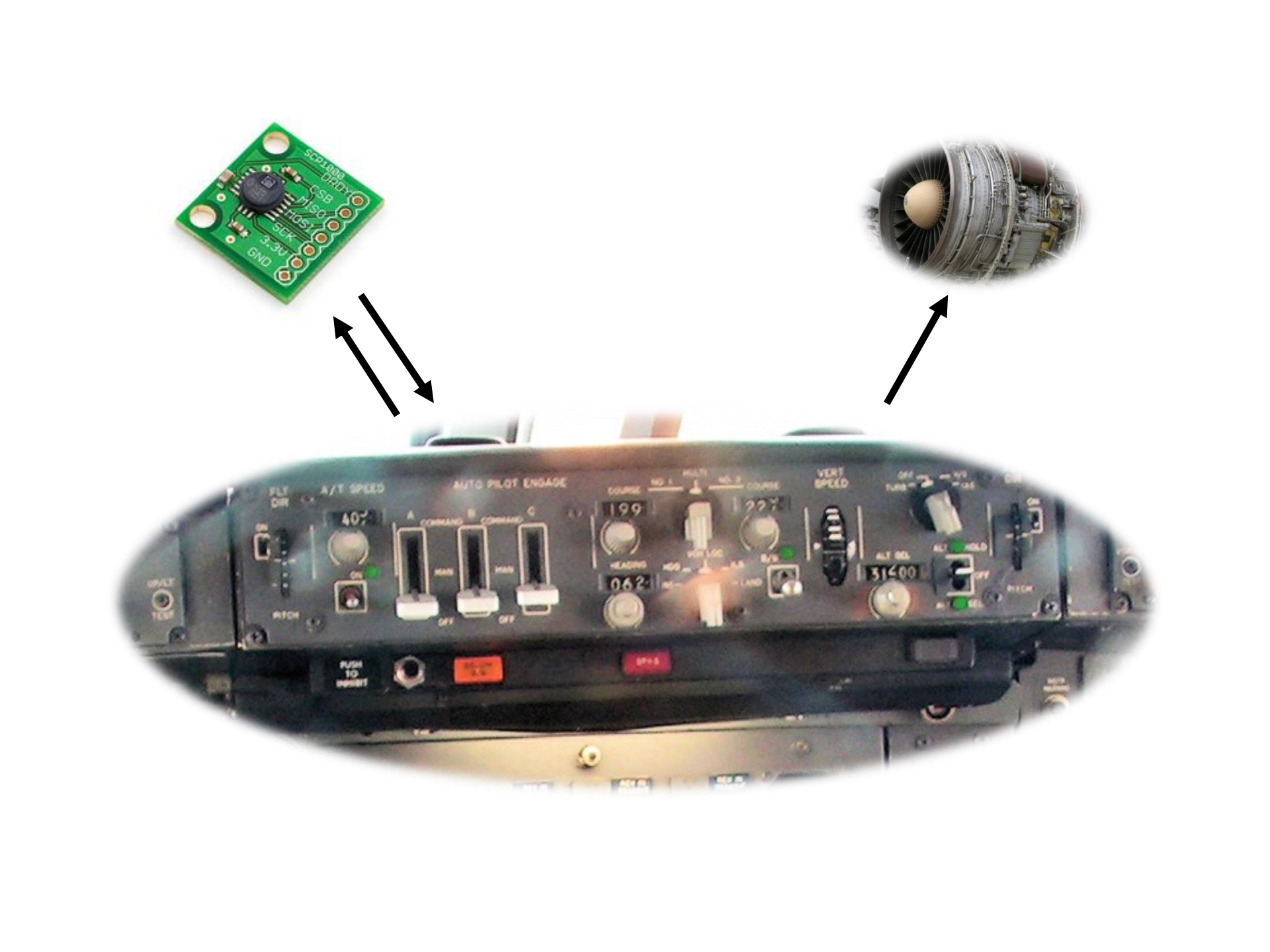
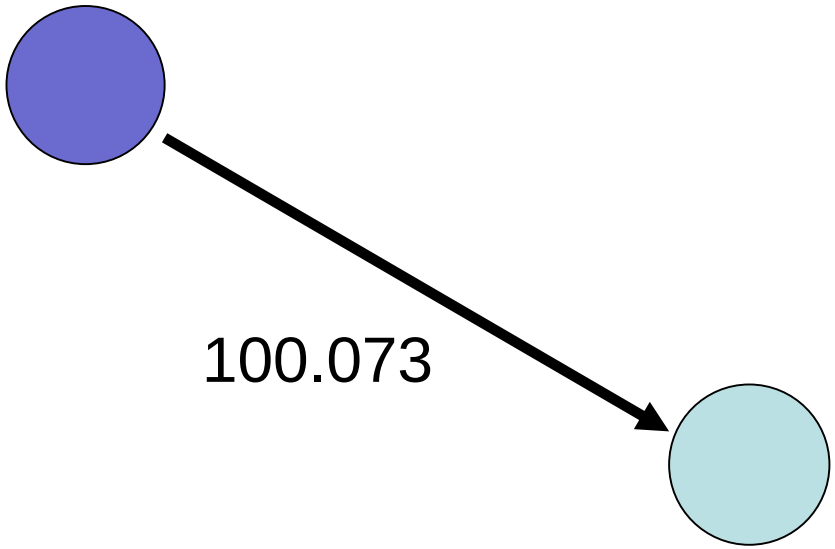
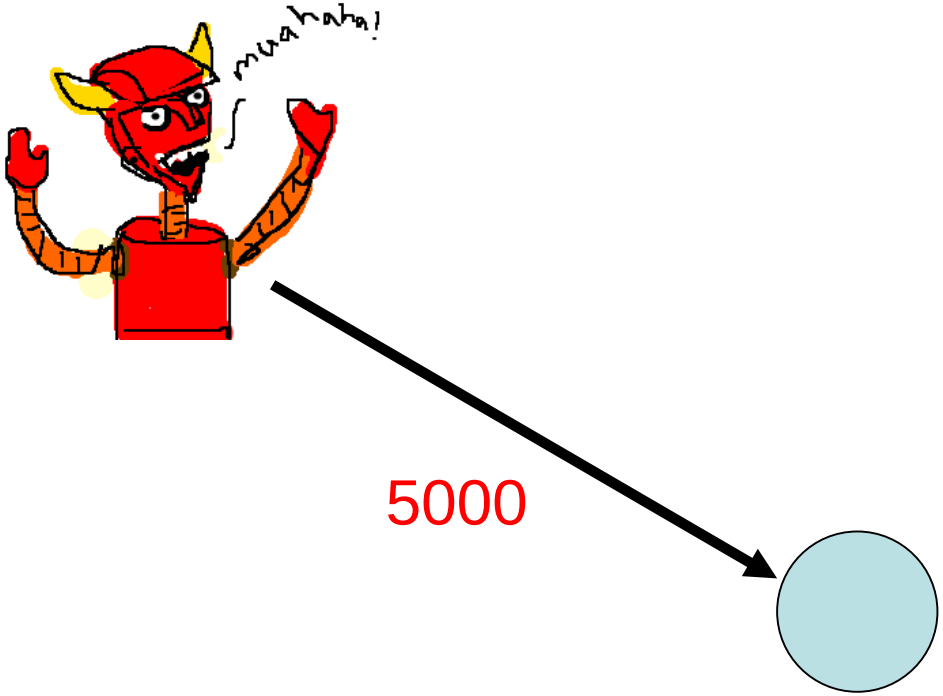
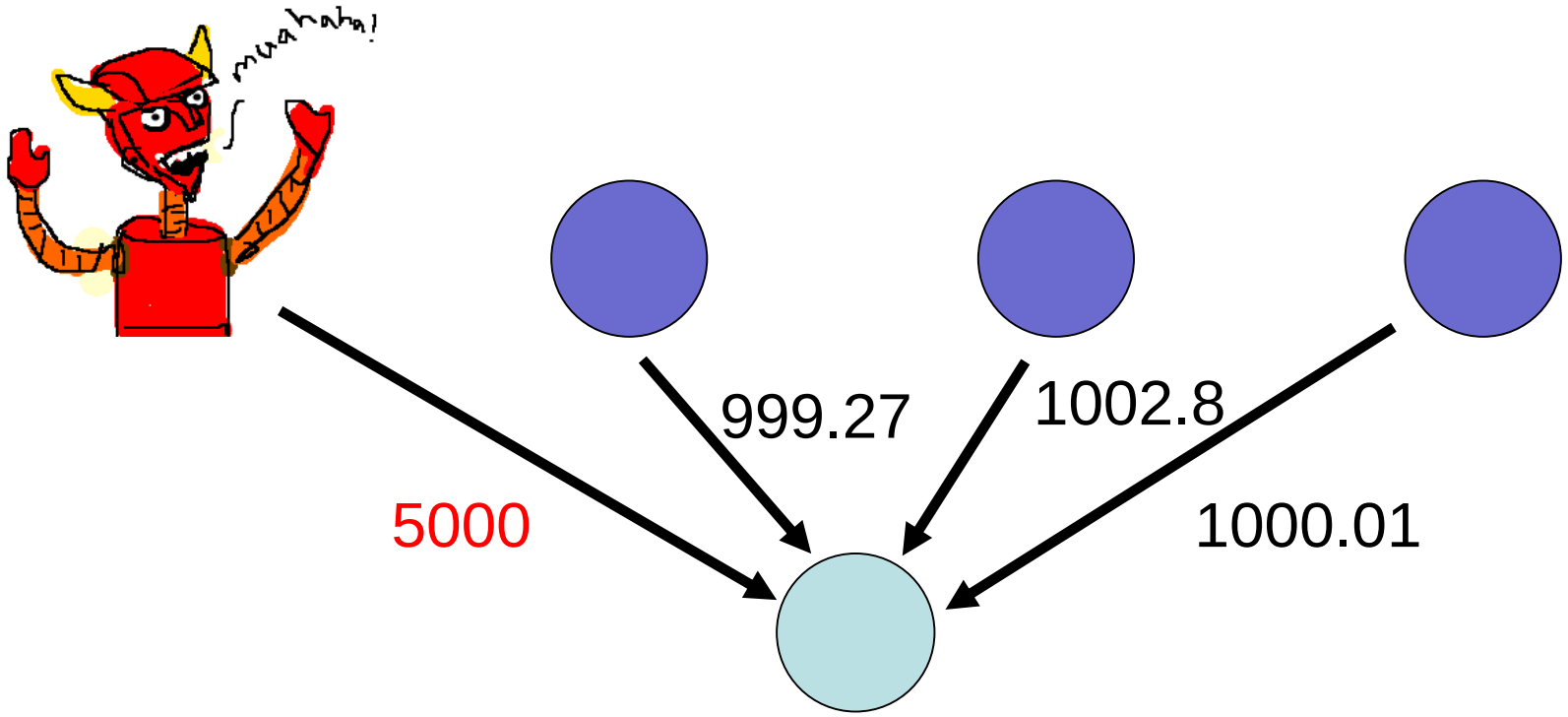
Byzantine Agreement with Median Validity

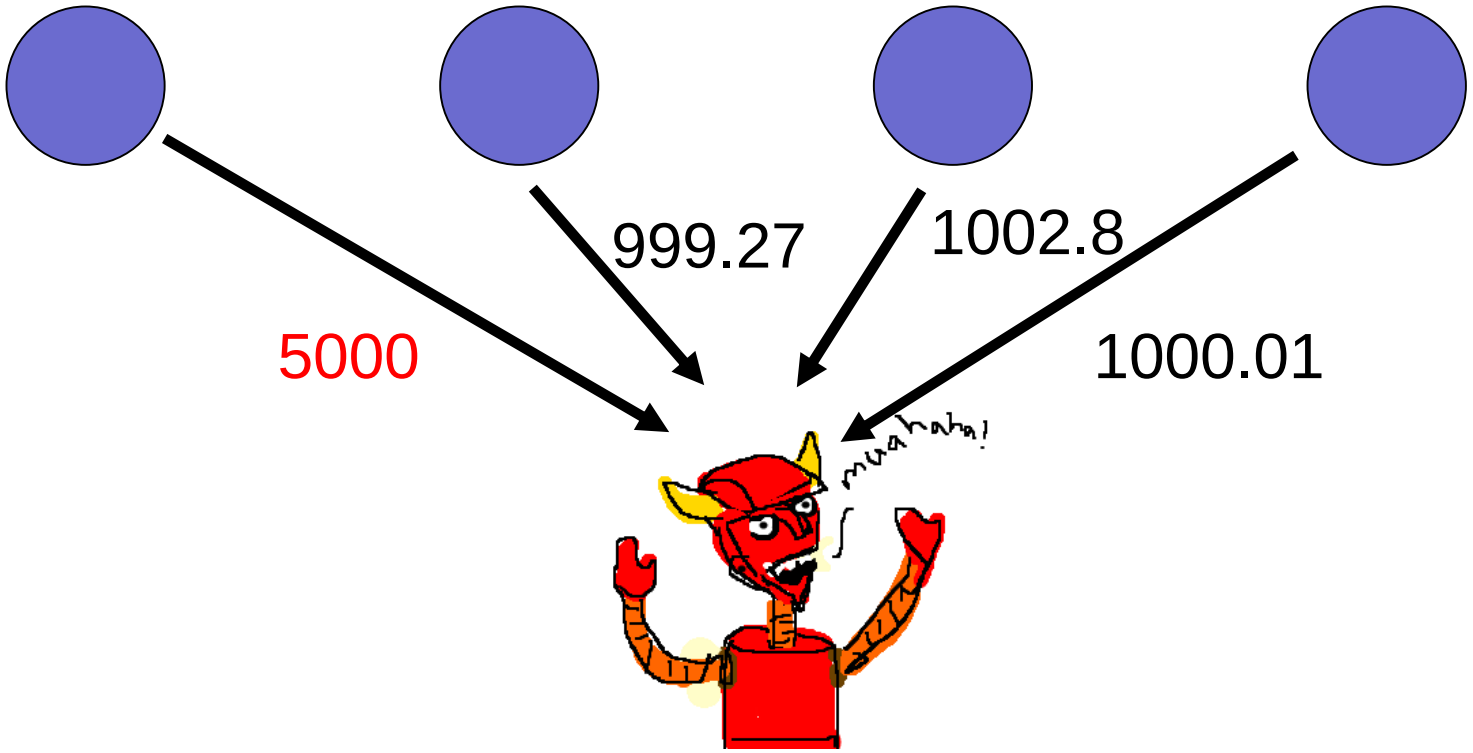
David Stolz *and Roger Wattenhofer*

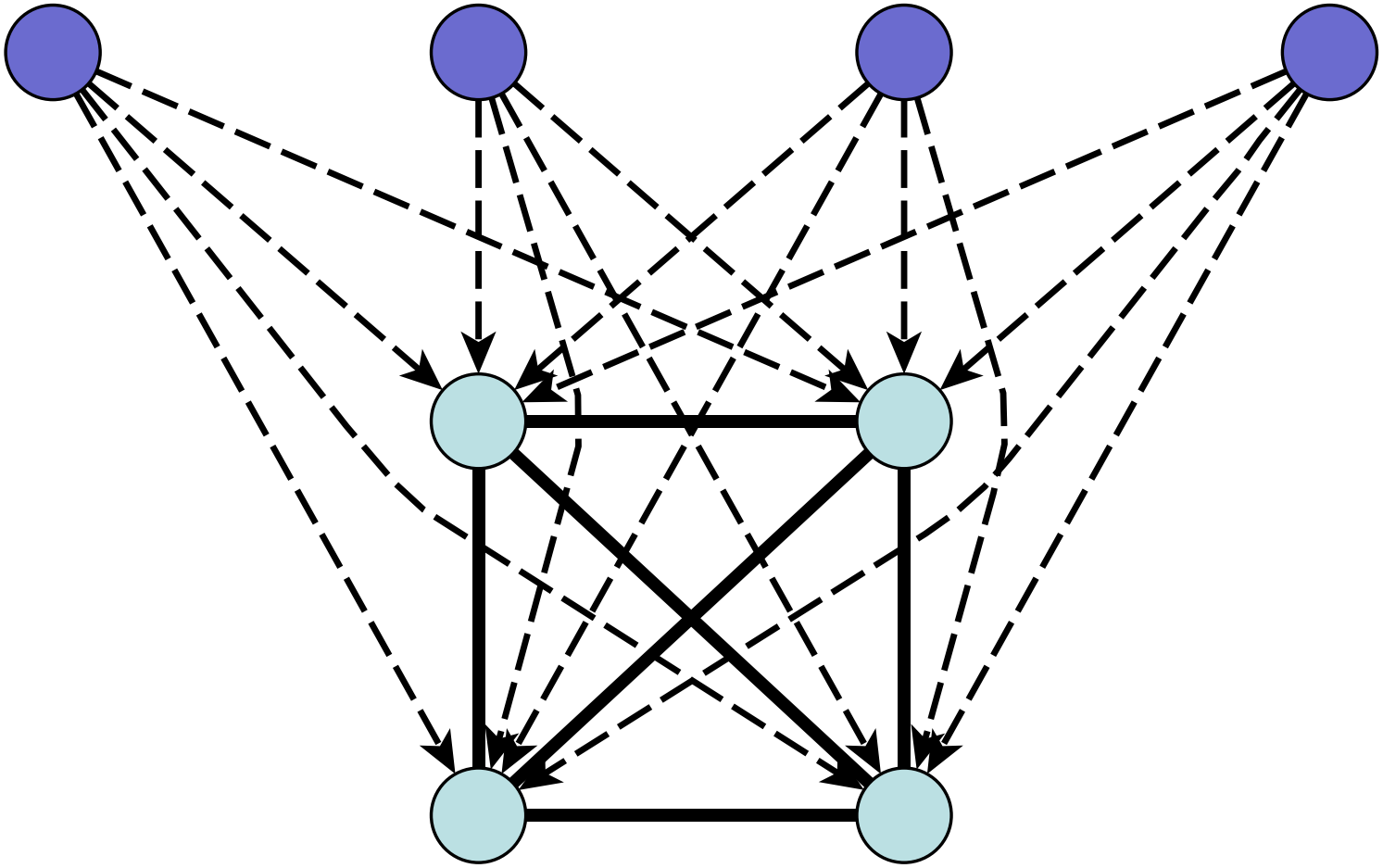

SCP1000
DRDY
CSB
MISO
MOSI
SCK
3.3V
GND
FLT DIR
A/T SPEED
AUTO PILOT ENGAGE
VERT SPEED
199
062
31500
PUSH TO INHIBIT

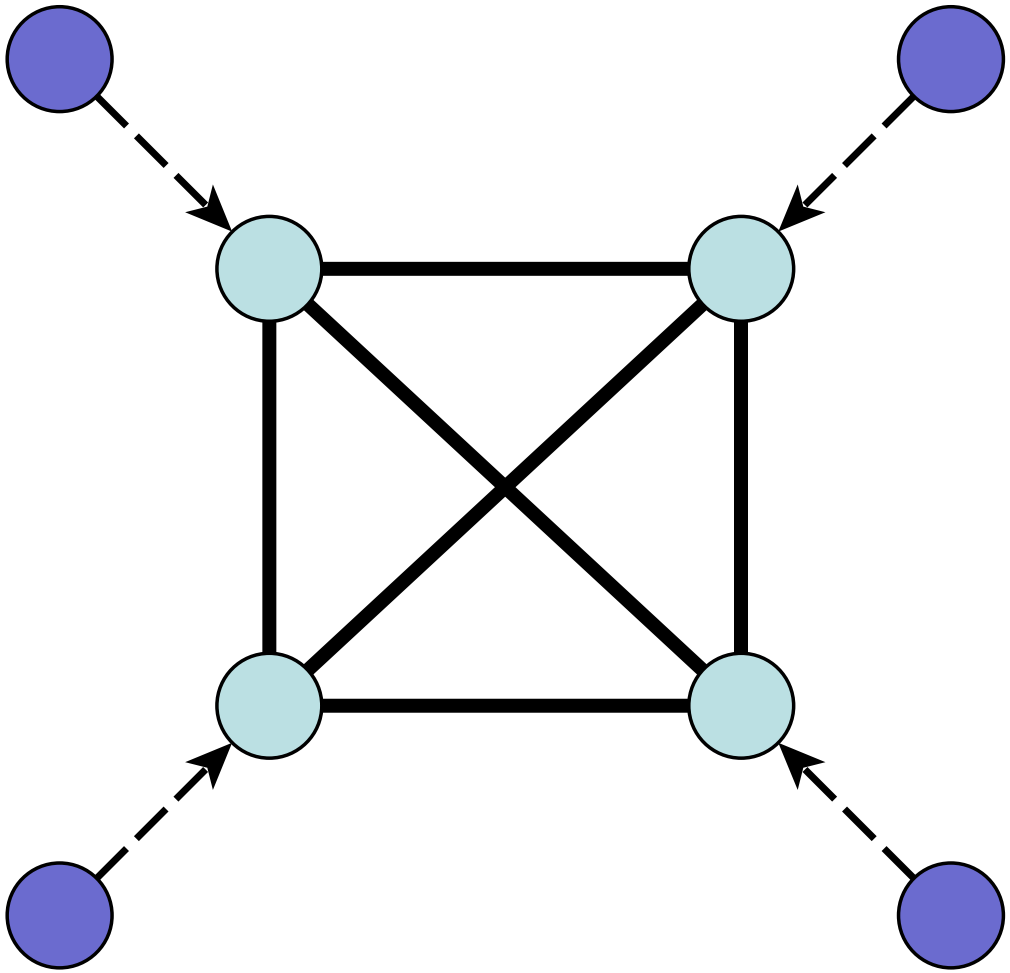

100.073


muahaha!
5000


muahaha!
5000
999.27
1002.8
1000.01


999.27
1002.8
5000
1000.01
muahaha!

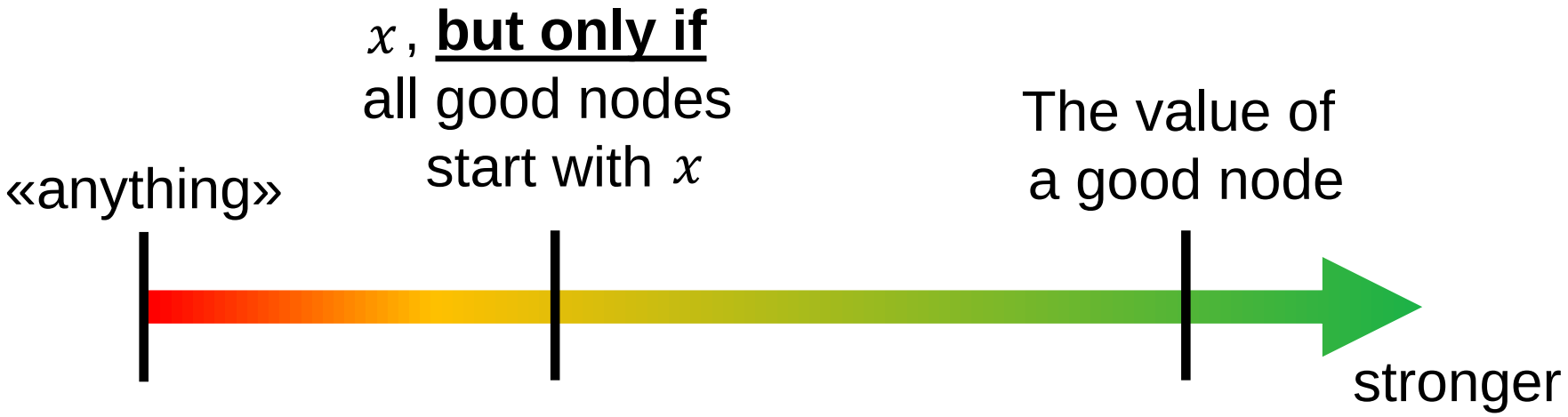




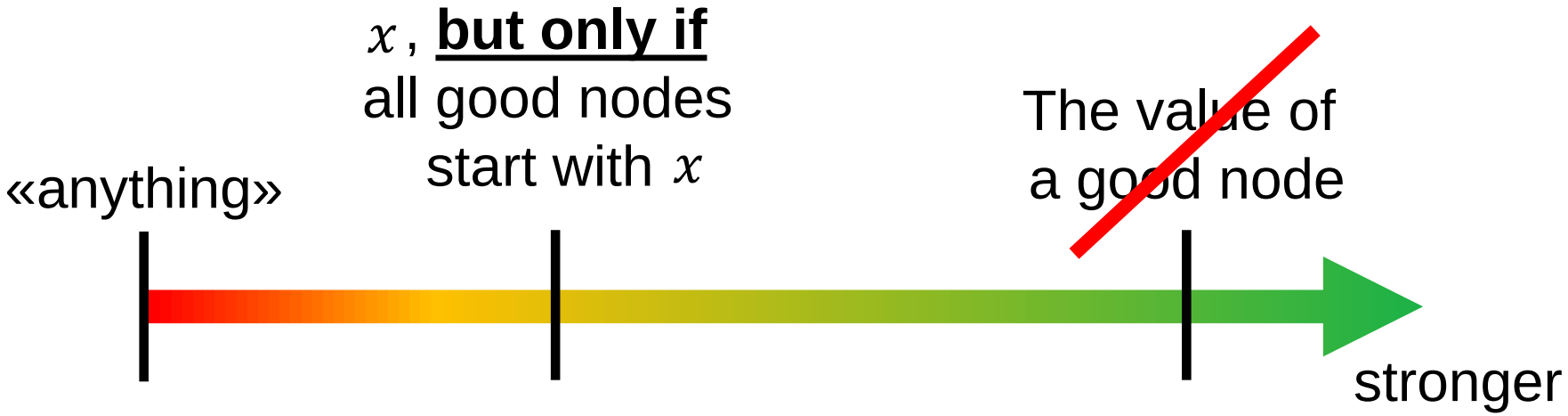
Byzantine Agreement

1. Agreement
2. Termination
3. Validity

Different Validity Properties

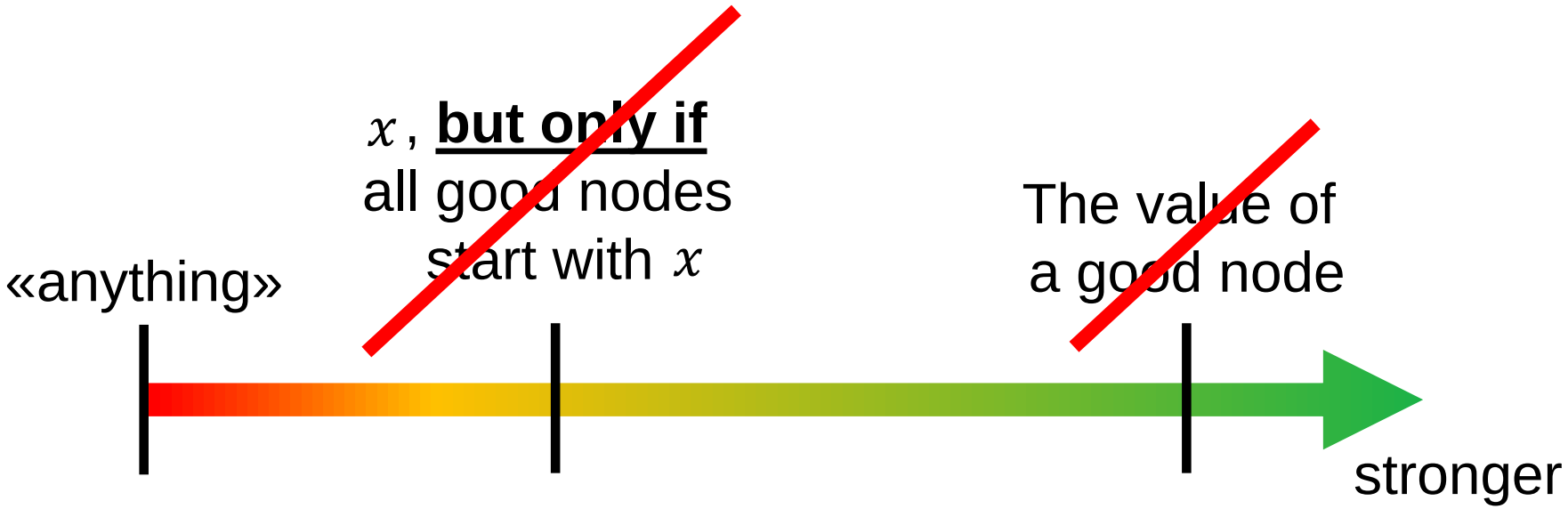


Different Validity Properties for values in $\mathbb{R}$



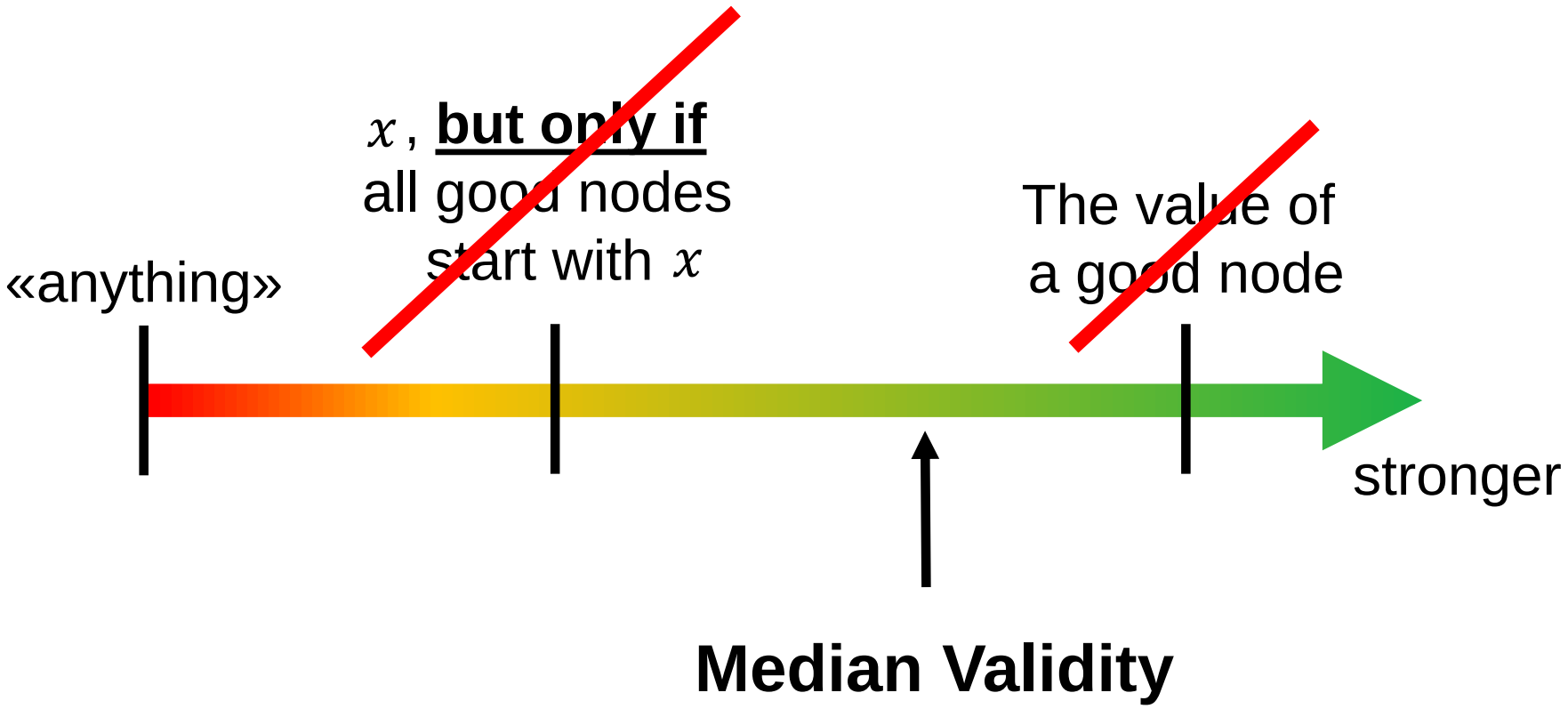
$D \geq 3\mathbb{R}$
[Neiger 94]

Different Validity Properties for values in $\mathbb{R}$



$D \geq 3\mathbb{R}$
[Neiger 94]

Different Validity Properties for values in $\mathbb{R}$



Related Work

- Distributed Average Consensus

  ⇨ no byzantine failures

- Byzantine Multi-Agent Optimization: Part I

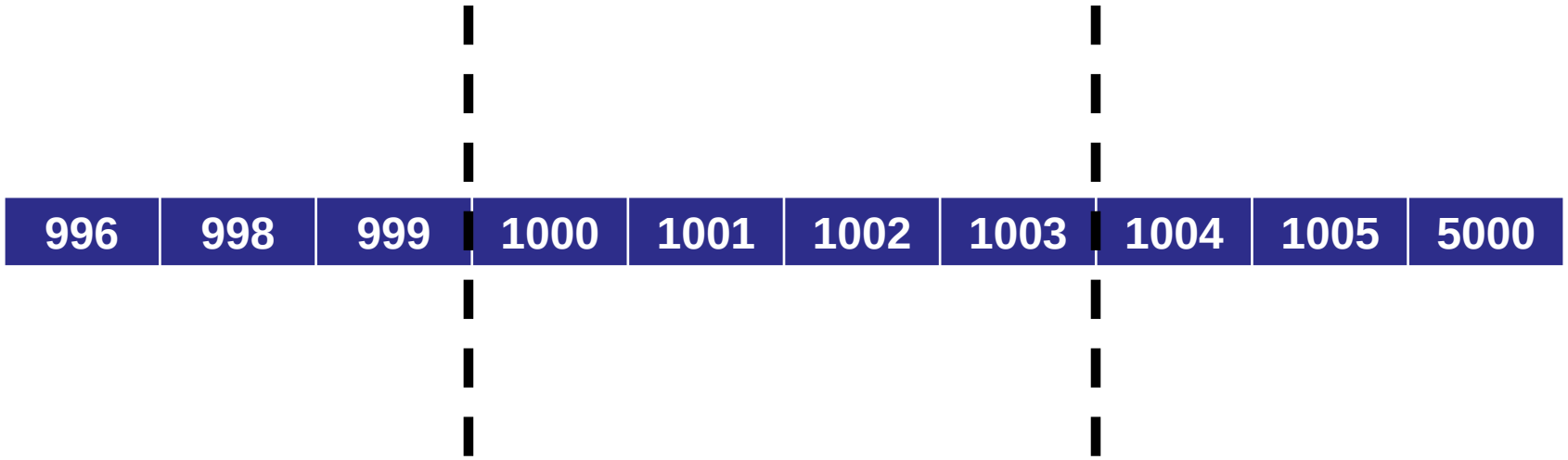
  [Su, Vaidya 15]

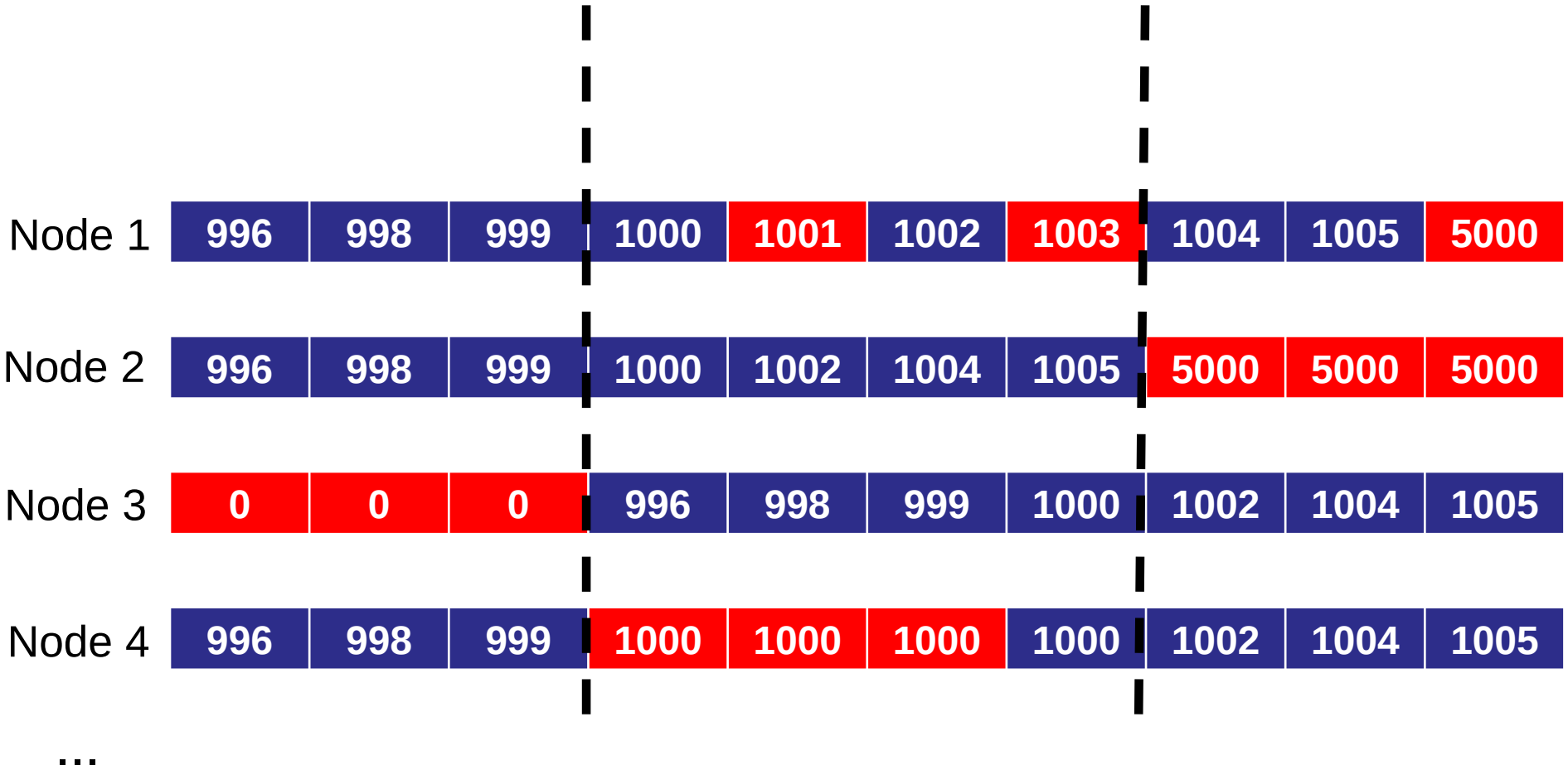
  ⇨ optimization of cost functions

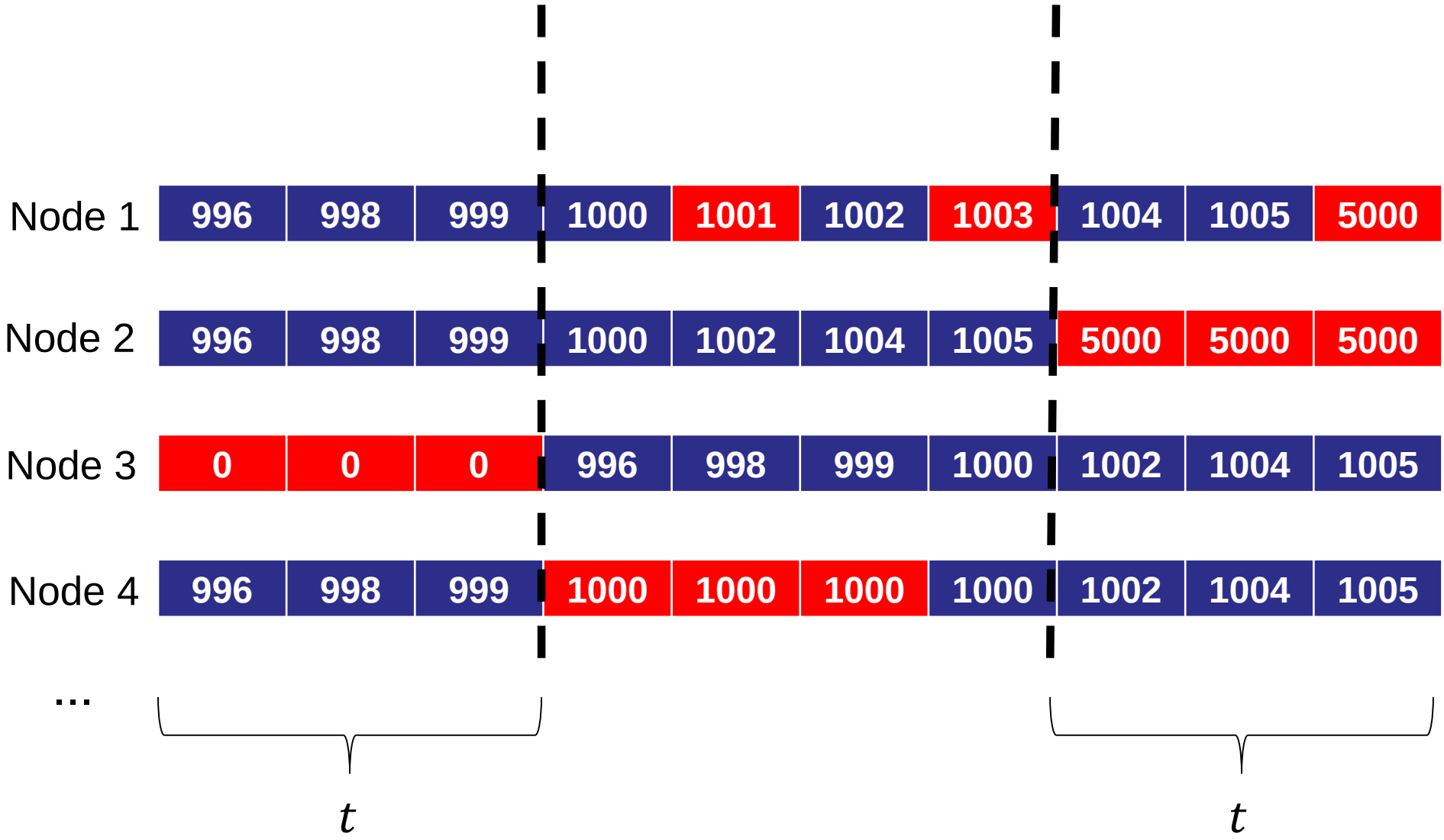
Model

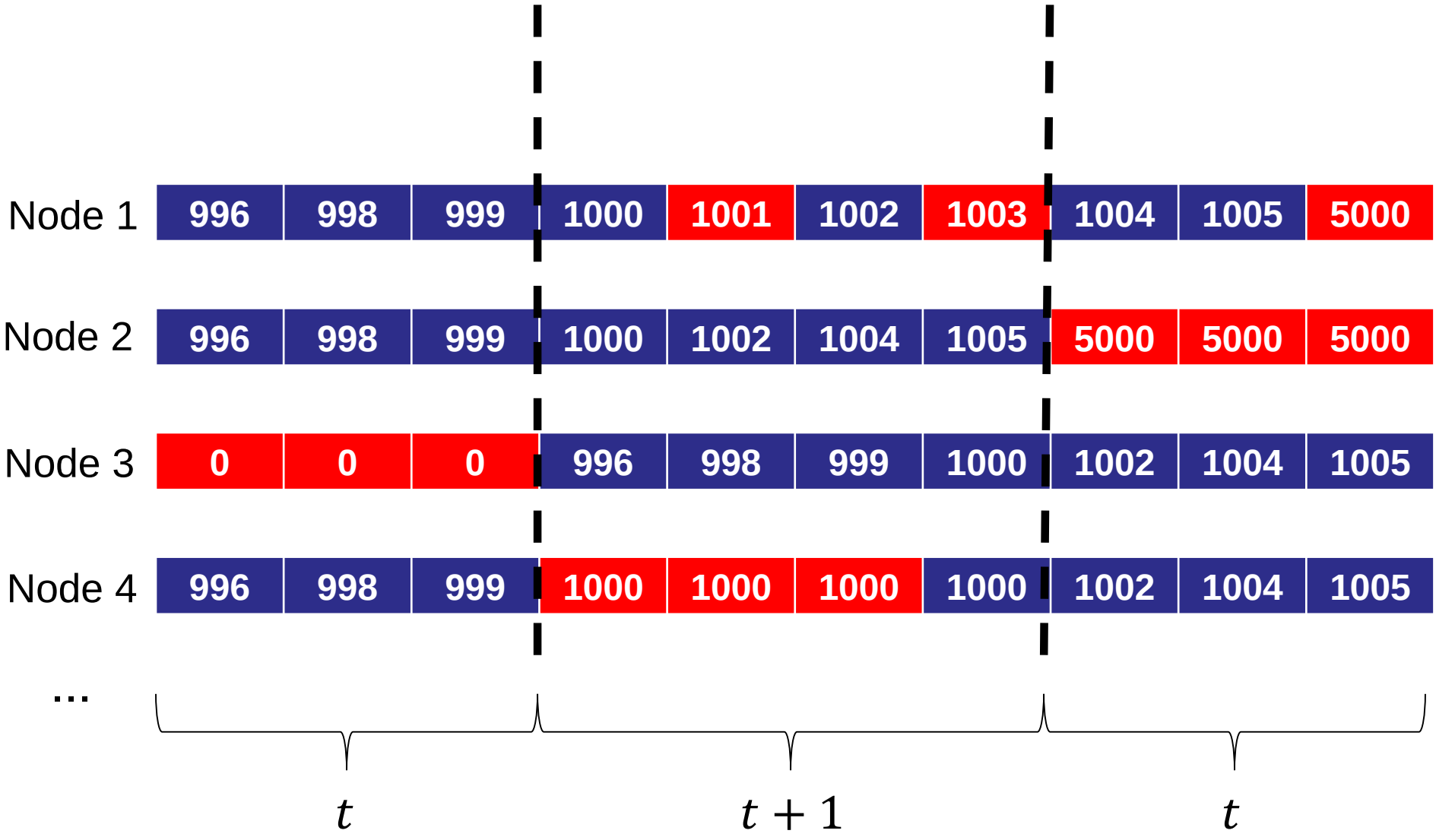
- n nodes
- $f \leq t$ byzantine nodes
- synchronous time

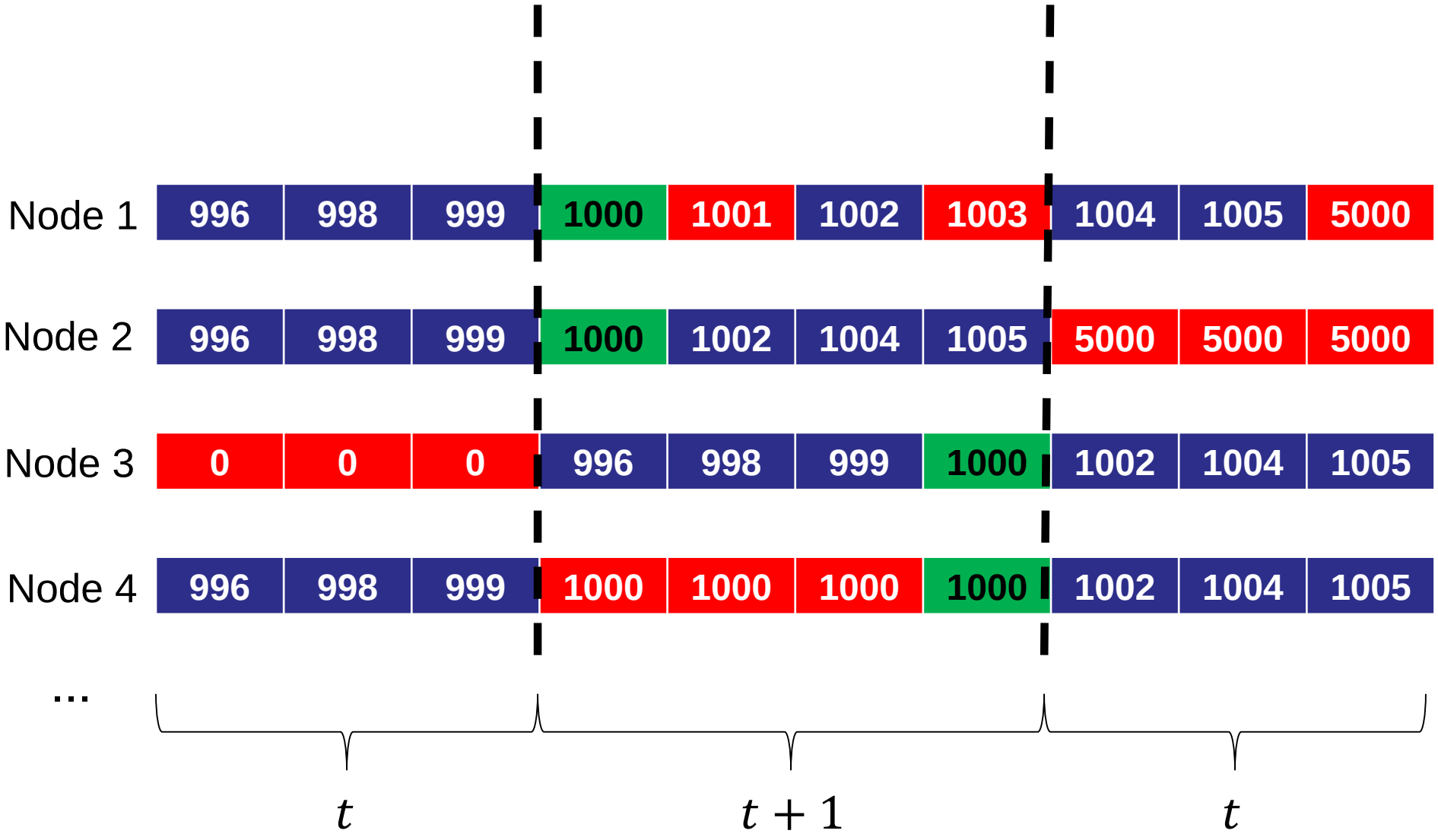
996	998	999	1000	1001	1002	1003	1004	1005	5000

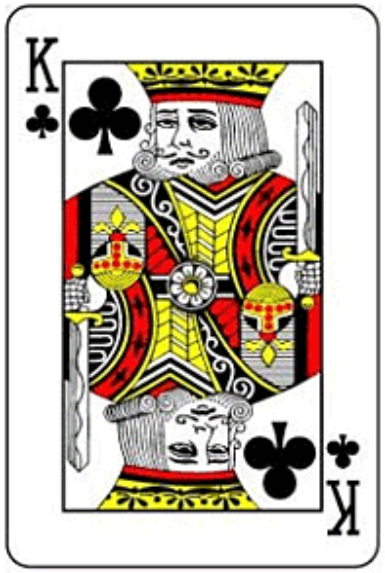

996
998
999
1000
1001
1002
1003
1004
1005
5000


Node 1
996
998
999
1000
1001
1002
1003
1004
1005
5000
Node 2
996
998
999
1000
1002
1004
1005
5000
5000
5000
Node 3
0
0
0
996
998
999
1000
1002
1004
1005
Node 4
996
998
999
1000
1000
1000
1000
1002
1004
1005
...


Node 1
996 998 999 1000 1001 1002 1003 1004 1005 5000
Node 2
996 998 999 1000 1002 1004 1005 5000 5000 5000
Node 3
0 0 0 996 998 999 1000 1002 1004 1005
Node 4
996 998 999 1000 1000 1000 1000 1002 1004 1005
...
t
t


Node 1
996
998
999
1000
1001
1002
1003
1004
1005
5000
Node 2
996
998
999
1000
1002
1004
1005
5000
5000
5000
Node 3
0
0
0
996
998
999
1000
1002
1004
1005
Node 4
996
998
999
1000
1000
1000
1000
1002
1004
1005
...
t
$t+1$
t

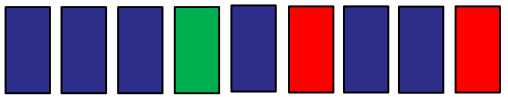

Node 1
996
998
999
1000
1001
1002
1003
1004
1005
5000
Node 2
996
998
999
1000
1002
1004
1005
5000
5000
5000
Node 3
0
0
0
996
998
999
1000
1002
1004
1005
Node 4
996
998
999
1000
1000
1000
1000
1002
1004
1005
...
t
$t+1$
t



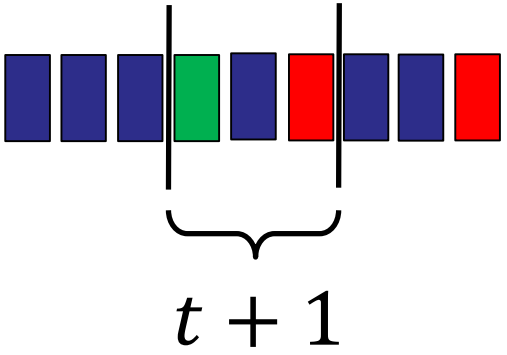

J
9
UNDER
UNDER
K

Setup Stage

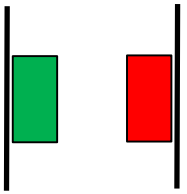
- Broadcast & Gather all values



- Remove potential outliers



- Broadcast & Gather all bounds



Search Stage ($f + 1$ phases)

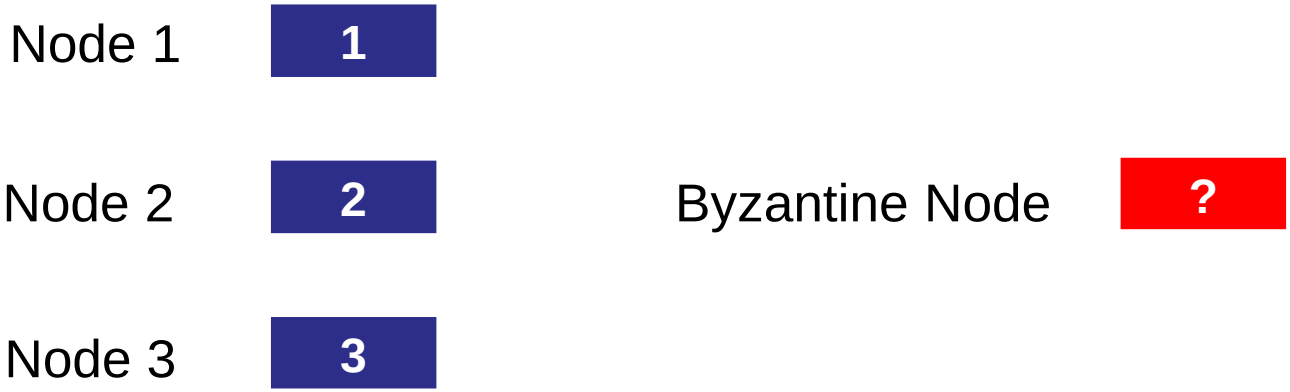
- Broadcast current value

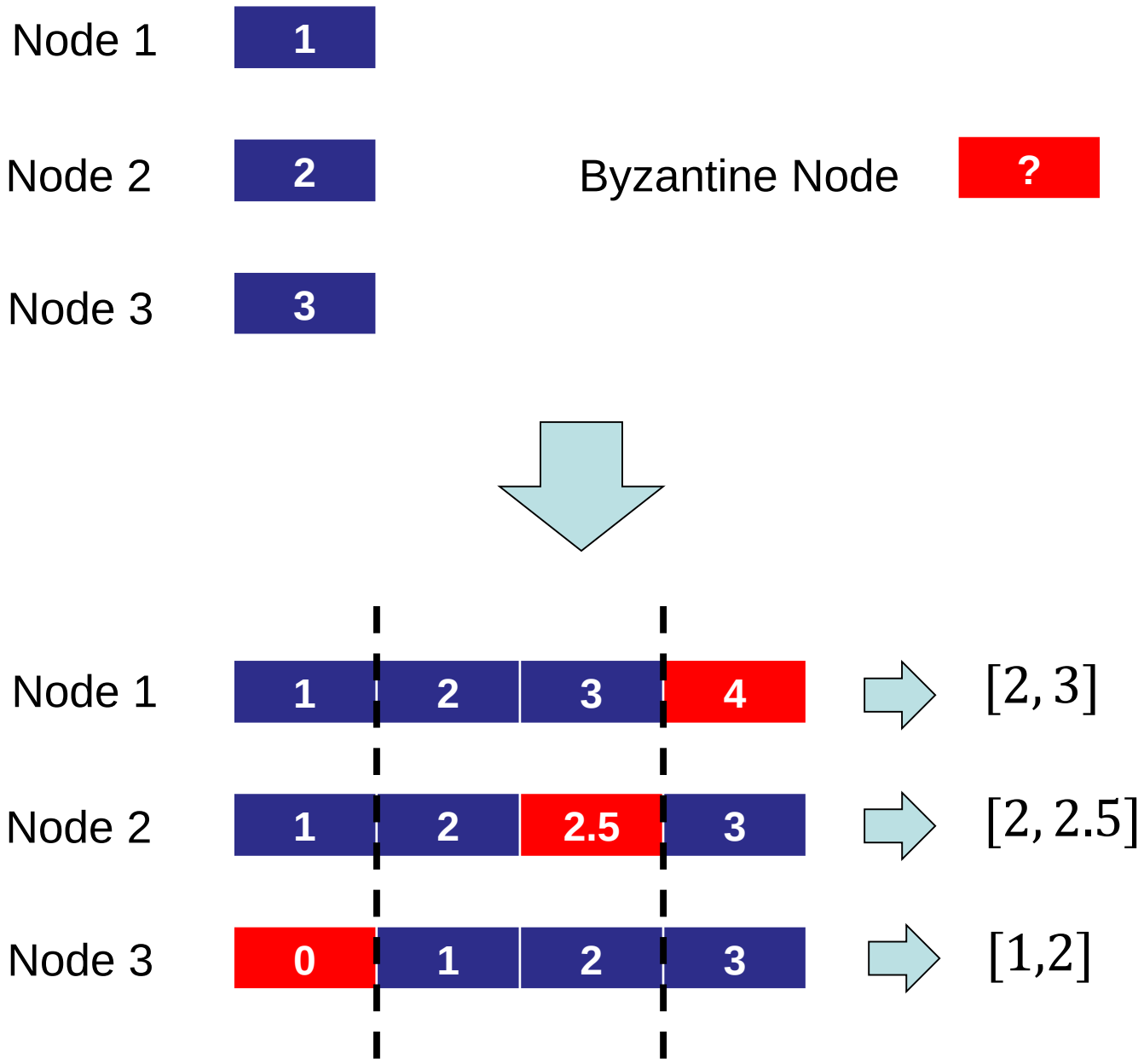
  ⇨ **<u>if</u>** agreement already, don't change

- If no agreement, let jack suggest a value

  ⇨ support the suggestion, **<u>if</u>** in own interval

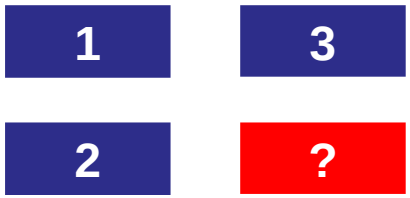
- Adapt jack suggestion, **<u>if</u>** enough support


Node 1
1
Node 2
2
Byzantine Node
?
Node 3
3


Node 1
1
Node 2
2
Byzantine Node
?
Node 3
3
Node 1
1
2
3
4
[2, 3]
Node 2
1
2
2.5
3
[2, 2.5]
Node 3
0
1
2
3
[1,2]

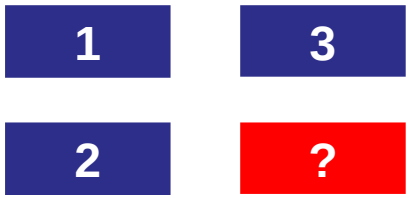
1. Phase

Step 1
Is there already Agreement?



1. Phase

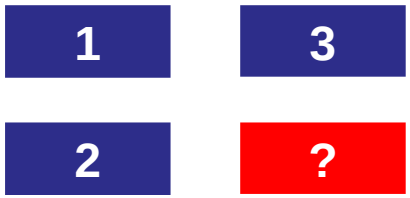
Step 1
Is there already Agreement?



Step 2
Byzantine Jack

1. Phase

Step 1
Is there already Agreement?



Step 2
Byzantine Jack

Step 3
Support Jack?

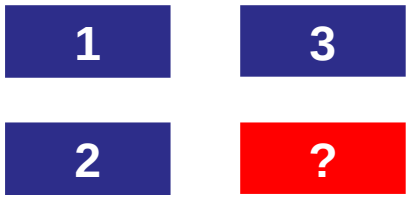
$[2, 2.5]$

$[2, 3]$ $[1,2]$

⇨ **No!**

1. Phase

Step 1
Is there already Agreement?



Step 2
Byzantine Jack

Step 3
Support Jack?

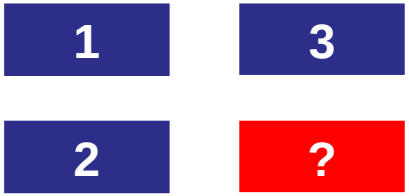
$[2, 2.5]$

$[2, 3]$ $[1,2]$

⇨ **No!**

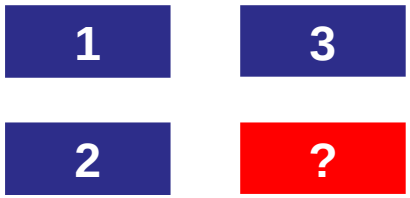
2. Phase

Step 1
Is there already Agreement?



1. Phase

Step 1
Is there already Agreement?



Step 2
Byzantine Jack

Step 3
Support Jack?

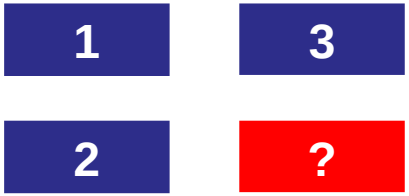
$[2, 2.5]$

$[2, 3]$ $[1,2]$

No!

2. Phase

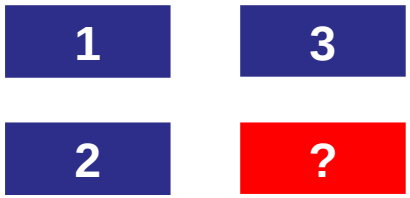
Step 1
Is there already Agreement?



Step 2
Good Jack

1. Phase

Step 1
Is there already Agreement?



Step 2
Byzantine Jack

Step 3
Support Jack?

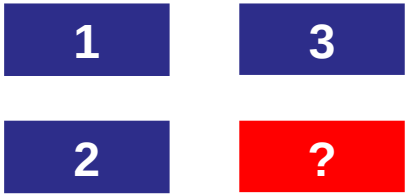
$[2, 2.5]$

$[2, 3]$ $[1,2]$

⇨ **No!**

2. Phase

Step 1
Is there already Agreement?



Step 2
Good Jack

Step 3
Support Jack?

$[2, 2.5]$

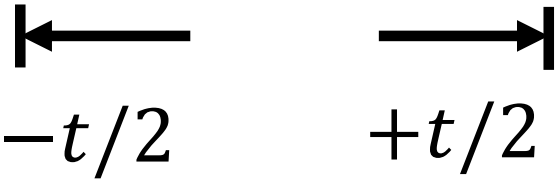
$[2, 3]$ $[1,2]$

⇨ **Yes!**

Only good values

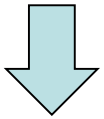
Median Validity

Lower bound (tight)

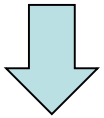


Conclusion

Validity property is essential



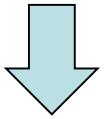
Median Validity



Efficiently achievable

Optimal* time	$\boldsymbol{O}(t+1)$ rounds
Optimal resilience	$n > 3t$
Small messages	1 value / message

* if $f = t$



Good quality

2-Approximation in index distance
Always in the range of the good values