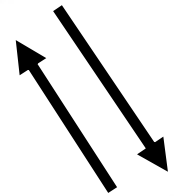
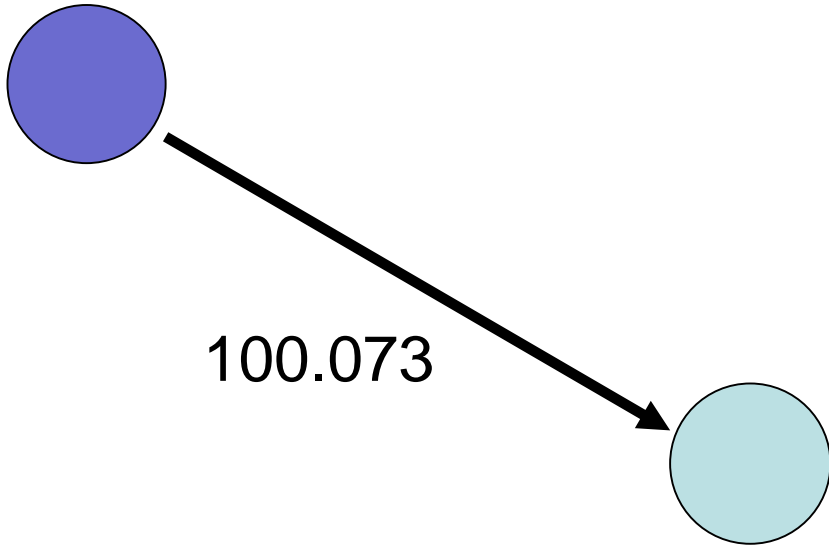


# *Byzantine Agreement with Median Validity*

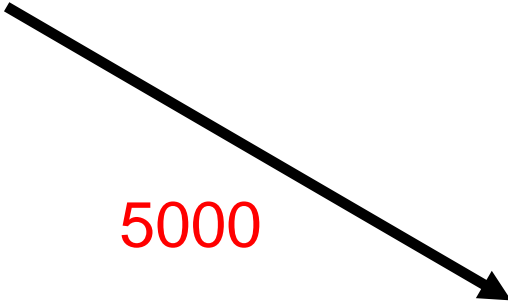
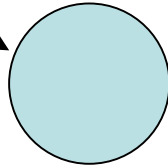
*David Stolz and Roger Wattenhofer*

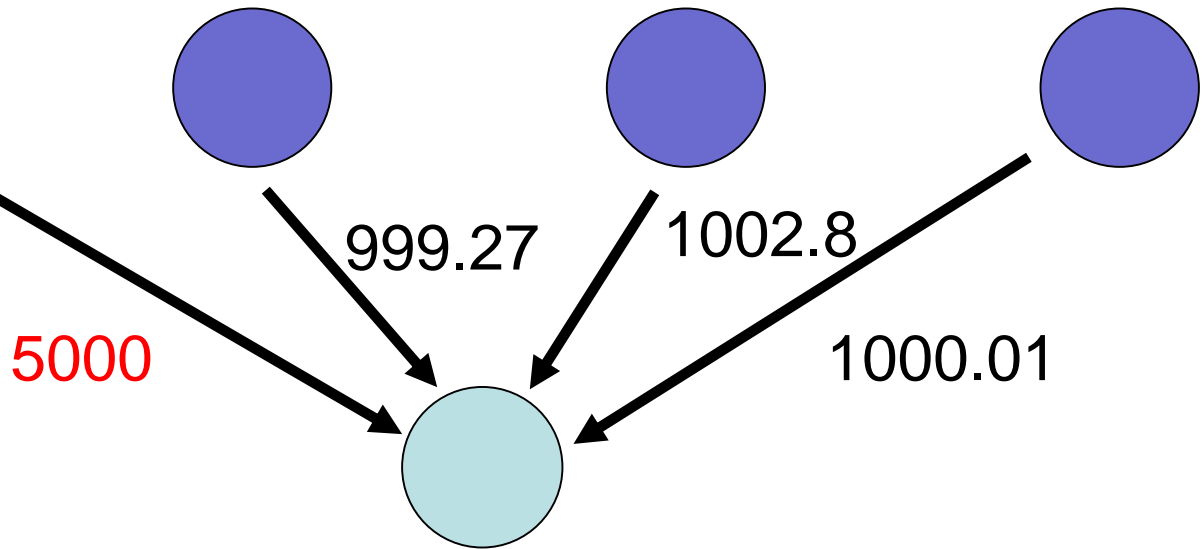


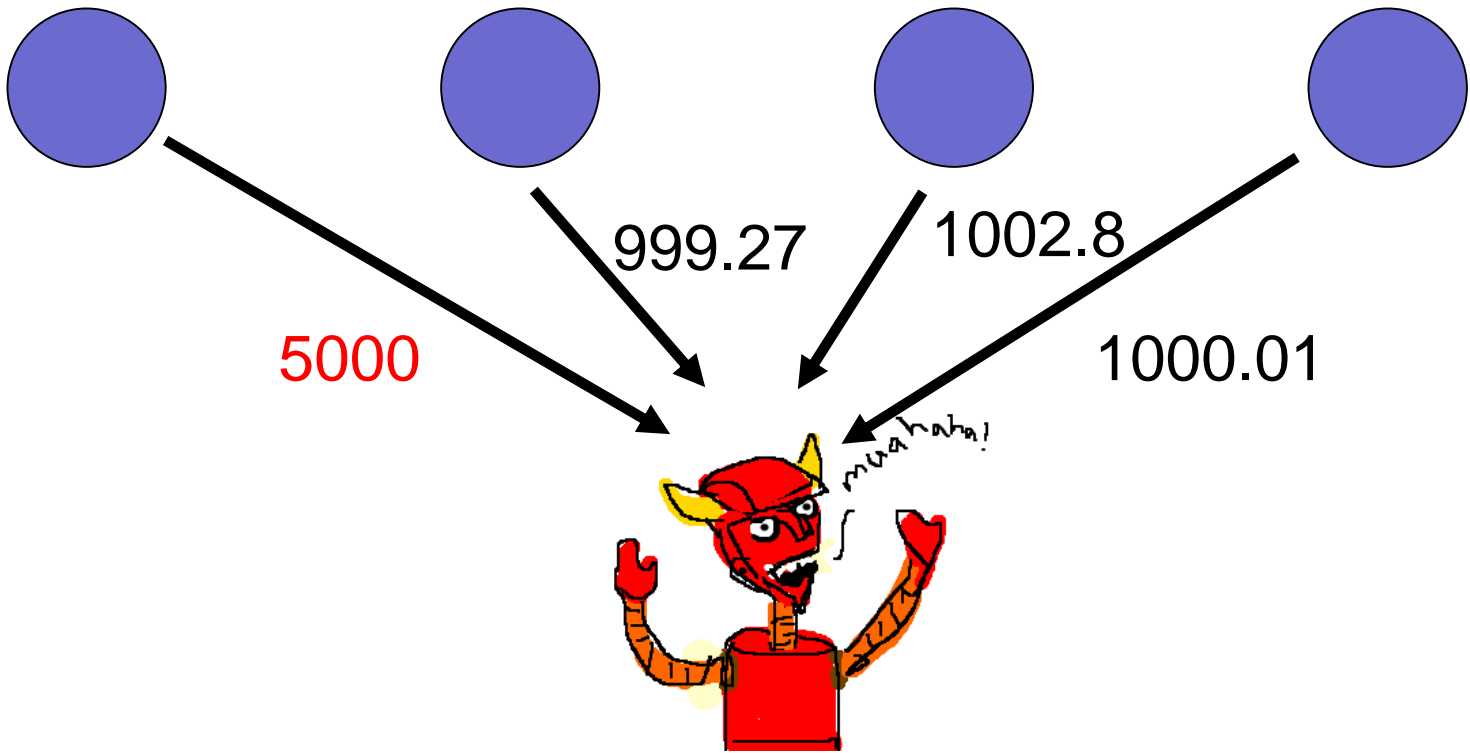


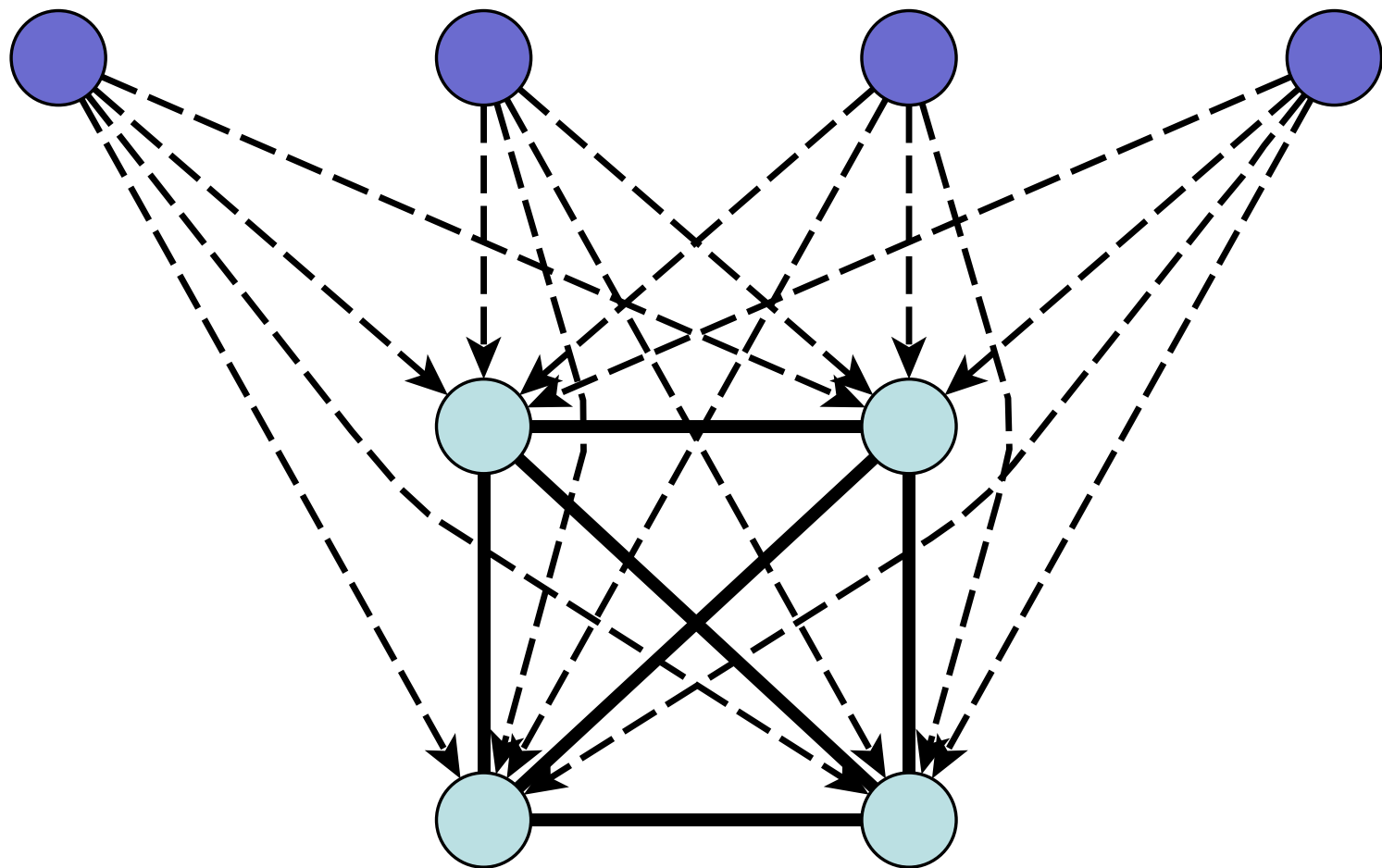


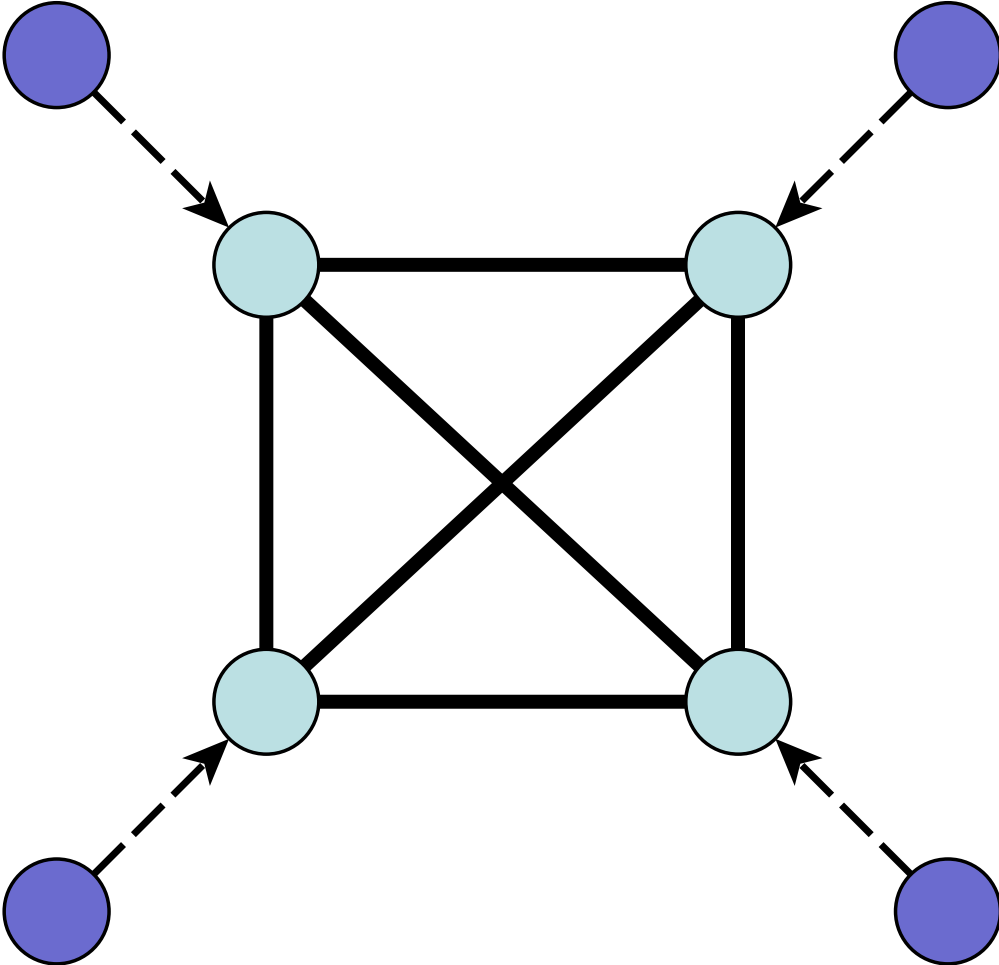
5000













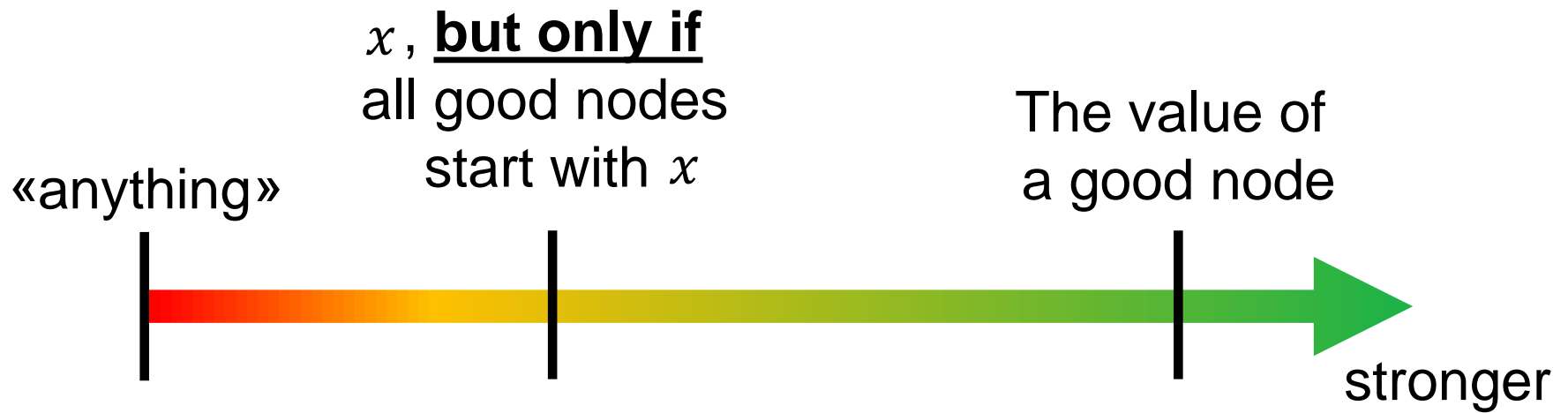
# Byzantine Agreement

1. Agreement

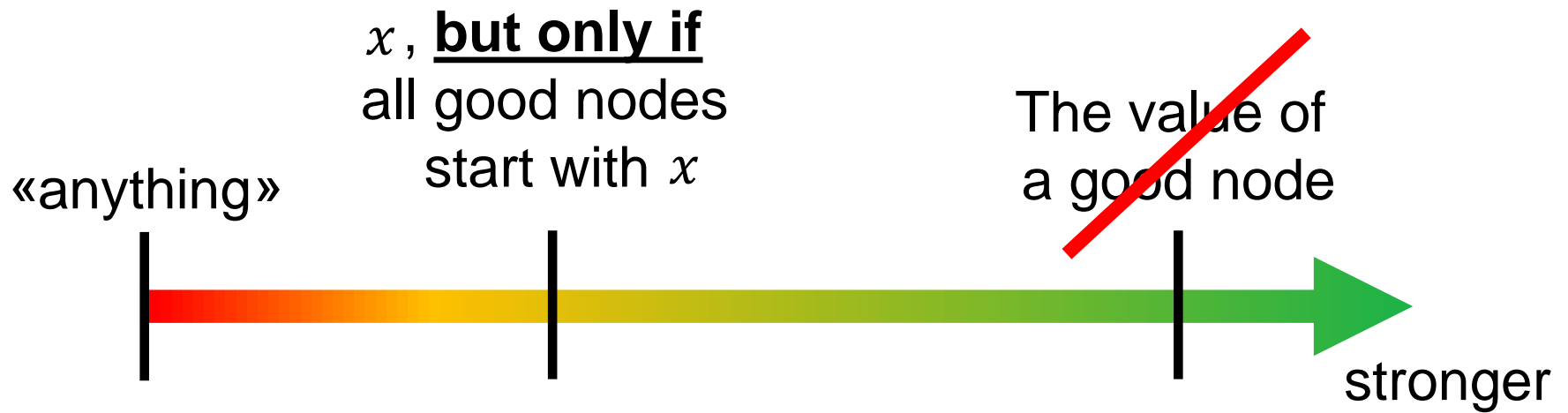
2. Termination

3. Validity

# Different Validity Properties

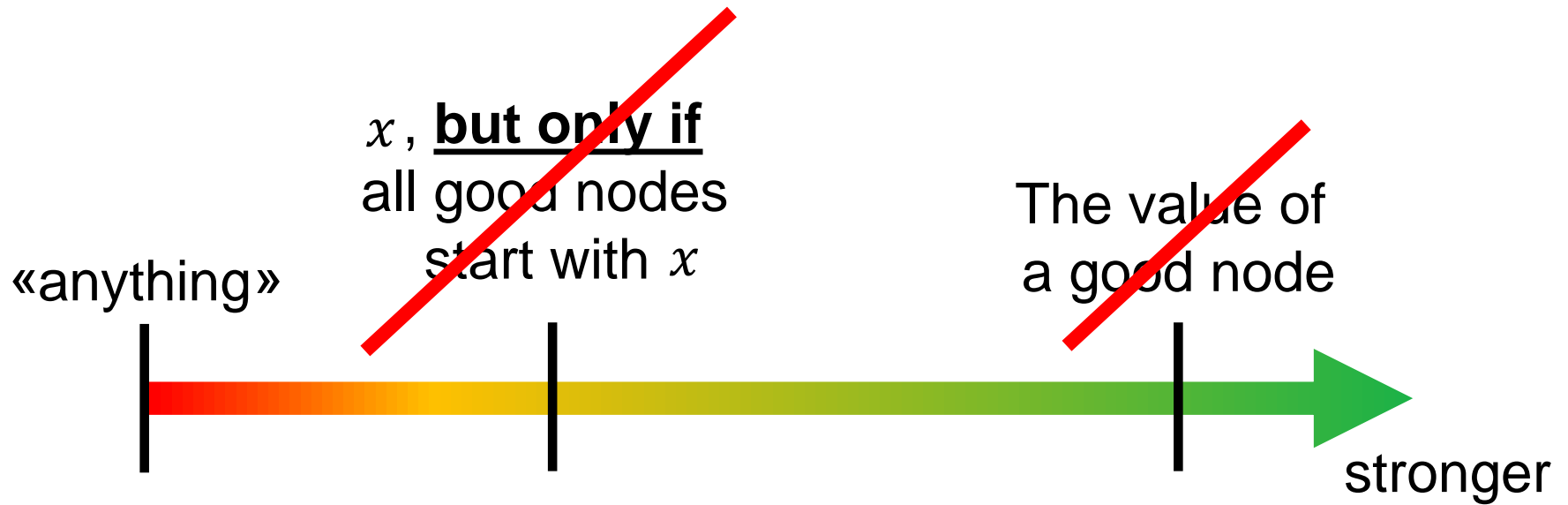


# Different Validity Properties for values in $\mathbb{R}$



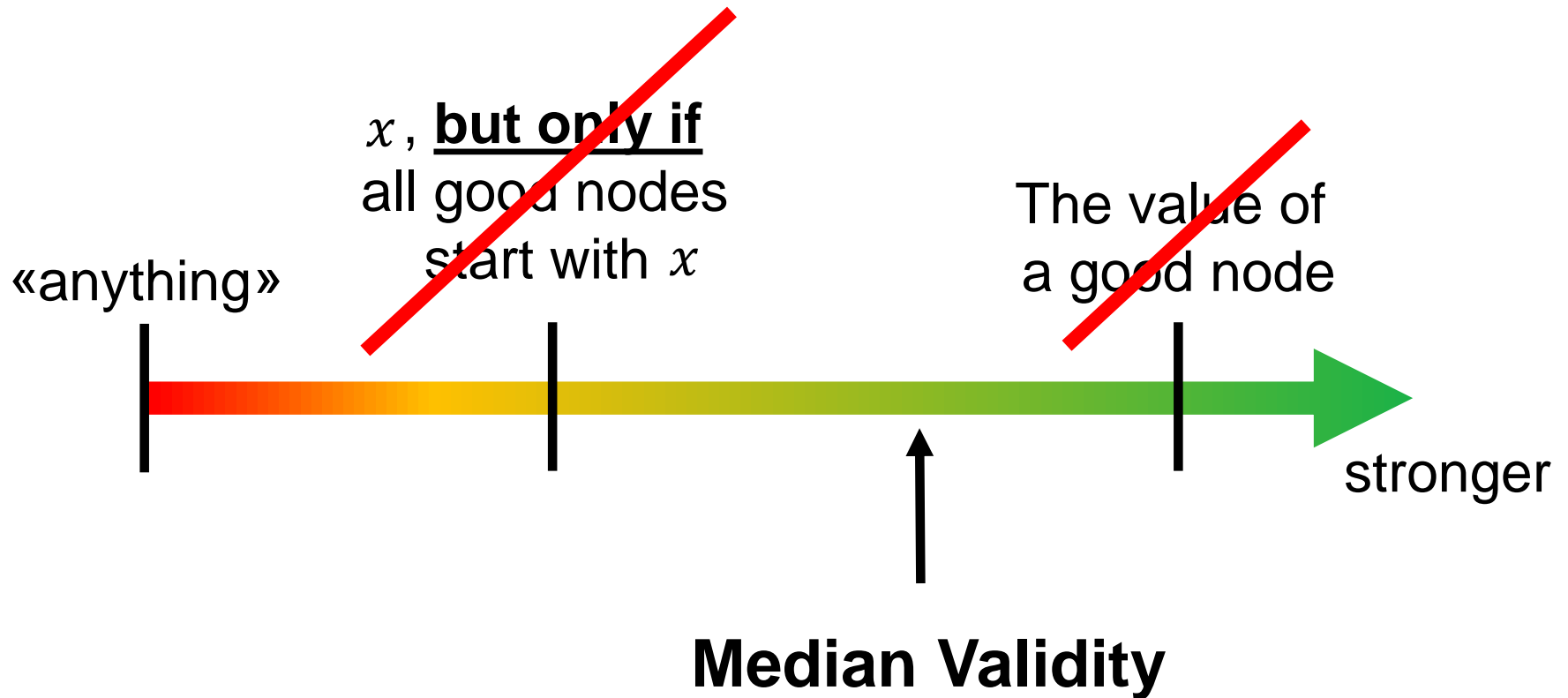
$D \geq 3\mathbb{R}$   
[Neiger 94]

# 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

➡ optimization of cost functions

[Su, Vaidya 15]

# Model

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

996

998

999

1000

1001

1002

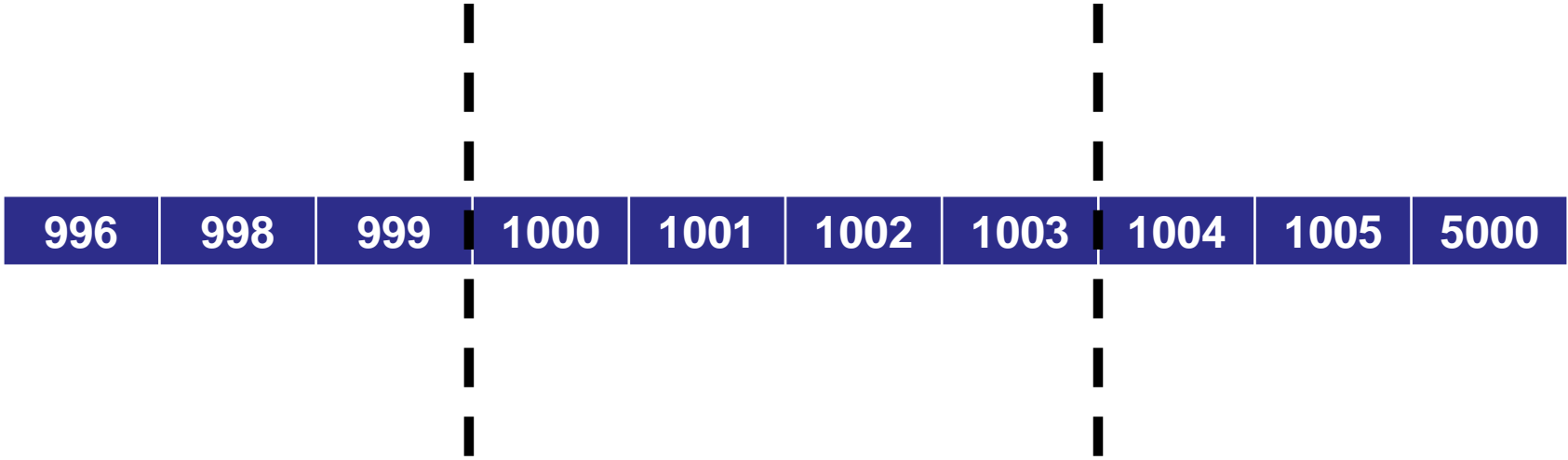
1003

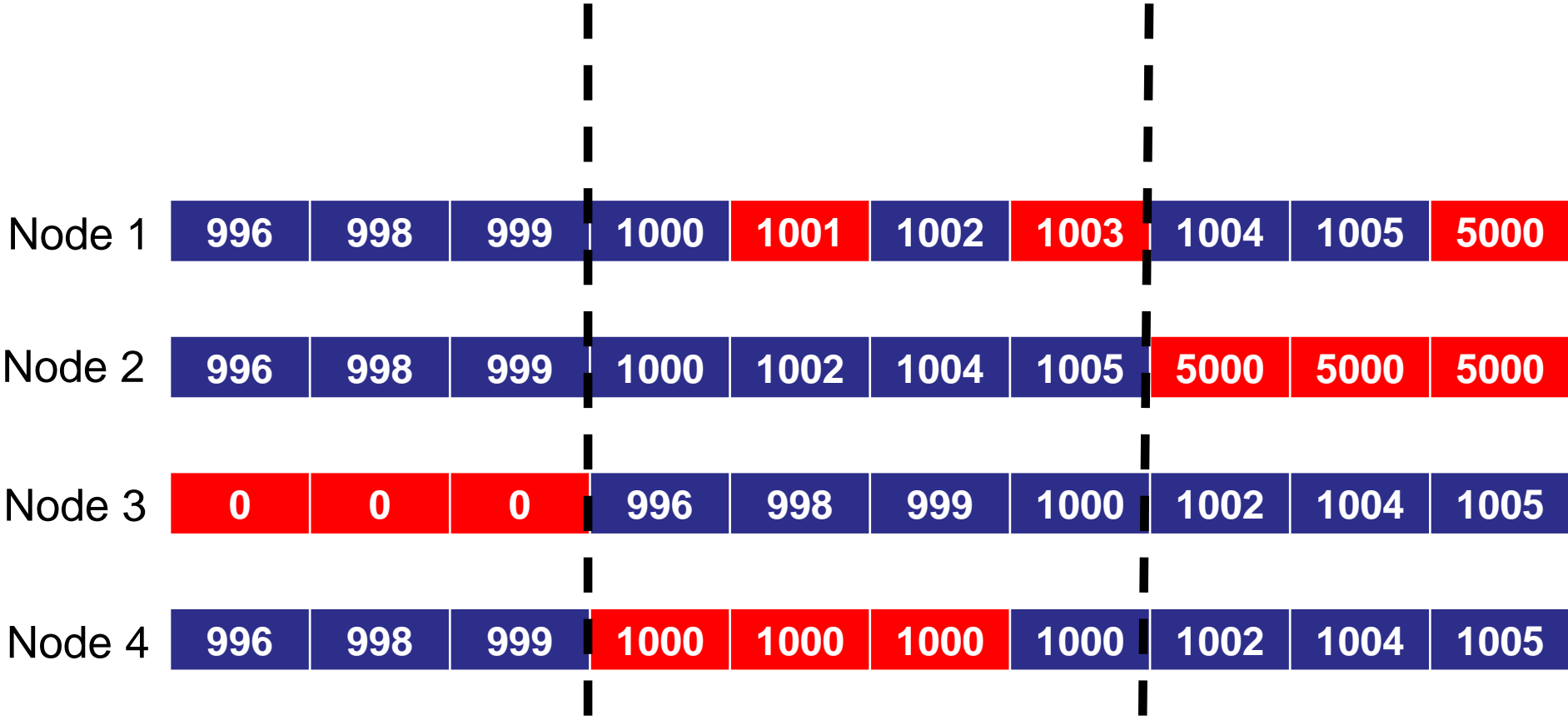
1004

1005

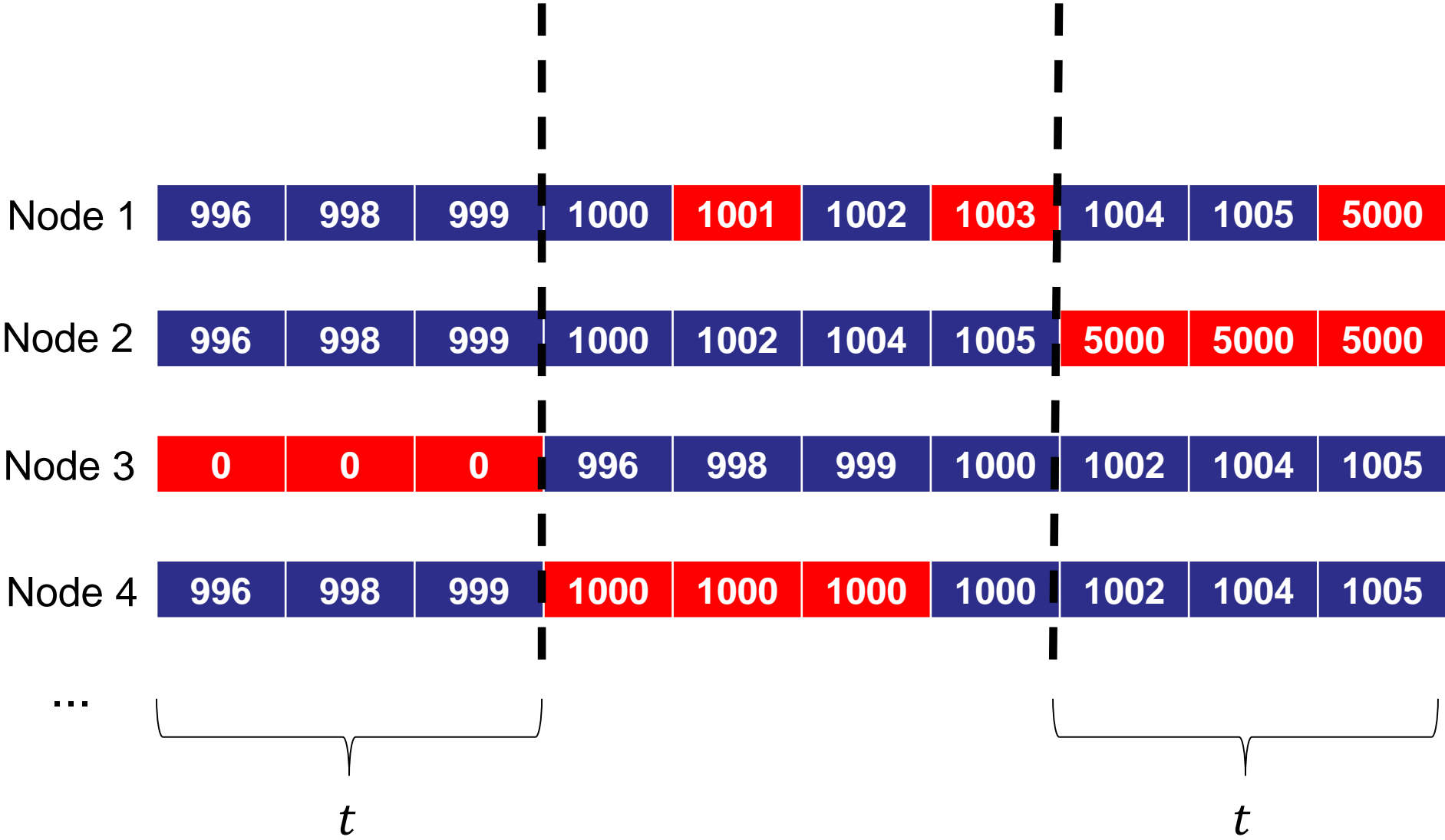
5000

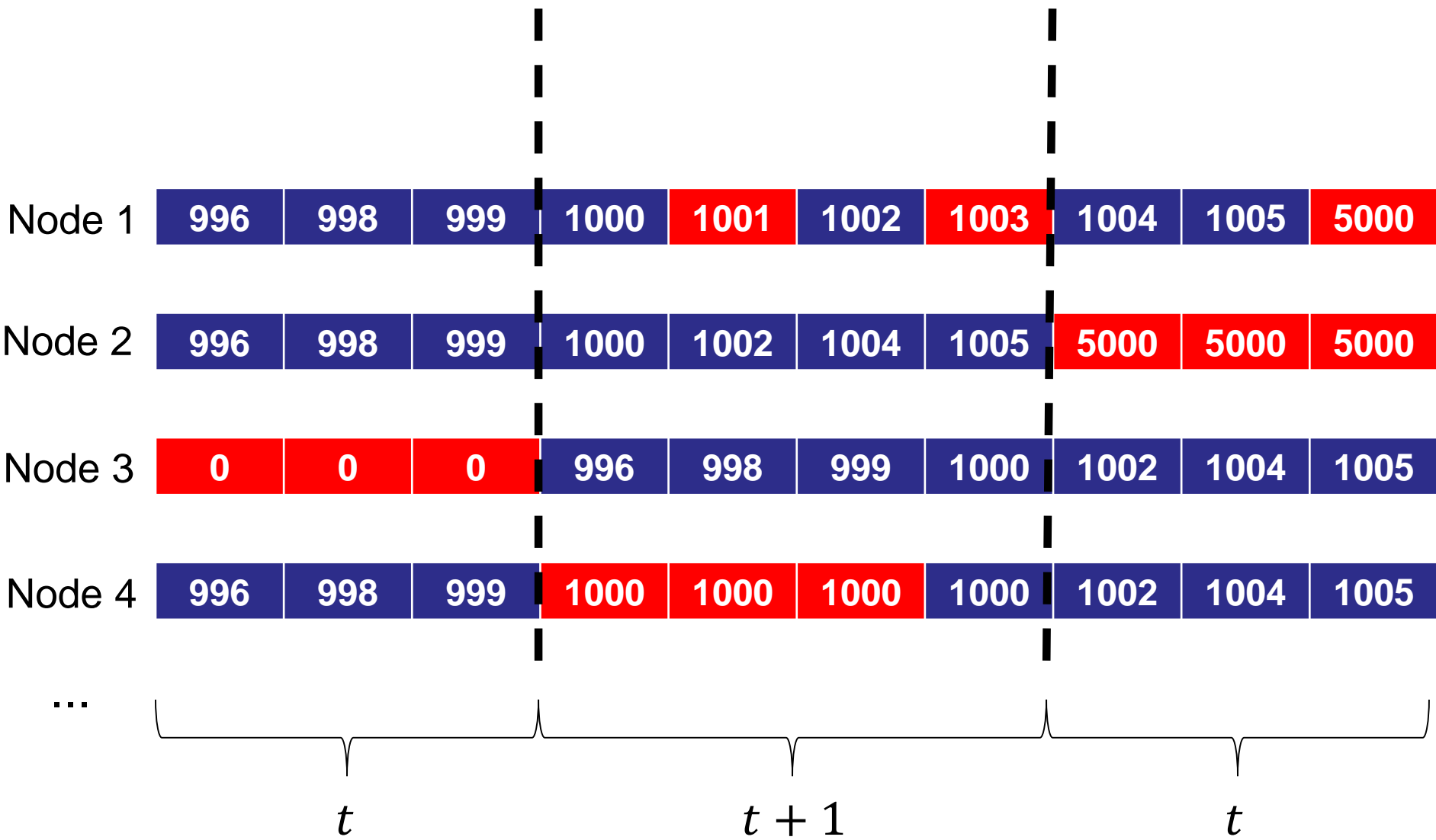


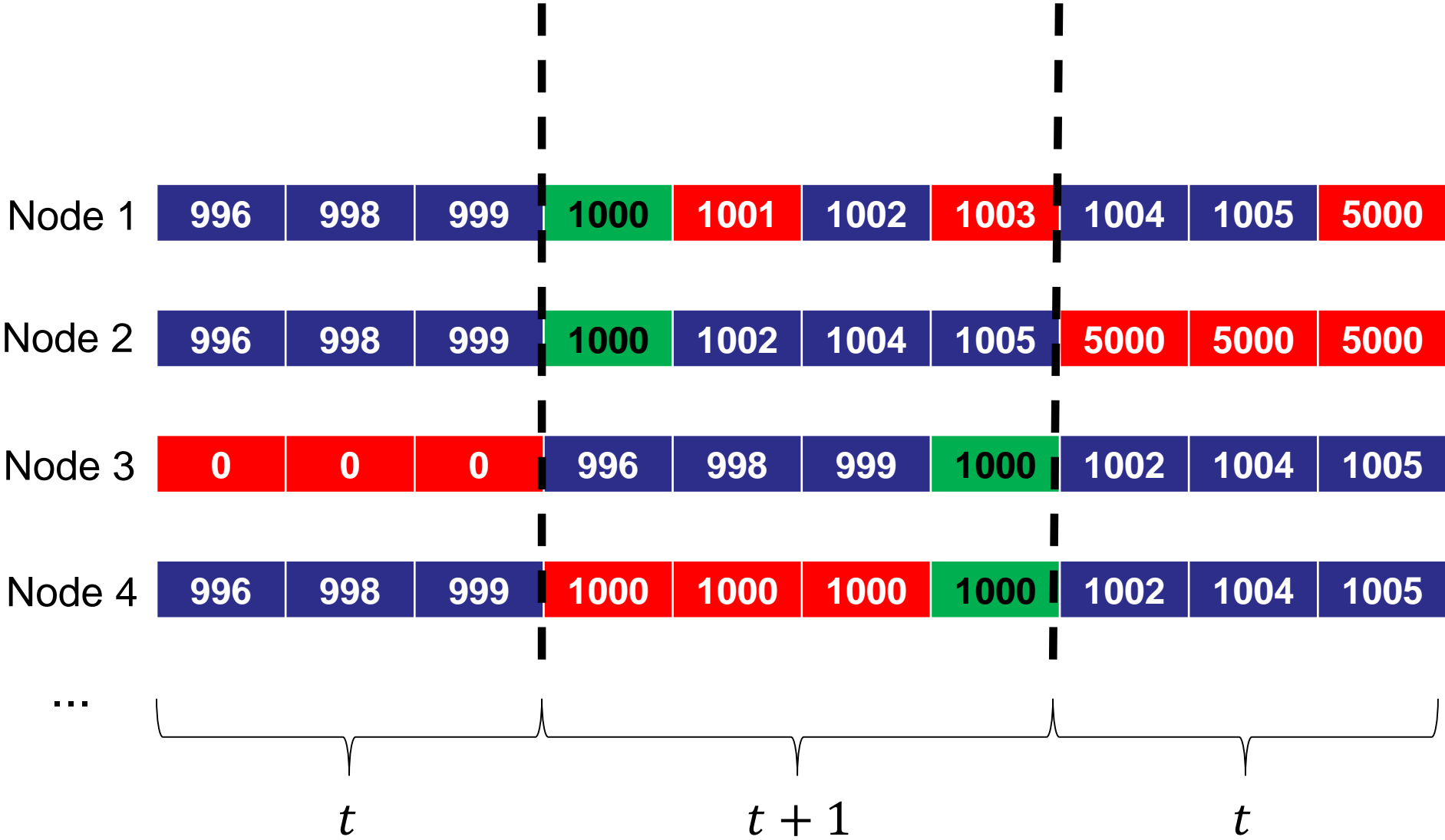




...









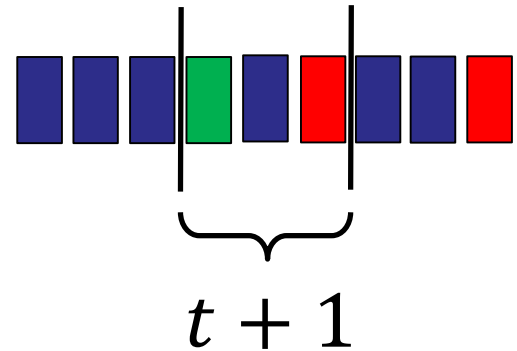


# Setup Stage

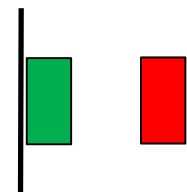
- Broadcast & Gather all values



- Remove potential outliers



- Broadcast & Gather all bounds





## Search Stage ( $f + 1$ phases)

- Broadcast current value
  - ➔ if agreement already, don't change
- If no agreement, let jack suggest a value
  - ➔ support the suggestion, if in own interval
- Adapt jack suggestion, if enough support

Node 1

1

Node 2

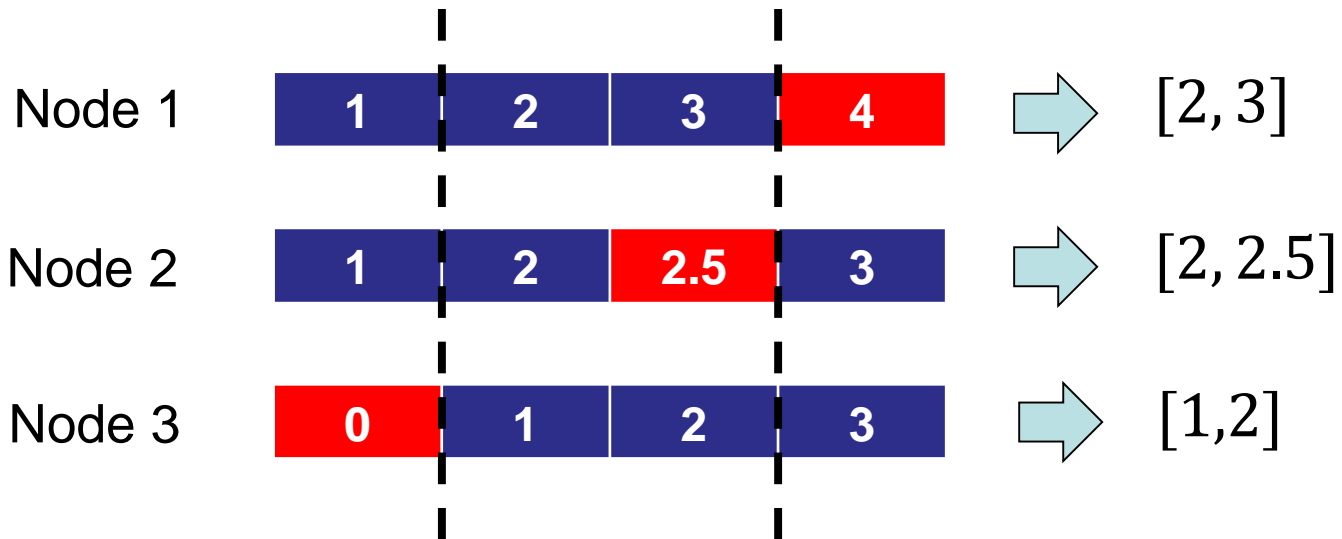
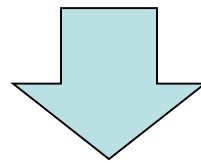
2

Node 3

3

Byzantine Node

?



# 1. Phase

## Step 1

Is there already  
Agreement?

1

3

2

?

# 1. Phase

## Step 1

Is there already  
Agreement?

1

2

3

?

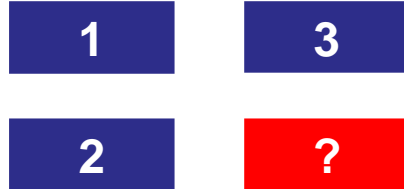
## Step 2

Byzantine Jack

999

# 1. Phase

**Step 1**  
Is there already  
Agreement?



**Step 2**  
Byzantine Jack

999

**Step 3**  
Support Jack?

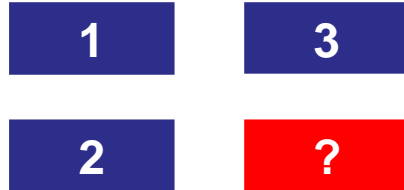
[2, 2.5]

[2, 3] [1,2]

➡ **No!**

# 1. Phase

**Step 1**  
Is there already  
Agreement?



**Step 2**  
Byzantine Jack

999

**Step 3**  
Support Jack?

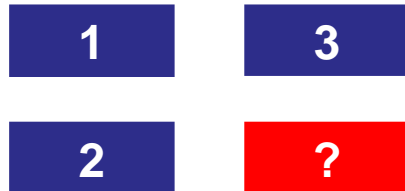
[2, 2.5]

[2, 3] [1,2]

➡ **No!**

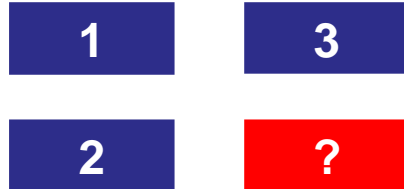
# 2. Phase

**Step 1**  
Is there already  
Agreement?



# 1. Phase

**Step 1**  
Is there already  
Agreement?



**Step 2**  
Byzantine Jack

999

**Step 3**  
Support Jack?

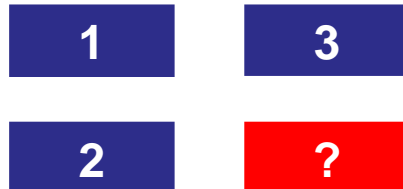
[2, 2.5]

[2, 3] [1,2]

➡ **No!**

# 2. Phase

**Step 1**  
Is there already  
Agreement?



**Step 2**  
Good Jack

2



# 1. Phase

**Step 1**  
Is there already Agreement?

1	3
2	?

**Step 2**  
Byzantine Jack

999

**Step 3**  
Support Jack?

[2, 2.5]  
[2, 3] [1,2]

➡ **No!**

# 2. Phase

**Step 1**  
Is there already Agreement?

1	3
2	?

**Step 2**  
Good Jack

2

**Step 3**  
Support Jack?

[2, 2.5]  
[2, 3] [1,2]

➡ **Yes!**

# Only good values



Median Validity

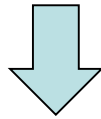


Lower bound  
(tight)

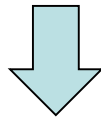


# Conclusion

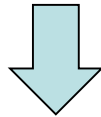
Validity property is essential



Median Validity



Efficiently achievable



Good quality

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

\* if  $f = t$

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