1차 프로포절

Advanced Software Engineering

2017.05.16

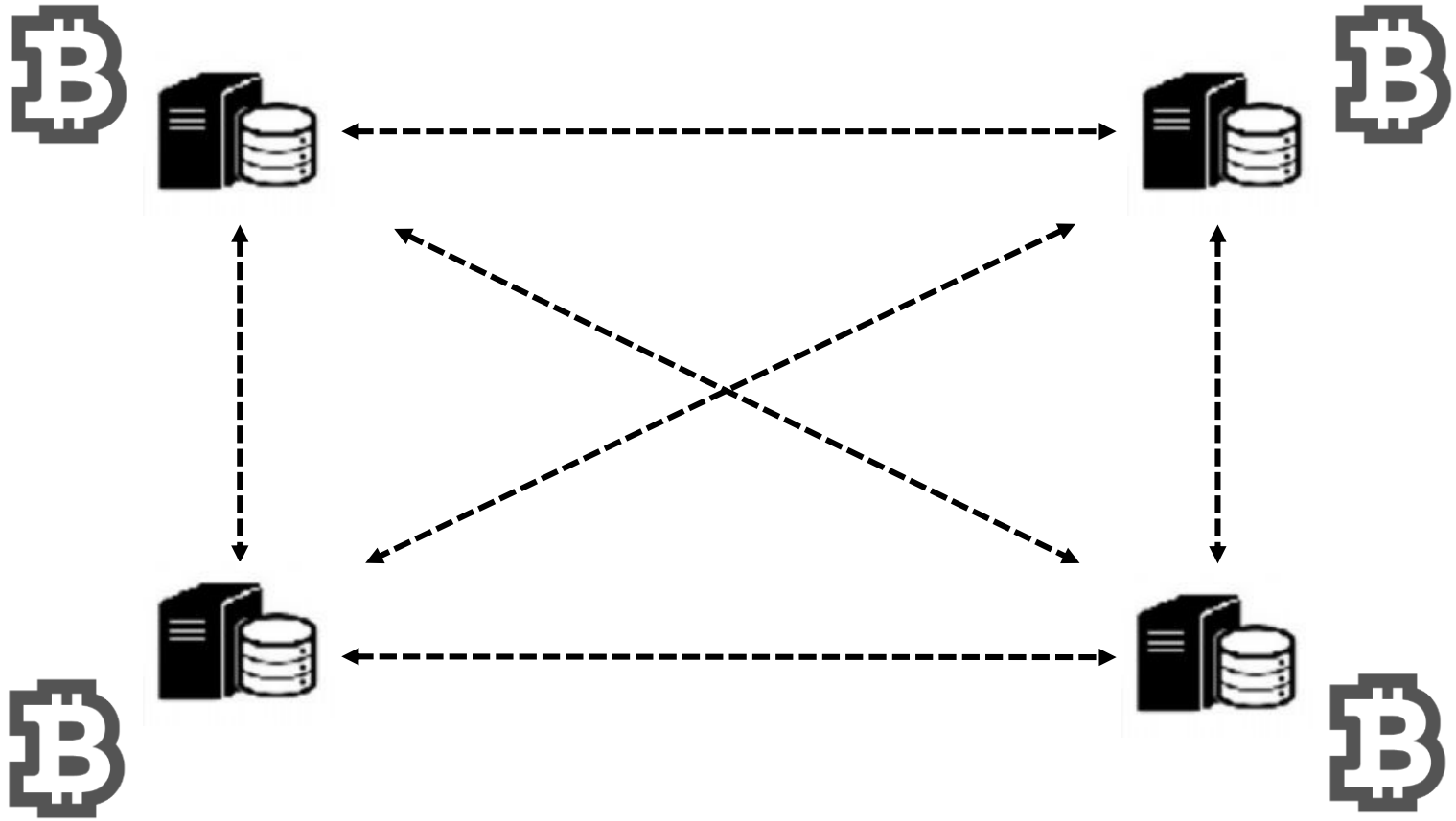
KONKUK UNIVERSITY ITCS

노은방, 심우진

CONTENTS

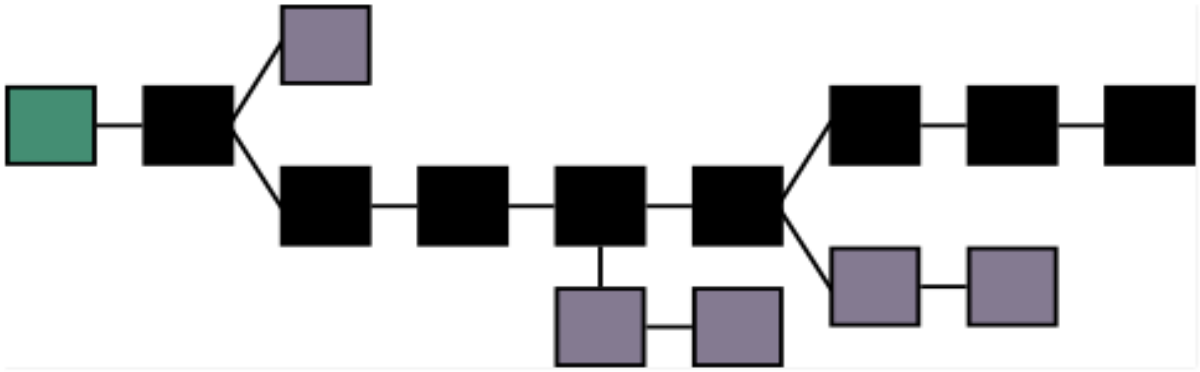
Blockchain & Bitcoin

- Blockchain이란?

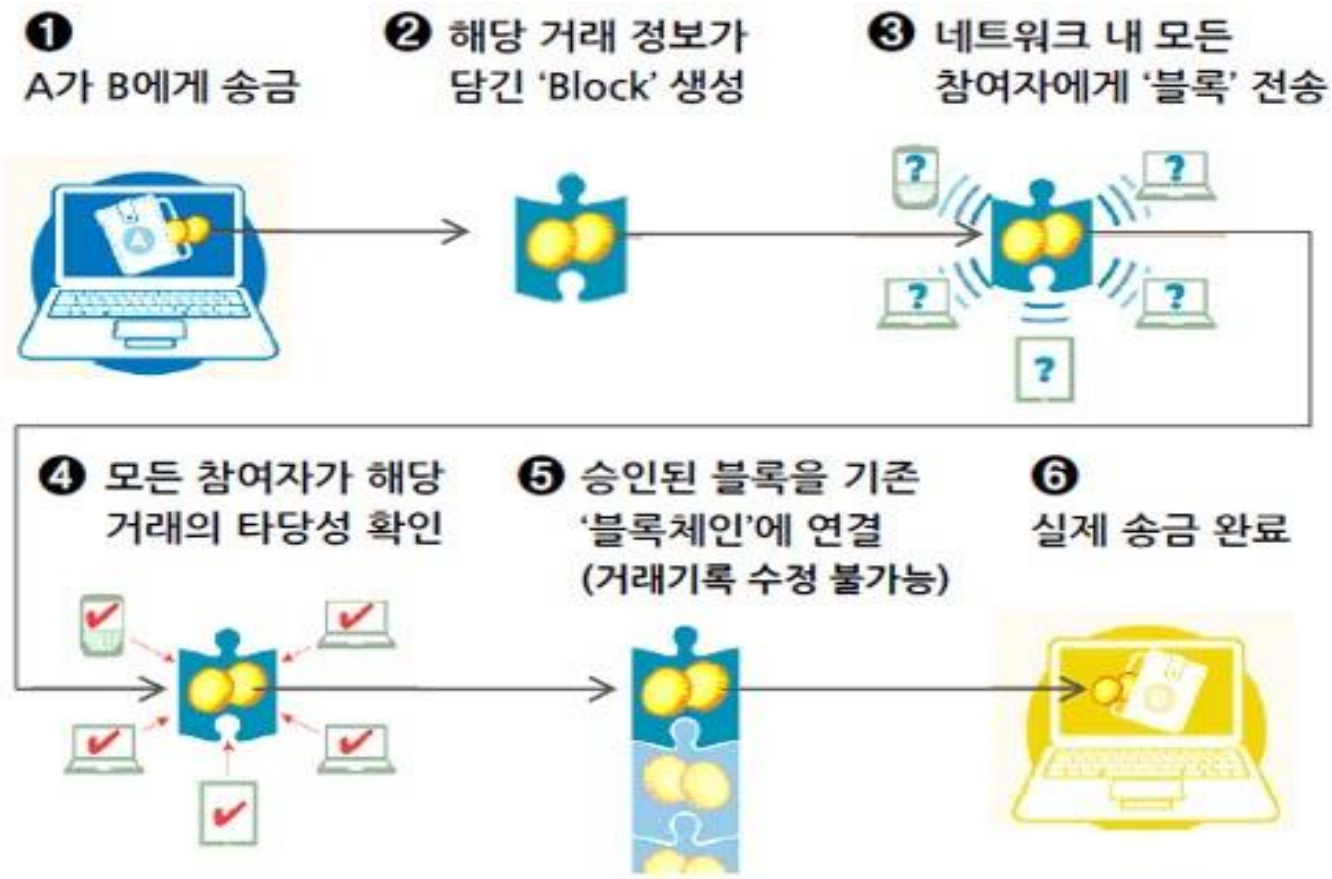


Blockchain & Bitcoin

- Blockchain이란?
  - 가상 화폐 거래 시 발생할 수 있는 해킹을 막는 기술로 공공 거래 장부라 지칭.
  - 분산 데이터베이스의 형태로, 분산 노드의 운영자에 의한 임의 조작이 불가능.
  - 데이터를 일정 시간 단위로 서로 비교하며 데이터 훼손, 변조, 변질 등을 검증.
  - 블록은 이전 블록에 대한 연결고리를 가지고 있으며 해당 블록들의 집합을 지칭.

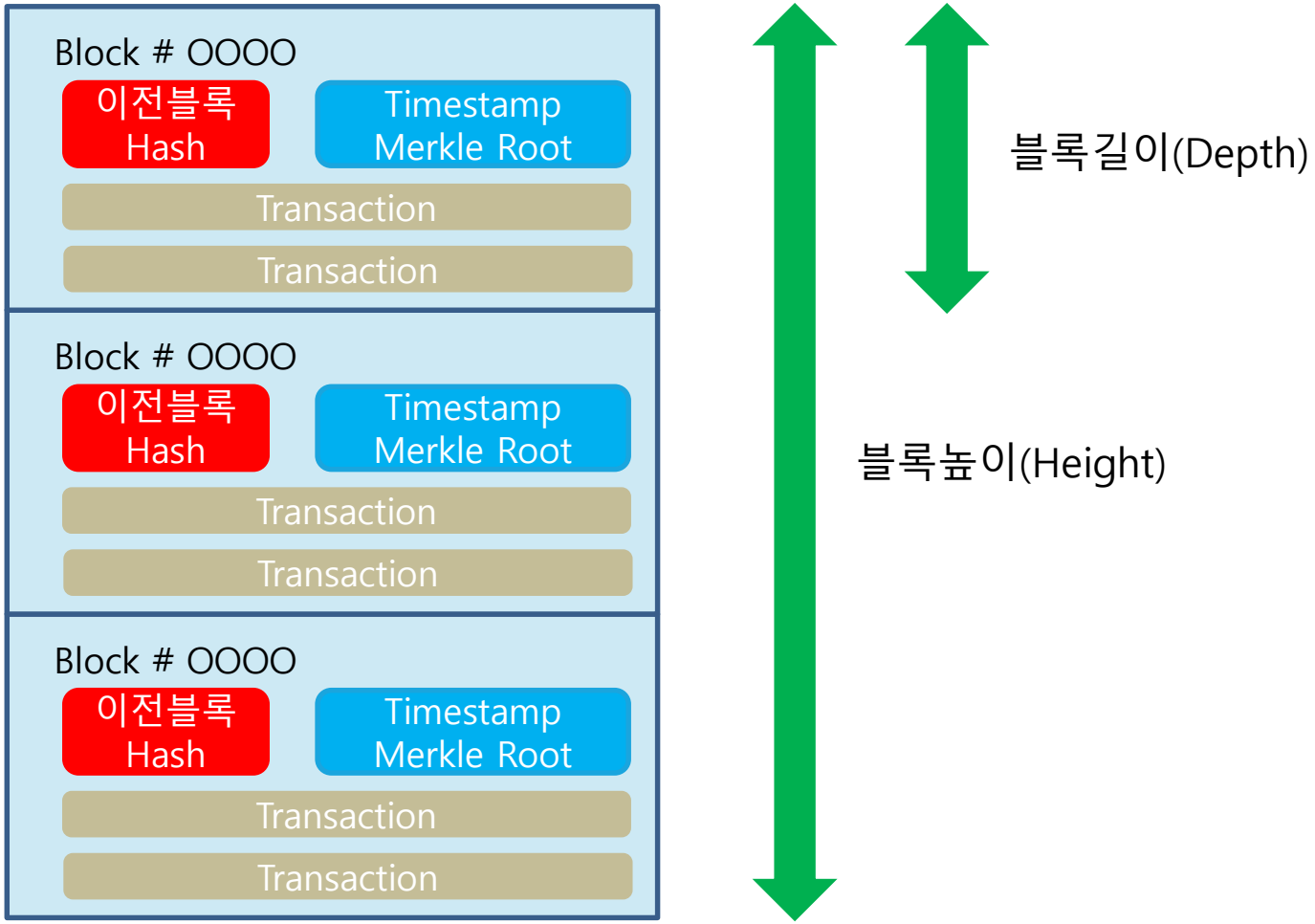


Blockchain Process

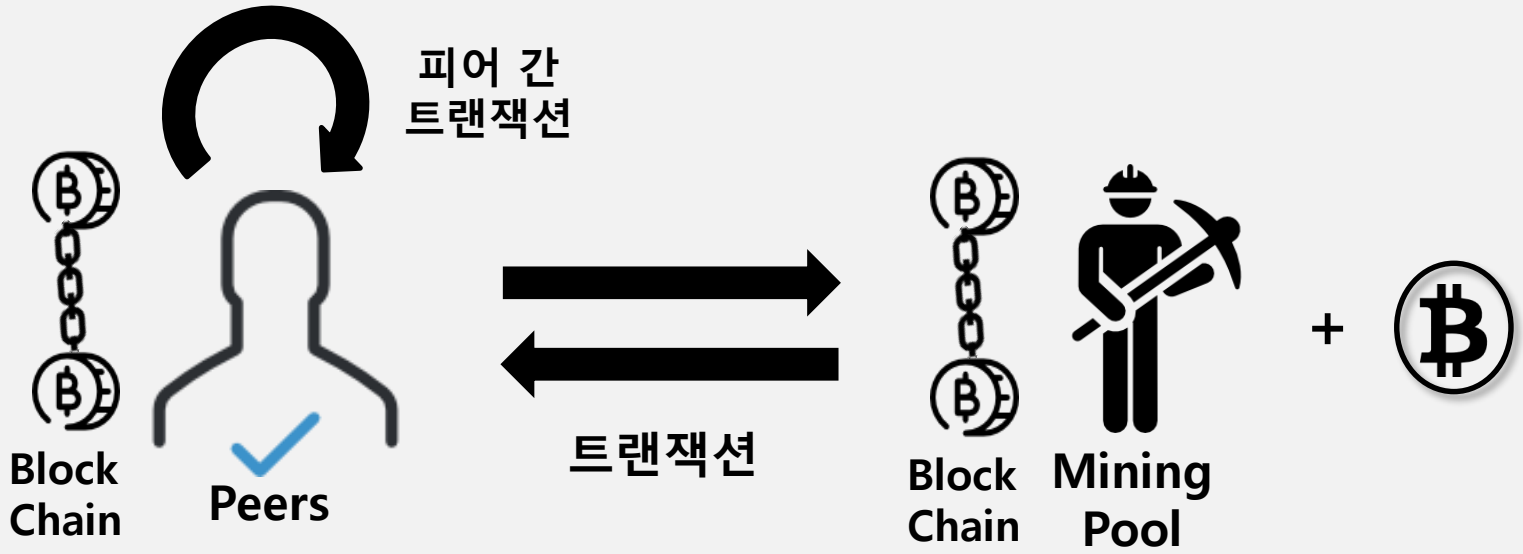


Specification

Block Structure

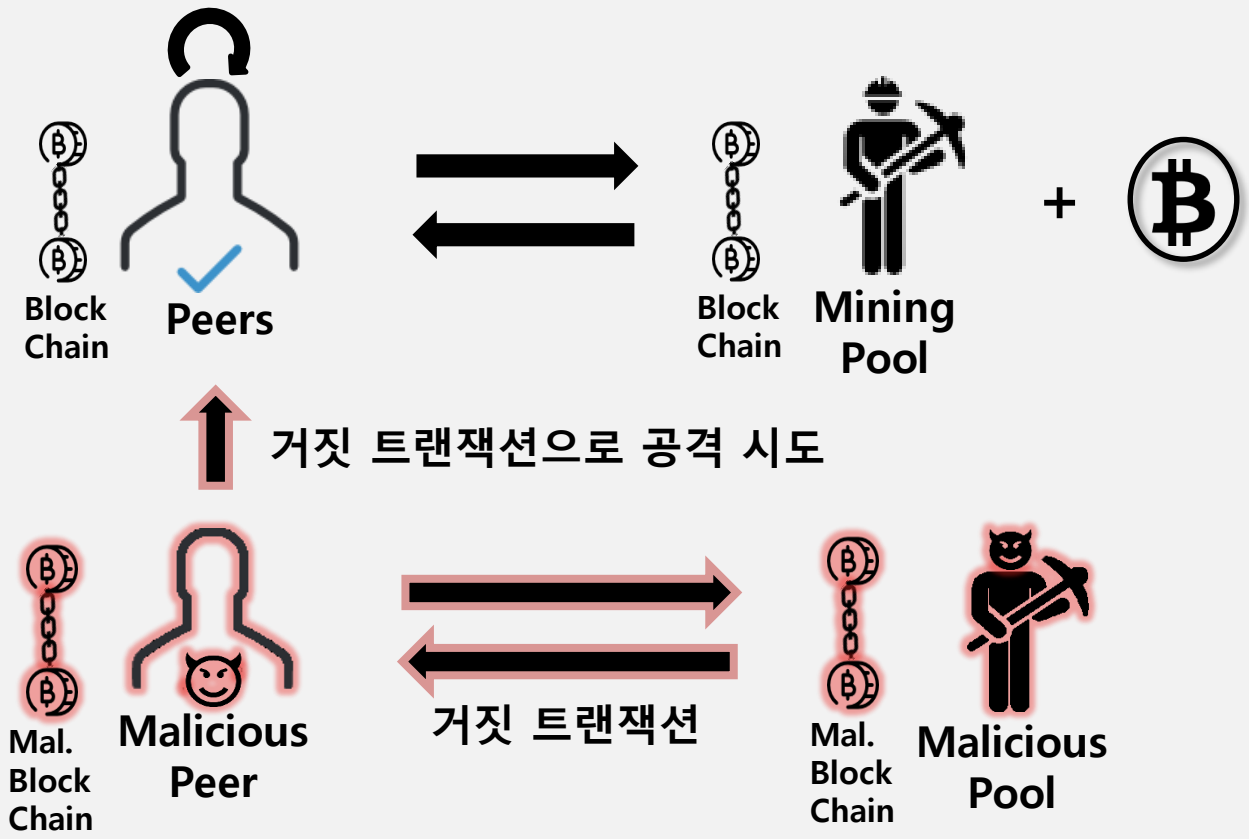


Specification

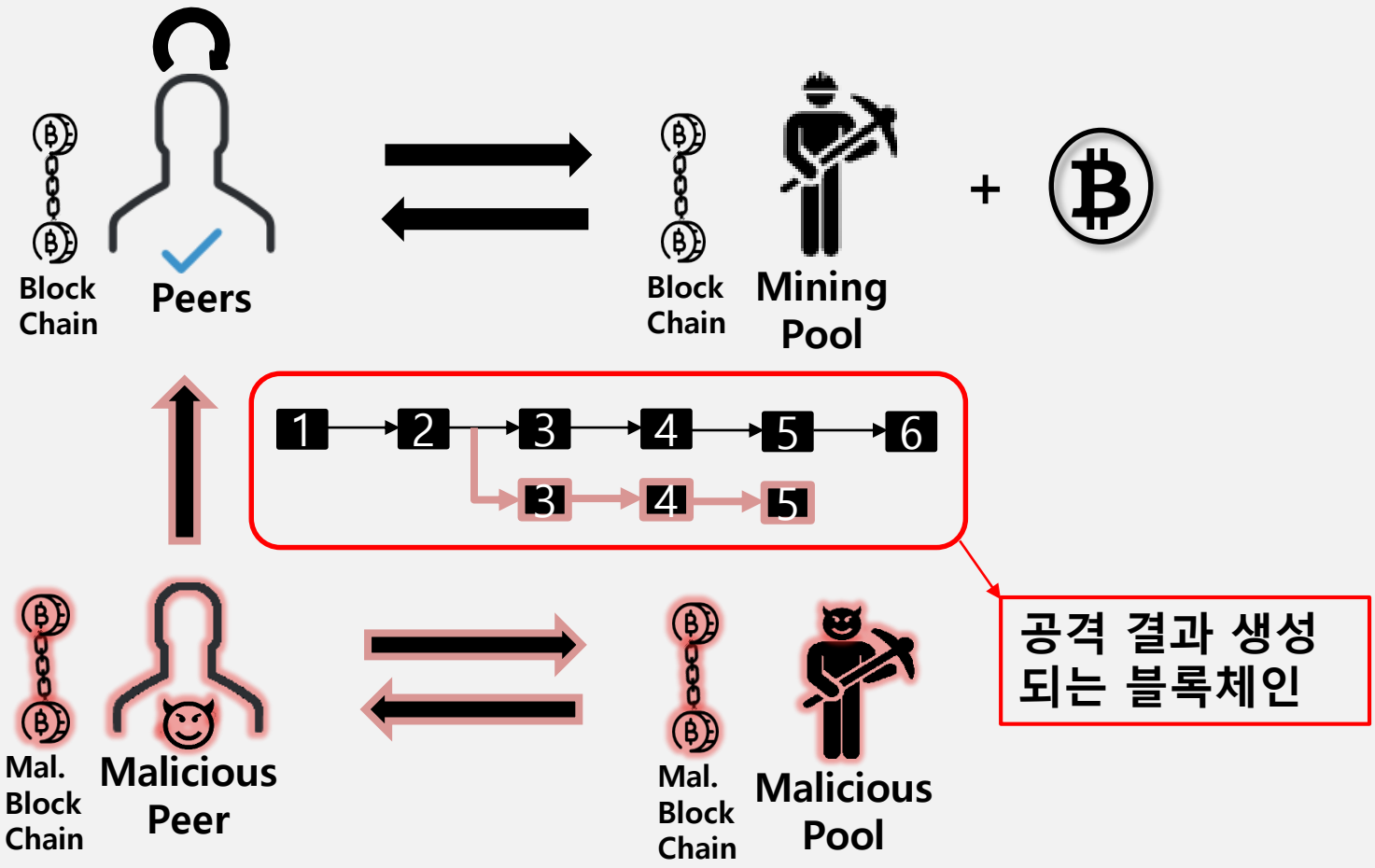


- ❖ Peer: 각 피어 간 거래(트랜잭션)을 수행하고, 블록체인 네트워크에 전파한다.
- ❖ Mining Pool : POW기반으로 약 10분마다 채굴을 수행하며 블록을 생성하고, 비트코인을 발행한다.

Specification



Specification



Expected Properties

Candidate Properties

- 모든 블록마다 유일한 해시 값을 지녀야한다.
- 모든 Peer가 가지는 지갑(Wallet)은 유일하게 구분되어야 한다.
- 피어 간 일어나는 모든 거래(Transaction)은 유일하게 구분되어야 한다.
- 모든 거래는 그 내역이 블록안에 포함되기 전, 검증 받아야 한다.
- 모든 거래는 언젠가 검증되거나, 부적합 판정을 받아야 한다.

Expected Properties

Candidate Properties

- ❖ 생성되는 BTC(비트코인 단위)와 피어들 사이에서 거래되는 총량은 동일해야 한다.
- ❖ 악의적인 공격자에 의한 변조된 블록체인의 길이는 올바른 블록체인의 길이보다 작아야 한다.

THANK YOU