성 속도(Block Interval)를 조정하면 보안성(Security) 문제를 개선할 수 있게 된다.

[0064] 블록 생성 속도가 감소하면 Selfish mining, Double Spending, Eclipse의 3가지 공격에 대한 확률이 높아지는 것은 사실이다. 또한, 채굴 풀(Mining Pool) 간의 경쟁에서 스테일 블록(Stale Block)의 채굴에도 보상량을 부여하여야 하는 문제가 필연적으로 발생한다.

[0065] 그러나, 스테일 블록 채굴 보상을 고려한 최적의 블록 생성 속도로 조정하면 작업증명(Proof-of-Work) TPS가 최소 2배 이상까지 개선된다. 결국, 블록 생성 시간(블록 생성 속도)을 현재보다 작게 하여도, 스테일 블록 비율이 늘어나는 보안 상의 문제는 테스트넷에서 1.21%의 하락률뿐이지만 성능 향상은 메인넷 기준 3배의 120 TPS까지 개선 가능하며 지속적인 최적의 블록 생성 시간에 대한 데이터가 축적된다면 추후 머신러닝을 이용한 이상적인 합의 시간을 도출해낼 수 있을 것이다.

[0066] 다음의 표 1은 블록 생성 속도(Block Interval)를 25초부터 0.5초까지 비균일한 간격으로 줄이면서 작업증명 채굴부(111)를 통해 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 얻

은 결과를 예시한 것이다.

표 1

[0067]

	Case 1			Case 2		
블록 생성속도 (s)	전파 Time(s)	전파 비율(%)	스테일 블록 비율(%)	전파 Time(s)	전파 비율(%)	스테일 블록 비율(%)
25	35.73	96	1.72	25.66	96	0.16
15	14.7	96	1.51	10.65	96	0.13
10	4.18	96	1.82	2.91	91	0.16
9	2.08	95	2.15	1.34	88	0.35
7	1.43	81	2.54	0.84	71	0.45
5	1.21	77	3.20	0.67	69	0.86
3	1.00	60	4.77	0.35	61	1.73
2	0.89	52	8.64	0.37	56	2.94
1	0.84	29	16.65	0.40	28	6.98
0.5	0.82	31	26.74	0.53	17	12.44

[0068] 10초의 블록 생성 속도에서 Case 1의 전파 시간은 약 4.18초, 전파 비율은 96%, 스테일 블록 비율은 1.82%, Case 2의 전파 시간은 약 2.91초, 전파 비율은 91%, 스테일 블록 비율은 1.16%로 나타났다. 블록 생성 속도 10초 구간에서는 전파 비율이 Case 1에서 96%, Case 2에서 91%이기 때문에 전파 비율이 Case 2에서 약 5% 하락 차이를 보인다.

[0069] 블록 생성 속도를 줄인 구간에서 전파 시간 하락 발생을 살펴보면, 블록 생성 속도를 9초에서 7초의 구간으로 하락시키면 Case 1에서 전파 시간이 2.08초에서 1.43초로 0.65초, 전파 비율은 95%에서 81%로 14% 감소되고, Case2에서 전파 시간이 1.34초에서 0.84초로 0.5초, 전파 비율은 98%에서 71%로 17% 감소됨을 볼 수 있다.

[0070] 만약, 파라미터 정의부(112)에서 최적의 합의 조건 도출에 필요한 파라미터(Parameter)로 성능 파라미터의 전파 비율(Propagation Rate)을 91% 내지 96%로 정의한다면, 합의 조건 도출부(122)의 보안성 문제 개선부(122b)에 의해 전파 비율(Propagation Rate)이 91% 내지 96% 구간인 블록 생성 속도 10초를 최적의 합의 조건으로 도출한다.

[0071] 표 2 는 블록 생성 속도와 TPS(Transaction Per Second)의 관계를 예시한 것이다. 표 2 를 참조해 보면, 블록 생성 속도가 15초에서 5초로 단축되면, TPS(Transaction Per Second)가 40에서 120으로 3배 성능 향상됨을 볼 수 있다.

표 2

[0072]

Tx in a Block(Tx)	Block interval(s)	TPS(Tx/s)
600 (On Average)	25	24
	15	40
	10	60
	9	66.6
	7	85.7
	5	120
	3	200
	2	300
	1	600
	0.5	1200

[0073] 본 발명은 작업증명 블록체인 네트워크(PoW Blockchain network) 상에서 합의(Consensus) 과정시 발생하는 낮은 확장성(Scalability) 문제를 해결하기 위한 최적의 블록 생성 속도를 성능과 보안성 측면에서 미치는 영향을 정밀 분석하여 도출할 수 있기 때문에 블록체인 기반 서비스 적용 도메인에 따라 고성능/고신뢰(보안성)를 기대할 수 있다.

[0074] 이와 같이 구현함에 의해 본 발명은 블록 생성 속도와 블록 전파 비율의 관계와 보안성을 유지하면서도 확장성(Scalability)을 높일 수 있으므로, 퍼블릭(Public) 블록체인의 확장성(Scalability) 문제를 어느 정도 해소함

에 따라 난이도(Difficulty)가 지속적으로 높아지며 작업증명(Proof-of-Work)의 단점으로 꼽히는 H/W 리소스(resources) 증가량을 낮출 수 있다.

[0075] 도 2 는 본 발명에 따른 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 방법의 일 실시예의 구성을 도시한 흐름도이다. 도 2 를 참조하여 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치에 의한 최적 합의 도출 동작을 알아본다.

[0076] 먼저, 테스트넷 처리단계(210)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 탈중앙화(Decentralization)에 장점이 있는 퍼블릭 블록체인 메인넷(Public Blockchain Main Net)과 유사한 테스트넷(Test Net)을 구성한다.

[0077] 예컨대, 테스트넷은 높은 탈중앙화의 전제조건으로 충분히 많은 노드가 뒷받침되어, 유효한 블록이 채굴된 후에도 채굴되는 스테일 블록(Stale Block) 비율이 다소 증가하더라도 보안성(Security) 문제가 발생하지 않도록 구현될 수 있다.

[0078] 이 때, 테스트넷이 블록 생성 속도(Block Interval)로 블록(Block)들을 반복 채굴(Mining)하여, 블록(Block)들이 체인(Chain) 형태로 연결되는 합의(Consensus) 과정을 수행한다.

[0079] 테스트넷 처리단계(210)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치는 작업증명(PoW : Proof-of-Work) 채굴(Mining) 과정을 블록 생성(Block Generation), 블록 전파(Block Propagation), 블록 검증(Block Verification) 3부분으로 나누어 실제 구축하기 원하는 퍼블릭 블록체인 메인넷과 유사하게 디자인된 테스트넷을 통해 작업증명(PoW : Proof-of-Work) 채굴(Mining)을 수행한다.

[0080] 작업증명(PoW : Proof-of-Work) 채굴(Mining)에 참여하는 채굴 노드(Mining Node)를 구성할 때 해시(Hash) 비율별로 애드버서리(adversary)하게 구성하고, 새로운 블록을 채굴하고 난 뒤에는 작업증명 알고리즘(Proof-of-Work Algorithm)과 'Deepeest subtree process'대로 블록체인을 구성한다.

[0081] 한편, 작업증명 알고리즘(Proof-of-Work Algorithm)에서 블록 크기, 네트워크 속도 등 다른 변수를 고려하지 않고, 오직 난이도(Difficulty)를 낮춰 'hash Proof-of-Worker'에 대한 변화를 매집하도록 구현하여, 채굴(Mining) 경쟁에서 'Hash Proof-of-Worker'가 낮아져도 큰 보안 문제가 발생하지 않도록 한다.

[0082] 한편, 테스트넷 처리단계(210)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들을 정의하도록 구현될 수 있다.

[0083] 이 때, 최적의 합의 조건 도출에 필요한 파라미터(Parameter)가 확장성(Scalability) 문제 개선을 위한 성능 파라미터(Performance Parameter)와, 보안성(Security) 문제 개선을 위한 보안성 파라미터(Security Parameter)를 포함할 수 있다.

[0084] 예컨대, 성능 파라미터는 블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 포함할 수 있고, 보안성 파라미터는 네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 포함할 수 있다.

[0085] 그 다음, 최적 합의 분석단계(220)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 테스트넷 처리단계(210)에 의해 구성된 테스트넷을 이용해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하여 퍼블릭 블록체인 메인넷의 태생적으로 낮은 확장성(Scalability) 문제를 개선할 수 있는 최적의 합의 조건을 도출한다. 예컨대, 최적 합의 분석단계(220)가 작업증명 테스트단계(221)와, 합의 조건 도출단계(222)를 포함할 수 있다.

[0086] 작업증명 테스트단계(221)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 테스트넷을 통해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)한다.

[0087] 예컨대, 작업증명 테스트단계(221)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 블록 생성 속도(Block Interval)를 25초부터 0.5초까지 균일 또는 비균일한 간격으로 줄이면서 테스트넷을 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)하도록 구현될 수 있다.

[0088] 그 다음, 합의 조건 도출단계(222)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 작업증명 테스트단계(221)에 의한 시뮬레이팅 결과를 분석하여 정의된 최적의 합의 조건 도출에 필요한 파

라미터(Parameter)들의 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출한다.

[0089] 이 때, 합의 조건 도출단계(222)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 파라미터(Parameter)들에 대한 트레이드 오프(Trade-off) 분석을 통해 특정 파라미터에 정의된 파라미터 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출하도록 구현될 수 있다. 한편, 합의 조건 도출단계(222)에서 인공 지능 러닝 머신 학습 기반으로 최적의 합의 조건을 도출하도록 구현될 수도 있다.

[0090] 예컨대, 합의 조건 도출단계(222)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 블록 생성 속도(Block Interval)에 영향을 주는 난이도(Difficulty)와, 채굴 보상에 영향을 주는 채굴력(Mining Power)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 확장성(Scalability) 문제를 개선하도록 구현될 수 있다.

[0091] 난이도(Difficulty)는 채굴자(Miner)가 새로운 블록을 생성하기 위해 암호를 풀게 되는데, 이 암호의 어려움 또는 쉬움을 나타내는 정도를 말한다. 채굴 난이도가 높다는 것은 암호를 풀기 어렵다는 뜻이고, 채굴 난이도가 낮다는 것은 상대적으로 암호를 풀기 쉽다.

[0092] 블록체인 채굴 경쟁이 심화돼 채굴 속도가 빨라질 것 같으면, 채굴자가 풀어야 하는 암호 문제의 난이도를 자동으로 높이고, 반대로 채굴 경쟁이 완화되면 블록 생성 함수 문제의 난이도를 낮도록 설계가 되어있다.

[0093] 난이도가 높아지면 이전과 동일한 블록을 만들기 위해 더 많은 해시레이트(hashrate)를 필요로 하고, 반대로 난이도가 낮아지면 이전과 동일한 블록을 만들기 위해 더 적은 해시레이트(hashrate)를 필요로 하므로, 난이도(Difficulty)는 블록 생성 속도(Block Interval)에 영향을 준다.

[0094] 따라서, 합의 조건 도출단계(222)를 통해 성능 파라미터에 정의된 난이도(Difficulty) 값에 맞도록 블록 생성 속도(Block Interval)를 조정하면 확장성(Scalability) 문제를 개선할 수 있게 된다.

[0095] 채굴(Mining) 과정에서 비중이 대다수를 차지하는 채굴 풀 즉 채굴력(Mining Power)이 51%가 넘는 풀이 채굴에 성공하여 보상을 가져가므로, 채굴력(Mining Power)의 비율은 채굴 경쟁과 관련되어 블록 생성 속도(Block Interval)에 영향을 준다.

[0096] 또한, 채굴력의 비율에 따라 'Selfish Mining Attacks'을 방지할 수 있기 때문에 채굴력(Mining Power)은 성능 파라미터에 속하는 동시에 보안성과도 관련된다.

[0097] 따라서, 합의 조건 도출단계(222)를 통해 성능 파라미터에 정의된 채굴력(Mining Power) 값에 맞도록 블록 생성 속도(Block Interval)를 조정하면 확장성(Scalability) 문제를 개선하는 동시에 보안성(Security) 문제도 개선할 수 있게 된다.

[0098] 한편, 합의 조건 도출단계(222)에서 작업증명 합의 알고리즘을 사용하는 블록체인에서의 최적 합의 도출 장치가 네트워크의 유효 처리량(Effective Throughput)에 영향을 주는 전파 비율(Propagation Rate)과, 보안성에 반비례하는 스테일 블록 비율(Stale Block Rate)을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출함으로써 퍼블릭 블록체인 메인넷의 보안성(Security) 문제를 개선하도록 구현될 수 있다.

[0099] 유효 처리량은 평균 블록 생성 속도(Block Interval) 내에 블록을 전파하는 노드의 비율(평균 블록 생성 속도라는 시간 단위 안에서 전체 네트워크상에서 가장 최신 블록을 전파받고 검증하는 노드의 비율)로, 전파 비율(Propagation Rate)에 영향을 준다. 만일 유효 처리량이 90%라 한다면 해당 대역폭에서 네트워크의 노드 중 10%는 지체된다는 말이며, 잠재적으로 서비스 거부가 발생하여 네트워크의 유효 채굴력(Mining Power)이 줄어들 수 있다.

[0100] 채굴이 끝난 블록을 전체 블록체인 네트워크에 전파하는 블록 전파(Block Propagation) 과정에서 전파 비율(Propagation Rate)이 최대한 100%에 수렴할 수 있도록 해야 하기 때문에, 전파 비율(Propagation Rate)은 'Double-Spending Attacks'을 방지하기 위한 보안성 파라미터이다.

[0101] 따라서, 합의 조건 도출단계(222)를 통해 보안성 파라미터에 정의된 전파 비율(Propagation Rate) 값에 맞도록 블록 생성 속도(Block Interval)를 조정하면 보안성(Security) 문제를 개선할 수 있게 된다.

[0102] 스테일 블록 비율(Stale Block Rate)은 메인 체인블록에 포함되지 않는 채굴 보상을 받지 못하는 블록으로, 두 명의 채굴자들이 비슷한 시기에 블록을 생성할 때, 혹은 해커가 거래를 교란시키기 위한 공격을 시도할 때 생성되므로, 보안성(Security)에 반비례한다.

[0103] 따라서, 합의 조건 도출단계(222)를 통해 보안성 파라미터에 정의된 스테일 블록 비율(Stale Block Rate) 값에 맞도록 블록 생성 속도(Block Interval)를 조정하면 보안성(Security) 문제를 개선할 수 있게 된다.

[0104] 블록 생성 속도가 감소하면 Selfish mining, Double Spending, Eclipse의 3가지 공격에 대한 확률이 높아지는 것은 사실이다. 또한, 채굴 풀(Mining Pool) 간의 경쟁에서 스테일 블록(Stale Block)의 채굴에도 보상량을 부여하여야 하는 문제가 필연적으로 발생한다.

[0105] 그러나, 스테일 블록 채굴 보상을 고려한 최적의 블록 생성 속도로 조정하면 작업증명(Proof-of-Work) TPS가 최소 2배 이상까지 개선된다. 결국, 블록 생성 시간(블록 생성 속도)을 현재보다 작게 하여도, 스테일 블록 비율이 늘어나는 보안 상의 문제는 테스트넷에서 1.21%의 하락률뿐이지만 성능 향상은 메인넷 기준 3배의 120 TPS까지 개선 가능하며 지속적인 최적의 블록 생성 시간에 대한 데이터가 축적된다면 추후 머신러닝을 이용한 이상적인 합의 시간을 도출해낼 수 있을 것이다.

[0106] 본 발명은 작업증명 블록체인 네트워크(PoW Blockchain network) 상에서 합의(Consensus) 과정시 발생하는 낮은 확장성(Scalability) 문제를 해결하기 위한 최적의 블록 생성 속도를 성능과 보안성 측면에서 미치는 영향을 정밀 분석하여 도출할 수 있기 때문에 블록체인 기반 서비스 적용 도메인에 따라 고성능/고신뢰(보안성)를 기대할 수 있다.

[0107] 이와 같이 구현함에 의해 본 발명은 블록 생성 속도와 블록 전파 비율의 관계와 보안성을 유지하면서도 확장성(Scalability)을 높일 수 있으므로, 퍼블릭(Public) 블록체인의 확장성(Scalability) 문제를 어느 정도 해소함에 따라 난이도(Difficulty)가 지속적으로 높아지며 작업증명(Proof-of-Work)의 단점으로 꼽히는 H/W 리소스(resources) 증가량을 낮출 수 있다.

[0108] 본 명세서 및 도면에 개시된 다양한 실시예들은 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며, 본 발명의 다양한 실시예들의 범위를 한정하고자 하는 것은 아니다.

[0109] 따라서, 본 발명의 다양한 실시예들의 범위는 여기에서 설명된 실시예들 이외에도 본 발명의 다양한 실시예들의 기술적 사상을 바탕으로 도출되는 모든 변경 또는 변형된 형태가 본 발명의 다양한 실시예들의 범위에 포함되는 것으로 해석되어야 한다.

산업상 이용가능성

[0110] 본 발명은 블록체인(Blockchain) 관련 기술분야 및 이의 응용 기술분야에서 산업상으로 이용 가능하다.

부호의 설명

[0111] 100 : 최적 합의 도출 장치

110 : 테스트넷 처리부

111 : 작업증명 채굴부

112 : 파라미터 정의부

120 : 최적 합의 분석부

121 : 작업증명 테스트부

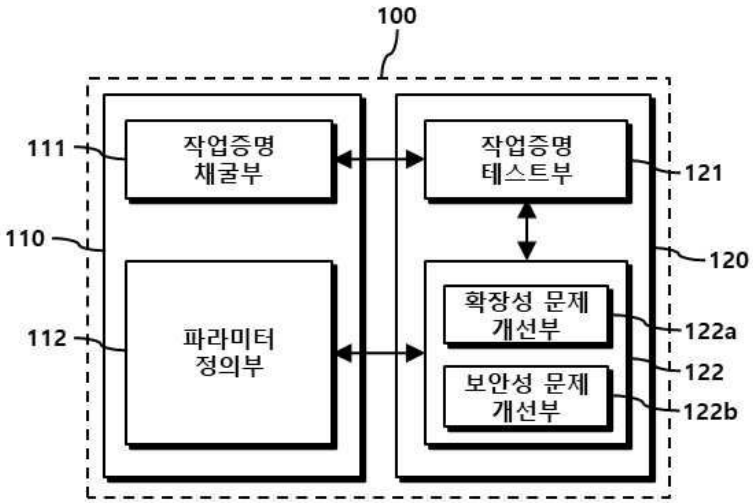
122 : 합의 조건 도출부

122a : 확장성 문제 개선부

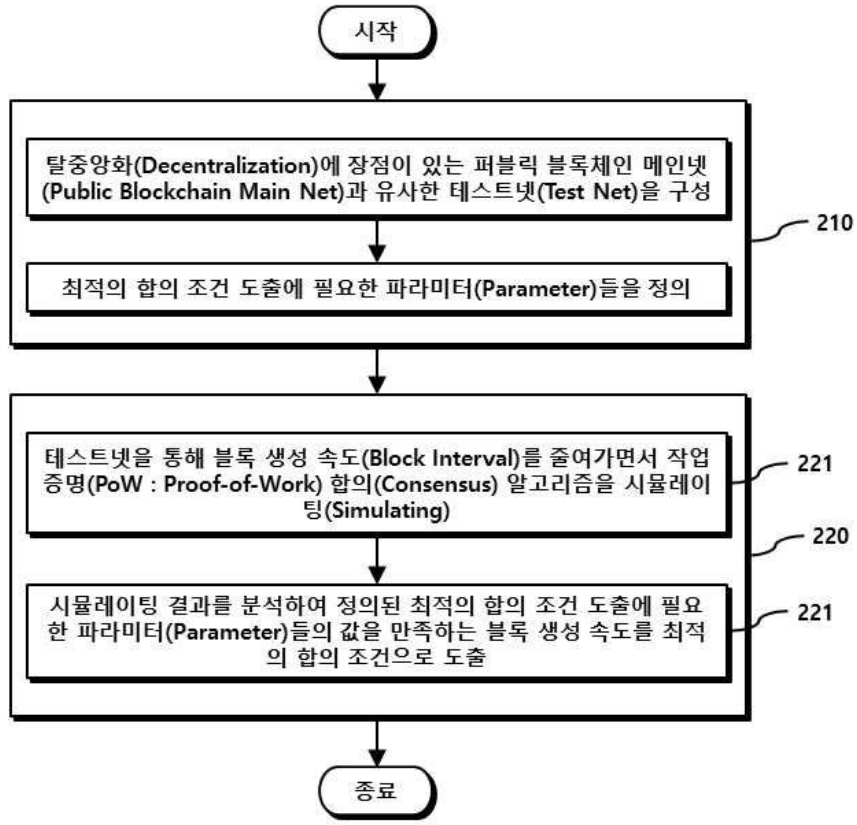
122b : 보안성 문제 개선부

도면

도면1


100
111
작업증명
채굴부
작업증명
테스트부
121
110
120
확장성 문제
개선부
122a
112
파라미터
정의부
122
보안성 문제
개선부
122b

도면2


시작
탈중앙화(Decentralization)에 장점이 있는 퍼블릭 블록체인 메인넷(Public Blockchain Main Net)과 유사한 테스트넷(Test Net)을 구성
최적의 합의 조건 도출에 필요한 파라미터(Parameter)들을 정의
210
테스트넷을 통해 블록 생성 속도(Block Interval)를 줄여가면서 작업증명(PoW : Proof-of-Work) 합의(Consensus) 알고리즘을 시뮬레이팅(Simulating)
221
220
시뮬레이팅 결과를 분석하여 정의된 최적의 합의 조건 도출에 필요한 파라미터(Parameter)들의 값을 만족하는 블록 생성 속도를 최적의 합의 조건으로 도출
221
종료