**디지털 금, 비트코인**

* 비트코인: 개인 대 개인 전자화폐 시스템
* 2008년 10월 리먼브라더스 사태
  + 이 사건이후 중앙화된 금융기관 불신
  + 기존의 가상화폐는 중앙화된 금융기관을 거침
  + 이중지불을 막기위해 제3자를 필요로 한다면 가상화폐는 그 이점을 잃어버린다.
* 피자데이 – 5월 22일

**블록체인 이해하기**

* Block : Data
* Chain : Link
* 블록은 거래정보와 이전블록에 대한 정보를 담고있다.
  + 거래정보 (transaction) : 특정시간동안 블록체인 사용자들이 비트코인을 전송하는등의 내용을 담음
  + 이전블록 (previousblockhash) : 현재블록 직전의 거래정보가 담긴 블록에 대한 정보를 담음
* 이러한 정보를 가진 블록들을 노드라는 블록체인을 운영하는 컴퓨터들이 서로 나눠가지며 하나의 블록체인 네트워크 구성
* 기존 IT는 중앙집권화된 서버가 존재 거기서 데이터를 받아서 운영
* 블록체인의 특징:
  + 탈중앙화
  + 보안성 : 악의적인 의도로 블록체인에 다른 정보를 심고자한다면 이는 다른 노드와 다르기에 불가능함 (51%의 네트워크를 차지하면 가능)
  + 투명성 : 누구나 노드에 참여가능 = 누구나 조회가능함
  + 확장성 : 데이터 뿐 아니라 기술자체도 오픈소스로 공개돼 있음 -> 더욱 안전하고 발전된 블록체인 개발가능

**블록의 구조 살펴보기**

블록의 구조:

* 현재 블록 해시
* 블록 헤더
* 거래 개수
* 블록 바디
  + 해시(hash) : 함수의 한 종류
    - 항상 같은 길이의 값 출력
    - 조금만 입력값이 달라도 다른 결과 출력
    - 역산이 불가함(단방향 함수)
* **블록 생성 과정**
  + 거래내역들을 해시함수를 통해 거래 해시값으로 변환
  + 거래 해시값들을 묶어서 다시 해시값으로 변환(홀수인경우 마지막 해시값을 복사해서 다시 해시 진행)
  + 계속 이 과정을 진행하면 단하나의 해식ㅄ만 남고 이를 머클루트 해시값이라고 하며 이를 우리는 블록에 저장하고 새로운 블록이 탄생하게됨
  + 블록에는 소프트웨어 버전, 이전블록 해시, 블록 생성시간, 난이도, Nonce, 머클루트 해시값을 지님
* **채굴**
  + 채굴이라는 과정을 통해 검증절차에 들어감 (블록 생성 시간, 난이도, Nonce에 따라)
  + 생성된 블록을 검증해 나가는 과정이며 채굴을 성공한 작업자에게 가상화폐를 주어 이를 격려함
  + 2016번째 블록이 생성될때마다 난이도 조정이 들어감(블록생성시간에 따라)
  + PoW : Proof of Work : 작업증명방식 : Cpu 동작이 한번 작업증명을 충족하는데 동원됐다면 그 블록은 해당 작업을 재수행하지 않고는 변경될 수 없다.
    - 만일 다수 CPU파워가 정직한 노드에 의해 통제된다면, 가장 정직한 사슬이 가장 빠르게 늘어나 다른경쟁 사슬을 압도할 것이다.
  + PoS : Proof Of Stake : 블록을 검정하는 방식을 지분을 통해 결정, 전력소비가 적다, 네트워크 지분 == 가상화폐 보유량

**2세대 블록체인, 이더리움**

* 비트코인의 한계점: 전자화폐시스템,
* TPS (Transaction Per Second) 초당 거래 처리량
* 비트코인은 거래속도가 실생활에서 사용하기엔 느리다는 문제점
* 비트코인 네트워크는 누구나 참여가 가능함, 블록을 채굴가능, -> 어떤 노드가 채굴한 것을 정식블록으로 인정할 것인지 기준이 필요함
  + 가장 많이 블록을 생성한, 가장 길이가 긴 것을 정식으로 인정하기로 함-> Longest chain, 나머지는 고아블록
* 비탈릭 부테린: 2세대 블록체인 이더리룸의 개발자
* 이더리움 : 차세대 스마트 컨트랙트와 탈중앙화된 어플리케이션 플랫폼

**스마트 컨트랙트** : 기존의 계약은 중개인이 필요함, 하지만 스마트 컨트랙트는 코드상에 계약내용을 명시하여 중개인이 필요하지 않음

* 이터리움이 제공하려는 것은 완벽한 튜링완전(turing-complete) 프로그래밍 언어가 심어진 블록체인이다.
  + 튜링완전(turing – complete) : 어떠한 질문을 통해 사람인지 컴퓨터인지 구분하지 못한다면 튜링완전이라고 부른다.
    - 조건설정과 반복명령어가 반드시 필요함
  + 비트코인에서는 단순히 누가 누구에게 얼마를 전송한다 정도의 기능만 구현가능
  + 이더리움에서는 복잡한 방법으로 송금가능, 특정한 조건 부여해서 이 조건이 충족되었을때만 전송되게 -> 이더리움이 플랫폼으로 나아감
    - NFT, Defi, DAO 등 블록체인 플랫폼을 기반으로하는 서비스들이 등장
      * 이때 블록체인상에서 제공되는 서비스들을 Decentralized Application, Dapp이라고 부름

**탈중앙화 앱, Dapp**

* **Defi : 탈중앙화 금용**
  + 가상화폐가 탈중앙화돼 있더라도 그 돈을 중앙화된 금융기관이 운용한다면 기존 문제가 똑같이 발생가능
  + PancakeSwap : 코드로만 구성됨
* **DAO : 탈중앙화 자율 조직**
  + 의사결정규약 : 코드(스마트 컨트랙트)
  + 의사결정구조: 분산형 거버넌스, 직접민주주의
  + 거래방식: 암호화폐, NFT
  + DAO’s dilemma:
    - 특정 몇 명이 토큰을 독점한다면 기존방식과 차이없음
    - 모두가 공평하게 나눠가지면 책임소재 불분명