



# 작업 증명(PoW)의 메커니즘 (비유적으로)

- 사람들의 송금 신청서를 수집한다.
- 택배 박스에 송금 신청서들을 집어 넣는다.
  - 박스 크기는 제한적
  - 내 계좌로 돈을 입금하라는 신청서와 여러 정보를 같이 집어 넣는다.
- 박스를 잠궈서 보내야 하는데, 박스를 통째로 검사 기계에 넣으면 숫자 자물쇠를 준다.
- 자물쇠가 열리는 숫자를 찾으면 해당 숫자를 박스에 적는다.
- 박스를 보내고 주변 사람들에게 소문낸다.

# 트랜잭션

# 트랜잭션

學

堂

豊平

平 子

平 子



貴子

보상

**블록헤더**

해시함수

그리 바와한다.

블록 해시값

平 平

해시값



실제 용어로

三 五 卅

전파한다.

서로부러

**체인은 어디있지?**

# 작업 증명(PoW)의 메커니즘 (실제 용어로)

풀노드로부터 트랜잭션 을 수집한다.

- 블록 에 트랜잭션 들을 집어 넣는다.

체인은 어디있지?

- 블록 크기는 제한적


- 내 계좌로 보상 와 블록헤더 를 같이 집어 넣는다.


- 블록 을 잠궜서 보내야 하는데, 블록 을 통째로 해시함수 에 넣으 해시값 를 반환한다.

- 자물쇠가 열리는 숫자를 찾으 블록 해시값 를 블록 에 적는다.

- 블록 을 보내고 풀노드 한테 전파한다.

# 전자 화폐로서 동작하기 위해 필요한 요소

- 소유 할 수 있어야 한다.
  - 안전하게 거래 할 수 있어야 한다.
- 
- 원장(Ledger), 디지털 서명

- 마이너스 잔액이 불가해야 한다. (초과 지출 문제)
  - 거래 내역 복사가 불가해야 한다. (이중 지불 문제)
- 
- 작업 증명(PoW)

How?

비트코인이 블록체인을 통해 해결한 문제

디지털 서명

작업 증명

해시 함수