디지털 서명, 나의 돈을 **남이 함부로 다루지 못하게** 한다.

- **누구나** 장부에 거래 내역을 **기록할 수 있다.**

복사 철수 → 짱구 1BTC 전송 **[철수 사인(0xabc123)]**

철수 → 짱구 1BTC 전송 **[철수 사인(0xabc123)]**

짱구가 철수 **거래 내역을 복사** 할 경우

2. 철수 → 짱구 1BTC 전송 **[철수 사인(0x87c8a1)]**

1. 철수 → 짱구 1BTC 전송 **[철수 사인(0xabc123)]**

3. 철수 → 짱구 1BTC 전송 **[철수 사인(0x913bf5)]**

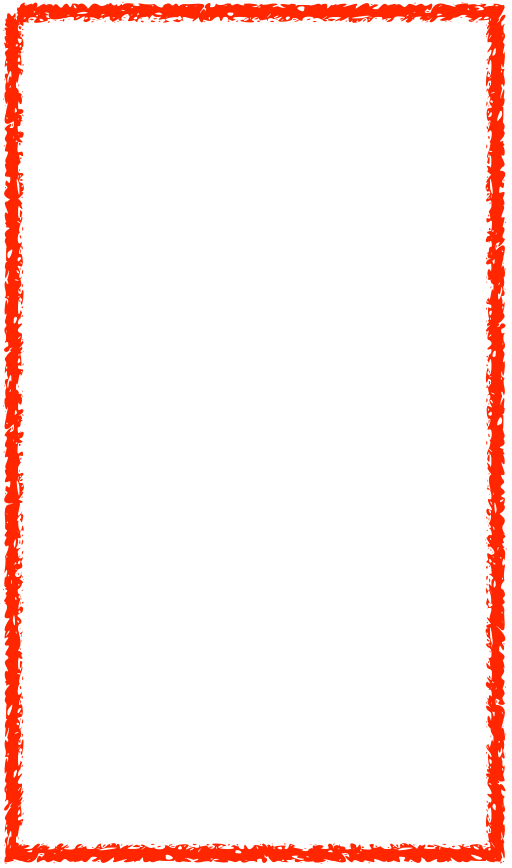
4. 철수 → 짱구 1BTC 전송 **[철수 사인(0xfac6cd)]**

5. 철수 → 짱구 1BTC 전송 **[철수 사인(0x010b95)]**

6. 철수 → 짱구 1BTC 전송 **[철수 사인(0xaa92bf)]**

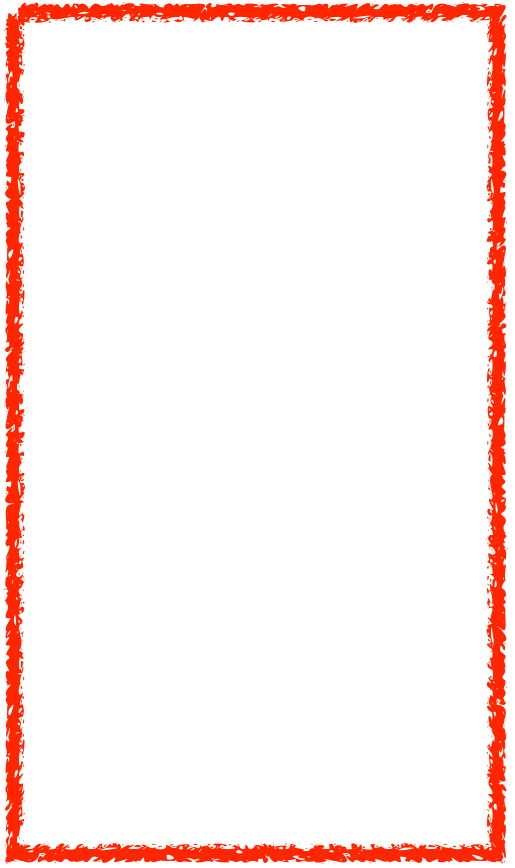
7. 철수 → 짱구 1BTC 전송 **[철수 사인(0x10394d)]**

철수가 실제로 **같은 내용을 여러 번 실행**한 경우



디지털 서명이 동일하다 → 잘못된 서명

이유는 해시 함수 때문 → 뒤에서 자세히



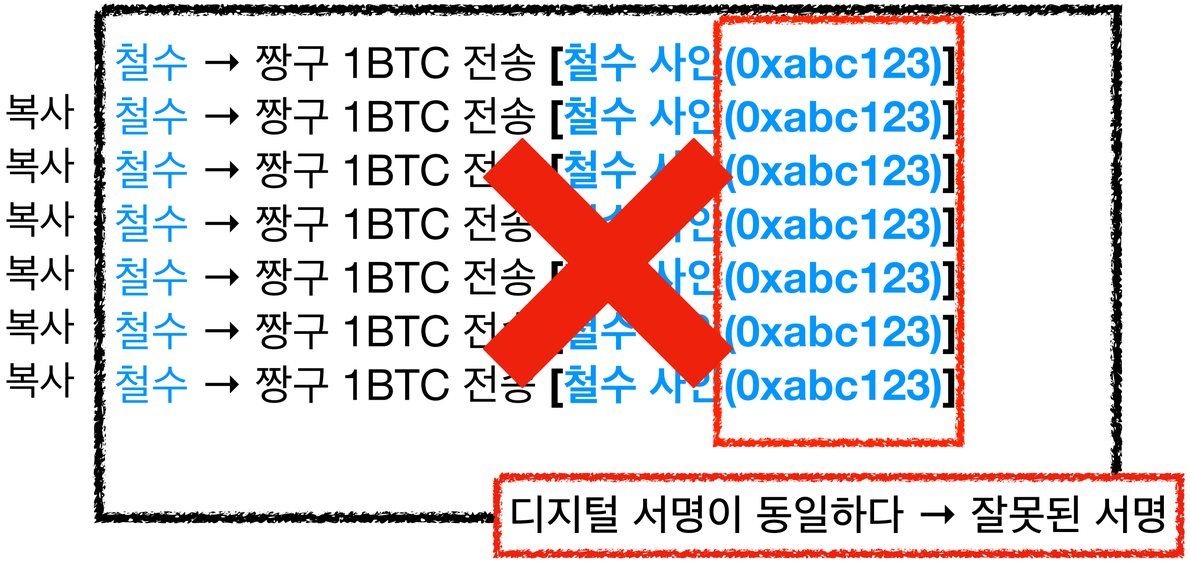
번호(타임스탬프)로 해결 가능

정상 서명 → 서명이 모두 다르다

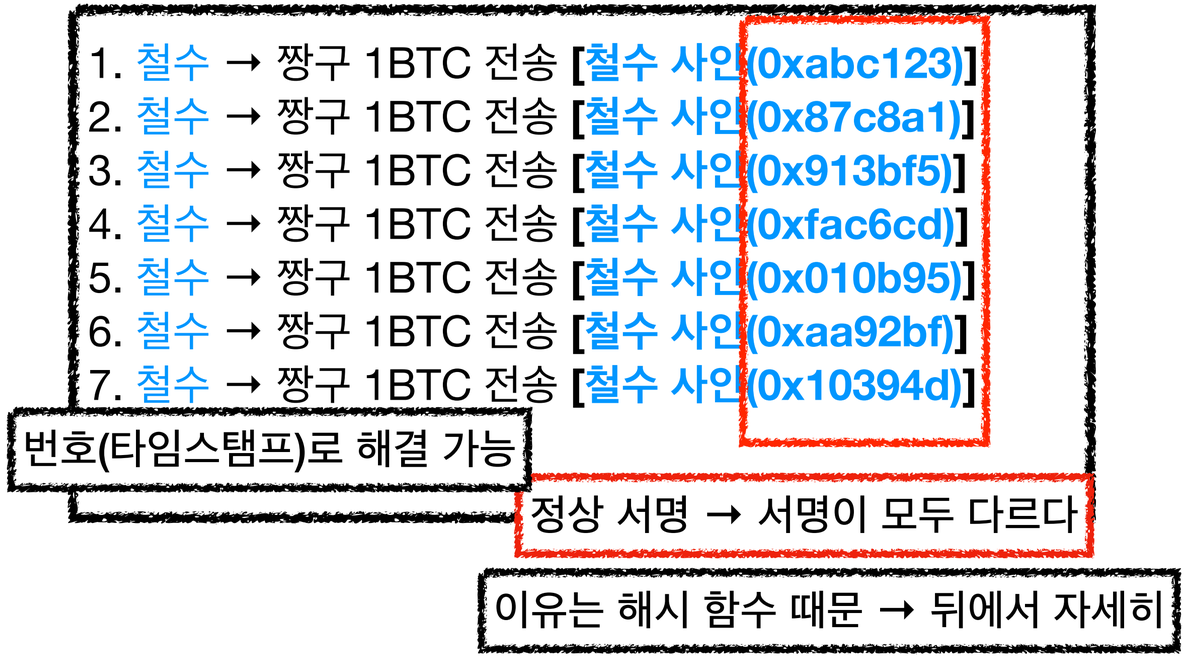
디지털 서명, 나의 돈을 **남이 함부로 다루지 못하게** 한다.

- **누구나** 장부에 거래 내역을 **기록할 수 있다.**

짱구가 철수 **거래 내역을 복사** 할 경우



철수가 실제로 **같은 내용을 여러 번 실행**한 경우



이유는 해시 함수 때문 → 뒤에서 자세히

돈 복사를 못 하게 해야한다.

- **초과 지출**(overspending), **이중 지불**(double spending) 문제

  → **돈 복사**가 가능한 문제