introduction

- 은행은 사람에게 돈을 빌려준다
- 그럼 그 은행의 돈은 어디서 오는가?
  - 개인이 대출하는 소액의 돈은 은행에 예금된 돈으로 충당
  - 하지만 기업이 대출하는 천문학적 돈은?

- 미국 연방 준비은행
  - 개개인이 아니라, 국가 단위 공인 은행과 거래하는 은행
  - 매일 수 조 달러 규모의 거래 처리
  - 금액이 금액인 만큼 보안에 엄청난 신경을 써야 함

motivation

- 이런 거래Transaction은 몇가지 불편 사항이 존재
  - 기술적인 강제성 대신 신뢰에 기반하여 거래하는 것이 보통
    - ex) 이 기업을 믿을만하니 계약서를 쓰면 돈을 줄 것이다
    - 기업이 사기를 치면? 기업이 없어지면? 기업이 국유화되면?
  - 규모가 커지면 일반 사용자는 사용할 수가 없게됨
    - 조 단위 거래가 이루어지는데 초점을 맞춤
    - 몇만원짜리 일반 사용자간의 거래는 아예 불가능

- 해결 방법?
  - 기술적으로 트랜잭션을 완전한 보안과 안정성을 주자
  - 기업 같은 어떤 주체를 신뢰할 수 없다 → 분산 저장하자

Ethereum Virtual Machine

- 일반화된, 안전한, 소유자가 없은 거래 시스템
  - 일반화된 : 거대 기업/은행만 이용할 수 있는게 아니다
  - 안전한 : '믿음으로 하는' 거래가 아니라, 수학적으로 안전
  - 소유자가 없는 : 어떤 거대 기관의 관리가 아니라, 분산 시스템이다

- 일반 PC 프로그램처럼 작성하면, 알아서 분산 처리
- 개발자는 EVM 위에서 Javascript나 Python 프로그램과 같은 익숙한 언어로 만든 모델을 작동시킬 수 있다

blockchain과 병렬성

- 이더리움도 p2p 네트워크 프로토콜
- 이더리움은 데이터를 연결된 네트워크 상의 node에서 관리
  - node : 이더리움 네트워크에 참여한 컴퓨터
  - 모든 node는 EVM을 실행하고, EVM에서 동일한 명령어를 실행
    → 모든 node가 동일한 명령어? 비효율적인거 아닌가?
  - 대신 EVM에서 합의consensus를 하며 작동해나감
    → 누군가 실행한 명령을 모두가 consensus하여 인정
    → 어떤 node가 꺼졌다 켜졌으면, 빼먹은 내용을 전달
    → 악의적인 공격자 node의 제안을 거부

EVM의 장점

- 튜링 완전이기에 다른 언어처럼 그냥 사용해도 된다
- 하지만 장점을 꼽으라면..
  - 다른 사용자와 직접 상호작용하거나
  - 다른 그룹과 연결되어 작동하는 프로그램에 적합
- 예를 들어
  - 사용자들이 협력해야 되는 것 : 공유 자전거 사용 프로그램
  - 사용자들의 보안과 안전성이 중요한 것 : 영수증 발행

- 심지어 대통령 투표도 가장 안전하고 완벽하게 수행할 수 있다

EVM 비용

- EVM 프로그램을 꽁자로 돌린다면?
  - 사용자들의 node 위 EVM에 스팸 및 쓰레기 프로그램이 넘쳐남
  - 사용자들은 아무것도 얻지 못하니 EVM을 종료
  - 결국 아무도 EVM을 사용하지 않게 됨

- 따라서 EVM은 유료며, 적합한 가격이 책정되어야 함
  - 사용자들의 node 위 EVM에서 작업transaction을 수행하면, 보상을 얻음
  - 어떤 작업transaction을 수행하는데 드는 비용 = Gas
  - 주의 : Etherium 코인 가격과 Gas 가격은 동일하지가 않음

EVM 동작 순서

1. transaction이 올바른지 검증
2. transaction 수수료(gas) 계산
3. transaction 요청자(실행자)가 gas를 수행자(node)에게 지불
   - 이때 **지불하는 것 자체**에도 수수료가 듬
   - 왜냐면 1~2도 분명 계산이 필요하니까
   - 만약 gas가 불충분해 transaction이 실행이 안되도, 1~2에 대한 수수료는 node에게 지불하게 되고, 환불 안됨
   - 그게 아니라 node에 문제가 있는 경우에는 환불됨
4. 문제 없으면 gas 지불하고 transaction 실행

EVM과 앱토큰

- EVM 위에서 대형 플랫폼을 개발한다고 하자
  - 플랫폼 개발 비용을 어떻게 충당하는가?
  - 이더리움은 '앱토큰' 발행을 허용한다
- 예를 들면
  - 현식이는 과외 매칭 앱을 EVM 위에서 개발하려고 한다
  - 현식이는 이더리움 위에서 <과외 코인>을 발행한다
  - <과외 코인>을 가지고 있으면, 과외 매칭 앱이 만들어진 후 쓸 수 있다
    - 물론 실제로 쓸 생각을 가지고 사는 사람보다, 투자/투기 목적으로 사는 사람이 대부분
- xx코인, xx토큰 등이 이렇게 만들어지는 경우가 많다

work to do

- 이더리움 개발?
  - https://www.trufflesuite.com/docs/truffle/reference/choosing-an-ethereum-client
- 이더리움 클라이언트?
  - https://www.ethdocs.org/en/latest/ethereum-clients/choosing-a-client.html
- 이더리움 rust 클라이언트?
  - https://openethereum.github.io/
- 스마트 컨트랙트 개발 메소드?
  - https://www.trufflesuite.com/