Sessions 07
Blockchain Protocol (1)

Blockchain Protocols and Decentralized Applications

Comments

- A new computing paradigm
  - Programmable computer not owned by anyone and everyone can use
  - Think of a few use cases?
- Cryptocurrencies are the means, not the ends
  - Charging for blockchain usage and rewarding actors that contribute to the protocol
- Principles over protocols
  - Explain about blockchain fundamentals and combine with protocol examples

Permanents Assumptions

- Internet exists
  - Semi-reliable mechanism for p2p communication between untrusted parties
- Cryptography exists
  - Hashing functions and Digitals signatures
  - Impossible to forge signature without private key

State Machine Replication (SMR) Problem

- Managing a replicated database
  - SMR Motivation: increase uptime
- Blockchain
  - State: current status of blockchain and its users
  - State transition: transaction (payment) from one account to another
- Blockchain SMR motivation?
  - decentralization

Problem Definition

- Goal
  - Keep nodes in sync
  - Same sequence of state transitions
  - Agree on the current state
- Two types of actors:
  - Nodes: responsible for consensus protocol
  - Users/Clients: submit “transactions” to one/more nodes
- Nodes - ordered list of transactions that only grows over time
- Order matters?

Solution

- Protocol
  - Piece of code ran by nodes
  - Computation (transactions) and communication (consensus)
- Node
  - Perform computation (transactions) - change state
  - Receive message from other nodes & clients
  - Send messages to other nodes
- Goals?

Goals

- Consistency
  - History agreement
  - What about the “lazy nodes”?
  - Is Consistency enough?
- Liveness
  - Every transaction submitted to at least one node is eventually added to every node’s history
- Issues
  - Communications
  - Fault tolerance

Assumptions

- Permissioned setting
  - Number of nodes are known
  - Each node is identifiable (IP addr, number, name, etc.)
  - Before Bitcoin, only permissioned
- PKI (*public key infrastructure*)
  - pki/ski pair; pki known to all nodes upfront
- Synchronous Model
  - Global clock
  - Round 1,2,3,4…
  - Msg sent at round **t**, will be received at **t+1**
- All honest nodes
  - Way too strong