Revisiting the Federated Byzantine Agreement Model

Giuliano Losa

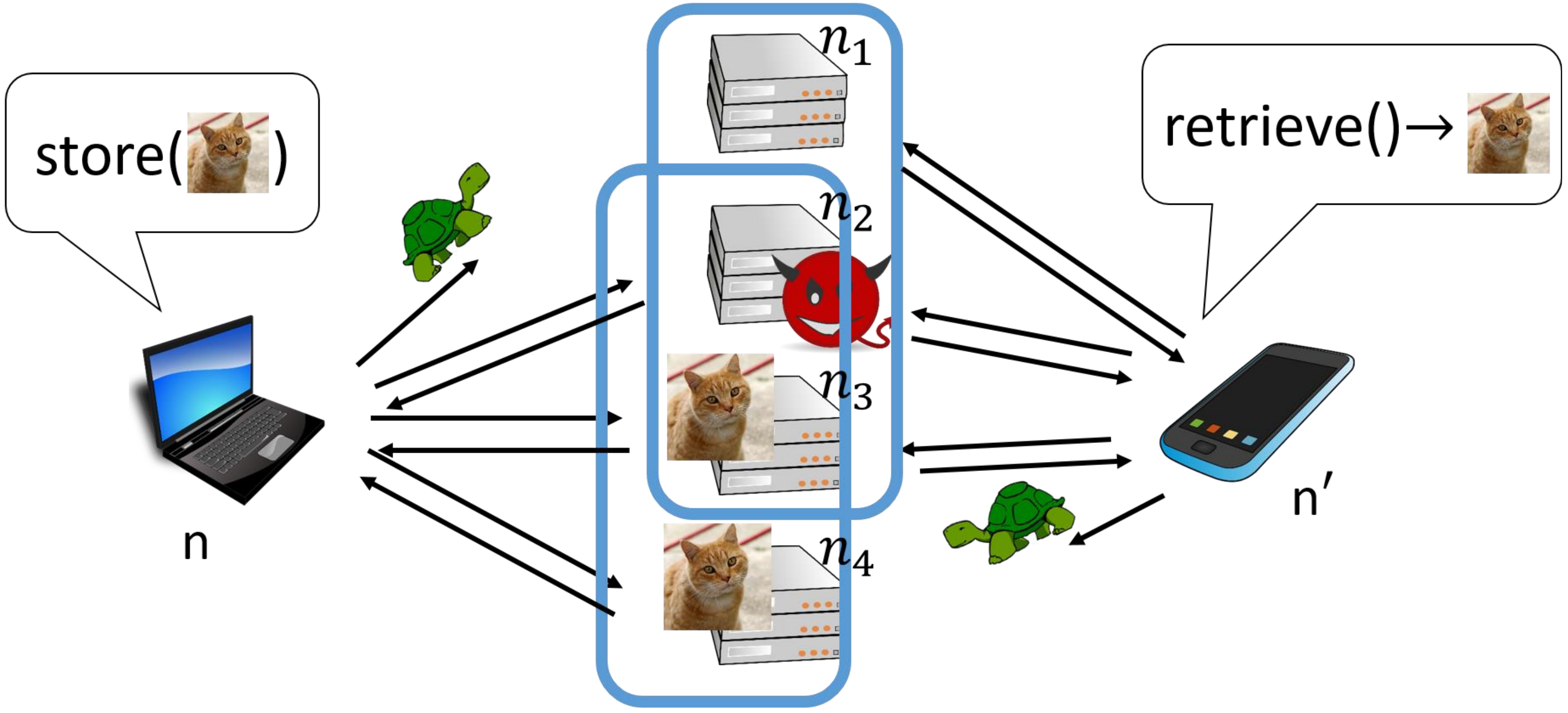
Stellar Development Foundation

Joint work with Christian Cachin, James Murdoch Gabbay,

Eli Gafni, David Mazières, and Luca Zanolini

Example: storing a file reliably in an asynchronous network with 4 servers among which 1 unknown server may fail

- To store the file, make sure at least 3 servers have it
- To retrieve the file, query at least 3 servers



Quorum systems formalize access structures under failure assumptions

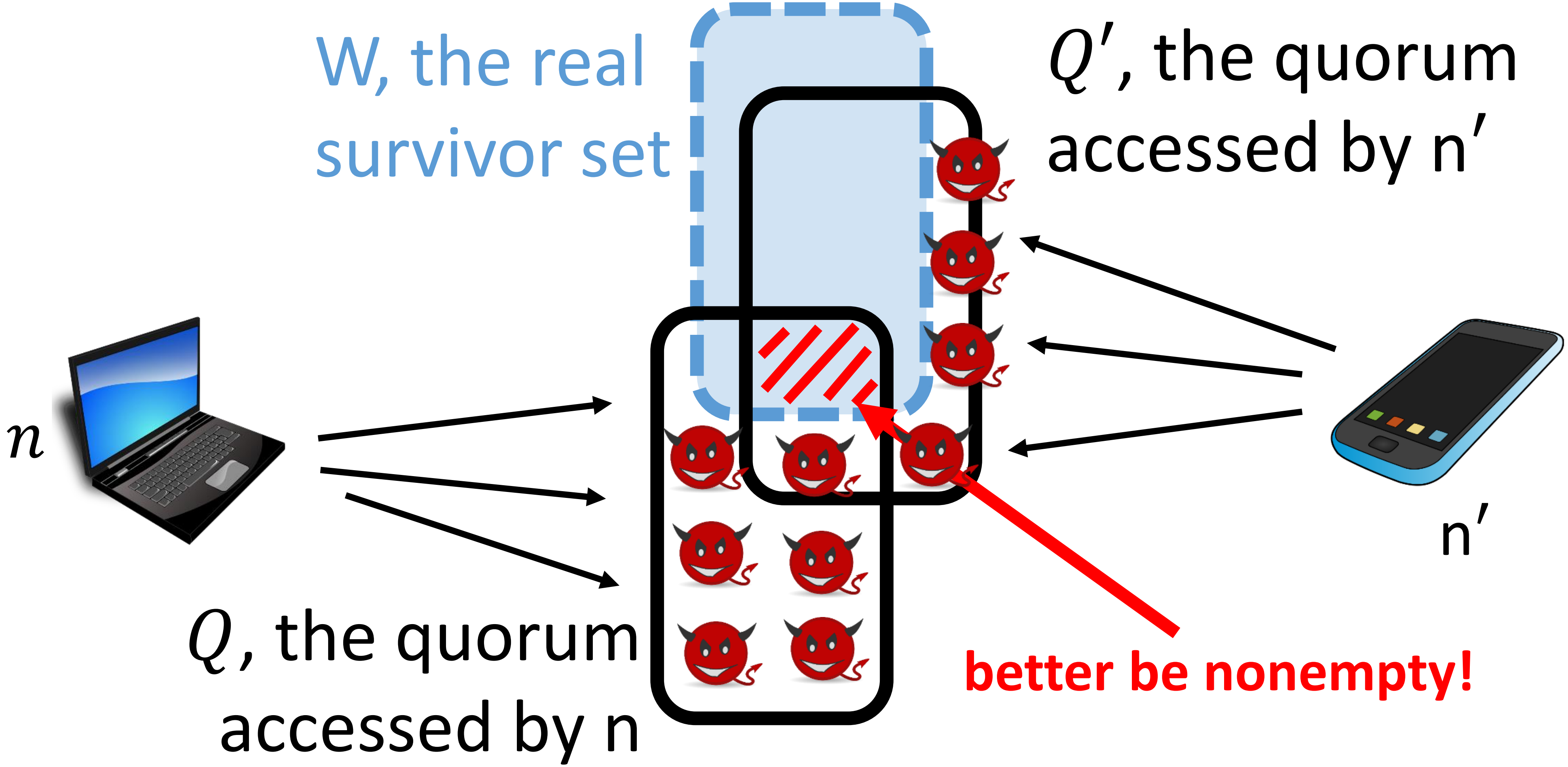
We have:

- A set of nodes N
- A quorum system $\mathbb{Q} \subseteq 2^N$
  What the nodes access
- A survivor-set system $\mathbb{S} \subseteq 2^N$
  At least one survivor set does not fail

$\mathbb{Q}$ is a quorum system for $\mathbb{S}$ when:

1. For liveness: every survivor set includes a quorum
2. For safety: every two quorums and one survivor set have nonempty intersection

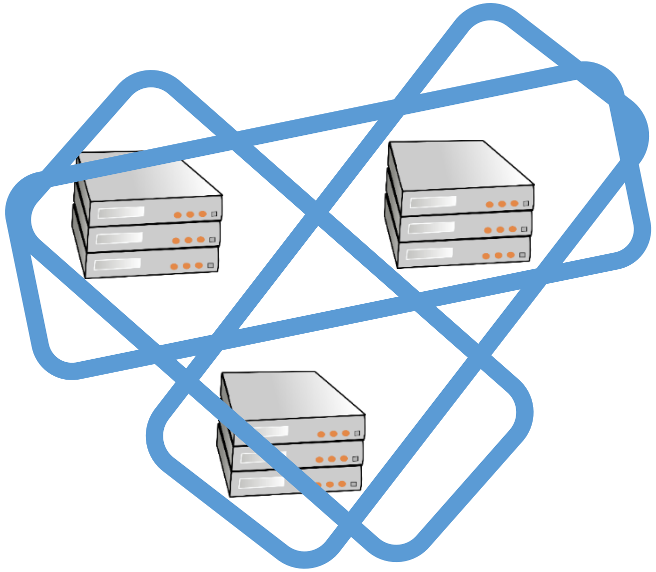
Every 2 quorums and 1 survivor set must have nonempty intersection



There exists a quorum system for $\mathbb{S}$ if and only if every three survivor sets intersect

This is the $\boldsymbol{Q^3}$ property:

$$\boldsymbol{Q^3} \equiv \forall S_1, S_2, S_3 \in \mathbb{S}. S_1 \cap S_2 \cap S_3 \neq \emptyset$$



With 3 serves, we cannot tolerate even 1 failure

1 failure = survivor sets of cardinality 2

$$\{n_1, n_2\} \cap \{n_2, n_3\} \cap \{n_3, n_1\} = \emptyset$$

Quorum systems formalize access structures under failure assumptions

We have:

- A set of nodes N
- A quorum system $\mathbb{Q} \subseteq 2^N$
  What the nodes access
- A survivor-set system $\mathbb{S} \subseteq 2^N$
  At least one survivor set does not fail

$\mathbb{Q}$ is a quorum system for $\mathbb{S}$ when:

1. For liveness: every survivor set includes a quorum
2. For safety: the intersection of any two quorums and a survivor set is nonempty

$\mathbf{Q^3}$: There exists a quorum system for $\mathbb{S}$ if and only if every three survivor sets intersect

When $\mathbf{Q^3}$ holds, we can take $\mathbb{Q} = \mathbb{S}$ the canonical quorum system

Quorum systems are the framework behind the classic distributed-computing toolbox

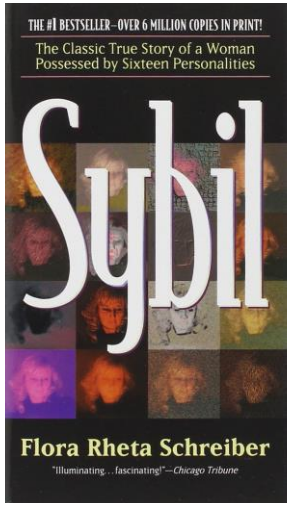
Reliable broadcast, consensus, shared-memory emulation, group membership, atomic commit, distributed transactional memory, etc. with algorithms such as Bracha broadcast, PBFT, Byzantine Paxos, …

Great, but developed for centrally managed systems
Now we care about permissionless systems

Can traditional quorum systems work in a permissionless system?

- Anybody can unilaterally join or leave the system at any time
- No one knows precisely who is in the system at a given time
- Attackers can try to overwhelm the system with many puppets, also called Sybils

➔ A fixed set of quorums will not work



We can use proof-of-stake

- In proof-of-stake, we count money instead of identities
  - E.g. the survivor sets are the sets collectively holding more than 2/3rds of the money
- Caveats
  - Long-range attacks
  - Centralization risk
  - Does wealth reflect trustworthiness or reliability?

Why not let each node make its own failure assumptions and pick its own quorum system?

Each node n chooses a survivor set system $\mathbb{S}_n \subseteq 2^N$ for itself

$\mathbb{S}_n$ encodes the assumptions of node n

Two nodes $n \neq n'$ may make different assumptions and have $S_n \neq S_{n'}$

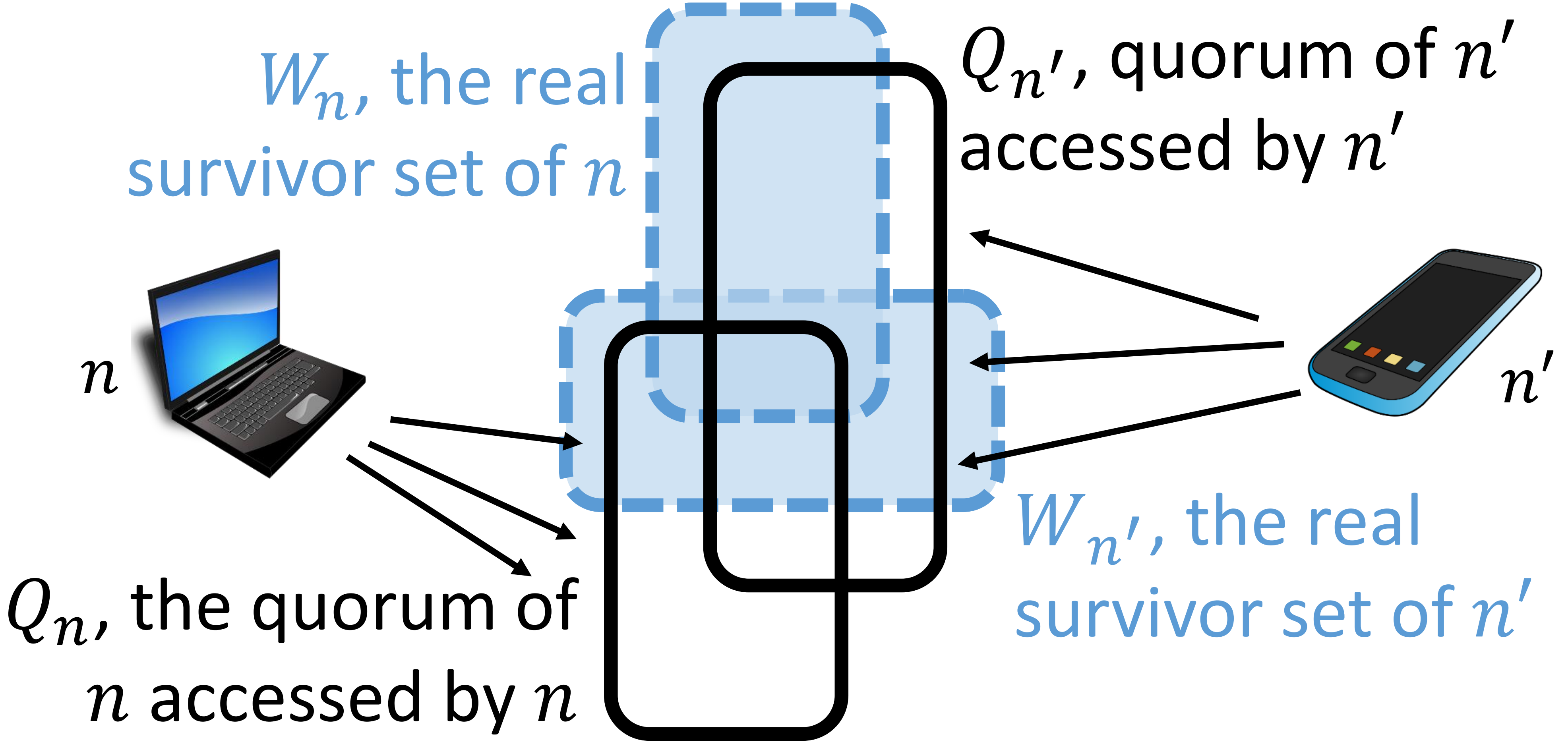
We call this the asymmetric model

Each node n chooses a quorum system $\mathbb{Q}_n \subseteq 2^N$ for itself

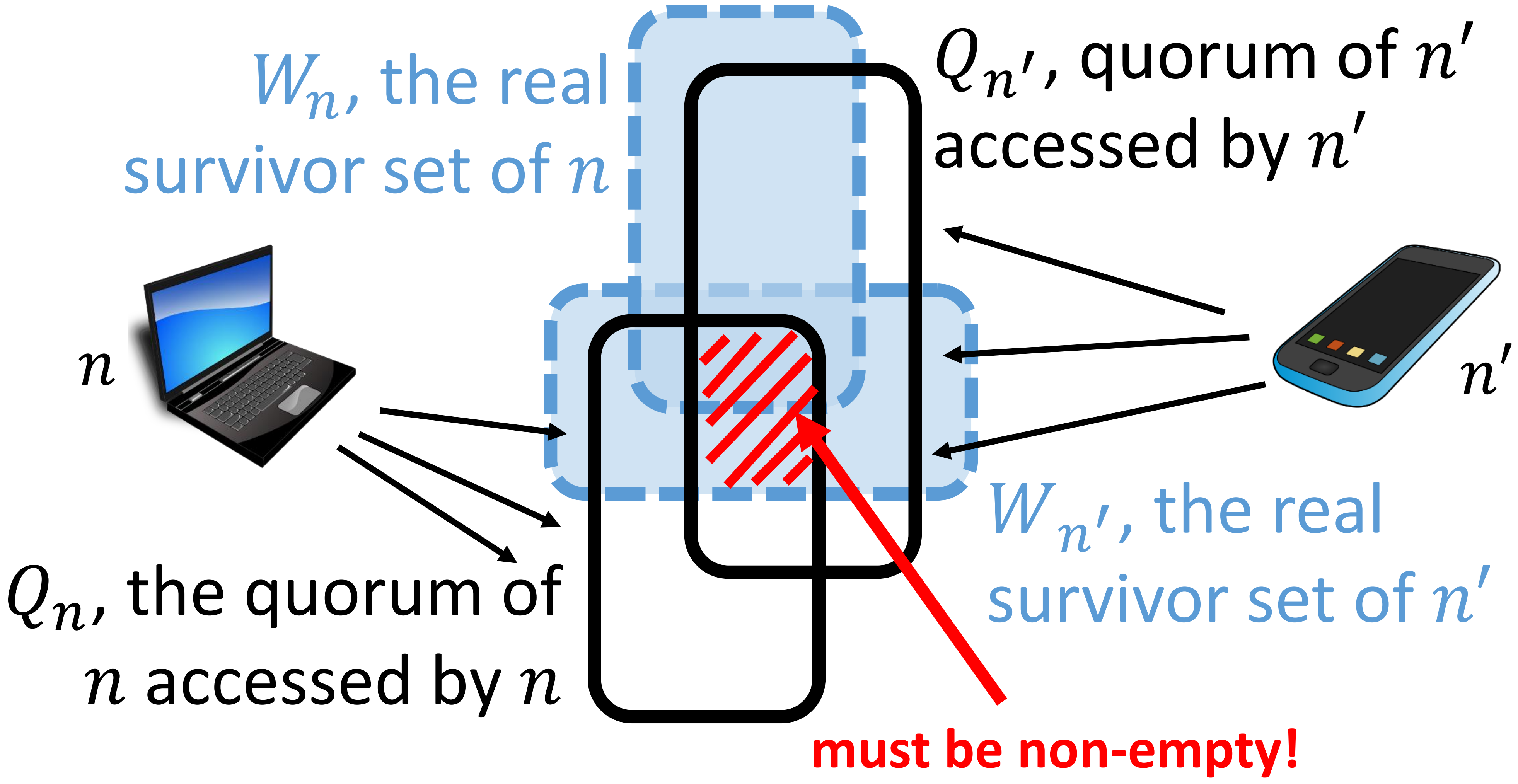
Requirements:

1. For liveness: every survivor set of n contains a quorum of n
2. For safety: $\forall n, n'. \forall Q_n \in \mathbb{Q}_n, W_n \in \mathbb{S}_n, Q_{n'} \in \mathbb{Q}_{n'}, W_{n'} \in \mathbb{S}_{n'}.$
$$Q_n \cap Q_{n'} \cap \left(W_n \cup W_{n'}\right) \neq \emptyset$$

When does the store-retrieve algorithm work?



$$\boxed{Q_n \cap Q_{n'} \cap \left(W_n \cup W_{n'}\right) \neq \emptyset}$$



There exists a quorum system for $\{\mathbb{S}_n . n \in N\}$ if and only if $\mathbf{B^3}$ holds

$$S_1, S_2 \ \in \mathbb{S}_n, S_1', S_2' \in \mathbb{S}_{n'} \Rightarrow S_1 \cap S_1{}' \cap (S_2 \cup S_2{}') \neq \emptyset$$

When B^3 holds, we can take $\mathbb{Q}_n = \mathbb{S}_n$ for all n (the canonical quorum system)

We can solve reliable broadcast and shared memory for subsets called guilds

Say nodes are faulty, naïve, or wise

naïve = well-behaved but assumptions violated
wise = well-behaved + assumptions satisfied

The set of nodes G is a guild when

1. G is wise and
2. G satisfies it own assumptions

Maybe we don't need proof-of-stake after all…


Asymmetric Distributed Trust

Christian Cachin[1]
University of Bern
cachin@inf.unibe.ch

Björn Tackmann[2]
IBM Research - Zurich
bta@zurich.ibm.com

2019-06-20

Abstract

Quorum systems are a key abstraction in distributed fault-tolerant computing for capturing trust assumptions. They can be found at the core of many algorithms for implementing reliable broadcasts, shared memory, consensus and other problems. This paper introduces *asymmetric Byzantine quorum systems* that model subjective trust. Every process is free to choose which combinations of other processes it trusts and which ones it considers faulty. Asymmetric quorum systems strictly generalize standard Byzantine quorum systems, which have only one global trust assumption for all processes. This work also presents protocols that implement abstractions of shared memory and broadcast primitives with processes prone to Byzantine faults and asymmetric trust. The model and protocols pave the way for realizing more elaborate algorithms with asymmetric trust.

1 Introduction

Byzantine quorum systems [19] are a fundamental primitive for building resilient distributed … on untrusted components. Given a set of nodes, a quorum system captures a trust … nodes in terms of potentially malicious protocol participants and colluding … quorum systems, many well-known algorithms for *reliable broadcast* … more have been implemented; these are the main abstractions … other and to achieve consistency despite the actions of …

How do we make sure that $\mathbf{B^3}$ holds at least for a large fraction of the system?

$\mathbf{B^3}$ is an intersection property that must hold for every two nodes

How can it possibly work in open systems where some nodes do not even know each other exist?

Maybe there will be a cartel that everyone trusts to put in their quorums. This seems to be the assumption behind Ripple.

We can do better with FBA!

Federated Byzantine Agreement: make assumptions about assumptions

Each node n picks a set of *quorum slices* $\mathbb{SI}_n$ and assumes that it has at least one slice $S \in \mathbb{SI}_n$ such that:

1. All members of S are well-behaved
2. All members of S in turn have their assumptions satisfied

W is a minimal survivor-sets/quorum of n when:

a. $n \in Q$

b. every member of W has a slice in W

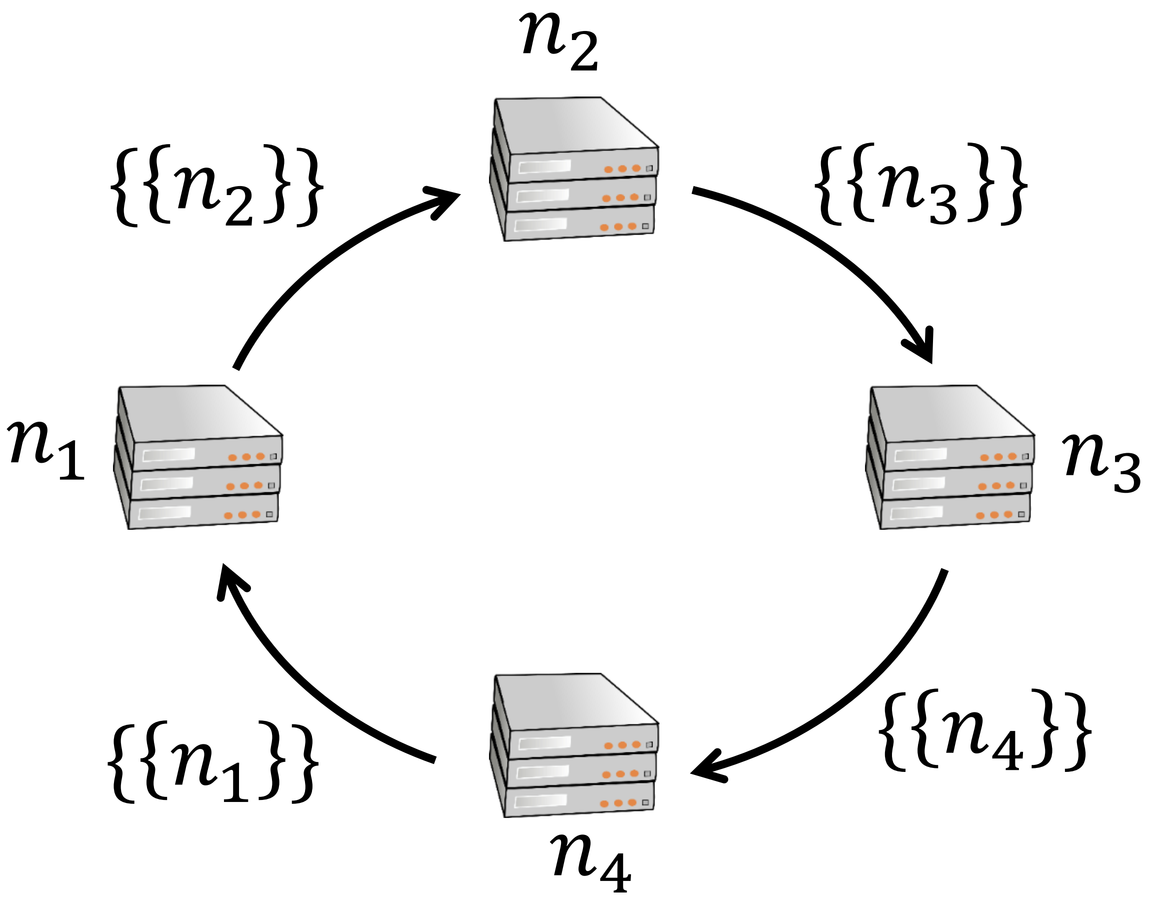
We will use quorums $\mathbb{Q}_n = \mathbb{S}_n$

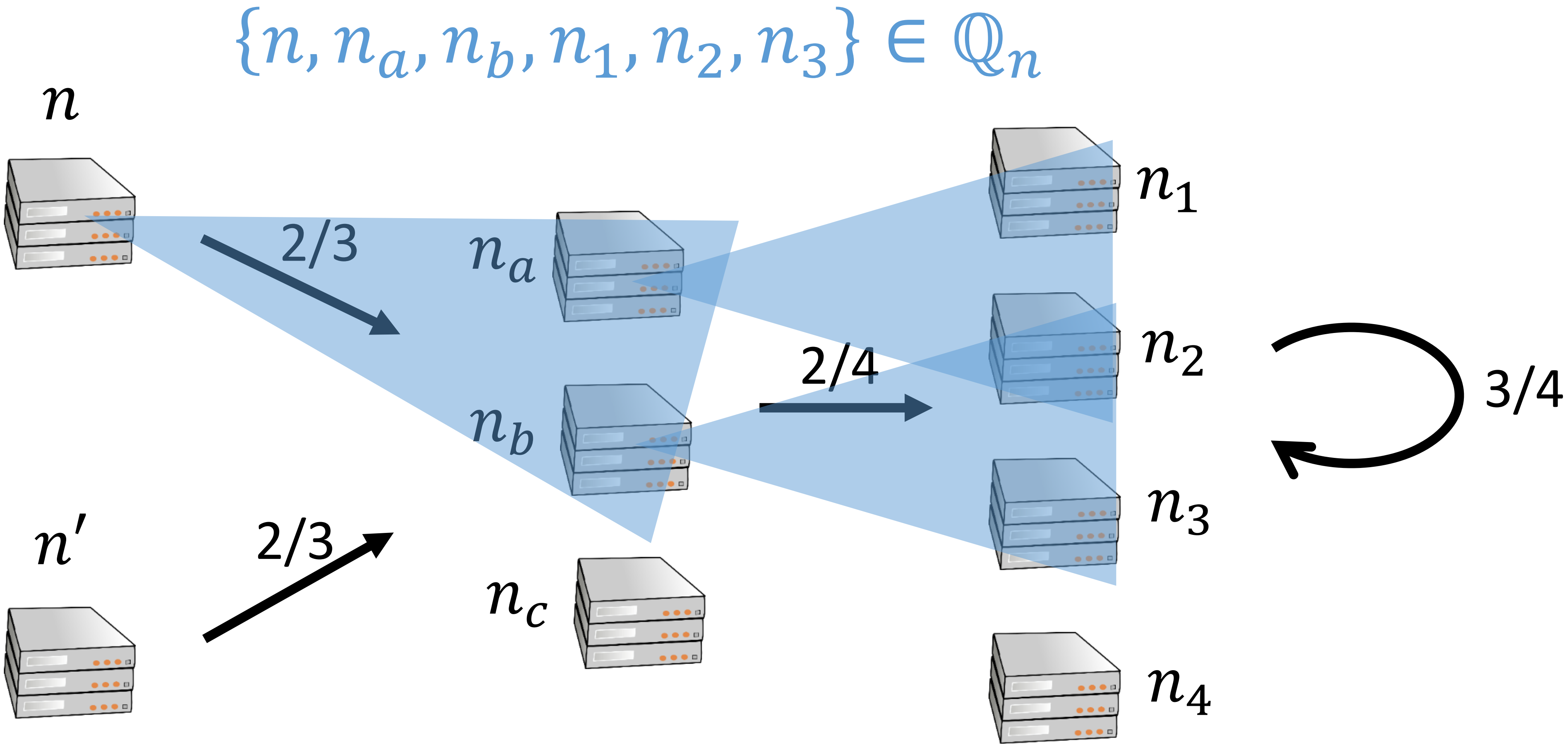
$\{\mathbb{SI}_n . n \in N\}$ determines $\mathbb{S}_n$ and $\mathbb{Q}_n$ for every node n

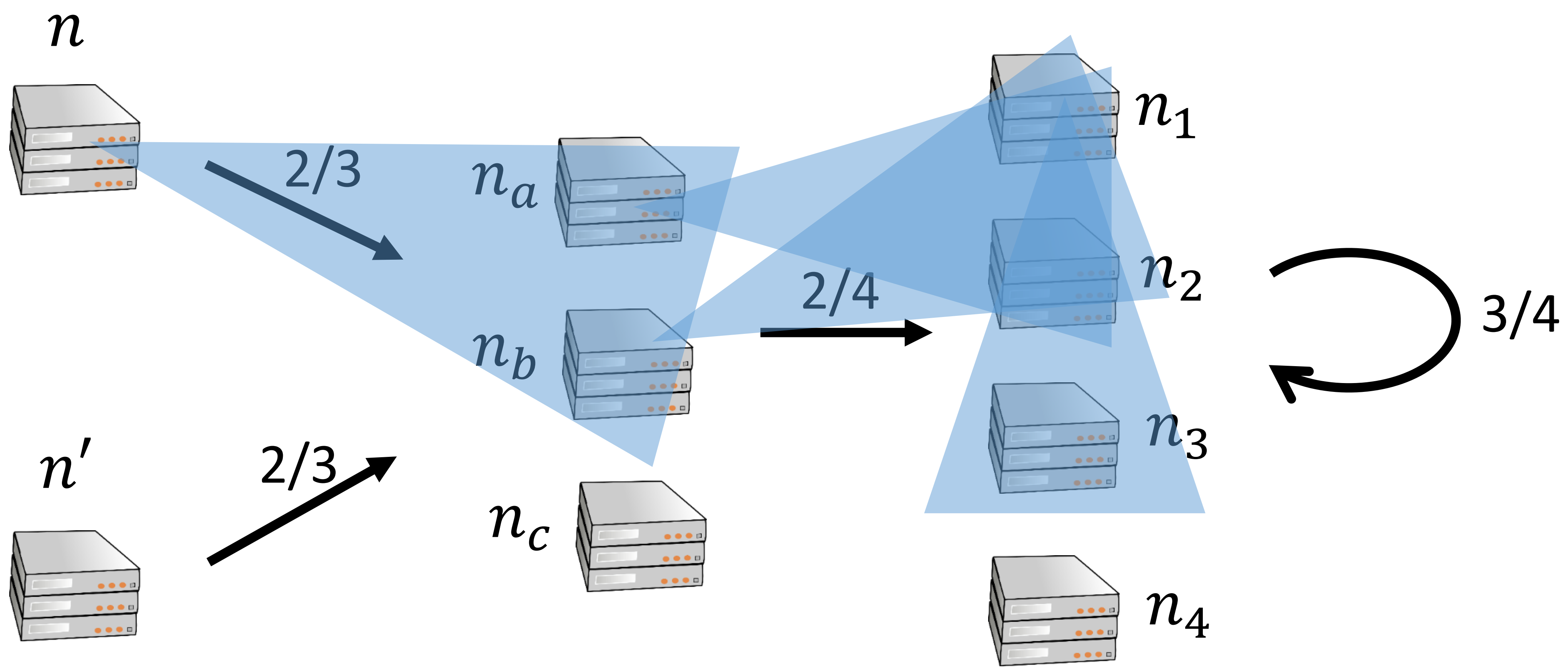
Each node has a unique singleton slice:
$\mathbb{SI}_i = \{\{i\%4 + 1\}\}$

Every node has the unique quorum:

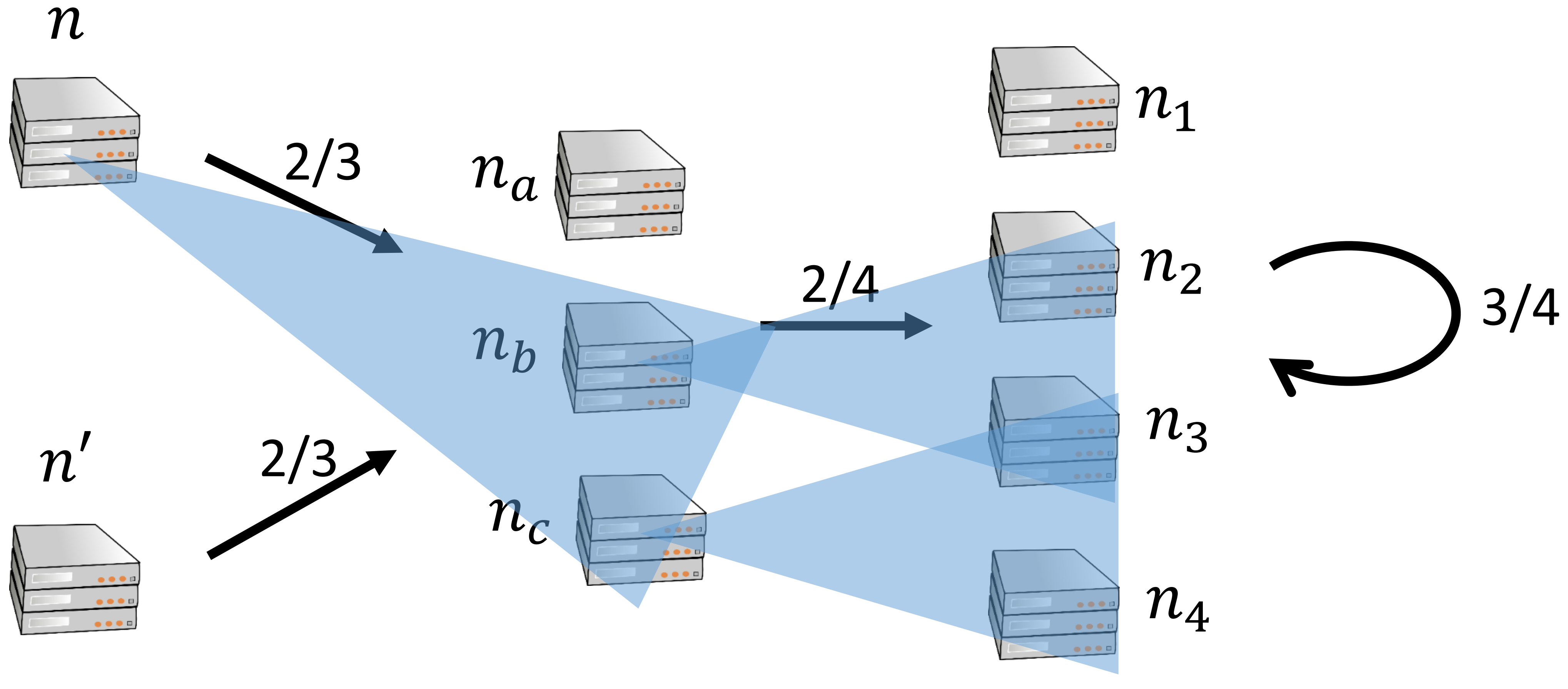
$\{n_1, n_2, n_3, n_4\}$



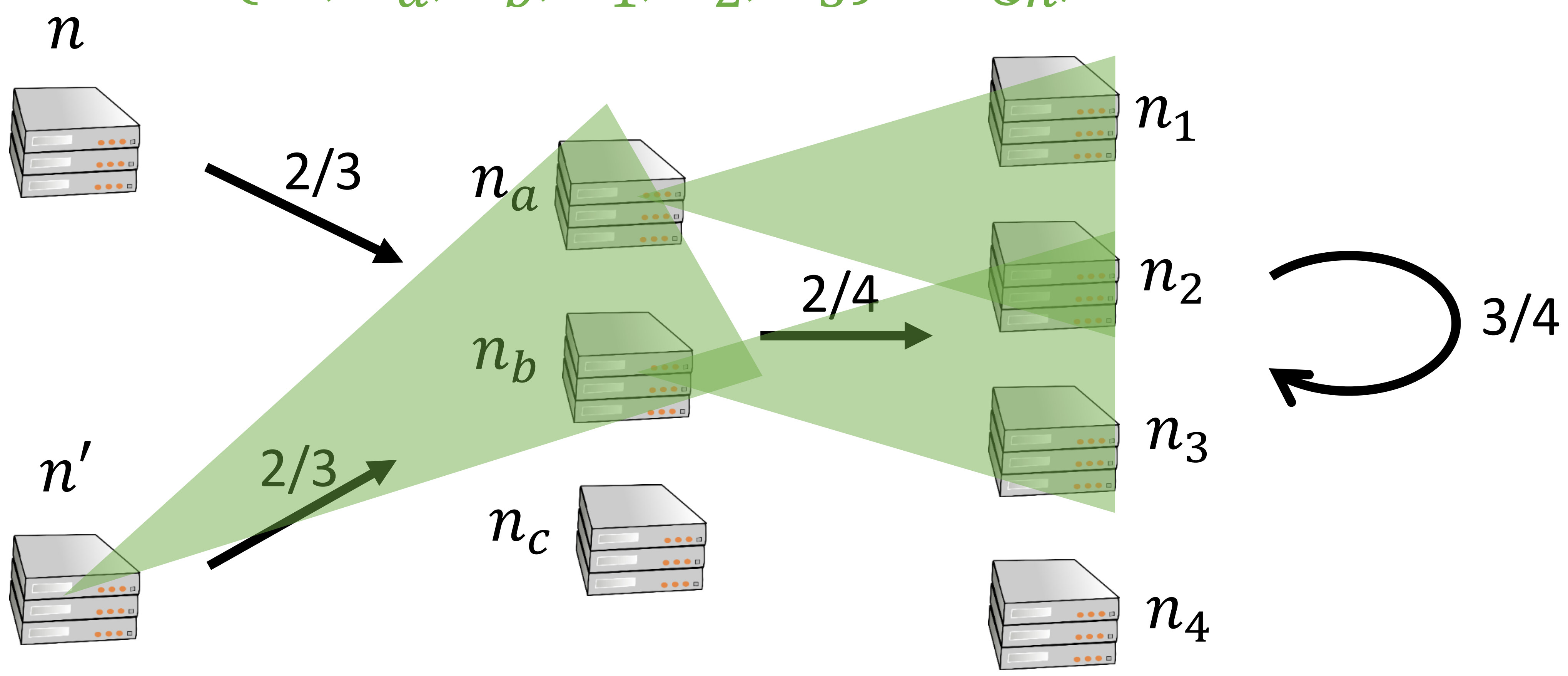

$\{n, n_a, n_b, n_1, n_2, n_3\} \in \mathbb{Q}_n$
n
n_a
n_b
n_c
n'
n_1
n_2
n_3
n_4
2/3
2/3
2/4
3/4

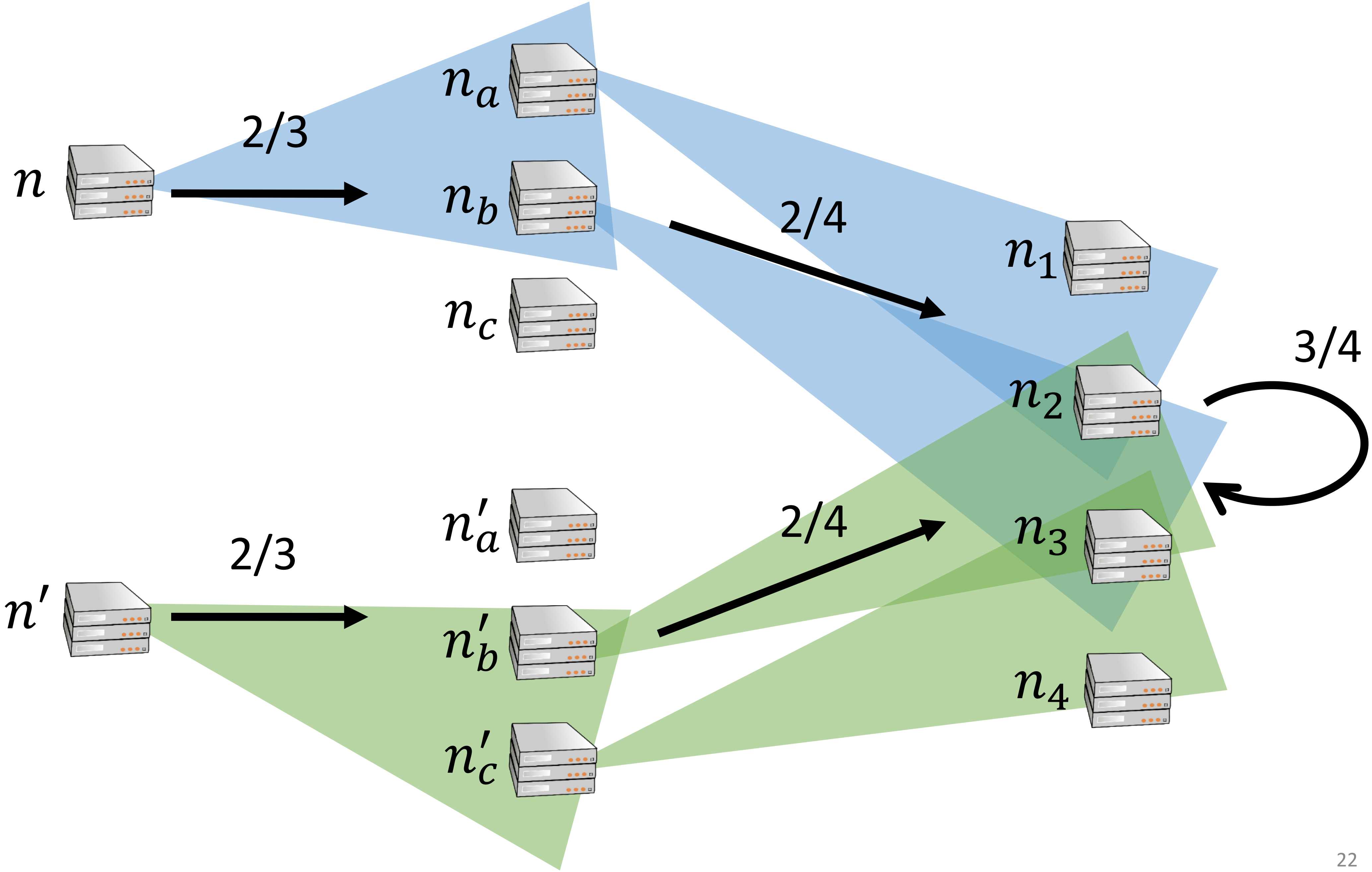

n
n_a
n_b
n_c
n'
2/3
2/3
2/4
n_1
n_2
n_3
n_4
3/4

$\{n, n_b, n_c, n_2, n_3, n_4\} \in \mathbb{Q}_n$



$$\{n', n_a, n_b, n_1, n_2, n_3\} \in \mathbb{Q}_{n'}$$

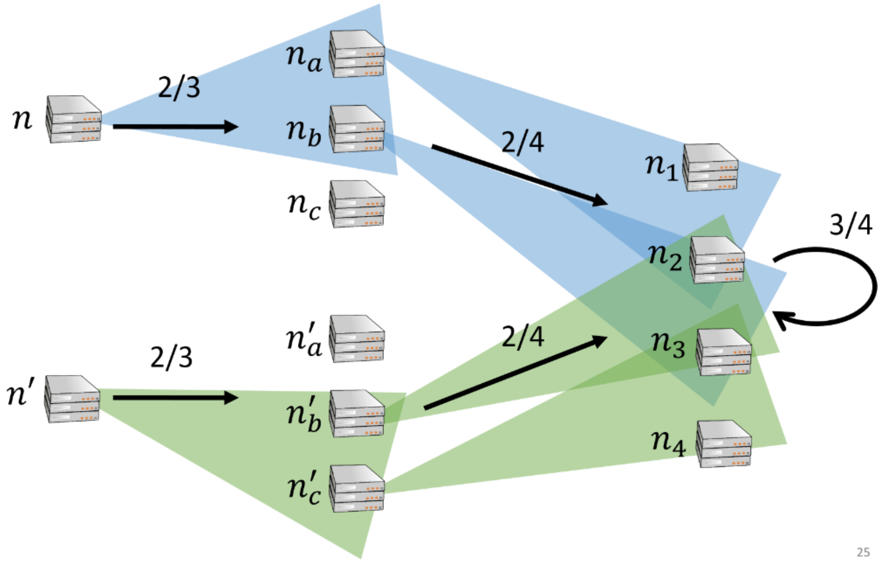




n
n_a
n_b
n_c
n'
n'_a
n'_b
n'_c
n_1
n_2
n_3
n_4
2/3
2/3
2/4
2/4
3/4

The Internet hypothesis: like the Internet, a global FBA system will be robustly connected

- Nodes make assumptions about failures and about other's assumptions ➔ we can obtain quorum intersection by transitivity
- Hypothesis: market/social forces will keep a global FBA system connected enough to ensure quorum intersection



In FBA, asymmetric quorums are generated collectively

- In the asymmetric model, each nodes picks its survivor sets and quorums
- In FBA, quorums and survivor sets emerge from slices
- The resulting quorum system nevertheless seems to be an asymmetric quorum system
- Algorithms for the asymmetric model should work, but…
  - Quorums are not given upfront, nodes have to compute their quorums

Malicious nodes can forge their slices and lie about them!

- Each node independently chooses its slices
- Quorums depend on the slices of their members

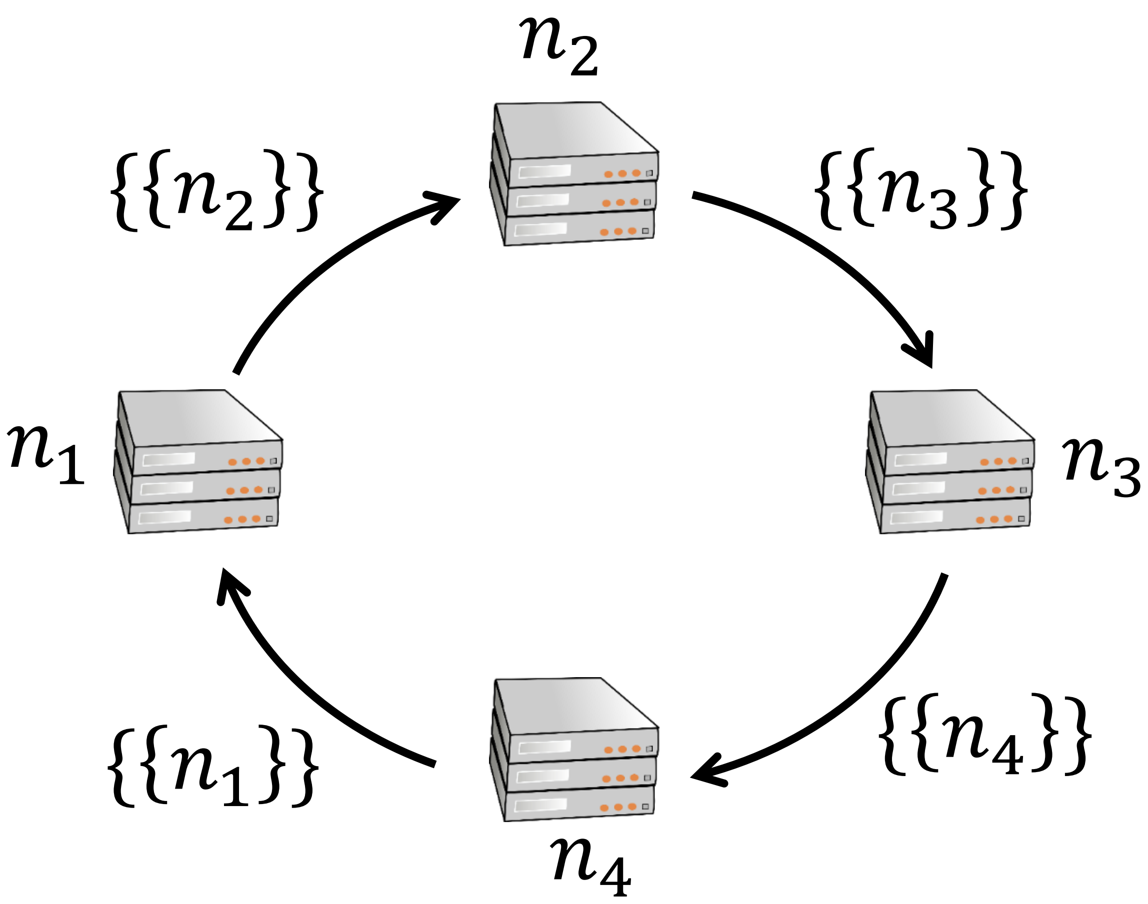
➔ Nodes need to know each other's slices

How do they learn each others' slices? By communicating

➔ Malicious nodes can lie about their slices

Without failures, every node has the unique quorum $\{n_1, n_2, n_3, n_4\}$

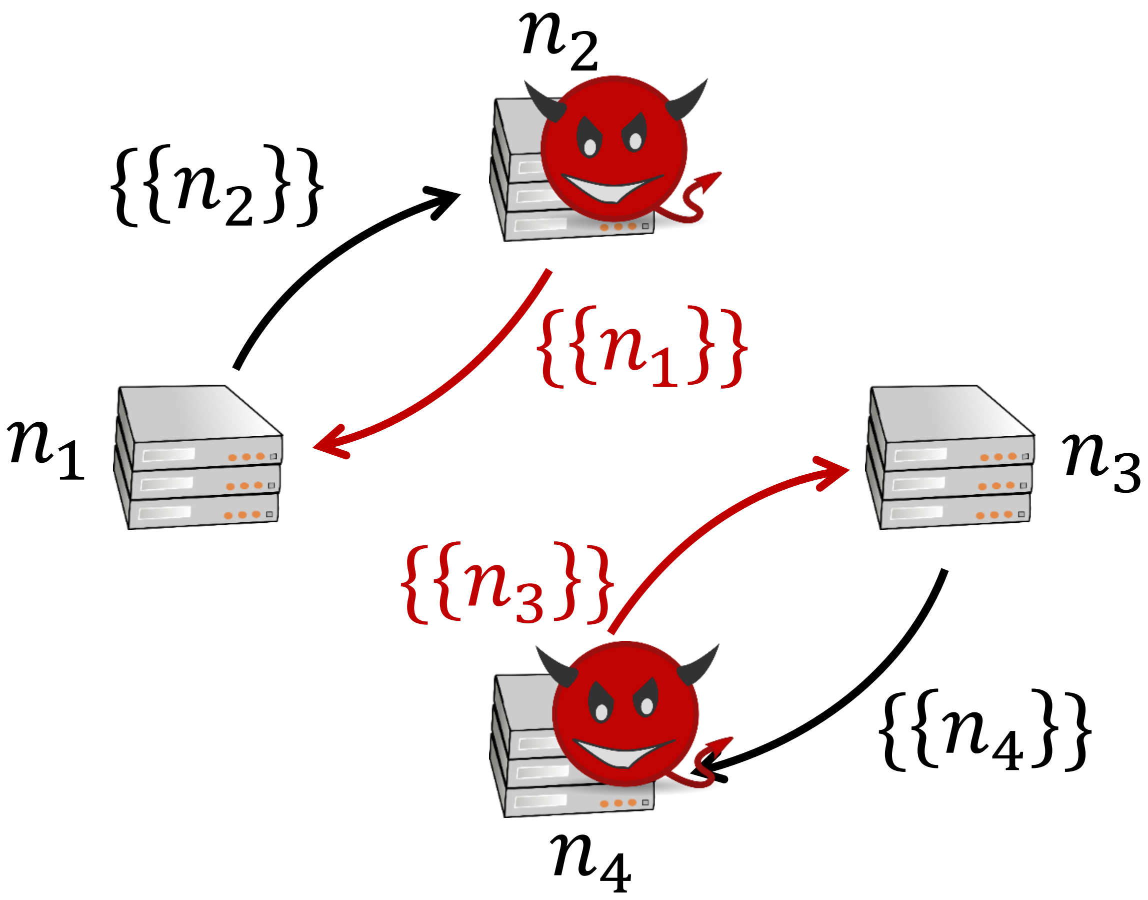
But, 2 failures compromise quorum intersection!

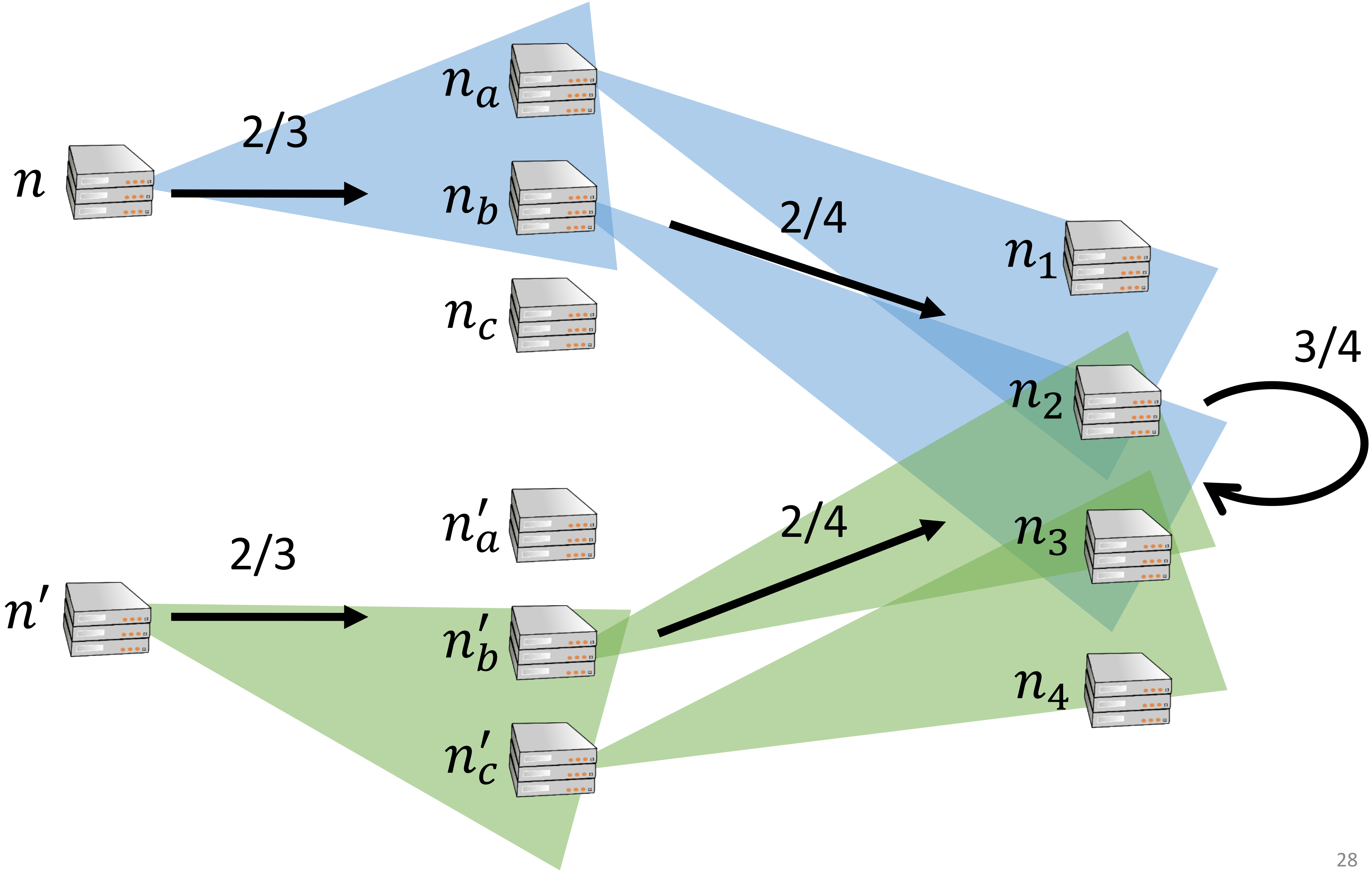


Without failures, every node has the unique quorum $\{n, n_2, n_3, n_4\}$

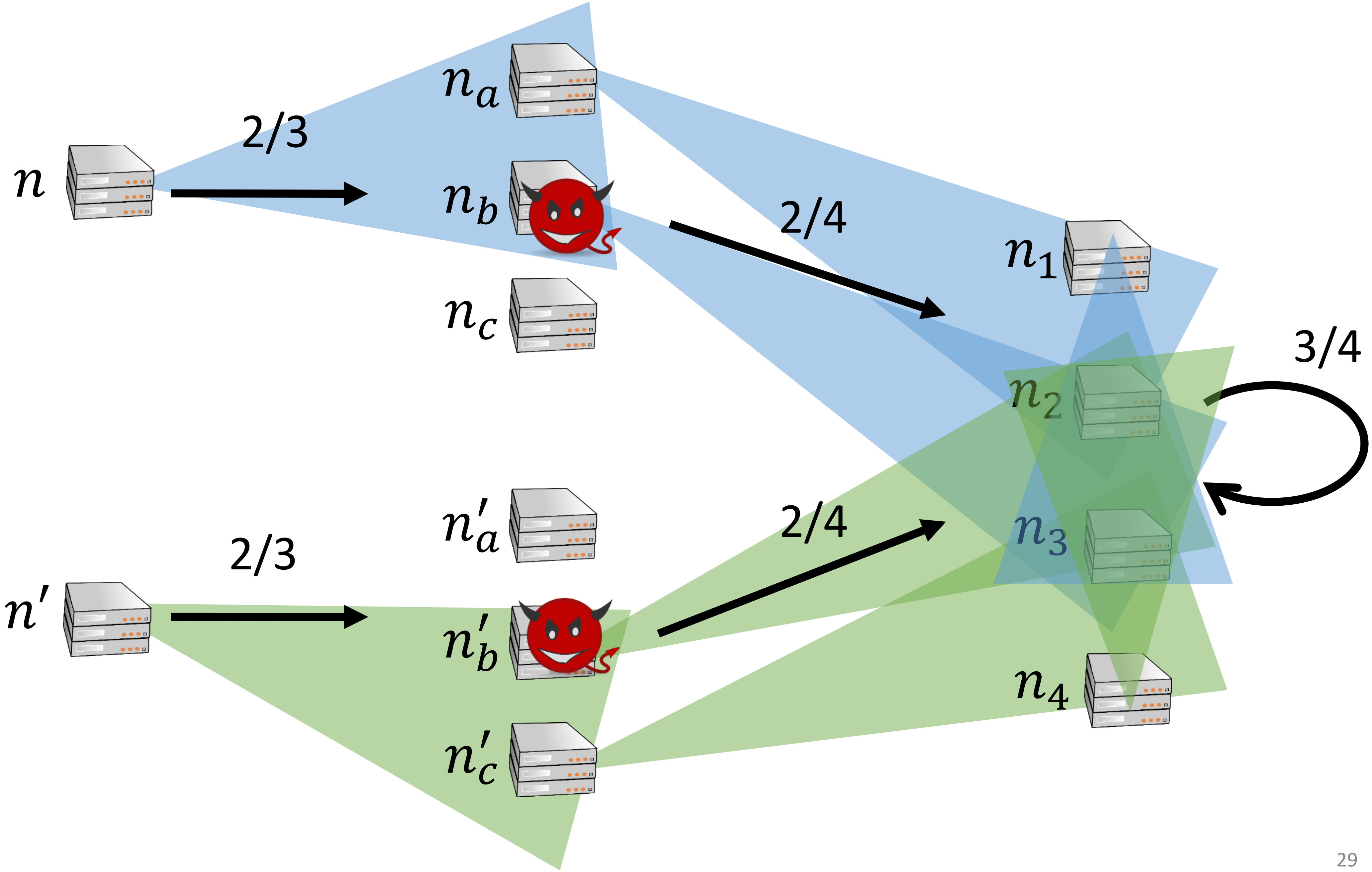
But, 2 failures compromise quorum intersection!

Now we have two disjoint quorums: $\{n_1, n_2\}$ and $\{n_3, n_4\}$

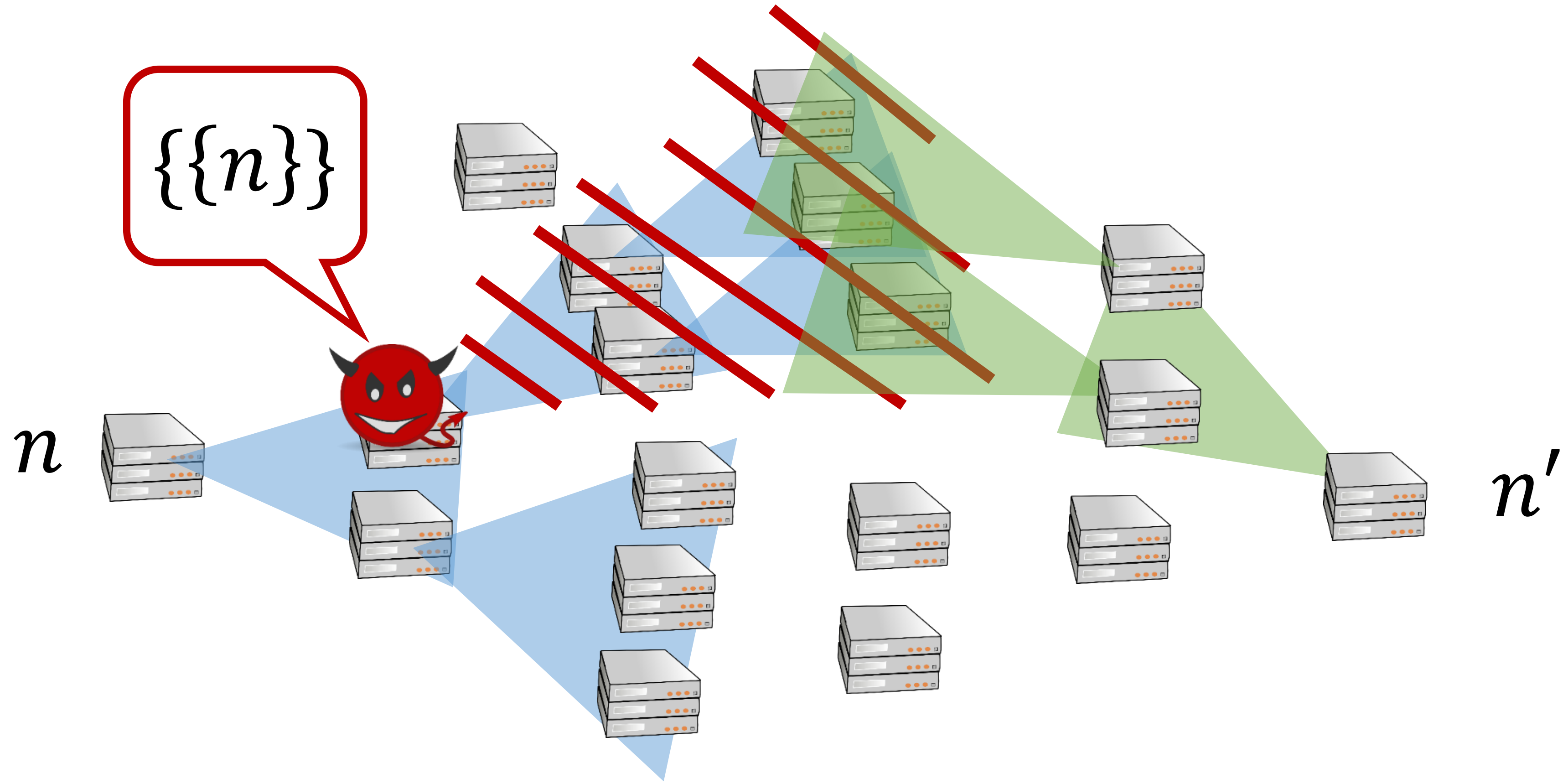




n
2/3
n_a
n_b
n_c
2/4
n_1
n_2
3/4
n_3
n_4
n'_a
2/3
n'
n'_b
2/4
n'_c


n
n'
2/3
2/3
n_a
n_b
n_c
n'_a
n'_b
n'_c
2/4
2/4
n_1
n_2
n_3
n_4
3/4

In the worst case, malicious nodes make quorums as small as possible



FBA enjoys the quorum-sharing property

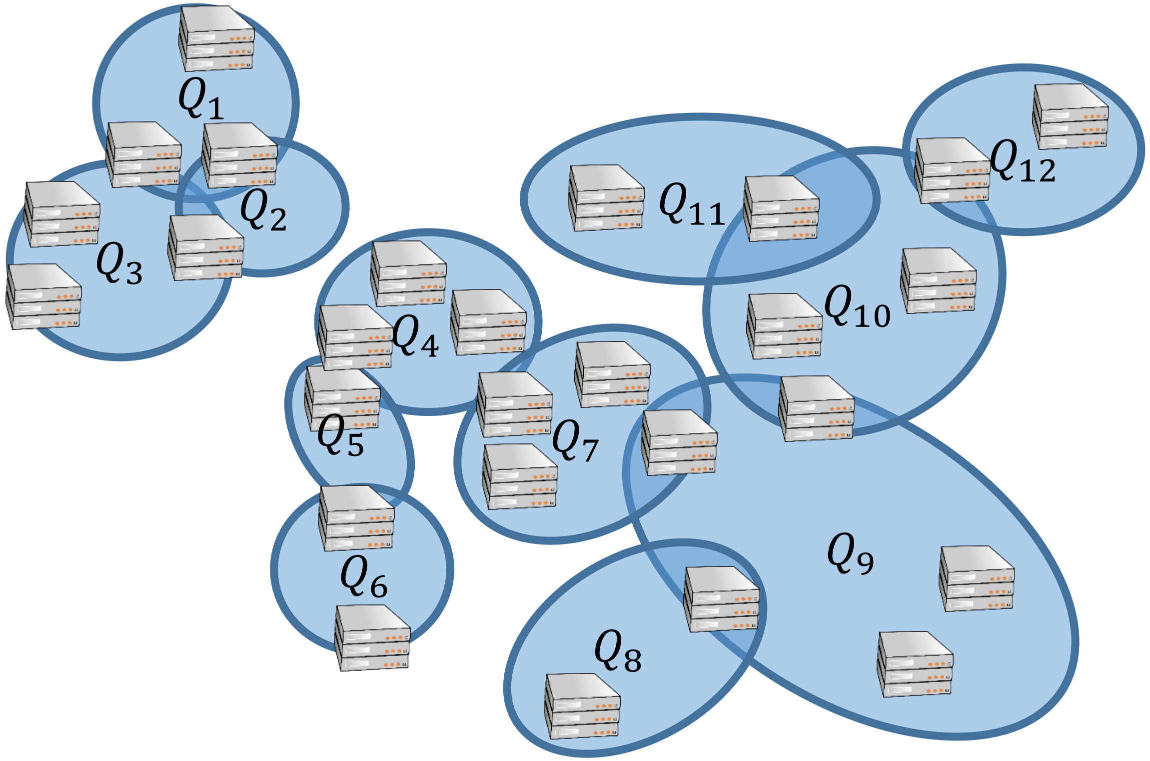
"A quorum is a quorum for all its members"

We can think of the system as just a set of quorums!

Remember Q is a quorum when:

a. $n \in Q$
b. every member of Q has a slice in Q

Also, if Q and Q' are quorums, then so is $Q \cup Q'$



A topology must satisfy 3 axioms

A *topology* is

- A set of points P (nodes)
- A set of open sets $Open \subseteq 2^P$ (quorums)

With axioms:

1. $\emptyset \in Open$ and $P \in Open$
2. If $X \subseteq Open$ then $\bigcup X \in Open$
3. If $O, O' \in Open$ then $O \cap O' \in Open$

But, the intersection of two quorums is usually not a quorum!

Semitopology is like topology but without the intersection axiom

A *semitopology* is

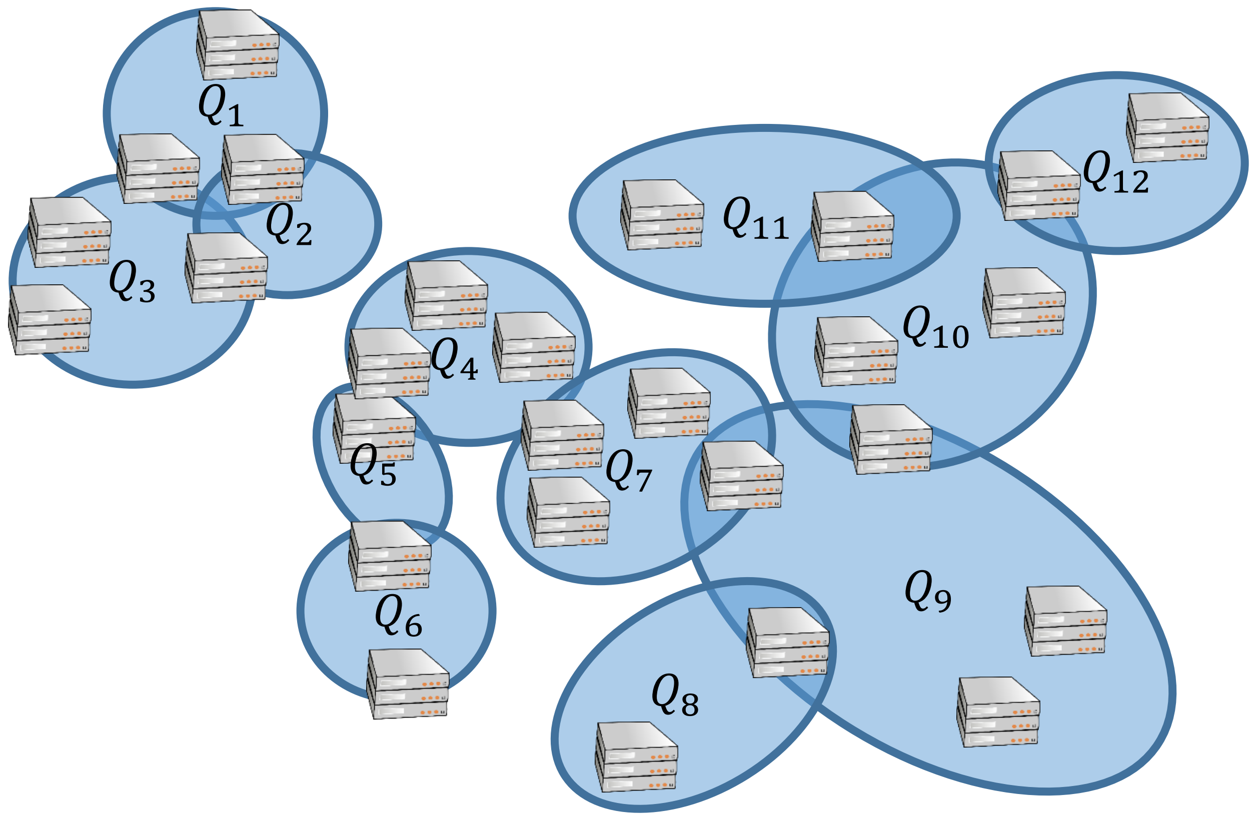
- A set of points P (nodes)
- A set of open sets $Open \subseteq 2^P$ (quorums)

With 2 axioms:

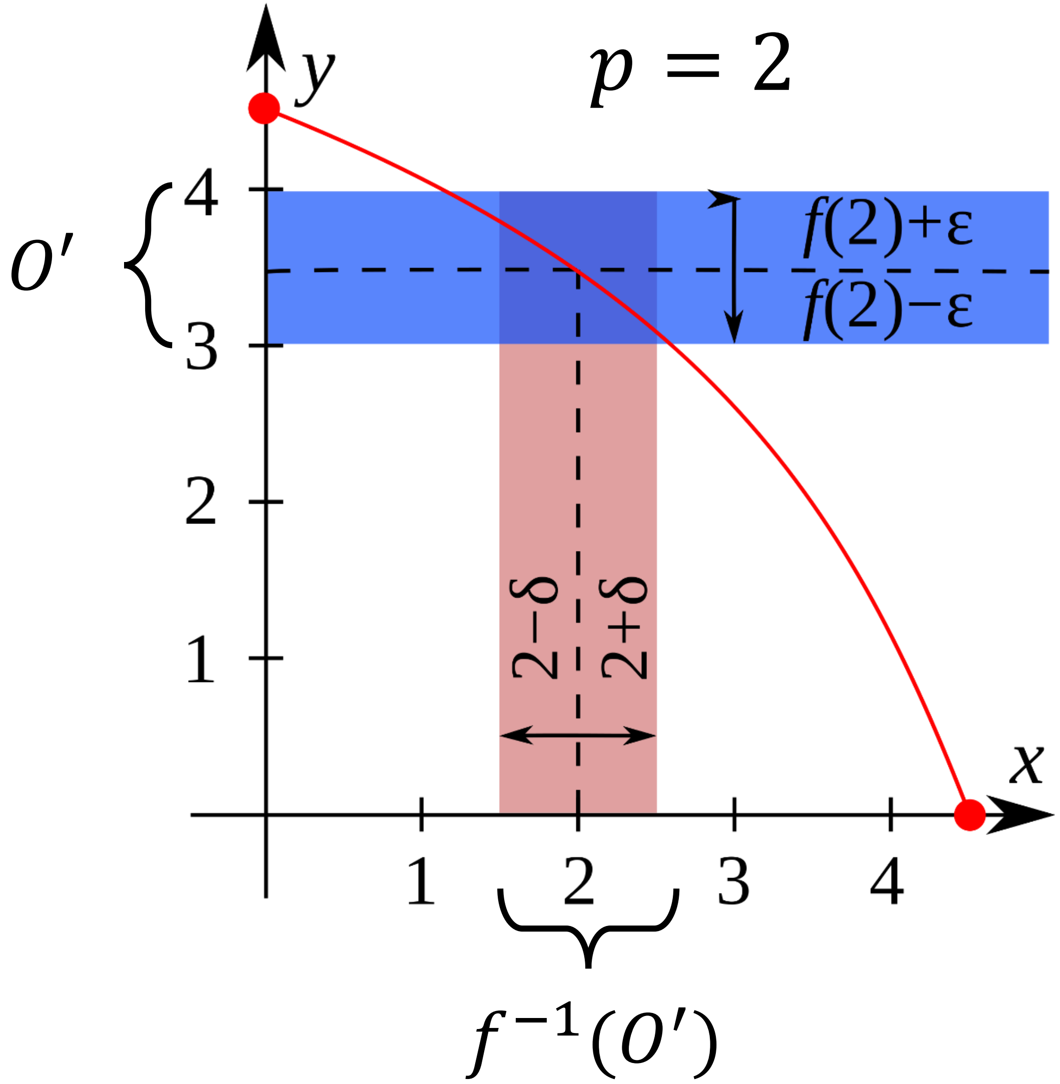
1. $\emptyset \in Open$ and $P \in Open$
2. If $X \subseteq Open$ then $\bigcup X \in Open$
3. ~~If $O, O' \in Open$ then $O \cap O' \in Open$~~

We can now turn to familiar topology notions to answer questions about FBA systems

Example: what does it mean to be in agreement?



Recall the definition of continuity at a point p



f is continuous at p when:
for every open neighborhood O' of $f(p)$,
$f^{-1}(O')$ contains an open neighborhood of p

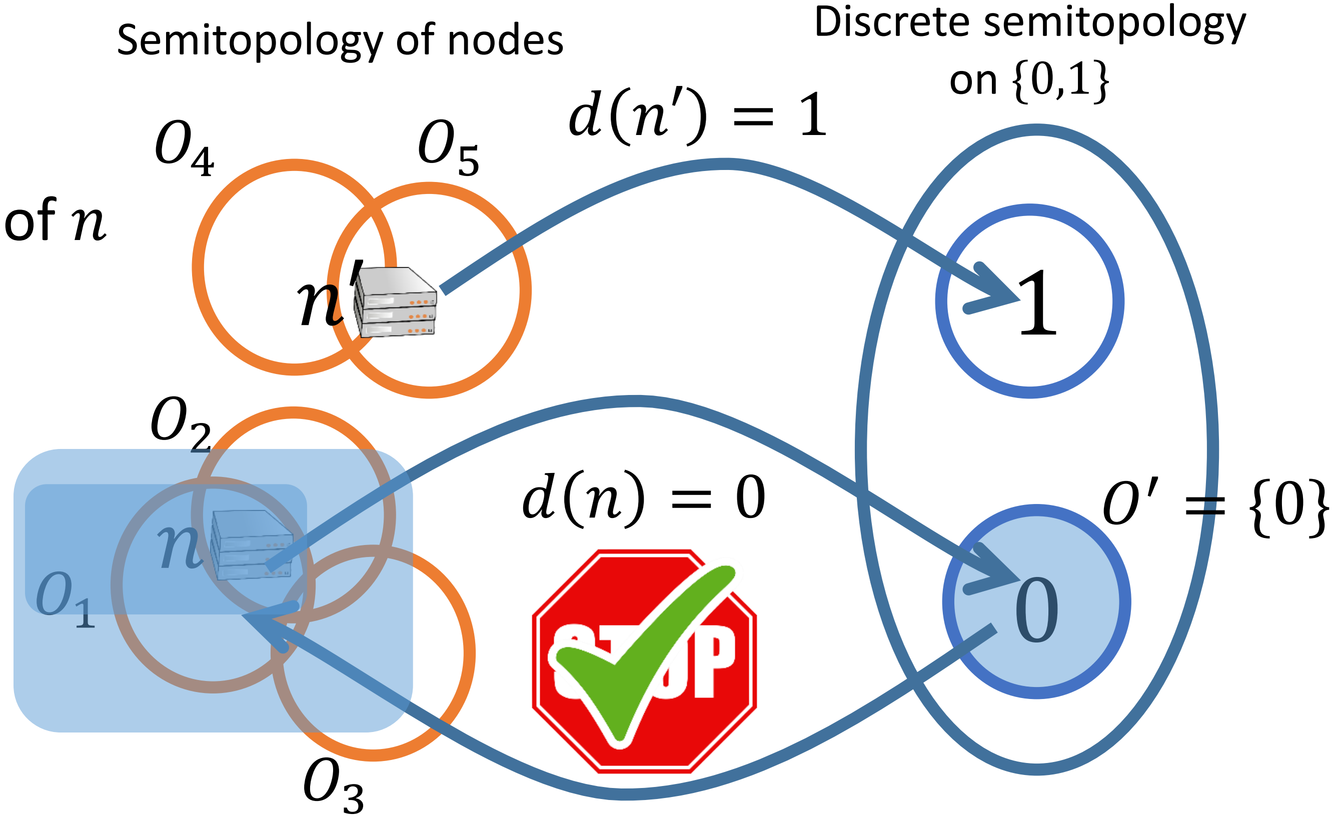
Take $p = 2$ and $O' = (3, 4)$

- $f(p) = 3.5 \in O'$
- $f^{-1}(O') = (1.5, 2.5)$ is open
- $2 \in f^{-1}(O')$

Agreement = continuity

d continuous at n when:
for every open neighborhood O' of d(n),
$d^{-1}(O')$ contains an open neighborhood of n

Translation:
"if n decides v then there is a quorum of n that decides v"



Semitopology: a new topological model of heterogeneous consensus

Murdoch J. Gabbay and Giuliano Losa

A distributed system is *permissionless* when participants can join and leave the network without permission from a central authority. Many modern distributed systems are naturally permissionless, in the sense that a central permissioning authority would defeat their design purpose: this includes blockchains, filesharing protocols, some voting systems, and more. By their permissionless nature, such systems are heterogeneous: participants may only have a partial view of the system, and they may also have different goals and beliefs. Thus, the traditional notion of consensus — i.e. system-wide agreement — may not be adequate, and we may need to generalise it.

This is a challenge: how should we understand what heterogeneous consensus is; what mathematical framework might this require; and how can we use this to build understanding and mathematical models of robust, effective, and secure permissionless systems in practice?

In this paper we offer a new definition of heterogeneous consensus, using *semitopology* as a framework. This is like topology, but without the restriction that intersections of opens be open.

Semitopologies have a rich theory which is related to topology, but with its own distinct character and mathematics. We introduce novel well-behavedness conditions, including an anti-Hausdorff property and a new notion of 'topen set', and we show how these structures relate to consensus. We give a restriction of semitopologies to *witness semitopologies*, which are an algorithmically tractable subclass corresponding to Horn clause theories, having particularly good mathematical properties. We introduce and study several other basic notions that are specific and novel to semitopologies, and study how known quantities in topology, such as dense subsets and closures, display interesting and useful new behaviour in this new semitopological context.

Additional Key Words and Phrases: Topology, Semitopology, Permissionless Network, Heterogeneous consens[...] programming

Contents

1 Intro[...]

We discover a zoo of semitopological structures

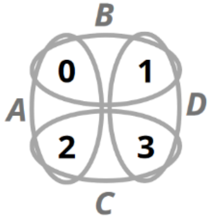


Fig. 3: Illustration of Example 4.2.1(3&4)

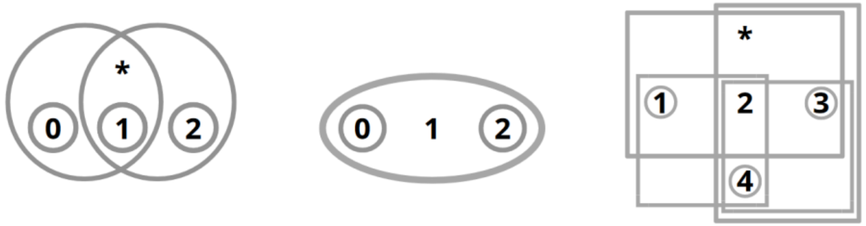


Fig. 5: Examples of boundary points (Example 6.2.3).

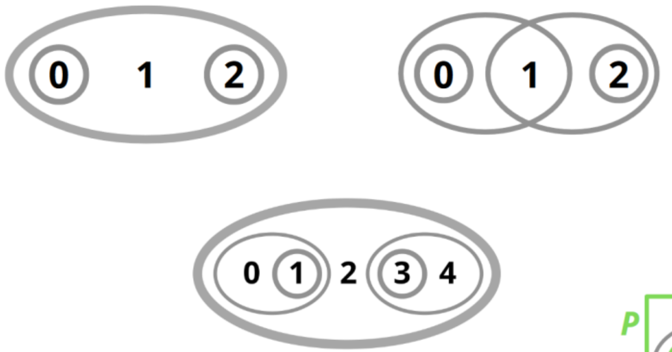


Fig. 1: Examples of topens (Example 3.3.3)

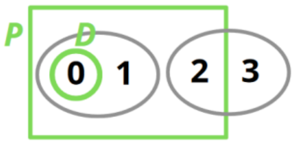


Fig. 10: The semitopologies in Example 10.3.3

(a) Regular boundary point of closed neighbourhood that is not intertwined with its interior (Lemma 6.3.11(2))

(b) Regular point in kissing set of closed neighbourhoods, not intertwined with interiors (Lemma 6.3.14(2))

Fig. 7: Two counterexamples

(a) A topen that is not strong (Lemma 3.7.2)

(b) A transitive set that is not strongly transitive (Lemma 3.7.4(2))

Fig. 2: Two counterexamples for (strong) transitivity

Fig. 9: Illustration of Example 10.1.3(3&4)

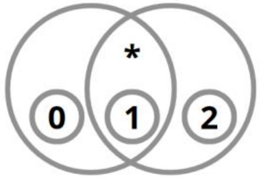


Fig. 8: Example 7.3.5: $|*| \subsetneq *_{\between} \subsetneq \{0,1,*\}$

A semitopology partitions itself into maximal transitive open sets (topens) plus one non-topen set

$Topen(T) \equiv$

1. T is open (is a quorum)
2. $O \between T \wedge T \between O' \Rightarrow O \between O'$ (T has quorum intersection)

Now show: $Topen(T) \wedge Topen(T') \wedge T \between T' \Rightarrow Topen(T \cup T')$

1. By the union axiom, $T \cup T'$ is open
2. Consider $O \between T$ and $T' \between O'$

$$\text{T' transitive; O, O' opens}\;\dfrac{\text{T transitive; O, T' open}\;\dfrac{O \between T \qquad T \between T'}{O \between T'} \qquad T' \between O'}{O \between O'}$$

Topens have useful closure properties

Recall, in topology, $|R|$ the closure of R is the set of points whose open neighborhoods all intersect R

If T is a topen, we have

1. $\forall O. O \in Open \wedge O \between T \Rightarrow T \subseteq |O|$
2. $\forall R. |R| \between T \Rightarrow R \between T$

Reliable broadcast implements all-or-nothing message broadcasting

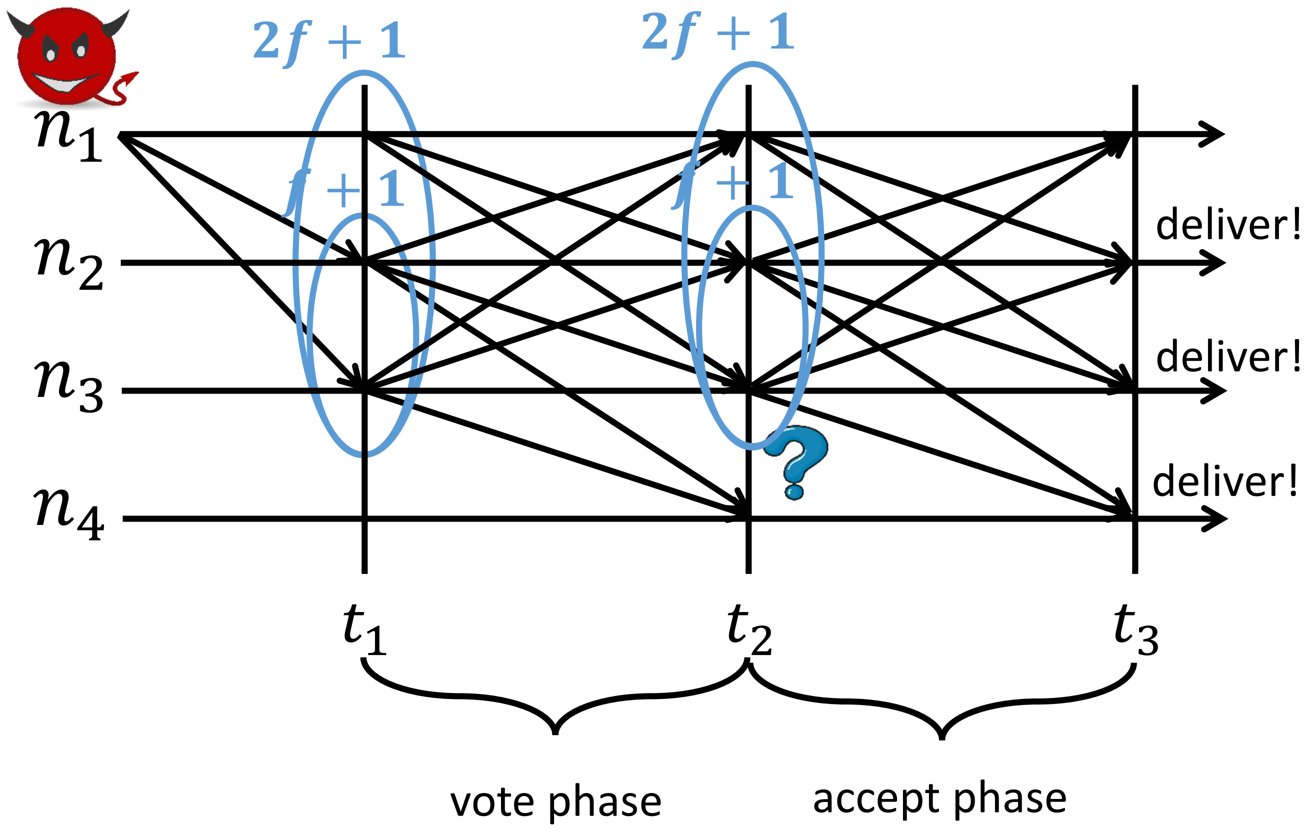
There is a designated sender and:

- If n and n' are well-behaved, n delivers message v if and only if n' delivers v
- If the sender is well-behaved, every node eventually delivers its message

Bracha broadcast implements reliable broadcast

The rules:

1. $announce(sender, \boldsymbol{v}) \Rightarrow vote(\boldsymbol{n}, \boldsymbol{v})$
2. $vote(\boldsymbol{2f+1}, \boldsymbol{v}) \Rightarrow accept(\boldsymbol{n}, \boldsymbol{v})$
3. $accept(\boldsymbol{f+1}, \boldsymbol{v}) \Rightarrow accept(\boldsymbol{n}, \boldsymbol{v})$
4. $accept(\boldsymbol{2f+1}, \boldsymbol{v}) \Rightarrow deliver(\boldsymbol{n}, \boldsymbol{v})$



Bracha broadcast relies on 4 properties

The rules:

1. $announce(sender, \boldsymbol{v}) \Rightarrow vote(\boldsymbol{n}, \boldsymbol{v})$
2. $vote(\boldsymbol{2f} + \boldsymbol{1}, \boldsymbol{v}) \Rightarrow accept(\boldsymbol{n}, \boldsymbol{v})$
3. $accept(\boldsymbol{f} + \boldsymbol{1}, \boldsymbol{v}) \Rightarrow accept(\boldsymbol{n}, \boldsymbol{v})$
4. $accept(\boldsymbol{2f} + \boldsymbol{1}, \boldsymbol{v}) \Rightarrow deliver(\boldsymbol{n}, \boldsymbol{v})$

Sufficient properties:

P-1: There are 2f+1 well-behaved nodes

P-2: Every two set of 2f+1 have a well-behaved member in common

P-3: Every set of 2f+1 includes f+1 well-behaved nodes

P-4: There is one well-behave node among f+1

P-3?: $\forall O.\, O \in Open \wedge O \between T \Rightarrow T \subseteq |O|$
P-4:? $\forall R.\, |R| \between T \Rightarrow R \between T$

Topological closure generalizes blocking sets

Classic threshold quorum system

- $3f + 1$ nodes; f may fail
- quorum threshold is $2f + 1$
- blocking set threshold is $f + 1$

Semitopology

- semitopology with topen T that does not fail
- the quorums are the opens
- R blocks n when $n \in |R|$

Bracha broadcast in a semitopology

The rules:

1. $announce(sender, \boldsymbol{v}) \Rightarrow vote(\boldsymbol{n}, \boldsymbol{v})$
2. $vote(\boldsymbol{Q}, \boldsymbol{v}) \Rightarrow accept(\boldsymbol{n}, \boldsymbol{v})$
3. $accept(\boldsymbol{R}, \boldsymbol{v}) \wedge n \in |\boldsymbol{R}| \Rightarrow accept(\boldsymbol{n}, \boldsymbol{v})$
4. $accept(\boldsymbol{Q}, \boldsymbol{v}) \Rightarrow deliver(\boldsymbol{n}, \boldsymbol{v})$

Sufficient properties:

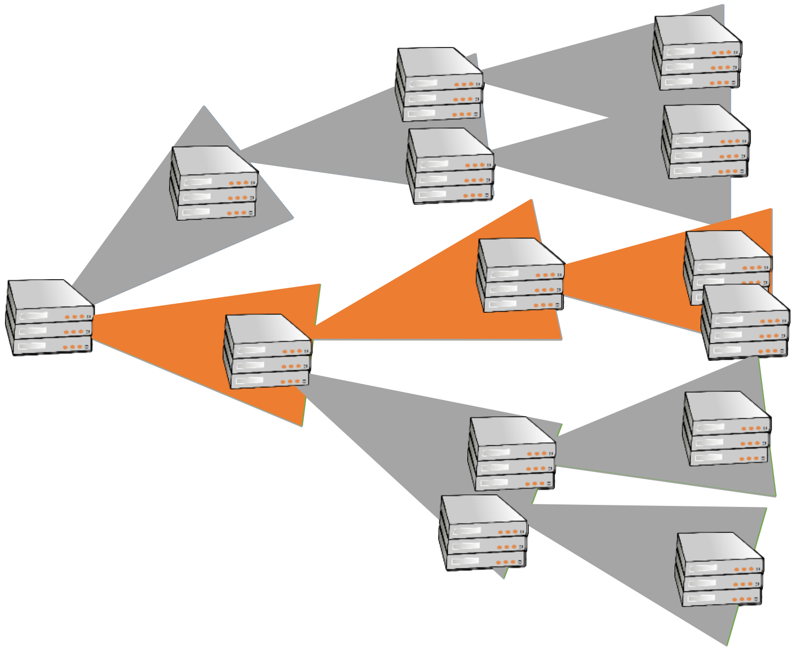
P-1: T *is an open*

P-2: T *is transitive*

P-3: $\forall O.\, O \in Open \wedge O \between T \Rightarrow T \subseteq |O|$

P-4: $\forall R.\, |R| \between T \Rightarrow R \between T$

We can compute closures using a distributed algorithm



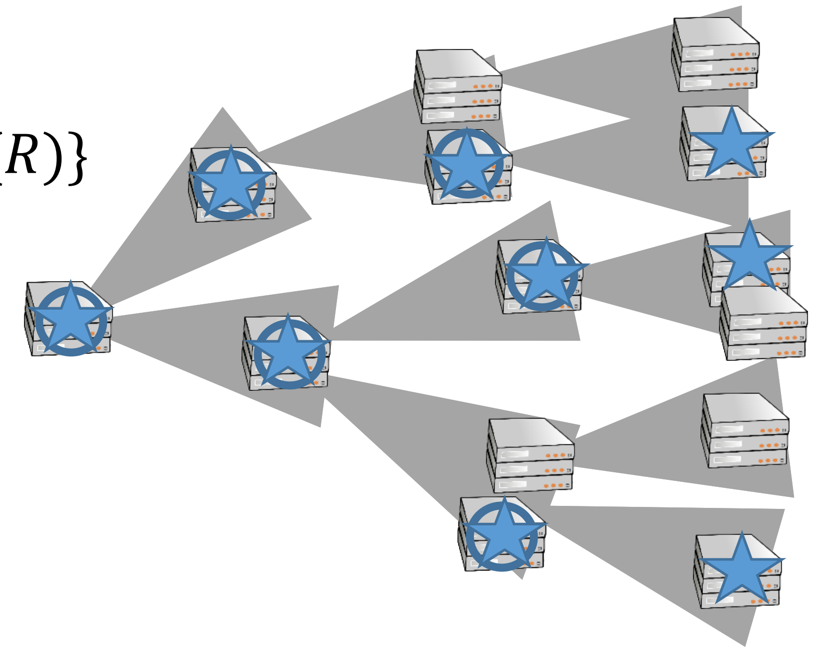
We can compute closures using a distributed algorithm

Define $\lim(R) = \bigcup_{i\geq 0} lim_i(R)$ where:

- $lim_0(R) = R$
- $lim_{i+1}(R) = lim_i(R) \cup \{n \,.\, \forall S \in \mathbb{SI}_n . S \between lim_i(R)\}$

Theorem:

$$|R| = \lim(R)$$



Consensus in FBA: quorum certificates do not work

- In algorithms like PBFT, nodes can prove to each other that a quorum Q is in a given state by exhibiting a *quorum certificate*, i.e. signed messages from the members of Q
- This is not very useful in FBA because the notion of quorum is not shared by everyone
- Solving consensus in FBA is reminiscent of solving consensus in the unauthenticated Byzantine model

Paxos solves consensus in an eventually synchronous crash-stop quorum system

In the consensus problem, nodes start with private inputs and must eventually agree on a common output among the inputs.

Node's outputs are called decisions

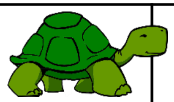
Paxos solves consensus in an eventually synchronous crash-stop quorum system

- Nodes execute a sequence of rounds 1,2,3… To simplify, we assume synchronous rounds where each nodes hears from at least a quorum in each round
- Each round has a unique pre-determined leader
- The leader proposes a value and nodes vote for the leader’s value
- Any value voted for by a quorum in a given round is decided
- The leader must only propose *safe values*, i.e. values that do not contradict any decision in a previous round

We represent an execution as a table

	Round 1	Round 2	Round 3	Round 4	Round 5
n_1		W	V		V
n_2	V		V		V
n_3					V

A leader proposes the value voted for in the highest round before the current round

	Round 1	Round 2	Round 3	Round 4	Round 5
n_1			V 		
n_2	V		V		
n_3		W			

 ➔ V

Inductively, all previous values are safe for the rounds in which they appear ➔ any previous decision must be equal to the value of the highest round

With malicious nodes, we cannot trust leaders or what nodes report

- Nodes and leaders need to double-check that value are safe
- For liveness, a leader must make sure that the value it proposes will be deemed safe by the nodes
- Quorum certificates do not work

Unauthenticated Paxos:

- 4 voting phases per round
- Decision if quorum in the last phase of a round

	Round 1				Round 2				Round 3			
	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4
n_1	V		V		W		W	W				
n_2	V	V	V	V		W	W	W				
n_3	V	V	V	V	W	W	W					
n_4		V			W	W		W				

Decision in round 2!

A value is safe if supported by $f + 1$ in the previous phase

	Round 1				Round 2				? → W Round 3			
	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4
n_1	V		V		W		W					
n_2	V	V	V	V		W	W					
n_3	V	V	V	V	W	W	W	W				
n_4		V			W	W	$f+1$					

- Nodes redo the leader's check for themselves
- The leader must not miss a value seen by other nodes, so it uses phase-3 values

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4
n_1	V				W			W?				
n_2	V	V	V			W						
n_3	V	V			W	W						
n_4		V			W	W						

Round 1 Round 2 ? → V Round 3

- Nodes redo the leader's check for themselves
- The leader must not miss a value seen by other nodes, so it uses phase-3 values

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4
n_1	V				W		W	W?				
n_2	V	V	V			W	W					
n_3	V	V			W	W	W					
n_4		V			W	W						

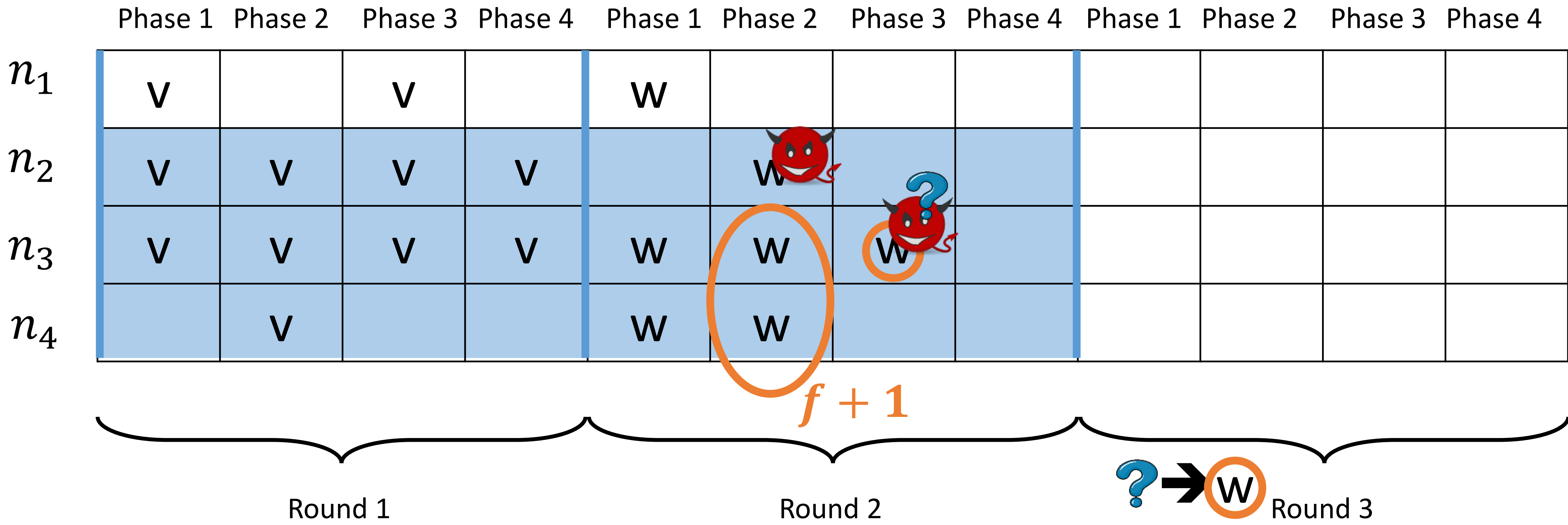
Round 1 — Round 2 — ? → W Round 3

We use phases 3 and 4 for the "highest-value" rule

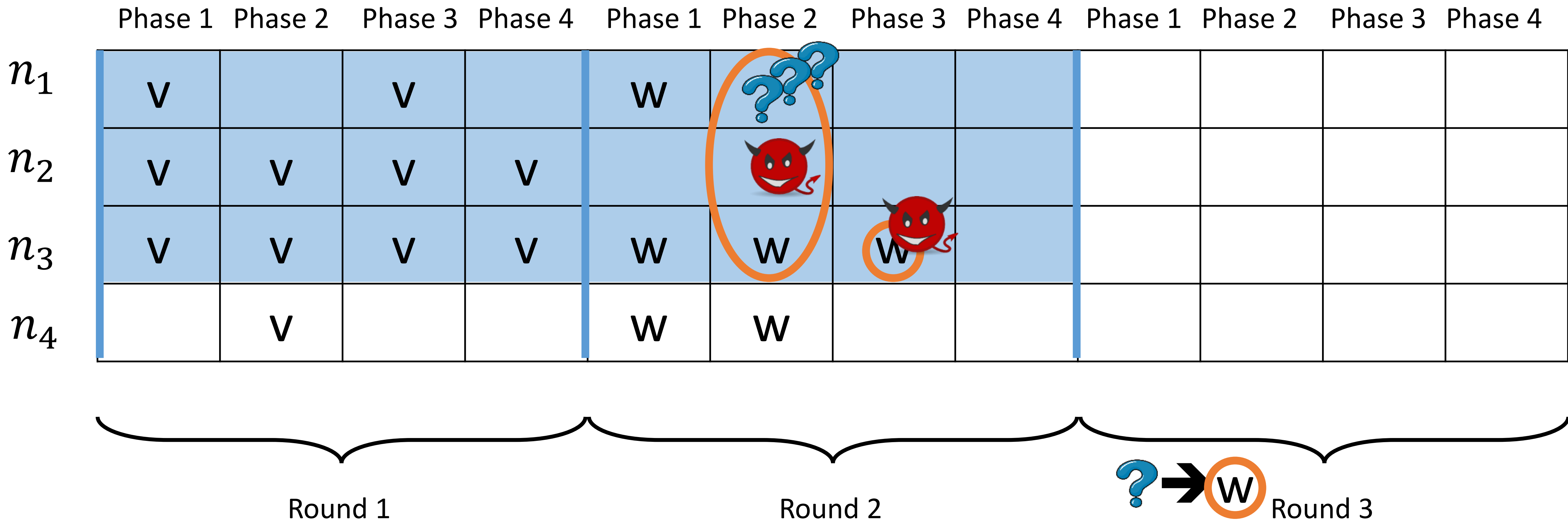
	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4	Phase 1	Phase 2	Phase 3	Phase 4
n_1	V		V		W		W					
n_2	V	V	V	V		W	W					
n_3	V	V	V	V	W	W	W	W				
n_4		V			W	W						
	Round 1				Round 2				Round 3			

 → W Round 3

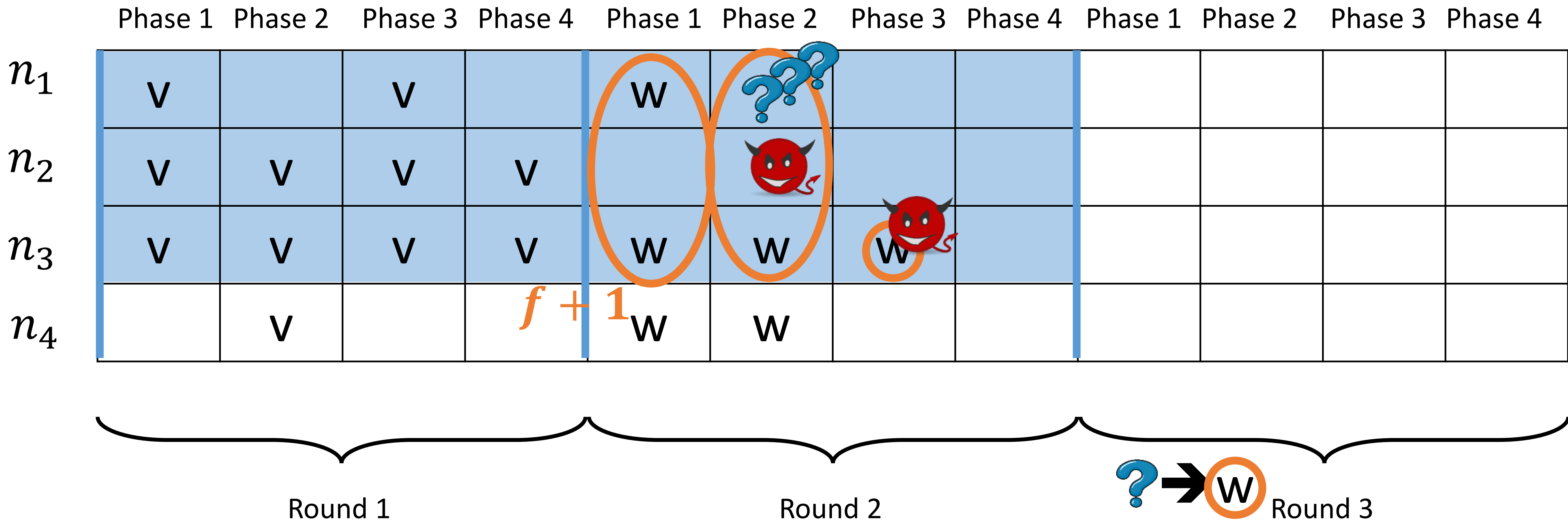
- We use phases 3 and 4 for the "highest-value" rule
- We use phases 1 and 2 to check for safety: a value is safe if supported by $f + 1$ in the previous phase



- We use phases 3 and 4 for the “highest-value” rule
- We use phases 1 and 2 to check for safety: a value is safe if supported by $f + 1$ in the previous phase



- We use phases 3 and 4 for the "highest-value" rule
- We use phases 1 and 2 to check for safety: a value is safe if supported by $f+1$ in the previous phase



Unauthenticated Byzantine Paxos is like Paxos, but:

There are 4 voting phases per round instead of 1

Leaders use highest phase-3 value and check safety with phase 2

Nodes use highest phase-4 value and check safety with phase 1

Conclusion

The Federated Byzantine Agreement model allows constructing quorum systems in permissionless networks, without proof-of-stake

Quorums in a FBA system are local and form a semitopology, which is a new mathematical object with rich structure and explanatory power

Solving consensus in an FBA system is reminiscent of solving consensus in the unauthenticated BFT model

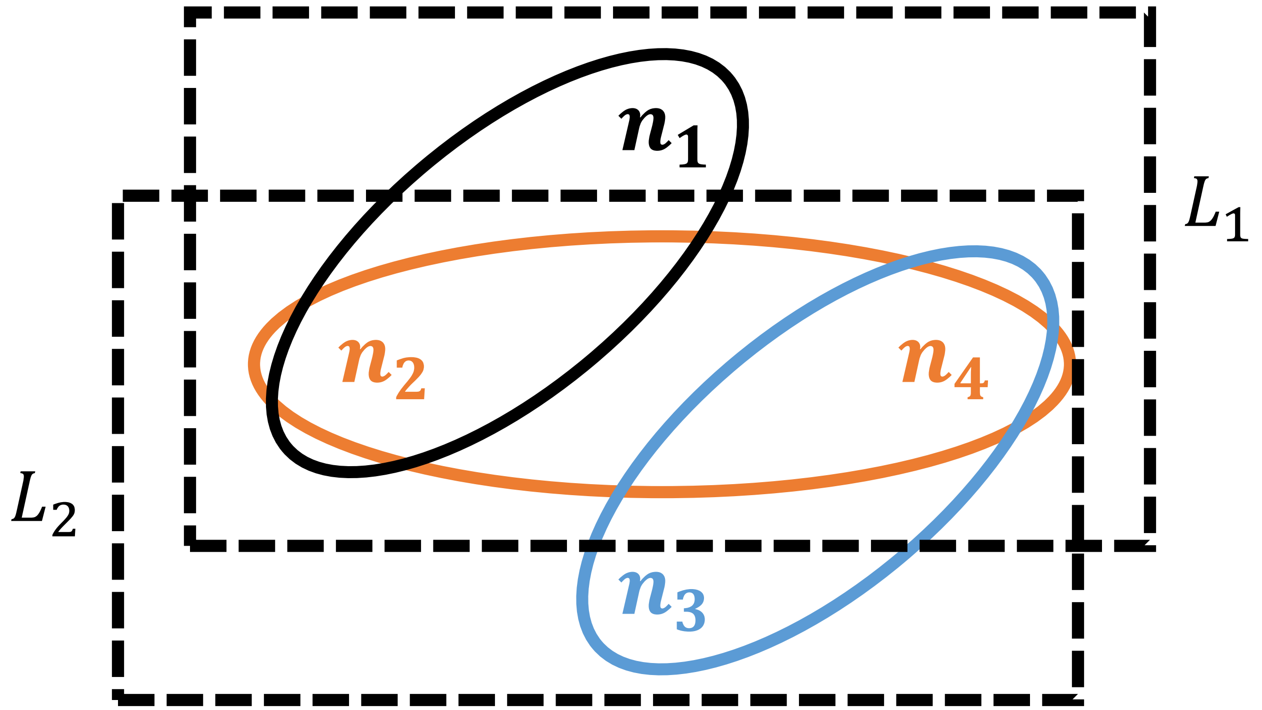
Open problems:

- Leader election
- Sybil-resistant P2P overlays for FBA
- Cryptography in the FBA model

References:

- Semitopology: a new topological model of heterogeneous consensus, arXiv
- Quorum systems in permissionless networks, OPODIS 2022
- Fast and secure global payments with Stellar, SOSP 2019
- Stellar consensus by instantiation, DISC 2019
- The Stellar whitepaper

Non-closure property of leagues in the asymmetric model



$$L_1 = \{n_1, n_2, n_4\}$$
$$L_2 = \{n_2, n_3, n_4\}$$

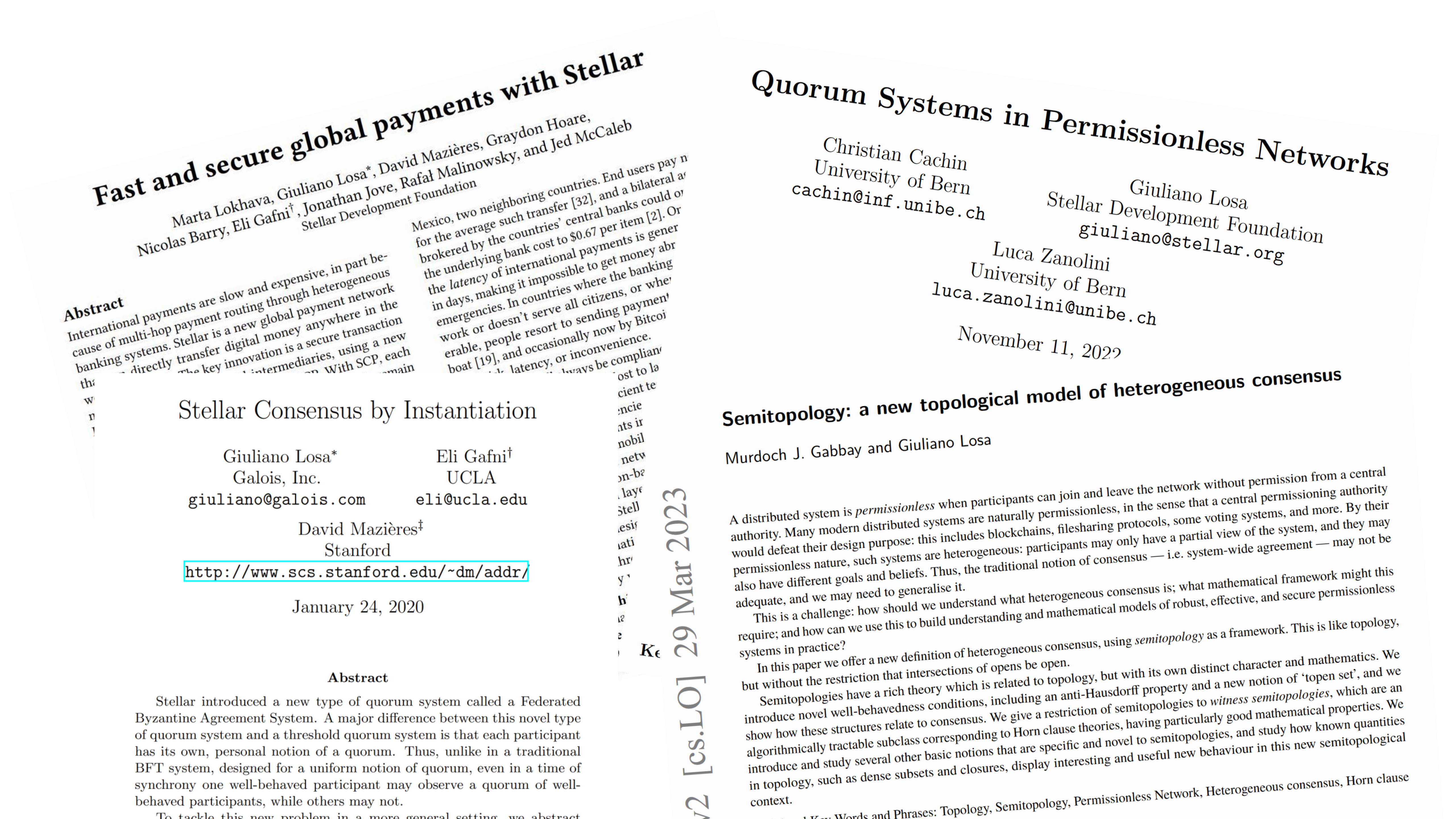
Classic $2/3$rd threshold quorum systems are an instance of FBA

Give every node p the set of slices:

$$\mathbb{S}_p = \{S \in 2^P : 3|S| = 2|P|\}$$

We obtain a classic BFT quorum system where every node p has the set of survivor-sets/quorums:

$$\mathbb{Q}_p = \{Q \in 2^P : 3|Q| \geq 2|P|\}$$



Fast and secure global payments with Stellar

Marta Lokhava, Giuliano Losa*, David Mazières, Graydon Hoare,
Nicolas Barry, Eli Gafni†, Jonathan Jove, Rafał Malinowsky, and Jed McCaleb
Stellar Development Foundation

Abstract

International payments are slow and expensive, in part because of multi-hop payment routing through heterogeneous banking systems. Stellar is a new global payment network ... directly transfer digital money anywhere in the ... The key innovation is a secure transaction ... intermediaries, using a new ... With SCP, each ...

Mexico, two neighboring countries. End users pay ... for the average such transfer [32], and a bilateral ... brokered by the countries' central banks could ... the underlying bank cost to $0.67 per item [2]. Or ... the *latency* of international payments is gener... in days, making it impossible to get money abr... emergencies. In countries where the banking ... work or doesn't serve all citizens, or whe... erable, people resort to sending payment... boat [19], and occasionally now by Bitcoi... latency, or inconvenience. ... always be complian...

Quorum Systems in Permissionless Networks

Christian Cachin
University of Bern
cachin@inf.unibe.ch

Giuliano Losa
Stellar Development Foundation
giuliano@stellar.org

Luca Zanolini
University of Bern
luca.zanolini@unibe.ch

November 11, 2022

Stellar Consensus by Instantiation

Giuliano Losa*
Galois, Inc.
giuliano@galois.com

Eli Gafni†
UCLA
eli@ucla.edu

David Mazières‡
Stanford
http://www.scs.stanford.edu/~dm/addr/

January 24, 2020

Abstract

Stellar introduced a new type of quorum system called a Federated Byzantine Agreement System. A major difference between this novel type of quorum system and a threshold quorum system is that each participant has its own, personal notion of a quorum. Thus, unlike in a traditional BFT system, designed for a uniform notion of quorum, even in a time of synchrony one well-behaved participant may observe a quorum of well-behaved participants, while others may not.

Semitopology: a new topological model of heterogeneous consensus

Murdoch J. Gabbay and Giuliano Losa

A distributed system is *permissionless* when participants can join and leave the network without permission from a central authority. Many modern distributed systems are naturally permissionless, in the sense that a central permissioning authority would defeat their design purpose: this includes blockchains, filesharing protocols, some voting systems, and more. By their permissionless nature, such systems are heterogeneous: participants may only have a partial view of the system, and they may also have different goals and beliefs. Thus, the traditional notion of consensus — i.e. system-wide agreement — may not be adequate, and we may need to generalise it.

This is a challenge: how should we understand what heterogeneous consensus is; what mathematical framework might this require; and how can we use this to build understanding and mathematical models of robust, effective, and secure permissionless systems in practice?

In this paper we offer a new definition of heterogeneous consensus, using *semitopology* as a framework. This is like topology, but without the restriction that intersections of opens be open.

Semitopologies have a rich theory which is related to topology, but with its own distinct character and mathematics. We introduce novel well-behavedness conditions, including an anti-Hausdorff property and a new notion of 'topen set', and we show how these structures relate to consensus. We give a restriction of semitopologies to *witness semitopologies*, which are an algorithmically tractable subclass corresponding to Horn clause theories, having particularly good mathematical properties. We introduce and study several other basic notions that are specific and novel to semitopologies, and study how known quantities in topology, such as dense subsets and closures, display interesting and useful new behaviour in this new semitopological context.

... Key Words and Phrases: Topology, Semitopology, Permissionless Network, Heterogeneous consensus, Horn clause

v2 [cs.LO] 29 Mar 2023