블록체인

https://youtu.be/4rIUDedVo1w

암호화폐

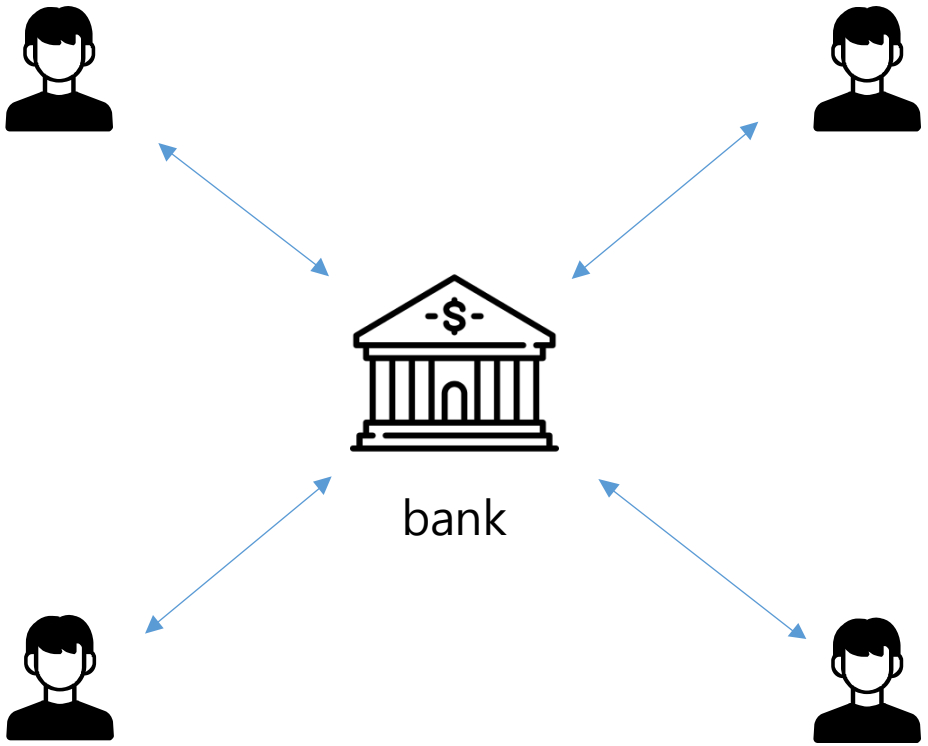
작업 증명

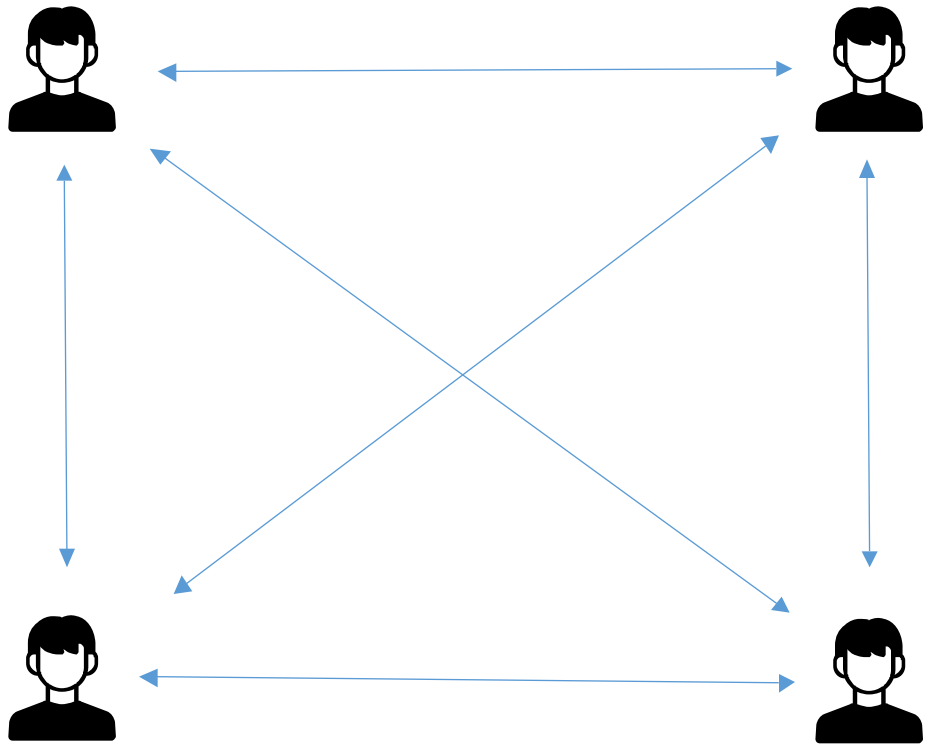
51% 공격

이더리움

암호화폐

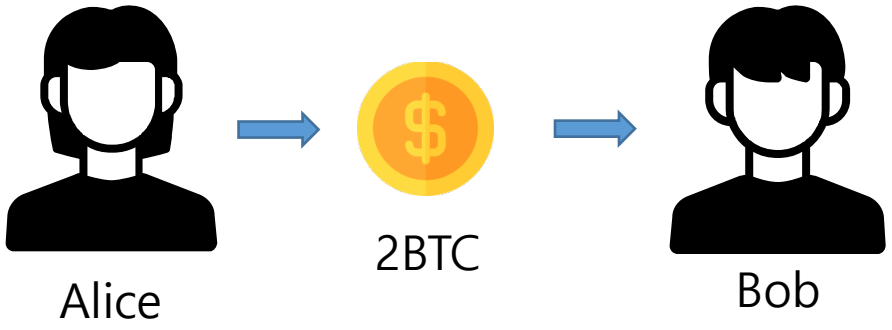
- 디지털 자산
- **탈중앙화** 된 거래방식 (peer-to-peer, p2p)
- **암호화 방식**을 통해 트랜잭션을 검증, 보호, 제어 -> 작업증명

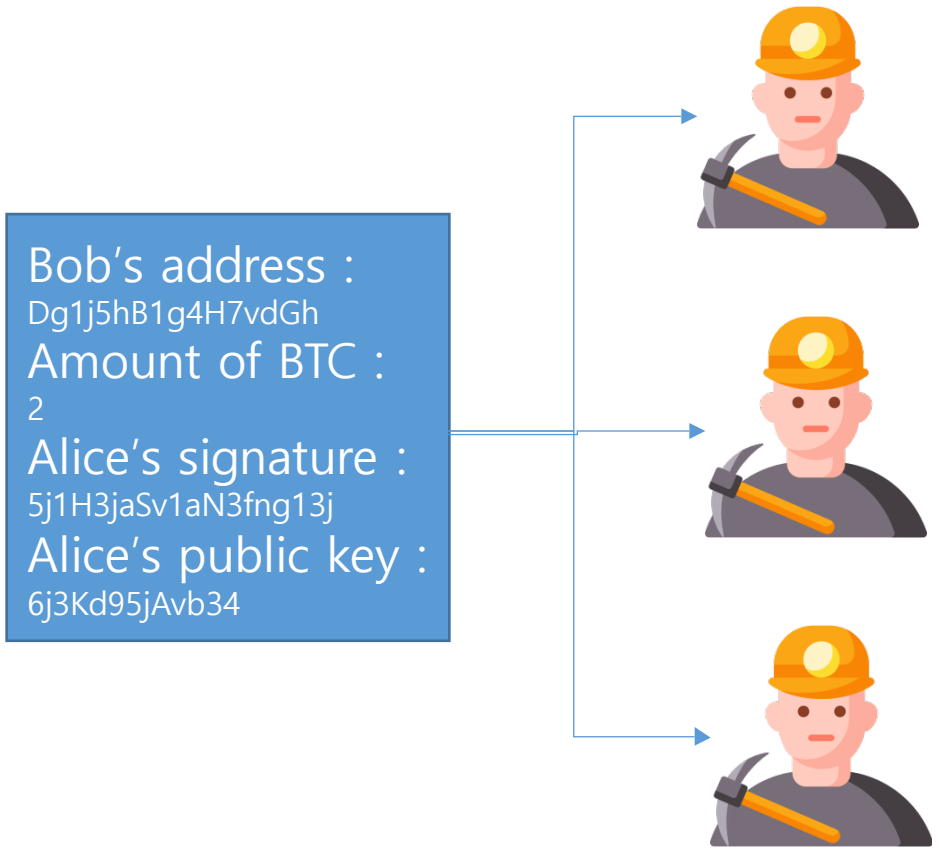




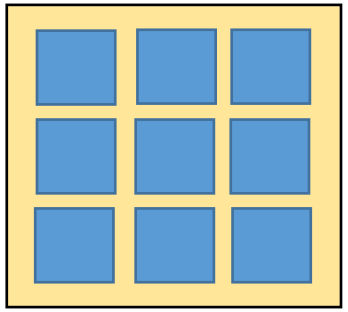
작업증명

- PoW(Proof of Work)
- 각 노드들(채굴자)에 의해서 거래 내용이 검증
- 해시함수, 공개키 암호, 전자서명이 사용됨





작업증명



+

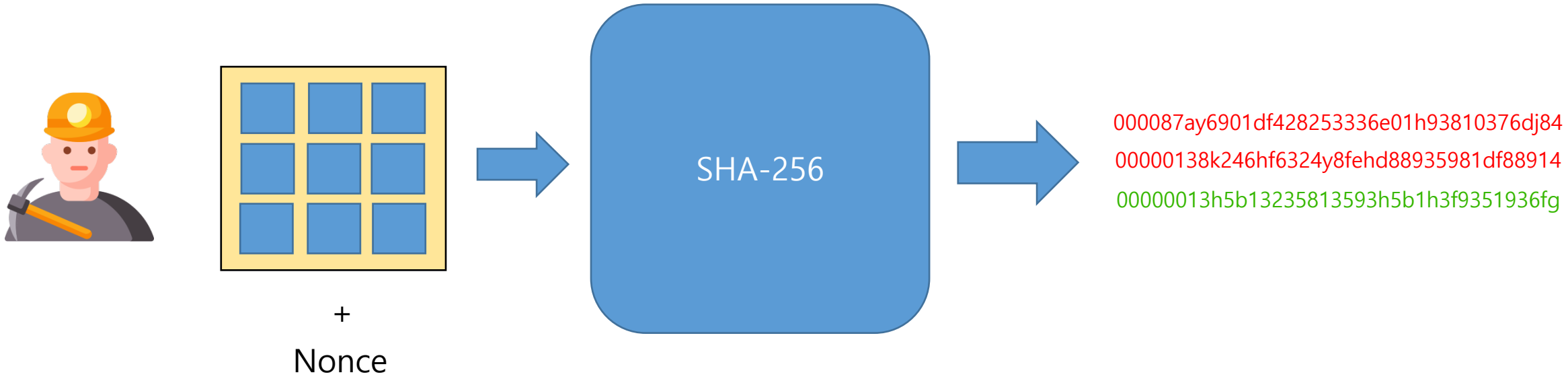
Nonce

SHA-256

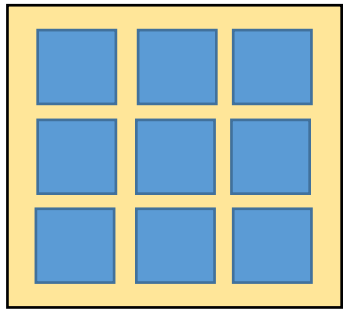
000087ay6901df428253336e01h93810376dj84

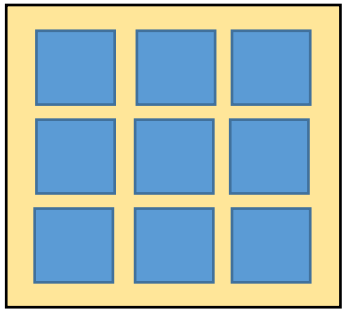
작업증명

- 작업 난이도 : 블록당 평균계산시간 10분을 기준으로 조절됨
  - 2,160개의 블록마다 21,600분 기준으로 조절
- bits로 조절

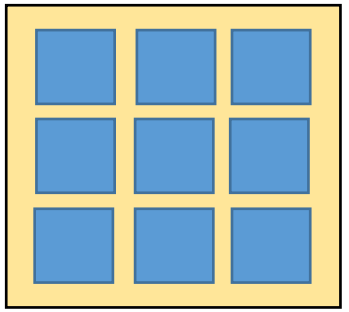


작업증명

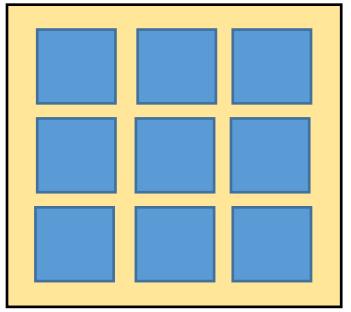




Good!

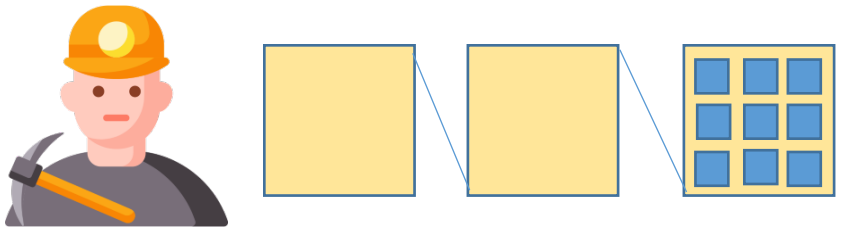


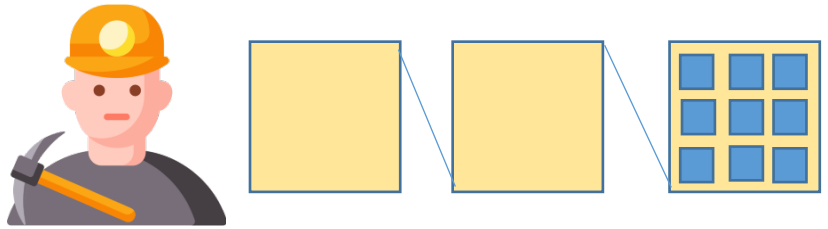
Good!

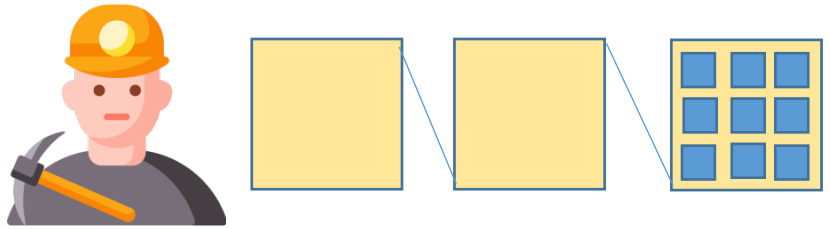


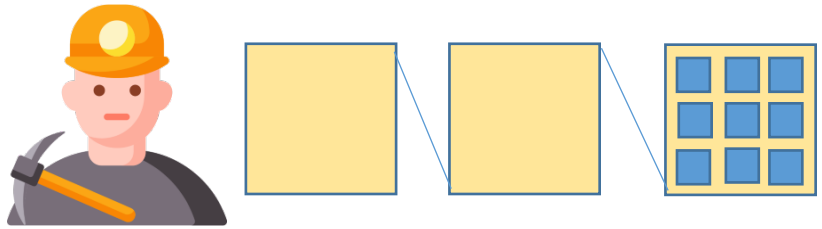
Good!

작업증명

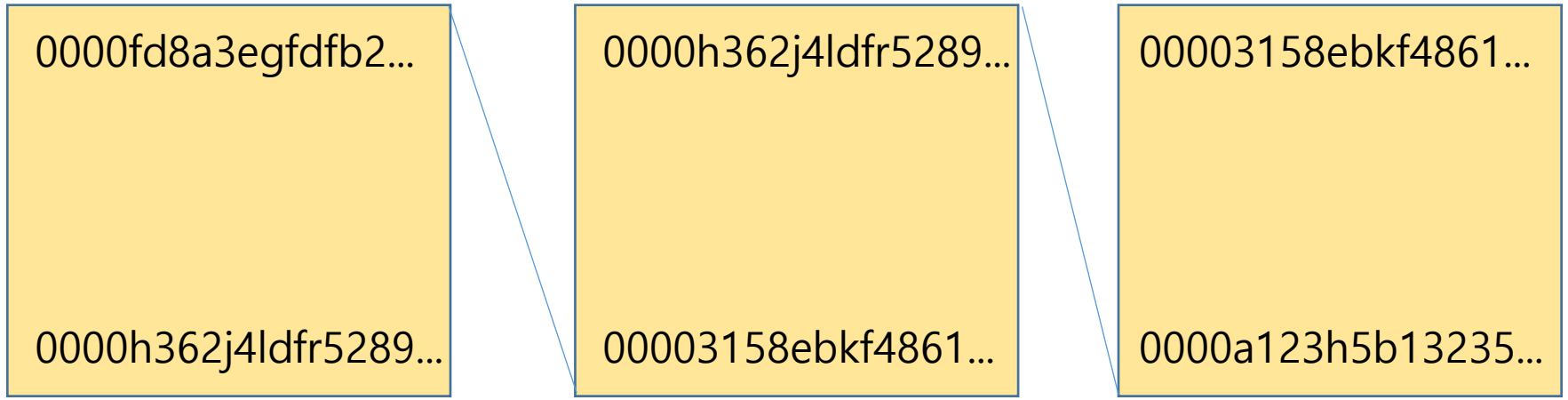




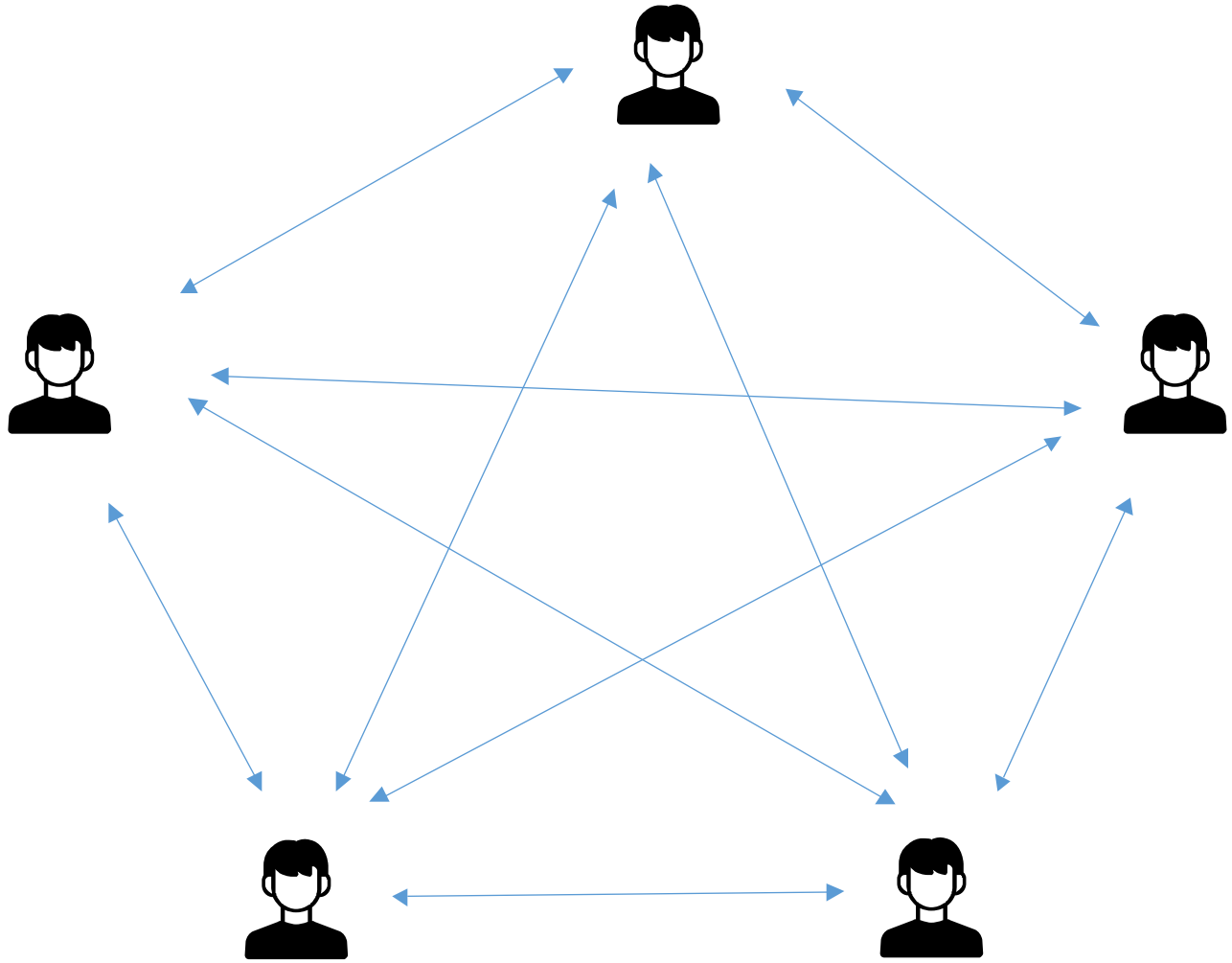




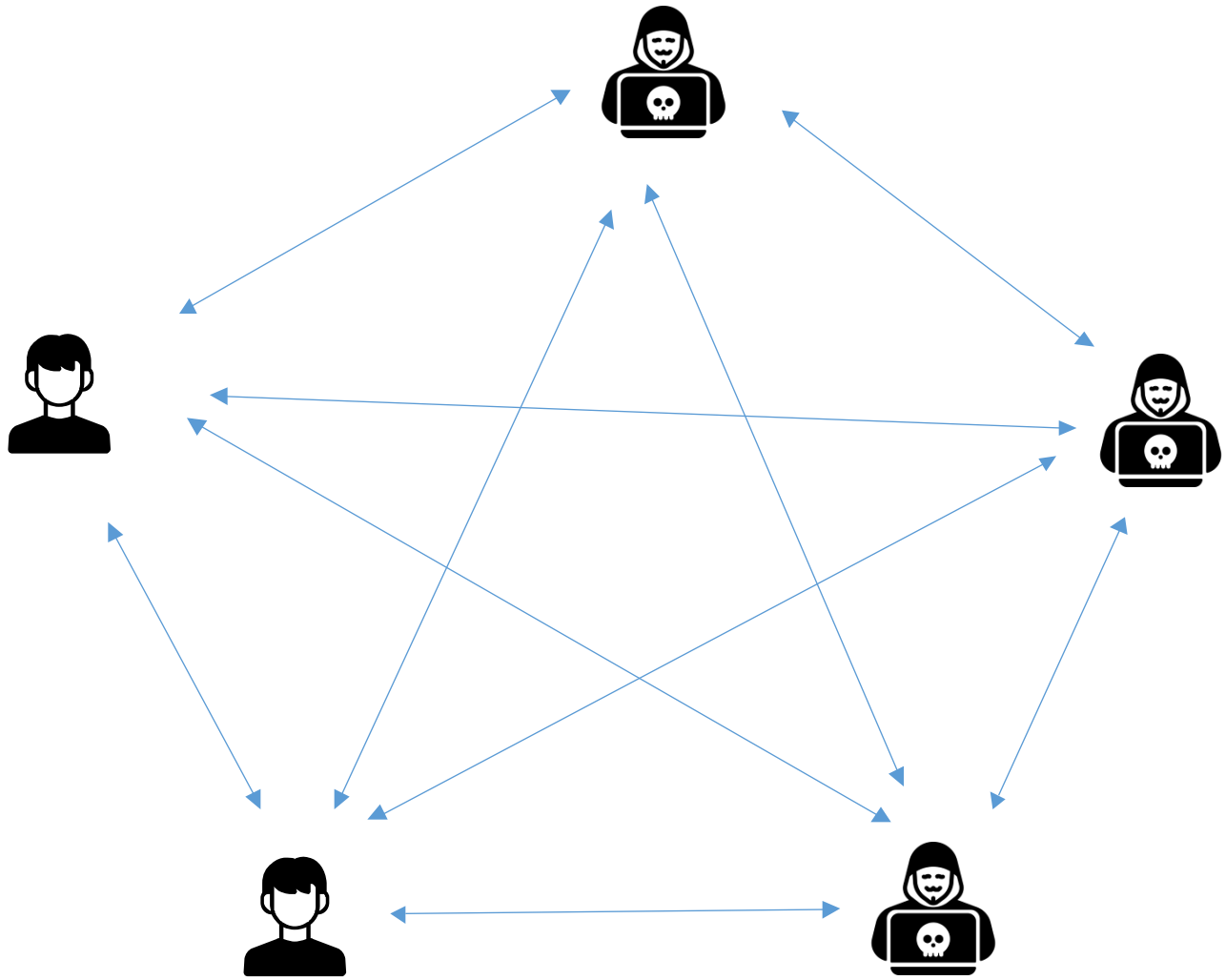
작업증명


0000fd8a3egfdfb2...
0000h362j4ldfr5289...
0000h362j4ldfr5289...
00003158ebkf4861...
00003158ebkf4861...
0000a123h5b13235...

51% 공격



51% 공격



51% 공격

- 다른 이들의 트랜잭션을 되돌릴 수 없음
- 생성되고 있거나 전송중인 트랜잭션을 차단할 수 없음
- 블록 보상 변경, 코인 생성, 코인 훔치기 등이 불가능

- 위변조된 신규 블록 생성
- 자신의 트랜잭션을 되돌림 -> **이중 지출 문제**
- 트랜잭션의 일부 또는 전체를 승인 거부할 수 있음 -> **마이닝 독점**

51% 공격

- 51% 공격 발생 가능성
  - 블록체인은 분산화 된 노드 네트워크에 의해서 관리됨
  - 즉, 네트워크가 클수록 공격 가능성 ↓
  - Ex) 비트코인
    - 보안을 위한 1차 마이너 투입
    - 채굴을 위한 2차 마이너 투입
    - 정직한 행동 정직한 보상 -> 자정작용
    - 51%의 해싱 파워를 보유하기 어려움
    - 보유하더라도 블록의 변경이 어려움

이더리움

- 2013년 Vitalik Buterin에 의해서 개발
- 비트코인의 분산 어플리케이션 구축을 위한
- 스크립팅 언어의 필요성 제기
- 오픈 소스, public, 블록체인 기반 분산 컴퓨팅 플랫폼
- 스마트 컨트랙트 기능 사용

Vitalik Buterin
(비트코인 매거진
공동 창업자)

이더리움

- 스마트 컨트랙트
  - 이더리움 내에서 실행되는 스크립트
  - 특정 조건이 성립될 경우 거래 성립
    - ex) 자판기
  - 이더리움 전용 언어, Solidity로 작성
  - EVM(Ethereum Virtual Machine)이라는 가상 머신 위에서 실행
    - 퍼블릭 노드 네트워크를 사용하여 검열 저항성 보장

- DApp(분산형 애플리케이션)
  - 이더리움 블록체인 내에서 실행되는 애플리케이션
  - 소셜 미디어 플랫폼, 도박 애플리케이션, 금융 거래 등

이더리움

- 자체 암호화폐 이더(ETH) 사용
- 이더리움 내에서 작업을 수행할 때 실행 수수료인 gas fee 발생
- 연산 ↑ => gas fee ↑
- 가스 당 지불하는 ETH의 양을 정할 수 있지만,
  지불한 금액에 따라 우선 순위가 결정됨
- Reliable Uptime 제공

이더리움

전용 프로그래밍 언어가 내장된 블록체인
합의된 내용 안에서 어플리케이션이 가동되는 세계의 컴퓨터

Q & A