

그래서, 어떻게 확신 할 수 있는데? → 합의를 해서 모든 사람이 동일한 거래 내역을 동일한 순서로 기록한 장부를 가지고 있다는 것을 확신 • 어떻게 확신 할 수 있나?







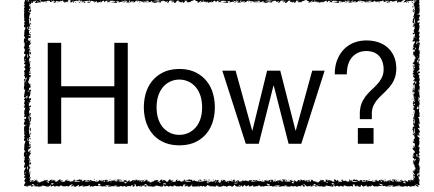
**→ 어떤 규칙**을 통해 어떤 순서로 내역을 결정할 지 **합의**를 하면 된다

→ 그러한 규칙을 **합의 프로토콜, 합의 알고리즘**이라 부르며 비트코인에서 사용한 합의 프로토콜은 작업 증명 (Proof of Work) 이다.

## 그래서, 어떻게 확신 할 수 있는데? → 합의를 해서

- 모든 사람이 동일한 거래 내역을 동일한 순서로 기록한 장부를 가지고 있다는 것을 확신
- 어떻게 확신 할 수 있나?
  - → **어떤 규칙**을 통해 어떤 순서로 내역을 결정할 지 **합의**를 하면 된다
  - → 그러한 규칙을 **합의 프로토콜, 합의 알고리즘**이라 부르며

비트코인에서 사용한 합의 프로토콜은 작업 증명 (Proof of Work) 이다.



## 작업 증명(PoW)의 메커니즘 (비유적으로)

- 사람들의 **송금 신청서**를 수집한다.
- 택배 박스에 송금 신청서들을 집어 넣는다.
  - 박스 크기는 제한적
  - 내 계좌로 **돈을 입금하라는 신청서**와 여러 정보를 같이 집어 넣는다.
- **박스**를 잠궈서 보내야 하는데, **박스**를 통째로 **검사 기계**에 넣으면 **숫자 자물쇠**를 준다.
- 자물쇠가 열리는 숫자를 찾으면 해당 숫자를 박스에 적는다.
- 박스를 보내고 주변 사람들한테 소문낸다.