On the Liveness Properties of the Stellar Consensus Protocol

Giuliano Losa

UCLA

SCP should satisfy the safety and liveness properties of Consensus

Safety:

Validity: an *intertwined* node must not externalize an invalid value

Agreement: *intertwined* nodes must never externalize different values

A set of nodes is intertwined when all their quorums intersect at well-behaved nodes

Liveness:

If we wait long enough, all *intact* nodes should externalize a value

SCP is not live under eventual synchrony if some nodes are malicious

Asynchronous		Eventually synchronous		
Crash-stop	Malicious	Crash-stop	Malicious	Eventually crash-stop
Intertwined are safe	Intertwined are safe	Intertwined are safe Intact are live with probability 1		

SCP is not live under eventual synchrony if some nodes are malicious

Asynchronous		Eventually synchronous		
Crash-stop	Malicious	Crash-stop	Malicious	Eventually crash-stop
Intertwined are safe	Intertwined are safe	Intertwined are safe Intact are live with probability 1		

SCP is not live under eventual synchrony if some nodes are malicious

Asynchronous		Eventually synchronous		
Crash-stop	Malicious	Crash-stop	Malicious	Eventually crash-stop
Intertwined are safe	Intertwined are safe	Intertwined are safe Intact are live with probability 1		

SCP is not live under eventual synchrony if some nodes are malicious

Asynchronous		Eventually synchronous		
Crash-stop	Malicious	Crash-stop	Malicious	Eventually crash-stop
Intertwined are safe	Intertwined are safe	Intertwined are safe Intact are live with probability 1	Intertwined are safe No liveness	

SCP is not live under eventual synchrony if some nodes are malicious

Asynchronous		Eventually synchronous		
Crash-stop	Malicious	Crash-stop	Malicious	Eventually crash-stop
Intertwined are safe	Intertwined are safe	Intertwined are safe Intact are live with probability 1	Intertwined are safe No liveness	Intertwined are safe Intact are live with probability 1

The Intact Set is a set of nodes that can enjoy safety and liveness

Whitepaper: a set I is intact when

- After deleting V \ I, I is intertwined
- I is a quorum

New definition: a set I is intact when

- After deleting B, I is intertwined
- I is a quorum

The Intact Set is a set of nodes that can enjoy safety and liveness

Whitepaper: a set I is intact when

- After deleting V \ I, I is intertwined
- I is a quorum

New definition: a set I is intact when

- After deleting B, I is intertwined
- I is a quorum

Note that B may be smaller than V \ I;
in this case the new Intact Set is larger than the old one

The Intact Set is a set of nodes that can enjoy safety and liveness

Whitepaper: a set I is intact when

- After deleting V \ I, I is intertwined
- I is a quorum

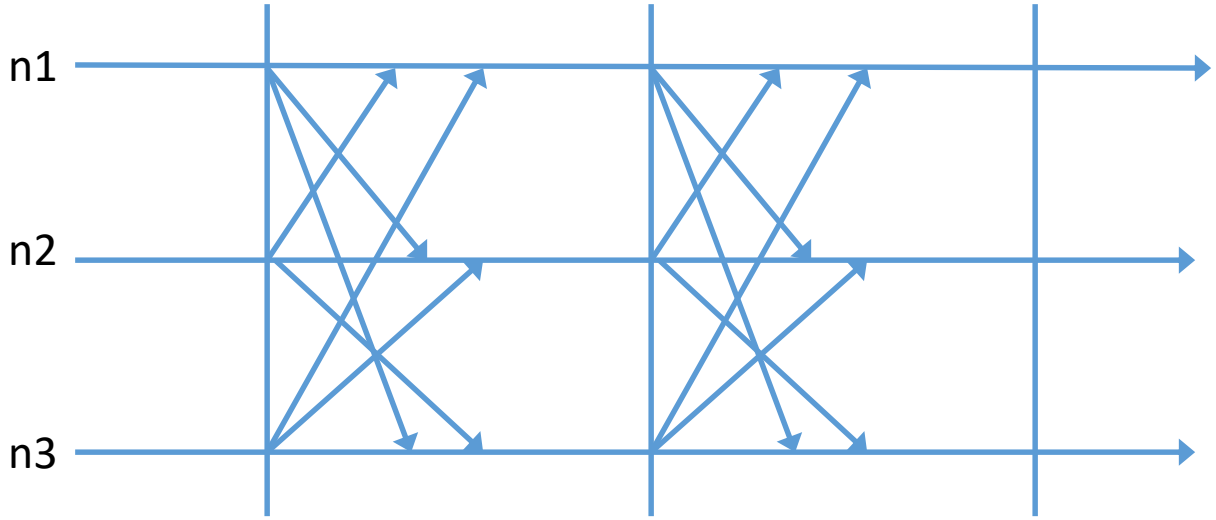
New definition: a set I is intact when

- After deleting B, I is intertwined
- I is a quorum

Note that B may be smaller than V \ I;
in this case the new Intact Set is larger than the old one

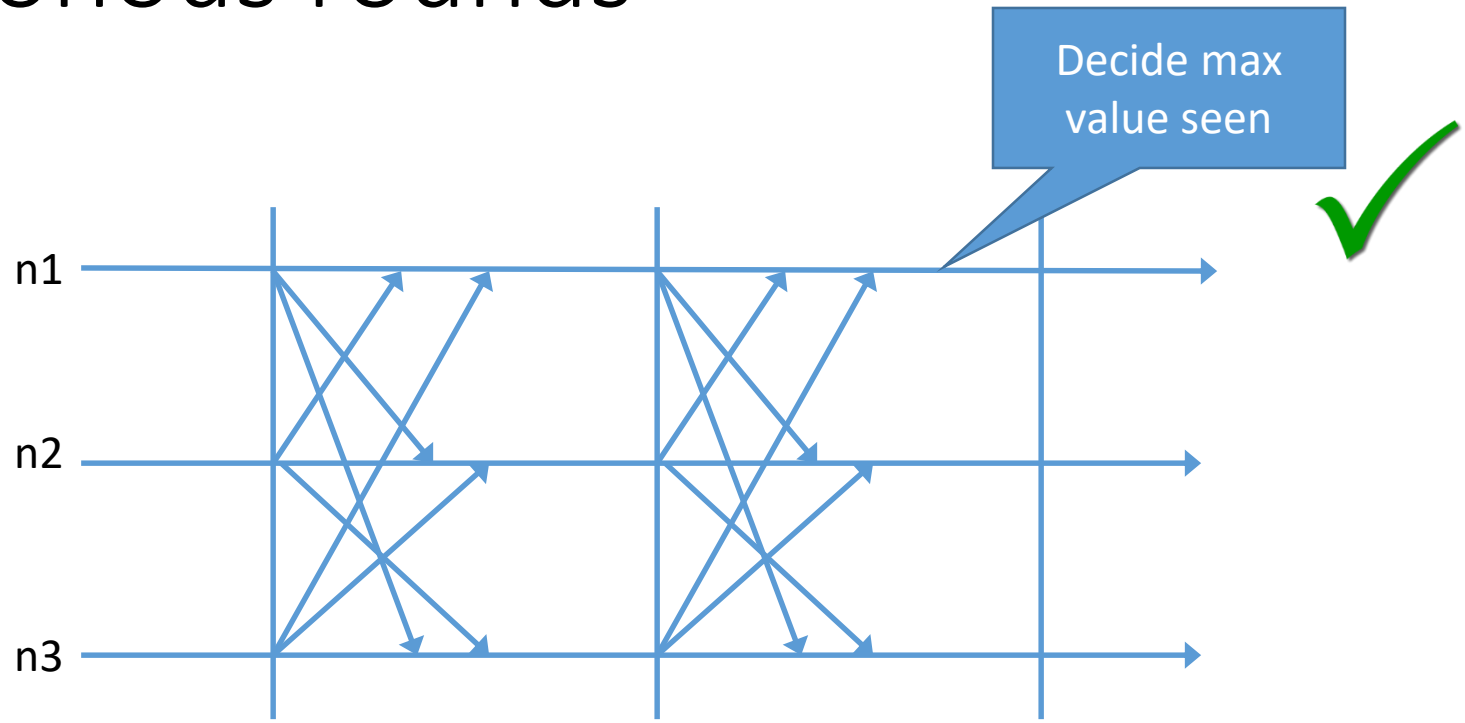
Conjecture: no protocol can ensure safety and liveness for a larger set

Eventual synchrony allows implementing synchronous rounds



Synchronous rounds in a crash-stop system

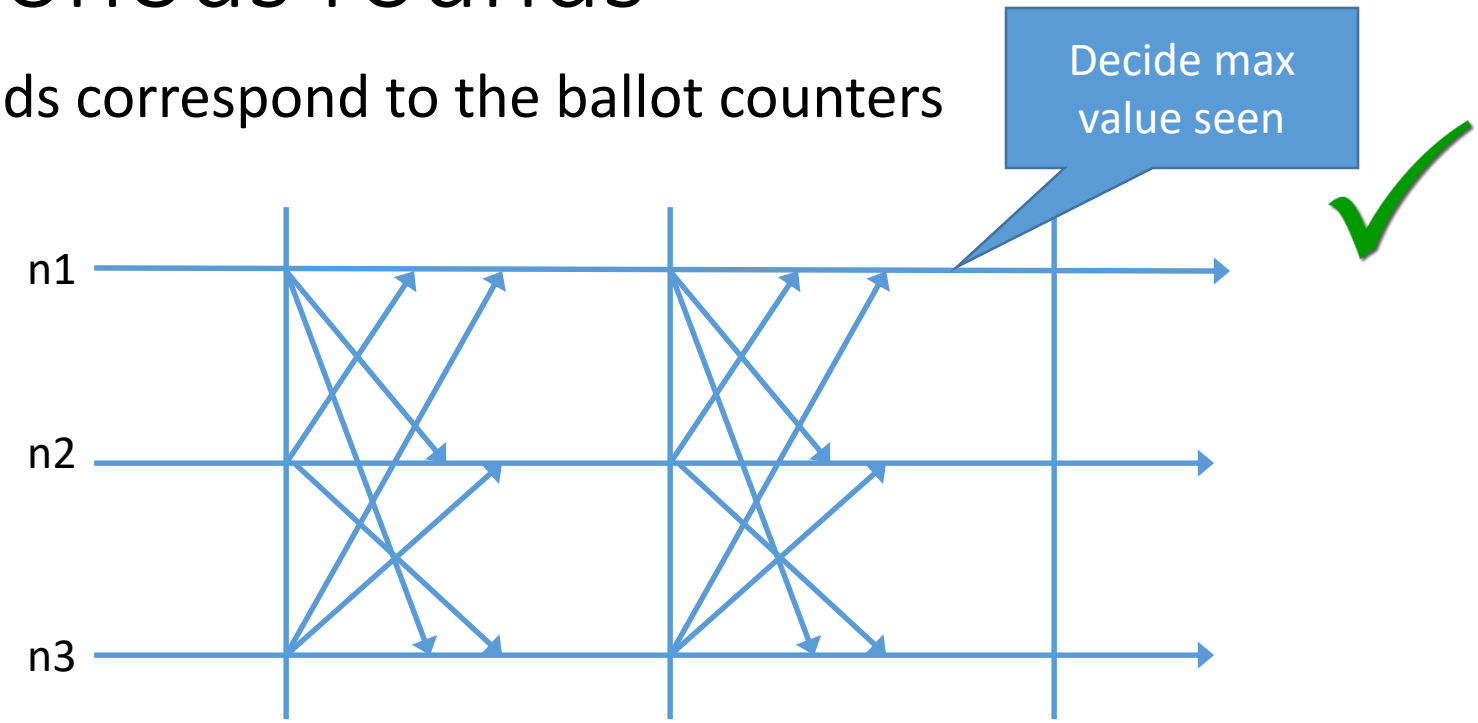
Eventual synchrony allows implementing synchronous rounds



Synchronous rounds in a crash-stop system

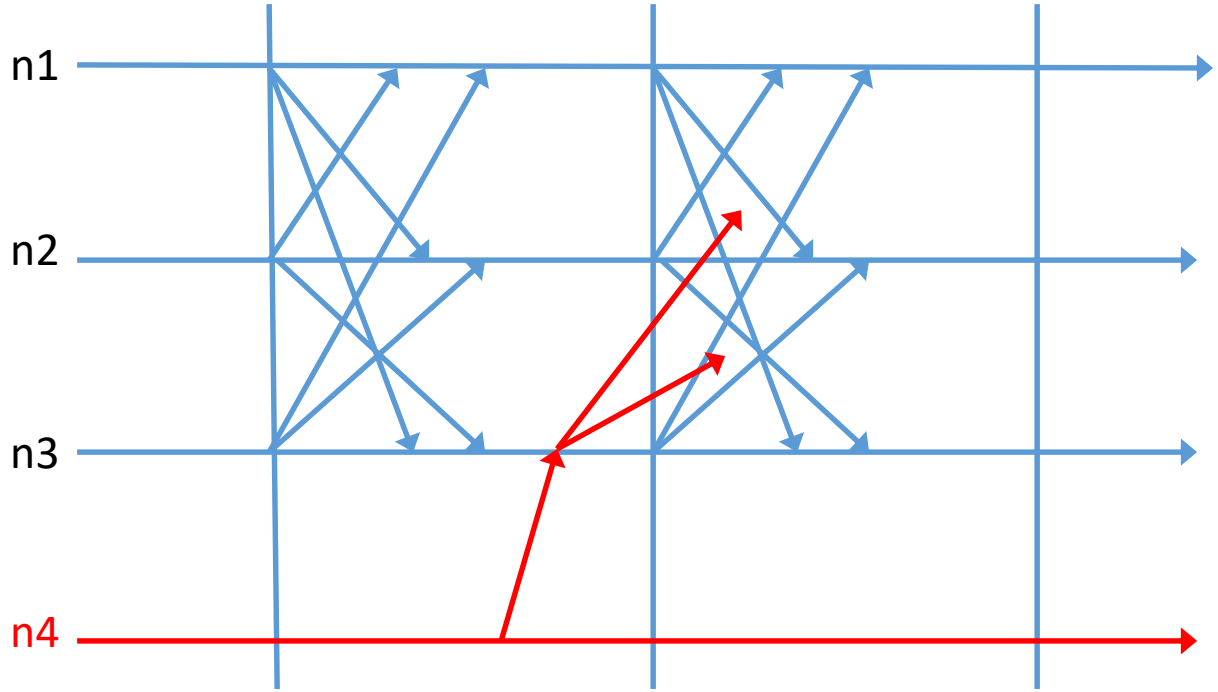
Eventual synchrony allows implementing synchronous rounds

In SCP, rounds correspond to the ballot counters



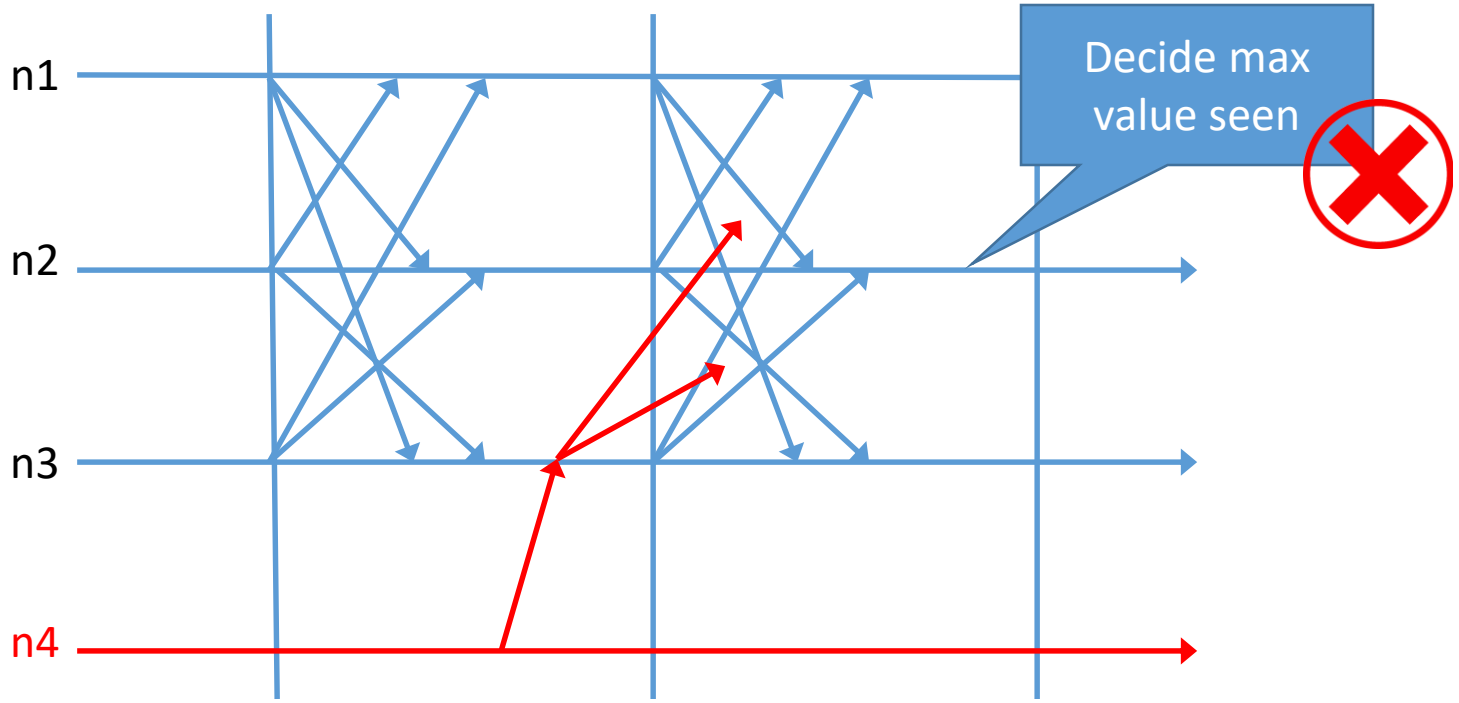
Synchronous rounds in a crash-stop system

Malicious nodes may not follow the round structure



In SCP, n4 cannot cause disagreement but can delay a decision forever

Malicious nodes may not follow the round structure



In SCP, n4 cannot cause disagreement but can delay a decision forever

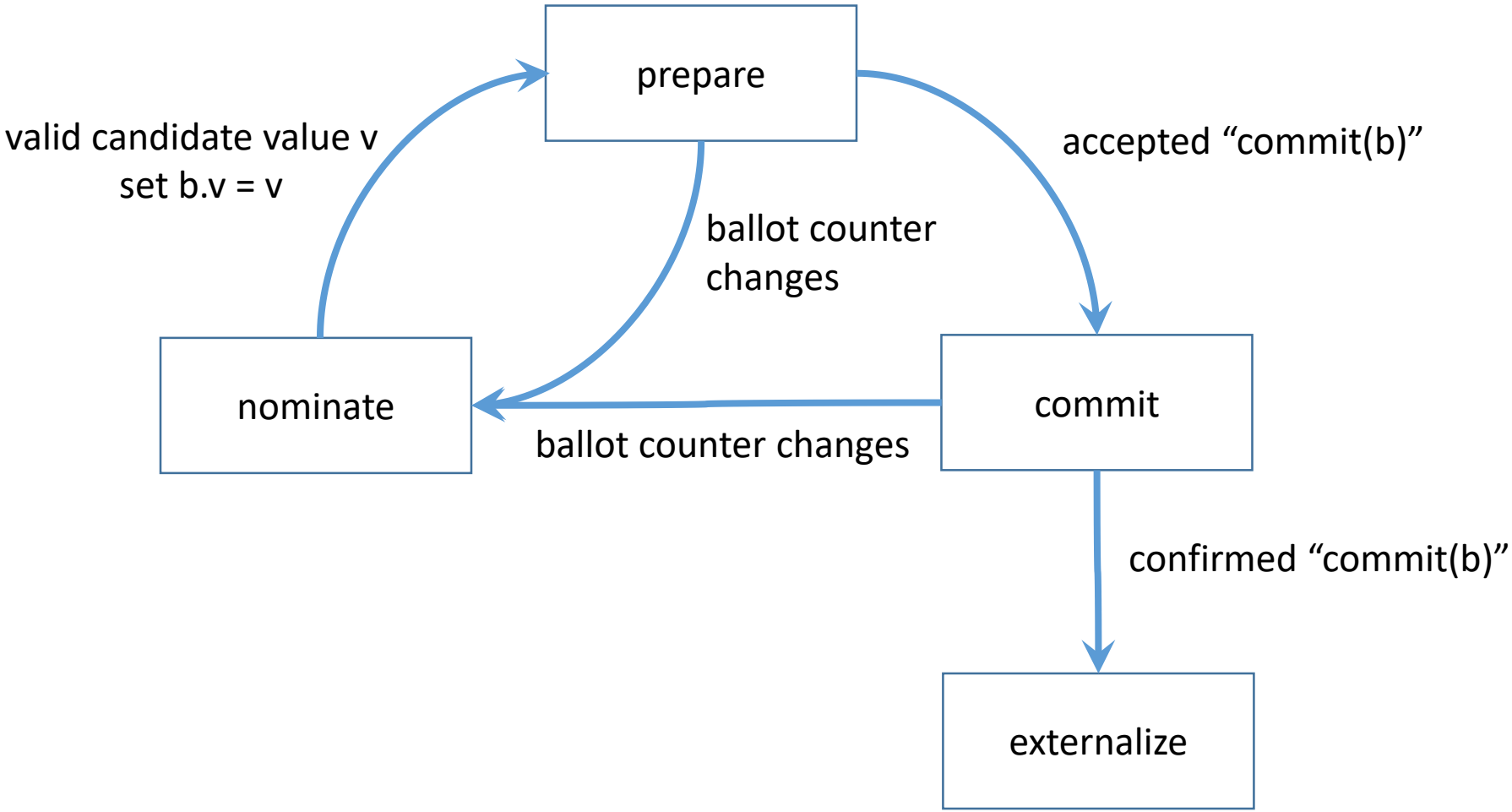
Classic solution in a closed system: use a round-robin leader

- Statically map rounds to leaders round-robin (e.g. node number i is leader of every ith round out of N)
- Nodes do not accept values not signed by the leader
- Still need to be warry of a malicious leader: cross-check value to ensure safety
- There must come a round in which the leader is well-behaved, which ensures liveness

In SCP, the nomination protocol can achieve the effect of leaders

- Round-robin leader not possible without known, fixed configuration
- Nomination guarantees agreement on a value with non-zero probability; like having a well-behaved leader with non-zero proba.
- Idea: run nomination at the beginning of every round

New phase diagram



SCP is live if malicious nodes can be identified and removed from slices

In practice, is it worth changing SCP?

Upcoming

- Streamlined theory of slice infrastructures (including new definition of intact)
- New, simpler consensus algorithm