

학습 정리

팀	그니코인	구성원	송건희, 조호근
---	------	-----	----------

일정	발제자	주제
6/4	송건희	블록체인 기초 이론 공부

주요 내용 요약

- 이더리움 설계 목표
 - 거래 승인 성능 향상
 - 10초 단위의 블록 생성
 - 작업 증명 자원 낭비 축소
 - 수정 GHOST 프로토콜 사용
 - 채굴 역량 집중화 방지
 - 메모리 하드형 Ethash 작업 증명 알고리즘
- 블록 생성 간격
 - 블록 생성 간격이 10 ~ 19초 인가 되도록 조정
 - 짧은 블록 생성 간격으로 블록 전달 지연 시간 비중이 커져 블록 전달 시간 동안 생성되는 부실 블록 발생률이 상승
- GHOST 프로토콜
 - 비트코인은 가장 길이 체인을 메인 체인으로 선택
 - 이더리움은 가장 무거운 서브트리의 가장 길이 체인을 메인 체인으로 선택
 - 부실 블록이 블록 체인 조작 방지에 기여
- 블록 인센티브
 - 블록 보상
 - 정규 블록보상
 - 5 ETH로 고정
 - 삼촌 블록보상
 - 정규 블록보상 대비 87.5% 보상
 - 조카 블록보상
 - 삼촌 블록 하나당 정규 블록보상 대비 3.125% 보상
 - 삼촌 블록을 찾는 것을 유도 하고자 주는 보상
 - 거래 수수료
- Ethash 작업 증명 알고리즘
 - 비트코인은 해시캐쉬 알고리즘 사용
 - 이더리움은 Ethash 알고리즘 사용
- 블록 난이도 조정
 - 난이도 폭탄 로직
 - 난이도를 점차 지수적으로 증가 시켜 블록 채굴을 어렵게 함
 - 작업 증명 기반의 블록 생성 합의 알고리즘을 새로운 소유 기반의 블록 생성 합의 알고리즘으로 전환을 유도하기 위해 도입