



“신규 유저 한정”

BTCC에 가입 및 입금하고 최대 17,500 USDT를 받으세요!
친구 초대 시 더 많은 리베이트 획득 가능



지금 가입

작업증명(PoW)은 무엇입니까? | 코인 용어 소개

원문:

<https://www.btcc.com/ko-KR/academy/crypto-basics/what-is-proof-of-work>

블록 체인에 대해 이야기 할 때, 많은 사람들이 일반적으로 “채굴”을 생각합니다. 현재 가장 기본적인 채굴 방법은 작업증명(POW)과 지분증명(POS)입니다.

오늘은 작업증명(POW)에 대해 소개합니다.

작업증명(PoW)이란?

작업증명(PoW, Proof of Work)이란 목표값 이하의 해시를 찾는 과정을 무수히 반복함으로써 해당 작업에 참여했음을 증명하는 방식의 합의 알고리즘입니다. **채굴(mining)**을 통해 작업증명을 한다..

작업 증명(PoW)은 **비트코인**의 기본 합의 모델인 블록체인 네트워크에 대한 합의 알고리즘입니다. 비트코인은 PoW의 사용을 최초로 이끈 암호화폐입니다.

작업 증명이라는 용어는 1999년에 만들어졌습니다. “작업 증명 및 빵 푸딩 프로토콜” (저자 Markus Jakobsson 및 Ari Juels)이라는 기사에서 등장했습니다. 작업 증명이라는 개념은 “확인자”가 지정된 시간 경과 시 수행된 필수 컴퓨터 작업의 증거를 “확인자”에게 제공해야 한다고 가정합니다.

PoW방식은 채굴자들은 채굴을 통해 작업증명을 하게 되며, 네트워크에 자신의 컴퓨터의 연산력(해시파워)을 제공하여 블록을 검증하고 체인에 연결합니다.

연산력이 높다는 것은 주어진 시간당 더 많은 작업증명을 수행할 수 있다는 의미이므로, 연산력이 빠르면 빠를수록 블록에 기록할 수 있는 권한이 더 부여됩니다.

작업증명은 별도의 채굴기가 필요하고 높은 연산력과 성능이 필요하기 때문에 대량의 전력이 소모됩니다.

또한 작업증명은 일반적으로 시간이 지날수록 조금씩 채굴의 난이도가 높아지며 디지털자산은 어느 시점의 한계치를 가지고 일정 수준으로 유지되기 때문에 점점 채굴 소요 시간이 늘어나게 되어 일반적인 채굴자는 채굴을 점점 채굴에 참여하기 어려워집니다.



[안드로이드 버전 다운로드](#)

[iOS 버전 다운로드](#)

[신규 유저 한정 이벤트\(입금 및 거래 시 10,055USDT 보상\) <<<<](#)

주요 참여자

작업증명(PoW)은 두 가지의 주요 참여자가 있습니다: 바로 채굴자와 풀 노드 운영자입니다.

채굴자

채굴자는 다음 블록을 생성(10분 마다 생성됨)하고 이를 네트워크에 브로드캐스트하기 위해 경쟁적으로 문제를 푸는 네트워크 참여자들입니다. 이 각 10분의 라운드당 승리한 채굴자가 블록 보상(현재 12.5 BTC)과 블록의 트랜잭션 수수료 모두를 보상으로 받게 됩니다. 이러한 방식은 다음의 두 가지 주요 요소로 인해 블록 생성 과정에서 정직하게 행동하도록 추동하는 역할을 합니다.

풀 노드 운영자

PoW의 두 번째 객체는 풀 노드 운영자나 풀 노드를 실행하는 일반 사용자입니다. 풀 노드는 소프트웨어 클라이언트로, 비트코인 소프트웨어를 실행해 네트워크에서 트랜잭션과 블록을 자동으로 검증하고 생성합니다.

암호학적 증명과 비트코인의 합의 규칙을 사용하는 풀 노드 운영자는 네트워크의 상태에 대한 최종 검증인 이자 네트워크의 역동성을 상징합니다. 풀 노드 클라이언트는 또한 마이닝 클라이언트가 될 수도 있으며, 클라이언트는 네트워크상의 유효하지 않은 블록과 트랜잭션을 거부합니다.

작동원리

비트코인은 발생한 모든 비트코인 거래의 이력을 포함하는 공유 원장인 블록체인입니다. 이름에서 알 수 있듯 이 블록체인은 블록으로 구성되어 있습니다. 각 블록은 최신 트랜잭션을 저장합니다.

작업 증명은 비트코인 블록체인에 새 블록을 추가하는 데 필요한 부분입니다. 블록은 작업 증명을 수행하는 생태계의 플레이어인 채굴자에 의해 활성화됩니다. 네트워크는 채굴자가 새로운 성공적인 작업 증명을 제안할 때마다 새 블록을 수락하며, 이는 대략 10분마다 발생합니다.

한편, 마이닝(채굴)이란 임의의 nonce 값을 대입해서 블록해시(blockhash) 결과 값을 생성하고 블록해시 결과 값이 제시된 Target보다 작은 블록해시값이 되도록 찾는 것입니다.

nonce 값을 0부터 1씩 증가시키면서 제시된 Target보다 작은 결과값이 나올 때까지 무한 반복작업을 수행해야 하며, 이러한 문제를 풀이하는 과정을 1초 안에 몇 번이나 수행할 수 있는지를 해시파워라고 합니다.

해시파워가 높은 마이너(채굴자)일 수록 더 많은 문제를 풀 수 있고 더 많은 문제를 풀 수 있는 채굴자가 새로운 블록을 찾을 확률이 높습니다. 따라서 PoW를 정의할 때 많은 일을 한 채굴자에게 더 많은 보상이 주어지는 방식이라고 표현합니다.

채굴난이도는 지속적으로 높아지고 시간마다 채굴 될 수 있는 블록이 한정되어 있기에 이제는 개인이 채굴을 하는 것이 거의 불가능 합니다.

기업들은 더 많은 블록을 채굴하기 위해 해시파워를 유지해야하고 이를 위해 고사양 장비가 필요하다 보니 과도한 전력소모가 발생하게 되었습니다.

비트코인으로 인한 환경문제가 제기 되는 것도 이러한 채굴을 위한 전력 소모 때문입니다.



[안드로이드 버전 다운로드](#) [iOS 버전 다운로드](#)
[신규 유저 한정 이벤트\(입금 및 거래 시 10,055USDT 보상\) <<<<](#)

작업 증명(PoW) 특징

작업증명 방식의 합의 알고리즘은 어떤 트랜잭션이 발생했을 경우 해당 트랜잭션이 유효한 트랜잭션인지에 대한 합의 방법 및 새로운 블록이 진짜인지, 가짜인지에 대한 검증을 수행합니다.

채굴

마이닝(Mining, 채굴)은 쉽게 말하면 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 실행됩니다.

이러한 수학 문제를 풀이하는 과정을 1초에 몇 번이나 수행할 수 있는지에 대한 수치 정보를 해시파워라고 표현합니다.

해시파워가 높다는 것은 주어진 시간당 더 많은 문제를 풀어낼 수 있다는 의미이며 이에 따라 새로운 블록을 찾을 확률이 더 높아집니다. 결국 높은 해시파워를 가진 채굴자는 확률적으로 더 많은 보상을 받게 됩니다.

작업 난이도

작업 난이도는 논스값 계산의 어려운 정도를 나타냅니다. 작업 난이도는 블록 헤더 정보에서 bits라는 값으로 조절됩니다.

난이도는 2,016개의 블록이 생성되는데 소요되는 시간이 평균 시간인 20,160분보다 적게 걸리면 난이도가 올라가고, 오래 걸리면 낮아지는 방식이다, 대략 20,160분 주기로 전체적으로 평균 10분이 소요되는 하나의

난이도가 전체에 적용됩니다.

보상

보상은 새로 발행되는 비트코인과 해당 블록에 포함되는 거래의 거래 수수료의 합이다. 비트코인의 새로운 발행은, 채굴자가 블록을 처음 구성할 때 채굴자의 지갑으로 일정량의 비트코인이 입금되는 거래를 그 블록의 첫 거래(generation transaction)로 추가하는 방식으로 이루어집니다.

새로 발행되는 비트코인의 시작은 50BTC이다. 그 후 21만개의 블록이 블록체인에 추가될 때마다 반감기를 겪게 됩니다. 거래 수수료는 각 거래 당사자끼리 자율적으로 정할 수 있습니다. 또한 거래 수수료는 거래가 블록에 추가되는 우선 [순위](#)를 결정하는데 입력 값으로 작용하기도 합니다.

작업증명(PoW)의 장점 및 단점

장점

- 최소 가격대 형성이 확실하게 정해져 있음
- 강력한 보안성
- 서비스 남용을 쉽게 방지

단점

- 채굴난이도가 높아지면서 연산에 필요한 고사양 장비가 많이 필요하고, 과도한 전력소모로 인한 에너지 낭비가 커짐
- 채굴난이도가 높아지면서 개인 채굴자는 채굴을 할 수 없는 수준까지 옴
- 지속적으로 해시파워를 유지해야 함
- 채굴하는 업자끼리의 단합 문제

투자 교육 더 보기:

[이더리움 채굴이란? 이더리움 2.0 에도 계속 채굴할 수 있을까?](#)

[페이코인\(PCI\)이란? 2주 안에 재탄생할 수 있을까?](#)

[더 샌드박스\(The Sandbox\)란? | 블록체인 게임 소개](#)

[유니스왑\(UNI\)이란? 유니스왑 사용 방법](#)

[스테이블 코인\(Stable\)이란? 어떤 종류가 있을까? 코인 전망은?](#)

[엑시 인피니티\(AXS\)란 무엇인가요? AXS 코인 전망 분석](#)

[다오\(DAO\)란 무엇입니까? 다오의 참여 방법은?](#)

[비트코인 채굴 소개-비트코인 채굴 방법 및 현황은?](#)

[비트코인 채굴 방법 소개-수익을 낼 수 있는 3가지 방법!](#)

[이더리움 창시자 비탈릭 부테린,어떤 사람인가요?](#)

[하드포크\(hardfork\)란? 하드포크는 호재일까? 코인 대한 미치는 영향은?](#)

[메타버스 관련주 리스트 정리, 메타버스 ETF는? 관련주 투자 전망 및 방법](#)

[니어 프로토콜\(NEAR\) 이란?](#)

[NFT 코인이란? NFT 코인 종류 정리 및 소개](#)

[비트코인 도미넌스 뜻은? 선물 거래에 비트 도미넌스 사용 소개!](#)

[위믹스 코인\(WEMIX\) 은? 국내 4대 거래소 상폐...향후 전망은?](#)

[코인 차트 보는 법 소개 \(캔들차트\) | 초보자 가이드](#)

[میم 코인이란? 어떤 인기 밈 코인있을까? 향후 전망은?](#)

[리플\(XRP\) 코인이란? 어떤 용도가 있을까? 향후 전망은?](#)

[메타버스 관련주 리스트 정리, 메타버스 ETF는? 관련주 투자 전망 및 방법](#)

[코스피\(200\) 야간 선물 이란? 그의 거래시간 및 투자 방법은?](#)

[2023년 비트코인 투자 가이드 총 6개 정리 및 코인 거래소 추천](#)

[레버리지란 무엇인가요? 가상화폐 레버리지 거래는 방법은?](#)

[레버리지/ 마진을 통해 비트코인을 늘리는 방법 \(뉴비\)](#)

[2023 국내 TOP 암호화폐 거래소 리스트 정리 및 해외 거래소 추천](#)

[암호화폐 사는 법 소개 -안전하고 편리하게 수익을 냅니다.](#)

[마진거래 소개,마진 및 레버리지 어떤 관계? 마진거래 방법은?](#)

[비트코인 구입 방법 - \(업비트, BTCC\) 초보자 가이드](#)

[비트코인 레버리지/마진거래 하는법 및 관련 거래소 순위](#)

[USDT 구매방법 알아보기, BTCC에서 코인교환 및 계좌이체로 USDT 구매](#)