사이드 체인

https://youtu.be/3l5kAGiW1y8

사이드체인(Sidechain)

- 사이드 체인

  - 블록체인의 메인체인 네트워크와 연결된 블록체인

  - 기존 메인 블록체인 노드 + 사이드 블록체인 노드

  - 서로 다른 블록체인들 위에 존재하는 자산을 쉽게 거래 할 수 있도록 하는 기술

비트코인의 한계점

- Slow
- Only Bitcoin
- Only Bitcoin Script
- Non-Confidential Transaction

비트코인의 한계점

- Slow

- 각 블록 생성 간격 10분

- 자신의 거래가 블록체인에 기록되었는지 확인하려면 몇 초~ 수십분 소요

- 이체확인을 받는 시간까지 포함하면 더 길어짐

비트코인의 한계점

- Only Bitcoin

- 오직 비트코인만 이체 가능

- 이종 화폐와의 교환을 위해 중앙화된 웹거래소 서비스 사용

  -> 보안적, 탈중앙화적 이점 사라짐

비트코인의 한계점

- Only Bitcoin Script

- 사용할 수 있는 기능 제한적

- 창의성 발휘 & 고급이체 조건 설정 & 스마트 컨트랙트 코딩 불가

비트코인의 한계점

- Non-Confidential Transaction

- 비트코인 상에서 일어나는 모든 거래 공개됨

->기밀성 x

사이드 체인의 특징

- 저렴한 수수료
- 빠른 트랜잭션 처리 시간
- 각각 존재하는 서로 다른 암호화폐들 사이의 다리 역할
- 사이드체인 기술 활용시, 해당 암호화폐의 성능 업그레이드 가능

거래방식

- 멀티시그(multi-sig)
- 브릿지(bridge)
- 멀티시그 브릿지
- 콜레트럴 브릿지
- 플라즈마

거래방식

- 멀티시그(multi-sig)

- 개인키를 세 곳(본인, 대행업체, 기관 등)에 등록

- 가장 간단한 방식 -> 암호화폐 지갑에 적용

- 사용자의 개인키를 포함해 두 곳의 개인키 서명 필요

거래방식

- 브릿지(bridge)

- 멀티시그의 다중 서명을 통해 토큰의 출입을 허가하는 방식

- 토큰을 이동시키는 행위 외에도 주기적으로 검증을 위한 앵커링 작업

*앵커링?

브릿지의 오퍼레이터가 각 체인에 상대방 체인 내역을 모았다가 주기적으로 병합하여 브릿지로 연결되더라도 시스템에 별도의 거래 장부가 필요하지 않은 것

거래방식

- 멀티 브릿지(multi - bridge)

1. 송금을 원하는 거래자는 먼저 브릿지에 자신의 토큰 등록
   ->토큰이 등록되면 브릿지는 잠김
2. 요청자 개인키 = 건너편 상대방 개인키의 멀티시그 합
   -> 토큰의 이동 승인
3)토큰 이동 승인시 잠금 해제

* 오퍼레이터는 토큰을 전송해주는 대가로 수수료 얻음
* 트랜젝션의 서명을 검증하는 수수료가 많이 들어 사용료 비쌈
* 오퍼레이터는 사용자들이 발생시킨 모든 트랜잭션과 이로 발생하는 이벤트를 전부 감시해야하는 제약이 있음.

거래방식

- 콜레트럴 브릿지

- 어떤 거래자도 신뢰할 수 없는 환경에서도 가능할 효율적인 브릿지

1) 사용자가 브릿지에 전송할 금액을 에치

2) 검증자는 누가 금액을 넣었는지 확인 후 브릿지 잠금

3) 전송이 성공적으로 이뤄지면 잠금이 풀려 브릿지에서 인출

-> 이 과정에서 예치된 금액을 훔치거나 비정상행위 발생시 콜레트럴 브릿지의 검증자가 담보로 예치된 금액의 일부를 사용자에게 지급

거래방식

- 플라즈마

- 브릿지 노드 필요x
-수수료 경제 모델에 기반하여 오프체인에서 거래 진행
-사용자들이 콘인을 직접 관리 가능
-데이터를 처리하는 방식과 블록생성자를 다루는 정책에 따라 다양한 버전 존재
- 이더리움 블록체인 내부에 작은 블록체인 만드는 방식
- 내부에 별도의 합의 알고리즘 필요x
- 이더리움 메인체인과 플라즈마는 평소에는 별개의 블록체인으로
    -> 필요시, 사용자가 백도어를 통해 자발적으로 드나들 수 있음.

Mechanism 비교

비트코인의 소유권 이전 행위	비트코인을 텐더민트 블록체인 위에서 거래
1) 누군가가 특정 비트코인(Unspent Bitcoin Output)의 소유권 이전을 공개키와 개인키로 증명을 통해 승인 2) 승인하는 순간 비트코인은 이체 실행 3) 이렇게 다른 계좌로 이동된 코인을 또 다른 누군가가 공개키와 개인키를 이용 ->소유권 증명, 이체 승인 4) 승인하는 순간 비트코인은 이체	1) 비트코인을 특정한 목적으로 생성된 계좌에 전송 2) 계좌에 전송하는 당사자는 해당 비트코인에 대한 권한을 잃게 되며 그 비트코인은 동결(immobilized)됨 3) 동시에, 그 비트코인에 상응하는 코인이 텐터민트 블록체인 위에 생성 4) 해당 코인을 텐더민트 블록체인 위에서 다양한 다른 코인이나 기타 상응물들과 자유롭게 거래 5) 해당 비트코인의 최종 소유자가 이를 비트코인 블록체인에 있는 원래 비트코인으로 바꾸길 희망 6) 텐더민트 위에 생성되었던 비트코인 삭제-> 실제 비트코인 블록체인 위의 비트코인의 동결 풀림 7) 최종 소유자는 자신의 이체 권한을 해당 비트코인에 행사 가능

Q & A