디지털 서명, 나의 돈을 **남이 함부로 다루지 못하게** 한다.

- **누구나** 장부에 거래 내역을 **기록할 수 있다.** → 문제가 발생할 수 있다.
  - 이번엔 짱구가 다음과 같이 기록한다면?

철수 돈을 짱구가 맘대로 빼가서

철수는 화난다 

철수야 1BTC 주면 내가 2BTC 줄게

복사 철수 → 짱구 1BTC 전송 **[철수 사인]**

철수 → 짱구 1BTC 전송 [철수 사인]

갚아라

Digital Signature

디지털 서명을 이용해 방지

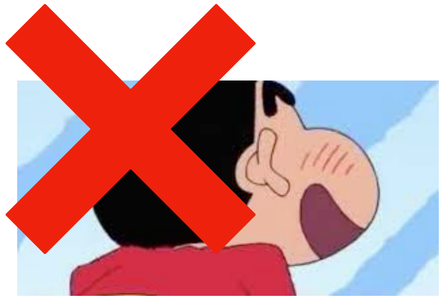
디지털 서명, 나의 돈을 **남이 함부로 다루지 못하게** 한다.

- **누구나** 장부에 거래 내역을 **기록할 수 있다.** → 문제가 발생할 수 있다.
  - 이번엔 짱구가 다음과 같이 기록한다면?

Digital Signature

디지털 서명을 이용해 방지

철수 → 짱구 1BTC 전송 [**철수 사인**]
복사 철수 → 짱구 1BTC 전송 [**철수 사인**]
복사 철수 → 짱구 1BTC 전송 [**철수 사인**]
복사 철수 → 짱구 1BTC 전송 [**철수 사인**]
복사 철수 → 짱구 1BTC 전송 [**철수 사인**]
복사 철수 → 짱구 1BTC 전송 [**철수 사인**]
복사 철수 → 짱구 1BTC 전송 [**철수 사인**]



철수 돈을 짱구가 맘대로 빼가서

철수는 화난다 🤬

디지털 서명, 나의 돈을 **남이 함부로 다루지 못하게** 한다.

- **누구나** 장부에 거래 내역을 **기록할 수 있다.**

짱구가 철수 **거래 내역을 복사** 할 경우

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

철수가 실제로 **같은 내용을 여러 번 실행**한 경우

1. 철수 → 짱구 1BTC 전송 **[철수 사인(0xabc123)]**
2. 철수 → 짱구 1BTC 전송 **[철수 사인(0x87c8a1)]**
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)]**