이더리움 작업증명(PoW) 및 지분증명(PoS), 더 좋은 것?

원문:
https://www.btcc.com/ko-KR/academy/research-analysis/ethereum-proof-of-work-pow-and-proof-of-stake-pos-which-one-is-better

지난 11일(한국시간) 이더리움의 '머지(Merge, 병합)' 업그레이드를 선행하는 세 번째이자 마지막 '골리'(테스트 환경 네트워크, 테스트넷)' 병합이 성공적으로 진행됐습니다. 이와 동시에 이더리움을 POW와 POS의 두 블록체인으로 하드포크해야 하는지도 암호화폐 업계에서 화두가 됐습니다.

미국 암호화폐 거래소 크라켄이 두 매커니즘을 분석하고 각각의 장단점을 비교했습니다.11일(현지시간) 크립토슬레이트에 따르면 크라켄은 PoW와 PoS에 대해 "한 쪽이 다른 한 쪽보다 더 나은 옵션이 될 수 없다"고 밝혔습니다.

이더리움이 내달 작업증명(PoW)에서 지분증명(PoS)으로 합의매커니즘을 변경하는 대규모 업그레이드 '머지(Merge)'를 준비 중인 가운데, 한쪽에서 하드포크(블록체인 분리)를 통해 PoW 기반 이더리움을 유지하려는 움직임이 나오면서 두 합의매커니즘에 대한 관심이 커지고 있습니다.

관련페이지:

이더리움, 마지막 테스트넷 '골리' 병합 완료...ETH 급상승 - BTCC

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 합니다.

지분증명(POS,Proof-of-Stake)은 블록체인에서 거래를 처리하고 새로운 블록을 생성하는 데 사용되는 암호화폐 합의 메커니즘입니다. 디지털자산의 지분을 더 많이 가질수록 그에 비례하여 블록에 기록할 권한이 더 많이 부여됩니다.

관련페이지:

작업증명(PoW) 은 무엇입니까? | 코인 용어 소개 - BTCC

지분증명(POS)란 무엇입니까? | 코인 용어 소개 - BTCC

이더리움 POW VS POS

보안 PoW win

시빌 공격은 암호화폐 부문에선 '51% 공격'이라고 하는데, 전체 네트워크를 장악하려면 전체 노드의 최소

51%를 통제할 수 있어야 하기 때문이다. 블록체인의 핵심은 '탈중앙성'이기 때문에 시빌 공격에 대한 저항력은 블록체인에 대한 상당히 중요한 평가 기준이 될 수 있습니다.

PoS와 달리 PoW의 가장 큰 장점은 해킹을 방지하는 것입니다. 이 합의 모델은 많은 컴퓨팅 파워와 노력이 필요하기 때문에 해커가 시스템을 변경하는 것은 매우 어렵습니다. 그렇게 하려고 해도 장비, 전기 및 노력의 비용이 얻은 이익보다 클 것입니다. 그리고 블록은 변경이 거의 불가능하기 때문에 사용자는 모든 트랜잭션의 신뢰성과 추적성을 유지한다고 확보할 수 있습니다.

탈중앙화 PoW win

PoW는 거버넌스(운영)을 조작·통제하기 어렵습니다. 하나의 노드가 하나의 투표권을 행사해 네트워크 전체의 합의를 강제할 수 없기 때문입니다. PoS에서 지분이 많은 개인이 거버넌스 결정에 우위를 가질 수 있다는 점과 대조됩니다. PoS는 코인 예치를 많이 한 노드가 거버넌스 투표에서 우위를 점할 수 있어 중앙집중화될 가능성이 있습니다. 만약 노드가 되기 위한 초기 예치 기준이 높아져 진입까지 어려워지면 블록체인은 더욱 중앙화될 위험이 있습니다.

포크 위험 PoW win

PoW 설계 상 '포크(체인 분리)' 실행을 방해한다. PoW 채굴자는 채굴 작업에 '전력'을 투입하기 때문에 존폐 여부를 확신할 수 없는 '포크된 체인'을 위해 채굴에 나서는 위험을 감수하는 것을 꺼리게 된다. 반면, PoS는 채굴자가 수익을 늘리기 위해 원래 체인과 포크된 체인 모두에 쉽게 스테이킹(예치)할 수 있기 때문에 PoW보다 포크를 진행하는 것이 수월할 수 있다.

확장성 PoS win

확장성을 중시하는 블록체인의 경우, PoS가 훨씬 효율적인 솔루션이 될 수 있습니다. PoS는 블록 검증자를 무작위로 선정하기 때문에 채굴에 대한 경쟁이 없고 효율적입니다. 블록체인의 처리 속도를 높일 수 있고, 악의적 행위자를 차단할 수 있어 스마트 컨트랙트 운영에 적합할 수 있습니다.

환경 문제 PoS win

PoW의 단점은 전력 소비에 크게 의존한다는 점입니다. PoW 블록체인이 채택에 환경에 악영향을 미칠 것이라는 우려가 높아지면서 관련 규제 제약도 커지고 있습니다. PoS는 자신의 코인 보유량에 비례해 코인을 배분받기 때문에 채굴 작업이 필요 없습니다.

따라서 PoS로의 전환은 대규모의 해시파워 낭비를 줄이고 기존 방식에서의 탄소배출과 관련한 부정적인 인식에서도 자유로워지게 됩니다. 또 트랜잭션 처리 속도와 수수료 절감 등도 강점입니다. PoW에 비해 훨씬 더 환경 친화적입니다. 이더리움이 머지 업그레이드를 진행하는 주된 이유 중 하나입니다.

접근성 PoS win

PoW 채굴자는 고급 채굴 장비를 구입하기 위한 초기 비용이 들어간다. 아울러, 채굴 효율을 극대화하기 위해 지속적으로 장비를 업데이트해야 한다는 문제가 있습니다. PoS에서 검증인은 값비싼 하드웨어를 구입할 필요가 없으며 일반 PC를 사용하기만 하면 됩니다. 따라서 더 많은 사람들이 노드가 될 수 있습니다. 노드가 많을수록 탈중앙화 정도가 강해집니다. 또한, 합의 프로세스는 더 에너지 효율적이고 더 빠른 트랜잭션 속도를 제공합니다.이는 네트워크 접근성과 참여도를 높이는 데 긍정적입니다.

결론

작업 증명이 고성능 컴퓨터로 복잡한 수학 연산을 해결하는 방식을 통해 블록 생성과 채굴 작업이 진행돼 막대한 전기가 소모되는 반면, 지분 증명은 코인을 많이 예치한 검증인이 블록체인 네트워크의 거래 유효성을 확인하고 코인을 보상받는 방식으로 이뤄집니다.

이에 지분 증명은 전기를 소모하는 채굴 과정이 사라지고 네트워크의 에너지 효율성과 속도도 개선되는 것으로 알려져 있습니다.

이더리움 창업자 비탈릭은 "작업증명 방식은 메인넷에 많은 문제를 일으켰다. 작업증명 유지를 위해 하드포크가 발생한다면 NFT 등 시장의 여러 방면에 혼란을 줄 것으로 예상된다"고 우려했다. 이어 작업증명 고수로 발생하는 문제 해결책을 강구할 책임은 하드포크를 추진한 진영에 있다고 말했습니다.

관련페이지:

이더리움 미지(병합)가이드, 그것에 대한 알아야 할 것 – BTCC

비탈릭 부테린 "더 머지 9월 중하순에 이뤄어질 것", 이더리움 2.0 비전 공개 (btcc.com)

비탈릭 부테린"이더리움이 또 다른 포크로 큰 피해를 보는 일은 없을 것" (btcc.com)

서클 "이더리움 머지 이후 PoS 체인만 지지" – BTCC

바이낸스, 이더리움 머지 지원한다.... ETHW 상장 검토 예정 – BTCC