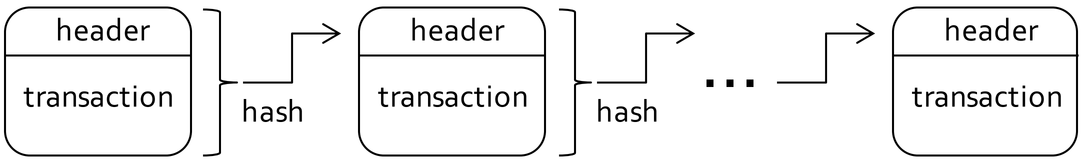
Federated Byzantine Quorum Systems

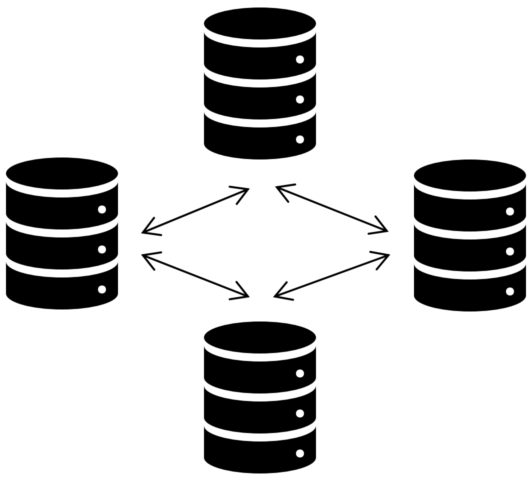
Álvaro García-Pérez and Alexey Gotsman

IMDEA Software Institute

Blockchains

- Append-only, distributed ledger.
- Uses a Byzantine fault-tolerant (BFT) consensus algorithm to ensure that distributed nodes agree on the next block to append.





Permissioned and permissionless blockchains

- Permissioned blockchains assume a fixed set of participants:
  - classic consensus algorithms, decisions rely on a quorum, I.e., $3f$+1.
- Permissionless blockchains have open membership:
  - often rely on proof-of-work, high energy consumption.

Flexible trust

- Combines quorum systems with decentralisation:
  - The set of participants is fixed, the choice of trust is not.

Flexible trust

- Combines quorum systems with decentralisation:
  - The set of participants is fixed, the choice of trust is not.
- Classic quorum systems:
  - Dissemination quorum systems (DQS) [Malkhi and Reiter, 1998].
  - Allow to choose a tailor-made quorum system.
- Stellar's federated systems [Mazières, 2016]:
  - Federated Byzantine quorum systems (FBQS) [Mazières, 2016].
  - Each participant decides who to trust, and participants may not know the whole system.

Broadcast and quorum systems

classic quorum systems

Stellar's federated systems

Broadcast and quorum systems

classic quorum systems

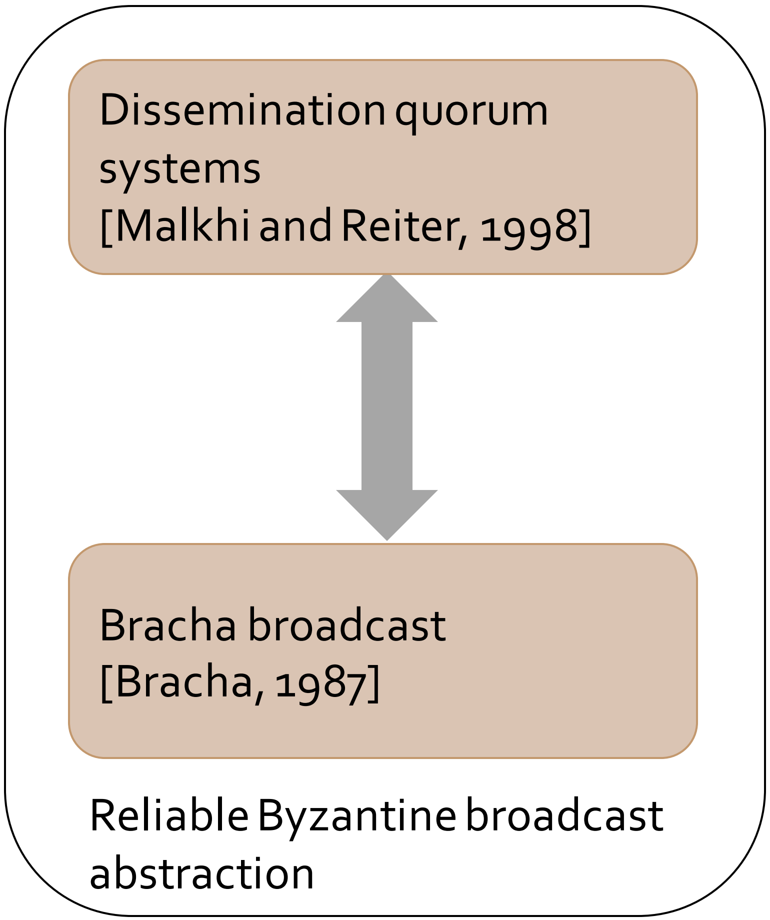
Stellar's federated systems

Dissemination quorum systems
[Malkhi and Reiter, 1998]

Bracha broadcast
[Bracha, 1987]

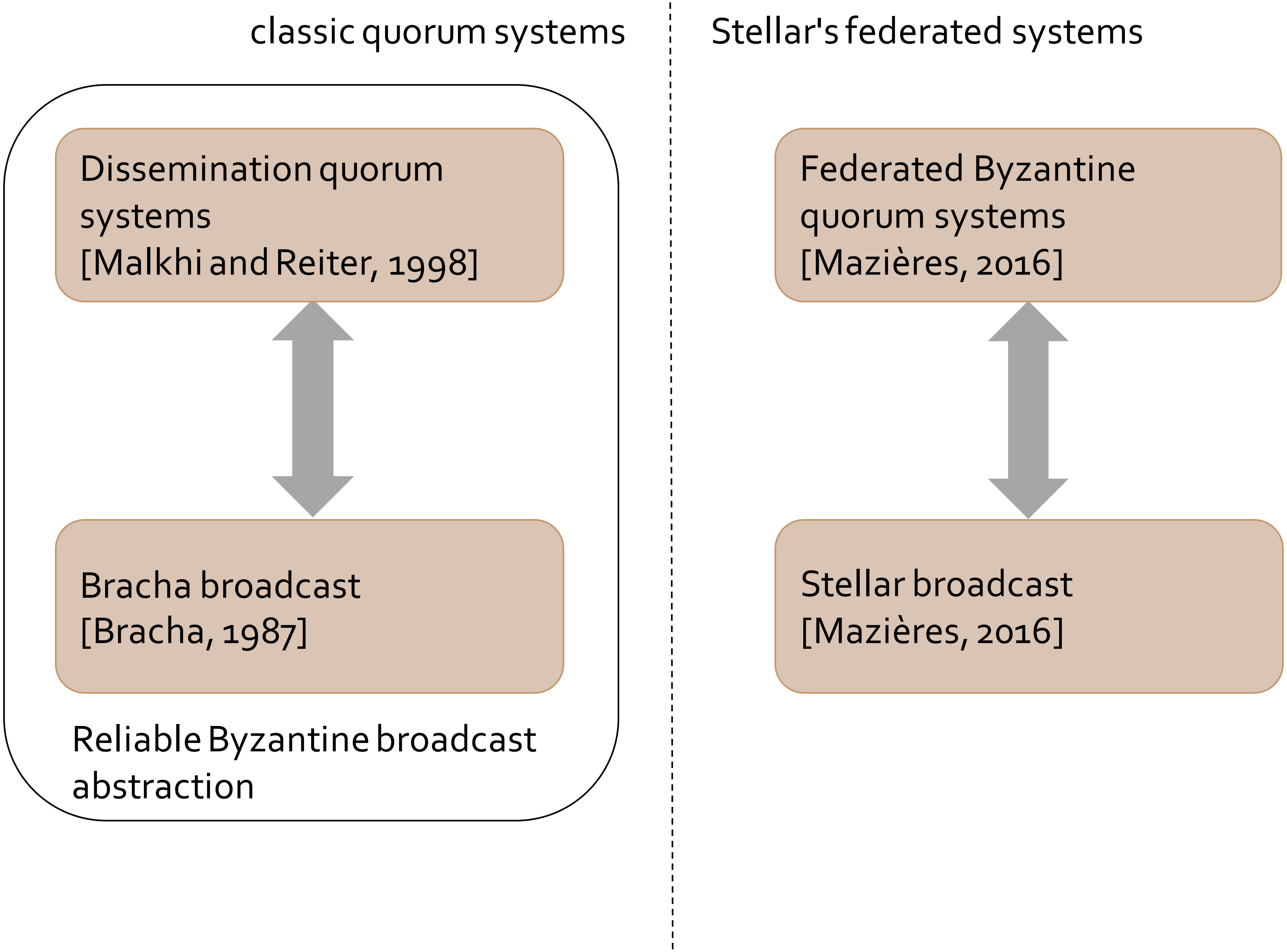
Broadcast and quorum systems

classic quorum systems

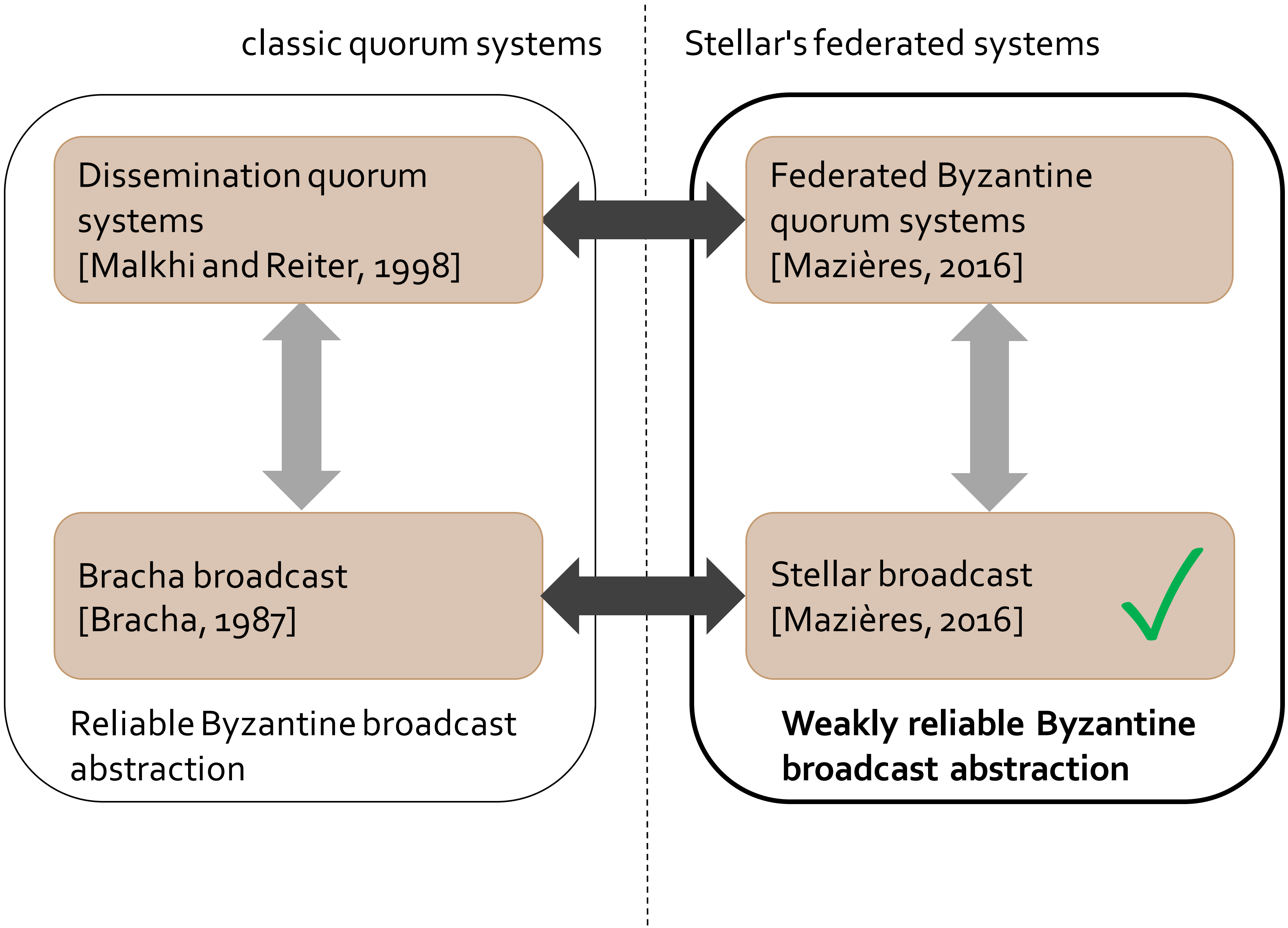


Stellar's federated systems

Broadcast and quorum systems



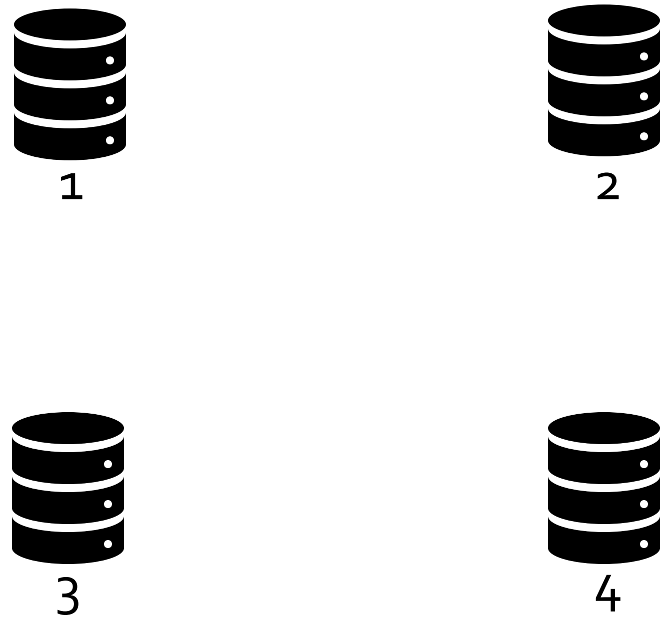
Our contribution



Dissemination Quroum System (DQS)

DQS

$\mathbb{V} = \{1,2,3,4\}$



$(\mathbb{Q} : 2^{2^{\mathbb{V}}}, \ \mathbb{B} : 2^{2^{\mathbb{V}}})$

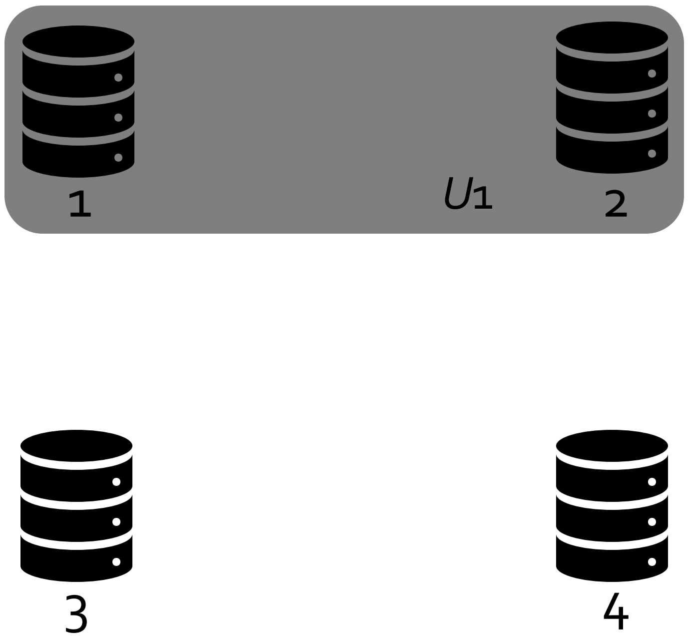
$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$
$U_4 = \{1,2,3,4\} \in \mathbb{Q}$

$B_1 = \{2\} \in \mathbb{B}$
$B_2 = \{3,4\} \in \mathbb{B}$

- **(Consistency)** The intersection of any two quorums U and U' in $\mathbb{Q}$ cannot lie within any element B of $\mathbb{B}$.
- **(Availability)** For any element B of $\mathbb{B}$ there exists some quorum U in $\mathbb{Q}$ that has empty intersection with B.

DQS

$\mathbb{V} = \{1,2,3,4\}$



$(\mathbb{Q} : 2^{2^{\mathbb{V}}},\ \mathbb{B} : 2^{2^{\mathbb{V}}})$

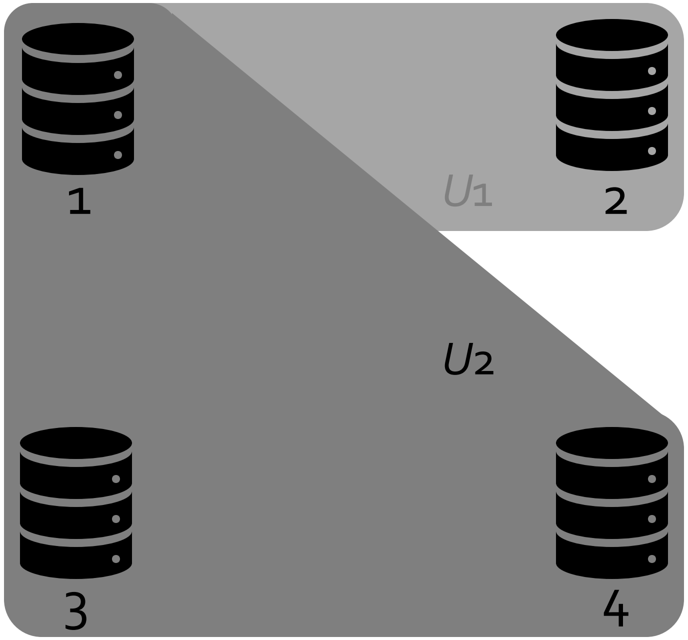
$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$
$U_4 = \{1,2,3,4\} \in \mathbb{Q}$

$B_1 = \{2\} \in \mathbb{B}$
$B_2 = \{3,4\} \in \mathbb{B}$

- **(Consistency)** The intersection of any two quorums U and U' in $\mathbb{Q}$ cannot lie within any element B of $\mathbb{B}$.
- **(Availability)** For any element B of $\mathbb{B}$ there exists some quorum U in $\mathbb{Q}$ that has empty intersection with B.

DQS

$\mathbb{V} = \{1,2,3,4\}$



$(\mathbb{Q} : 2^{2^{\mathbb{V}}},\ \mathbb{B} : 2^{2^{\mathbb{V}}})$

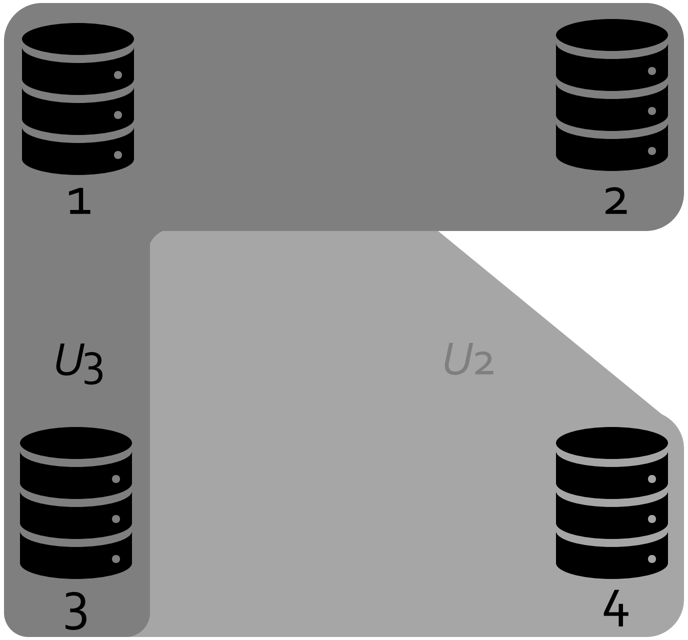
$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$
$U_4 = \{1,2,3,4\} \in \mathbb{Q}$

$B_1 = \{2\} \in \mathbb{B}$
$B_2 = \{3,4\} \in \mathbb{B}$

- **(Consistency)** The intersection of any two quorums U and U' in $\mathbb{Q}$ cannot lie within any element B of $\mathbb{B}$.
- **(Availability)** For any element B of $\mathbb{B}$ there exists some quorum U in $\mathbb{Q}$ that has empty intersection with B.

DQS

$\mathbb{V} = \{1,2,3,4\}$



$(\mathbb{Q} : 2^{2^{\mathbb{V}}},\ \mathbb{B} : 2^{2^{\mathbb{V}}})$

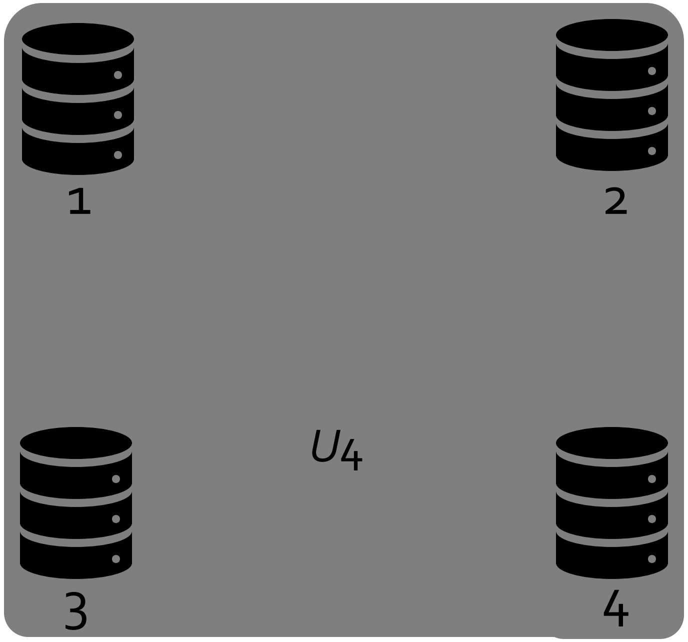
$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$
$U_4 = \{1,2,3,4\} \in \mathbb{Q}$

$B_1 = \{2\} \in \mathbb{B}$
$B_2 = \{3,4\} \in \mathbb{B}$

- **(Consistency)** The intersection of any two quorums U and U' in $\mathbb{Q}$ cannot lie within any element B of $\mathbb{B}$.
- **(Availability)** For any element B of $\mathbb{B}$ there exists some quorum U in $\mathbb{Q}$ that has empty intersection with B.

DQS

$\mathbb{V} = \{1,2,3,4\}$



$(\mathbb{Q} : 2^{2^{\mathbb{V}}},\ \mathbb{B} : 2^{2^{\mathbb{V}}})$

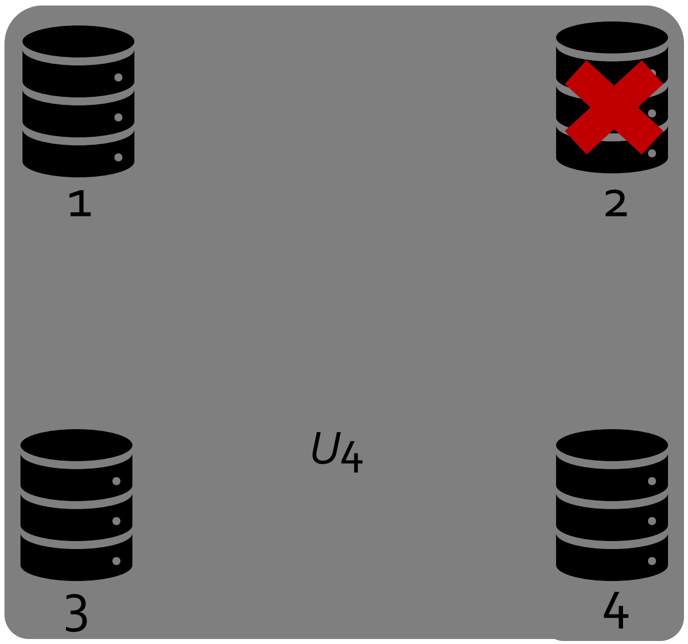
$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$
$U_4 = \{1,2,3,4\} \in \mathbb{Q}$

$B_1 = \{2\} \in \mathbb{B}$
$B_2 = \{3,4\} \in \mathbb{B}$

- **(Consistency)** The intersection of any two quorums U and U' in $\mathbb{Q}$ cannot lie within any element B of $\mathbb{B}$.
- **(Availability)** For any element B of $\mathbb{B}$ there exists some quorum U in $\mathbb{Q}$ that has empty intersection with B.

DQS

$\mathbb{V} = \{1,2,3,4\}$



$(\mathbb{Q} : 2^{2^{\mathbb{V}}},\ \mathbb{B} : 2^{2^{\mathbb{V}}})$

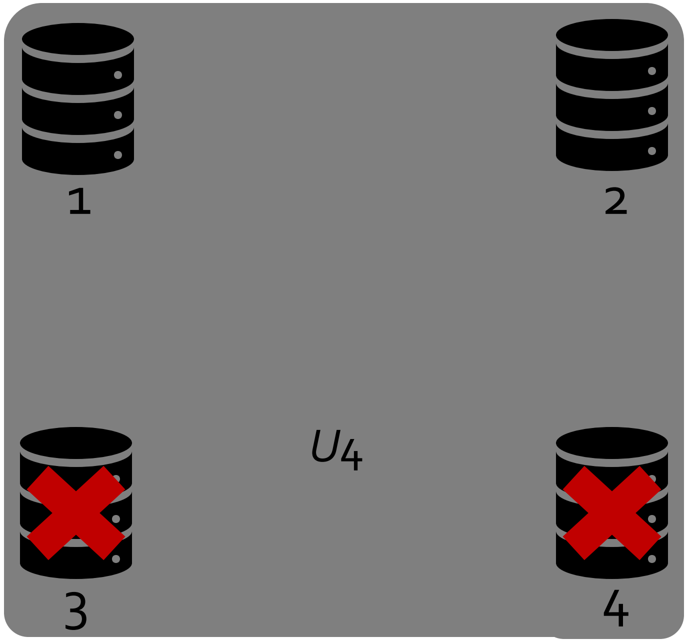
$U1 = \{1,2\} \in \mathbb{Q}$
$U2 = \{1,3,4\} \in \mathbb{Q}$
$U3 = \{1,2,3\} \in \mathbb{Q}$
$U4 = \{1,2,3,4\} \in \mathbb{Q}$

$B1 = \{2\} \in \mathbb{B}$
$B2 = \{3,4\} \in \mathbb{B}$

- **(Consistency)** The intersection of any two quorums U and U' in $\mathbb{Q}$ cannot lie within any element B of $\mathbb{B}$.
- **(Availability)** For any element B of $\mathbb{B}$ there exists some quorum U in $\mathbb{Q}$ that has empty intersection with B.

DQS

$\mathbb{V} = \{1,2,3,4\}$



$(\mathbb{Q} : 2^{2^{\mathbb{V}}}, \ \mathbb{B} : 2^{2^{\mathbb{V}}})$

$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$
$U_4 = \{1,2,3,4\} \in \mathbb{Q}$

$B_1 = \{2\} \in \mathbb{B}$
$B_2 = \{3,4\} \in \mathbb{B}$

- **(Consistency)** The intersection of any two quorums U and U' in $\mathbb{Q}$ cannot lie within any element B of $\mathbb{B}$.
- **(Availability)** For any element B of $\mathbb{B}$ there exists some quorum U in $\mathbb{Q}$ that has empty intersection with B.

DQS and threshold models

- DQS generalises usual BFT models with threshold f and $n = 3f+1$ servers.

DQS and threshold models

- DQS generalises usual BFT models with threshold f and $n = 3f+1$ servers.

$f = 1$, $n = 4$

DQS and threshold models

- DQS generalises usual BFT models with threshold f and $n = 3f+1$ servers.

$f = 1$, $n = 4$

Quorums equal or bigger than $2f+1 = 3$

$\mathbb{Q} = \{ \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\} \}$

Fail-prone sets exactly $f = 1$

$\mathbb{B} = \{ \{1\}, \{2\}, \{3\}, \{4\} \}$

DQS and threshold models

- DQS generalises usual BFT models with threshold f and $n = 3f+1$ servers.

$f = 1$, $n = 4$

Quorums equal or bigger than $2f+1 = 3$

$\mathbb{Q} = \{ \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\} \}$

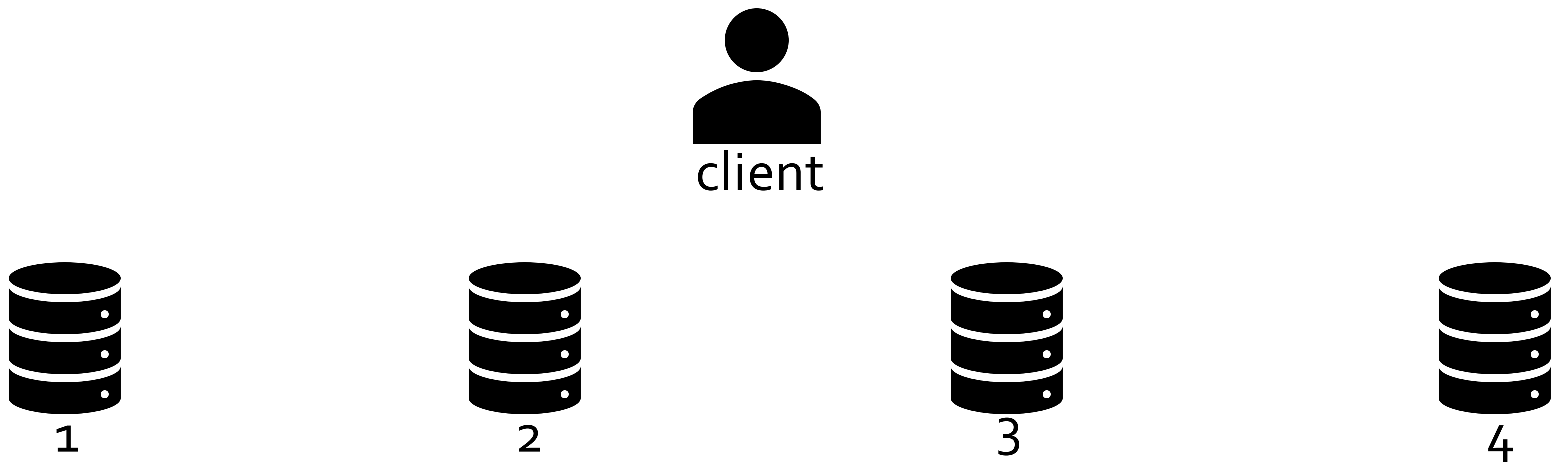
Fail-prone sets exactly $f = 1$

$\mathbb{B} = \{ \{1\}, \{2\}, \{3\}, \{4\} \}$

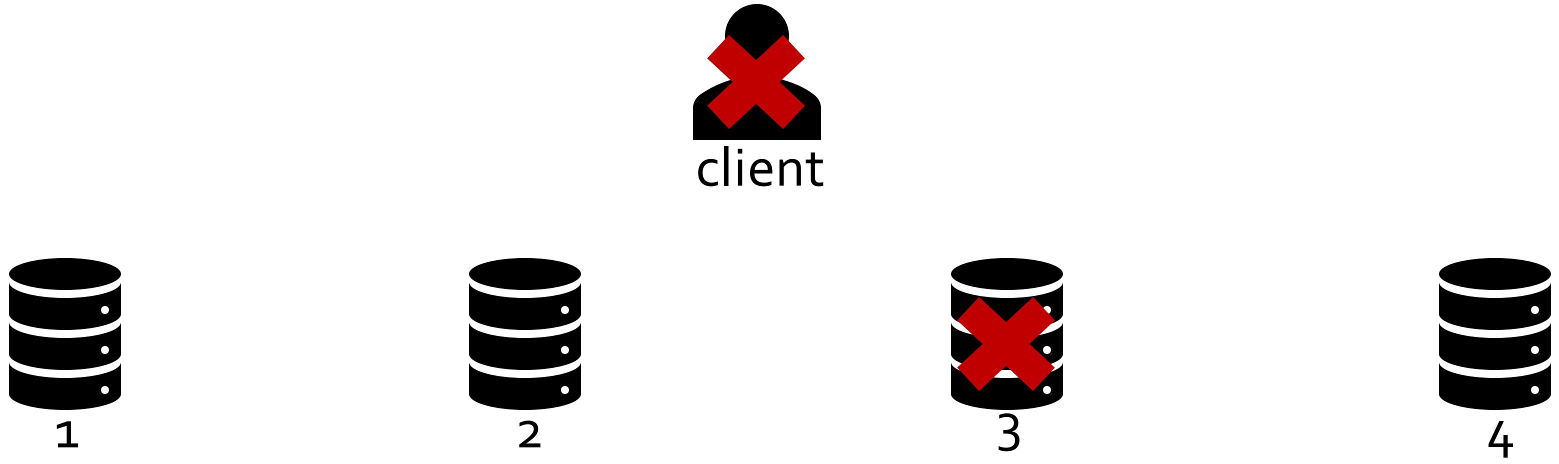
- **(Consistency)** Every two quorums intersect in at least f+1 servers.
- **(Availability)** If f servers fail, the remaining ones constitutes a quorum.

Bracha Broadcast

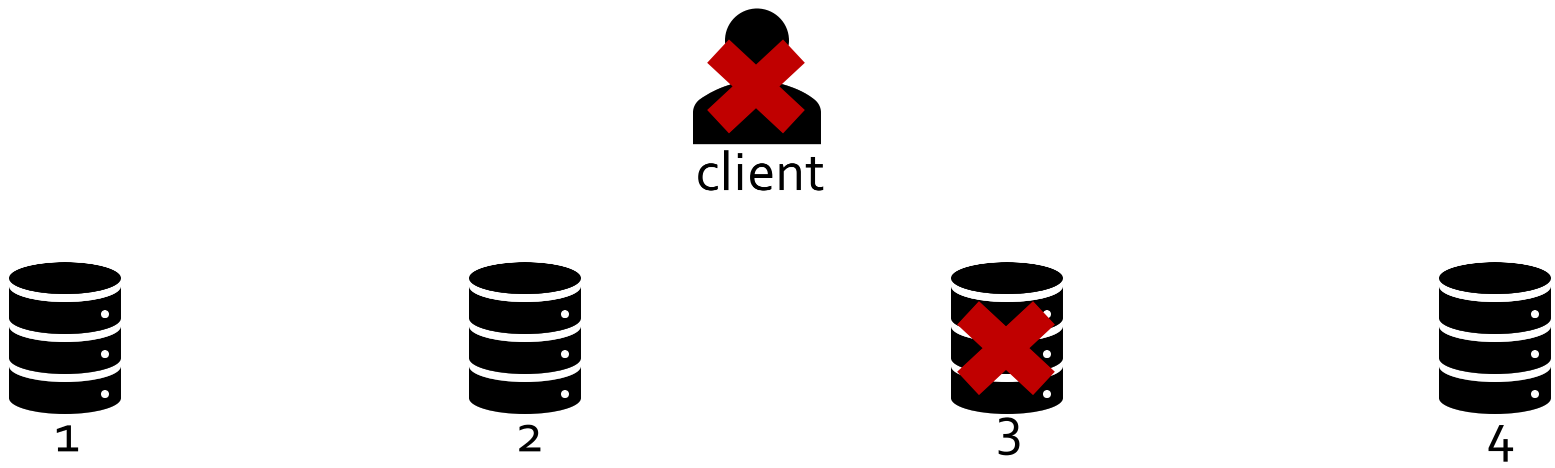
Example: $3f+1$



Example: $3f+1$



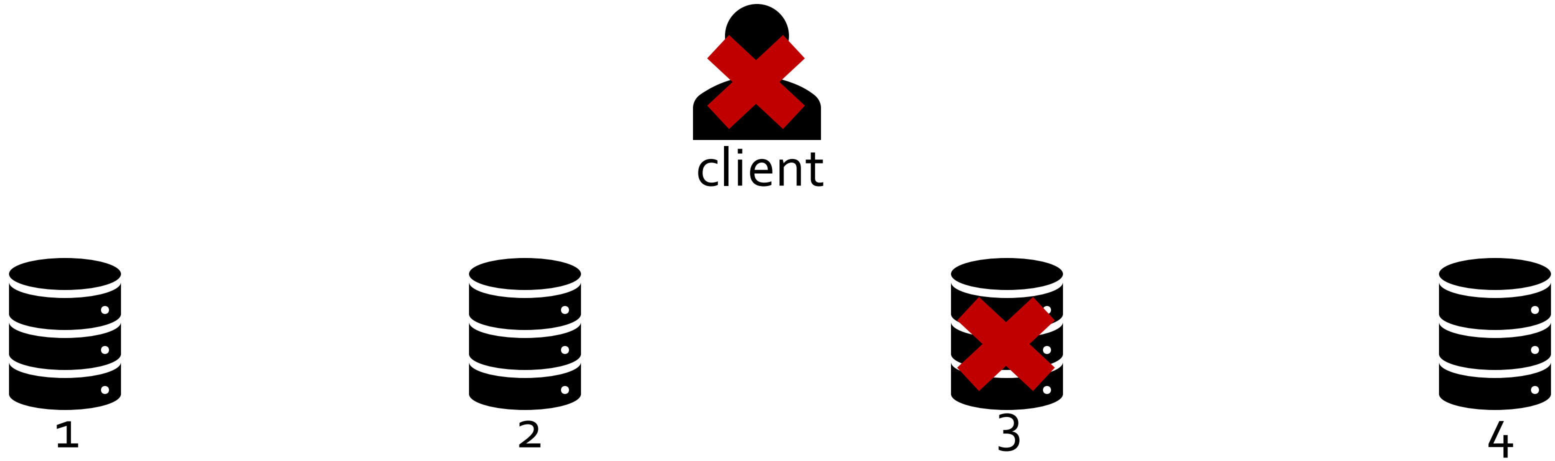
Example: $3f$+1



receive [BCAST *a*]	receive [BCAST *a*]		receive [BCAST *b*]

To broadcast a value *a*, the client sends `[BCAST` *a*`]` to every server.

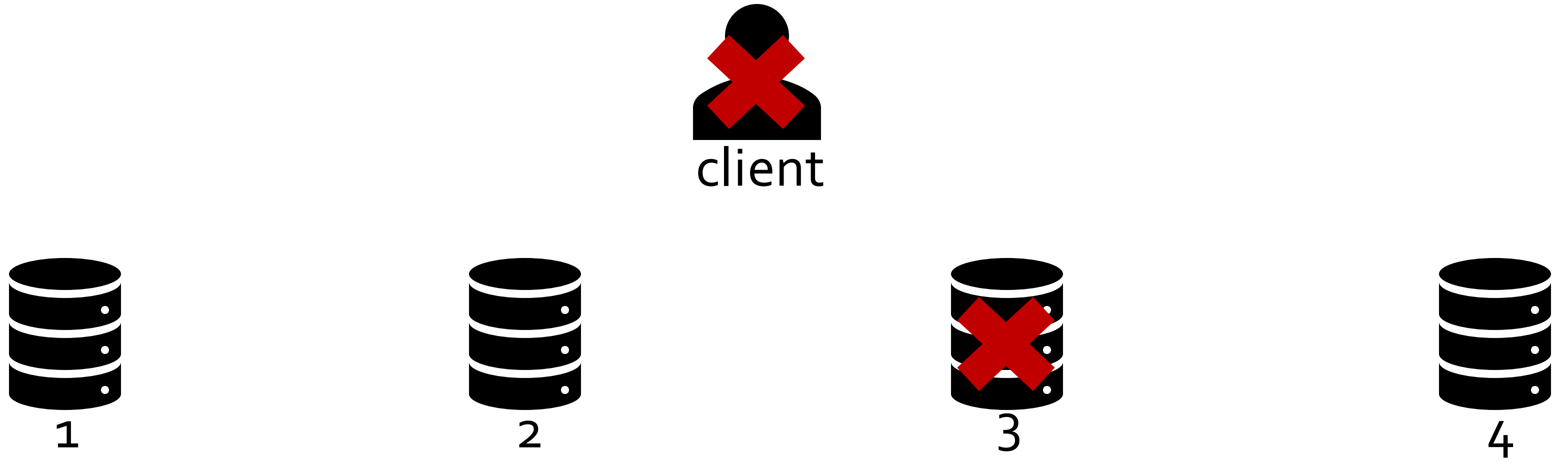
Example: $3f+1$



receive [BCAST a]	receive [BCAST a]		receive [BCAST b]
send [ECHO a] to all	send [ECHO a] to all		send [ECHO b] to all

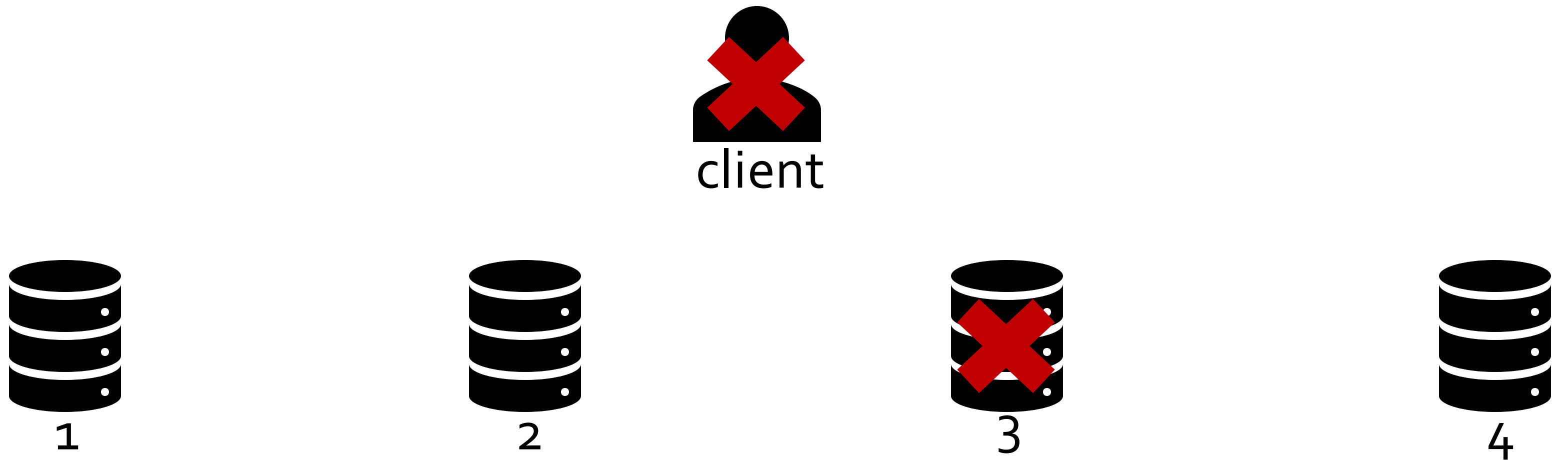
After receiving [BCAST a], a server sends [ECHO a] to every server.

Example: $3f$+1



receive [BCAST *a*]	receive [BCAST *a*]		receive [BCAST *b*]
send [ECHO *a*] to all	send [ECHO *a*] to all	send [ECHO *a*] to 1,2	send [ECHO *b*] to all

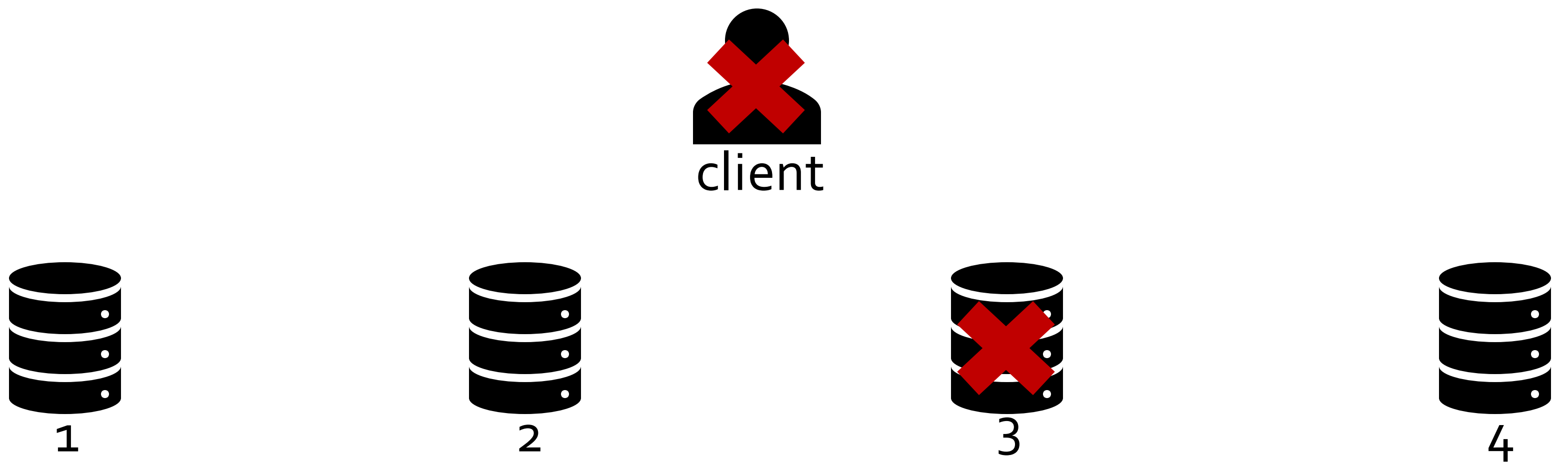
Example: 3*f*+1



receive [BCAST *a*]	receive [BCAST *a*]		receive [BCAST *b*]
send [ECHO *a*] to all	send [ECHO *a*] to all	send [ECHO *a*] to 1,2	send [ECHO *b*] to all
send [READY *a*] to all	send [READY *a*] to all		

After receiving [ECHO *a*] from a quorum, a server sends [READY *a*] to every server.

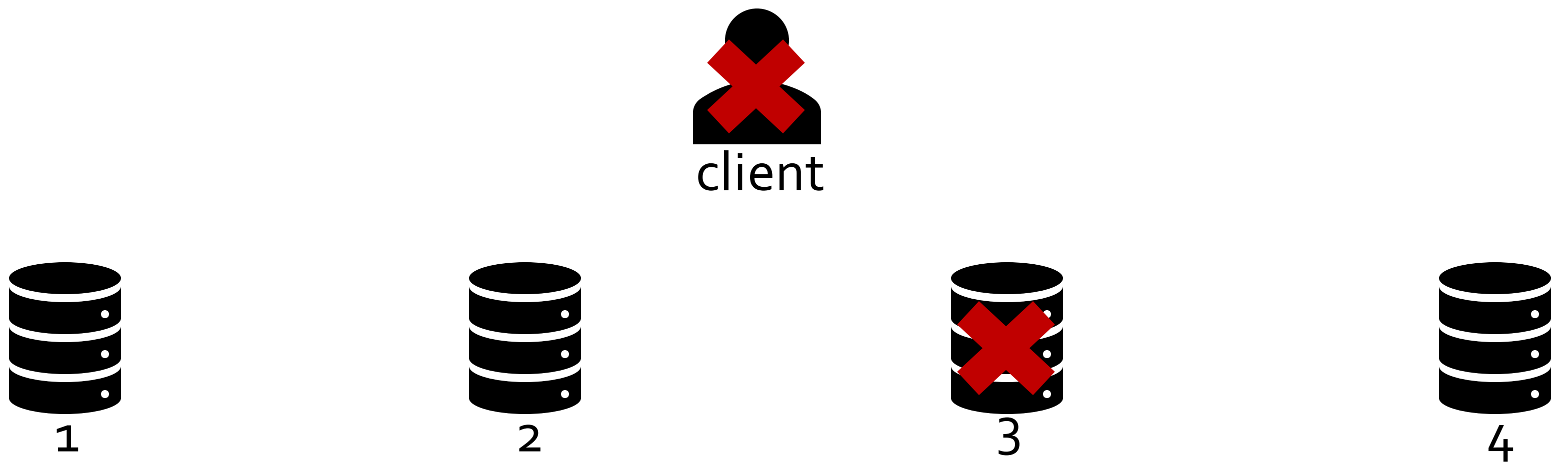
Example: $3f$+1



receive [BCAST a]	receive [BCAST a]		receive [BCAST b]
send [ECHO a] to all	send [ECHO a] to all	send [ECHO a] to 1,2	send [ECHO b] to all
send [READY a] to all	send [READY a] to all		
			send [READY a] to all

After receiving [READY a] from a set B such that $\forall B' \in \mathbb{B}, B \not\subseteq B'$, a server sends [READY a] to every server.

Example: $3f$+1



receive [BCAST *a*]	receive [BCAST *a*]		receive [BCAST *b*]
send [ECHO *a*] to all	send [ECHO *a*] to all	send [ECHO *a*] to 1,2	send [ECHO *b*] to all
send [READY *a*] to all	send [READY *a*] to all		
			send [READY *a*] to all
`deliver`(*a*)	`deliver`(*a*)		`deliver`(*a*)

After receiving `[READY` *a*`]` from a quorum, a server delivers value *a*.

Reliable Byzantine broadcast

Bracha broadcast satisfies the specification of reliable Byzantine broadcast when all faulty servers belong to some element of $\mathbb{B}$:

- ***Safety:*** If some correct server delivers a value a and another correct server delivers a value b, then $a = b$.
- ***Liveness:*** If a correct server delivers a value, then every correct server eventually delivers a value.

Reliable Byzantine broadcast

Bracha broadcast satisfies the specification of reliable Byzantine broadcast when all faulty servers belong to some element of $\mathbb{B}$:

- ***Safety:*** If some correct server delivers a value a and another correct server delivers a value b, then $a = b$.
- ***Liveness:*** If a correct server delivers a value, then every correct server eventually delivers a value.

The protocol needs to compute $\mathbb{B}$, which requires global information!

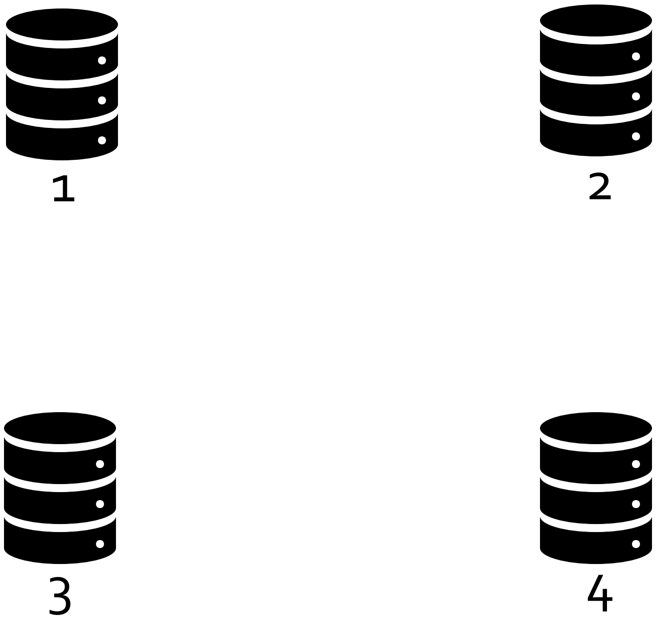
Federated Byzantine Quroum Systems (FBQS)

FBQS

$$\mathbb{V} = \{1,2,3,4\}$$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



FBQS

$\mathbb{V} = \{1,2,3,4\}$

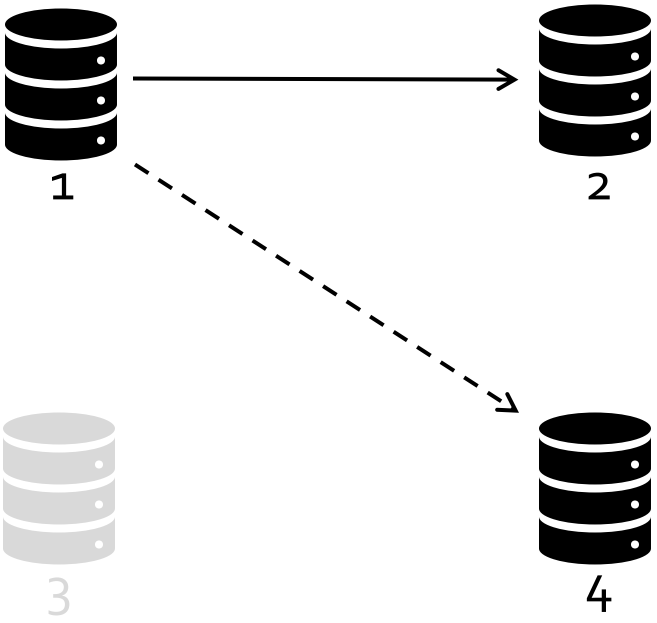
$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$

$\mathbb{S}(2) = \{\{1,2\}\}$

$\mathbb{S}(3) = \{\{1,3\}\}$

$\mathbb{S}(4) = \{\{3,4\}\}$



FBQS

$\mathbb{V} = \{1,2,3,4\}$

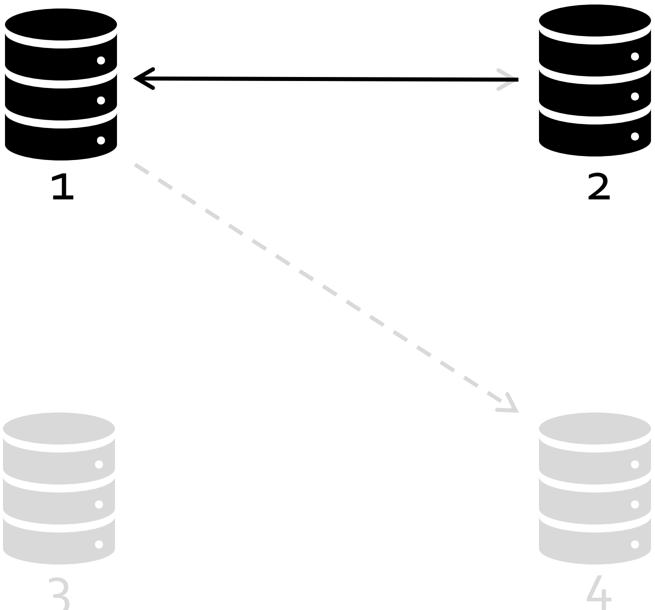
$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$

$\mathbb{S}(2) = \{\{1,2\}\}$

$\mathbb{S}(3) = \{\{1,3\}\}$

$\mathbb{S}(4) = \{\{3,4\}\}$

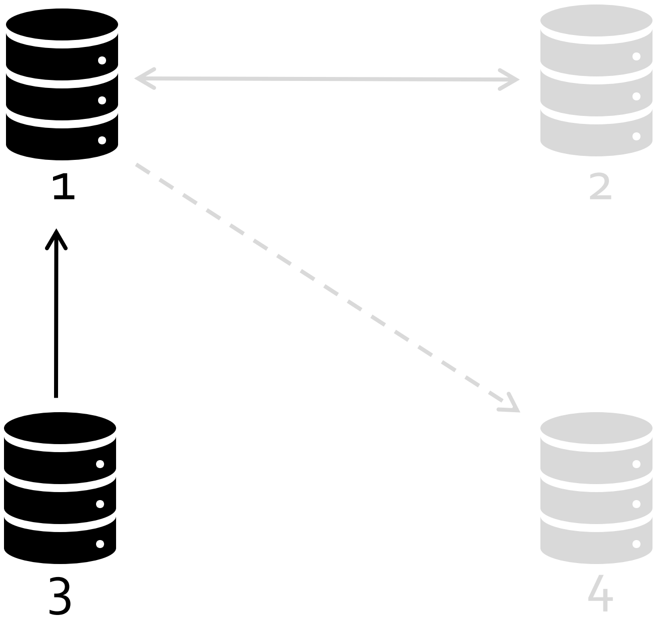


FBQS

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$

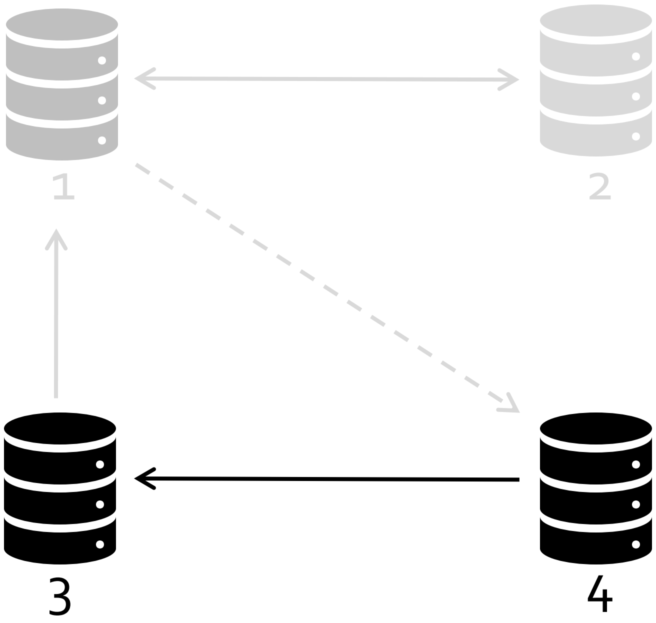


FBQS

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$

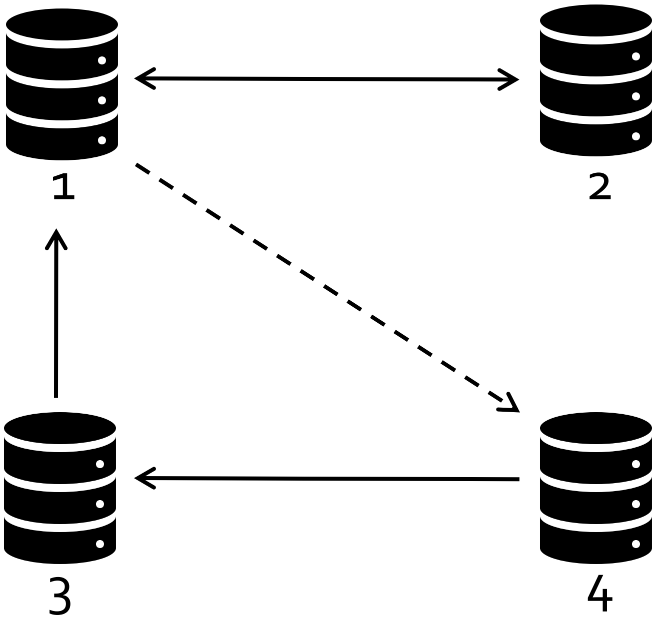


FBQS

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$

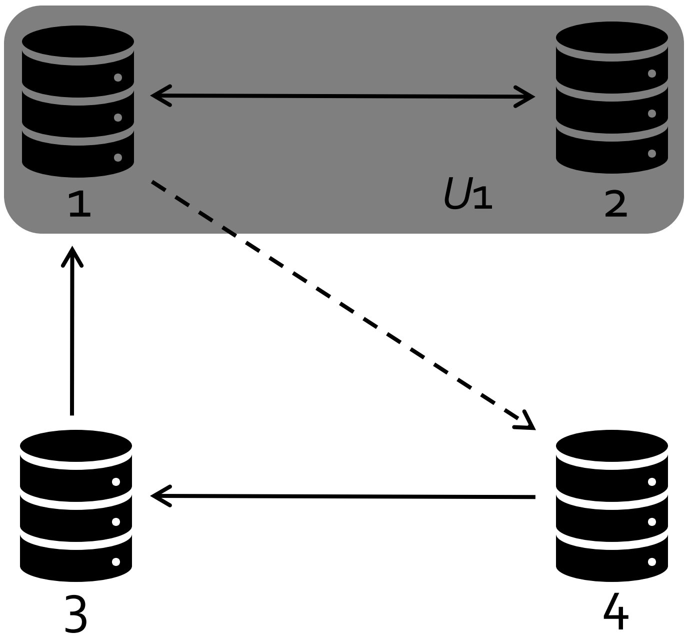


FBQS

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



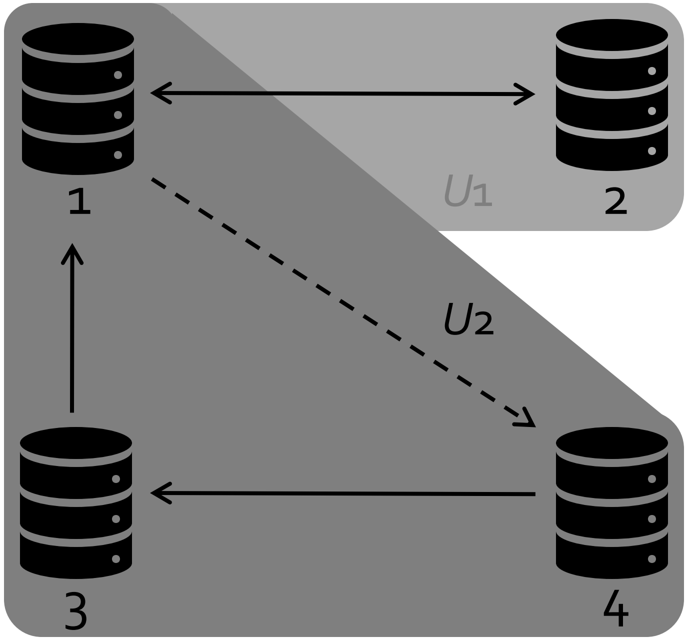
$U_1 = \{1,2\} \in \mathbb{Q}$

FBQS

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



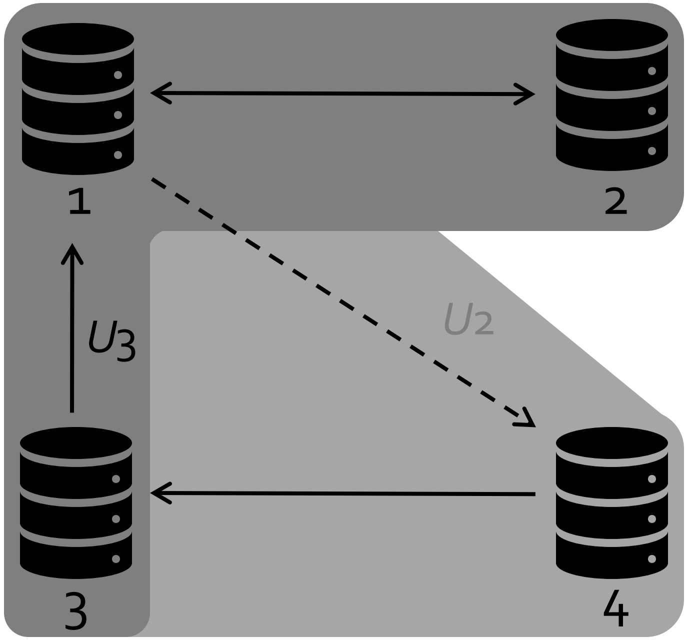
$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$

FBQS

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



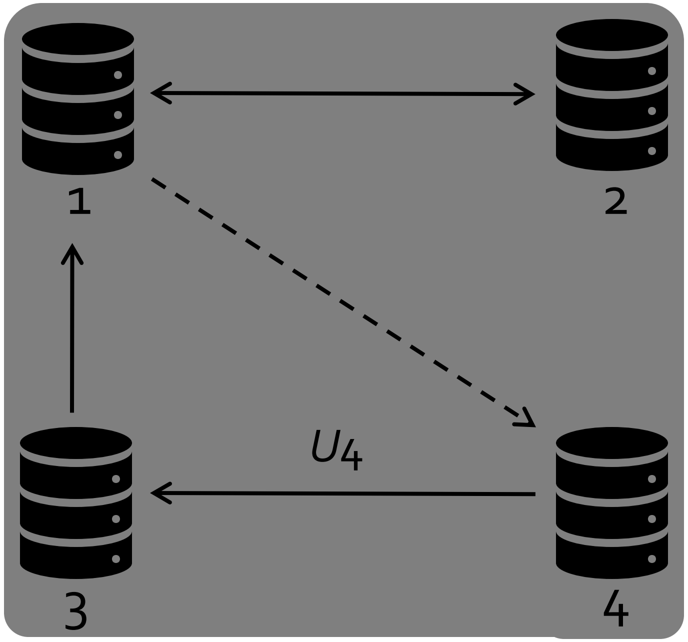
$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$

FBQS

$$\mathbb{V} = \{1,2,3,4\}$$

$$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



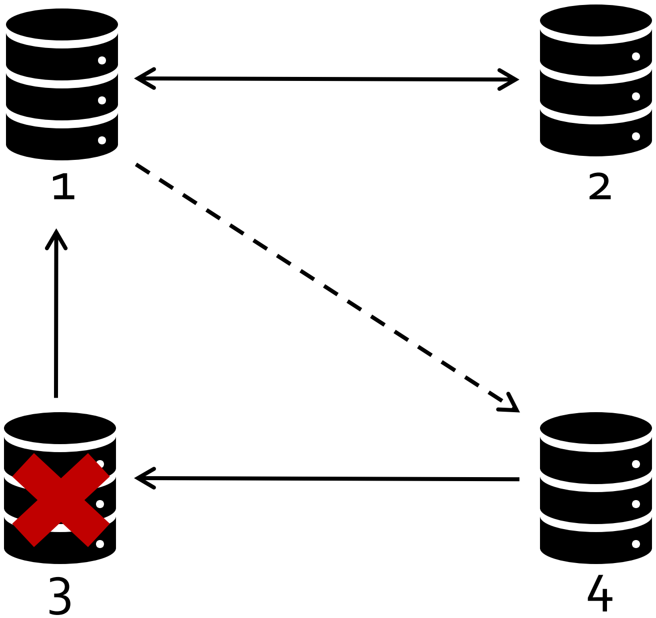
$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$
$U_4 = \{1,2,3,4\} \in \mathbb{Q}$

FBQS (Intact and befouled servers)

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



Given a set of faulty servers, $\mathbb{V}_{int}$ is the biggest quorum $\mathbb{V}_{int} \in \mathbb{Q}$ such that:

- $\forall v \in \mathbb{V}_{int}$, v is correct,
- $\mathbb{Q}|_{\mathbb{V}_{int}}$ has quorum intersection.

FBQS (Intact and befouled servers)

$\mathbb{V}\text{int} = \{1,2\}$

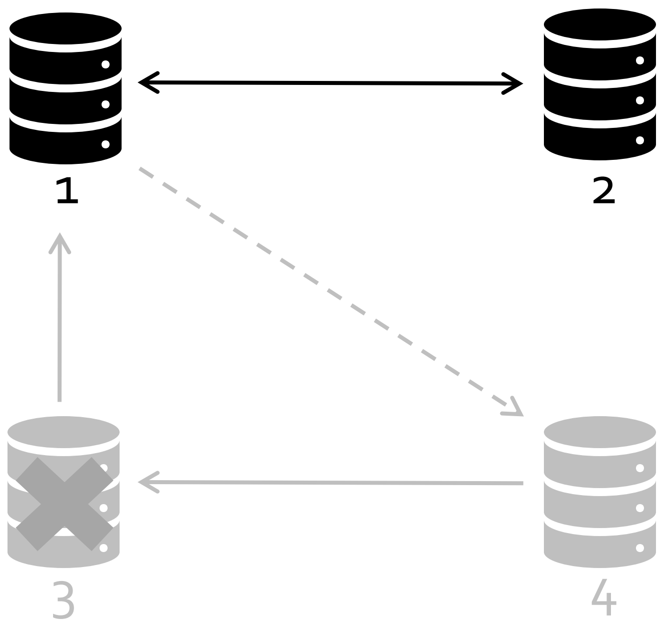
$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,\cancel{4}\}\}$

$\mathbb{S}(2) = \{\{1,2\}\}$

$\cancel{\mathbb{S}(3) = \{\{1,3\}\}}$

$\cancel{\mathbb{S}(4) = \{\{3,4\}\}}$



Given a set of faulty servers, $\mathbb{V}\text{int}$ is the biggest quorum $\mathbb{V}\text{int} \in \mathbb{Q}$ such that:

- $\forall v \in \mathbb{V}\text{int}$, v is correct,
- $\mathbb{Q}|_{\mathbb{V}\text{int}}$ has quorum intersection.

FBQS (Intact and befouled servers)

$\mathbb{V}_{int} = \{1,2\}$

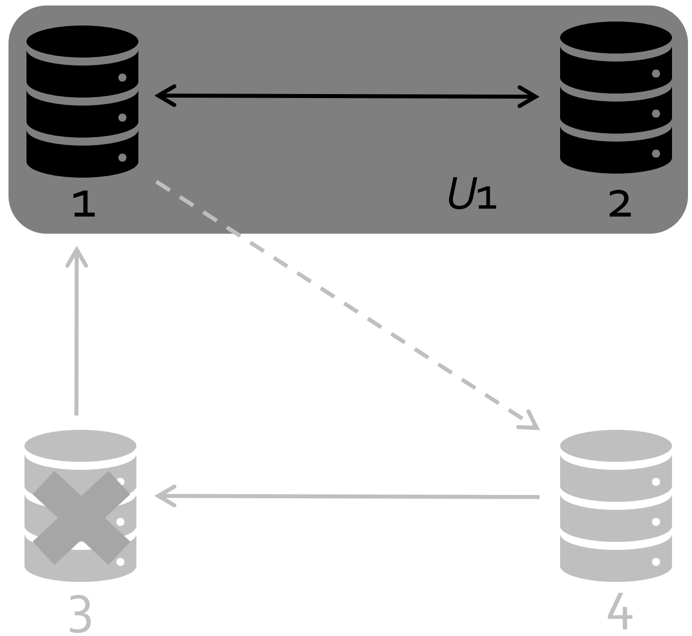
$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,\cancel{4}\}\}$

$\mathbb{S}(2) = \{\{1,2\}\}$

$\cancel{\mathbb{S}(3) = \{\{1,3\}\}}$

$\cancel{\mathbb{S}(4) = \{\{3,4\}\}}$



$U_1 = \{1,2\} \in \mathbb{Q}|_{\{1,2\}}$

Given a set of faulty servers, $\mathbb{V}_{int}$ is the biggest quorum $\mathbb{V}_{int} \in \mathbb{Q}$ such that:

- $\forall v \in \mathbb{V}_{int}$, v is correct,
- $\mathbb{Q}|_{\mathbb{V}_{int}}$ has quorum intersection.

FBQS (Intact and befouled servers)

$\mathbb{V}\text{int} = \{1,2\}$

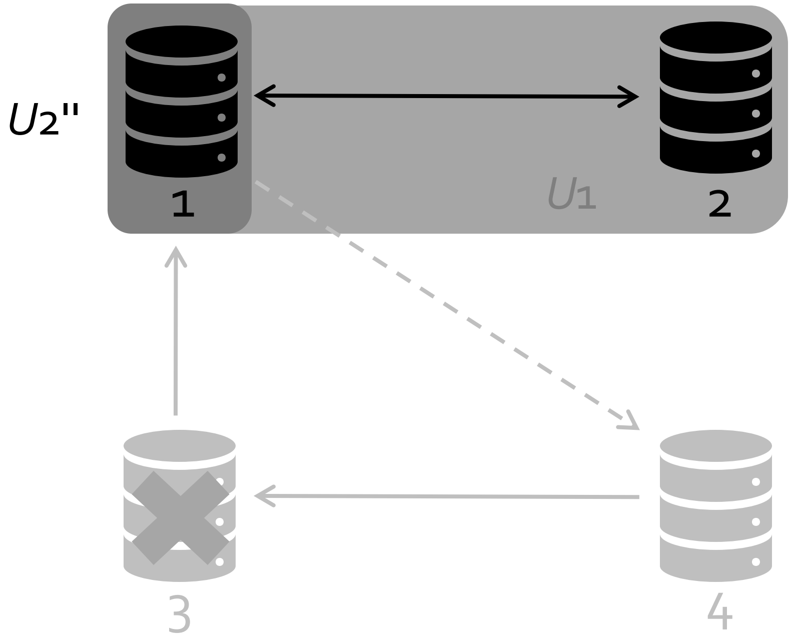
$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,\cancel{4}\}\}$

$\mathbb{S}(2) = \{\{1,2\}\}$

$\cancel{\mathbb{S}(3) = \{\{1,3\}\}}$

$\cancel{\mathbb{S}(4) = \{\{3,4\}\}}$



$U1 = \{1,2\} \in \mathbb{Q}|_{\{1,2\}}$

$U2'' = \{1\} \in \mathbb{Q}|_{\{1,2\}}$

Given a set of faulty servers, $\mathbb{V}\text{int}$ is the biggest quorum $\mathbb{V}\text{int} \in \mathbb{Q}$ such that:

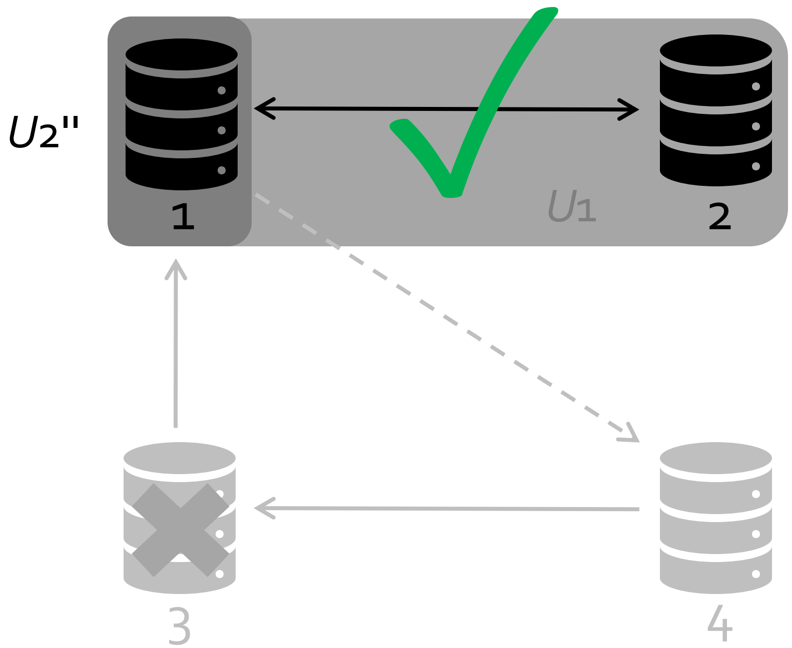
- $\forall v \in \mathbb{V}\text{int}$, v is correct,
- $\mathbb{Q}|_{\mathbb{V}\text{int}}$ has quorum intersection.

FBQS (Intact and befouled servers)

$\mathbb{V}\text{int} = \{1,2\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,\cancel{4}\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\cancel{\mathbb{S}(3) = \{\{1,3\}\}}$
$\cancel{\mathbb{S}(4) = \{\{3,4\}\}}$



$U1 = \{1,2\} \in \mathbb{Q}|_{\{1,2\}}$
$U2'' = \{1\} \in \mathbb{Q}|_{\{1,2\}}$

Given a set of faulty servers, $\mathbb{V}\text{int}$ is the biggest quorum $\mathbb{V}\text{int} \in \mathbb{Q}$ such that:

- $\forall v \in \mathbb{V}\text{int}$, v is correct,
- $\mathbb{Q}|_{\mathbb{V}\text{int}}$ has quorum intersection.

FBQS (Intact and befouled servers)

$\mathbb{V}_{\text{int}} = \{1,2\}$

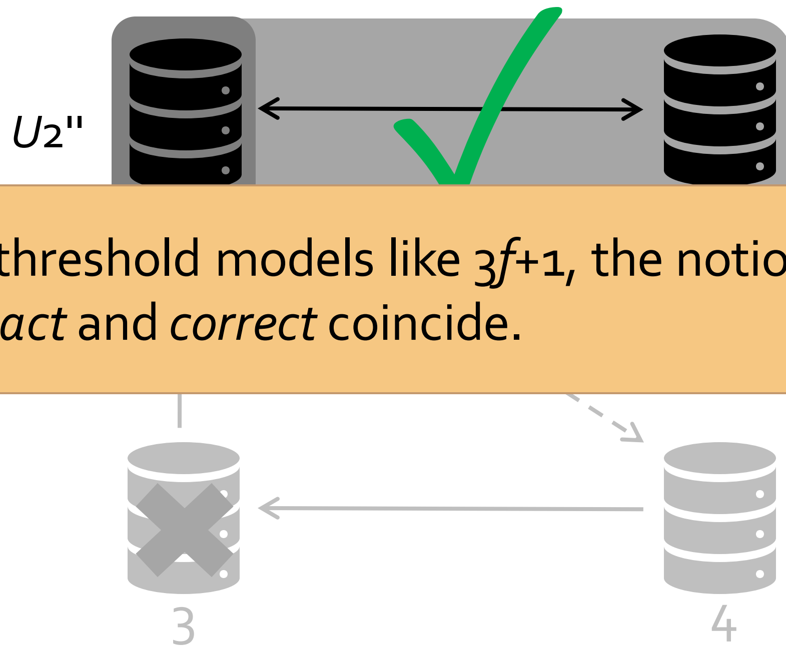
$\mathbb{S} : \mathbb{V} \to 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,\cancel{4}\}\}$

$\mathbb{S}(2) = \{\{1,2\}\}$

$\cancel{\mathbb{S}(3) = \{\{1,3\}\}}$

$\cancel{\mathbb{S}(4) = \{\{3,4\}\}}$



$U_1 = \{1,2\} \in \mathbb{Q}|_{\{1,2\}}$

$U_2'' = \{1\} \in \mathbb{Q}|_{\{1,2\}}$

In threshold models like $3f$+1, the notions of *intact* and *correct* coincide.

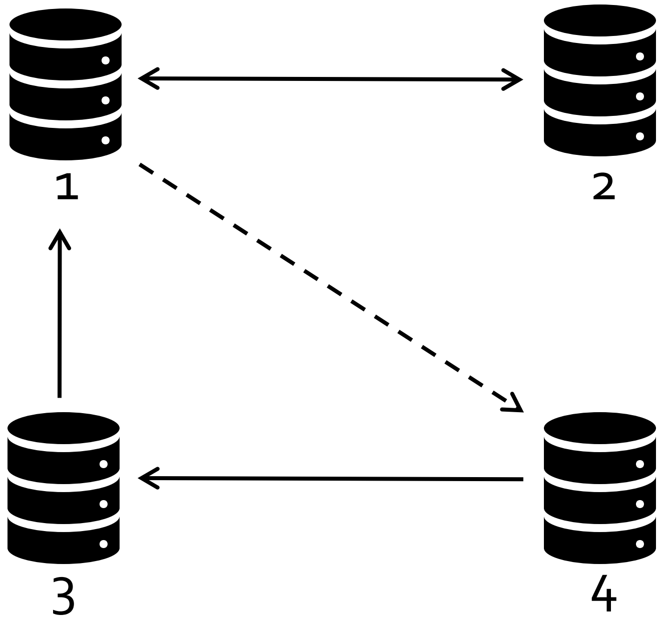
Given a set of faulty servers, $\mathbb{V}_{\text{int}}$ is the biggest quorum $\mathbb{V}_{\text{int}} \in \mathbb{Q}$ such that:

- $\forall v \in \mathbb{V}_{\text{int}}$, v is correct,
- $\mathbb{Q}|_{\mathbb{V}_{\text{int}}}$ has quorum intersection.

Mapping FBQS into DQS

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



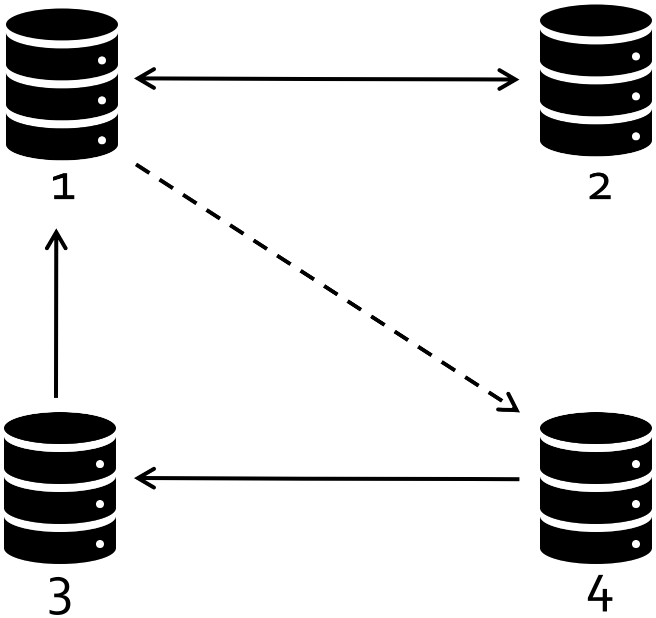
$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$
$U_4 = \{1,2,3,4\} \in \mathbb{Q}$

$B_1 = \{2\} \in \mathbb{B}$
$B_2 = \{3,4\} \in \mathbb{B}$

Mapping FBQS into DQS

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



$U_1 = \{1,2\} \in \mathbb{Q}$
$U_2 = \{1,3,4\} \in \mathbb{Q}$
$U_3 = \{1,2,3\} \in \mathbb{Q}$
$U_4 = \{1,2,3,4\} \in \mathbb{Q}$

$B_1 = \{2\} \in \mathbb{B}$
$B_2 = \{3,4\} \in \mathbb{B}$

The elements in $\mathbb{B}$ are the maximal sets whose failure leave some intact server in the system.

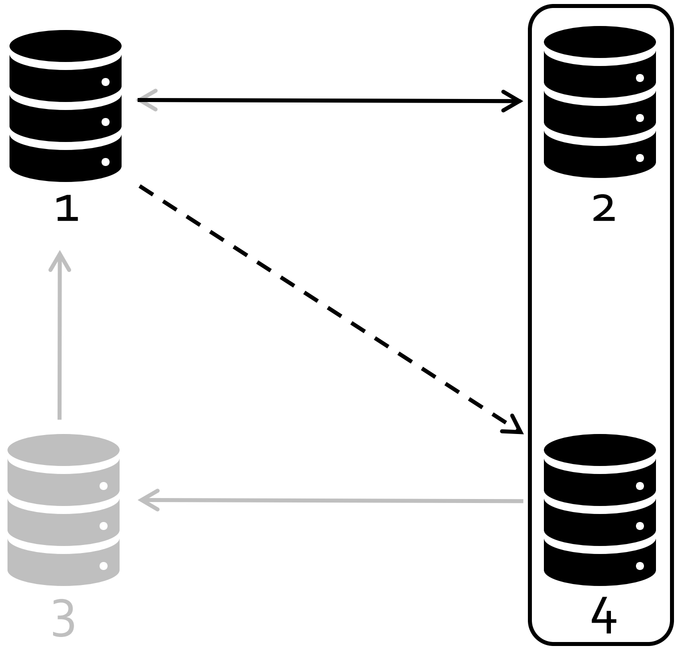
Stellar Broadcast

v-blocking mecahnism

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



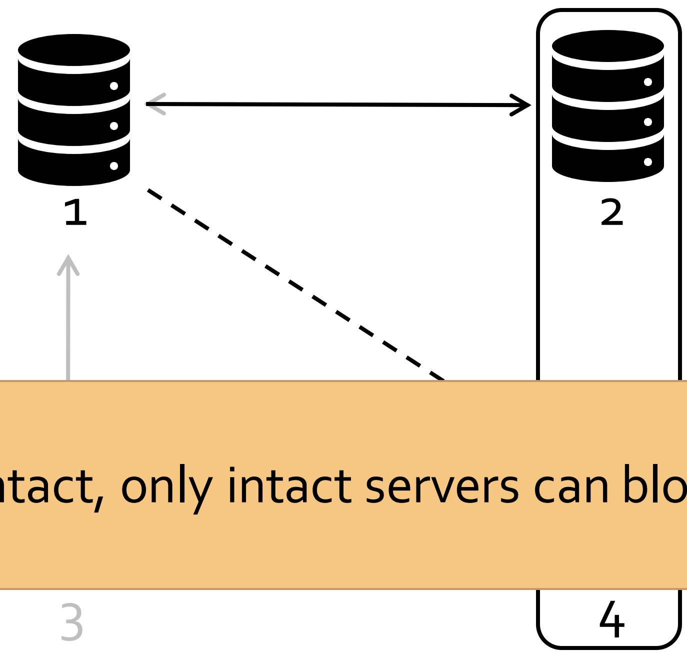
$B_1 \supseteq \{2,4\}$ is 1-blocking

v-blocking mecahnism

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



$B_1 \supseteq \{2,4\}$ is 1-blocking

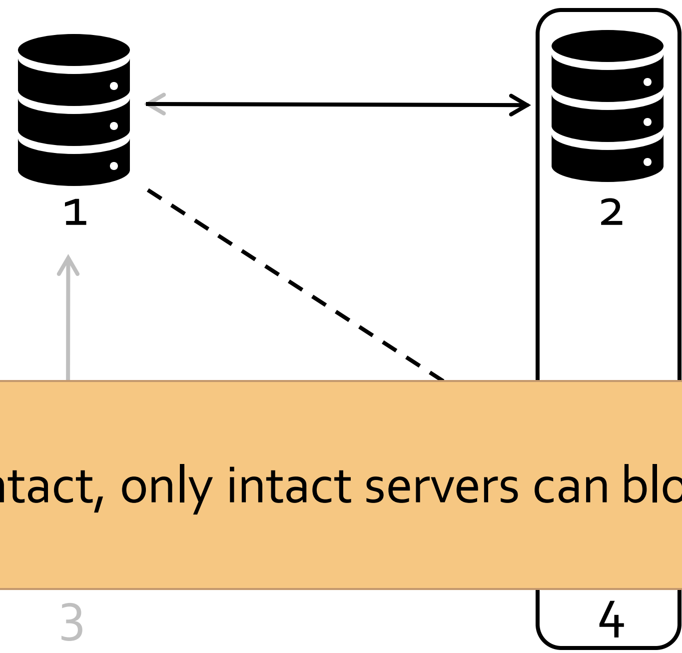
If *v* is intact, only intact servers can block *v*.

v-blocking mecahnism

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S} : \mathbb{V} \rightarrow 2^{2^{\mathbb{V}}}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$

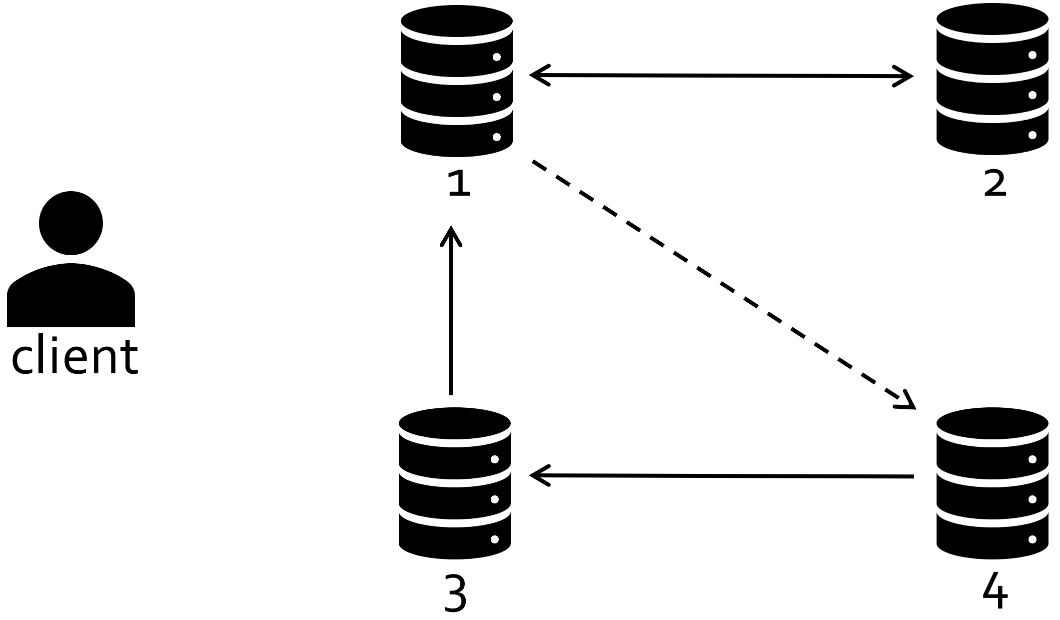


$B_1 \supseteq \{2,4\}$ is 1-blocking

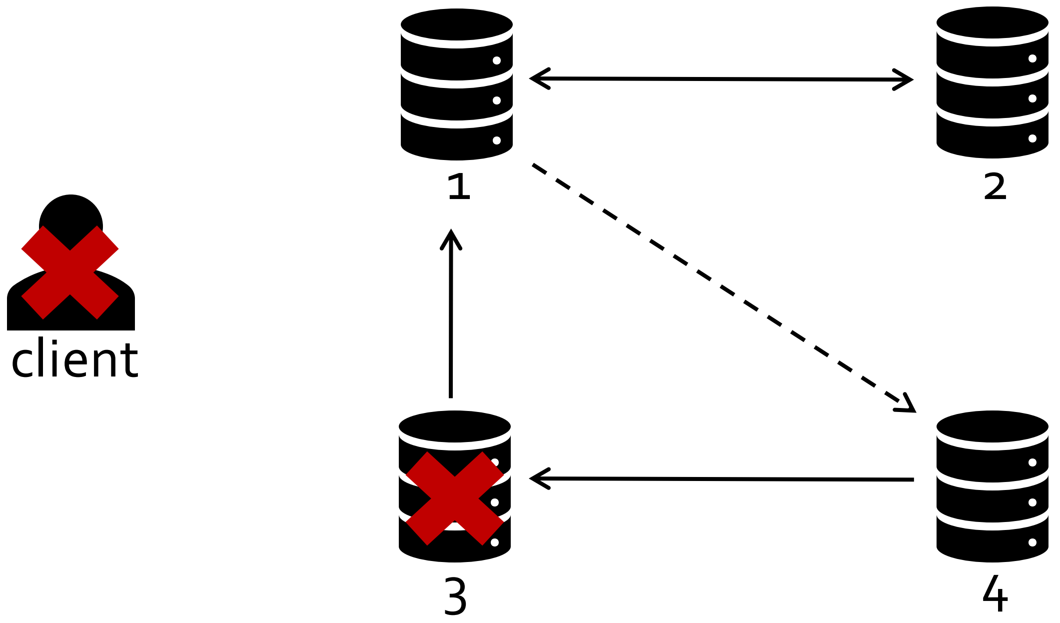
If *v* is intact, only intact servers can block *v*.

A *v*-blocking set can be computed by *v* locally!

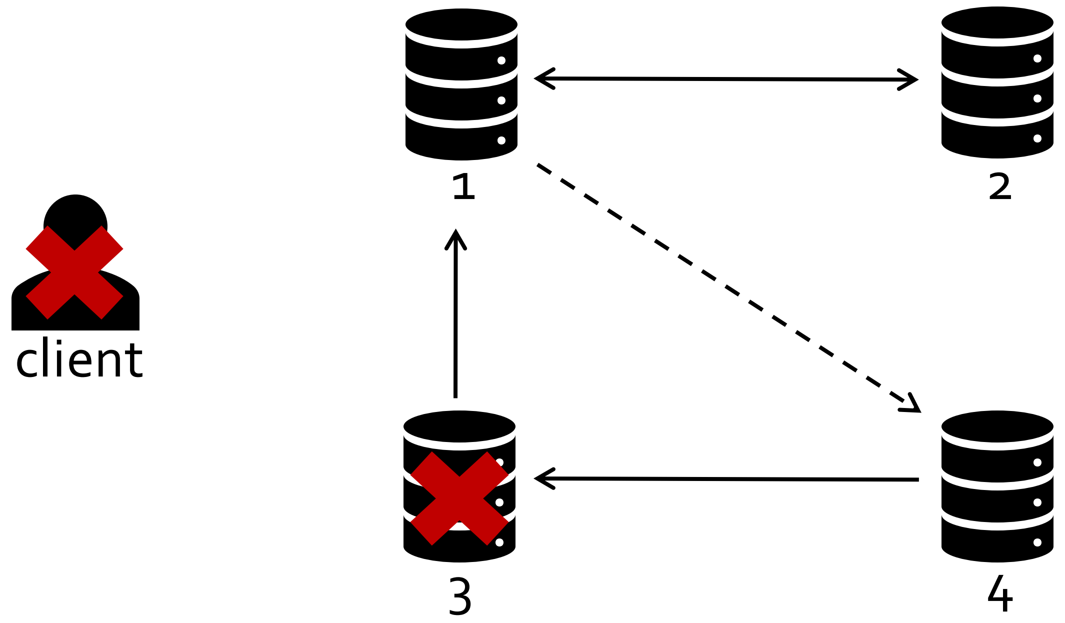
Example:



Example:



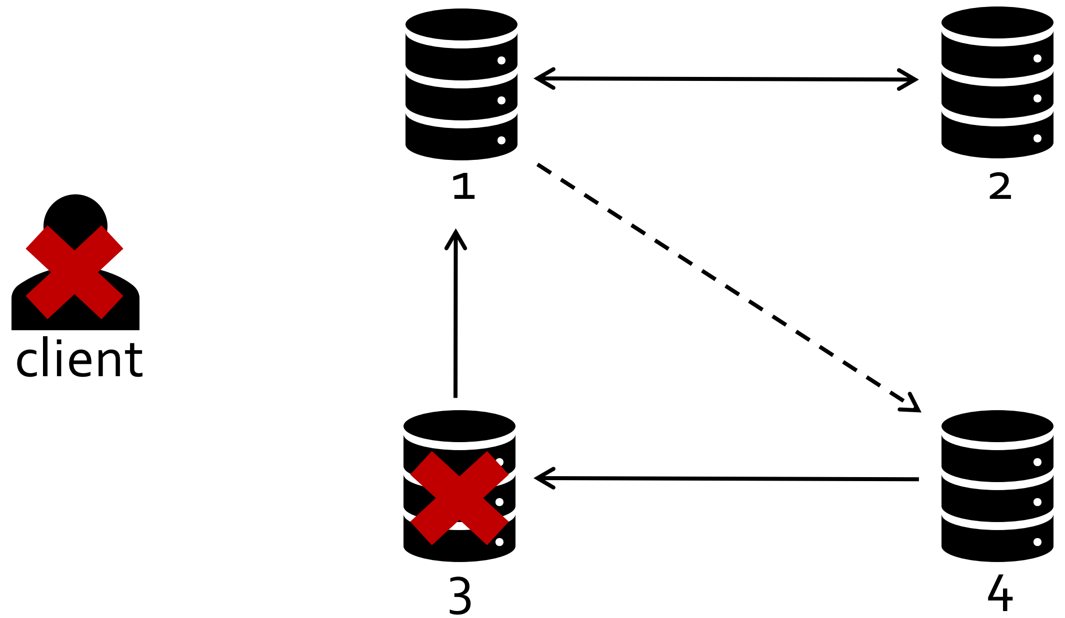
Example:



1	2	3	4
receive [BCAST a]	receive [BCAST a]		receive [BCAST b]

To broadcast a value a, the client sends [BCAST a] to every server.

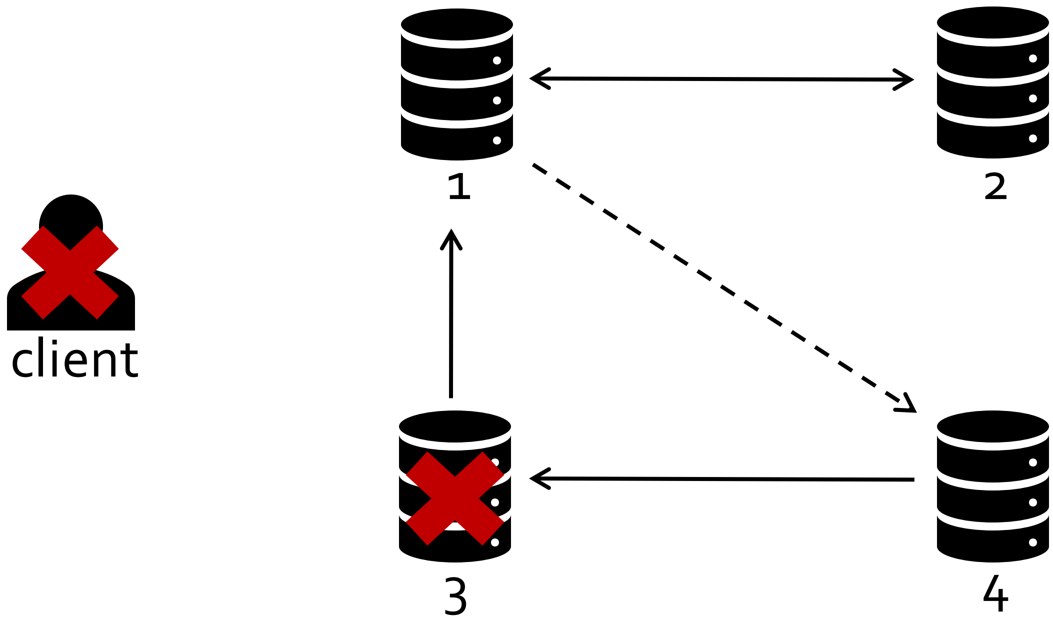
Example:



1	2	3	4
receive [BCAST a]	receive [BCAST a]		receive [BCAST b]
send [ECHO a] to all	send [ECHO a] to all		send [ECHO b] to all

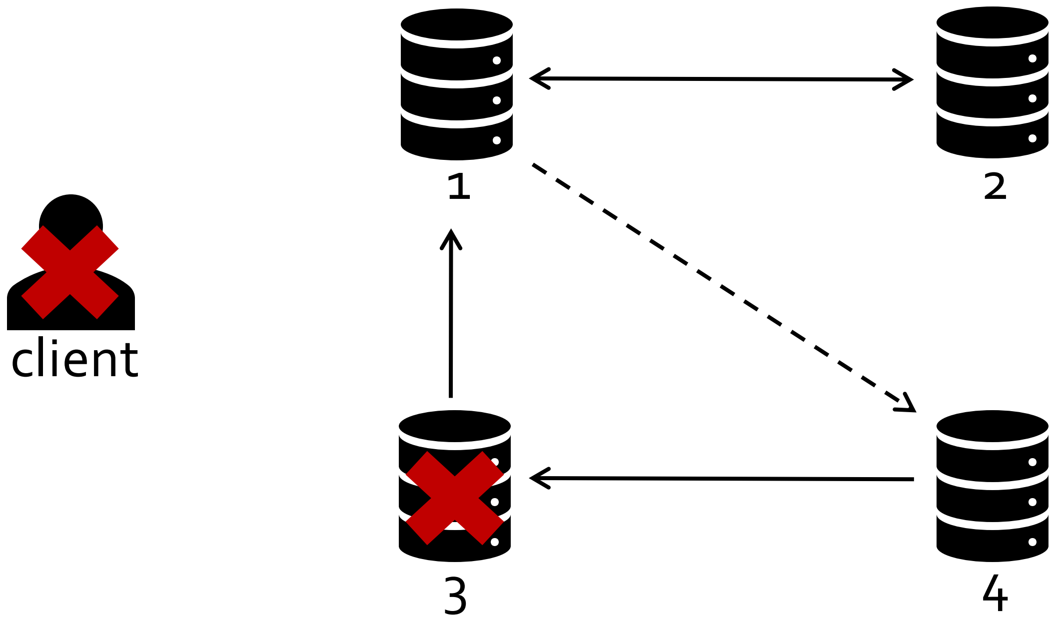
After receiving [BCAST a], a server sends [ECHO a] to every server.

Example:



1	2	3	4
receive [BCAST *a*]	receive [BCAST *a*]		receive [BCAST *b*]
send [ECHO *a*] to all	send [ECHO *a*] to all	send [READY *b*] to 4	send [ECHO *b*] to all

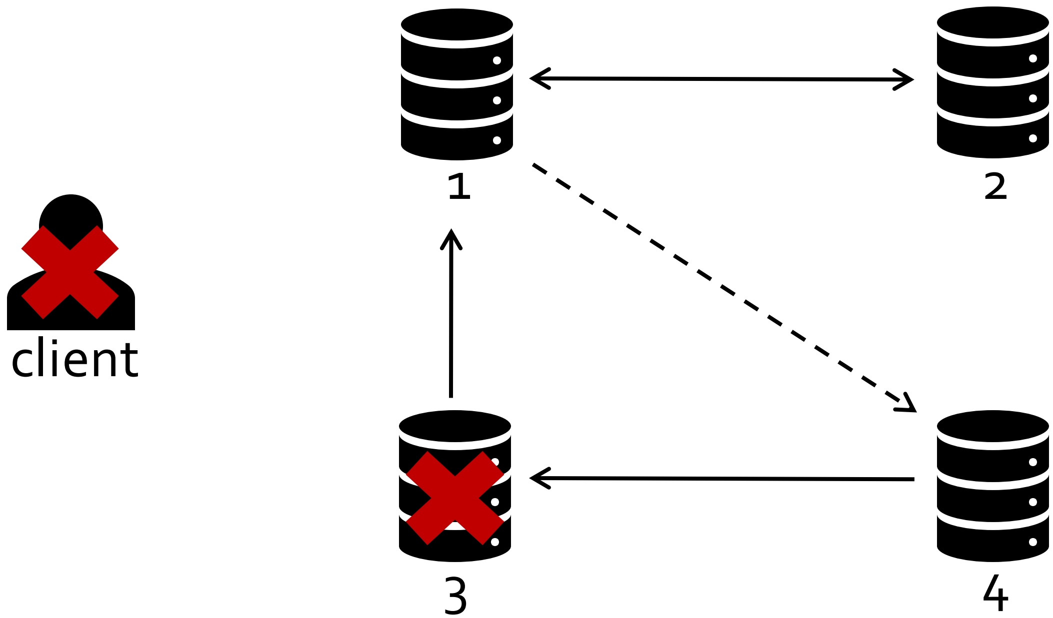
Example:



1	2	3	4
receive [BCAST a]	receive [BCAST a]		receive [BCAST b]
send [ECHO a] to all	send [ECHO a] to all	send [READY b] to 4	send [ECHO b] to all
send [READY a] to all	send [READY a] to all		

After receiving [ECHO a] from a quorum, a server sends [READY a] to every server.

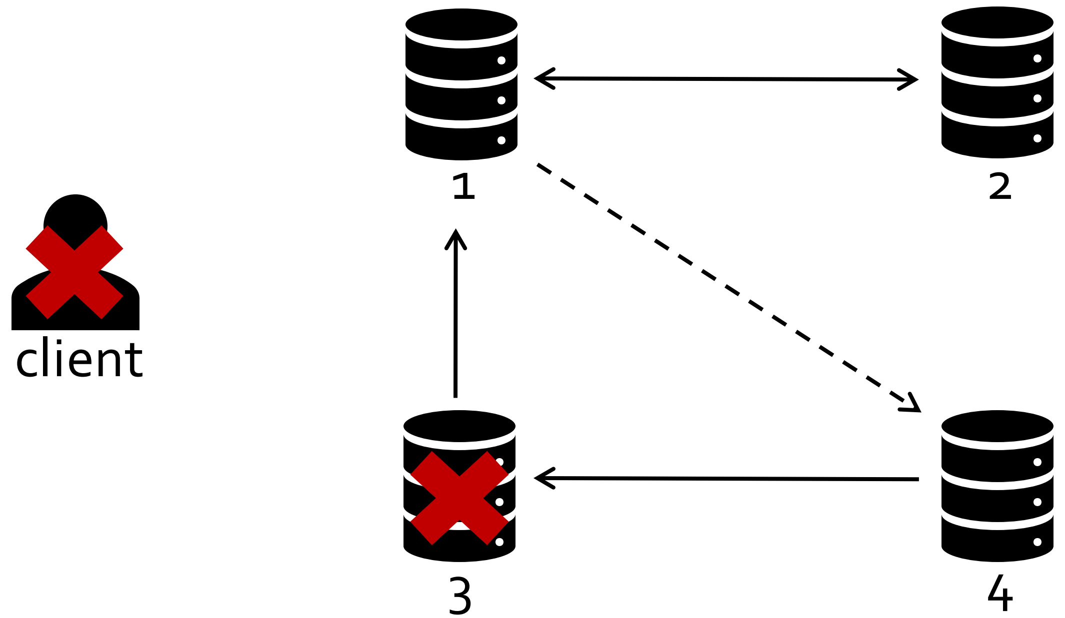
Example:



1	2	3	4
receive [BCAST *a*]	receive [BCAST *a*]		receive [BCAST *b*]
send [ECHO *a*] to all	send [ECHO *a*] to all	send [READY *b*] to 4	send [ECHO *b*] to all
send [READY *a*] to all	send [READY *a*] to all		send [READY *b*] to all

After receiving [READY *a*] from a *v*-blocking set, *v* sends [READY *a*] to every server.

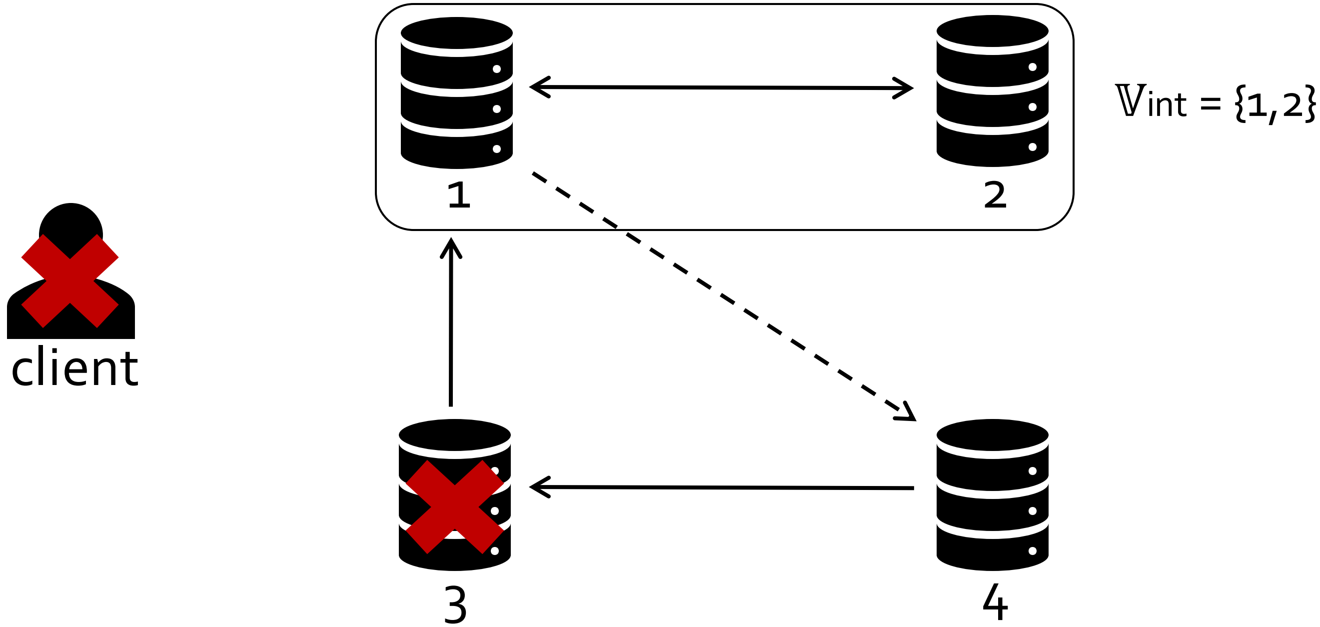
Example:



1	2	3	4
receive [BCAST *a*]	receive [BCAST *a*]		receive [BCAST *b*]
send [ECHO *a*] to all	send [ECHO *a*] to all	send [READY *b*] to 4	send [ECHO *b*] to all
send [READY *a*] to all	send [READY *a*] to all		send [READY *b*] to all
deliver(*a*)	deliver(*a*)		

After receiving [READY *a*] from a quorum, a server delivers value *a*.

Example:



1	2	3	4
receive [BCAST *a*]	receive [BCAST *a*]		receive [BCAST *b*]
send [ECHO *a*] to all	send [ECHO *a*] to all	send [READY *b*] to 4	send [ECHO *b*] to all
send [READY *a*] to all	send [READY *a*] to all		send [READY *b*] to all
deliver(*a*)	deliver(*a*)		

After receiving [READY *a*] from a quorum, a server delivers value *a*.

Weakly reliable Byzantine broadcast

Stellar broadcast satisfies the specification of weakly reliable Byzantine broadcast when the faulty servers leave at least one intact server:

- ***Safety:*** If some correct server delivers a value *a* and another correct server delivers a value *b*, then *a* = *b*.
- ***Liveness:*** If a correct server delivers a value, then every intact server eventually delivers a value.

Weakly reliable Byzantine broadcast

Stellar broadcast satisfies the specification of weakly reliable Byzantine broadcast when the faulty servers leave at least one intact server:

- ***Safety:*** If some correct server delivers a value a and another correct server delivers a value b, then $a = b$.
- ***Liveness:*** If a correct server delivers a value, then every intact server eventually delivers a value.

Weakly reliable Byzantine broadcast

Stellar broadcast satisfies the specification of weakly reliable Byzantine broadcast when the faulty servers leave at least one intact server:

- ***Safety:*** If some correct server delivers a value *a* and another correct server delivers a value *b*, then *a* = *b*.
- ***Liveness:*** If a correct server delivers a value, then every intact server eventually delivers a value.

Trade-off: operating on local information weakens the liveness properties to intact servers

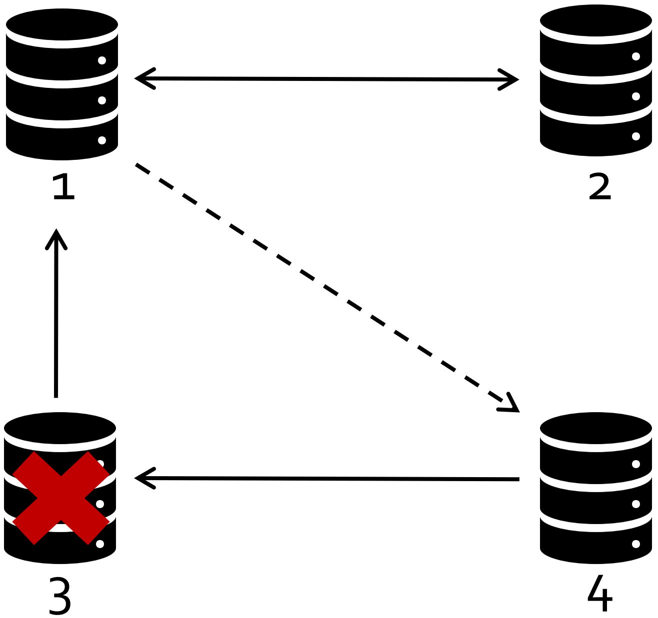
Subjective FBQS

Subjective FBQS

$\mathbb{V} = \{1,2,3,4\}$

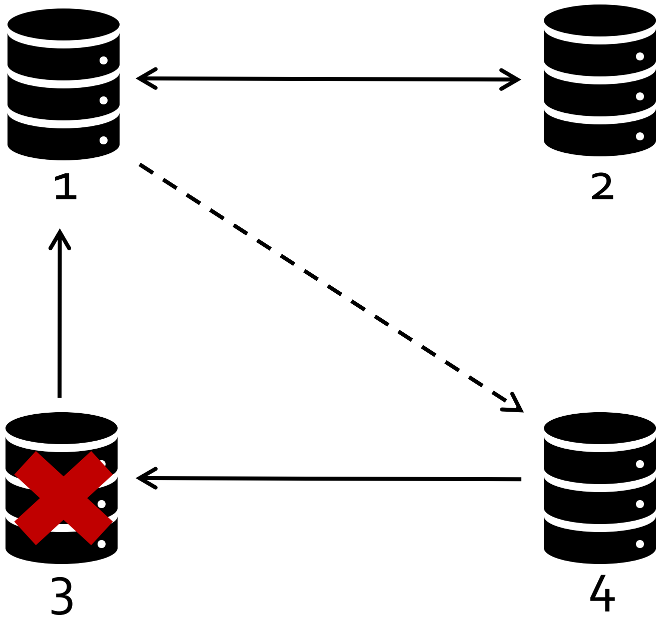
$\mathbb{S} : \mathbb{V} \longrightarrow 2^{2^{\mathbb{V}}} \setminus \{\emptyset\}$

$\mathbb{S}(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}(2) = \{\{1,2\}\}$
$\mathbb{S}(3) = \{\{1,3\}\}$
$\mathbb{S}(4) = \{\{3,4\}\}$



Subjective FBQS

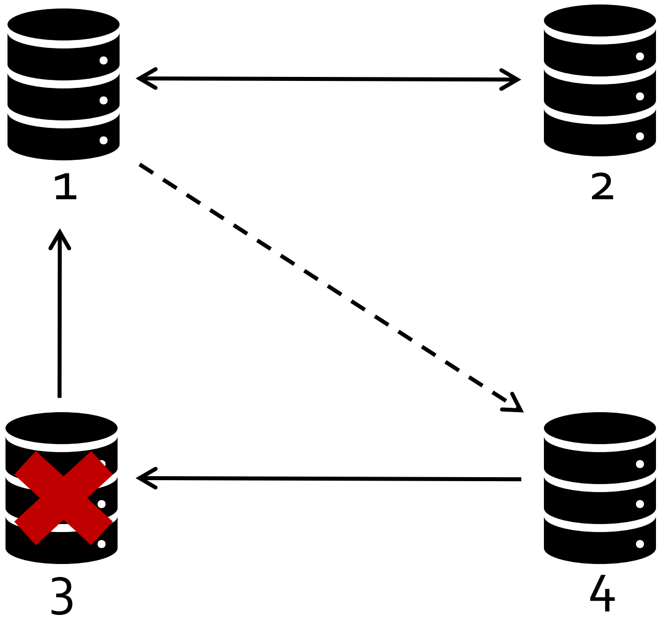
$\mathbb{V} = \{1,2,3,4\}$



Subjective FBQS

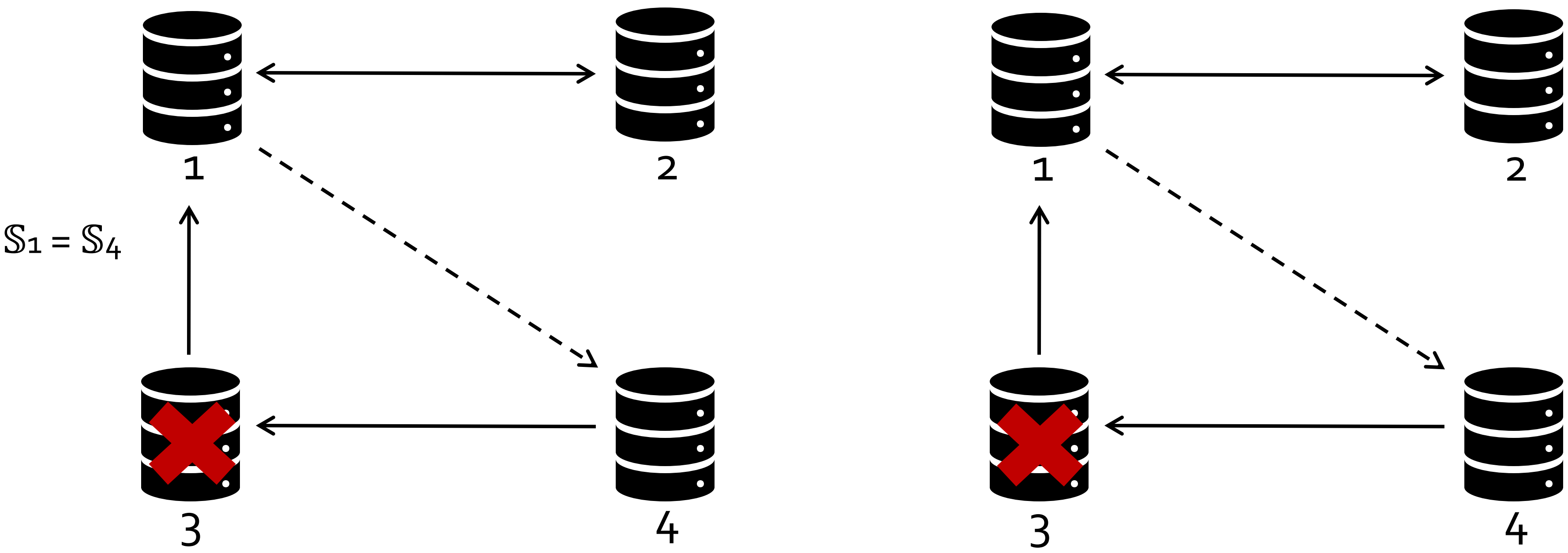
$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S}_1 = \mathbb{S}_4$



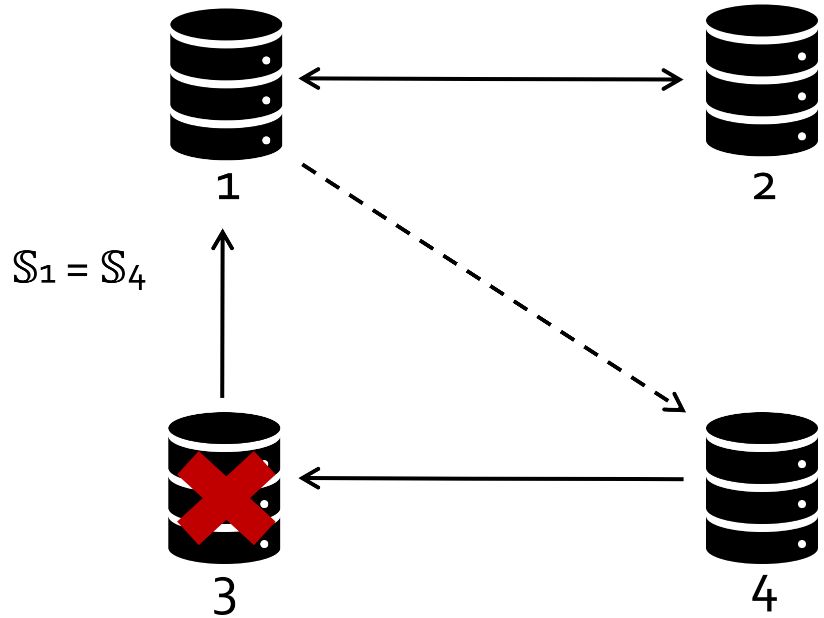
Subjective FBQS

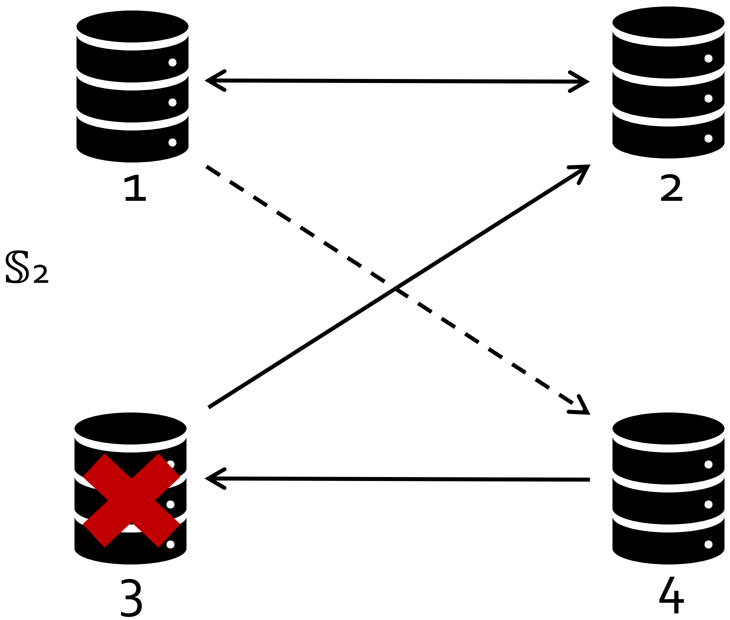
$\mathbb{V} = \{1,2,3,4\}$



Subjective FBQS

$\mathbb{V} = \{1,2,3,4\}$

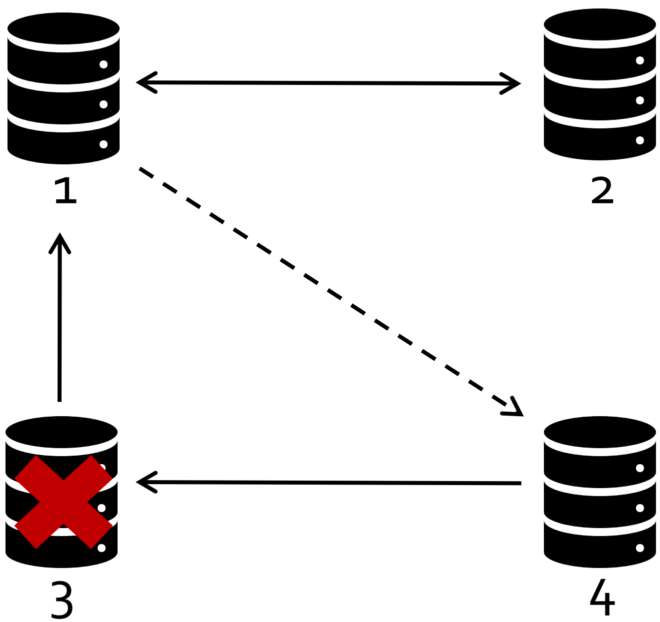




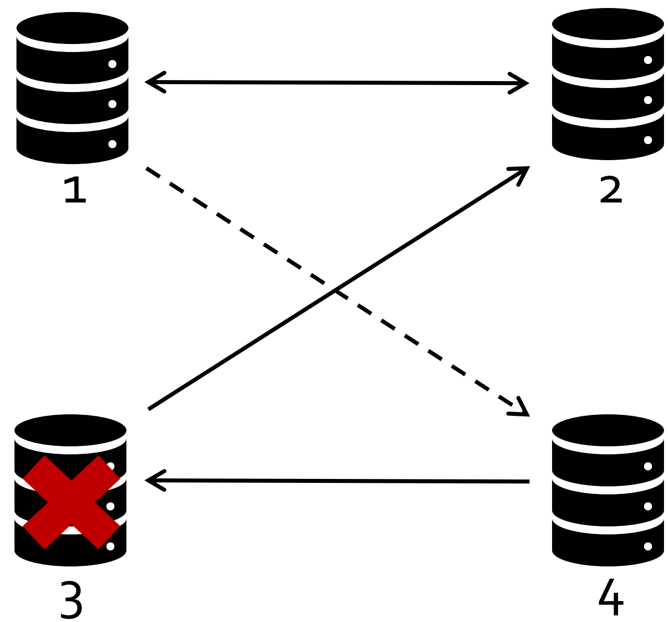
Subjective FBQS

$\mathbb{V} = \{1,2,3,4\}$

$\mathbb{S}_1 = \mathbb{S}_4$



$\mathbb{S}_2$

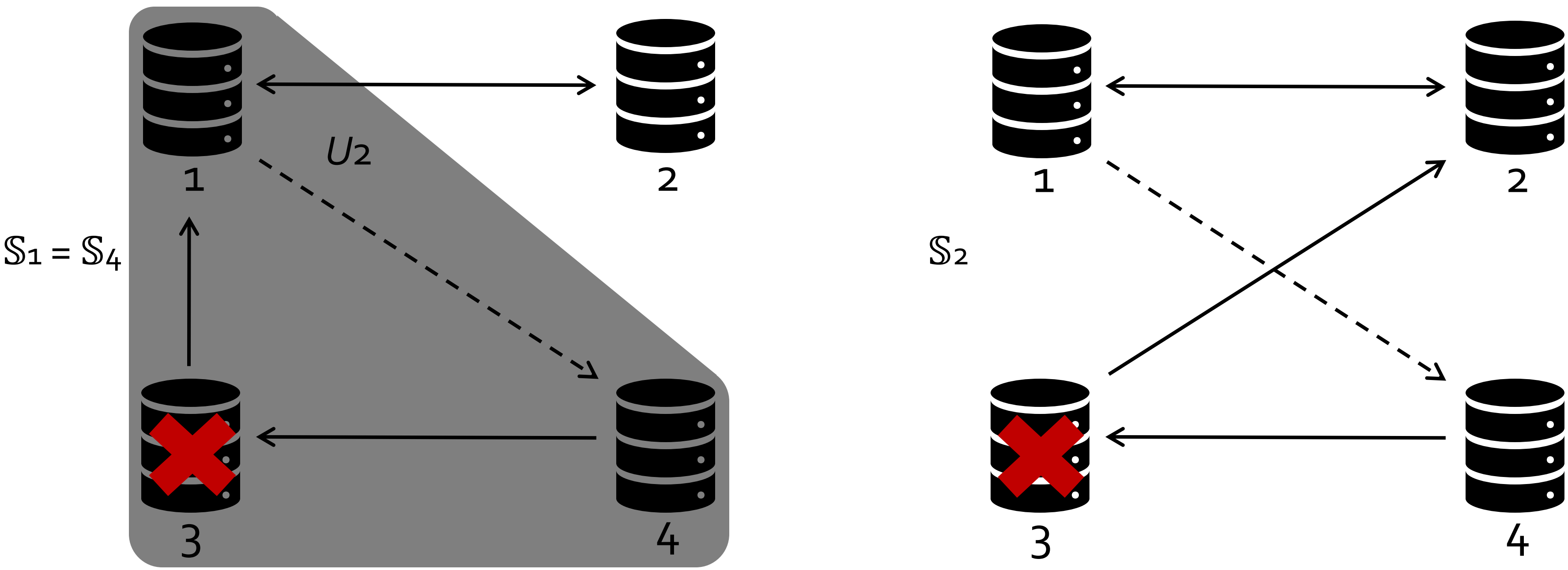


$\mathbb{S}_1(1) = \mathbb{S}_4(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_1(2) = \mathbb{S}_4(2) = \{\{1,2\}\}$
$\mathbb{S}_1(3) = \mathbb{S}_4(3) = \{\{1,3\}\}$
$\mathbb{S}_1(4) = \mathbb{S}_4(4) = \{\{3,4\}\}$

$\mathbb{S}_2(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_2(2) = \{\{1,2\}\}$
$\mathbb{S}_2(3) = \{\{2,3\}\}$
$\mathbb{S}_2(4) = \{\{3,4\}\}$

Subjective FBQS

$\mathbb{V} = \{1,2,3,4\}$

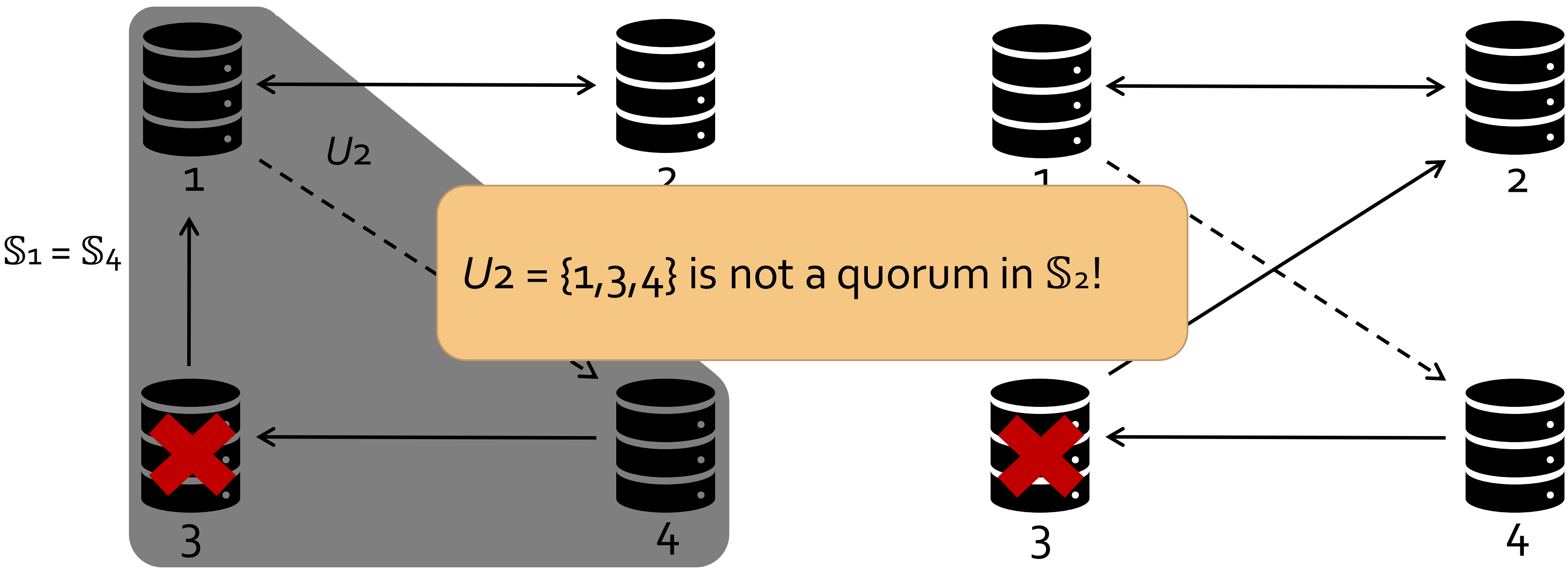


$\mathbb{S}_1(1) = \mathbb{S}_4(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_1(2) = \mathbb{S}_4(2) = \{\{1,2\}\}$
$\mathbb{S}_1(3) = \mathbb{S}_4(3) = \{\{1,3\}\}$
$\mathbb{S}_1(4) = \mathbb{S}_4(4) = \{\{3,4\}\}$

$\mathbb{S}_2(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_2(2) = \{\{1,2\}\}$
$\mathbb{S}_2(3) = \{\{2,3\}\}$
$\mathbb{S}_2(4) = \{\{3,4\}\}$

Subjective FBQS

$\mathbb{V} = \{1,2,3,4\}$



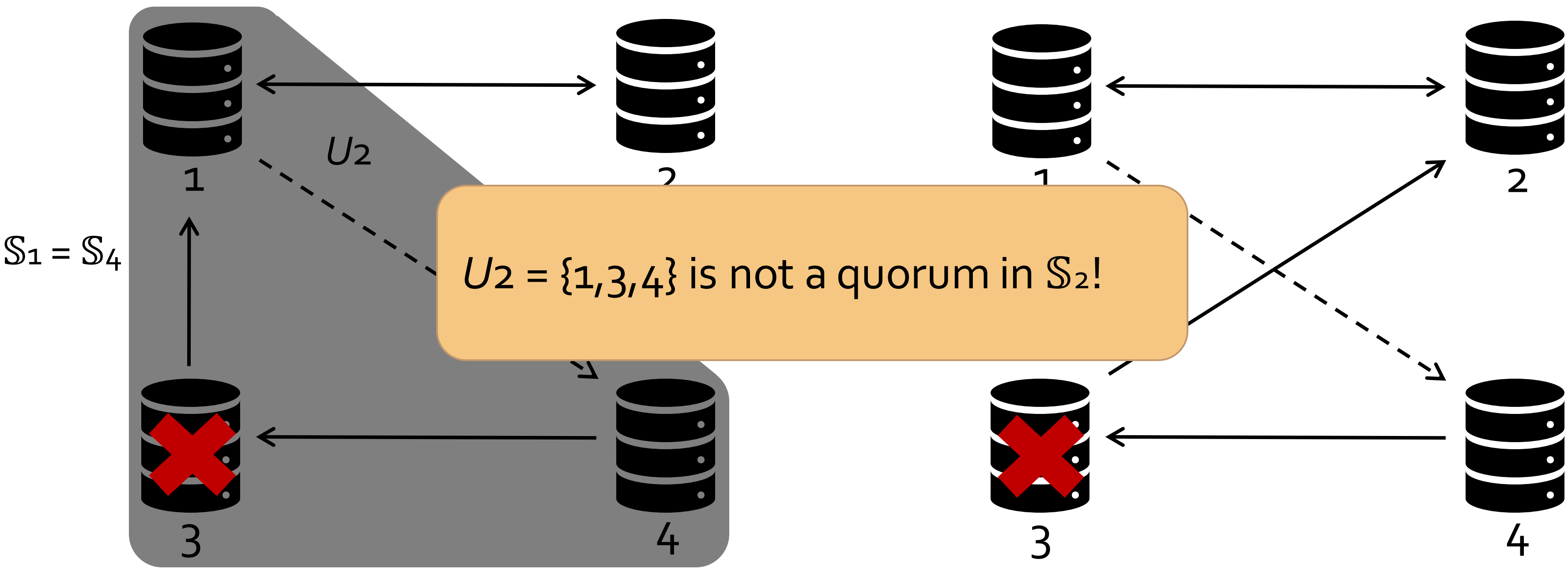
$U_2 = \{1,3,4\}$ is not a quorum in $\mathbb{S}_2$!

$\mathbb{S}_1(1) = \mathbb{S}_4(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_1(2) = \mathbb{S}_4(2) = \{\{1,2\}\}$
$\mathbb{S}_1(3) = \mathbb{S}_4(3) = \{\{1,3\}\}$
$\mathbb{S}_1(4) = \mathbb{S}_4(4) = \{\{3,4\}\}$

$\mathbb{S}_2(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_2(2) = \{\{1,2\}\}$
$\mathbb{S}_2(3) = \{\{2,3\}\}$
$\mathbb{S}_2(4) = \{\{3,4\}\}$

Subjective FBQS

$\mathbb{V} = \{1,2,3,4\}$



$\mathbb{S}_1(1) = \mathbb{S}_4(1) = \{\{1,2\},\{1,4\}\}$

$\mathbb{S}_1(2) = \mathbb{S}_4(2) = \{\{1,2\}\}$

~~$\mathbb{S}_1(3) = \mathbb{S}_4(3) = \{\{1,3\}\}$~~

$\mathbb{S}_1(4) = \mathbb{S}_4(4) = \{\{3,4\}\}$

$\mathbb{S}_2(1) = \{\{1,2\},\{1,4\}\}$

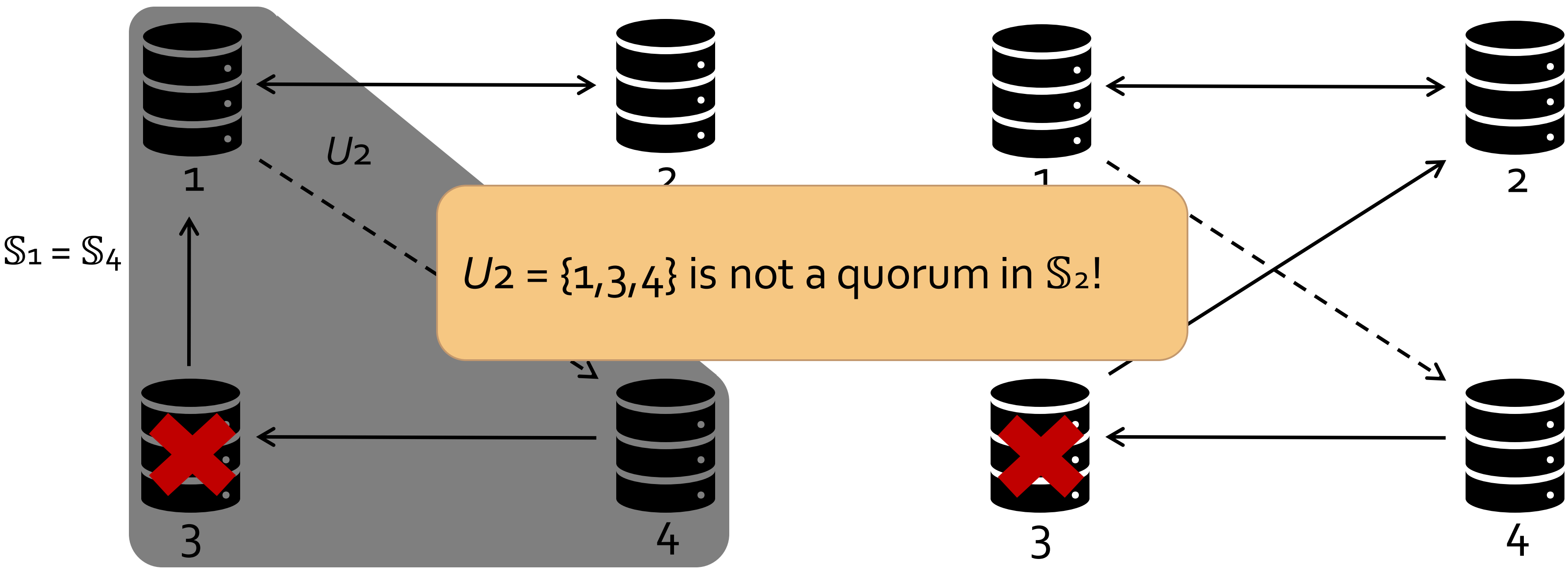
$\mathbb{S}_2(2) = \{\{1,2\}\}$

~~$\mathbb{S}_2(3) = \{\{2,3\}\}$~~

$\mathbb{S}_2(4) = \{\{3,4\}\}$

Subjective FBQS

$\mathbb{V} = \{1,2,3,4\}$

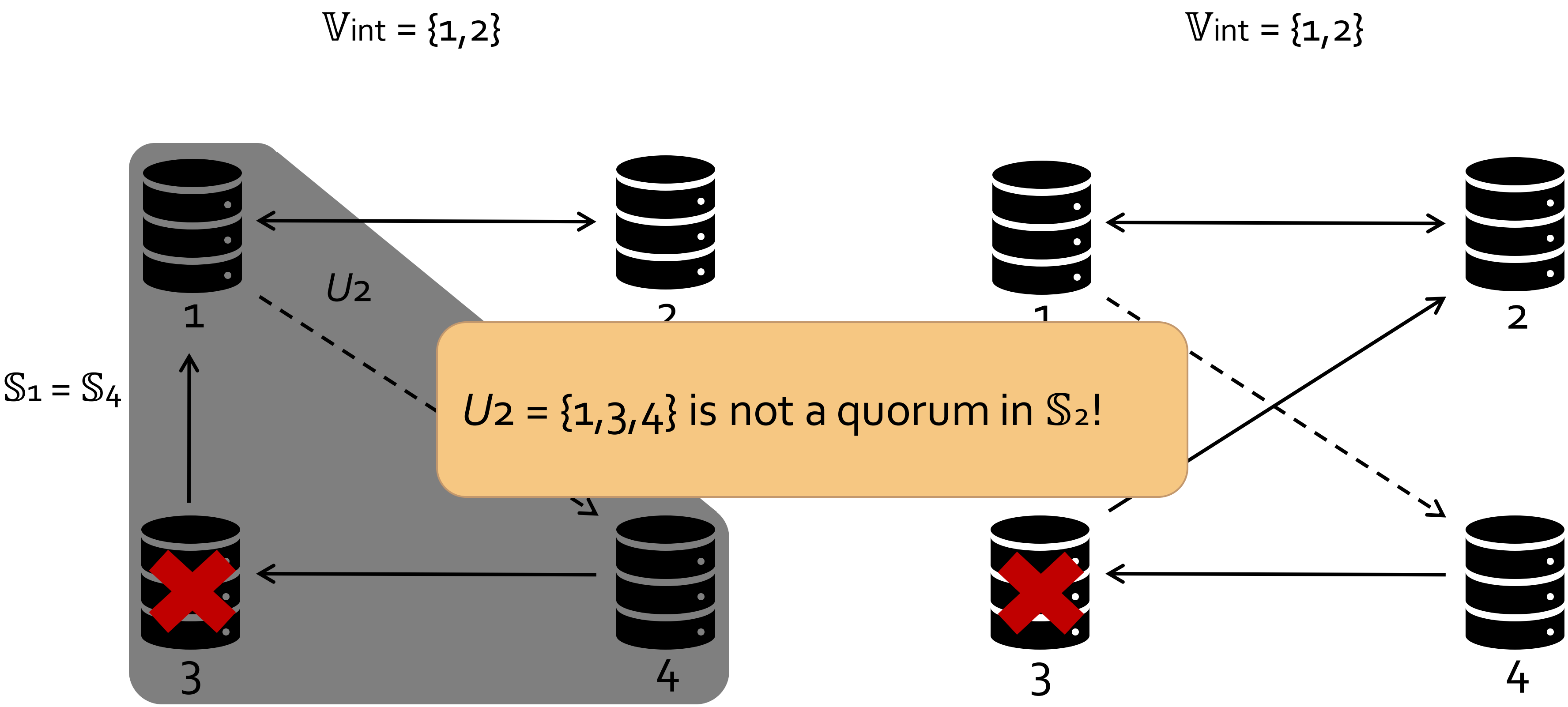


$\mathbb{S}_1(1) = \mathbb{S}_4(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_1(2) = \mathbb{S}_4(2) = \{\{1,2\}\}$
$\cancel{\mathbb{S}_1(3) = \mathbb{S}_4(3) = \{\{1,3\}\}}$
$\mathbb{S}_1(4) = \mathbb{S}_4(4) = \{\{3,4\}\}$

$=$

$\mathbb{S}_2(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_2(2) = \{\{1,2\}\}$
$\cancel{\mathbb{S}_2(3) = \{\{2,3\}\}}$
$\mathbb{S}_2(4) = \{\{3,4\}\}$

Subjective FBQS

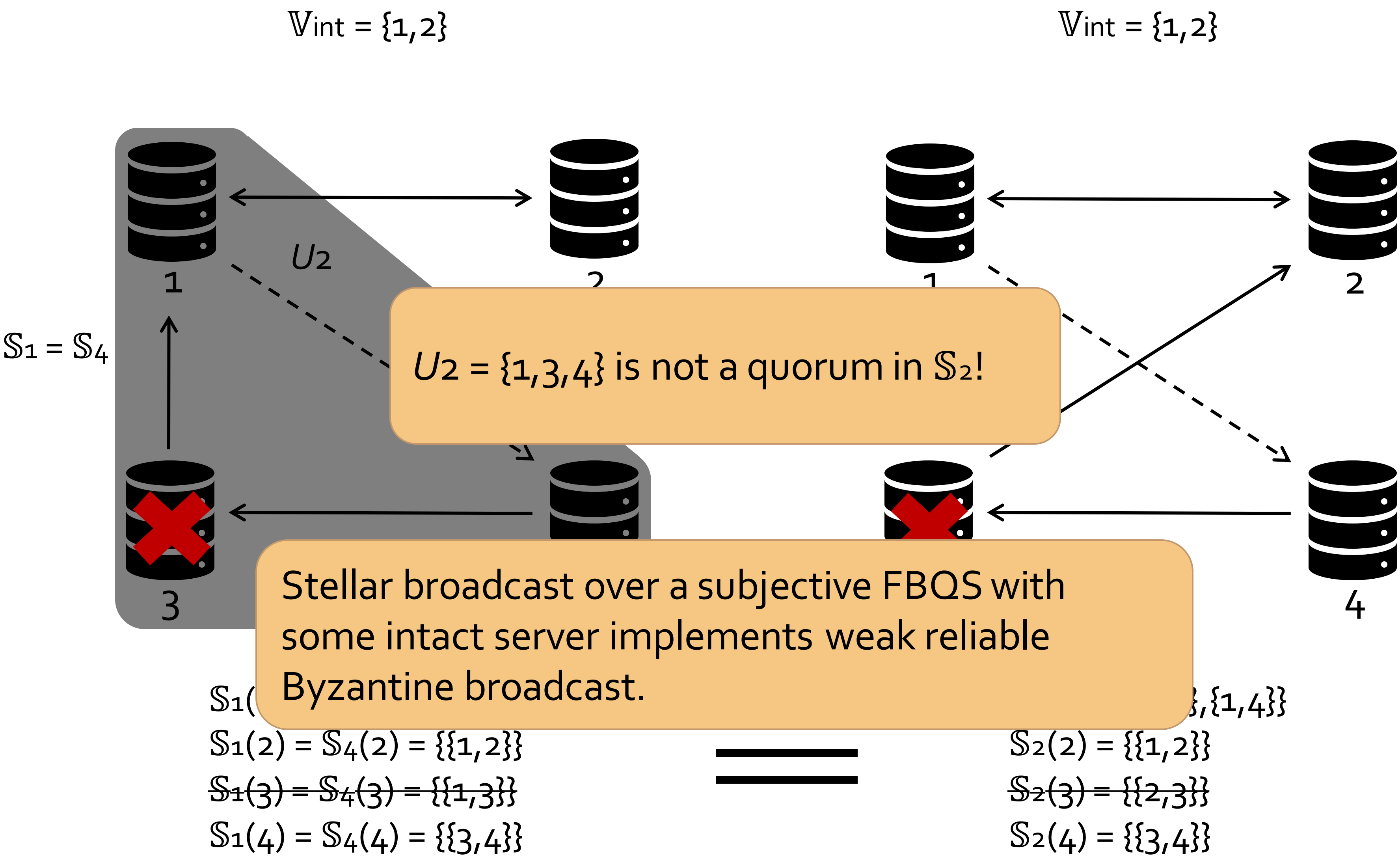


$\mathbb{S}_1(1) = \mathbb{S}_4(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_1(2) = \mathbb{S}_4(2) = \{\{1,2\}\}$
$\cancel{\mathbb{S}_1(3) = \mathbb{S}_4(3) = \{\{1,3\}\}}$
$\mathbb{S}_1(4) = \mathbb{S}_4(4) = \{\{3,4\}\}$

=

$\mathbb{S}_2(1) = \{\{1,2\},\{1,4\}\}$
$\mathbb{S}_2(2) = \{\{1,2\}\}$
$\cancel{\mathbb{S}_2(3) = \{\{2,3\}\}}$
$\mathbb{S}_2(4) = \{\{3,4\}\}$

Subjective FBQS



$U_2 = \{1,3,4\}$ is not a quorum in $\mathbb{S}_2$!

Stellar broadcast over a subjective FBQS with some intact server implements weak reliable Byzantine broadcast.

Work in progress

- Proof of correctness of the whole Stellar consensus protocol.
- Relation between Stellar consensus and existing BFT algorithms.

Conclusions

- An FBQS maps into a DQS, so off-the-shelf DQS algorithms can be run over FBQS:
  - Trade-off between servers relying on global/local information and liveness properties for correct/intact servers.
- If the set of intact servers coincides with the set of correct servers, then Stellar broadcast and Bracha broadcast are observtionally equivalent.
- We prove Stellar broadcast correct when servers lie about their slices.

Conclusions

- An FBQS maps into a DQS, so off-the-shelf DQS algorithms can be run over FBQS:
  - Trade-off between servers relying on global/local information and liveness properties for correct/intact servers.
- If the set of intact servers coincides with the set of correct servers, then Stellar broadcast and Bracha broadcast are observtionally equivalent.
- We prove Stellar broadcast correct when servers lie about their slices.

Thanks!