# Player-Centric Byzantine Agreement

**Vassilis Zikas**

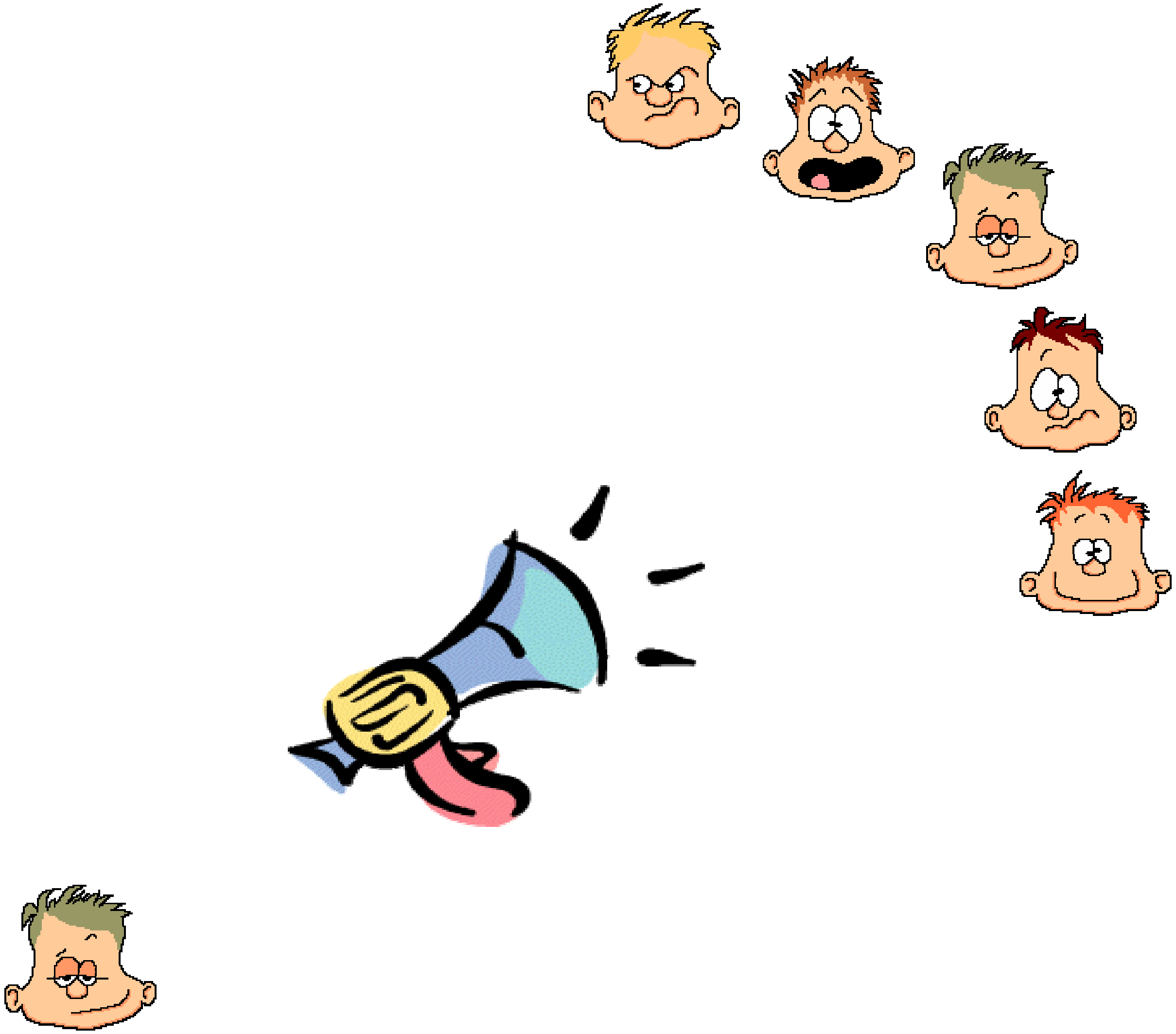
joint work with Martin Hirt

ETH Zurich

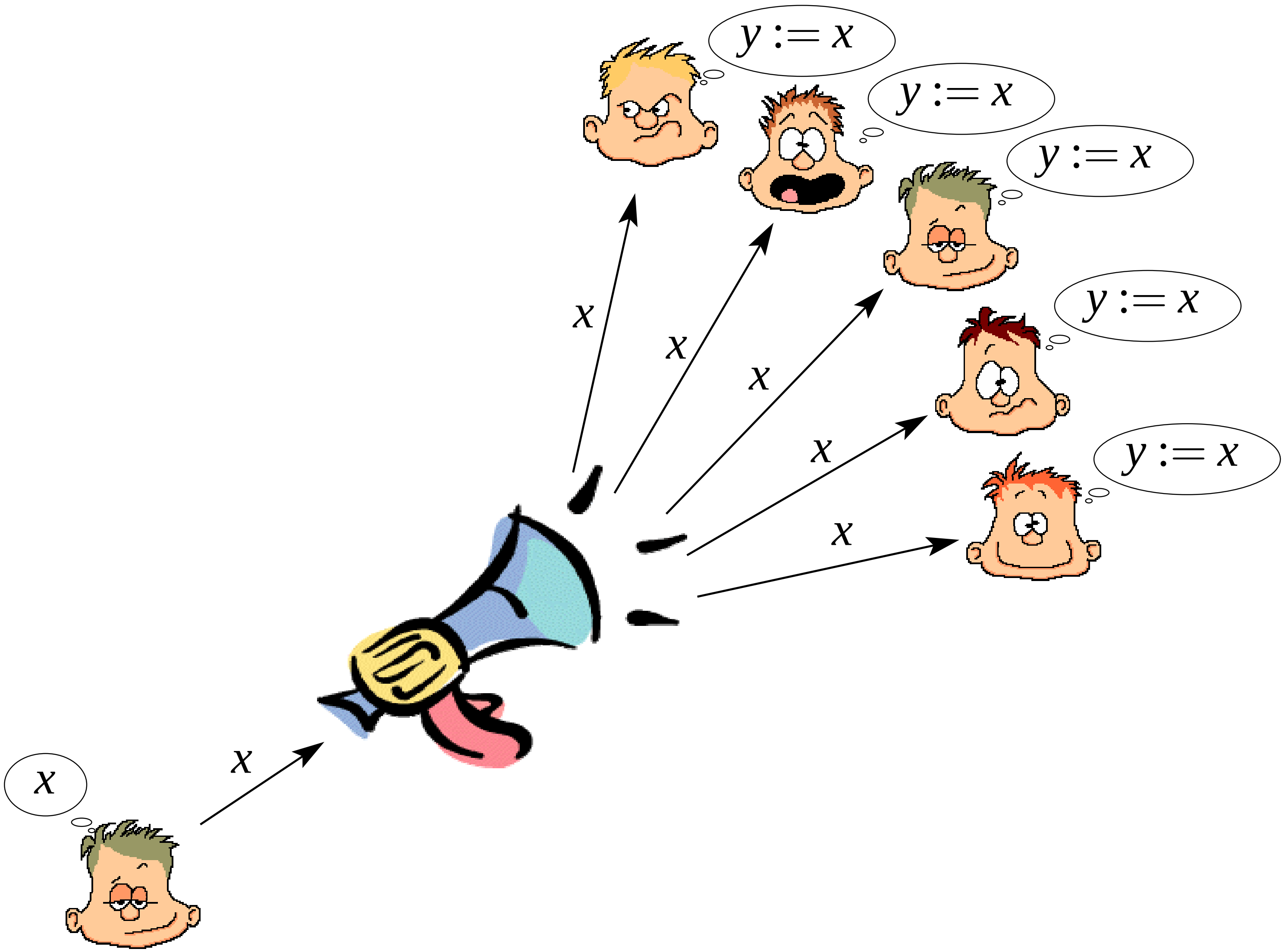
Rump Session

EUROCRYPT 2010

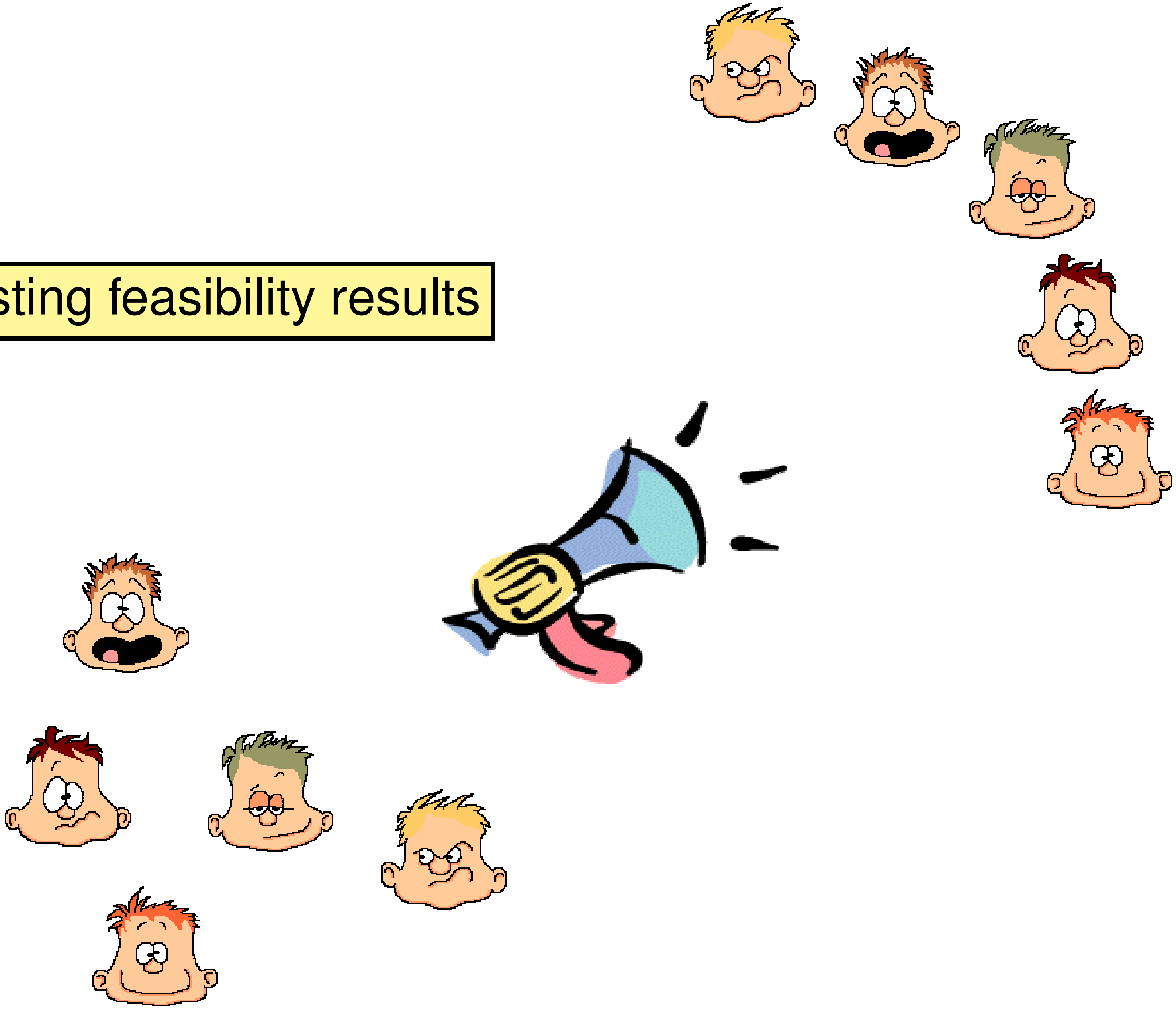
# BA Variant 1: Broadcast



# BA Variant 1: Broadcast

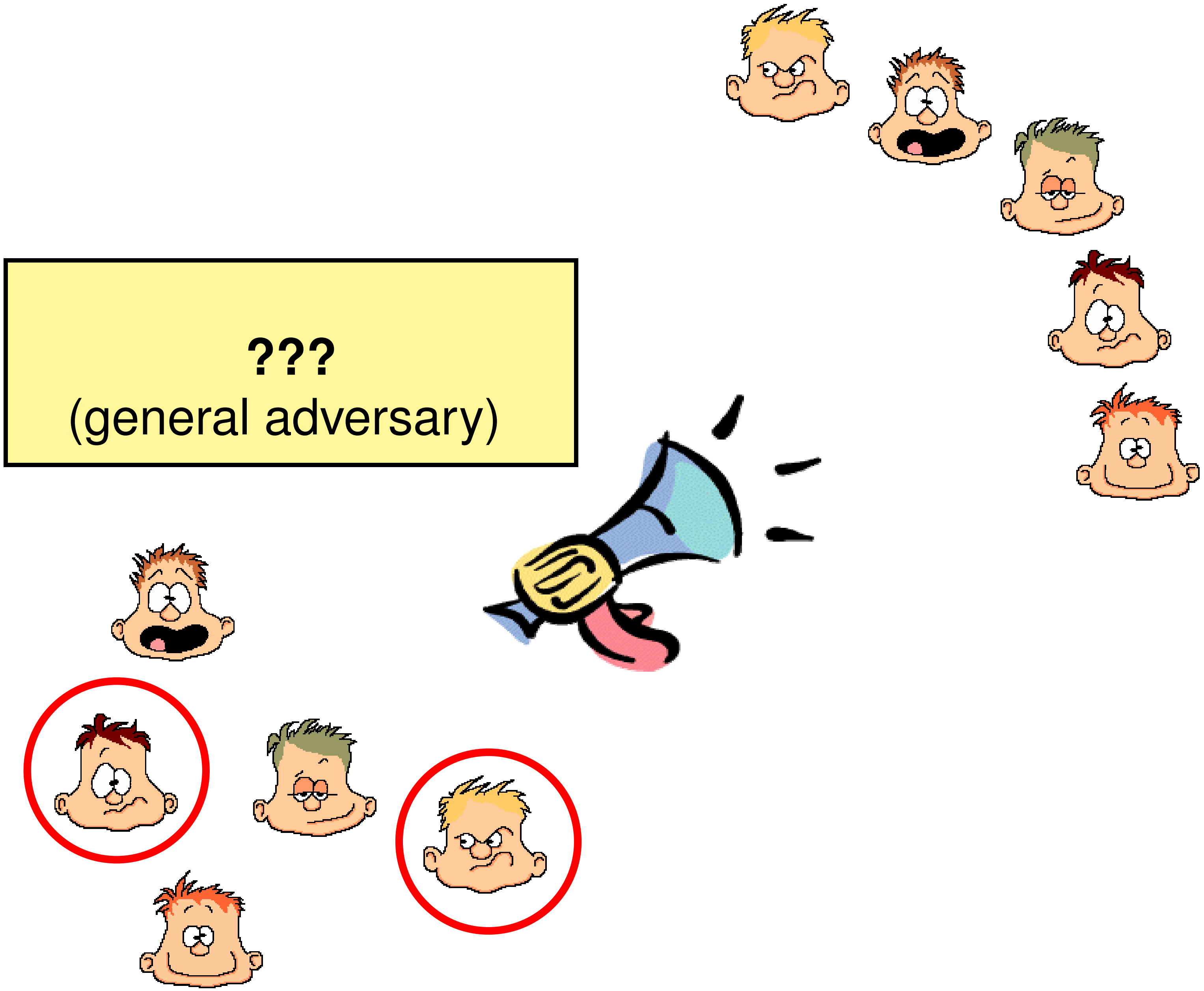


# BA Variant 1: Broadcast



Existing feasibility results

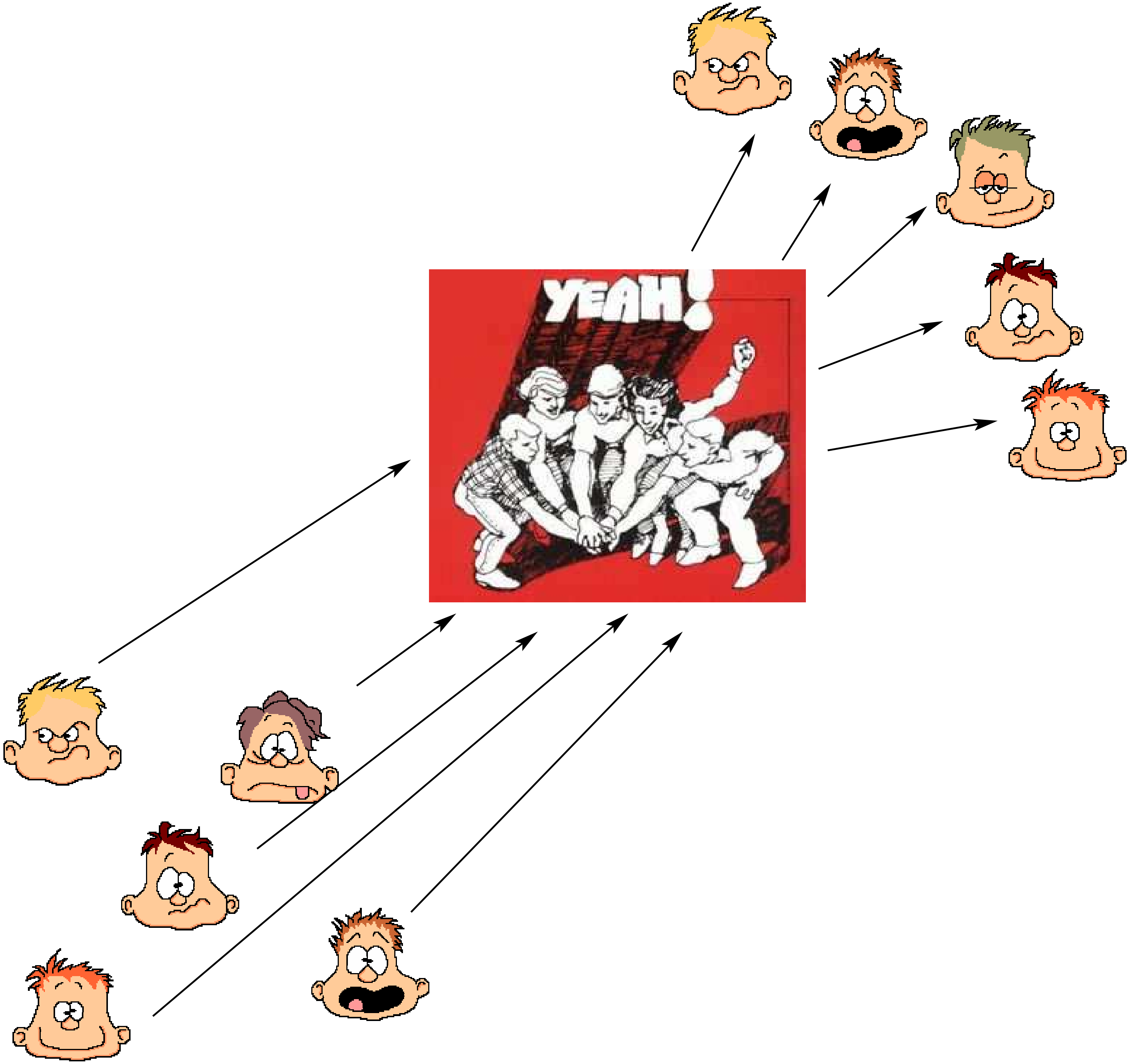
# BA Variant 1: Broadcast



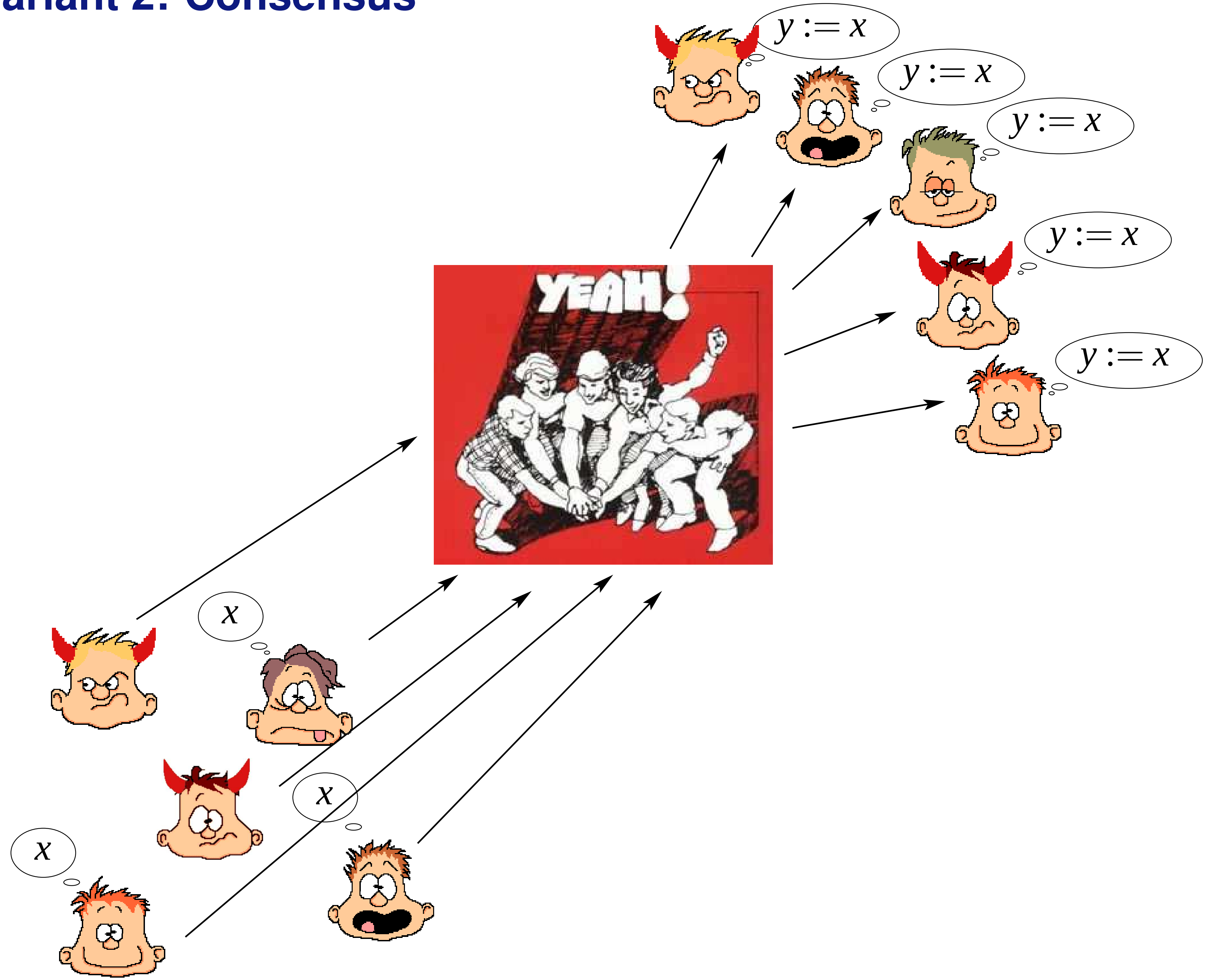
**???**

(general adversary)

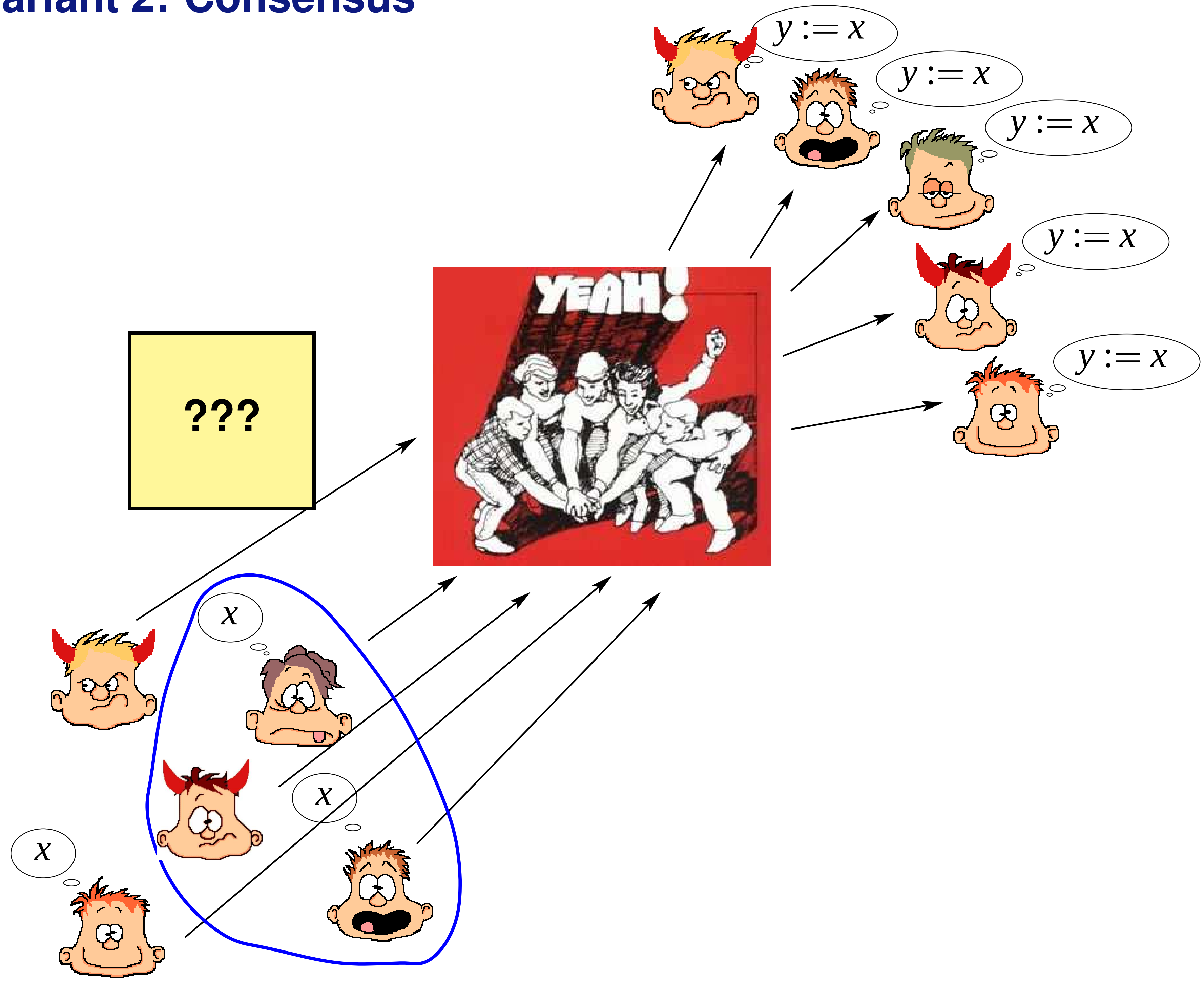
# BA Variant 2: Consensus



# BA Variant 2: Consensus



# BA Variant 2: Consensus



# Player-Centric Byzantine Agreement (BA)

**PCBA**$= \{P$**-BA**$\}_{P \subseteq \mathcal{P}}$

$P$-BA:

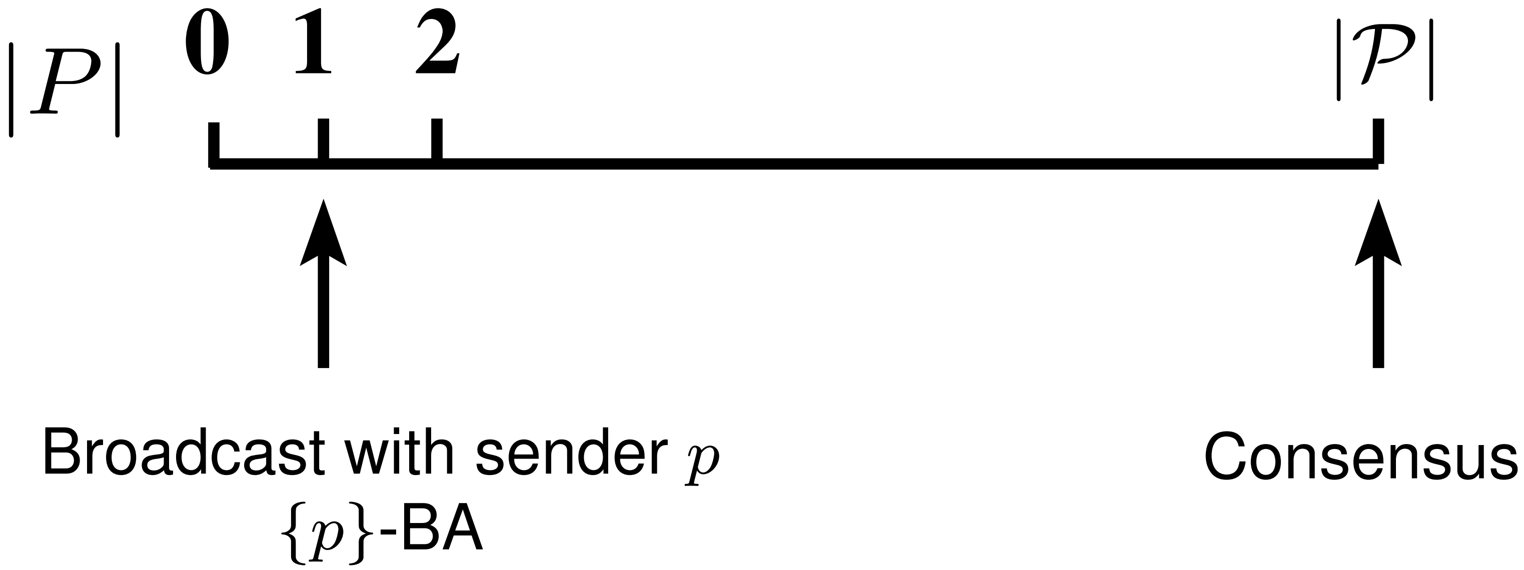
- (consistency) $\forall p \in \mathcal{P}$ output $y$.
- ($P$-validity) $\forall$ non-actively corrupted $p \in P$ has input $x \Rightarrow y = x$.

# Player-Centric Byzantine Agreement (BA)

**PCBA**$= \{P$**-BA**$\}_{P \subseteq \mathcal{P}}$

$P$-BA:

- (consistency) $\forall p \in \mathcal{P}$ output $y$.
- ($P$-validity) $\forall$ non-actively corrupted $p \in P$ has input $x \Rightarrow y = x$.



# Player-Centric Byzantine Agreement (BA)

Feasibility results for **general adversary**

- Active/Passive
  - **Perfect Security**
  - **Computational Security**

# Player-Centric Byzantine Agreement (BA)

Feasibility results for **general adversary**

- Active/Passive
  - **Perfect Security**
  - **Computational Security**

Player-Centric Broadcast (**Who** can broadcast?)

| $\mathcal{Z}$ | $p_1$ | $p_2$ | $p_3$ |
|---|---|---|---|
| $Z_1$ | $a$ | $e$ | $e$ |
| $Z_2$ | $e$ | $a$ | $e$ |
| $Z_3$ |  | $e$ | $a$ |

# Player-Centric Byzantine Agreement (BA)

Feasibility results for **general adversary**

- Active/Passive
  - **Perfect Security**
  - **Computational Security**

Player-Centric Broadcast (**Who** can broadcast?)

|  | ✓ | ✗ | ✗ |
|---|---|---|---|
| $\mathcal{Z}$ | $p_1$ | $p_2$ | $p_3$ |
| $Z_1$ | $a$ | $e$ | $e$ |
| $Z_2$ | $e$ | $a$ | $e$ |
| $Z_3$ |  | $e$ | $a$ |

# Player-Centric Byzantine Agreement (BA)

Feasibility results for **general adversary**

- Active/Passive
  - **Perfect Security**
  - **Computational Security**

Player-Centric Broadcast (**Who** can broadcast?)

|  | ✓ | ✗ | ✗ |
|---|---|---|---|
| $\mathcal{Z}$ | $p_1$ | $p_2$ | $p_3$ |
| $Z_1$ | $a$ | $e$ | $e$ |
| $Z_2$ | $e$ | $a$ | $e$ |
| $Z_3$ |  | $e$ | $a$ |

- Active/Passive/Fail: Exact Bound for Consensus

# Player-Centric Byzantine Agreement (BA)

Feasibility results for **general adversary**

- Active/Passive
  - **Perfect Security**
  - **Comp**

**Leads to . . .**

- Player-Centric MPC (**Who** can give input?)

Play

| | | | |
|---|---|---|---|
| $Z_1$ | $a$ | $e$ | $e$ |
| $Z_2$ | $e$ | $a$ | $e$ |
| $Z_3$ | | $e$ | $a$ |

- Active/Passive/Fail: Exact Bound for Consensus