

돈 복사를 못 하게 해야한다. - Double-spending 문제 해결

- 모든 사람이 동일한 거래 내역을 동일한 순서로 기록한 장부를 가지고 있다는 것을 확신
 - 하나의 거래 장부만 승인 → 중복 거래 방지 → double-spending 방지







철수

영희

짱구

맹구

분산 원장

분산 원장

분산 원장

분산 원장

동일한 거래 내역을 가진 분산 원장

철수 → 짱구 1BTC

영희 → 짱구 1BTC

맹구 → 짱구 1BTC

철수

영희

철수 → 짱구 1BTC

영희 → 짱구 1BTC

맹구 → 짱구 1BTC

철수 → 짱구 1BTC

영희 → 짱구 1BTC

맹구 → 짱구 1BTC

짱구

맹구

철수 → 짱구 1BTC

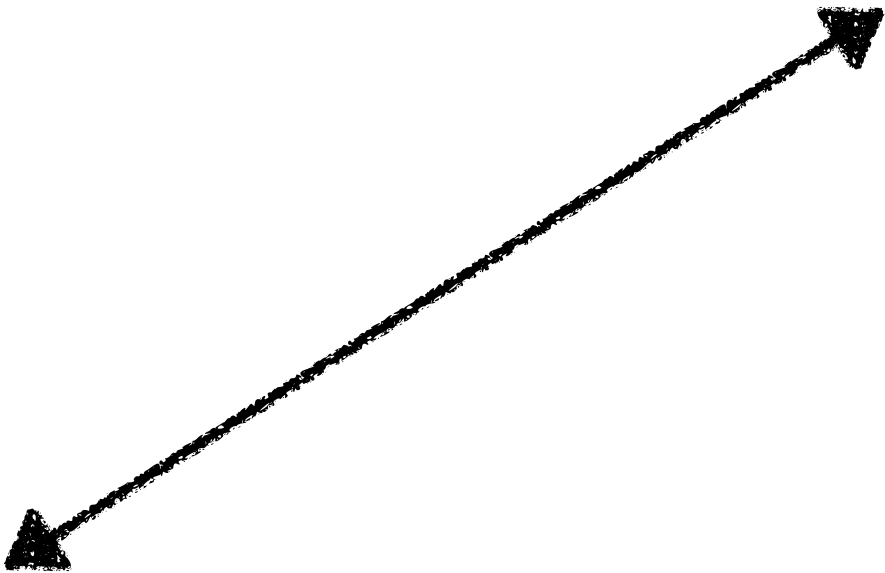
영희 → 짱구 1BTC

맹구 → 짱구 1BTC

장귀 → 천수 1BTC

장구 → 영화 1BTC

장꾸교 → 망꾸교 1BTC







중복 거래 방지



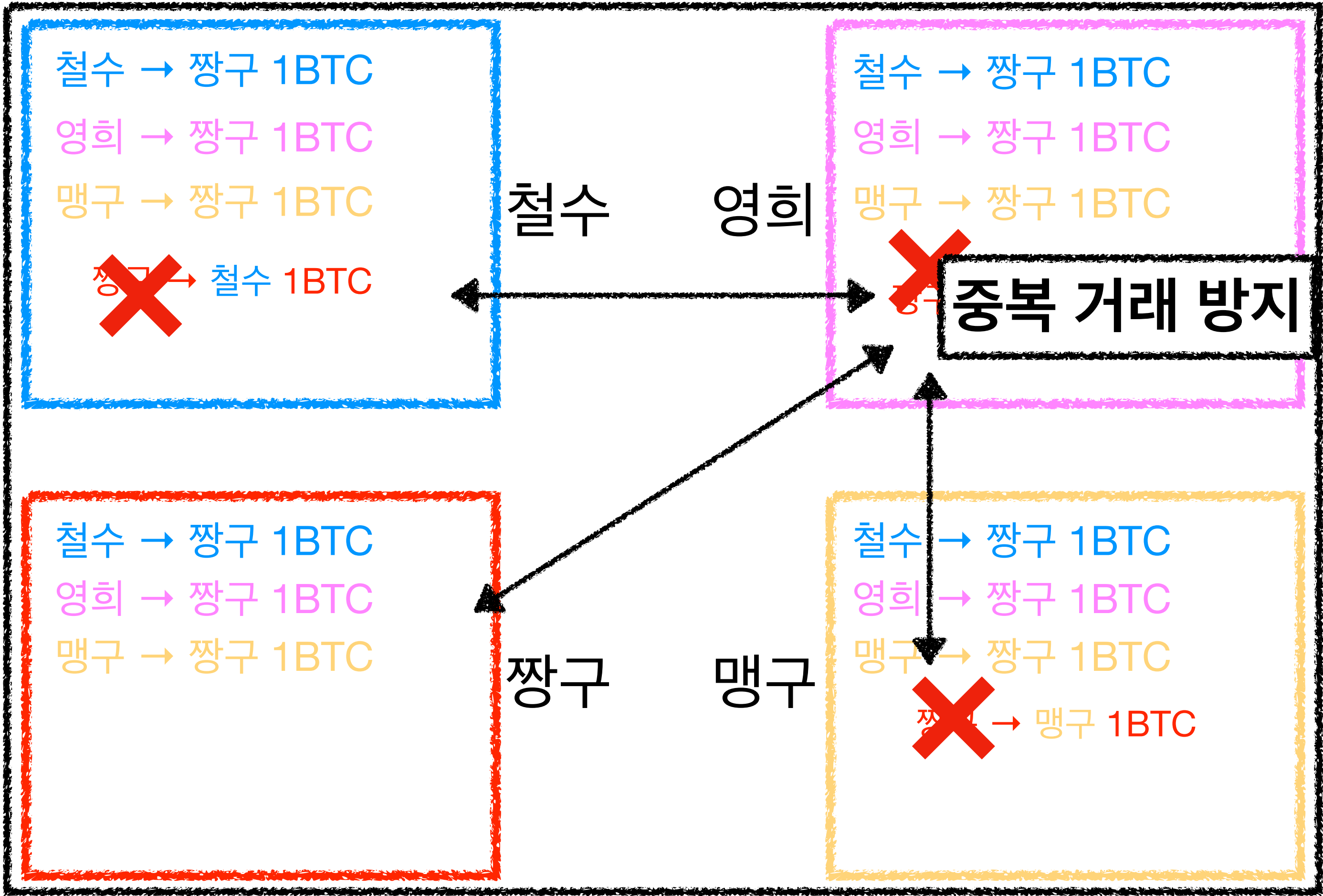
世臣





돈 복사를 못 하게 해야한다. - Double-spending 문제 해결

- 모든 사람이 동일한 거래 내역을 동일한 순서로 기록한 장부를 가지고 있다는 것을 확신



Double-spending 방지



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?