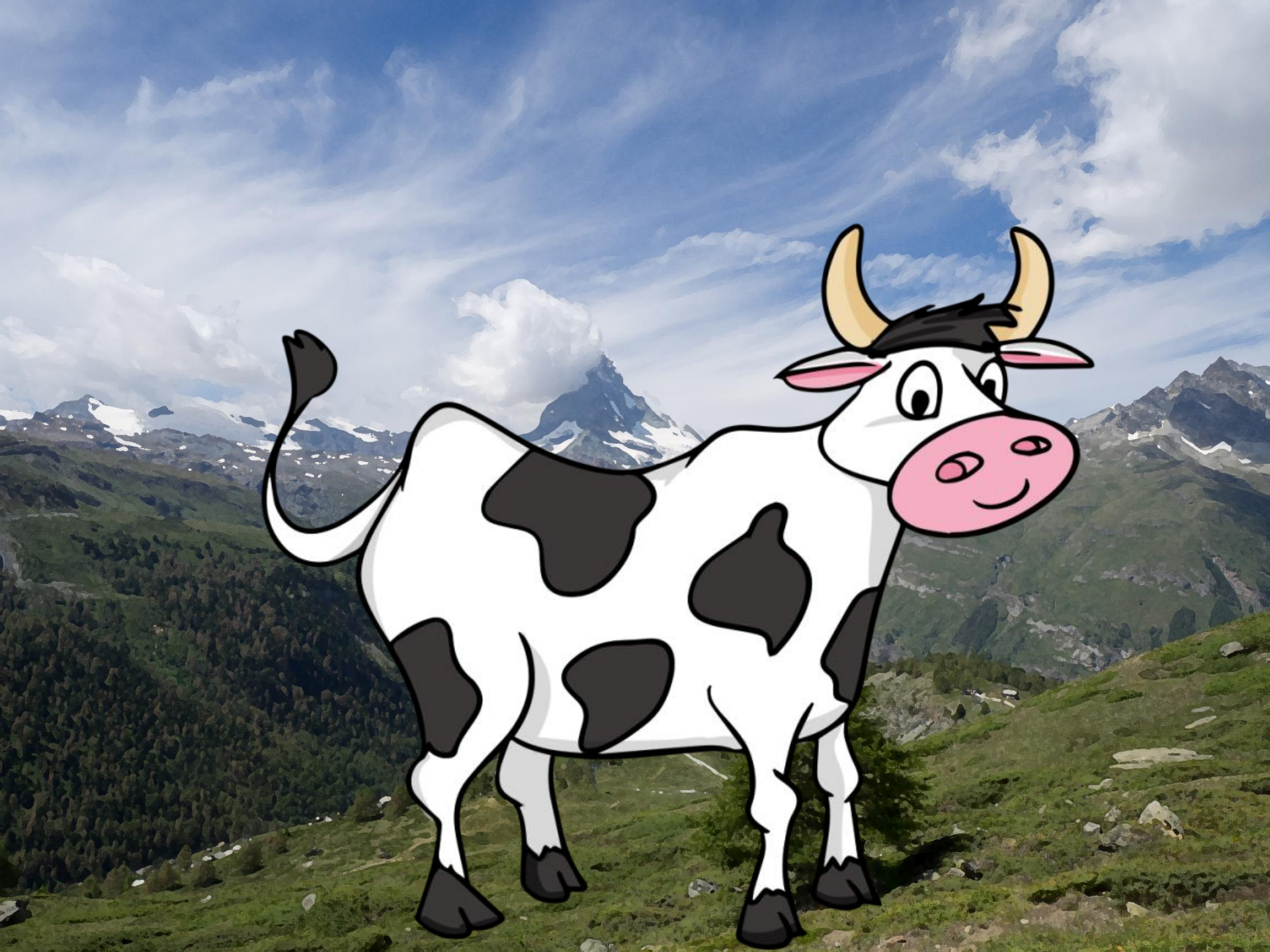
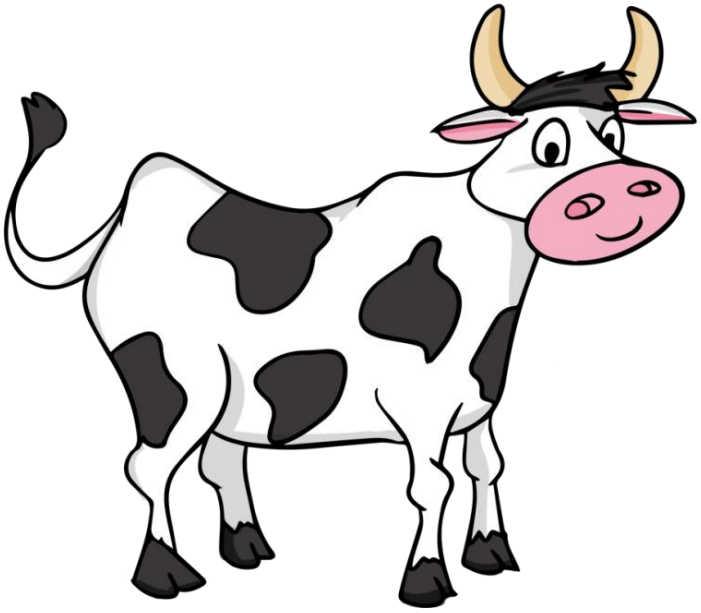
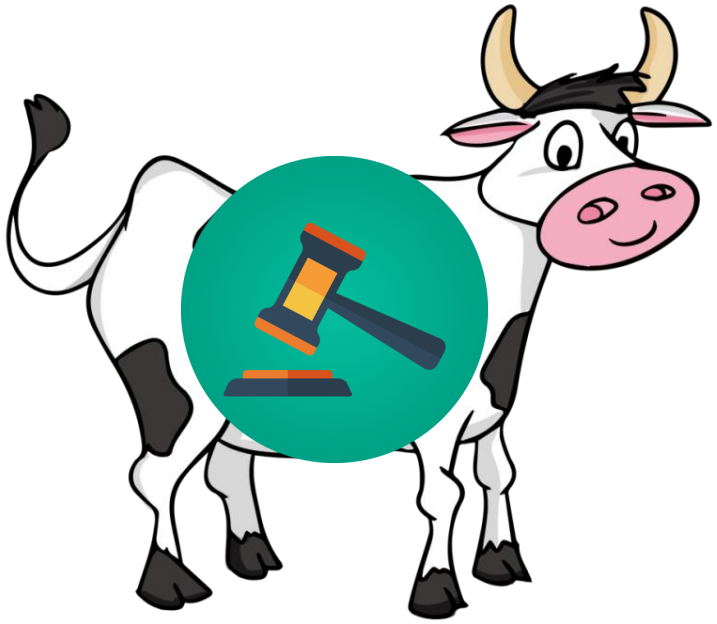
Byzantine Agreement with Interval Validity

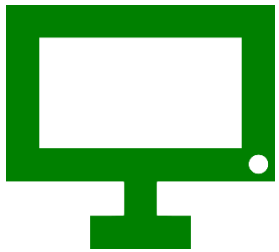
Darya Melnyk and Roger Wattenhofer

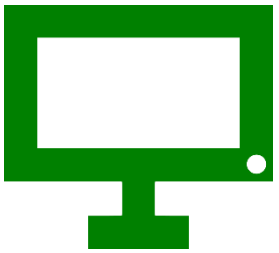


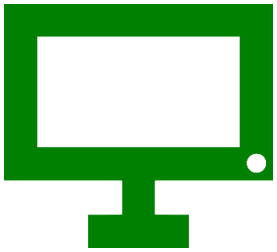


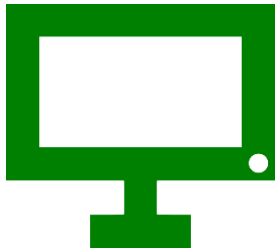
Distributed Auction

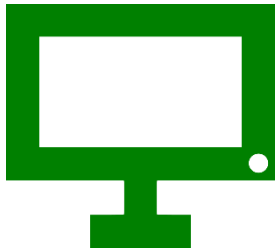


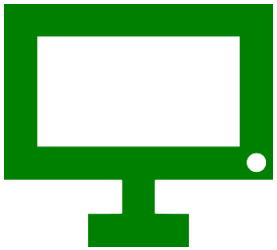


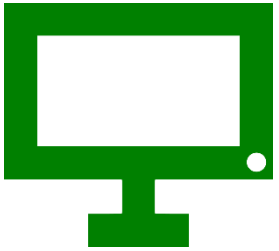




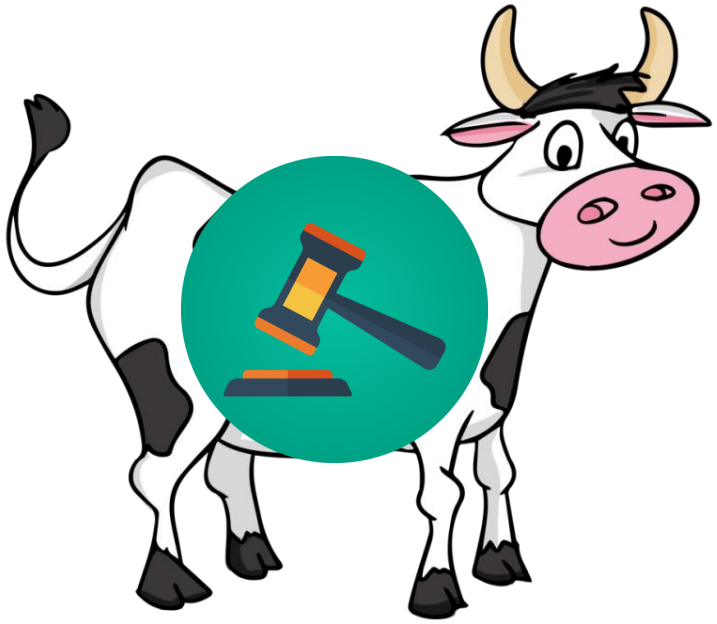








Distributed Auction



1500$

1250$

1350$

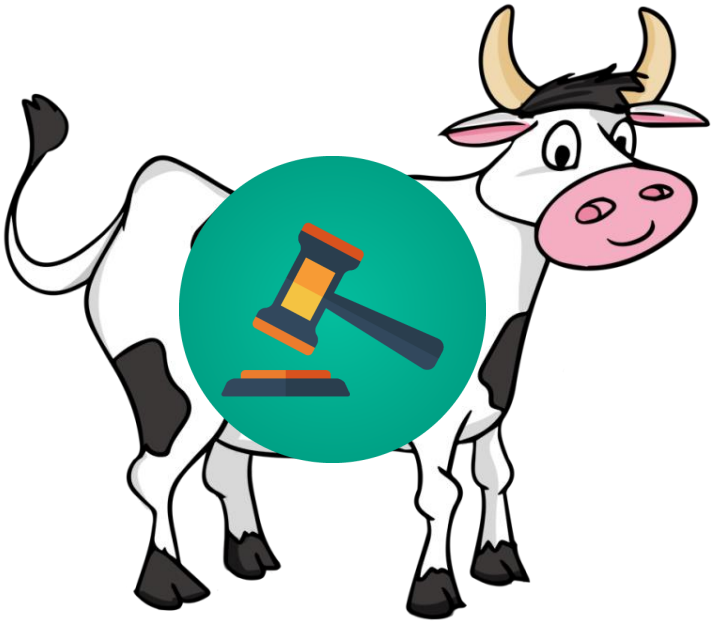
20$

1200$

1000$

2000$

Distributed Auction



1500$

1250$

1350$

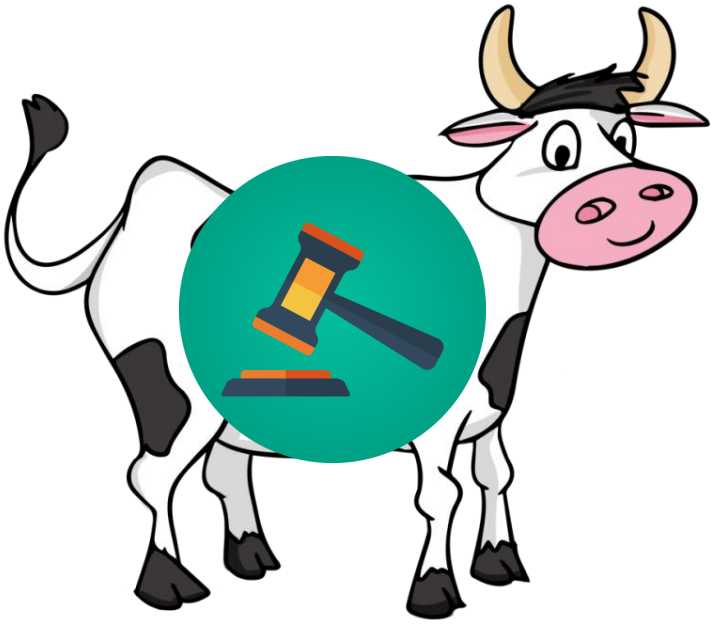
20$

1200$

1000$

2000$

Distributed Auction



1500$

1250$

1350$

20$

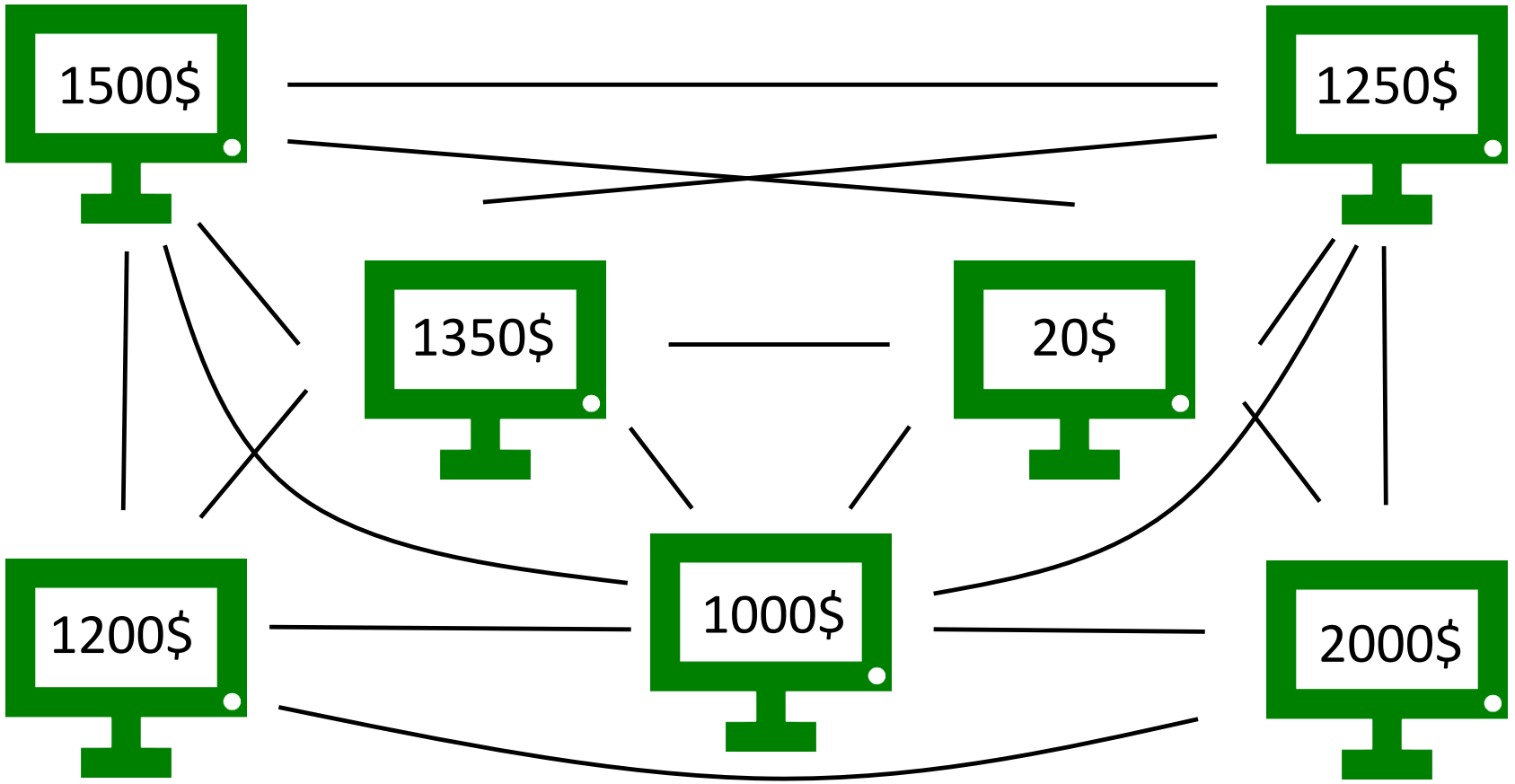
1200$

1000$

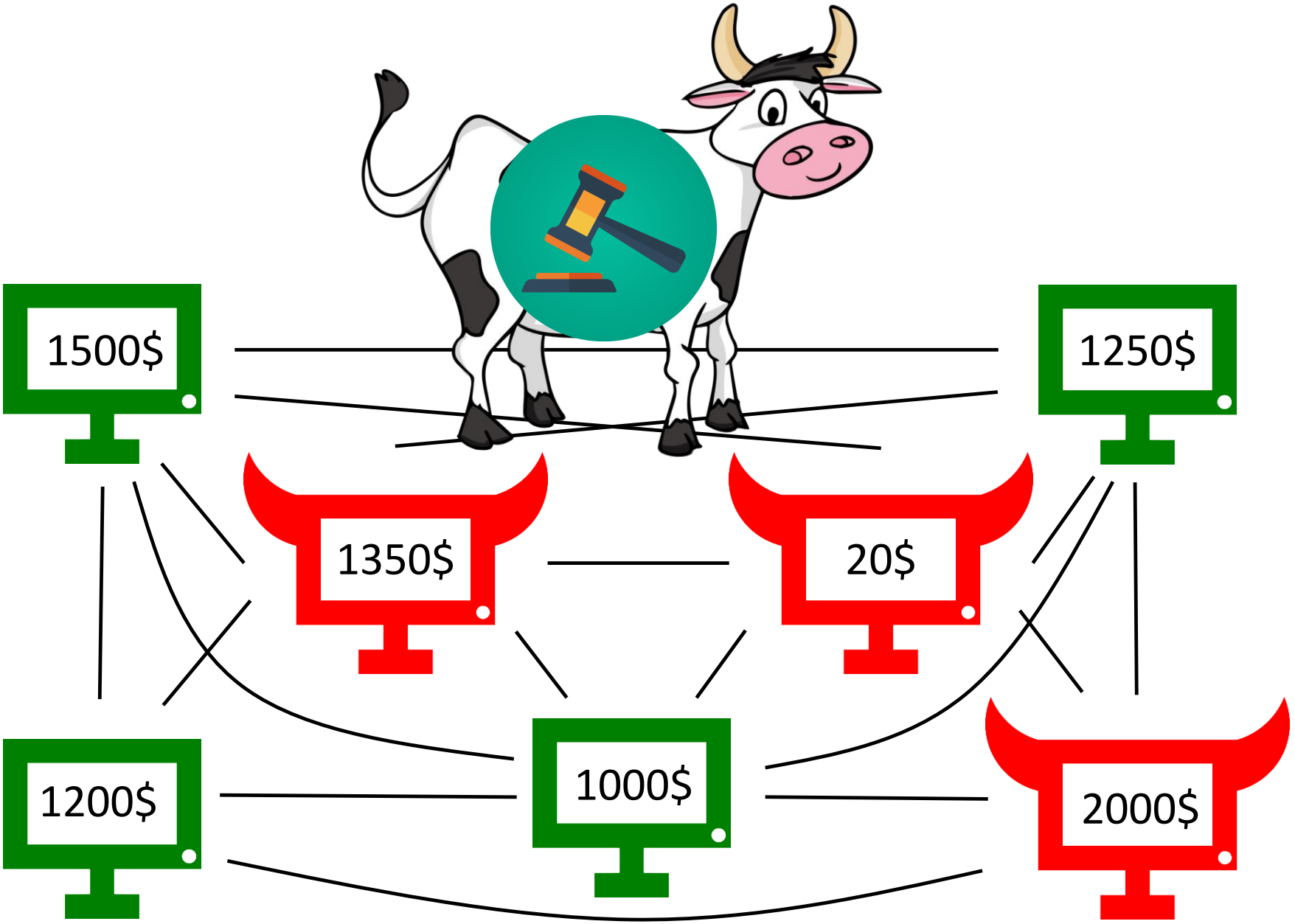
2000$

Distributed Auction

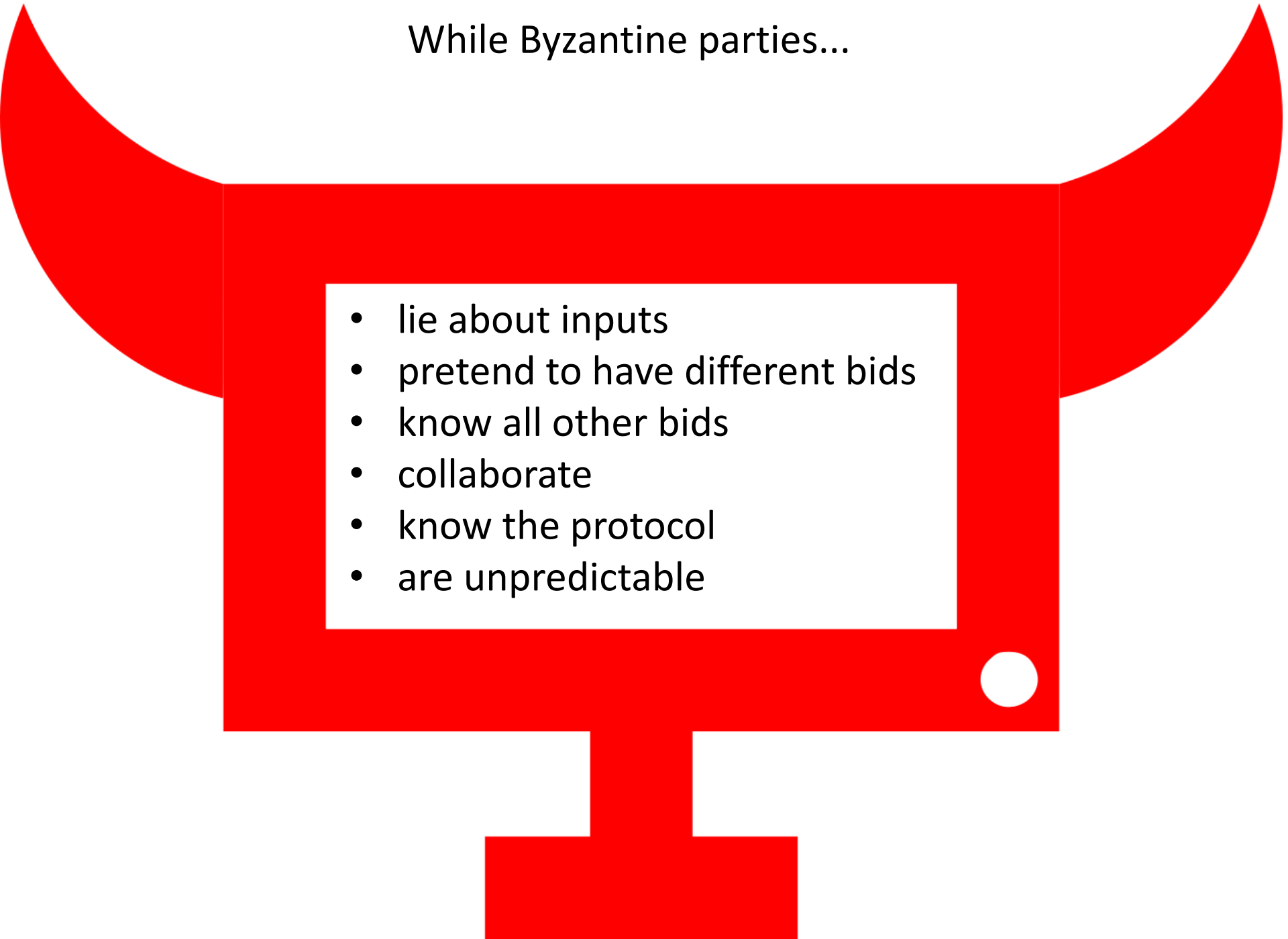
- Fully connected graph
- Synchronous communication



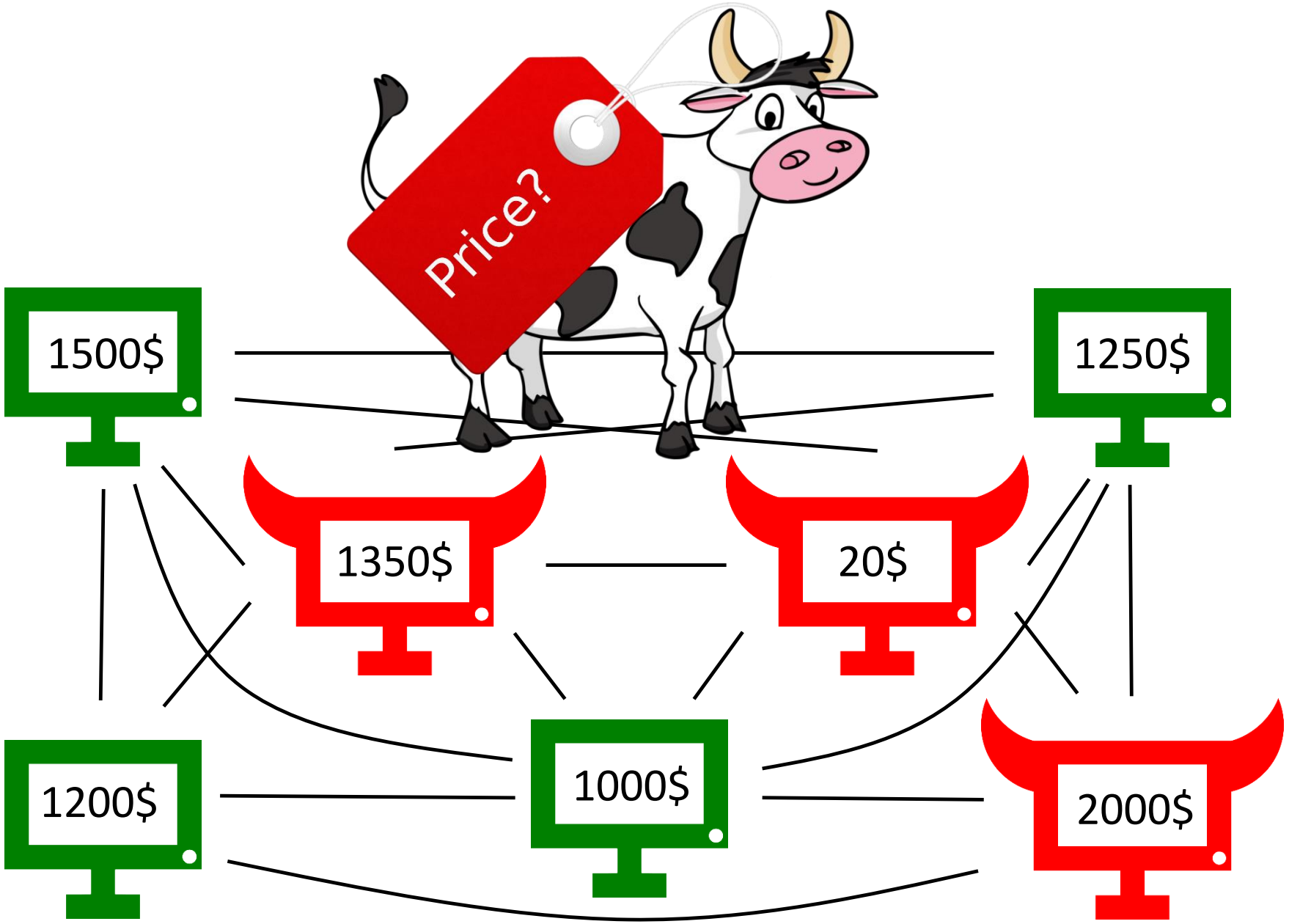
Distributed Auction with Byzantine Parties



While Byzantine parties...

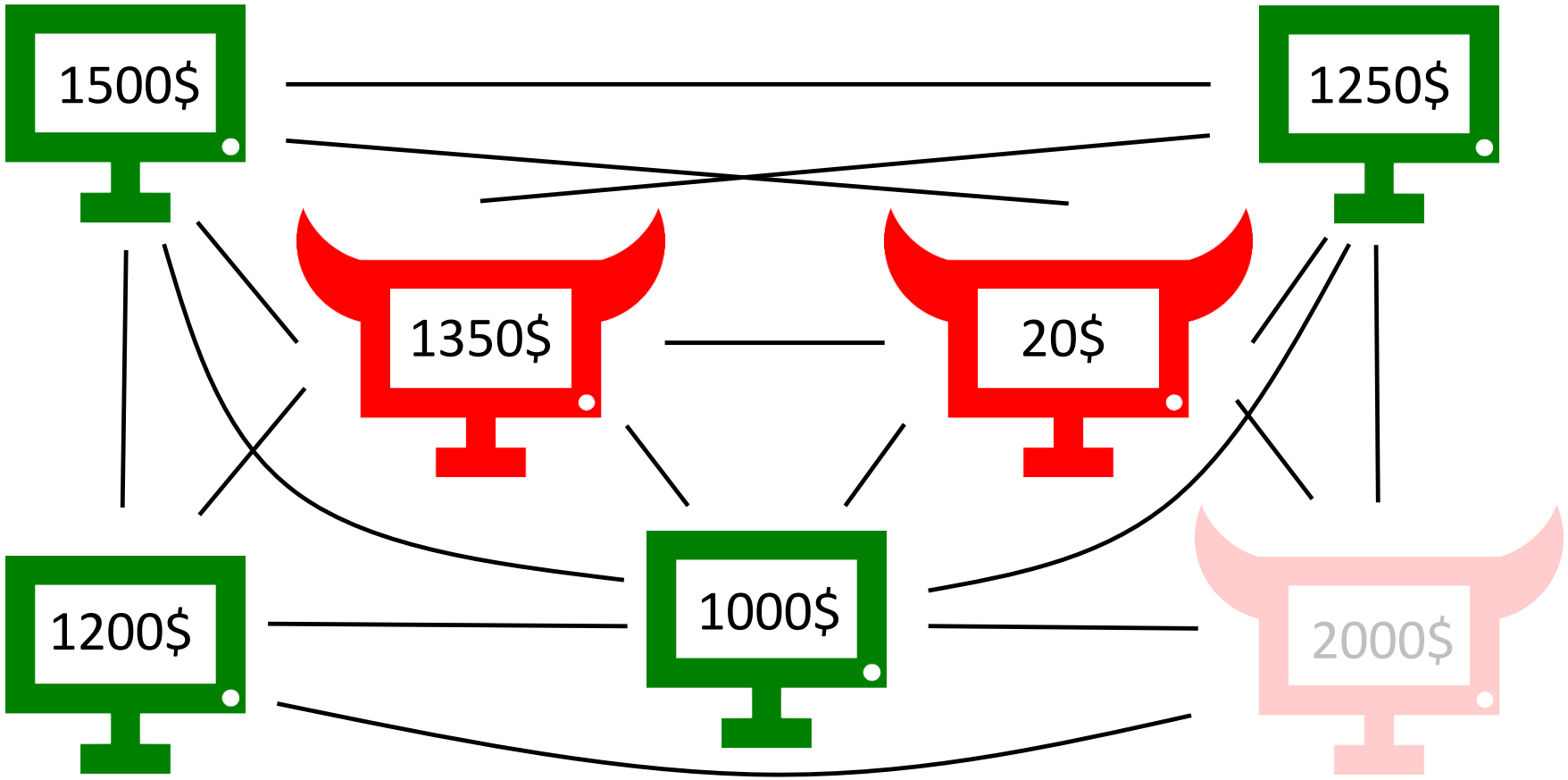


What‘s the fair price?



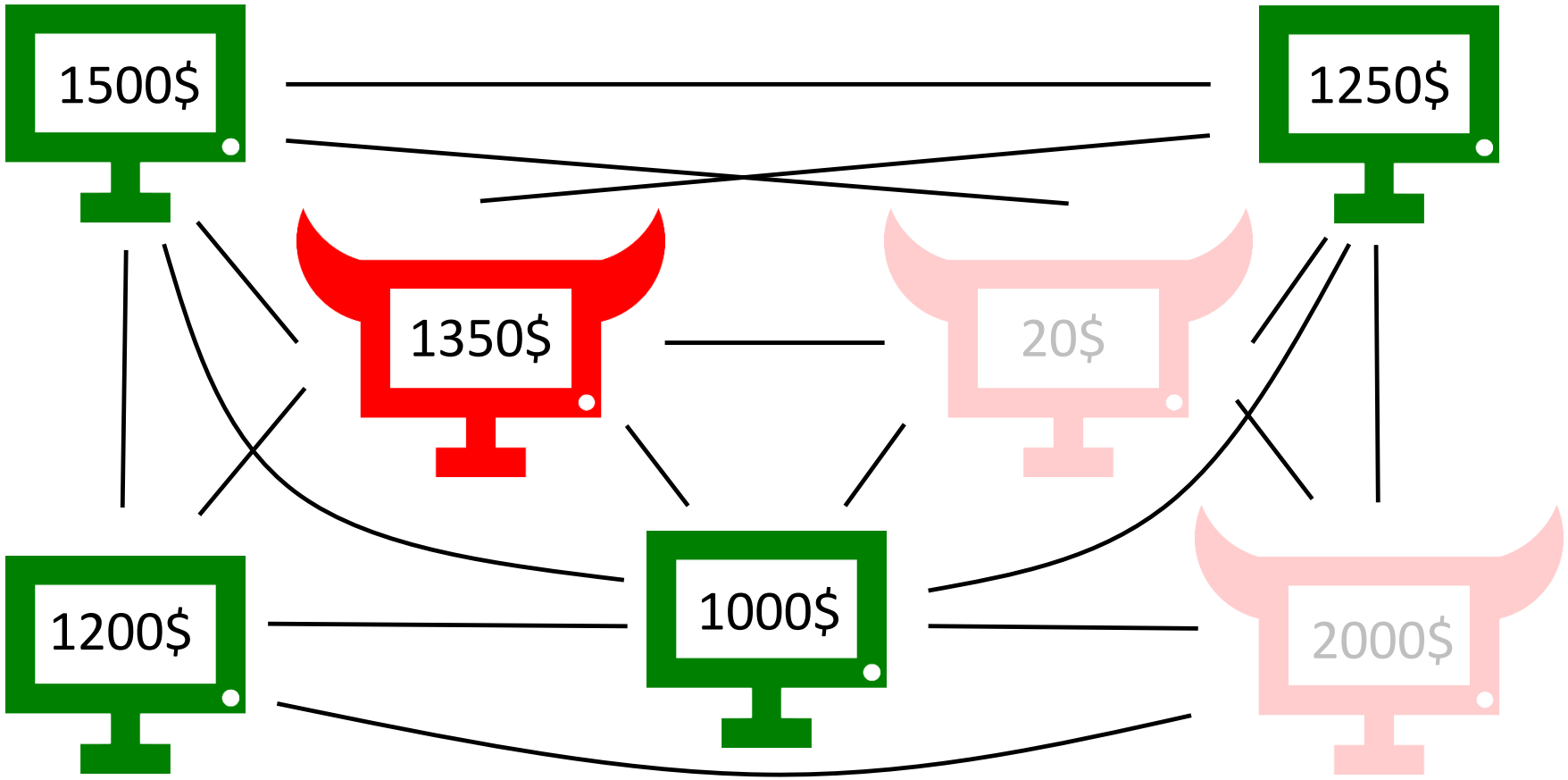
Valdidity Condition

- Remove too high bids

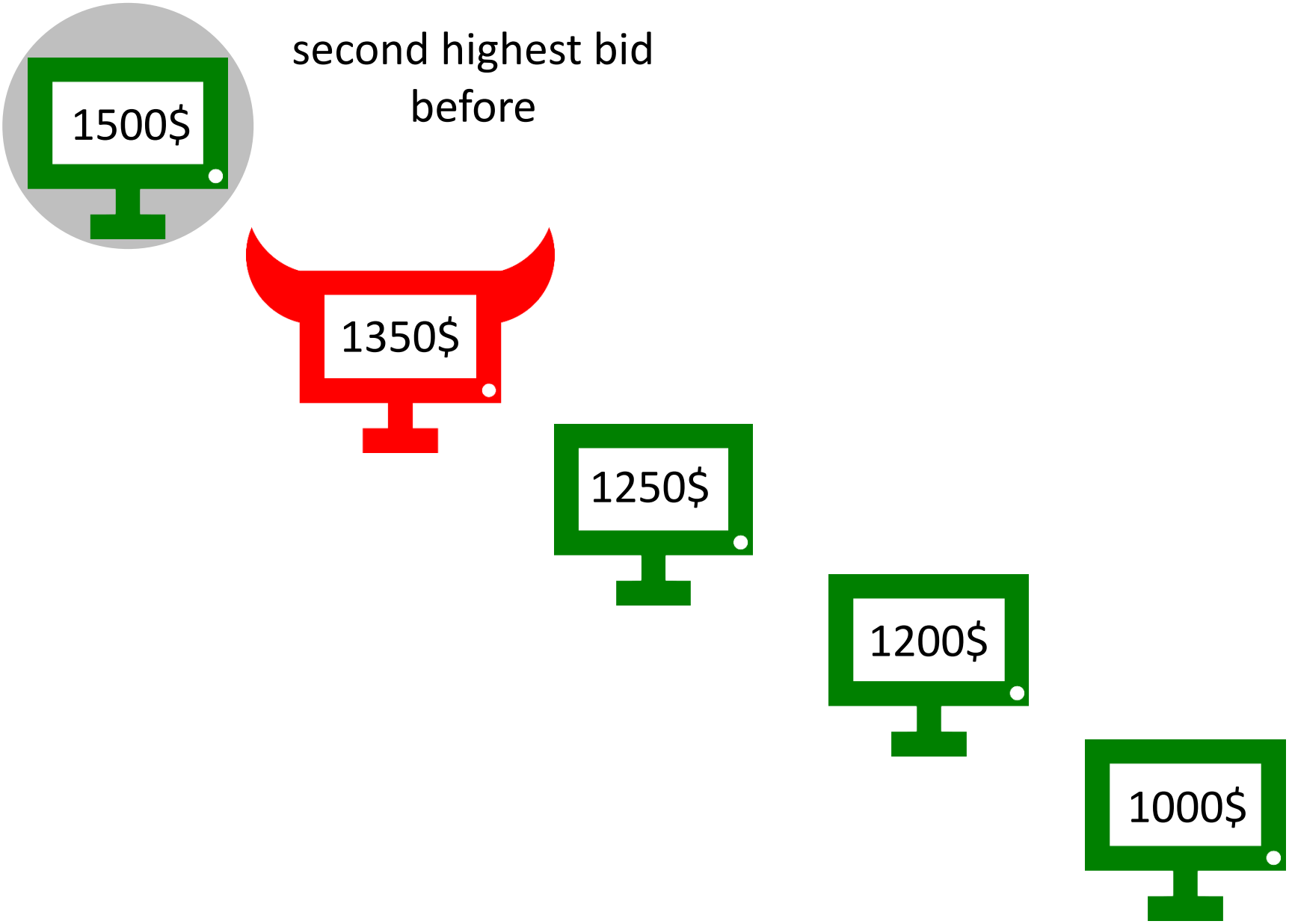


Validity Condition

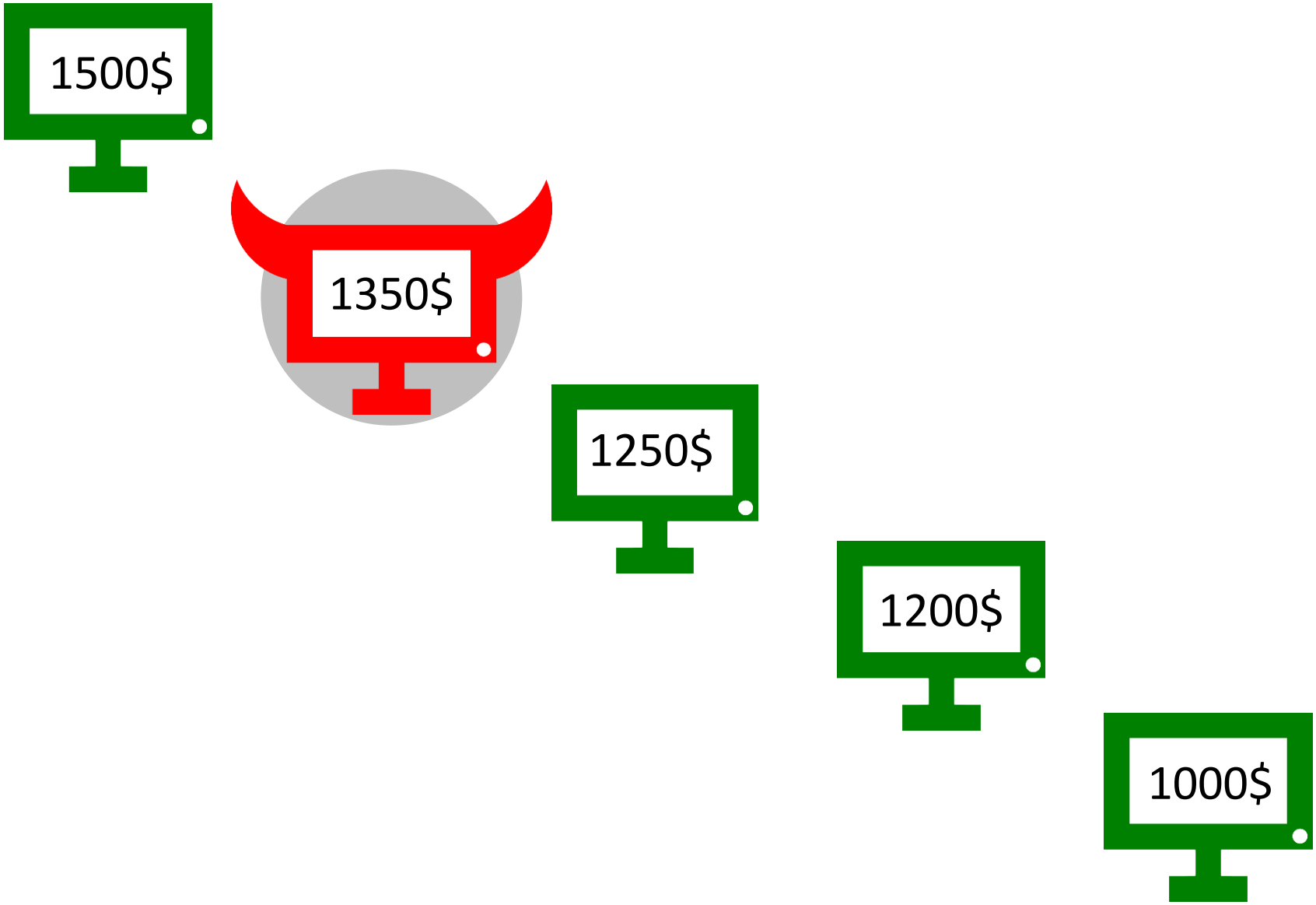
- Remove too high bids
- Remove loo low bids



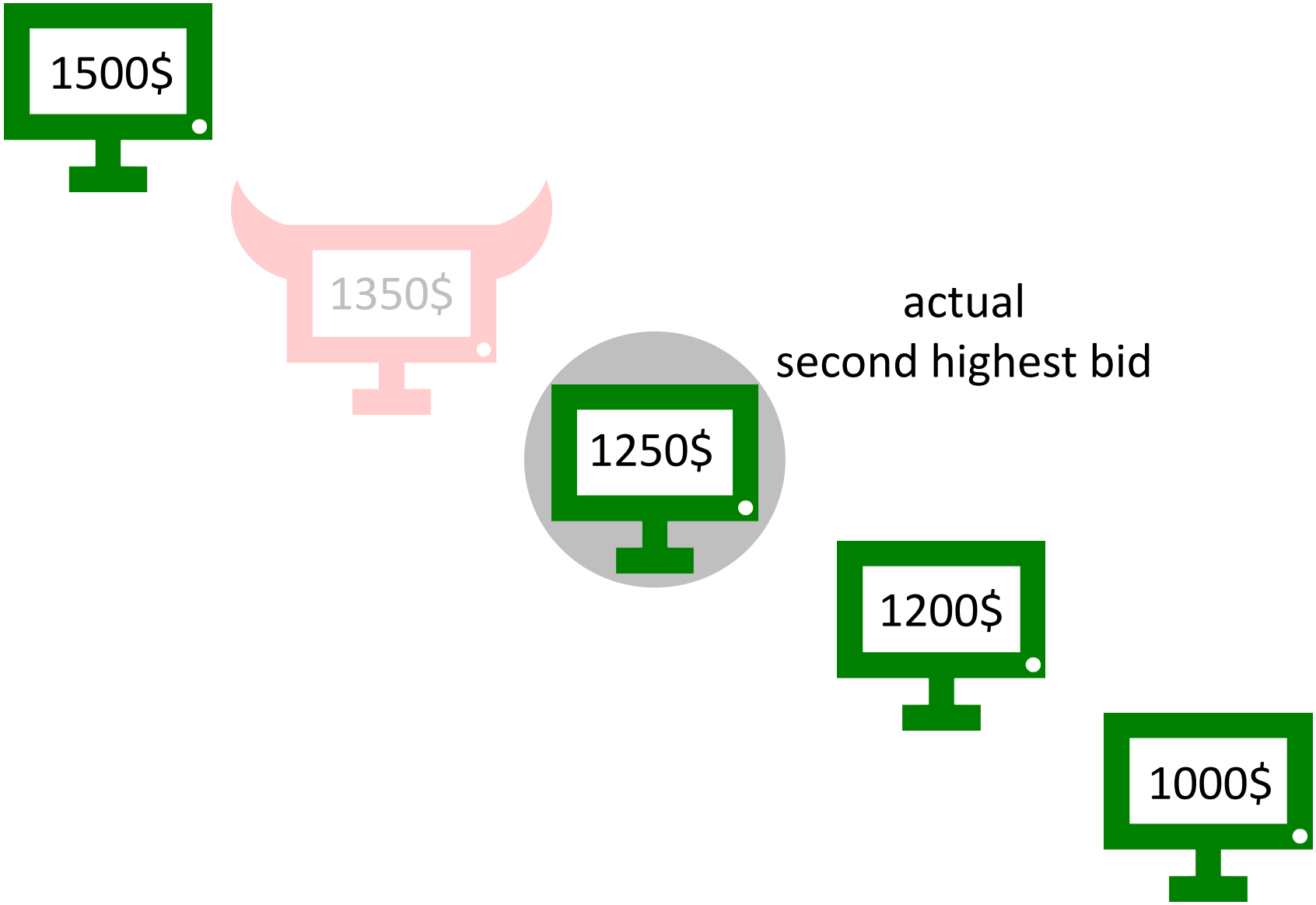
Validity Condition



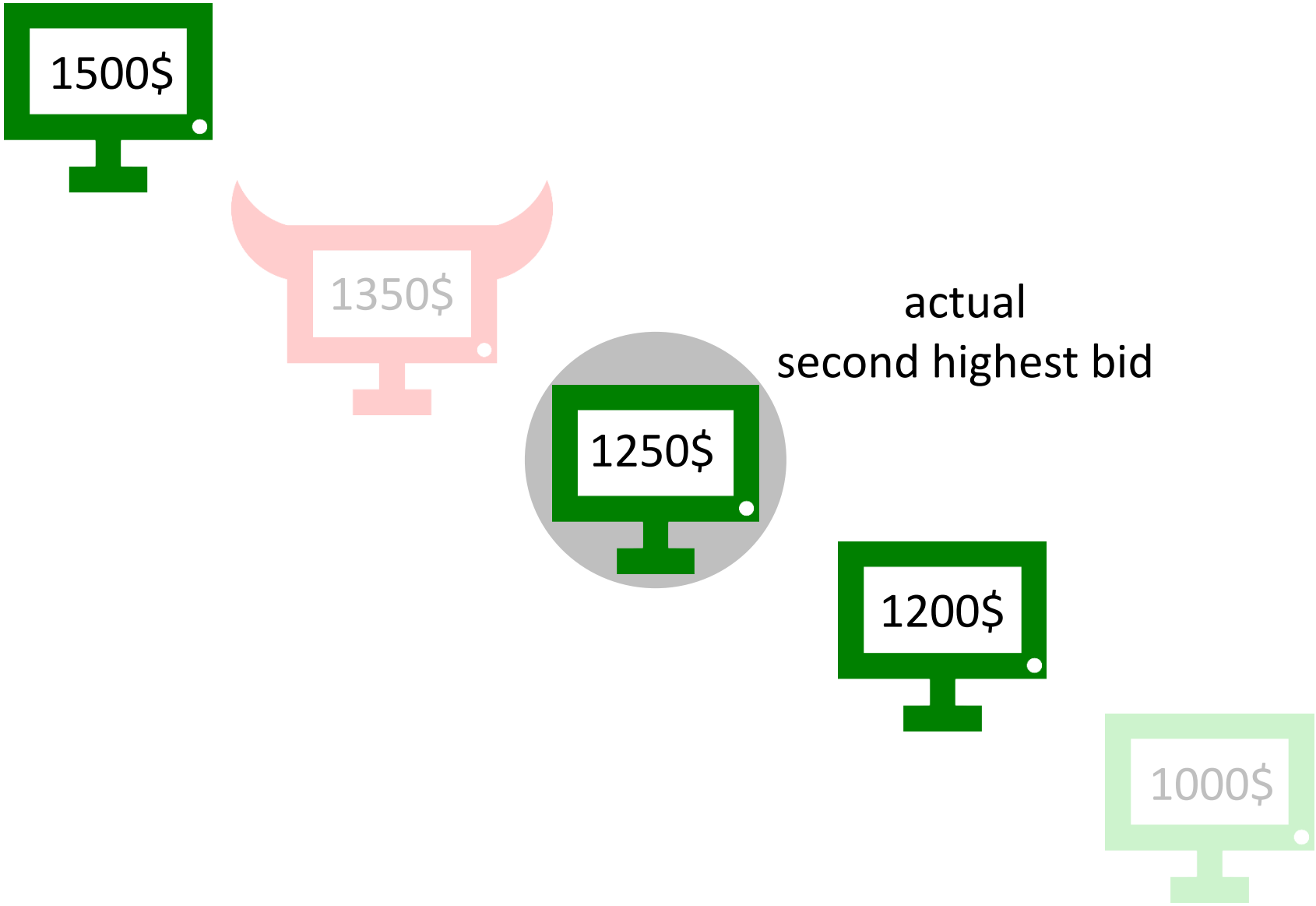
Validity Condition



Validity Condition

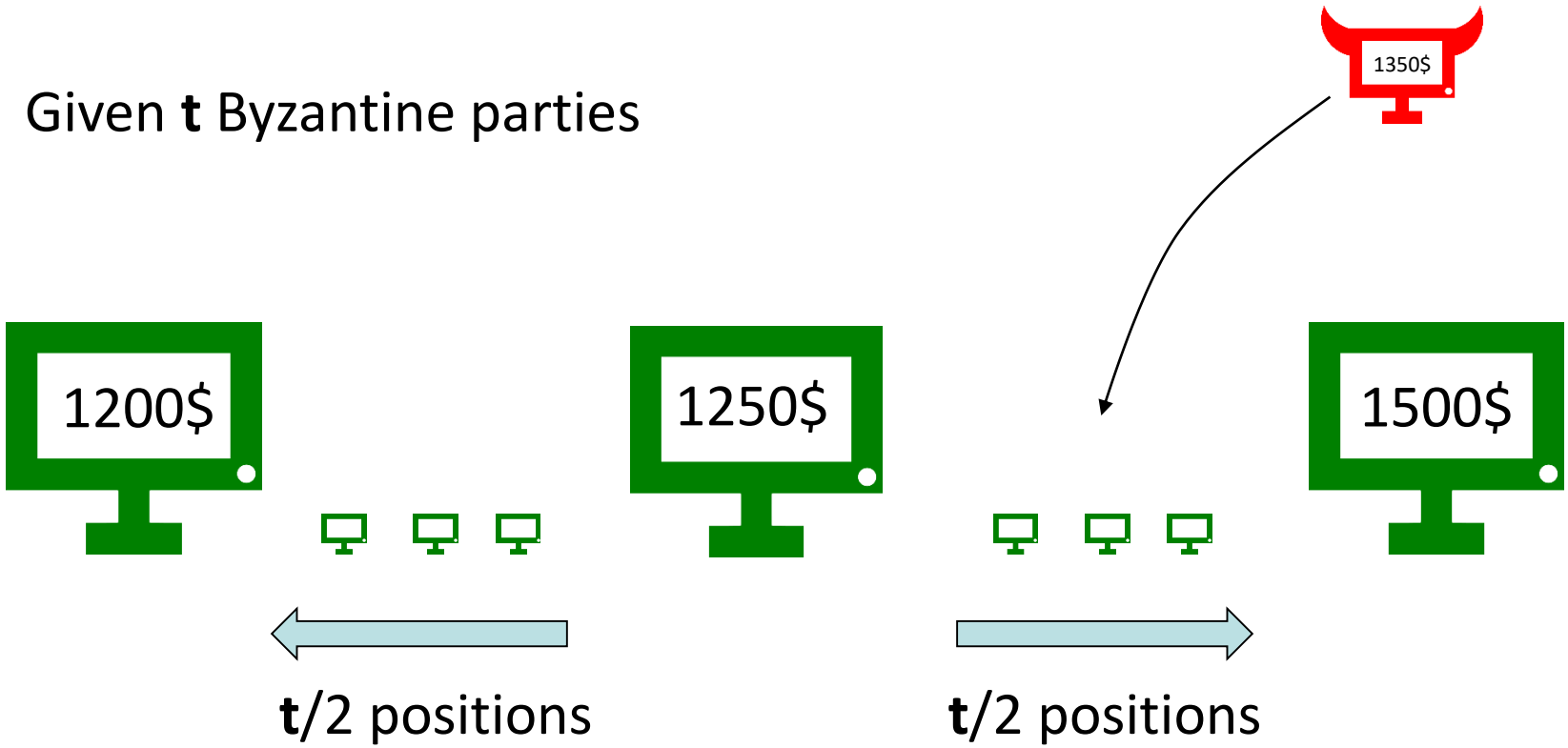


Validity Condition



Interval Validity

Given **t** Byzantine parties



we can accept all bids which are at most t/2 positions away from the wanted bid.

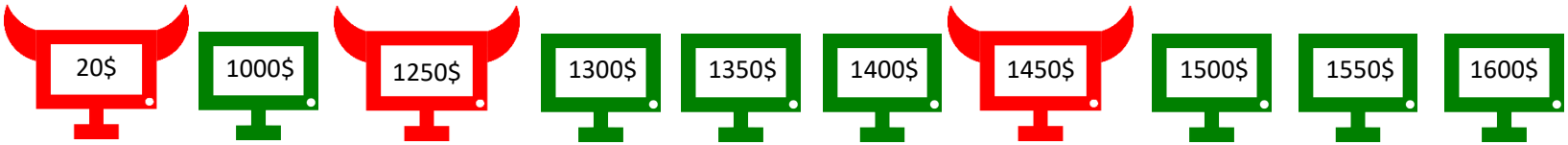
Want …

a synchronous Byzantine agreement algorithm that satsfies

Interval Validity

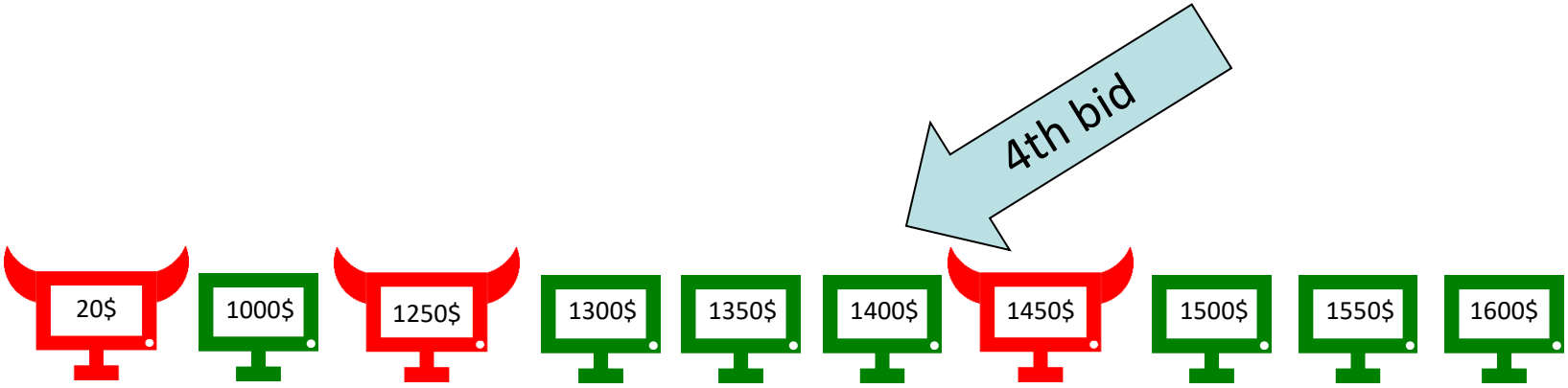
Naive Algorithm

- Byzantine Agreement on each bid
  - Can be done in t+1 rounds exchanging O(n^4) messages



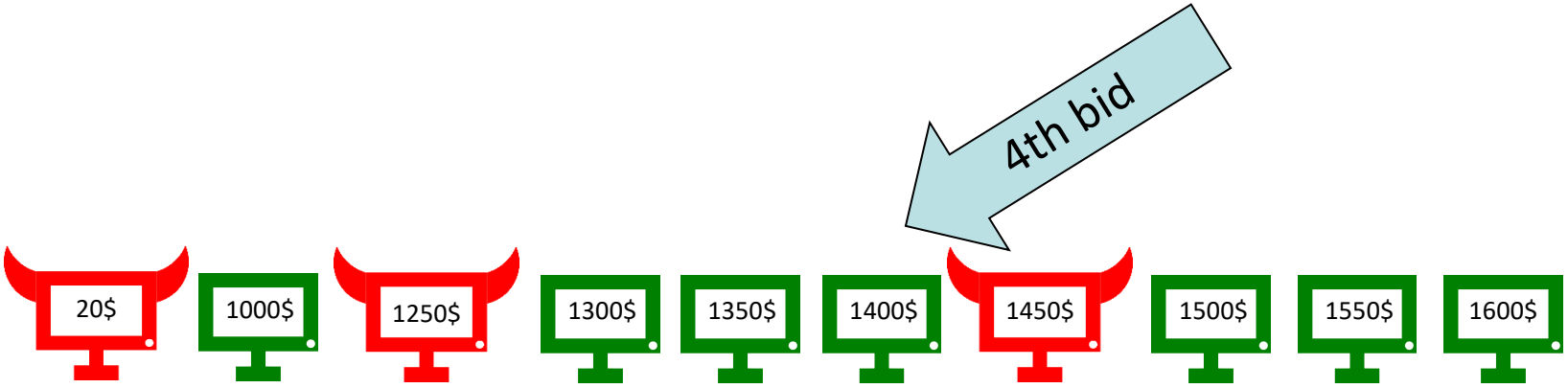
Naive Algorithm

- Choose the k-th smallest value



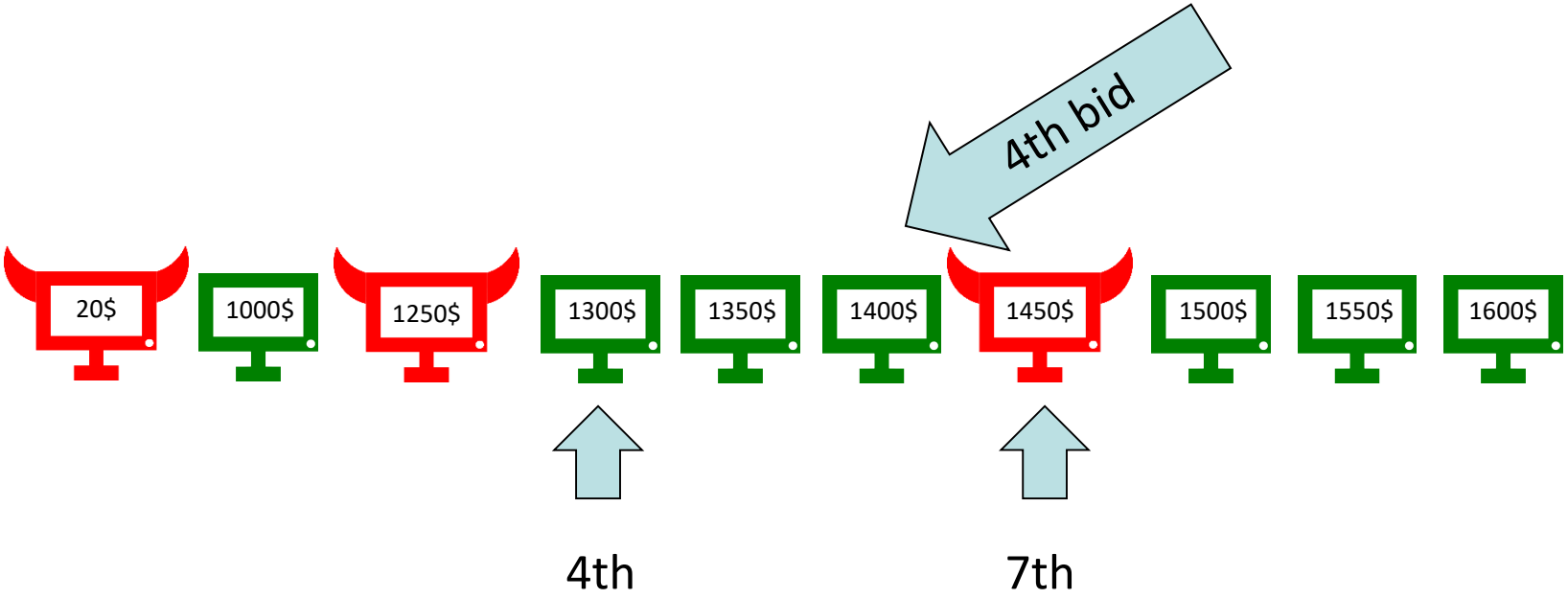
Naive Algorithm

- Choose the k-th smallest value
  - Choose the **median** between the **k-th** smallest and the **(k+t)** smallest value



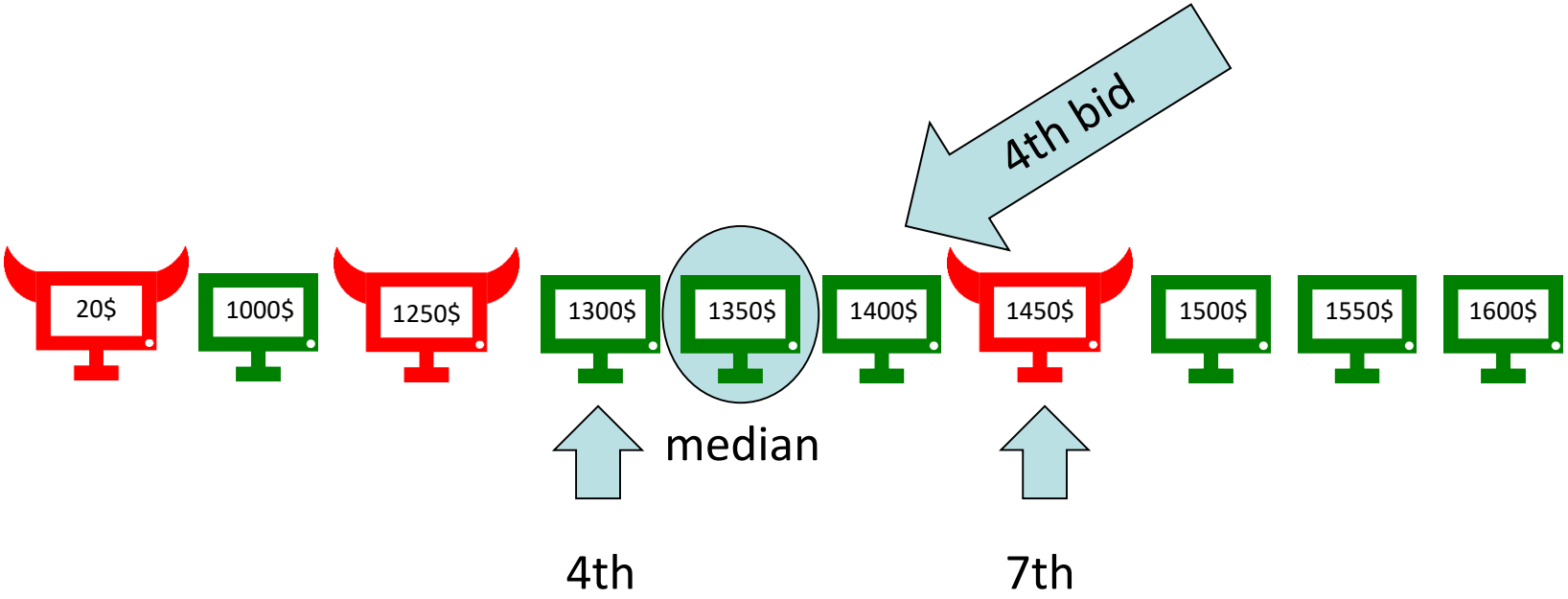
Naive Algorithm

- Choose the k-th smallest value
  - Choose the **median** between the **k-th** smallest and the **(k+t)** smallest value



Naive Algorithm

- Choose the k-th smallest value
  - Choose the median between the k-th smallest and the (k+t) smallest value

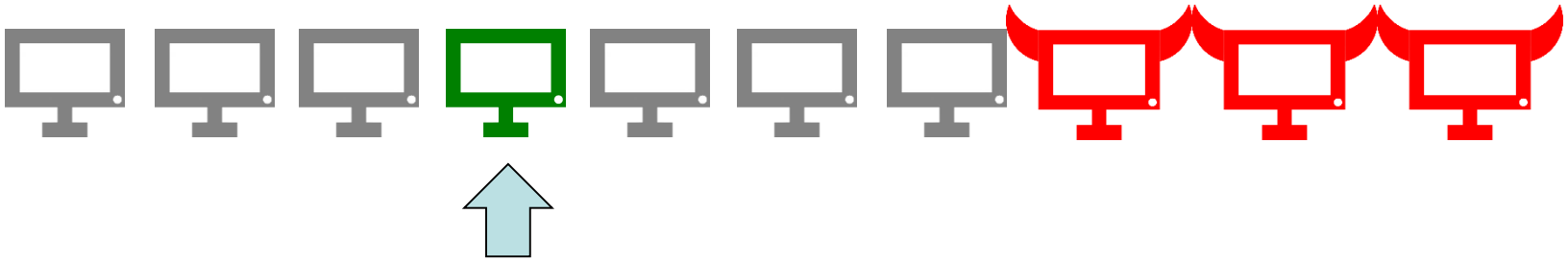


Lower Bound

10 bids, 3 Byzantine, look for the 4th smallest

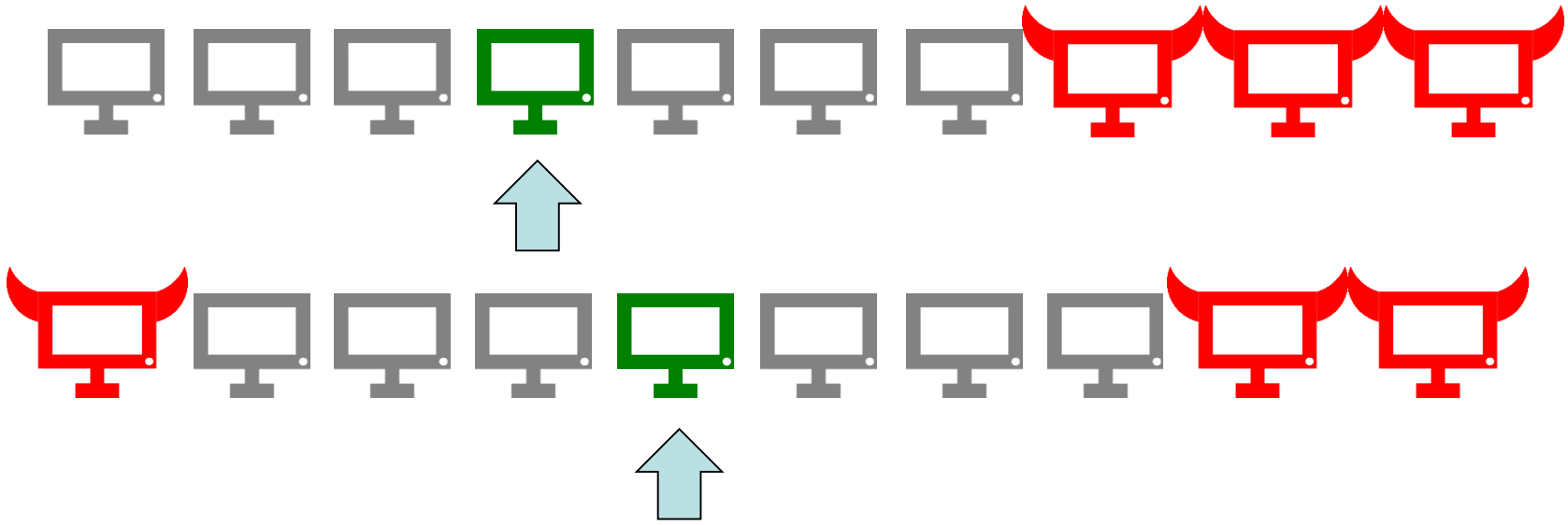
Lower Bound

10 bids, 3 Byzantine, look for the 4th smallest



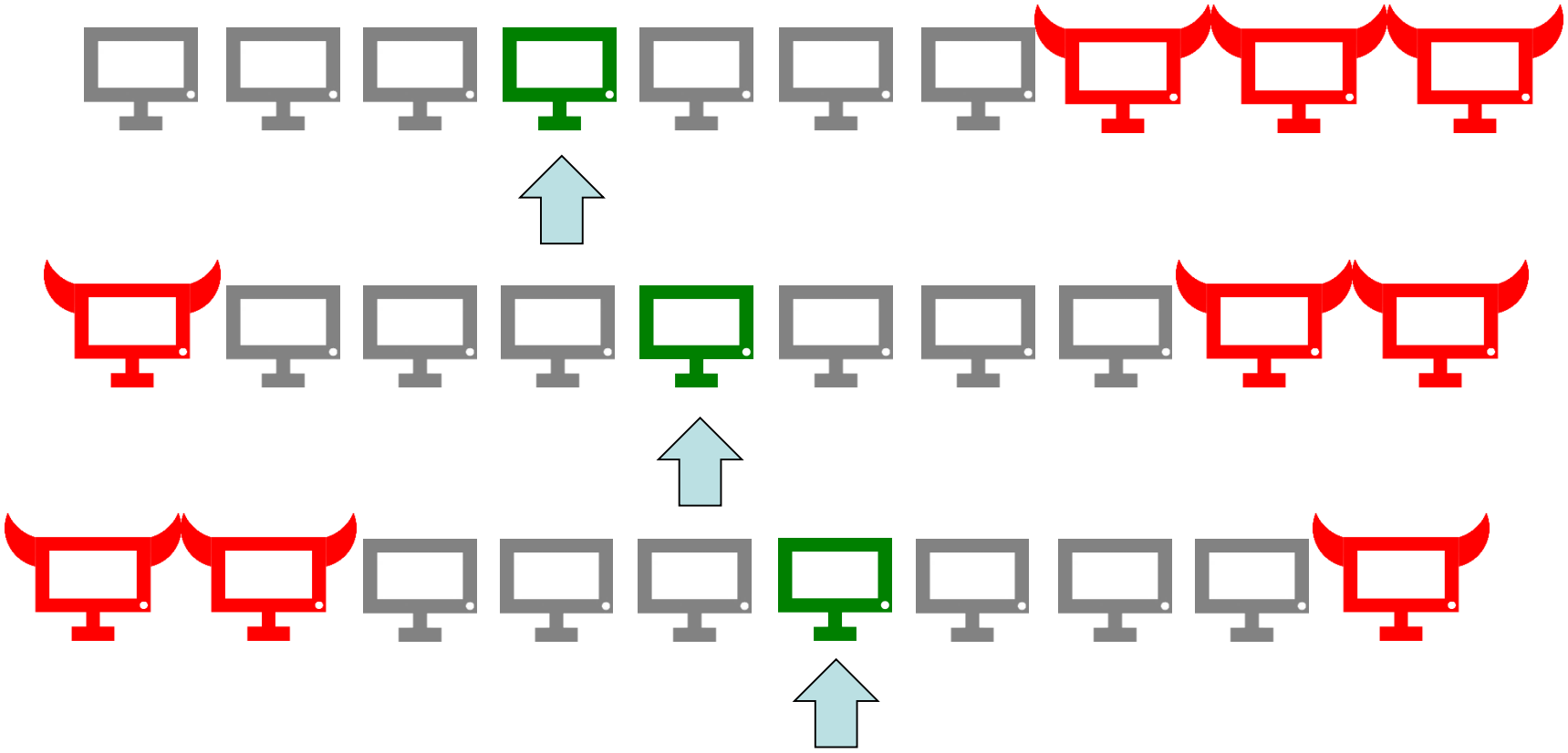
Lower Bound

10 bids, 3 Byzantine, look for the 4th smallest



Lower Bound

10 bids, 3 Byzantine, look for the 4th smallest

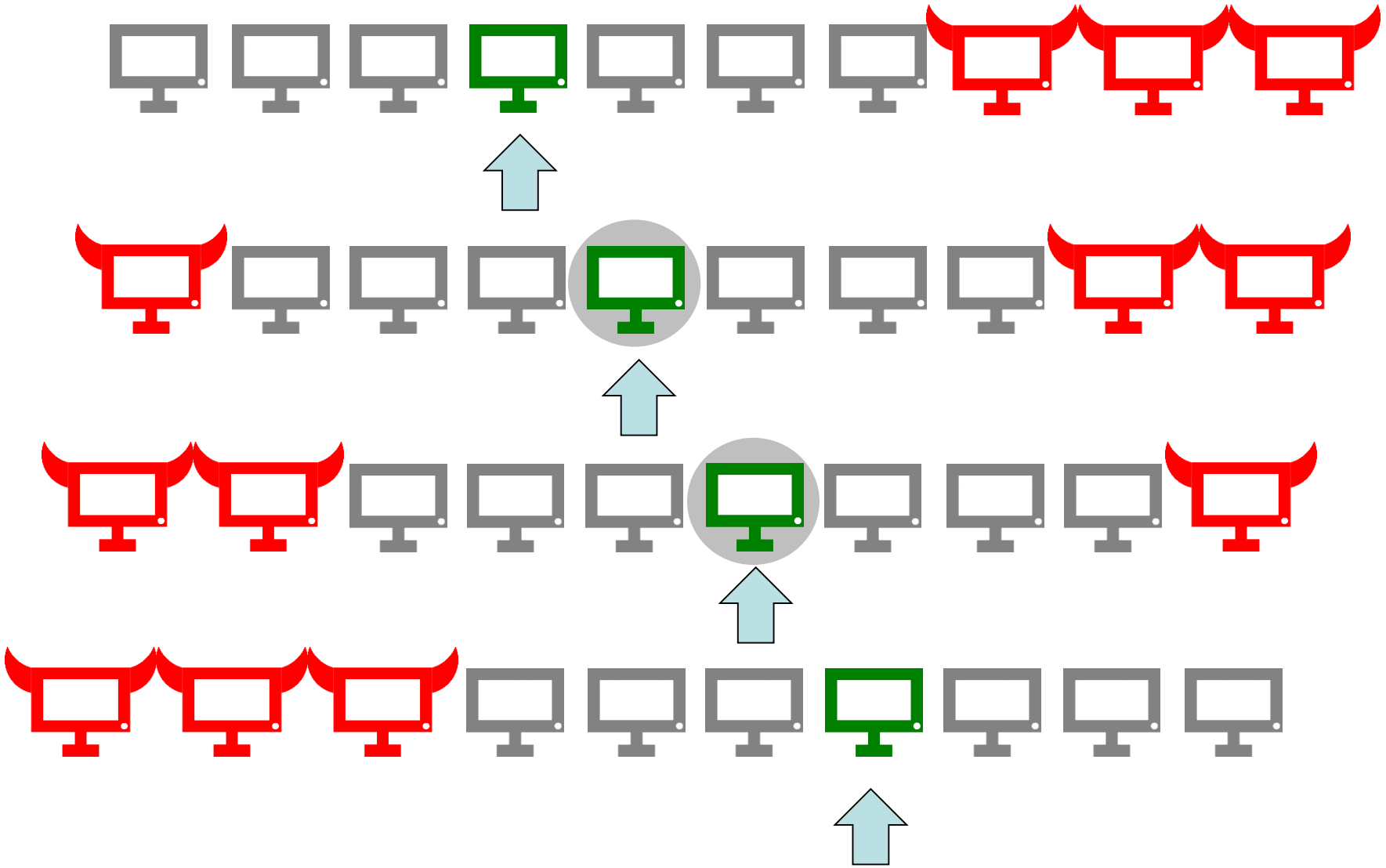


Lower Bound

10 bids, 3 Byzantine, look for the 4th smallest

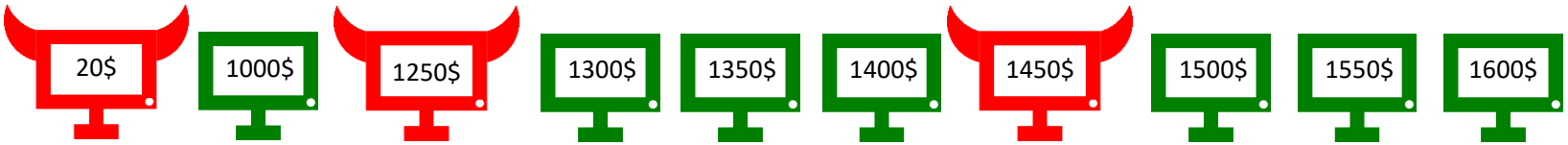
Lower Bound

10 bids, 3 Byzantine, look for the 4th smallest



Naive Algorithm

- Byzantine Agreement on each bid
  - Can be done in **t+1** rounds exchanging **O(n^4)** messages



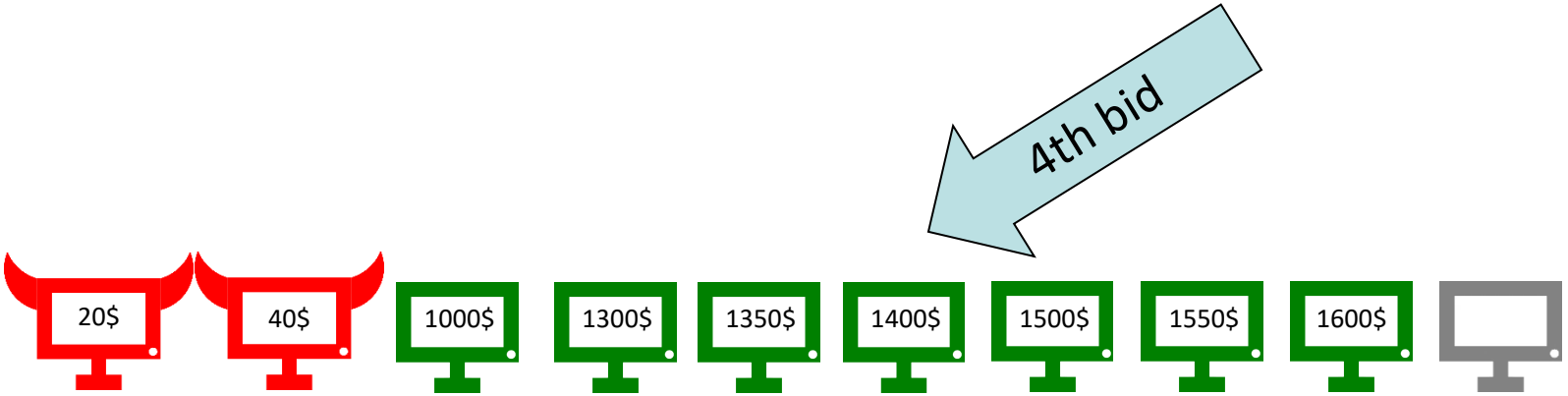
Our Algorithm

- each bidder locally chooses an approximation for the k-th smallest value

- bidders agree on any price inside the interval of all correct bids

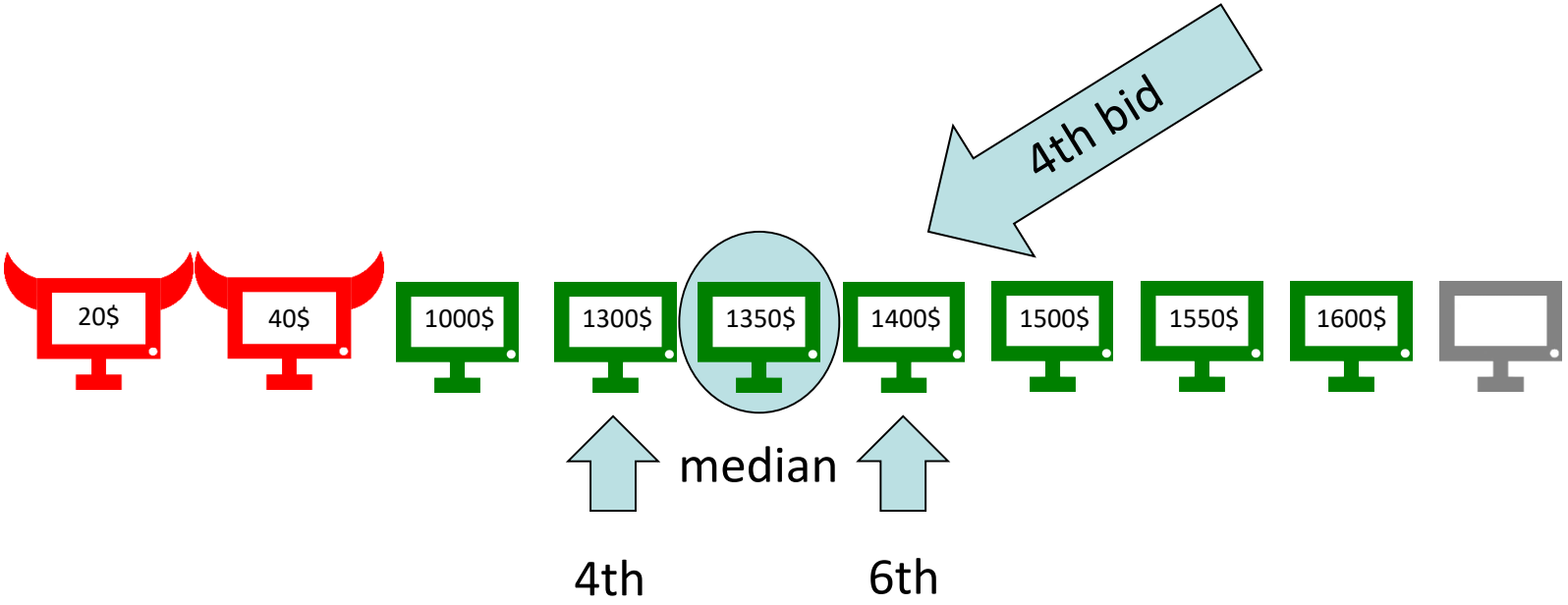
Our Algorithm

- each bidder locally chooses an approximation for the k-th smallest value
  - choose the **median** between the **k-th** smallest and the **(k+t)** smallest value



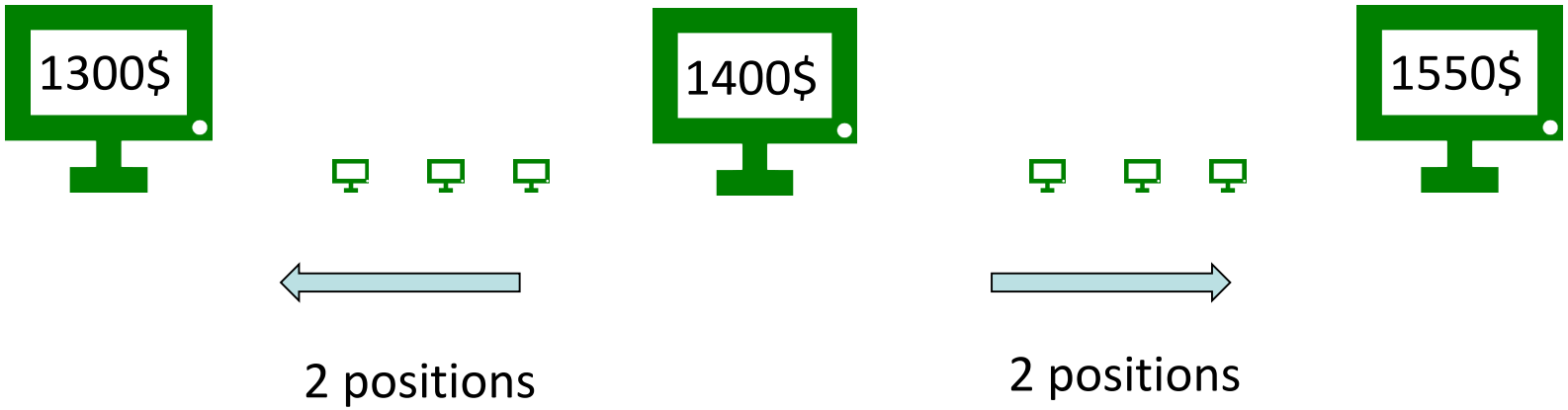
Our Algorithm

- each bidder locally chooses an approximation for the k-th smallest value
  - choose the **median** between the **k-th** smallest and the **(k+t)** smallest value



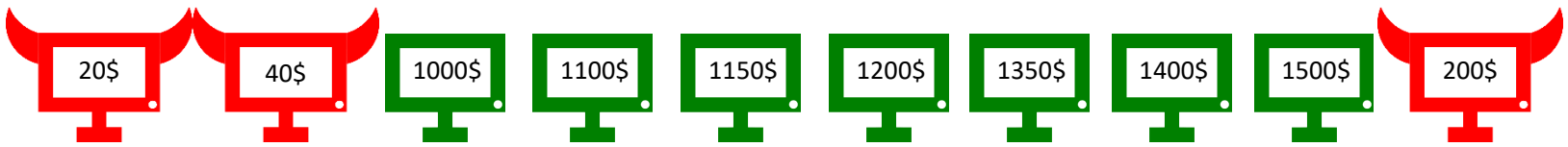
Our Algorithm

- bidders agree on any price inside the interval of all correct bids



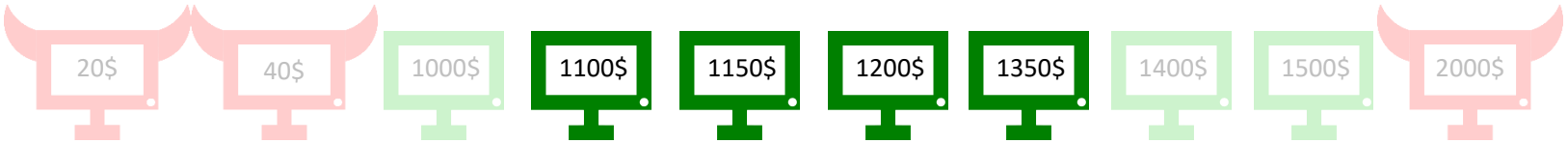
Our Algorithm

- bidders agree on any price inside the interval of all correct bids
  - receive approximations from every node



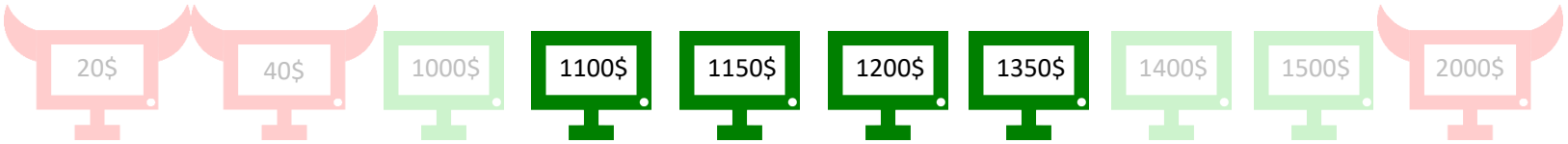
Our Algorithm

- bidders agree on any price inside the interval of all correct bids
  - receive approximations from every node
  - remove **too low** and **too high** bids



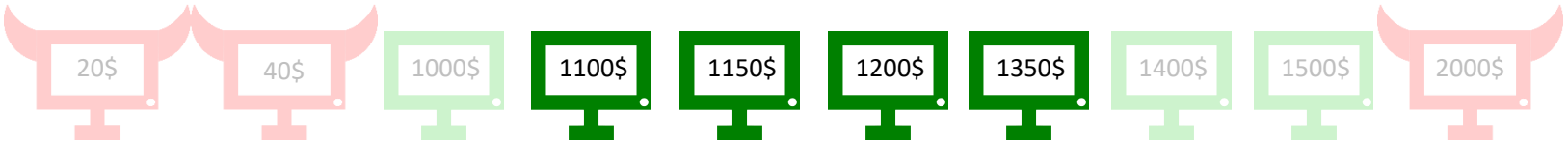
Our Algorithm

- bidders agree on any price inside the interval of all correct bids
  - receive approximations from every node
  - remove **too low** and **too high** bids
  - apply **King algorithm** for agreement



Our Algorithm

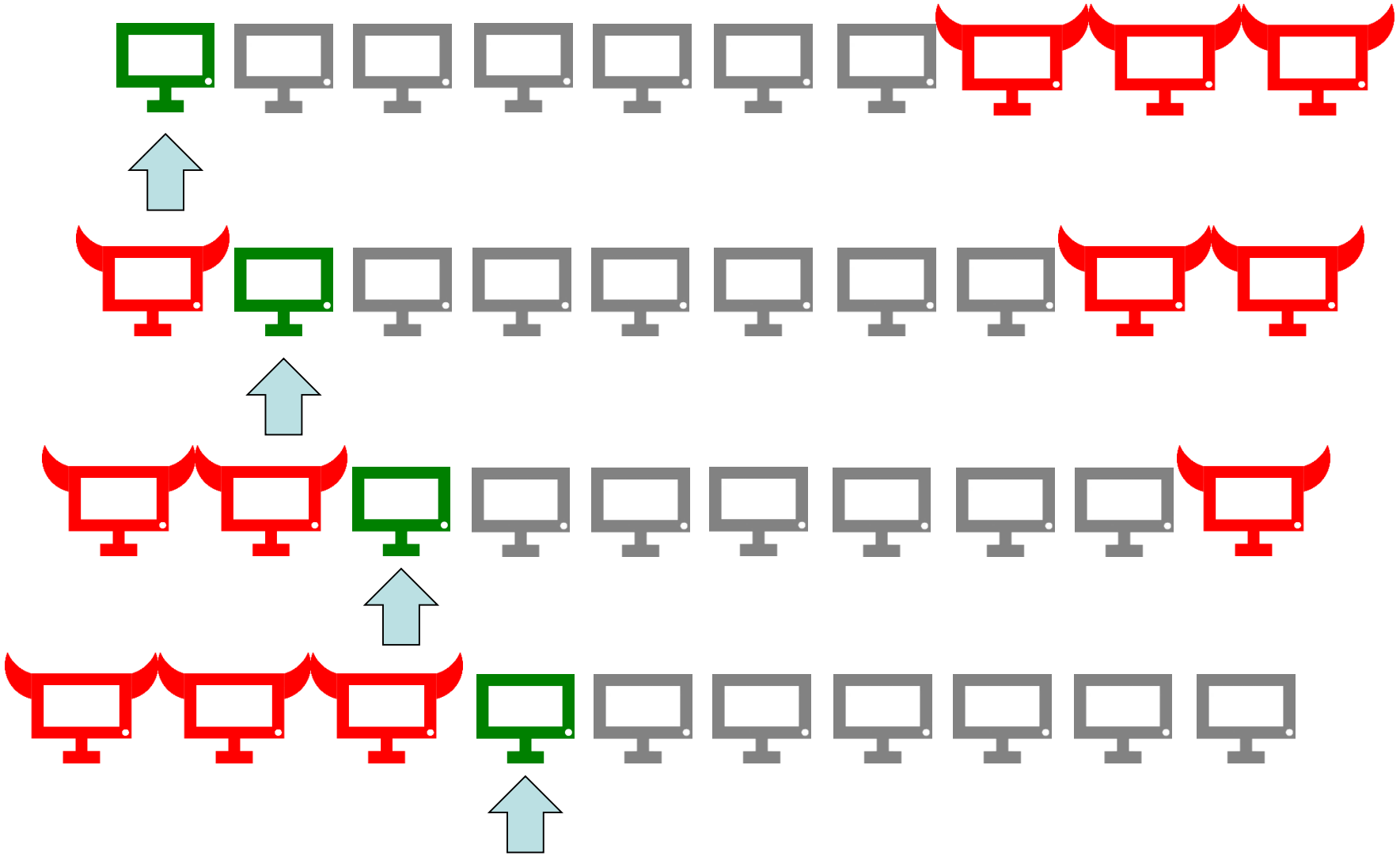
- bidders agree on any price inside the interval of all correct bids
  - receive approximations from every node
  - remove **too low** and **too high** bids
  - apply **King algorithm** for agreement



t+1 rounds and O(n^3) messages

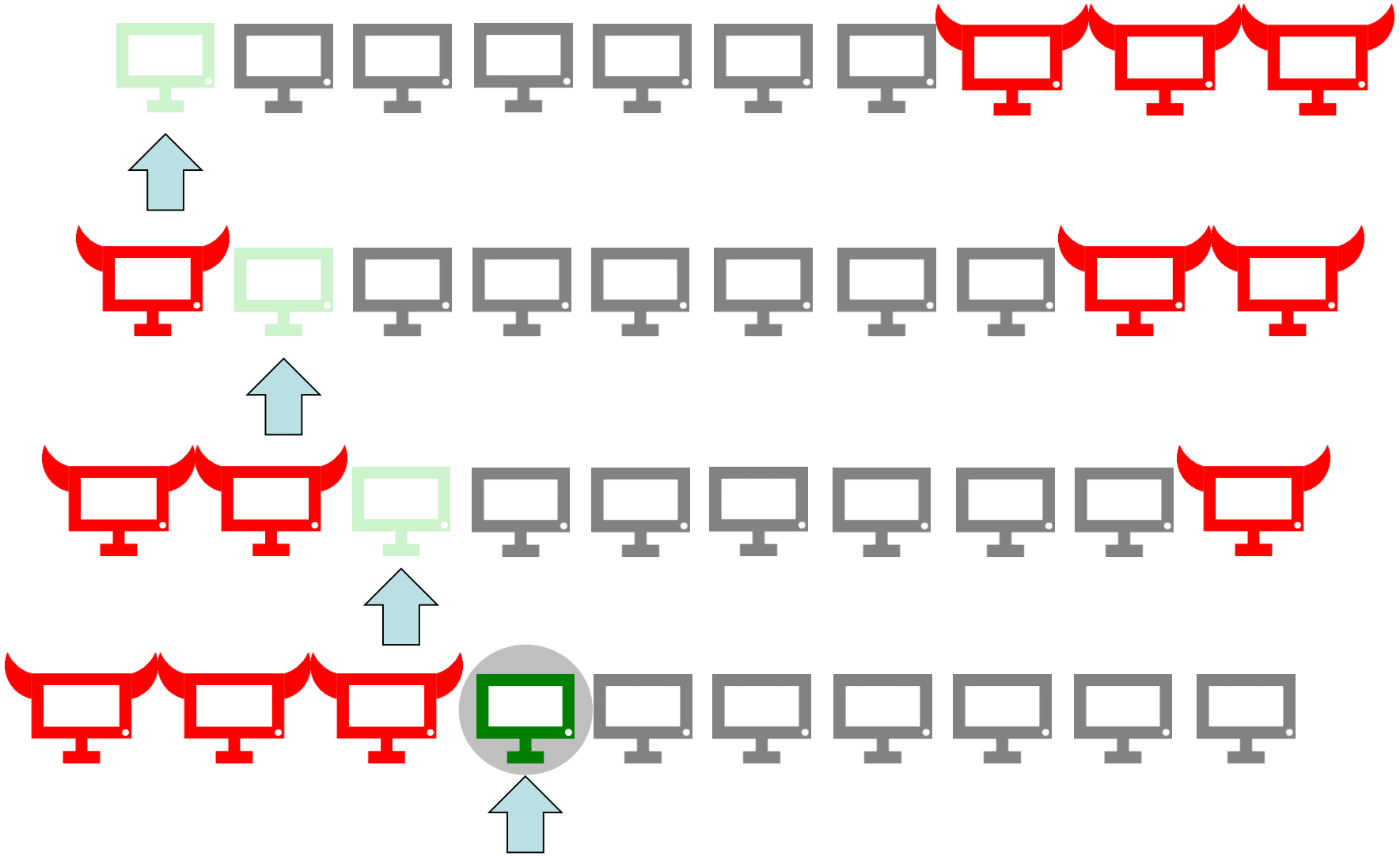
Special Cases - Minimum

10 bids, 3 Byzantine, look for minimum



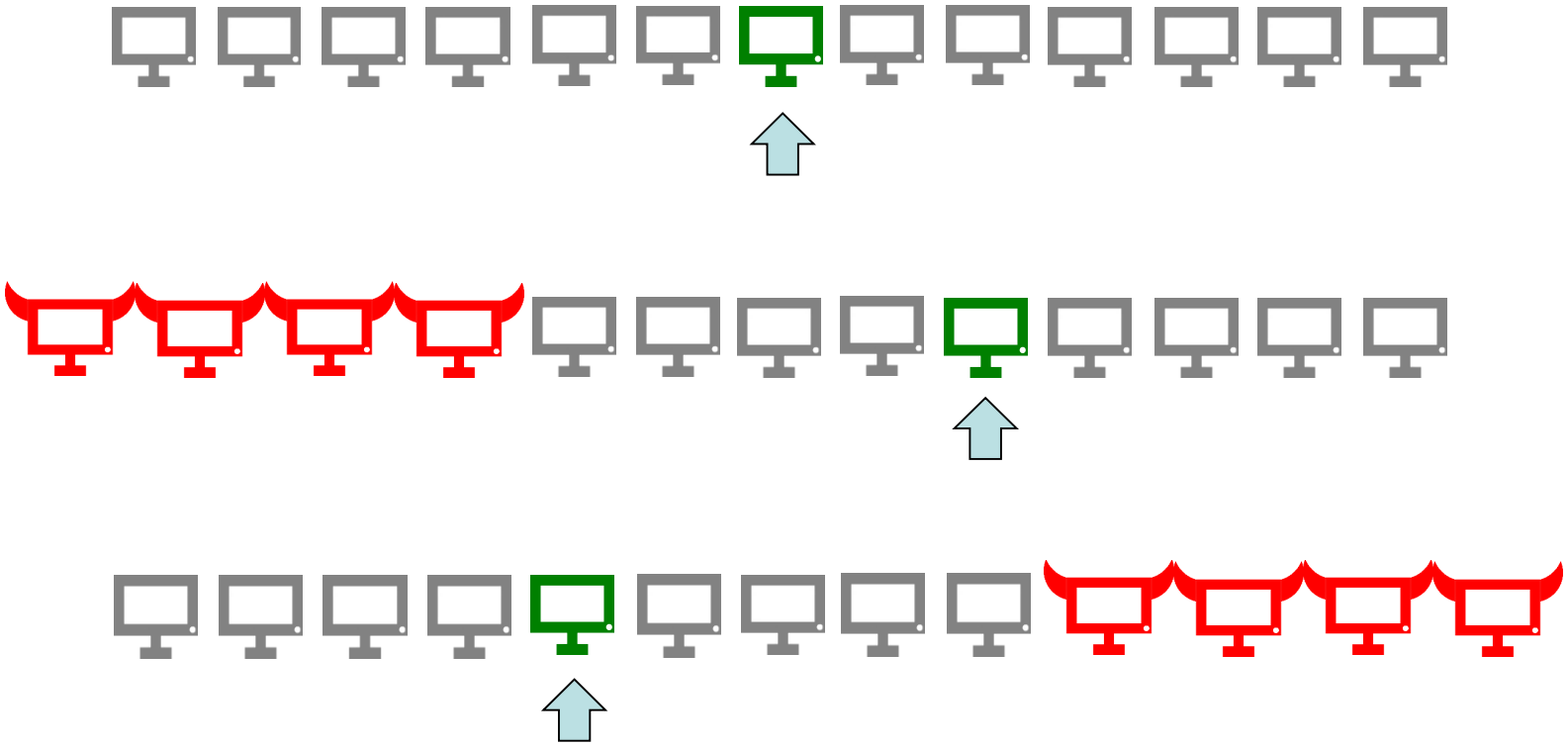
Special Cases - Minimum

10 bids, 3 Byzantine, look for minimum



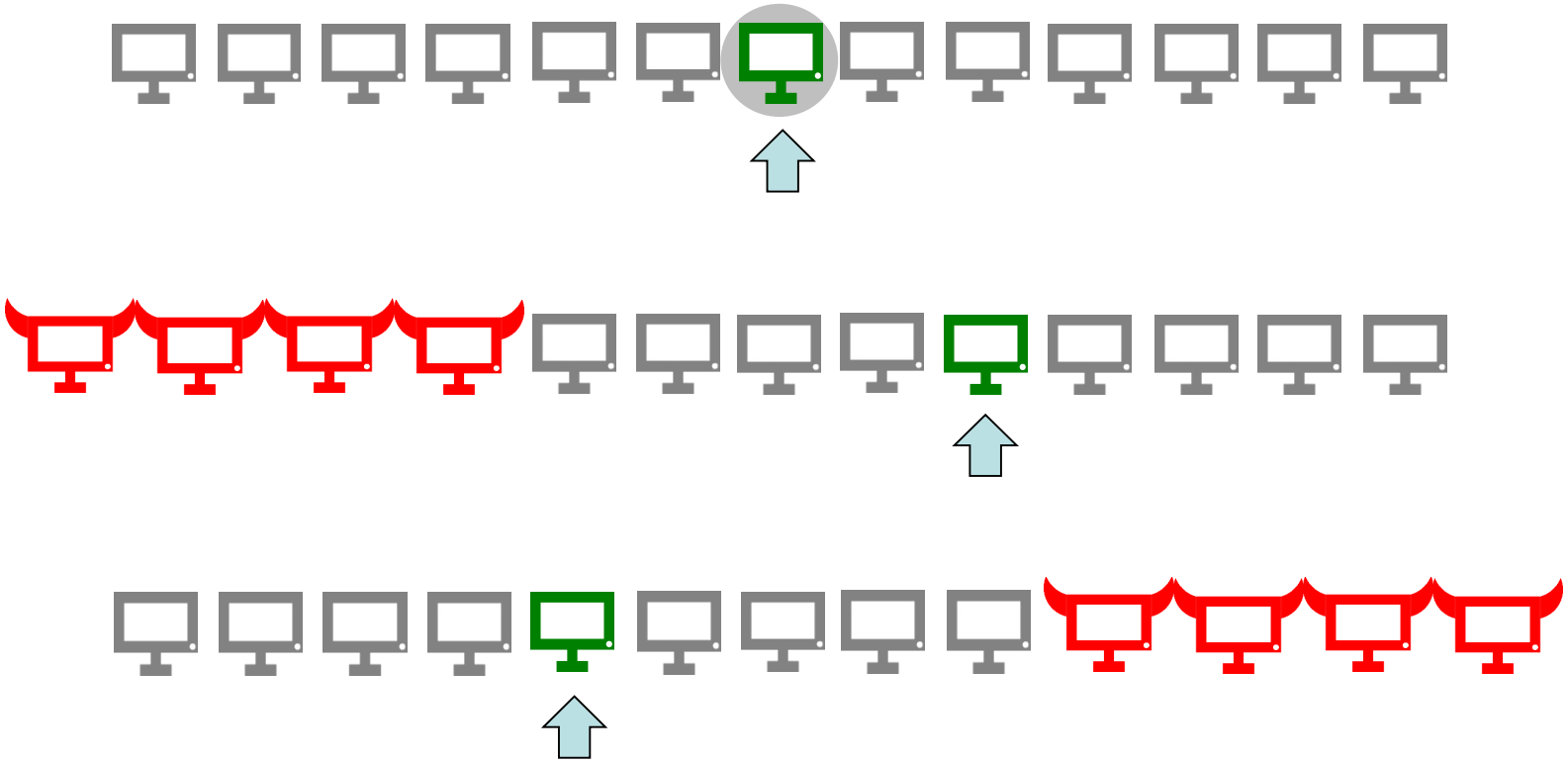
Special Cases – Median

13 bids, 4 Byzantine, look for the median



Special Cases – Median

13 bids, 4 Byzantine, look for the median



What did we achive?

Cow at an auction...	any real-valued agreement
Fair price...	any reasonable agreement value (also min, max, or median)
Bid close to the 4th smallest bid...	Interval Validity


Questions?