https://github.com/habit80/myBlockPanda

4. Advanced Concepts of Blockchain

Contents

1. 포크(Fork)의 이해

포크(Fork)란 무엇인가?

- **정의**
  - 블록체인의 규칙이 변경되어 기존 체인에서 새로운 체인이 분리되는 현상

- **원인**
  - 소프트웨어 업그레이드
  - 커뮤니티 분쟁
  - 보안 취약점 수정

- **포크의 유형**
  - **하드포크 :** 기존 체인과 호환되지 않음 (ex. 비트코인 캐시)
  - **소프트 포크 :** 기존 체인과 호환 가능 (ex. SegWit)

1. 포크(Fork)의 이해

하드 포크 vs 소프트 포크

특징	하드 포크 (Hard Fork)	소프트 포크 (Soft Fork)
정의	이전 블록과 호환되지 않는 새로운 체인 생성	이전 블록과 호환되는 체인 규칙 변경
네트워크 분리 여부	분리 가능 (두 개의 체인이 공존)	분리 없음 (하나의 체인 유지)
예시	비트코인 → 비트코인 캐시	SegWit (Bitcoin 에서 블록 크기 개선)

1. 포크(Fork)의 이해

포크의 실제 사례

- **비트코인 캐시 (Bitcoin Cash)**
  - 2017년 8월, 블록 크기 증가를 위해 하드 포크 발생
  - 블록 크기 : 1MB → 8MB

- **이더리움 클래식 (Ethereum Classic)**
  - 2016년, DAO 해킹 사건 이후 자금 복구를 위해 하드 포크 발생
  - 원래 체인(클래식)과 새로운 체인(이더리움)으로 분리

2. 레이어 2 솔루션

레이어 2 솔루션이란?

- **문제점**
  - 블록체인은 확장성이 낮고, 처리 속도가 느리며, 높은 수수료가 발생

- **해결책**
  - 레이어 2 솔루션을 통해 메인 체인 외부에서 작업을 처리

- **주요 레이어 2 솔루션**
  - 라이트닝 네트워크
  - 롤업 (Rollups)

2. 레이어 2 솔루션

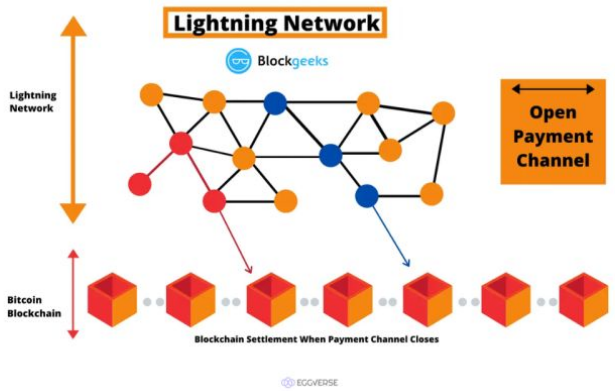
레이어 2 솔루션 (라이트닝 네트워크)

- **개요**
  - 비트코인의 확장성을 개선하기 위해 설계된 레이어 2 솔루션
  - 오프체인에서 다수의 트랜잭션을 처리하고, 최종 결과만 메인 체인에 기록

- **작동 원리**
  - 두 사용자 간에 결제 채널을 넣고, 다수의 거래를 오프체인에서 처리
  - 최종 결과만 메인 체인에 기록

- **장점**
  - 빠른 거래 처리 (즉각적)
  - 낮은 수수료

- **한계**
  - 초기 설정 비용 및 채널 관리 복잡성



2. 레이어 2 솔루션

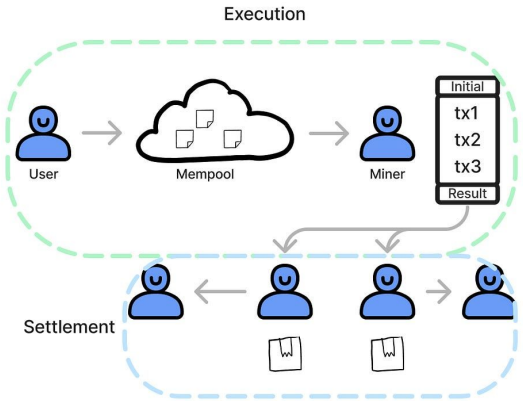
레이어 2 솔루션 (라이트닝 네트워크)

- **라이트닝 네트워크 관련 프로젝트**
  - **Strike**
    - 라이트닝 네트워크를 사용한 지불 및 송금 애플리케이션
    - 비트코인을 즉각적이고 저렴하게 송금 가능
  - **Lightning Labs**
    - 라이트닝 네트워크를 구현한 주요 개발사
    - 라이트닝 네트워크 프로토콜을 개선하고 확장성을 지원

2. 레이어 2 솔루션

레이어 2 솔루션 (롤업, Rollups)

- 개요
  - 이더리움의 확장성을 개선하기 위해 설계된 레이어 2 솔루션
  - 트랜잭션 데이터를 압축하고, 다수의 트랜잭션을 묶어 메인 체인에 기록
- 작동 방식
  - 다수의 트랜잭션을 묶어 메인 체인에 제출
- 종류
  - **ZK-Rollup**
    - Zero-Knowledge Proof를 사용해 빠르고 신뢰 가능한 검증
  - **Optimistic Rollup**
    - 트랜잭션을 유효하다고 가정하고, 이의가 있을 경우 검증
- 장점
  - 메인 체인 부하 감소
  - 더 많은 거래 처리 가능



2. 레이어 2 솔루션

라이트닝 네트워크 vs 롤업

기술	라이트닝 네트워크	롤업
주요 대상	비트코인 (BTC)	이더리움 (ETH)
주요 코인/프로젝트	BTC, LTC, Strike	Optimisim, Arbitrum, Polygon, zkSync
작동 방식	결제 채널을 통해 오프체인에서 다수의 트랜잭션 처리	트랜잭션 데이터를 압축해 메인 체인에 기록
장점	빠른 결제 처리, 낮은 수수료	이더리움의 확장성과 보안성 개선

2. 레이어 2 솔루션

레이어 2 솔루션 선택 시 고려 사항

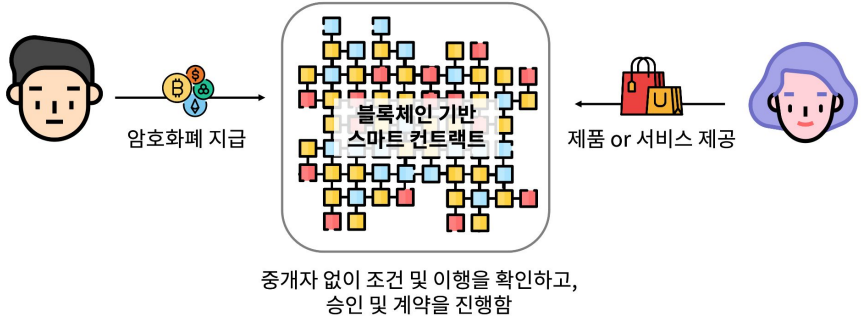
- **목적에 맞는 솔루션**
  - 비트코인 기반이라면 라이트닝 네트워크
  - 이더리움 기반이라면 롤업 기술

- **트랜잭션 유형**
  - 소액 결제 및 빠른 거래 : 라이트닝 네트워크
  - 스마트 컨트랙트와 복잡한 DApp 실행 : 롤업

3. 스마트 컨트랙트의 원리

스마트 컨트랙트란?

- **정의**
  - 조건이 충족되면 자동으로 실행되는 디지털 계약
- **특징**
  - 신뢰할 수 있는 제 3자 불필요
  - 거래와 계약의 투명성 보장
- **사용 사례**
  - 탈중앙화 금융 (DeFi)
  - NFT 마켓플레이스



3. 스마트 컨트랙트의 원리

스마트 컨트랙트란 예제 (Solidity)

```
pragma solidity ^0.8.0;

contract Voting {
    mapping(string => uint256) public votes;

    function vote(string memory candidate) public {
        votes[candidate]++;
    }
}
```

- 기능
  - 후보자 이름을 입력받아 투표수를 증가
  - 간단한 투표 시스템 구현

4. 샤딩(Sharding)

왜 샤딩이 필요한가?

- **블록체인의 확장성 문제**
  - 기존 블록체인(ex. 비트코인, 이더리움)은 모든 노드가 모든 트랜잭션을 저장하고 검증해야 함
  - 사용자가 많아질수록 트랜잭션 처리 속도가 느려지고, 비용(가스비)이 올라감
  - 샤딩은 이 문제를 해결하기 위해 설계된 기술

- **샤딩의 핵심 목표**
  - **병렬 처리 :** 여러 노드가 동시에 작업을 분담해 네트워크 처리량을 증가
  - **저장 공간 최적화 :** 모든 노드가 전체 데이터를 저장하지 않아도 됨

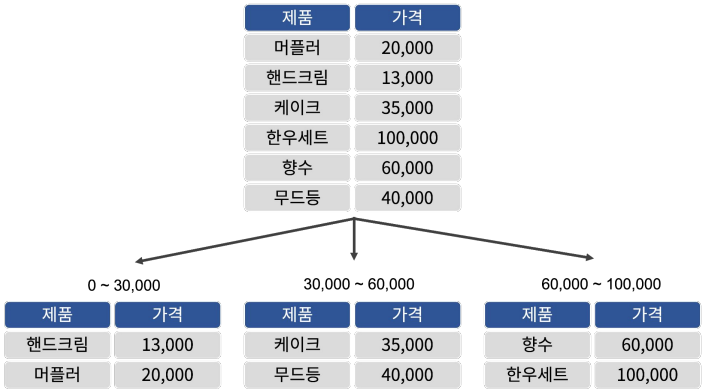
4. 샤딩(Sharding)

샤딩 동작 방식

- **네트워크를 분할**
  - 블록체인을 여러 개의 샤드(Shard)로 나눔
  - 각 샤드는 네트워크의 작은 부분으로, 자신만의 트랜잭션을 처리하고 데이터를 저장

- **샤드에 노드 할당**
  - 노드들은 특정 샤드에 할당되어 해당 샤드의 데이터만 처리하고 검증
    ex. 네트워크에 100개의 노드와 5개의 샤드가 있다면, 각 샤드에 약 20개의 노드가 배정 됨

- **샤드 간 통신**
  - 서로 다른 샤드에 있는 데이터나 트랜잭션이 연결되어야 할 때는 크로스샤드 통신을 통해 데이터 공유



5. 블록체인 보안 이슈

51% 공격

- **개요**
  - 한 그룹이 네트워크의 해시파워를 **51%** 이상 장악
  - 트랜잭션 취소, 이중 지불 가능

- **51% 공격 시나리오**
  - 공격자가 해시파워의 **51%** 이상 장악
  - 기존 블록을 재작성하거나 새로운 체인 생성
  - 이중 지불로 트랜잭션 무효화
  - **결과 :** 네트워크 신뢰 손실, 자산 손실

5. 블록체인 보안 이슈

Sybil 공격

- **정의**
  - 다수의 가짜 노드를 생성하여 네트워크를 혼란시키는 공격

- **영향**
  - 네트워크 신뢰 손상
  - 합의 과정 방해

- **방어책**
  - 합의 알고리즘(PoW, PoS)
  - 신뢰 기반 시스템 도입

5. 블록체인 보안 이슈

키 관리 문제

- **문제점**
  - 개인 키 분실 → 자산 복구 불가
  - 키가 유출되면 자산 도난 가능

- **해결책**
  - 하드웨어 월렛 : 키를 오프라인으로 안전하게 저장
  - 멀티시그 (Multi-Signature) : 여러 키 필요

https://github.com/habit80/myBlockPanda

End