

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 → 장꾸1BTC 전송 [철수사인(0xabc123)]1

장구가라춤새악을보사함경우



철수 → 장꾸1BTC전송 [철수사인(0x87c8a1)]

철수 → 장꾸1BTC전송 [철수사인(0xabc123)]1

철수 → 장꾸1BTC전송 [철수사인(0x913b15)]

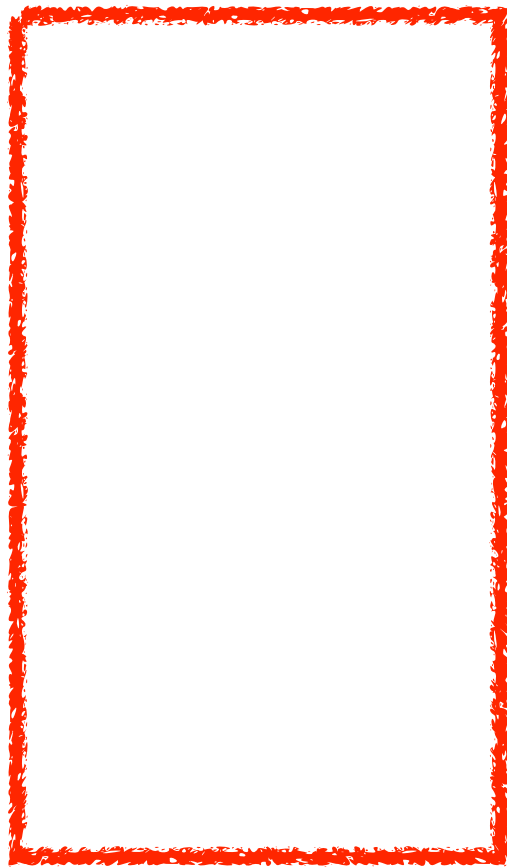
철수 → 장꾸1BTC전송 [철수사인(0xac6cd)]

철수 → 장꾸1BTC전송 [철수사원(0x010b95)1

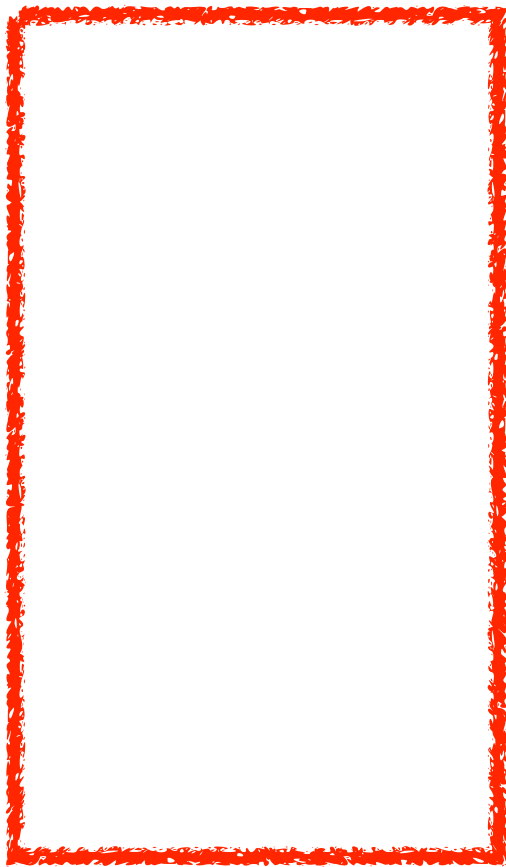
철수 → 장쿠1BTC전송 [철수사인(0xa92bf)]

철수 → 장꾸1BTC전송 [철수사인(0x10394d)]1

천수강을내려와서행하거요



디지털 서명이 동일하다 → 잘못된 서명



정상 서명 → 서명이 모두 다르다

이유는 기술적인 내용이 들어가는 스캔



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 실행한 경우

복사
복사
복사
복사
복사
복사
복사

철수 → 짱구 1BTC 전송 [철수 사인(0xabc123)]

철수 → 짱구 1BTC 전송 [철수 사인(0xabc123)]

철수 → 짱구 1BTC 전송 [철수 사인(0xabc123)]

철수 → 짱구 1BTC 전송 [철수 사인(0xabc123)]

철수 → 짱구 1BTC 전송 [철수 사인(0xabc123)]

철수 → 짱구 1BTC 전송 [철수 사인(0xabc123)]

철수 → 짱구 1BTC 전송 [철수 사인(0xabc123)]

디지털 서명이 동일하다 → 잘못된 서명

철수 → 짱구 1BTC 전송 [철수 사인(0xabc123)]

철수 → 짱구 1BTC 전송 [철수 사인(0x87c8a1)]

철수 → 짱구 1BTC 전송 [철수 사인(0x913bf5)]

철수 → 짱구 1BTC 전송 [철수 사인(0xfac6cd)]

철수 → 짱구 1BTC 전송 [철수 사인(0x010b95)]

철수 → 짱구 1BTC 전송 [철수 사인(0xaa92bf)]

철수 → 짱구 1BTC 전송 [철수 사인(0x10394d)]

정상 서명 → 서명이 모두 다르다

이유는 기술적인 내용이 들어가 스킵

돈 복사를 못 하게 해야한다.

- 초과 지출(overspending), 이중 지불(double spending) 문제
→ 돈 복사가 가능한 문제