10. 비트코인의 보안

- 보안 원리
    - 특정 가치에 대해서 특정인만 승인한다.
    - 네트워크를 암호화 할 필요가 없다.
    - 따라서, 보안에 대한 책임은 유저가 가지고 있다.
    - 분산화를 꼭 지켜야 한다. 중앙집중식 방법은 편할 수 있지만, 보안에 취약하다.
- 신뢰 루트
    - 양파껍질처럼 중앙에서부터 검증된 보안 체계를 감싸는 또다른 보안체계의 구조
    - 최초 블록을 신뢰 루트로 사용하여 블록을 확장
    - 블록체인이 아닌 다른 곳에 신뢰를 부여하여 아키텍쳐를 설계한다면 보안 취약성이 발생할 수 있다.
    - 비트코인 환전소(거래소)가 신뢰를 다른곳에 부여하여 망한 예.
- 실용적인 사용자 보안
    - 물리적 비트코인 저장
        - 물리적인 종이지갑에 저장
        - 인터넷에 연결되지 않은 오프라인 저장 시스템
    - 하드웨어 지갑
        - 제한된 인터페이스로만 연결되는 하드웨어 지갑 (Trezor - https://steemit.com/kr/@nomad135/trezor)
    - 리스크 균형 맞추기
        - 보안에 너무 신경써서 스스로도 접근하지 못하는 불상사가 잃어나지 않도록 주의하자.
        - 덩어리가 큰 코인을 하나에 담지 말고 여러 지갑에 나누어서 담자
    - 멀티시그
        - 3 - 5 멀티시그와 같이 리스크를 한곳에 두지 않고 분산화 할 수 있다.
    - 생존력(가용성)
        - 키 보유자가 사망시 어떻게 할 것인가? → 가족 혹은 변호사와 멀티시그 등의 방식을 통해서 계획을 세워야 한다.