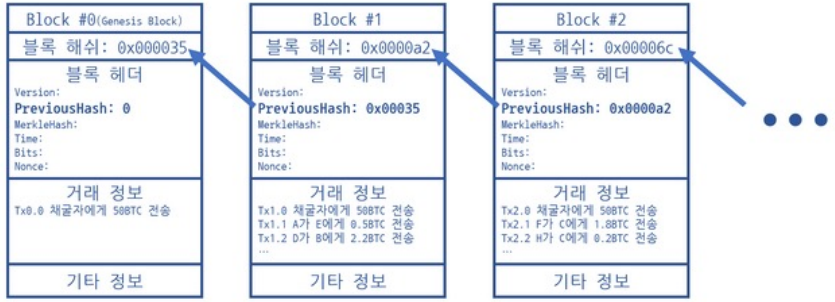
# 블록체인 및 합의 알고리즘

https://youtu.be/792N4OetlF8

# 블록 체인의 기본 원리

- 블록체인
  - 데이터를 가지고 있는 블록을 체인형태로 연결된 구조
  - 데이터에 따라서 다양하게 운용 가능

- 블록체인의 각 블록은 고유한 식별자인 해시 값을 가지고 있음. 이 해시 값은 이전 블록의 해시 값을 포함하여 계산되므로 각 블록은 체인처럼 서로 연결됨
  - 링크드 리스트와 비슷한 구조
  - 이러한 구조로 인해서 위변조가 매우 어려움



# 블록 체인의 특징

- 보안성과 투명성
  - 해시알고리즘을 활용하여 서로 체인을 연결된 구조를 가지고 있어 블록에 담겨 있는 데이터를 조작하는 것이 이론적으로 어려움.
  - 모든 블록안의 데이터는 공개되어 있기 때문에 모든 거래가 투명하게 기록되고 검증됨

- 분산화
  - 탈중앙화는 블록체인에서 빼놓을 수 없는 개념 중 하나.
    - 네트워크에 참여하는 수많은 노드에 거래 기록이 분산되어 저장됨.
  - 탈중앙화로 인해서 새로운 블록의 추가나 기존 블록의 유효성에 대해서 노드 간의 합의가 이루어 져야 함
    - 이를 위해 합의 알고리즘이 사용됨

# 합의 알고리즘의 역할과 중요성

- 합의 알고리즘
  - 블록체인 네트워크에서 네트워크 참여자들이 어떤 데이터가 유효하고 블록체인에 추가될 수 있는지에 대해 합의하는 방법
  - 블록체인은 중앙 집중식 권한이 없는 분산 네트워크이기 때문에 모든 참여자가 동일한 정보를 공유하고 신뢰할 수 있는 기록을 유지하기 위해서 합의가 필수적

- 합의 알고리즘은 블록체인 네트워크에서 보안 강화에서도 중요한 역할을 함
  - 합의 알고리즘는 네트워크의 51% 이상을 통제하지 않는 한, 공격자가 블록체인을 조작하는 것이 어렵도록 함

# 대표적인 합의 알고리즘 - PoW

- Proof of Work(PoW)
  - 참여자들이 복잡한 계산 문제를 해결하여 블록을 생성하는 방식
    - 대표적으로 비트코인이 사용하는 합의 알고리즘
  - 참여자가 새로운 블록을 생성하기 위해서 컴퓨터의 연산 능력을 통해서 특정한 조건을 만족하는 해시값을 찾는 방법
  - 모든 채굴자들은 같은 문제를 해결하기 위해서 경쟁하고 가장 먼저 문제를 해결한 채굴자가 새로운 블록을 추가하고 보상을 획득
    - 이러한 경쟁은 채굴자에게 더 높은 연산력을 갖기 위해서 경쟁
  - 난이도를 조정하여 문제가 너무 쉽거나 어렵지 않도록 조정함

# 대표적인 합의 알고리즘 - PoS

- Proof of Stake(PoS)
  - 참여자들이 네트워크에 보유한 지분에 따라 새 블록을 생성하는 권한을 받음
  - 높은 지분을 보유하고 있는 참여자가 새 블록 생성의 기회를 더 많이 얻을 수 있음
    - 일반적으로는 무작위 선택 과정을 통해 이루어지며, 더 많은 지분을 가지고 있는 참여자가 더 높은 확률로 선택될 수 있도록 되어 있음
  - 마찬가지로 블록 생성 기회를 얻은 참여자는 블록을 생성하고 보상을 얻음

# 대표적인 합의 알고리즘

- 기존 합의 알고리즘의 장점과 단점
  - PoW
    - 가장 큰 장점은 높은 보안성
      - 네트워크를 조작하려면 전체 네트워크의 51% 이상의 연산력을 가지고 있어야 가능
    - 막대한 에너지 소모
      - 경쟁을 통해서 합의가 이루어지기 때문에 이 과정에서 채굴자들은 더 높은 연산력을 위해서 더 많은 에너지를 소모
    - 처리 속도
      - 비교적 낮은 처리 속도, 새로운 블록은 생성하는데 걸리는 처리 속도가 오래걸림. 비트코인의 경우 블록 생성 시간은 10분으로 조절하고 있음
  - PoS
    - 에너지 효율성
      - PoW에 비해서 훨씬 적은 에너지를 사용함. 경쟁을 통해서 합의가 이루어지는 것이 아니기 때문에 높은 연산력을 필요로 하지 않음
    - 경제적 중앙화 문제
      - 지분이 많은 수록 블록을 생성할 기회를 더 많이 얻을 수 있기 때문에, 부유한 참여자가 더 부유해지는 문제가 발생
    - 보안성
      - PoW에 비해서 다른 보안 위험에 노출될 수 있다. 하지만 51%의 지분을 보유하기 위해서는 막대한 비용이 필요하기 때문에 안전하다고 하는 사람도 있음

# Proof of Stack의 종류

- Delegated Proof of Stake(DPoS)
  - 민주주의와 유사한 방식으로, 지분을 보유하고 있는 사람들이 대표를 선출. 대표는 네트워크에서 블록 생성과 거래 검증 등의 중요 역할을 수행
  - 높은 처리 속도와 효율적인 네트워크 운영이 가능하지만, 대표자로 인한 중앙화 경향이 발생하는 것 처럼 소수의 대표자에게 권력이 집중될 수 있음
- Leased Proof of Stake(LPoS)
  - 대출 시스템과 유사한 방법으로, 자신의 지분을 다른 사용자에게 임대할 수 있음. 이를 통해서 지분이 적은 참여자도 임대를 통해서 블록 생성 과정에 간접적으로 참여할 수 있음
    - 임대한 지분을 통해서 블록을 생성할 경우 임대자와 보상을 공유
- Byzantine Fault Tolerance Proof of Stack(BFT PoS)
  - 비잔틴 장군의 문제의 개념을 기반으로 하는 합의 알고리즘.
    - 여러 장군이 있을 때, 전령을 통해서 서로 소통할 경우 배신자가 있거나 중간의 정보 전달이 잘못되더라도 공통된 전략에 도달하도록 하는 개념
      - 즉, 신뢰할 수 없거나 잘못된 정보를 전달하는 참여자가 있더라도 올바른 합의에 도달할 수 있도록 하는 합의 알고리즘

감 사 합 니 다