Writing Smart Contracts
09 Oracles

Peter H. Gruber

Supported by the Algorand Foundation

Oracles

Oracle = Link between blockchain and outside world

- Record data about outside world on the blockchain
  - Prices of off-chain assets (stocks, commodities)
  - State of nature (temperature, CO_2 concentration, crops, ...)
  - Results of off-chain events (sports games, elections, ...)

Use of oracles

- Input value in smart contracts
  - Financial derivatives
  - Insurance
  - Betting

The oracle problem

- Weakest link in chain of trust along the blockchain
- Oracles can fail or be compromised
- Solutions
  - Technical: hardware oracles
  - Economic: majority oracles, economic incentives