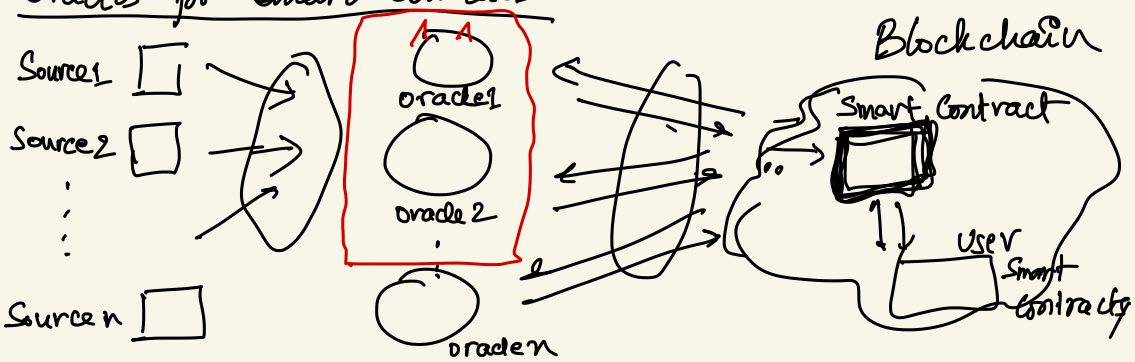
Oracles for Smart Contracts



- Decentralization (not a single oracle)
- Correctness of responses
- Availability
- Privacy Guarantees

Today.

Aggregation :- Majority (boolean values)

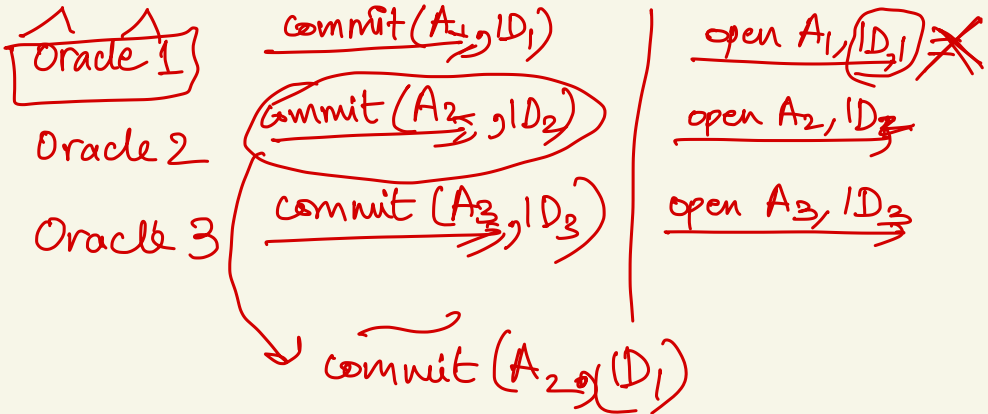
- Mean/Avg. (non-boolean/large space)

⋮

- Where should we do aggregation

  - On-chain (expensive, but convenient for record-keeping/certification system)
  - Off-chain (efficient, but more difficult to do record-keeping)
    - (Threshold Signatures)

Freeloading Problem.



Oracle2 commits
Oracle 3 commits
Oracle 1 commits

Oracle 1 open
oracle 3 opens
oracle 2 opens

- Either use "above order" ✓
  or non-malleable commitments
  (Hash-based comm work, atleast in RO model).

- Sybil attacks ?
- Mirroring attacks.

Is this necessary.

Chainlink.
on-chain agg.

Medium-term off-chain agg using Threshold Crypto

Long-term Trusted Hardware