Lecture 2: Byzantine Broadcast in the Synchronous Model via the Dolev-Strong Protocol

(Lecture Series on Foundations of Blockchains)

Recap of the SMR Problem

- Clients submit transactions to one or more nodes (machines running the blockchain protocol) (users of blockchain)
- each node maintains local history (append-only data structure)

Goal: a protocol (event-driven code) that satisfies:

(1) Consistency: all nodes agree on the same history

(2) liveness: every submitted tx eventually added to all nodes' histories

Plan: solve first under a bunch of assumptions, relax assumptions one-by-one.

Assumptions (to be relaxed)

1. permissioned. a priori known set of nodes $\{1, 2, \ldots, n\}$ (known IP addresses).
2. PKI ("public key infrastructure"). each node i has a pk_i/sk_i pair, pk_i known to all nodes upfront.
3. synchronous. (i) all nodes share a global clock, time steps $0, 1, 2, 3, \ldots$
   (ii) all msgs sent at time t arrive by time $t+1$ (in some arbitrary order)
4. all honest nodes: all nodes run intended protocol, no (intended or unintended) deviations.

Solution via Round-Robin Leaders

Idea: nodes take turns as "leaders." (e.g., round-robin, or choose randomly)

- leader sends ordered list of txs it knows about to all other nodes
  (plays the role of a "block")
- when node receives most recent leader's ordered list, appends it to local history

Note: satisfies consistency + liveness.

- consistency: nodes operate in lockstep
- liveness: every node eventually becomes leader, adds all txs it knows about

Faulty/Byzantine Nodes

Definition: a node that is not honest is called faulty.

Types of faulty nodes:

1. Crash fault. (run honestly until some failure time, then stop entirely – no more messages sent)
2. Omission fault. (can selectively withhold messages it's supposed to send)
3. Byzantine fault. (can behave arbitrarily) (though still can't break cryptography)

Canonical policy: send conflicting messages to different nodes.

New assumption (4): For known parameter f, $\leq f$ nodes are Byzantine, other $\geq n-f$ nodes are honest.

The Byzantine Broadcast Problem

Idea: stick with the rotating leaders approach.

Subroutine: Byzantine broadcast. (BB)

- one node is the sender (known to all up front)
- sender has a private input $v^* \in V$

Goals

1. termination. each honest node eventually halts w/ some value $v_i \in V$
2. agreement. all honest nodes choose the same value v_i.
3. validity. if sender is honest, all honest v_i's equal v^*.

'i's guess of what v^* is

SMR Reduces to BB

SMR Protocol: [given a Byzantine broadcast subroutine]

1. take turns as leader (e.g., round-robin)
2. run BB protocol (with sender = current leader), agree on a tx list L.
3. each node appends L to its local history

Why is the reduction correct?

- BB agreement $\Rightarrow$ SMR consistency (every time step, all honest nodes add the same tx list)
- BB validity $\Rightarrow$ SMR liveness
  (if honest node knows about a tx, eventually will become the leader (sender $\Rightarrow$ since honest, validity $\Rightarrow$ all other honest nodes add that tx))

Intuition: The $f = 1$ Case ($n \geq 4$)

Proposed protocol: (to be run by honest nodes)

$t=0$: sender sends its value v^* to all other nodes (signed, as always)

$t=1$: nodes echo msg from sender to all other nodes (signed again)

$t=2$: each node i chooses output v_i by majority vote (≤ 1 vote from sender, $\leq n-2$ from other non-senders)

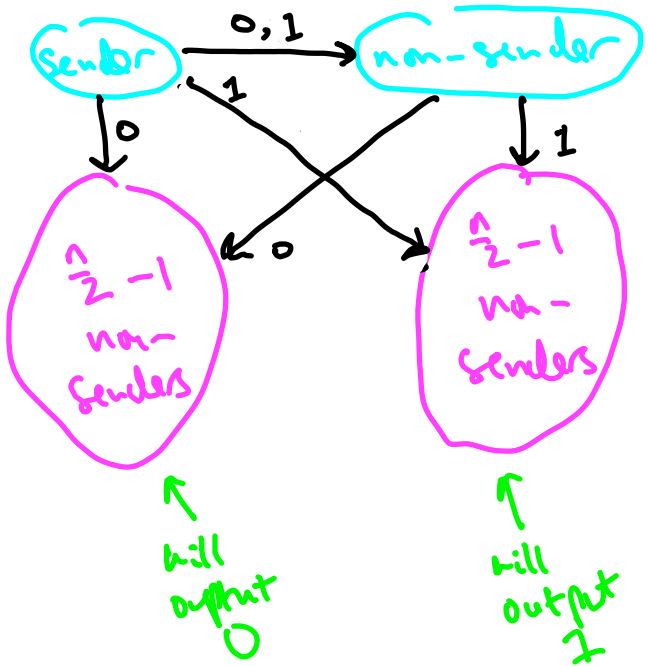
(if leader, output v^*) break ties consistently (e.g., lexicographically)

Note: validity + agreement (+ termination) hold.

- honest leader $\Rightarrow$ honest non-sender receives $\geq n-2$ votes for v^*
- Byzantine leader $\Rightarrow$ all (honest) non-senders collect exact same set of votes, all output the same value (chosen by majority vote)

Counterexample for $f = 2$

Claim: previous protocol does not satisfy agreement when $f = 2$.



The Dolev-Strong Protocol (I) (1983)

Definition: node i is convinced of value v at time t if it receives a message such that:

- references the value v
- signed first by the sender
- signed also by $\geq t-1$ other distinct nodes, none of which are i

The Dolev-Strong Protocol (II)

Protocol: (to be run by honest nodes)

$t=0$: Sender (with private input v^*) sends v^* (with its signature) to all other nodes

$t=1,2,3,\ldots,f+1$: if node i convinced of value v at this time step by a message m, add i's signature and echo to all other nodes

Final output: if node i convinced of exactly one value v, output v;

otherwise, output $\perp$. (default value, e.g. empty list of txs)

(convinced of 0 or ≥ 2 values)

Theorem: under current assumptions (permissioned, PKI, synchronous), the Dolev-Strong protocol satisfies validity + agreement.

Dolev-Strong Protocol: Validity

Claim: The Dolev-Strong protocol satisfies validity.

Proof: Assume sender is honest.

=> at $t=0$, will send v^* (with its signature) to all other nodes (received by time $t=1$)

=> all honest nodes convinced of v^* already at the $t=1$

Ideal signatures assumption => can't forge messages from the sender

=> no way to convince an honest node of any value $v \neq v^*$

=> all honest nodes output v^*

QED

Dolev-Strong Protocol: Agreement

Claim: the Dolev-Strong protocol satisfies agreement.

Sufficient: if an honest node i ever gets convinced of a value v
$\Rightarrow$ all honest nodes convinced of v by end of protocol.
($\Leftarrow$ all honest nodes convinced of same set of values $\Rightarrow$ all output the same thing)

Case 1: node i gets convinced of value v by message m at time $t < f+1$
$\Rightarrow$ will add its signature to m + send to all other nodes
$\Rightarrow$ all honest nodes convinced of v by the step $t+1 \leq f+1$.

Case 2: convinced at time $f+1$.
$\Rightarrow$ convinced by a message with $f+1$ distinct signatures
$\Rightarrow$ one of those must have been provided by an honest node (at some earlier timestep) ($\leq f$ non-honest nodes)
$\Rightarrow$ all honest nodes by now convinced of v

QED

Dolev-Strong: How Big Can f Be?

Question: how does value of f affect the DS protocol + its analysis?

- protocol's duration scales linearly with f
- validity, agreement hold no matter what f is (very unusual)

Note: but in SMR context, only useful if $f < n/2$.

- if $f < n/2$, can resolve conflicts through majority vote