학습 정리

팀	그니코인	구성원	송건희, 조호근

일정	발제자	주제
5/29	조호근	블록체인 기초 이론 공부

주요 내용 요약

- 비트코인 거래 시스템을 구축하며 블록체인에 대한 이해도를 높히기 위해 블록체인 이론을 공부

- 비트코인 암호 기초
    - 해시 함수
        - 특정 메시지에 대해 짧고, 일정하며, 고유한 해시값 생성
        - 서명을 위한 문서 지문 생성
        - 블록체인에서 블록간 연결에 활용
    - 공개키 암호
        - 수학적으로 한 쌍의 서로 다른 키를 생성하고 암호화와 복호화에 서로 다른 키를 사용
        - 공개키 : 주소 생성과 서명 검증
        - 개인키 : 서명 생성
    - 서명
        - 메시지에 대한 해시값 생성
        - 개인키로 메시지의 해시값을 암호화(서명)
        - 메시지와 서명을 전송
        - 공개키로 서명을 복호화
        - 계산된 해시값과 서명의 복호화 값을 비교

- 비트코인이란
    - 비트코인
        - 참여자간 직접 전자 현금 지불 시스템
    - 비트코인 목표
        - 참여자간 직접 거래
        - 투명한 화폐 발행
        - 투명하고 안전한 거래 승인 및 전자 화폐 이동 관리

- 비트코인 네트워크
    - 창여자들에 자발적으로 구축되고 운영
    - P2P 네트워크
    - 비트코인 네트워크를 운영하는 별도의 주체가 없음
    - 거래 정보는 broadcasting 형태로 비트코인 네트워크에 전송
    - 네트워크 참여자는 기본적으로 익명성 보장