# 한 번에 끝내는
# 블록체인 개발 A to Z

---

Chapter 1

## Blockchain 1.0 - Bitcoin

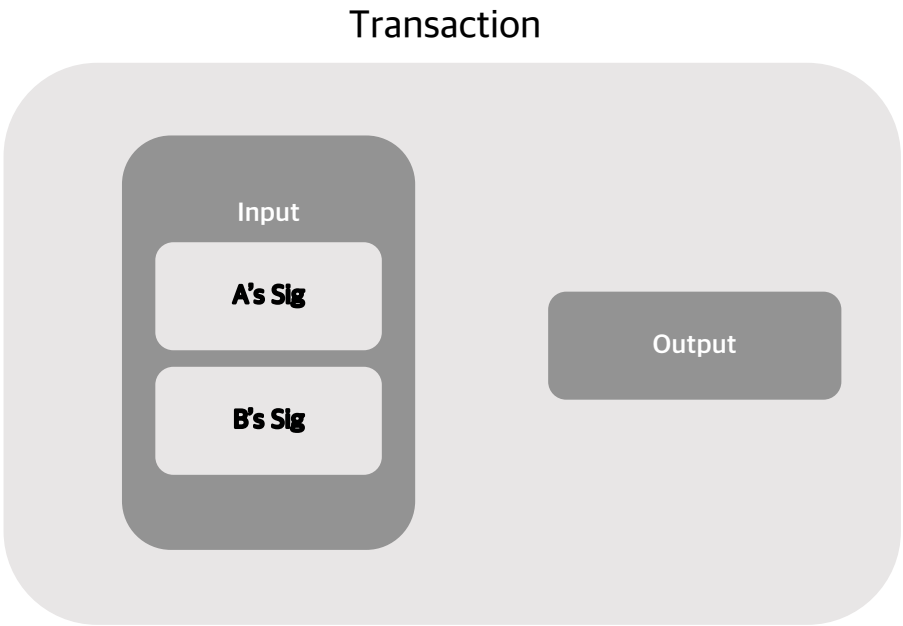
Chapter 1

Blockchain 1.0 - Bitcoin

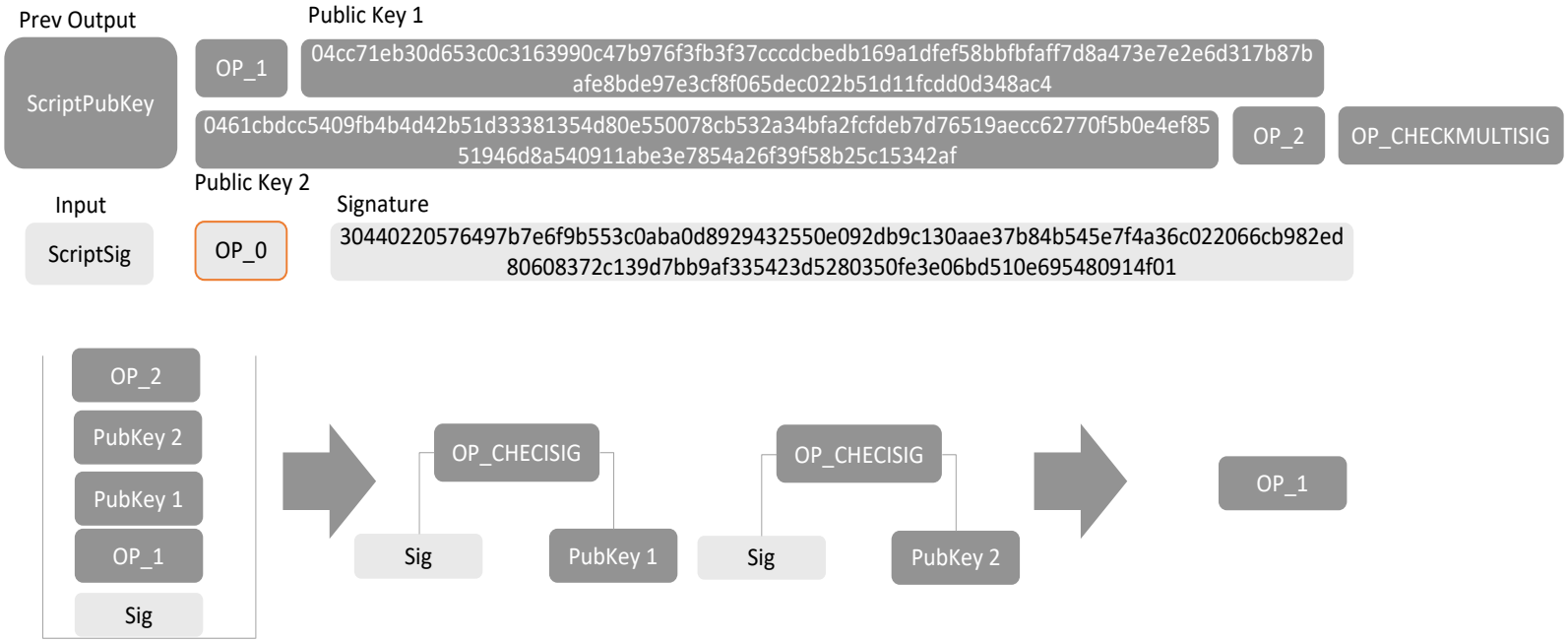
# Multisig와 Custody

# Multi-Signature란?

- Multi-Signature란 하나의 거래에 여러 명이 서명을 해야 승인 될 수 있는 거래를 의미합니다.
- 큰 금액을 보관하는 경우 사용자의 키 분실이나 해킹 위협에 대비하기 위하여 사용하고 있습니다.



# Multi-Signature Transaction



# Multi-Sig의 필요성은?

Netflix의 ‘Trust No One’ 은 캐나다 최대 가상자산 거래소의 사고를 소개한다. 이 거래소는 거래소의 모든 Wallet의 개인키를 혼자 소유하고 있다가 대표가 사망하자 모든 자산을 찾을 수 없게 되었다.


(출처 : Netflix)

# Custody 서비스

가상자산의 보관 관리를 대행해주는 서비스로 Multi-Sig 기반으로 하여
보다 안전한 환경에서 가상자산의 보관 및 입출금을 지원한다.
많은 거래소에서 Bitgo 지갑관리 서비스를 기반으로 운영중이다.

# Bitgo의 대표적인 서비스

## ❶ Wallet Platform

거래소에서 관리하는 Hot Wallet&Cold Wallet을 대행해주는 서비스이며, 사용자, Bitgo, Backup키 총 3개 중 2개의 서명이 이루어져야 거래가 이루어지는 기술을 제공한다.

## ❷ Qualified Custody

Multi-Sig 기반으로 가상자산 보관을 대행해주는 서비스이다. 250만 달러의 보험이 가입되어 있어, Bitgo가 해킹되는 경우에도 안전한 자산 보관이 보장된다.

## ❸ Self-Managed Custody

사용자가 직접 관리하는 서비스이지만 Bitgo에서 제공하는 툴을 이용하여, 키의 안전한 관리, 키 백업, Multi-Sig등의 기능을 제공한다.

# Multi-Party Computation

기존 Multi-Signature 방식의 여러 개의 키를 생성하여 거래를 승인하는 방식이지만 MPC(Multi-Party Computation)은 키 자체를 쪼개서 거래를 승인하는 새로운 기술이다.