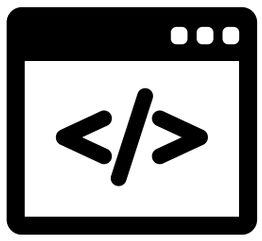
Bitcoin and Smart Contracts

Bitcoin and Smart Contracts



Bitcoin and Smart Contracts

A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.

- Nick Szabo “The Idea of Smart Contracts”

Smart Contract

- Arbitrary code executed by all participants
- Global consensus over execution
- Automated **verification** and **enforcement** of contracts
- Allow transfer of funds

Bitcoin and Smart Contracts

Alice will reveal to Bob a value x such that SHA-256(x) = 0x1b...

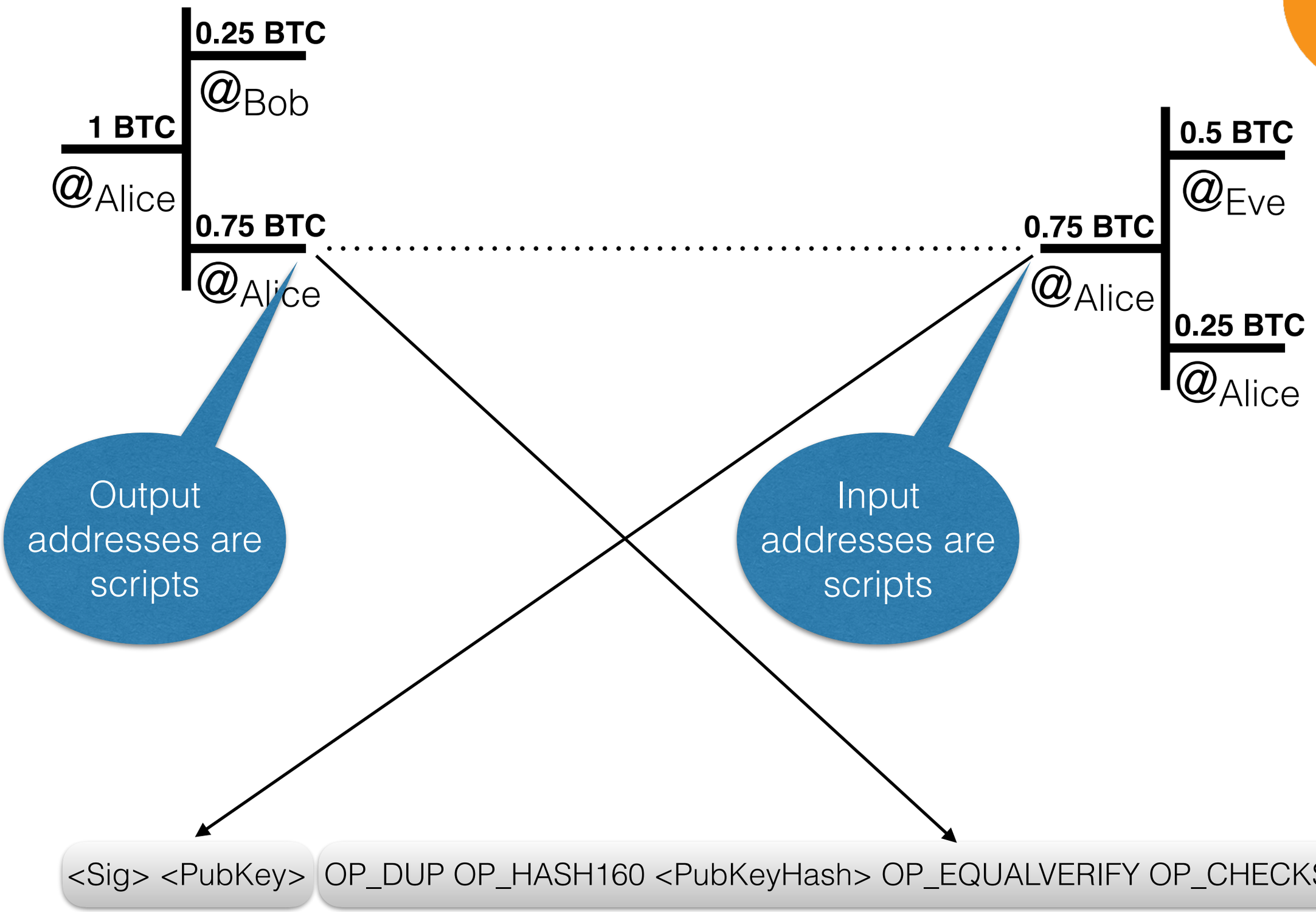
In exchange, Bob will pay USD 10.

If Alice does not reveal by July 1, 2032, then she will pay a penalty of USD 1 per day that she is late, up to USD 100.

Smart Contracts vs Traditional Contracts

	Traditional	Smart
Specification	Natural language	Code
Identity & consensus	Written Signatures	Digital signatures
Dispute resolution	Judges	Decentralized platform
Nullification	Judges	?
Payment	Legally enforced	Built-in
Escrow	Trusted Third Party	Built-in

Bitcoin Script



Bitcoin Script

- 256 opcodes total
  - 15 disabled (security!), 75 reserved
- Can handle
  - If/then
  - Arithmetic
  - Data handling
  - Crypto
    - Hashes
    - Signature verification
    - Multi-signature verification

Bitcoin Script

- Design goals
  - Simple, compact
  - Stack-based
  - No support for loops —> not Turing complete
  - Execution time/memory bound by program size

Not impressed

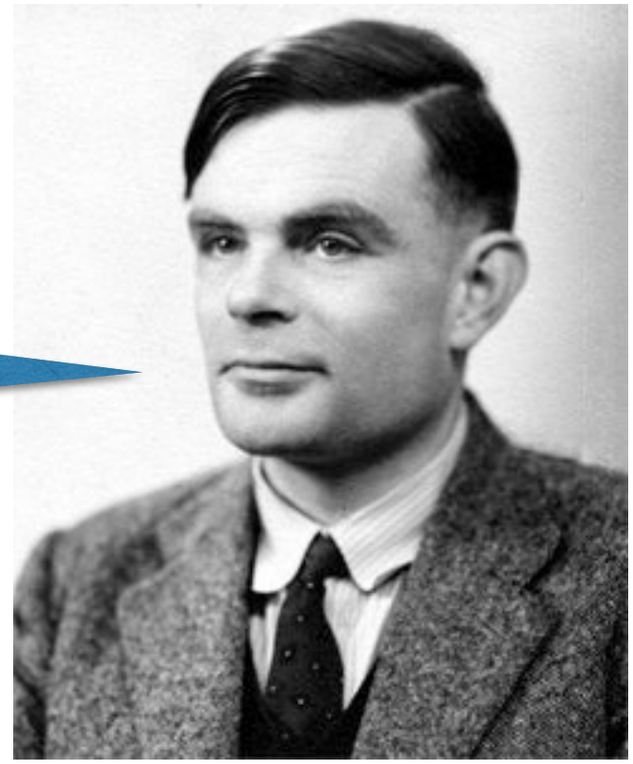


 image via Jessie St. Amand

Bitcoin Script Applications

- Proof of Burn
- Multisignature addresses
- Pay-for-hash preimage
  - Multiparty lotteries
  - Atomic cross-chain swap
- Micropayment channels
  - Use of OP_CHECKLOCKTIME

Extending Bitcoin Script

- Distributed Name Reservation (Namecoin)
- Prediction Markets (Augur, Futurecoin)
- Decentralized Markets (OpenBazaar)
- Financial Instruments (MasterCoin)

Why not a more flexible and open language?