PRIV LEDGE

Asymmetric Distributed Trust

Christian Cachin (University of Bern)
and Björn Tackmann (IBM)

May 18, PENCIL workshop

Byzantine fault tolerant consensus

- Active research since ~40 years
  - Guarantees consistency as long as at most <1/3 of the participants are misbehaving
  - Every participant makes the same trust assumption about the other participants in the network
  - But trust is subjective: *De gustibus non est disputandum*
  - The symmetry assumption is not justified in our daily experience

Related work

- Ripple's Unique Node Lists
  - But the protocol seems very heuristic and guarantees are unclear, some centralized structures
- Stellar's Federated Consensus
  - Do not generalize Byzantine quorums, system has experienced undesired states
- Damgård, Desmedt, Fitzi, Nielsen – ASIACRYPT 2007
  - MPC in asymmetric setting, focus on synchronous networks, conjecture broadcast

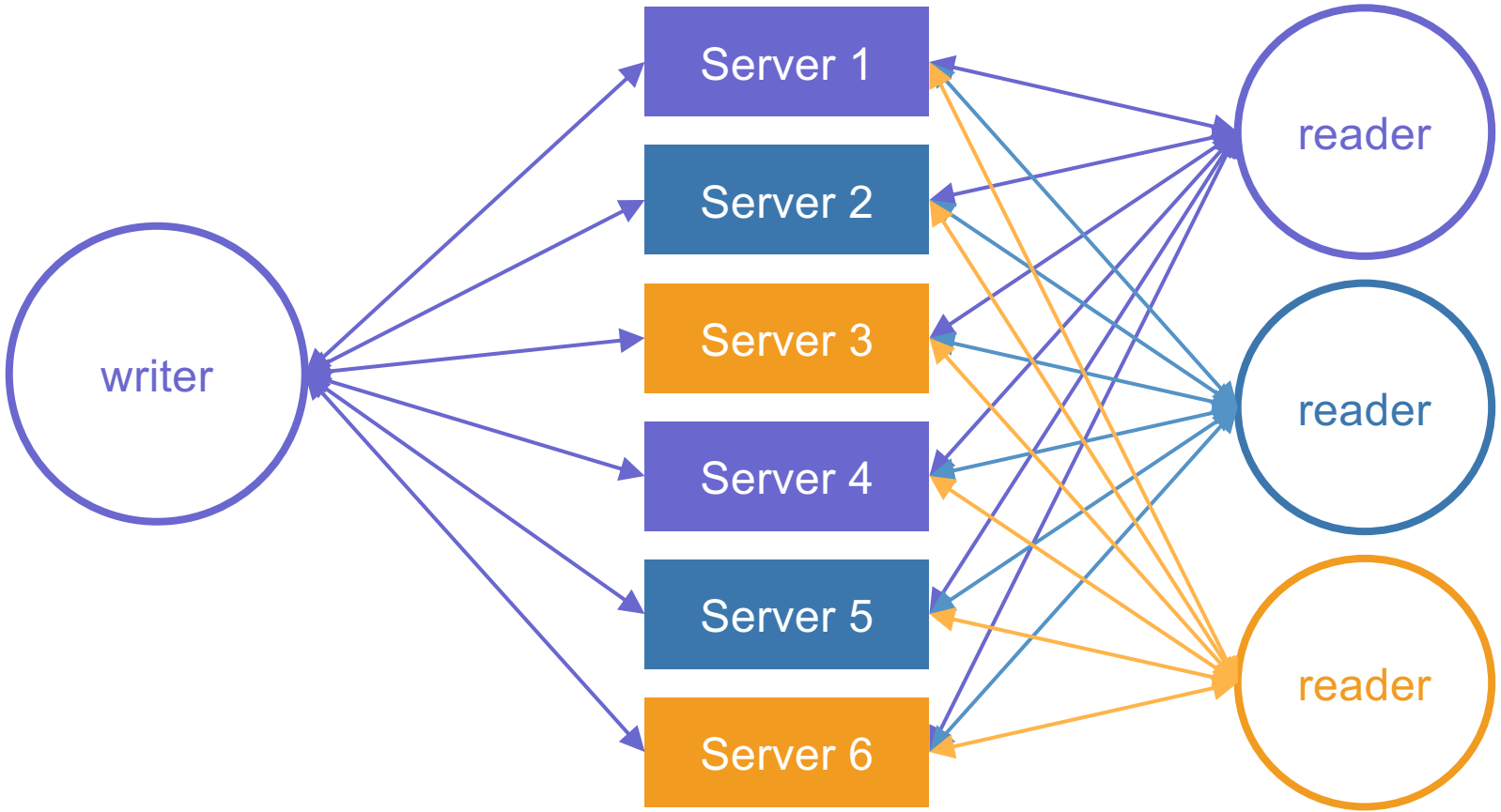
Quorum systems (Malkhi-Reiter)

- Consider parties $\mathscr{P} = \{p_1,\ldots,p_n\}$
- Fail-prone system $\mathscr{F} = \{F_1,F_2,\ldots\}$ with $F_j \subseteq \mathscr{P}$
- Byzantine quorum system $\mathscr{Q} = \{Q_1,Q_2,\ldots\}$ with $Q_j \subseteq \mathscr{P}$
  - Consistency: $Q_j \cap Q_k \not\subseteq F_k$
  - Availability: $\forall\, F_j\, \exists\, Q_k$ s.t. $F_j \cap Q_k = \emptyset$
- Theorem:
  A Byzantine quorum system exists
  iff.
  $\mathscr{P} \not\subseteq F_j \cup F_k \cup F_m$.

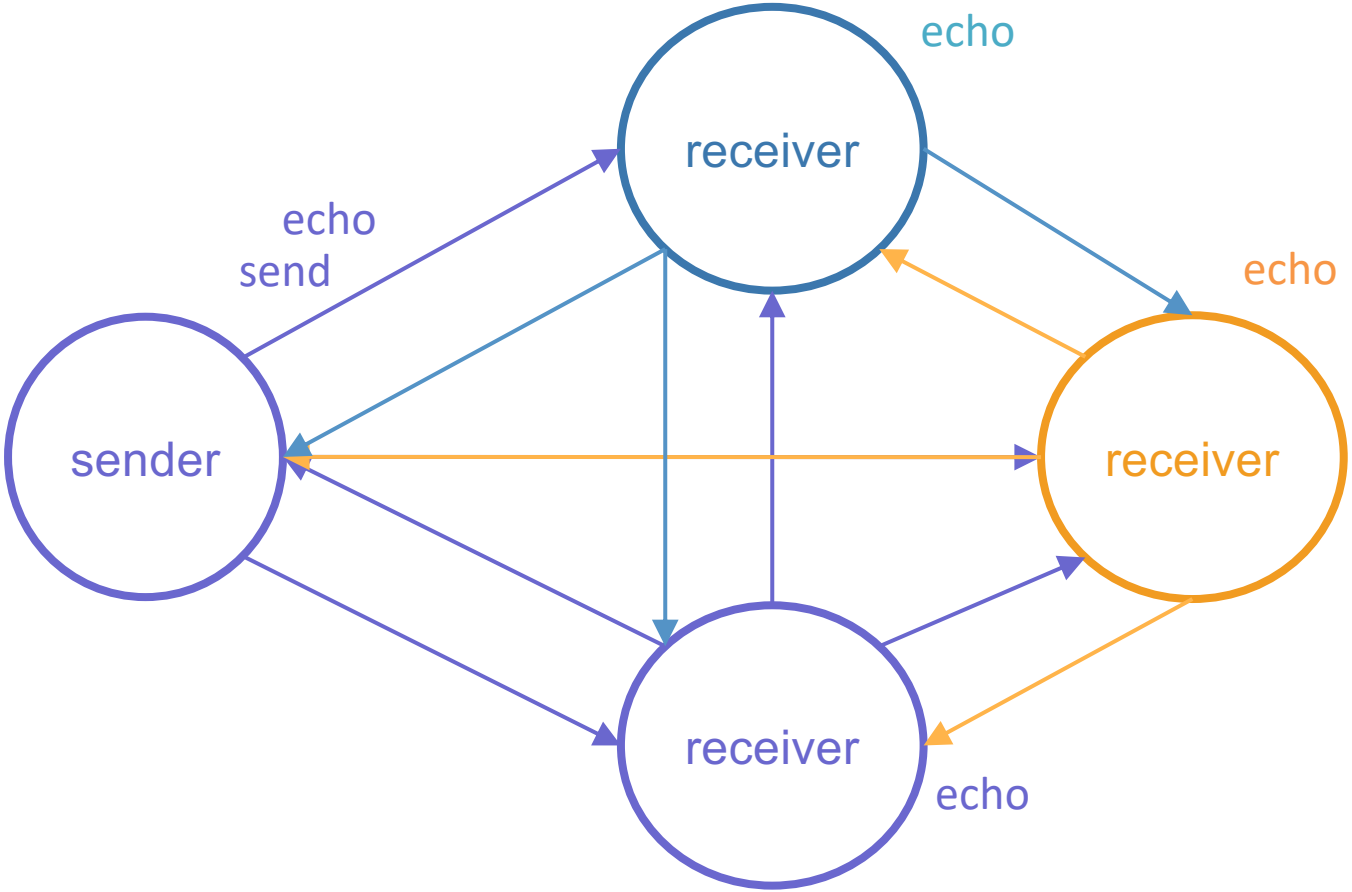
Asymmetric quorum systems

- Each p_i has their own fail-prone system $\mathcal{F}_i = \{F_1, F_2, \ldots\}$
- Also defines quorum set $\mathcal{Q}_i = \{Q_1, Q_2, \ldots\}$
- Condition for **asymmetric** Byzantine quorum system:
  - Consistency: quorums of *different* parties must intersect
  - Availability: same as before, per-party
- Theorem: Asymmetric BQS exists iff. $\mathcal{P} \notin F_j \cup F_k \cup F_{jk}$
- We have to distinguish between two types of honest parties:
  - *wise* parties whose trust assumption is **correct**
  - *naïve* parties whose trust assumption is **wrong**

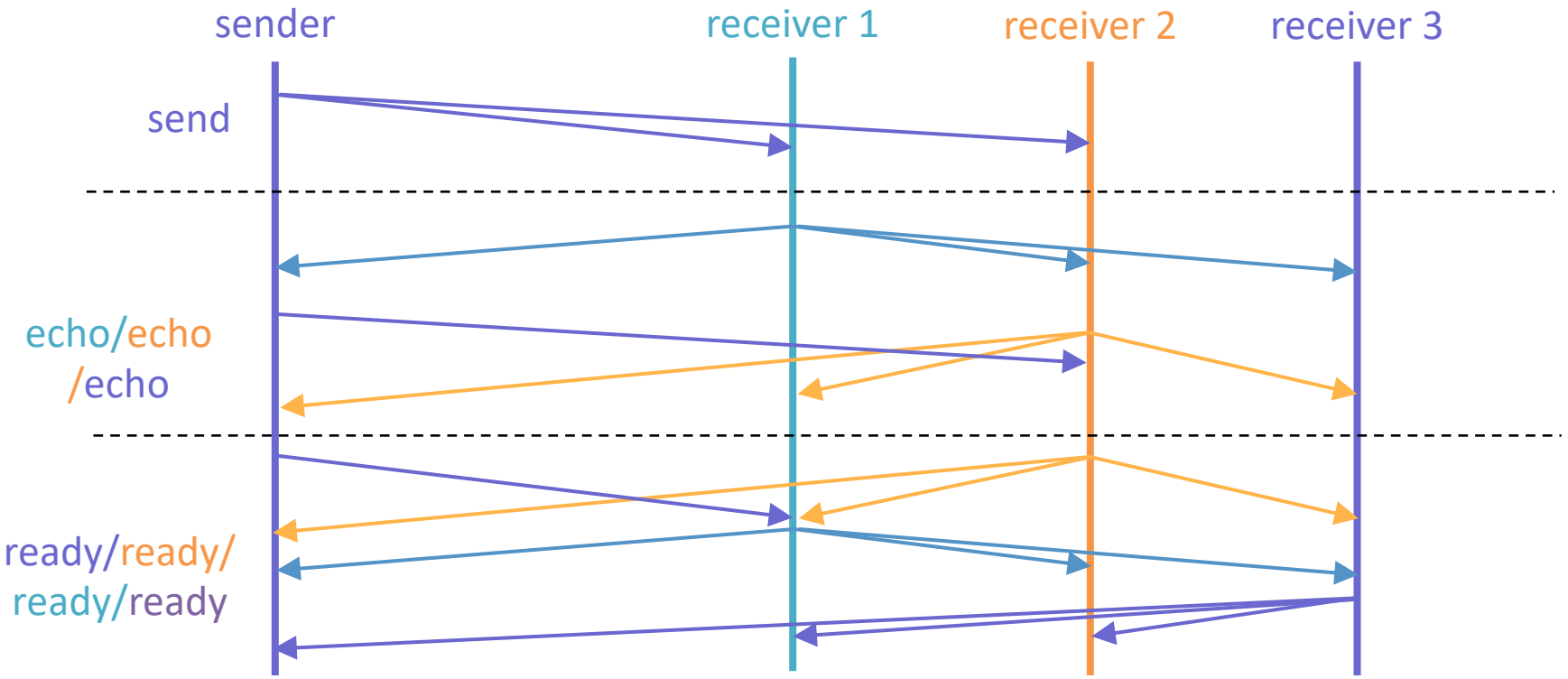
Results I – Shared memory



Results II – Consistent broadcast



Results III – Reliable broadcast



The extension of Bracha broadcast works *if* there exists a *guild*!

Summary

- We formalize an asymmetric notion of quorum systems
- Protocols for..:
  - Shared memory (w/ and w/o signatures)
  - Broadcast (consistent and reliable)
- Next steps:
  - Necessity of guilds?
  - Other protocols: consensus!

Thank you!