

학습 정리

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

일정	발제자	주제
5/31	조호근	블록체인 기초 이론 공부

주요 내용 요약

- 비트코인 작업 증명과 인센티브
 - 작업증명
 - 채굴자들간에 블록에 대한 합의
 - 블록 인센티브
 - 블록보상
 - 거래수수료
 - 인센티브는 코인베이스 거래로 블록 인센티브 지급
 - 작업증명방법
 - 채굴자는 블록 헤더에 대한 해시값이 목표보다 작아질 때 까지 블록 헤더의 너스값을 변경
 - 해시함수
 - 일방향성
 - 임의성
 - 작업난이도
 - 2016개 블록마다 한 번씩 이루어지도록 설계
- 비트코인 블록 체인 합의 프로토콜 1
 - 비트코인 시스템의 특징
 - 인터넷 상의 익명 기반 P2P 시스템
 - 비트코인 합의
 - 블록 합의 전제 조건
 - 자발적 참여 유도
 - 정직한 채굴자에 의해 생성된 블록
 - 합의 작업은 충분히 분산 제어되어야함
 - 분산된 블록체인은 충분히 동기화 상태를 유지해야함
 - 명시적 합의는 어려움
 - 익명성
 - Sybil 공격가능성
 - P2P 네트워크의 불안전성
 - 따라서 묵시적 합의 알고리즘 사용
 - 채굴자가 합의 규칙을 따르면 이익을 제공
 - 합의 규칙을 따르지 않으면 불이익을 받음
 - 비트코인 분산 합의 정책
 - 인센티브 정책
 - 작업 증명 정책