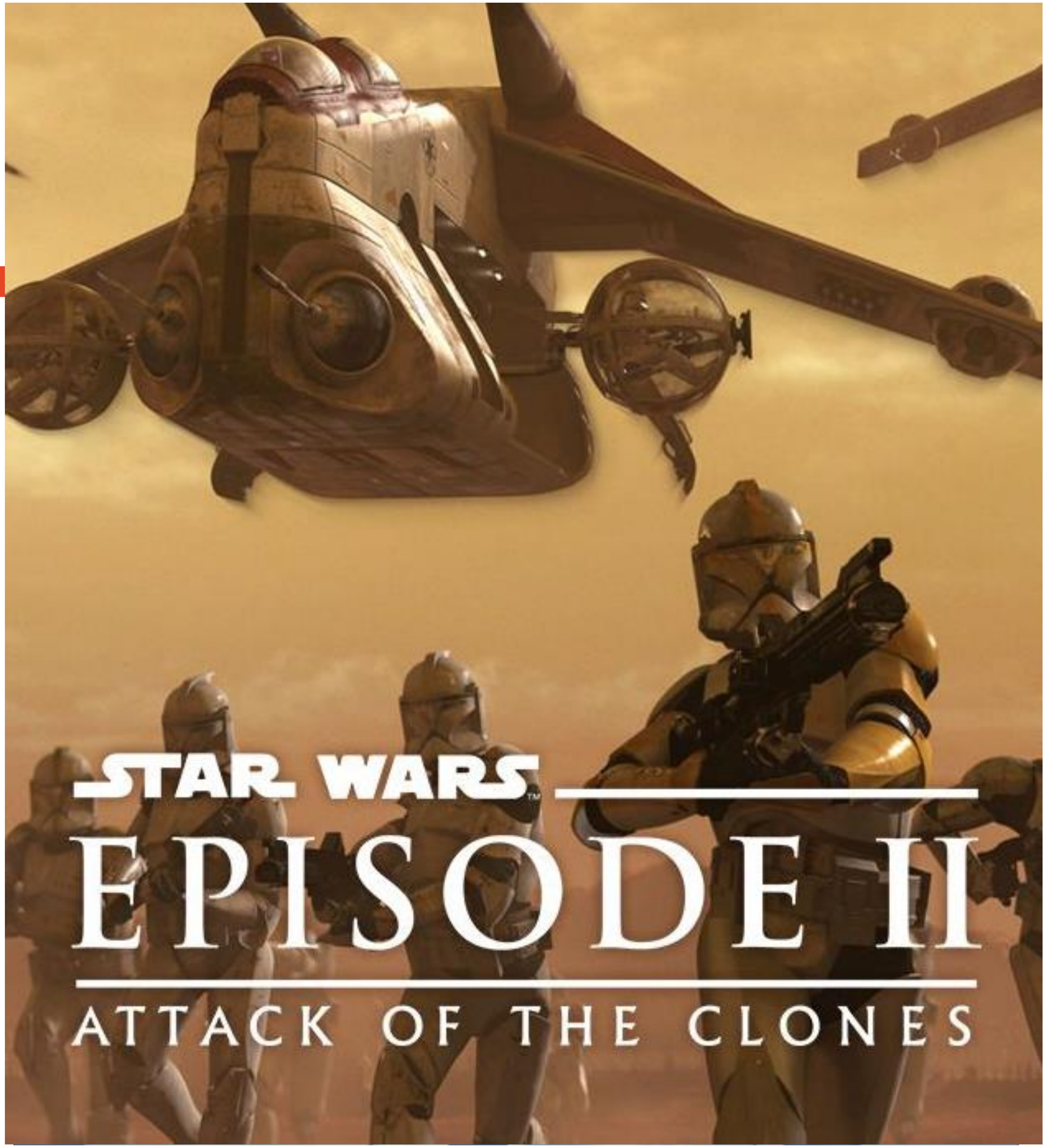
The Attack of the Clones against Proof-of-Authority

Parinya Ekparinya

Vincent Gramoli

Guillaume Jourjon



THE UNIVERSITY OF SYDNEY

DATA 61

CSIRO

Public Blockchains

Proof-of-Work

Consortium & Private Blockchains

Public Blockchains

Proof-of-Work

↓

Consortium & Private Blockchains

Proof-of-Authority

Azure

Grid Singularity

slock.it
A Blockchains Company

ALPHA
BLOCKCHAIN

energy web

Azure

Grid
Singularity

slock.it
A Blockchains Company

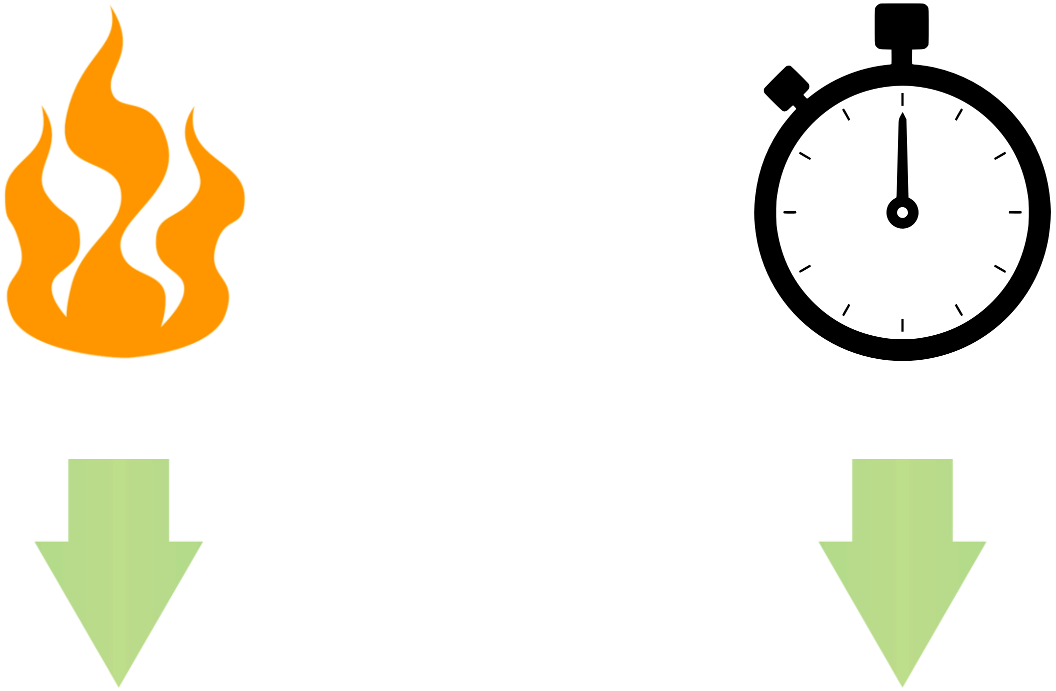
energy web

ALPHA
BLOCKCHAIN

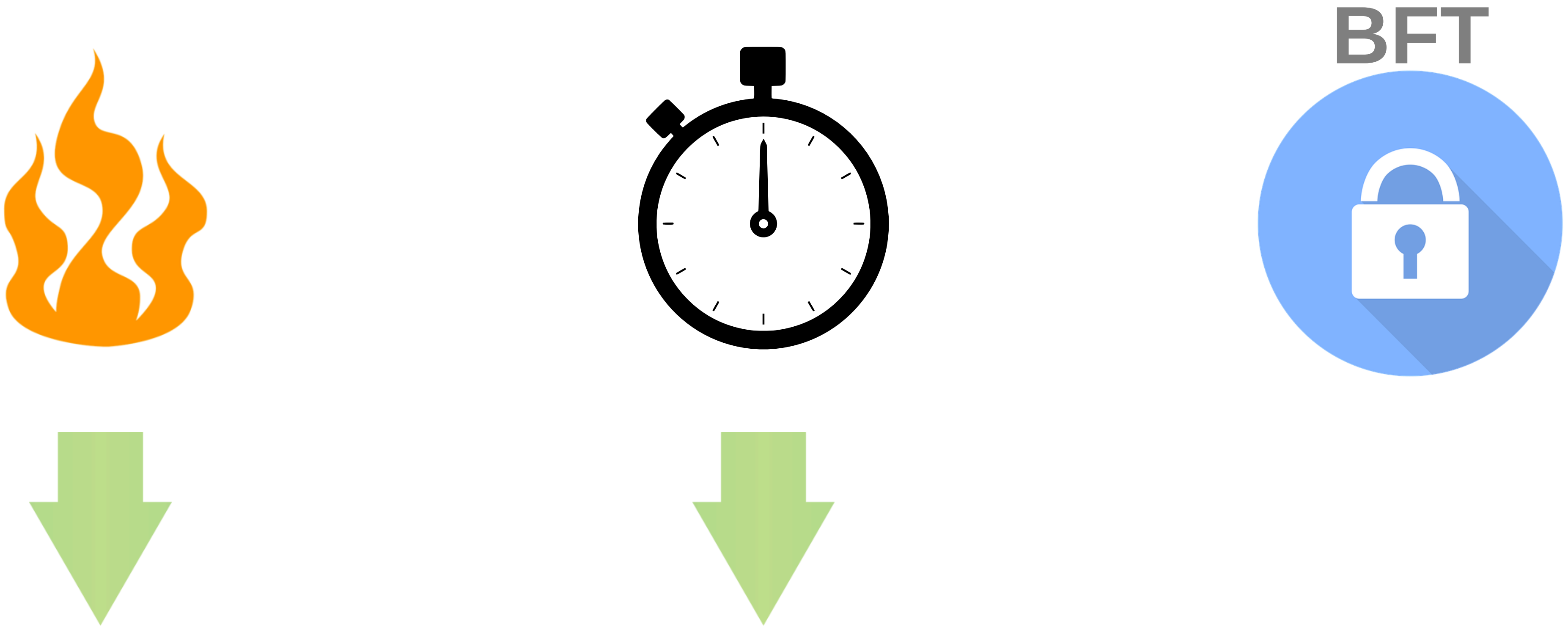
Why Proof-of-Authority (PoA)?

Why Proof-of-Authority (PoA)?

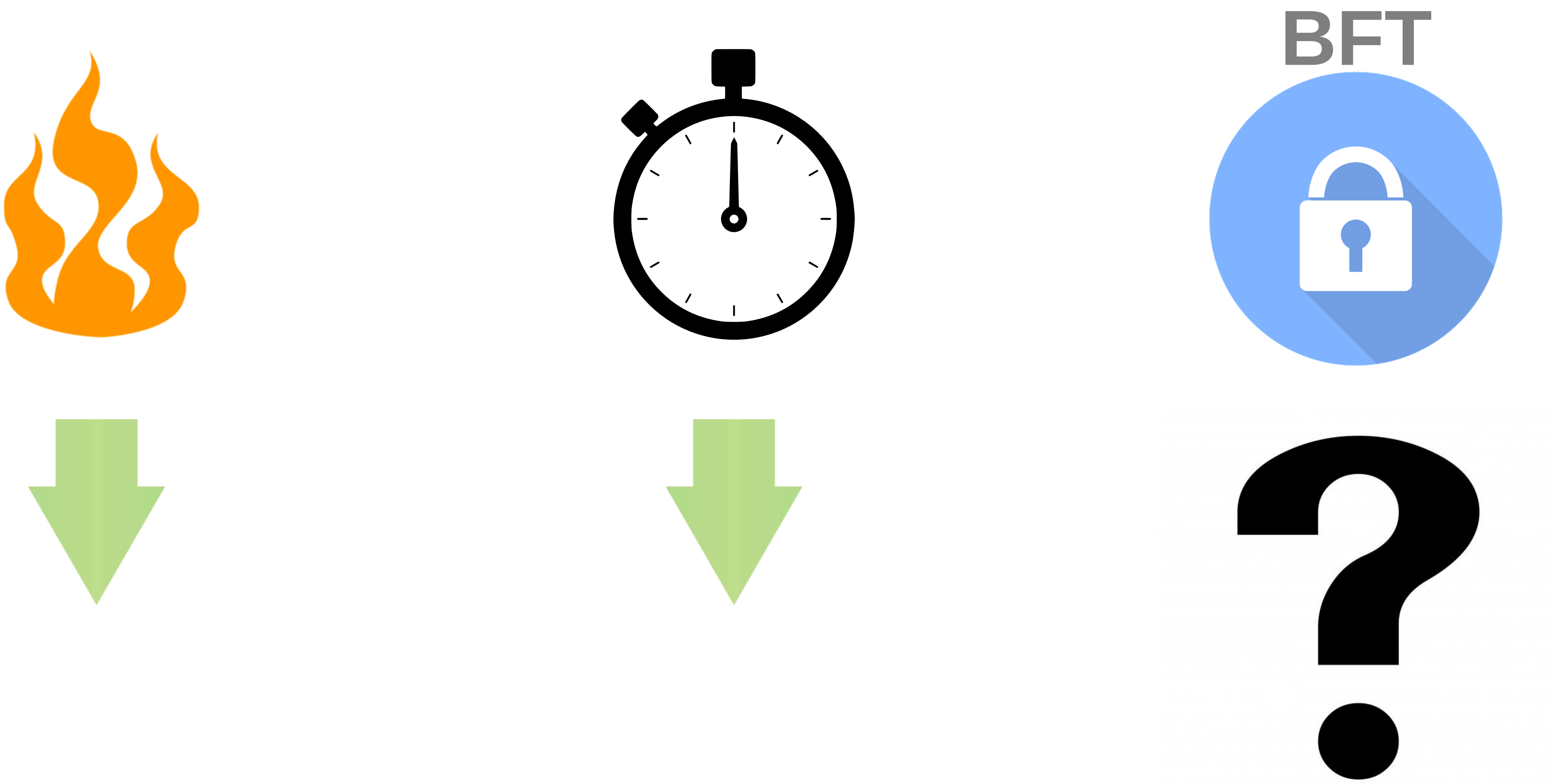
Why Proof-of-Authority (PoA)?



Why Proof-of-Authority (PoA)?

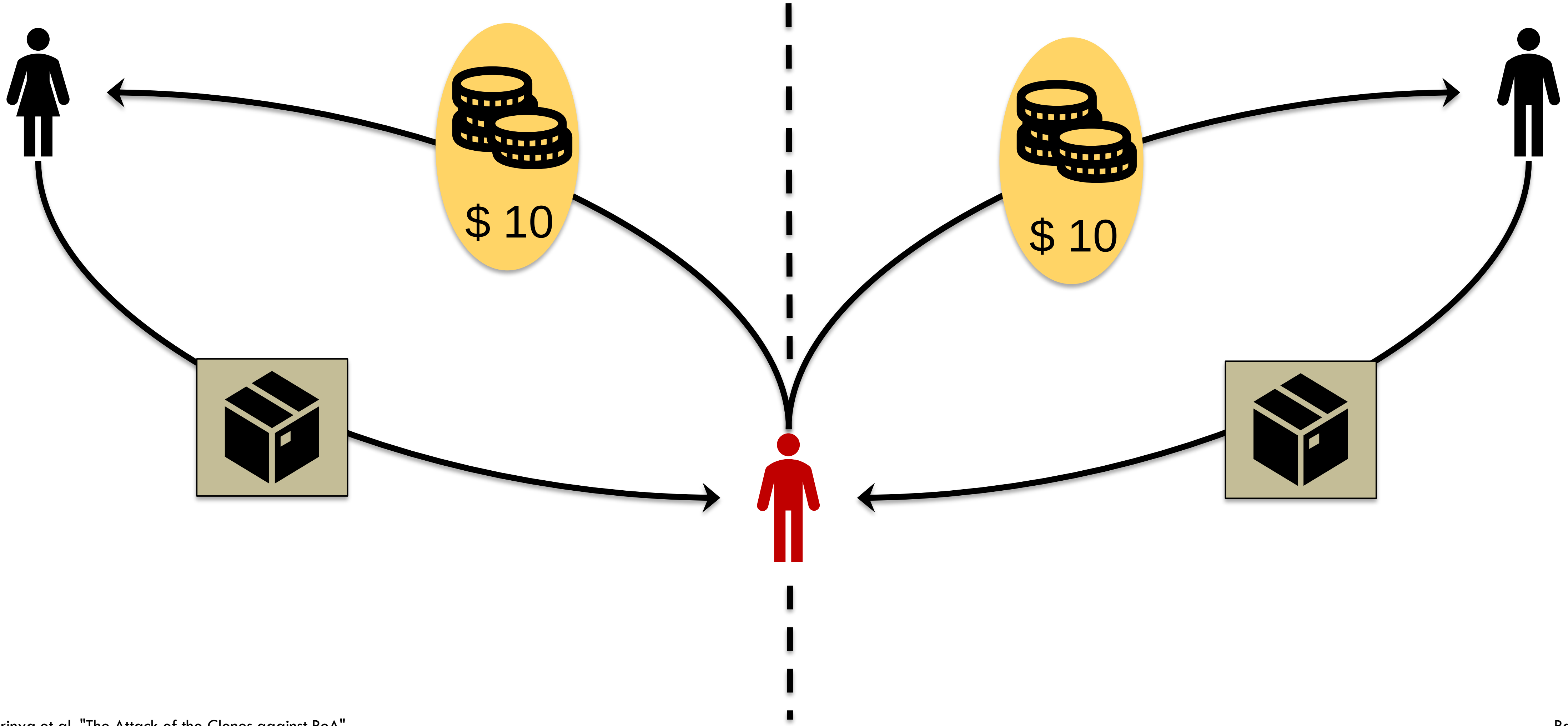


Why Proof-of-Authority (PoA)?

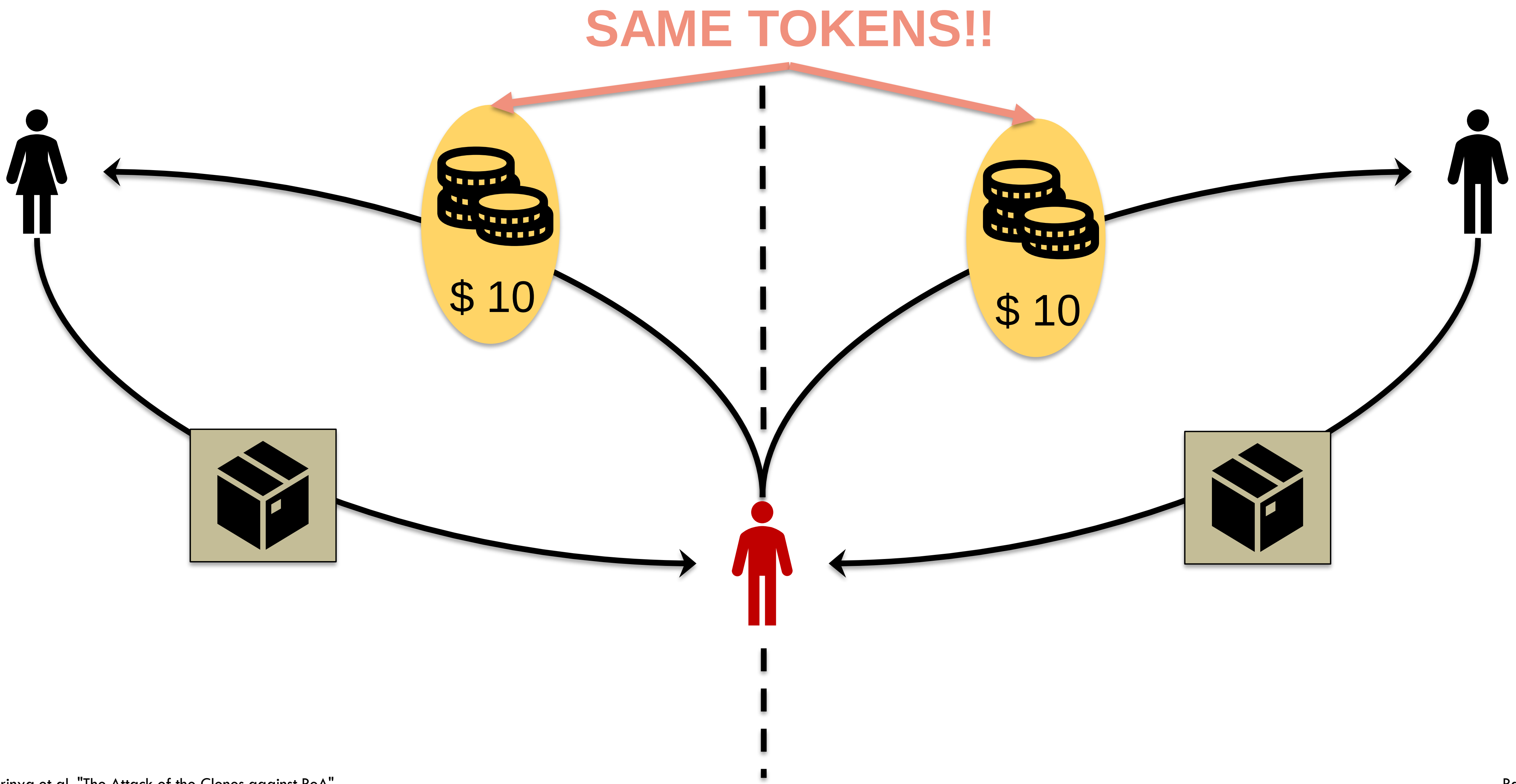


BFT

The Cloning Attack => Double-spending

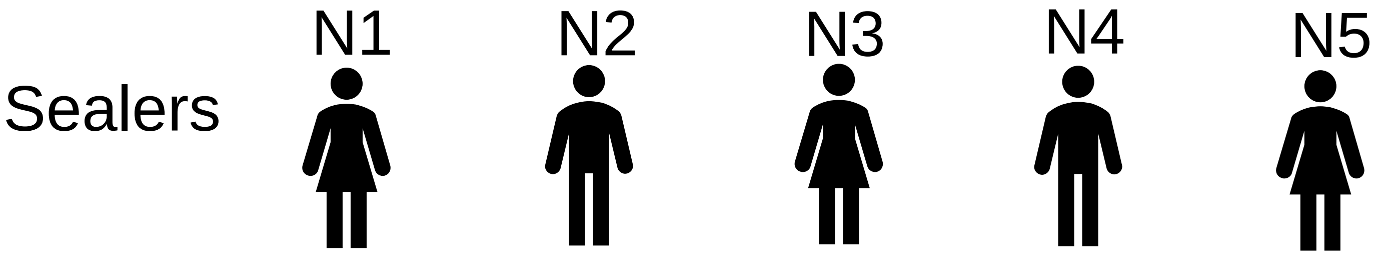


The Cloning Attack => Double-spending



Q: How is it possible to double spend on PoA/Ethereum?

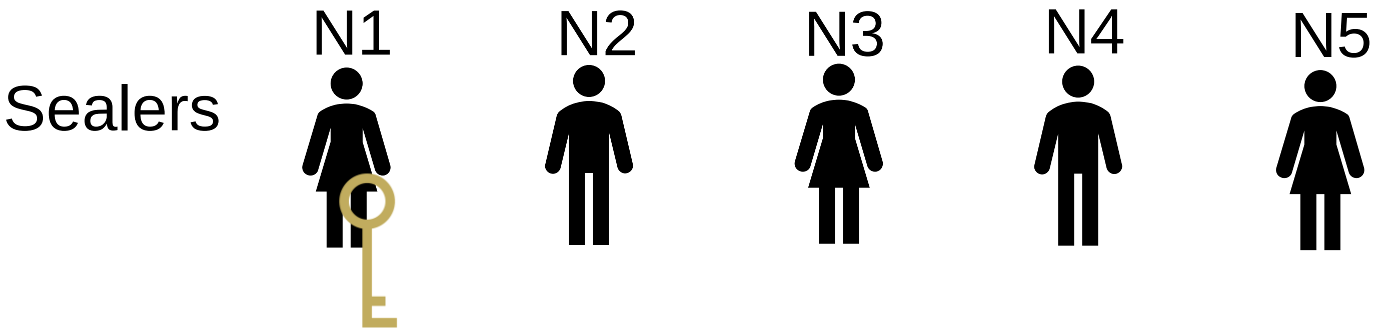
The Modus Operandi of AuRa



Sealers

N1 N2 N3 N4 N5

The Modus Operandi of AuRa



Sealers

N1

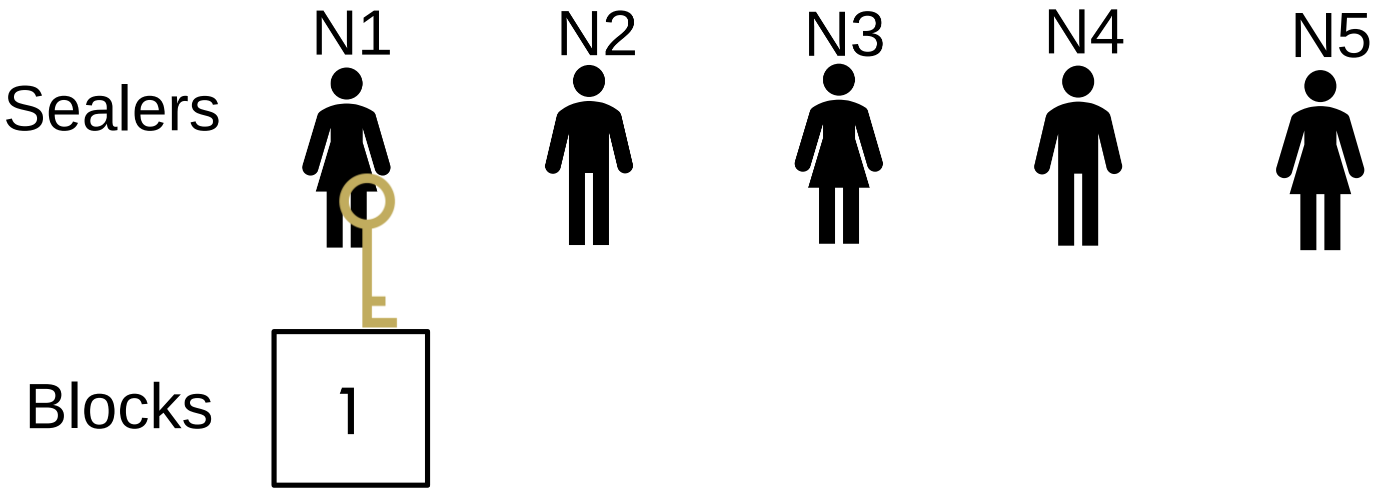
N2

N3

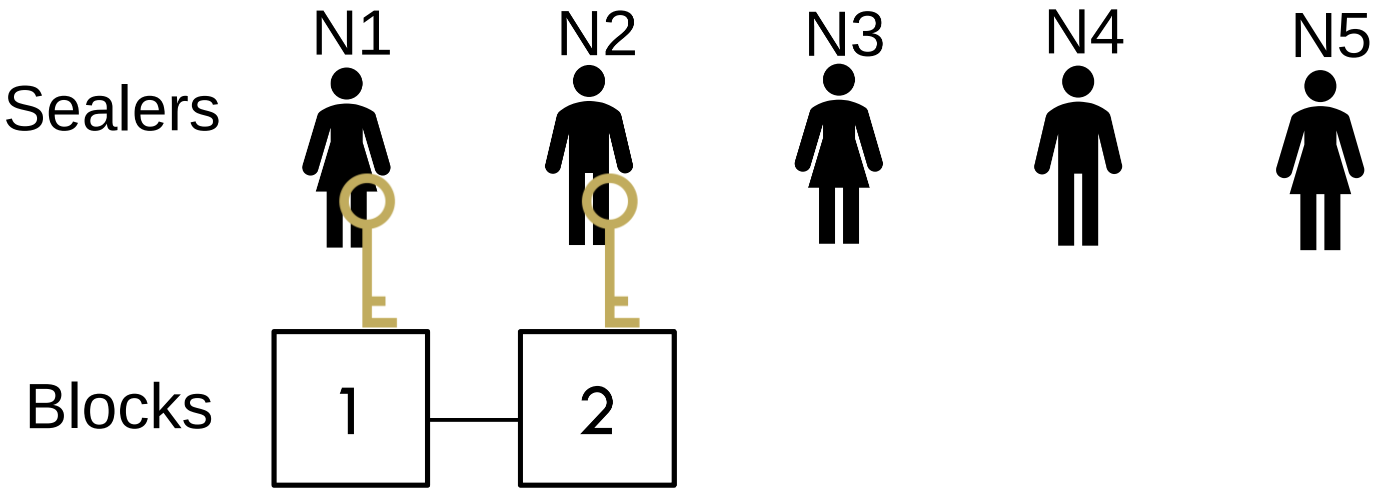
N4

N5

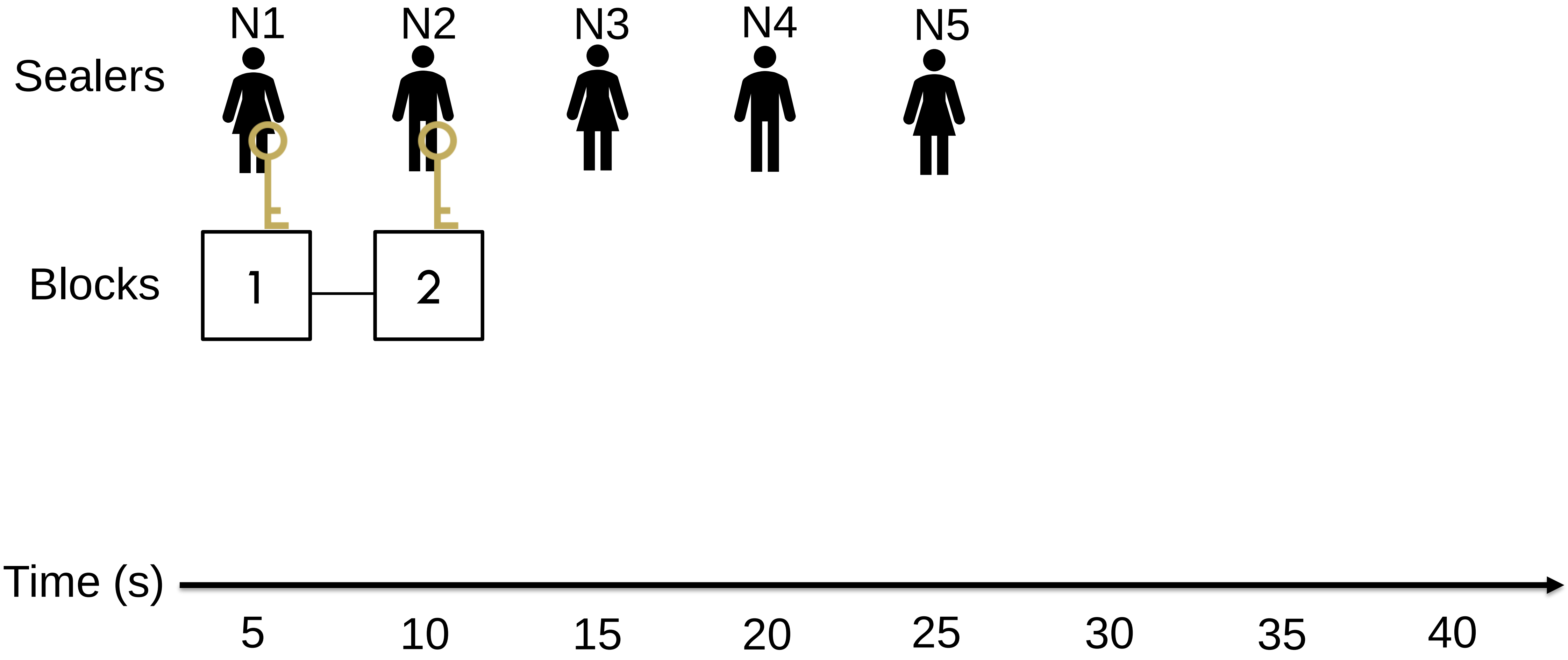
The Modus Operandi of AuRa



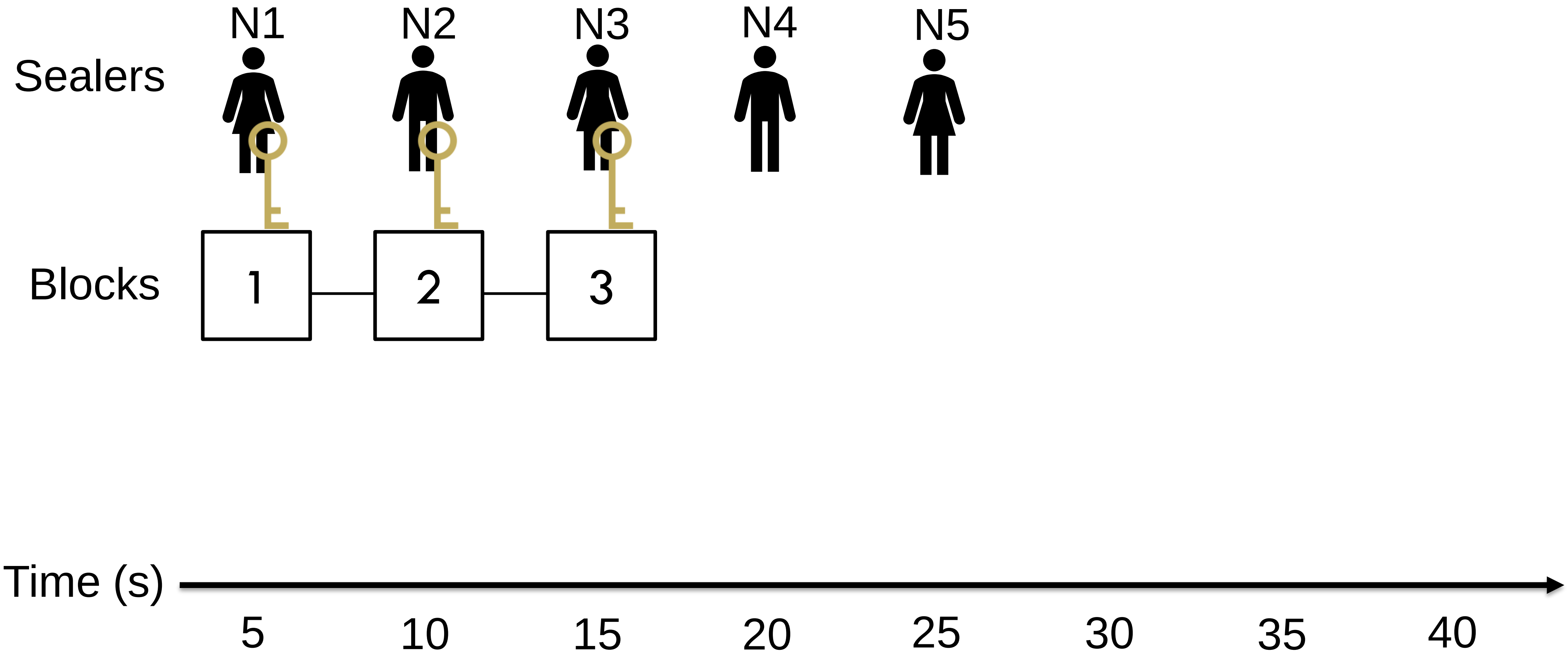
The Modus Operandi of AuRa



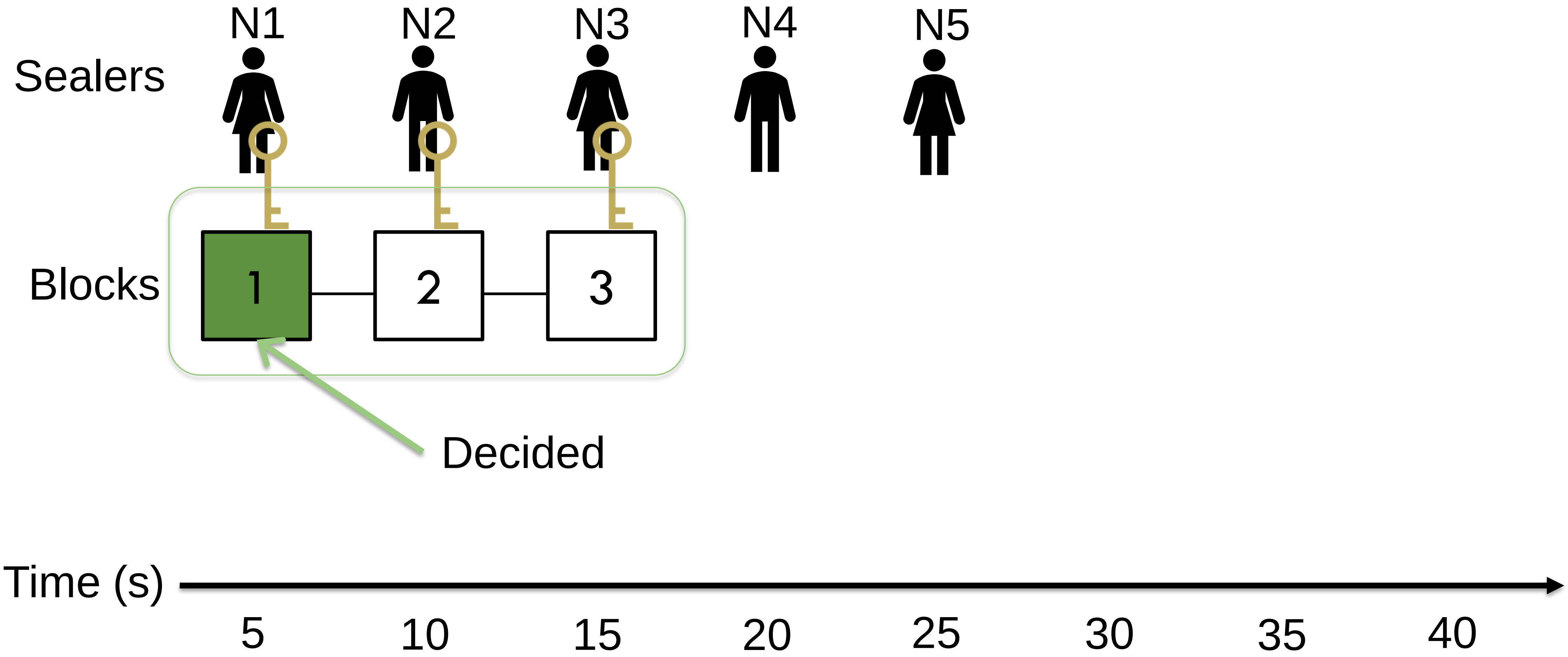
The Modus Operandi of AuRa



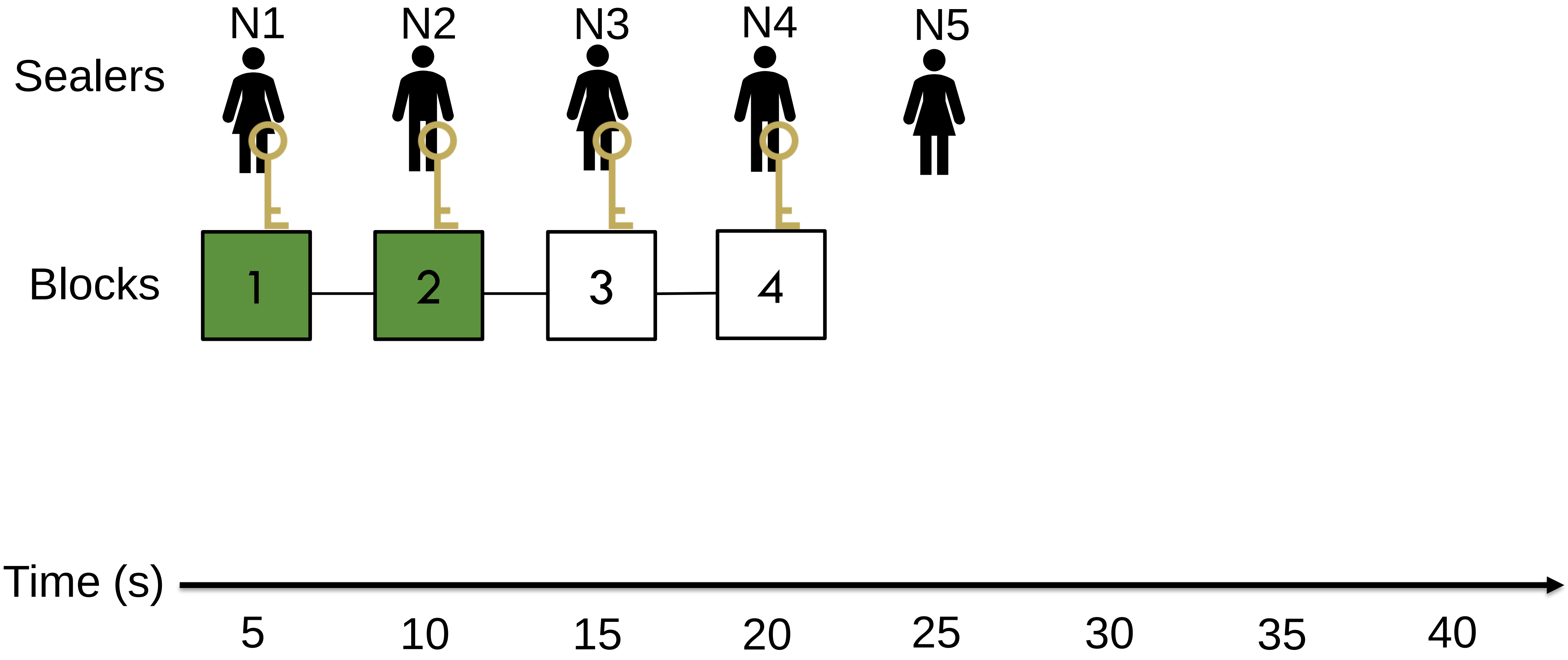
The Modus Operandi of AuRa



The Modus Operandi of AuRa

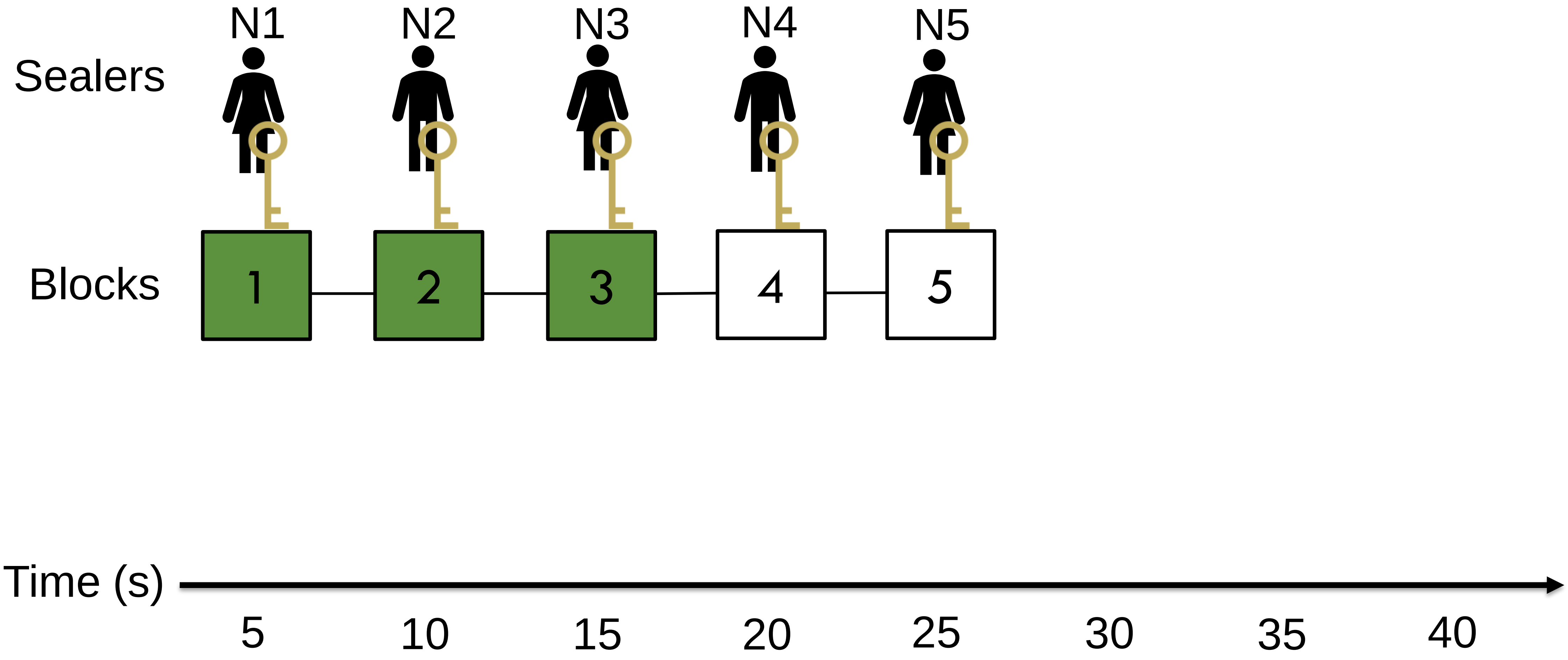


The Modus Operandi of AuRa



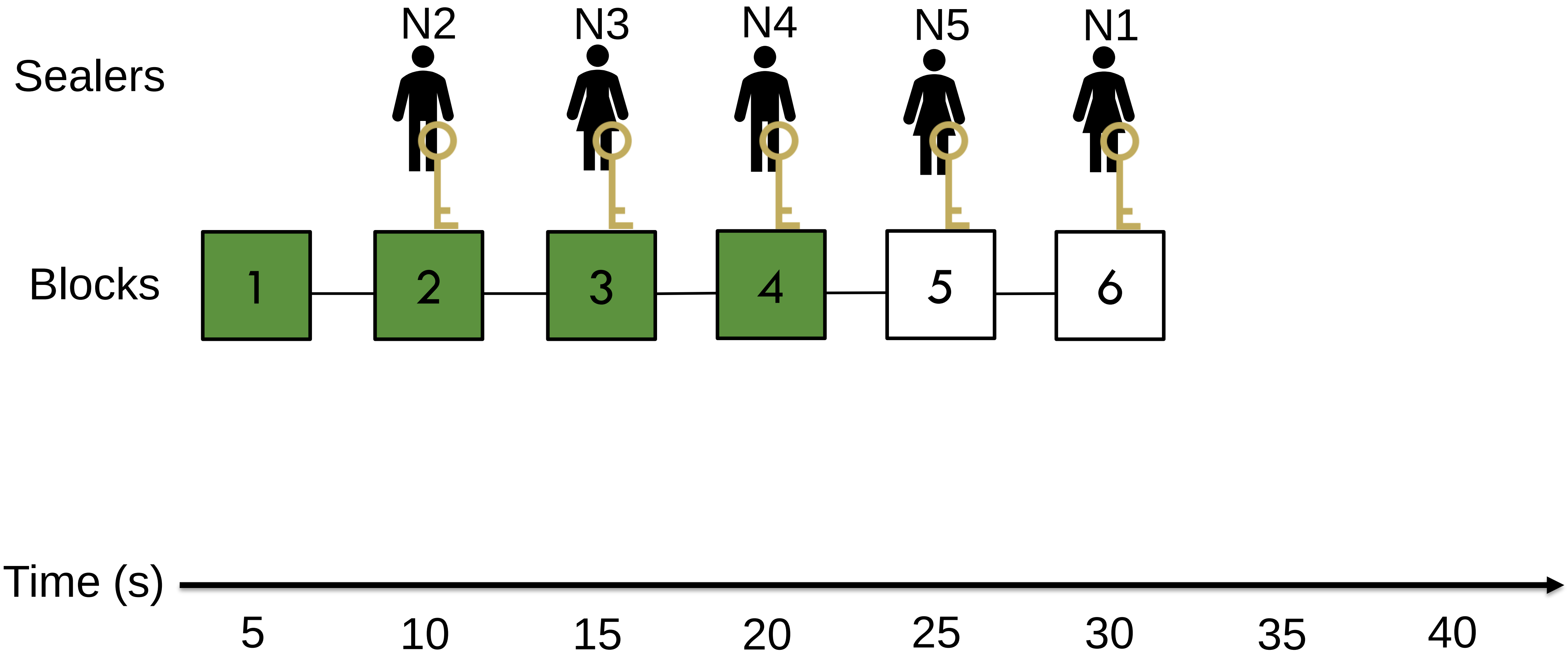
Ekparinya et al, "The Attack of the Clones against PoA"

The Modus Operandi of AuRa



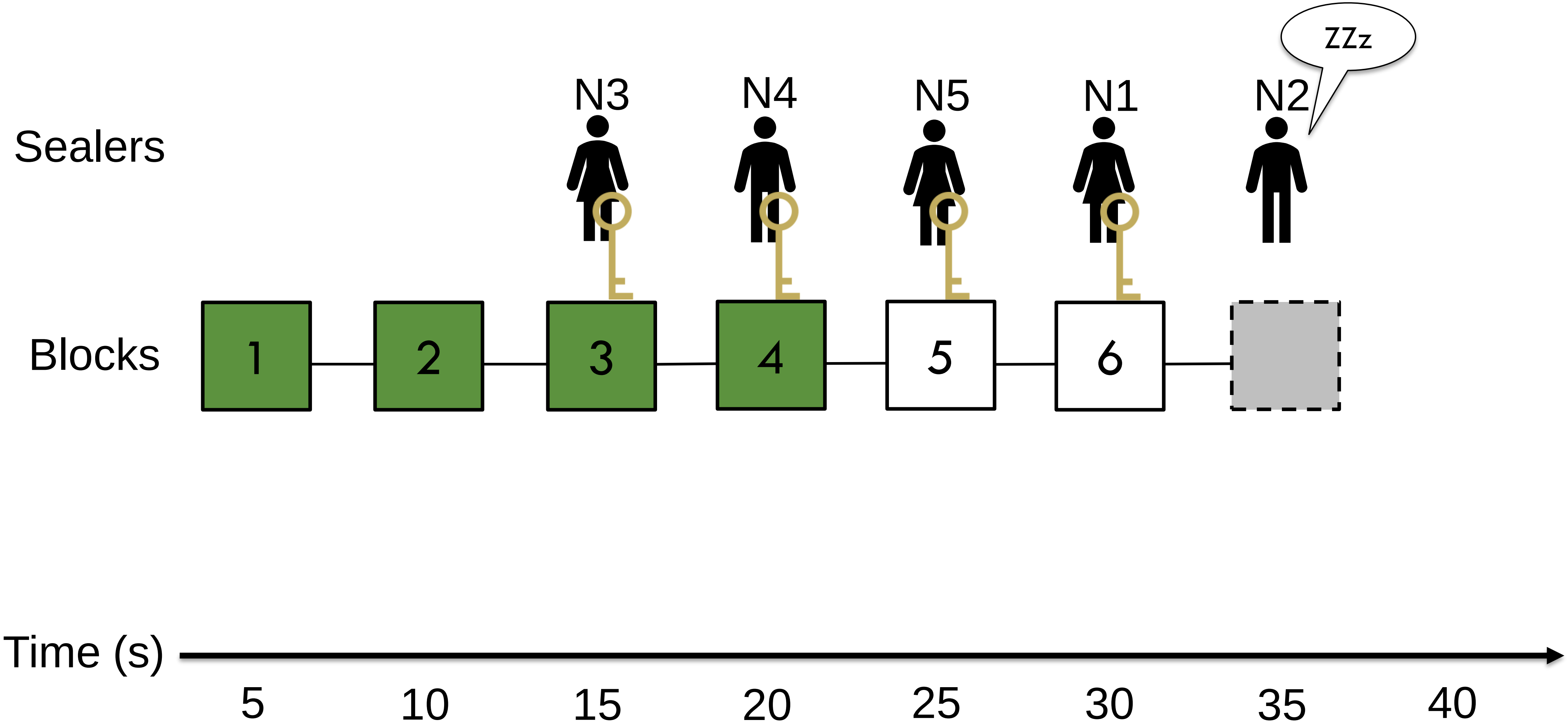
Ekparinya et al, "The Attack of the Clones against PoA"

The Modus Operandi of AuRa



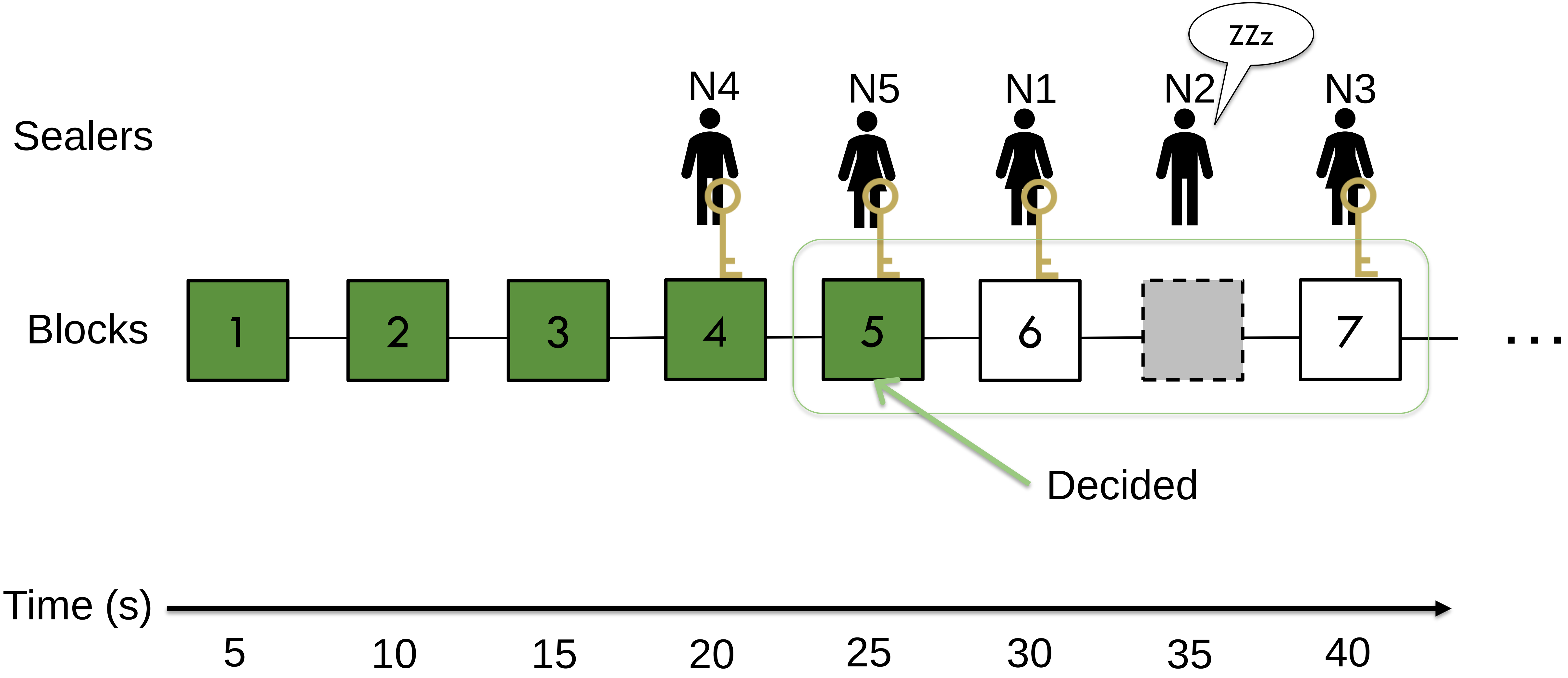
Ekparinya et al, "The Attack of the Clones against PoA"

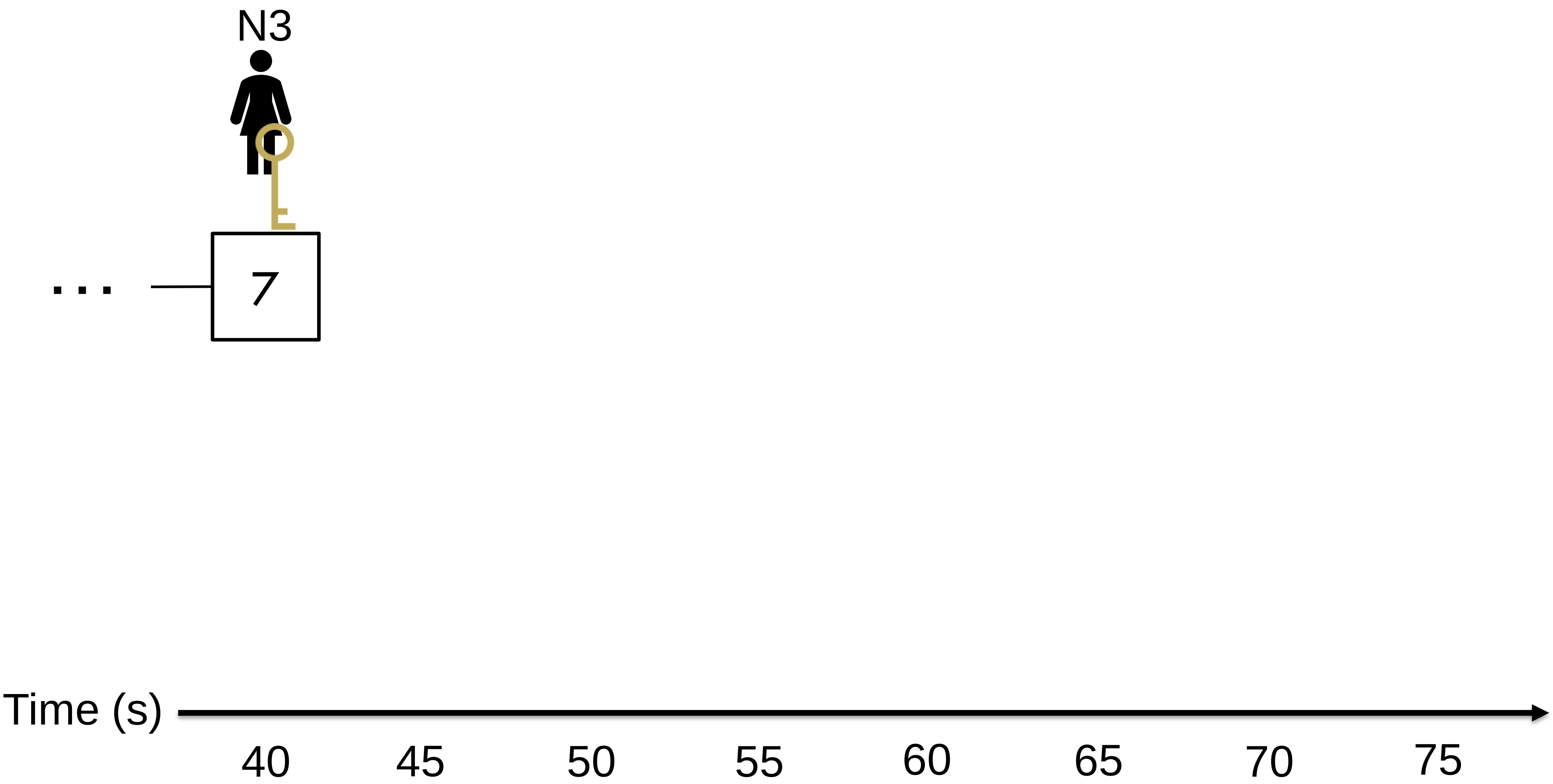
The Modus Operandi of AuRa

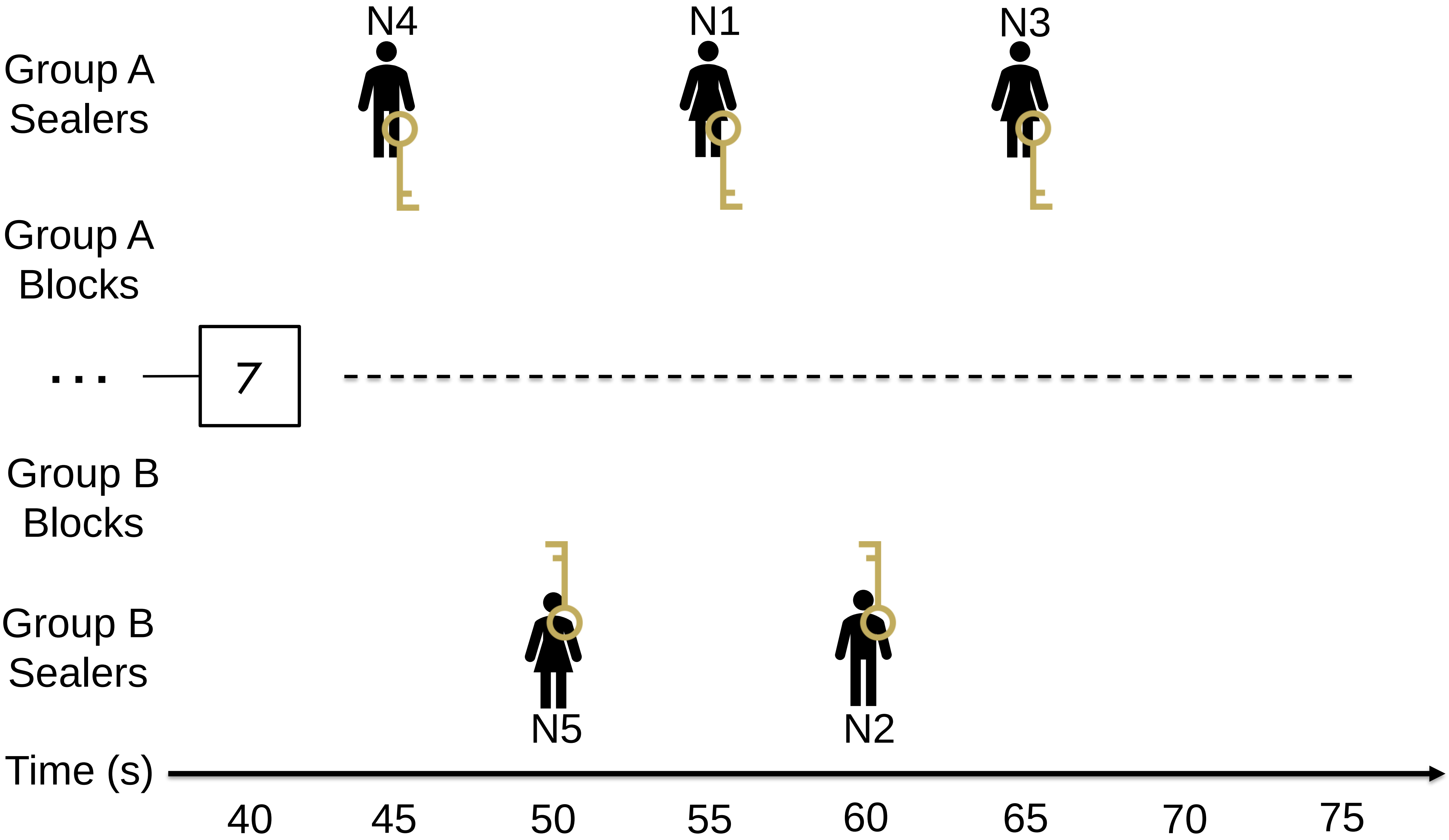


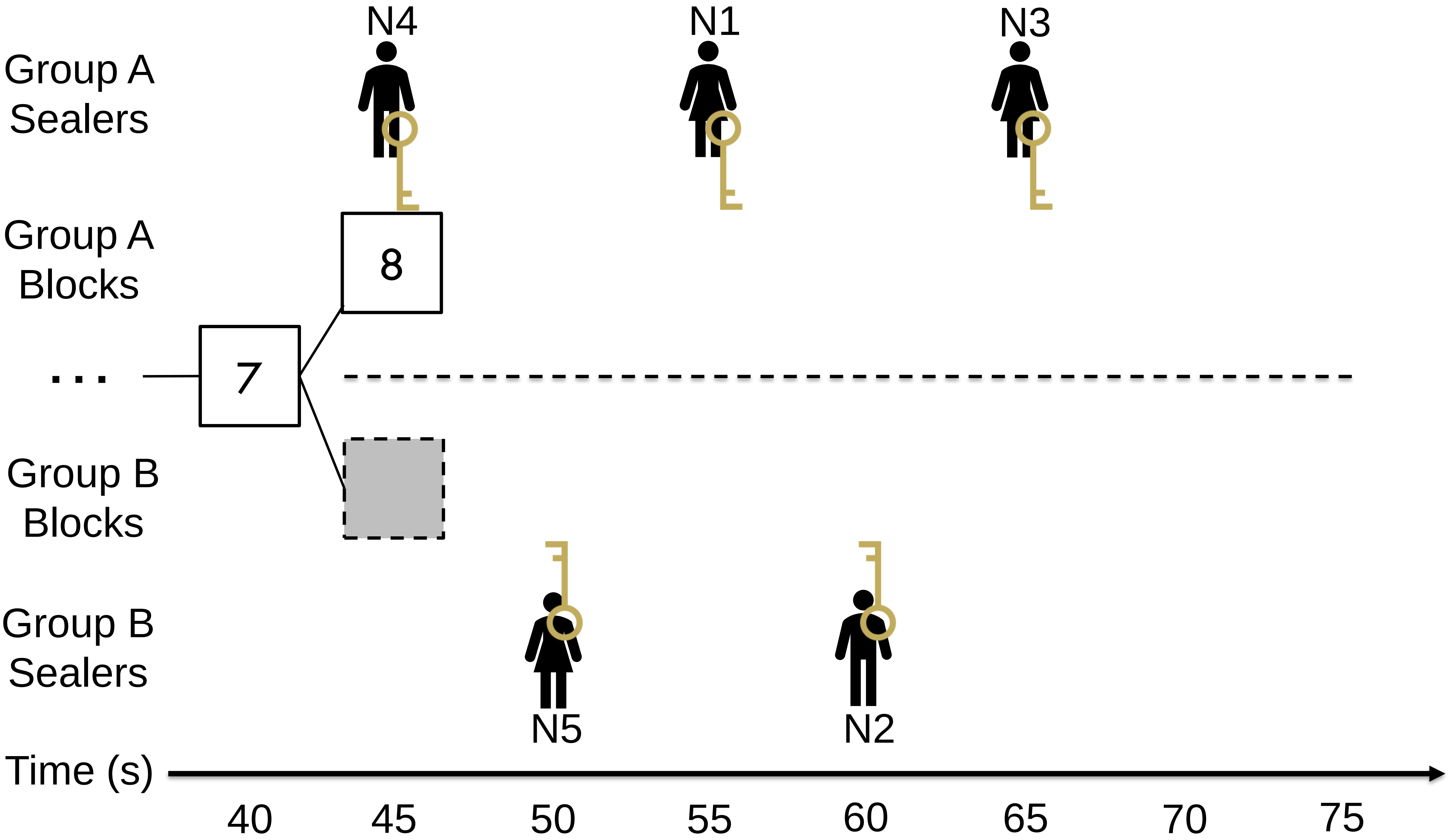
Ekparinya et al, "The Attack of the Clones against PoA"

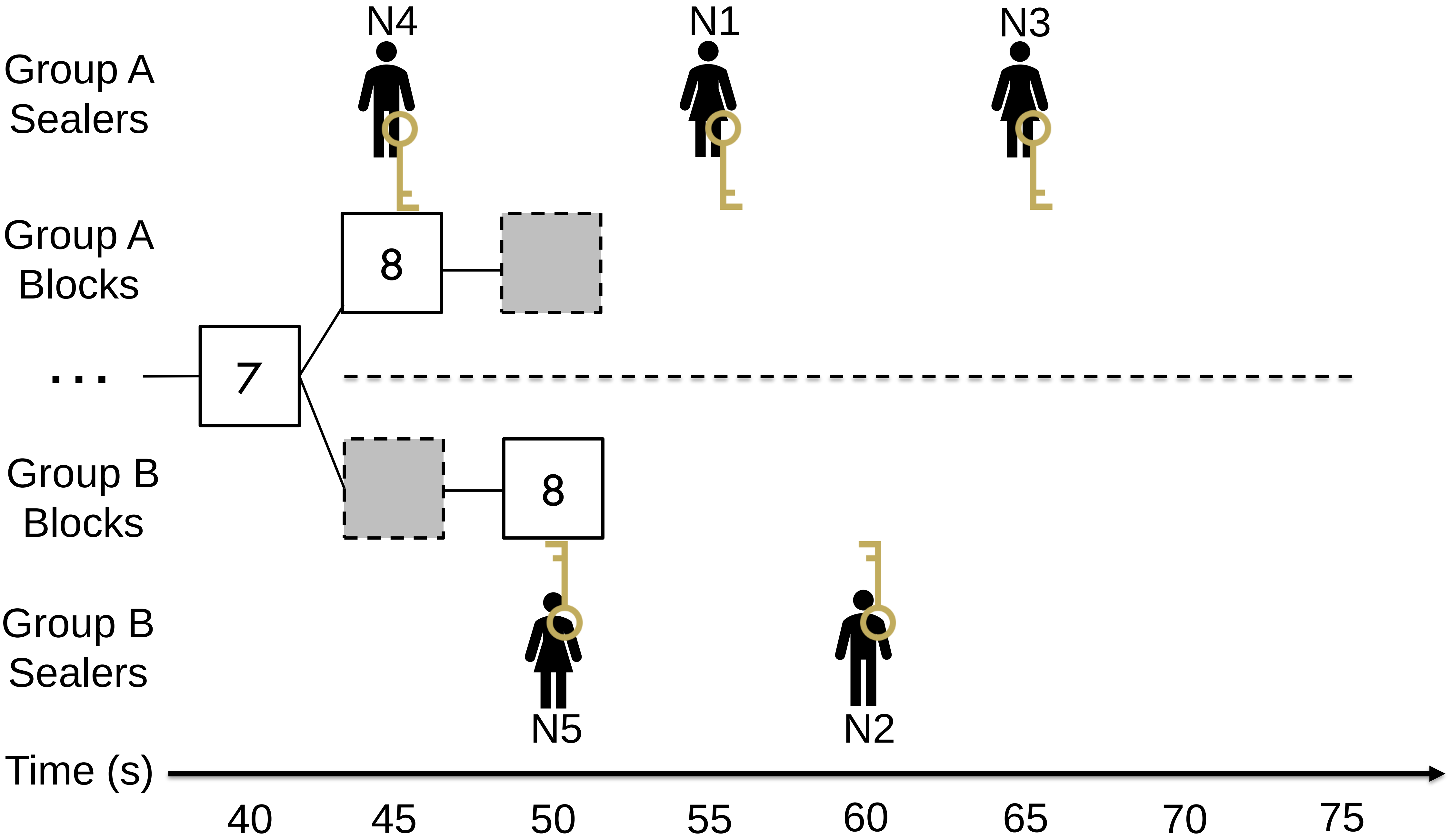
The Modus Operandi of AuRa

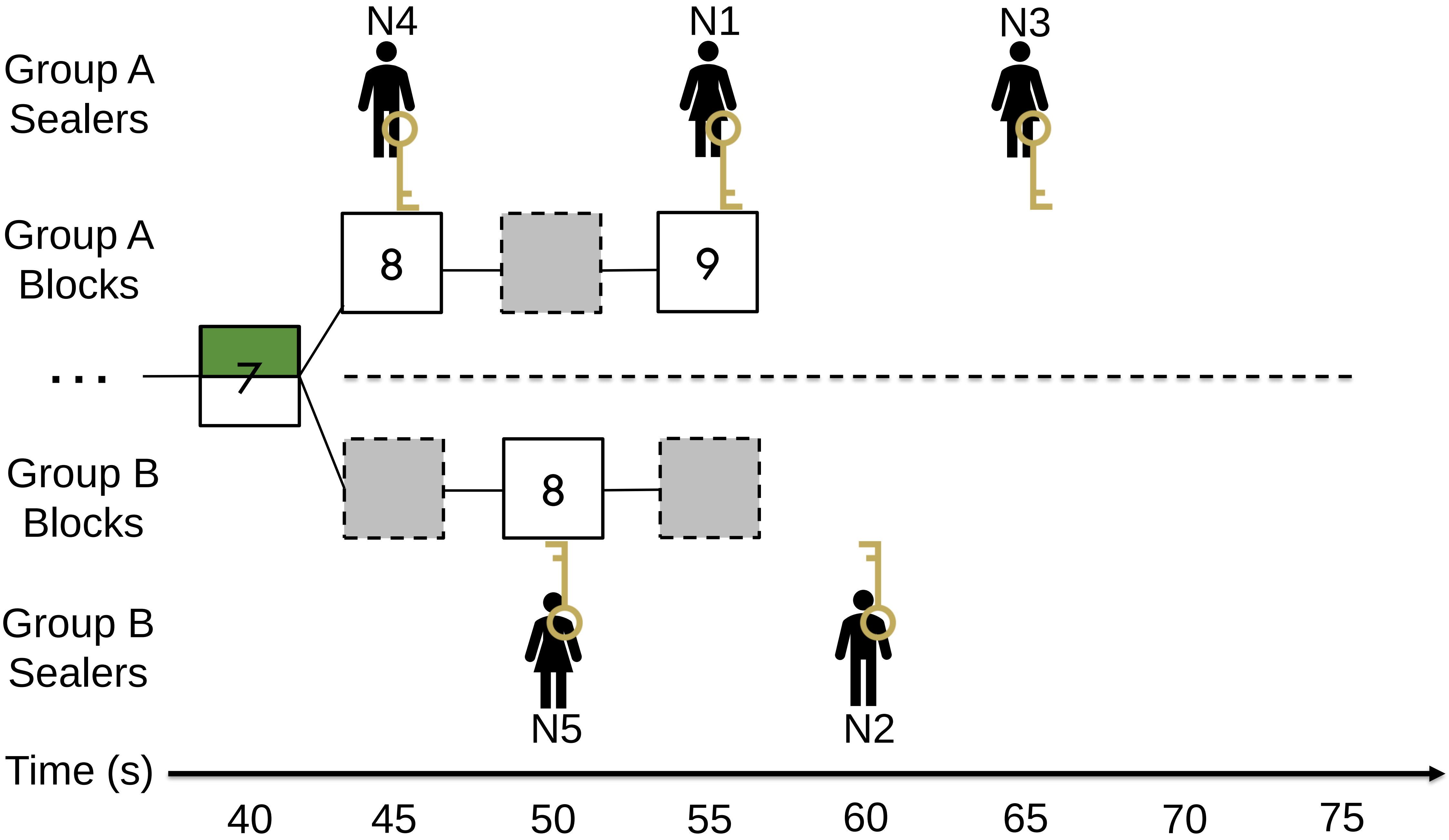


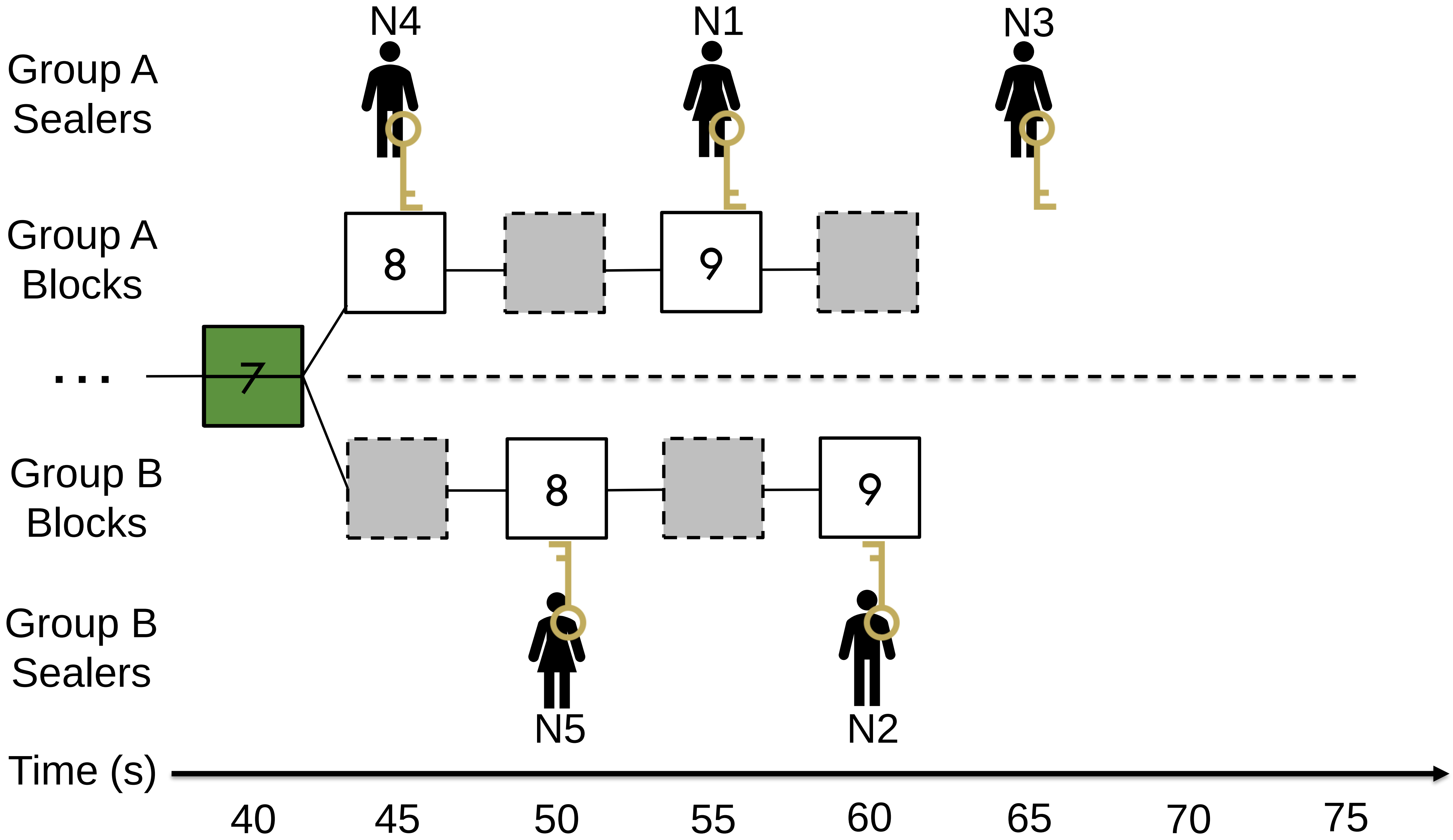

N3
...
7
Time (s)
40
45
50
55
60
65
70
75

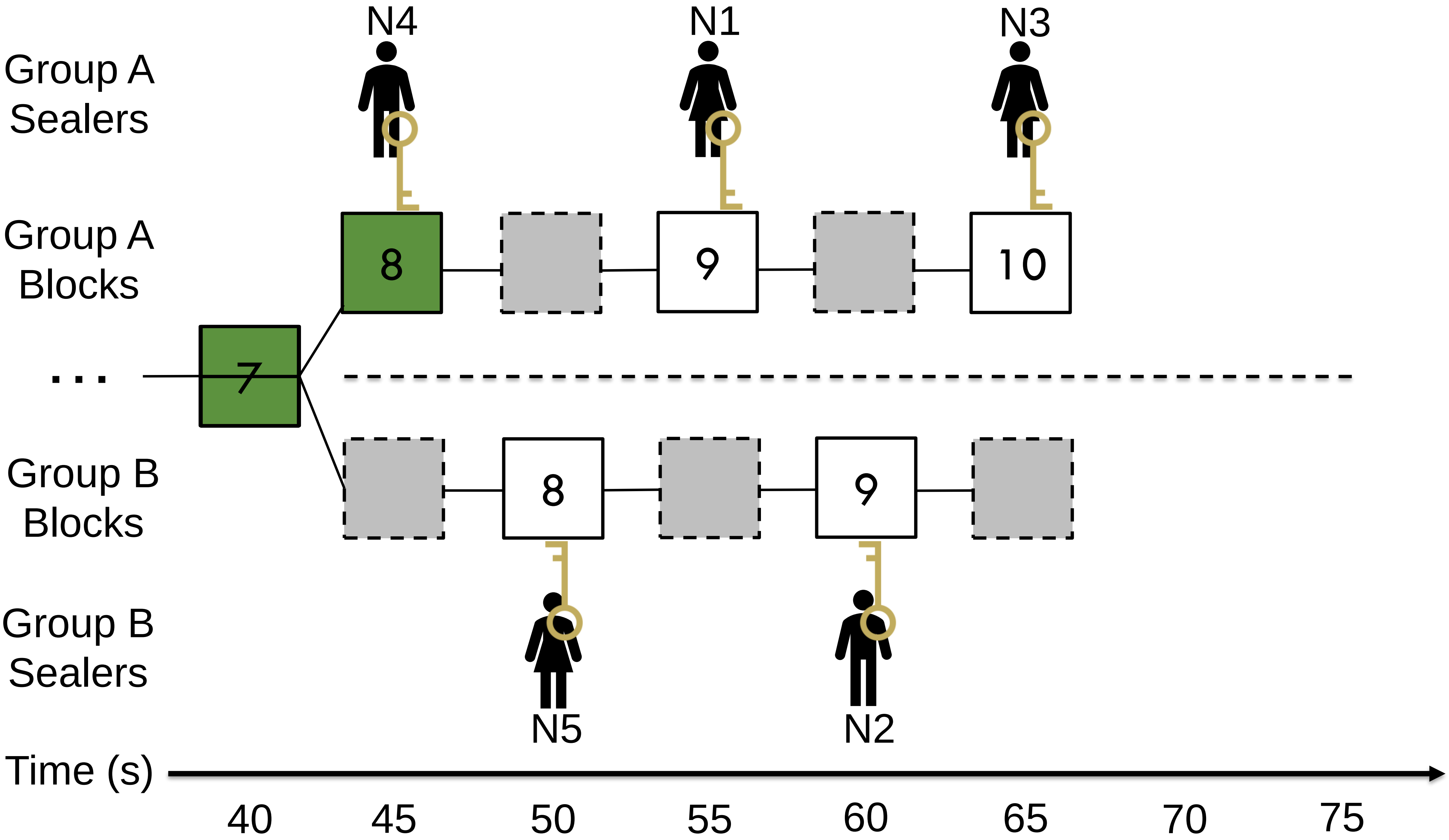

N4
N1
N3
Group A Sealers
Group A Blocks
...
7
Group B Blocks
Group B Sealers
N5
N2
Time (s)
40
45
50
55
60
65
70
75


N4
N1
N3
Group A Sealers
Group A Blocks
8
...
7
Group B Blocks
Group B Sealers
N5
N2
Time (s)
40
45
50
55
60
65
70
75

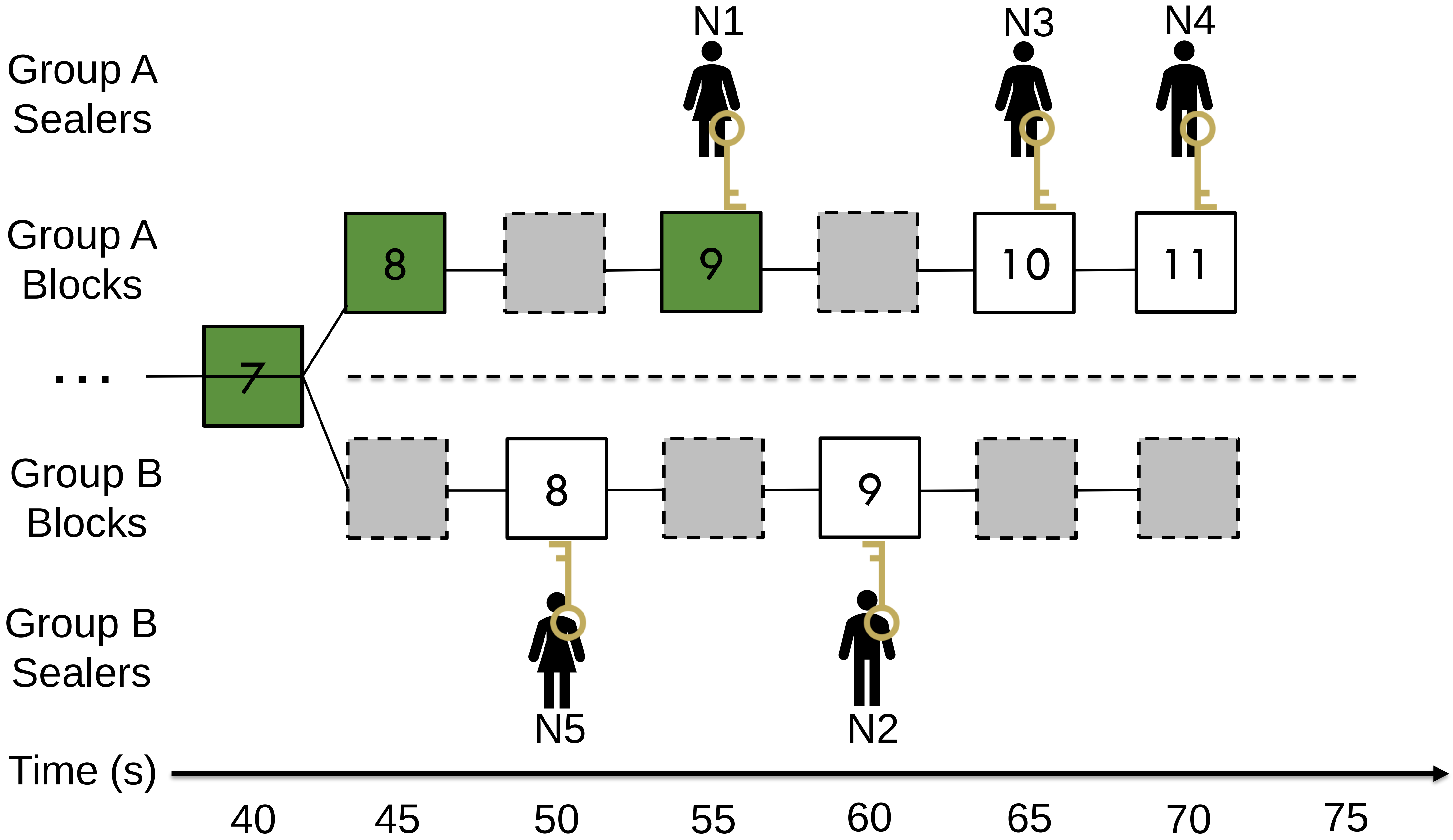

N4
N1
N3
Group A Sealers
Group A Blocks
8
7
...
Group B Blocks
8
Group B Sealers
N5
N2
Time (s)
40
45
50
55
60
65
70
75


N4
N1
N3
Group A
Sealers
Group A
Blocks
8
9
...
7
Group B
Blocks
8
Group B
Sealers
N5
N2
Time (s)
40
45
50
55
60
65
70
75

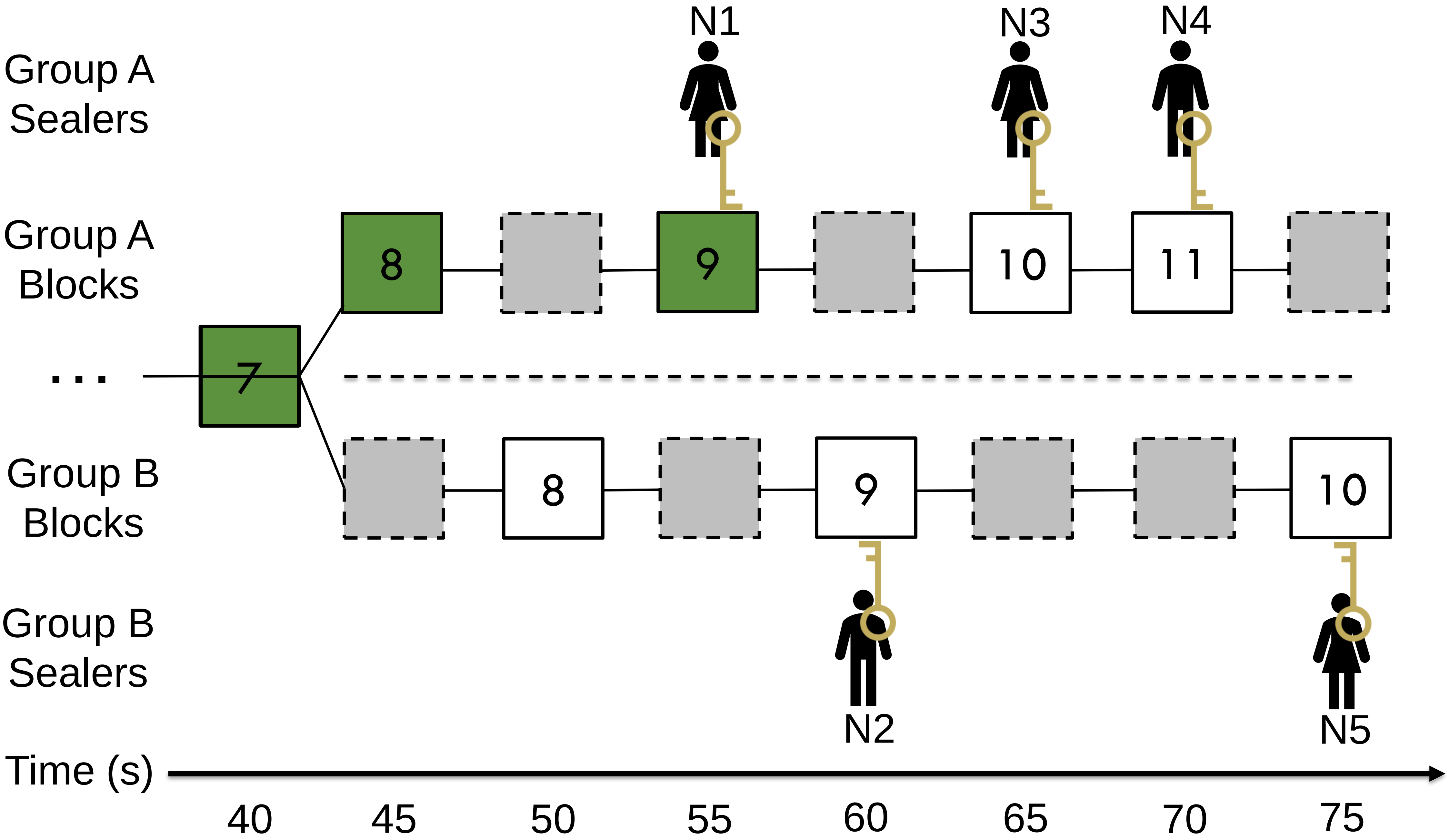

N4
N1
N3
Group A Sealers
Group A Blocks
8
9
...
7
Group B Blocks
8
9
Group B Sealers
N5
N2
Time (s)
40
45
50
55
60
65
70
75

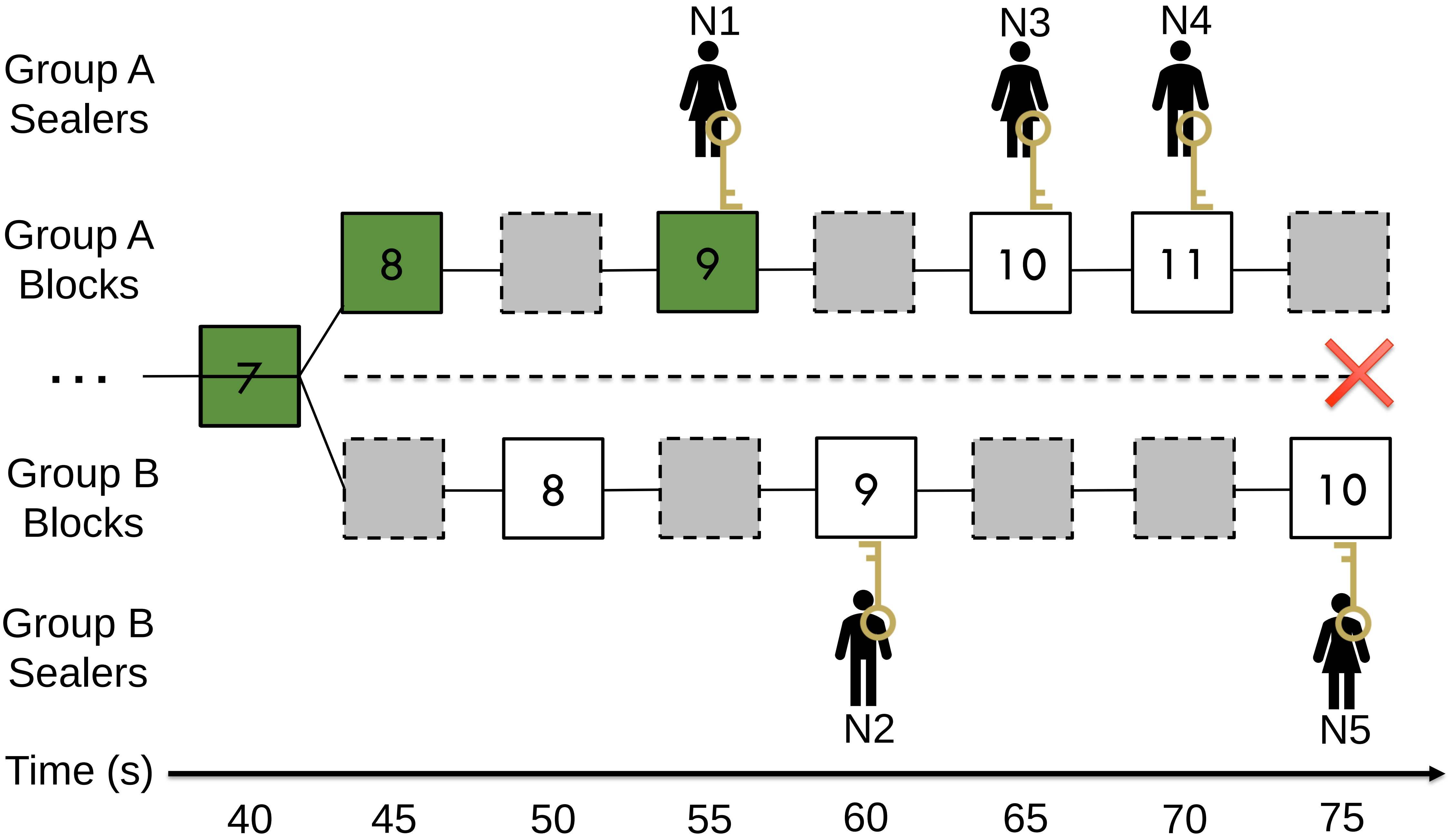


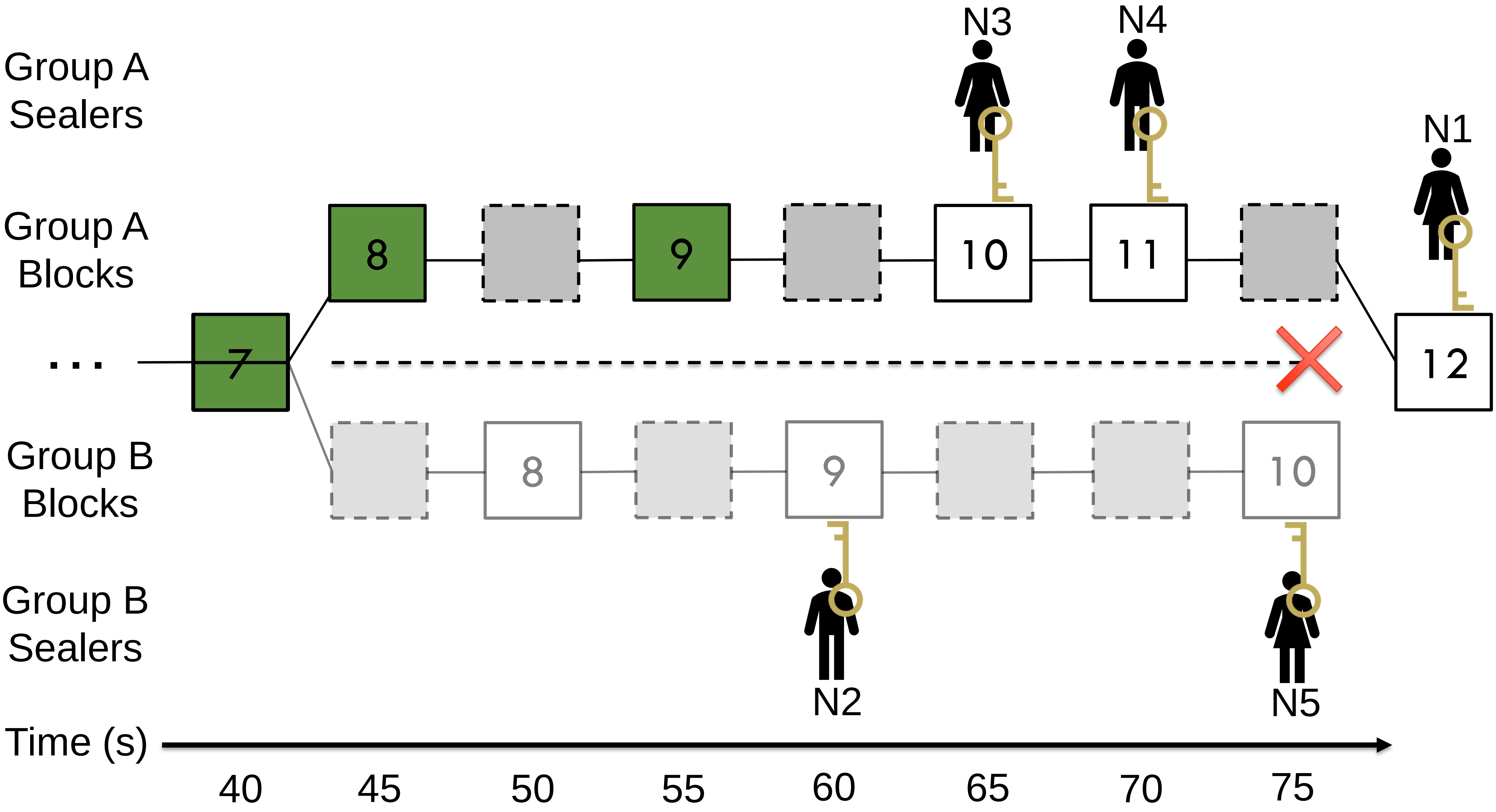
Ekparinya et al, "The Attack of the Clones against PoA"



Ekparinya et al, "The Attack of the Clones against PoA"


N1
N3
N4
Group A
Sealers
Group A
Blocks
8
9
10
11
...
7
Group B
Blocks
8
9
10
Group B
Sealers
N2
N5
Time (s)
40
45
50
55
60
65
70
75

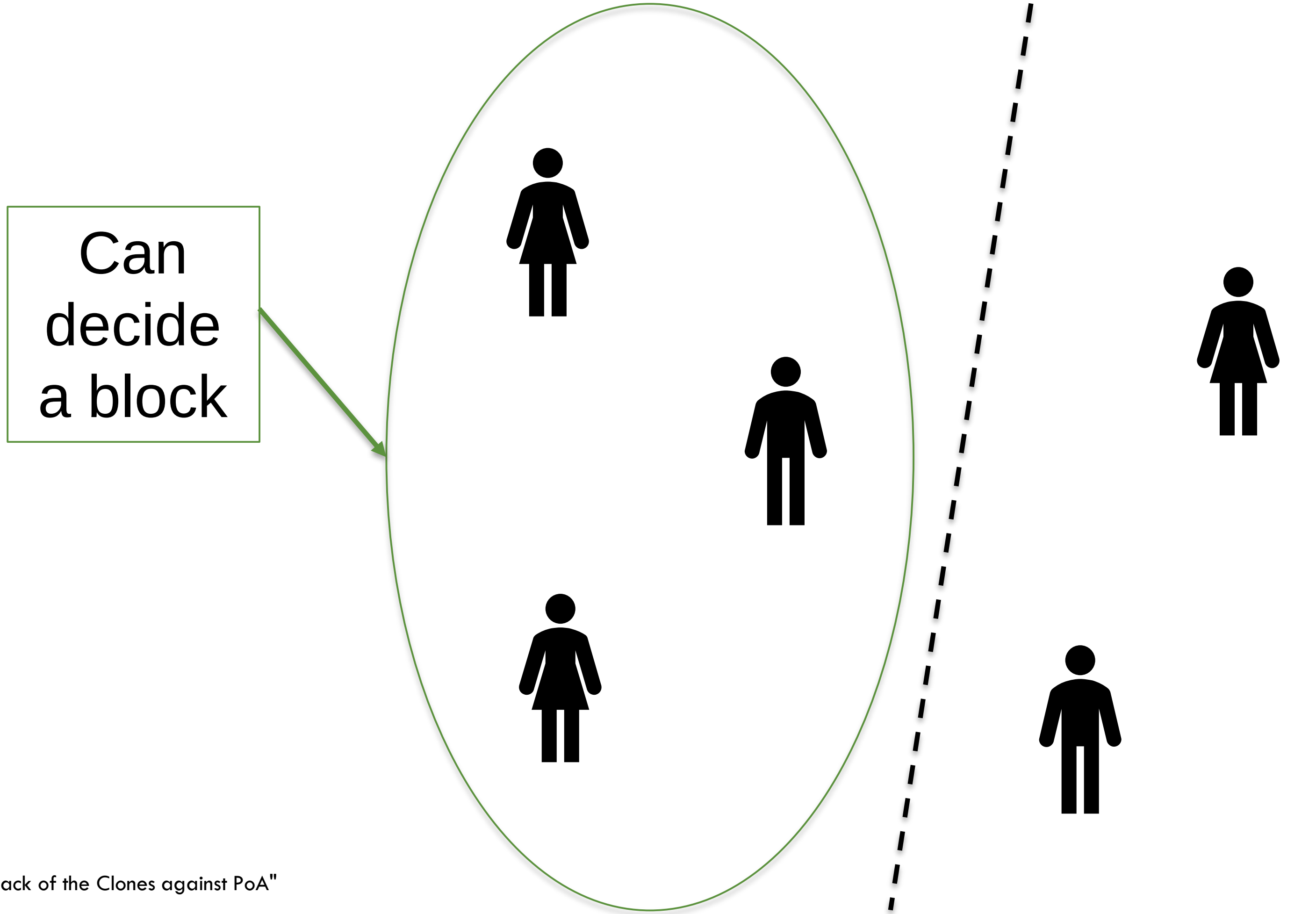

N1
N3
N4
Group A
Sealers
Group A
Blocks
8
9
10
11
...
7
Group B
Blocks
8
9
10
Group B
Sealers
N2
N5
Time (s)
40
45
50
55
60
65
70
75



Ekparinya et al, "The Attack of the Clones against PoA"

Block decision duration network partition

– Since decision requires strictly more than half, only one partition may decide blocks

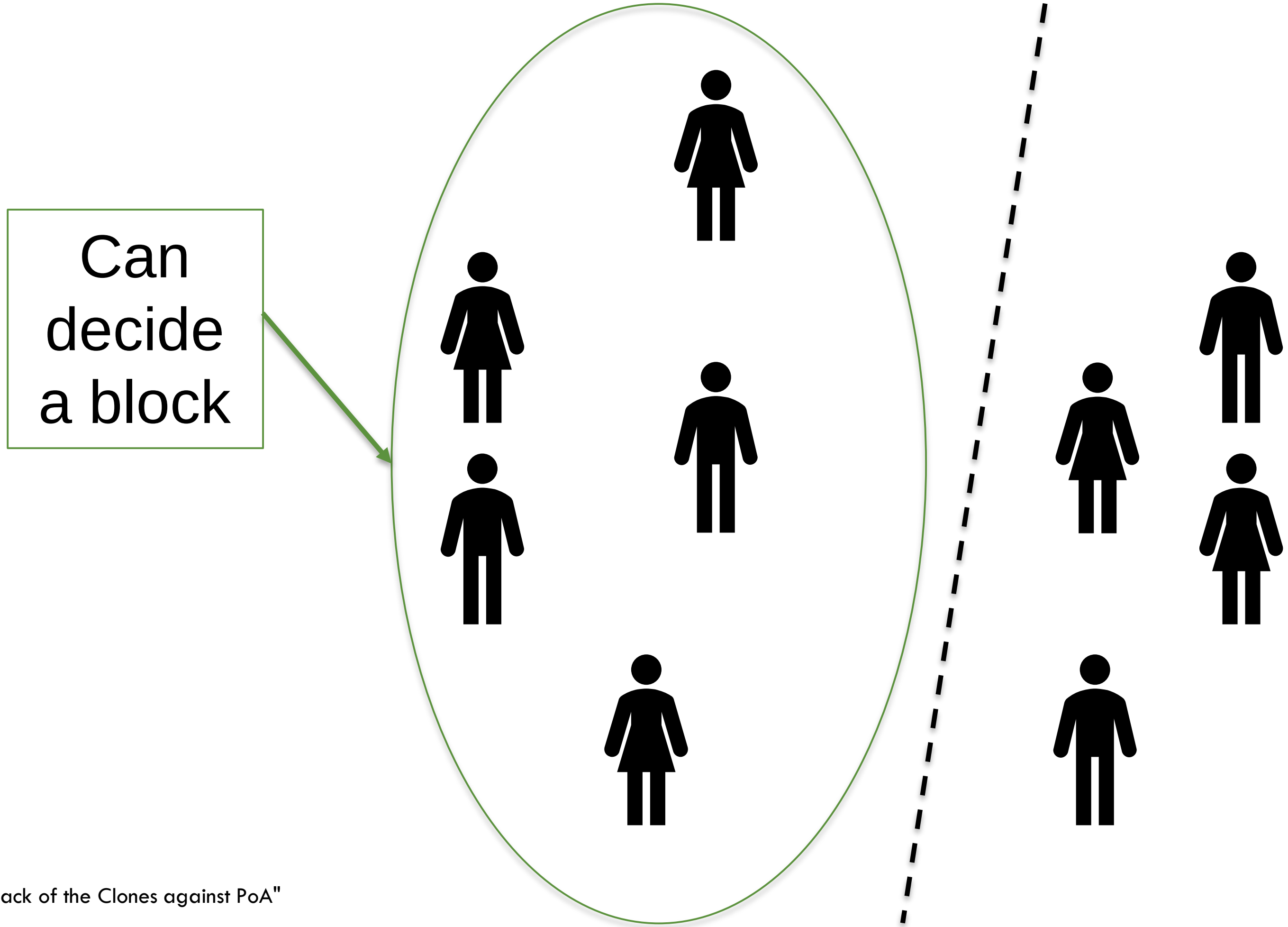


Can decide a block

Ekparinya et al, "The Attack of the Clones against PoA"

Block decision duration network partition

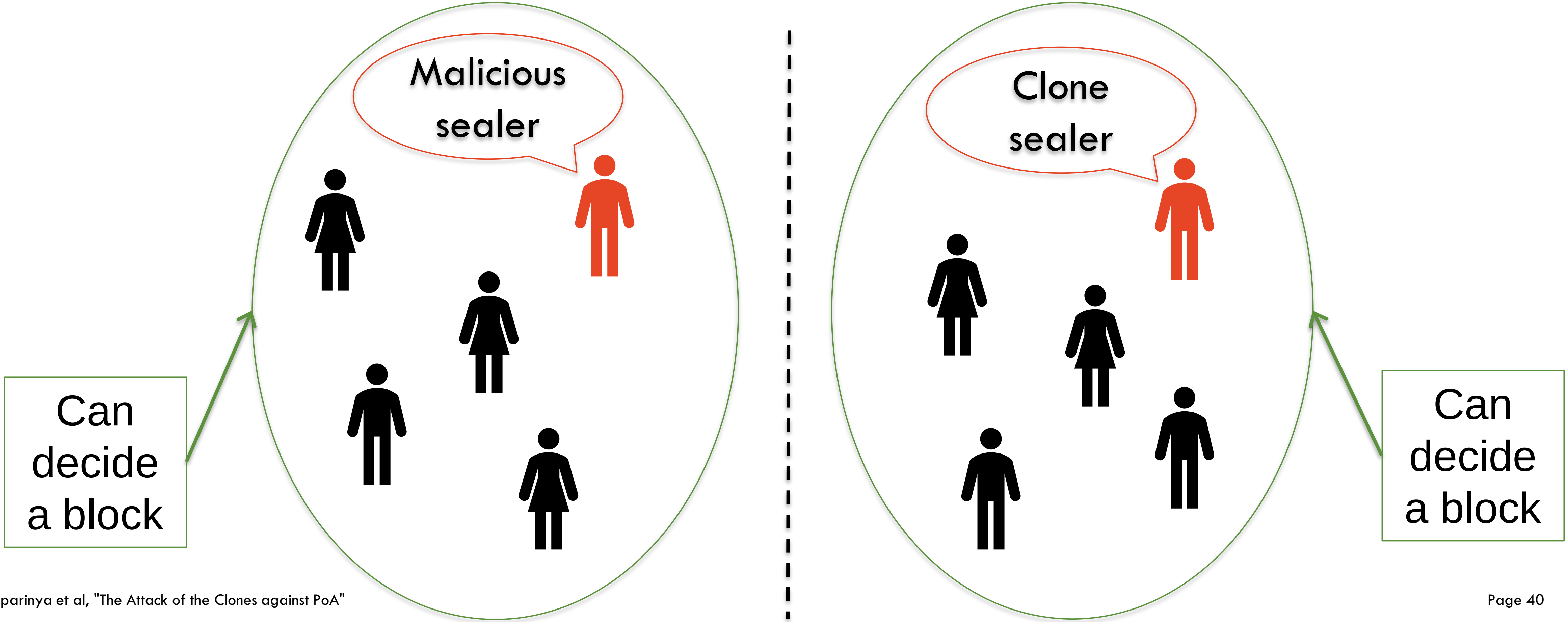
– Since decision requires strictly more than half, only one partition may decide blocks



Can decide a block

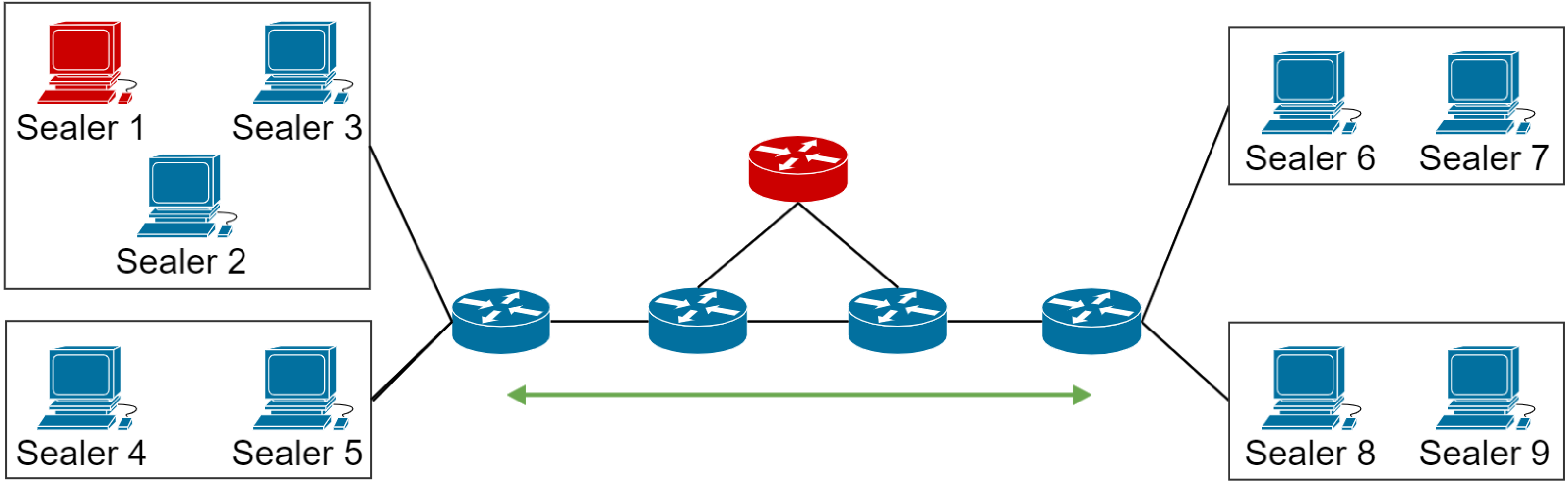
If one sealer become malicious

- A malicious sealer creates a clone to participate in both partitions!!
- If n = 9, both partitions contain 5 sealers, therefore both may decide a block!!



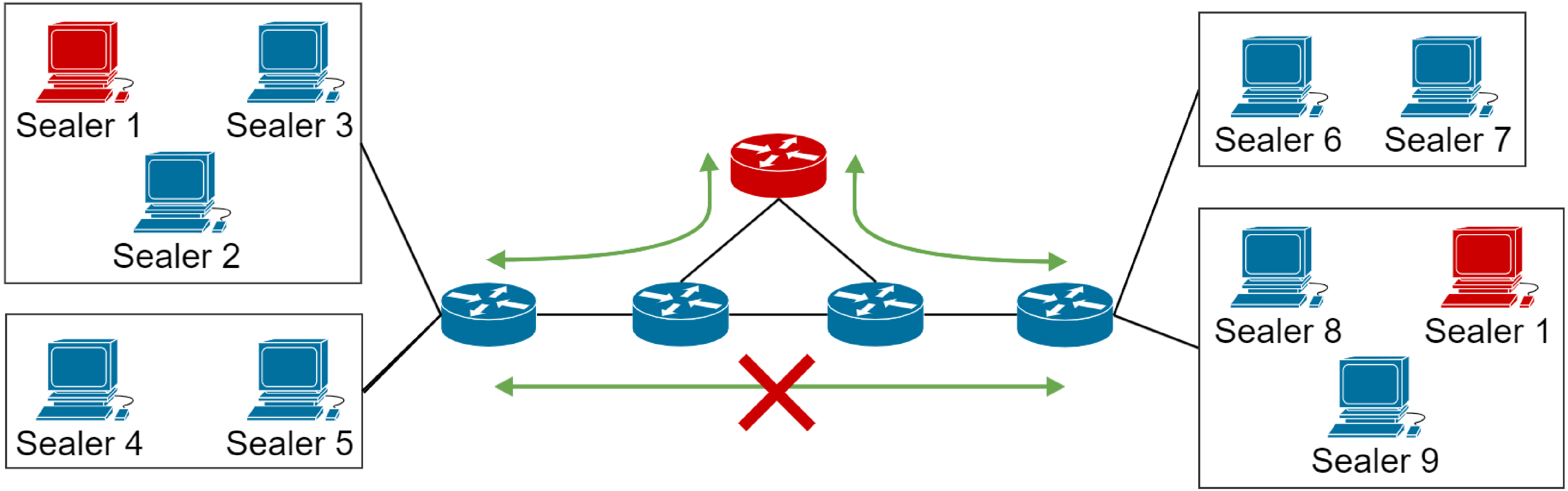
Ekparinya et al, "The Attack of the Clones against PoA"

The Cloning Attack



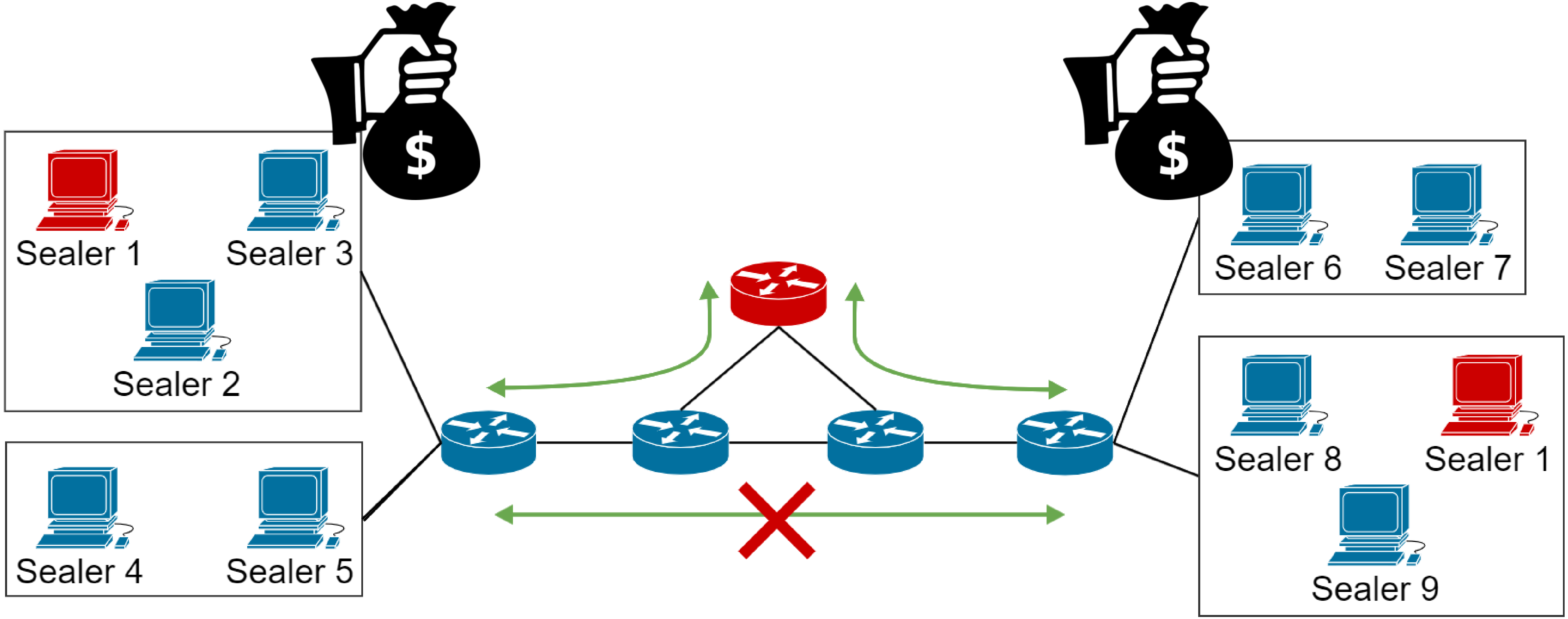
Ekparinya et al, "The Attack of the Clones against PoA"

The Cloning Attack



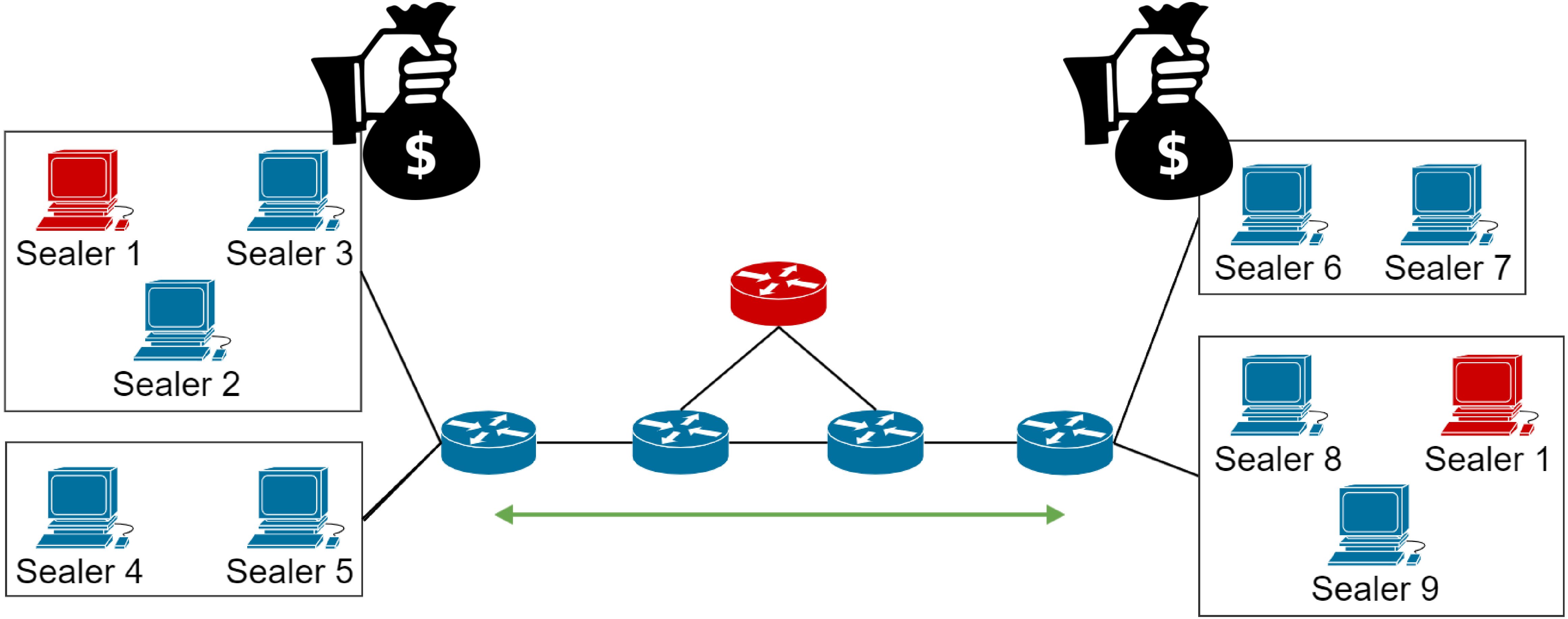
Ekparinya et al, "The Attack of the Clones against PoA"

The Cloning Attack



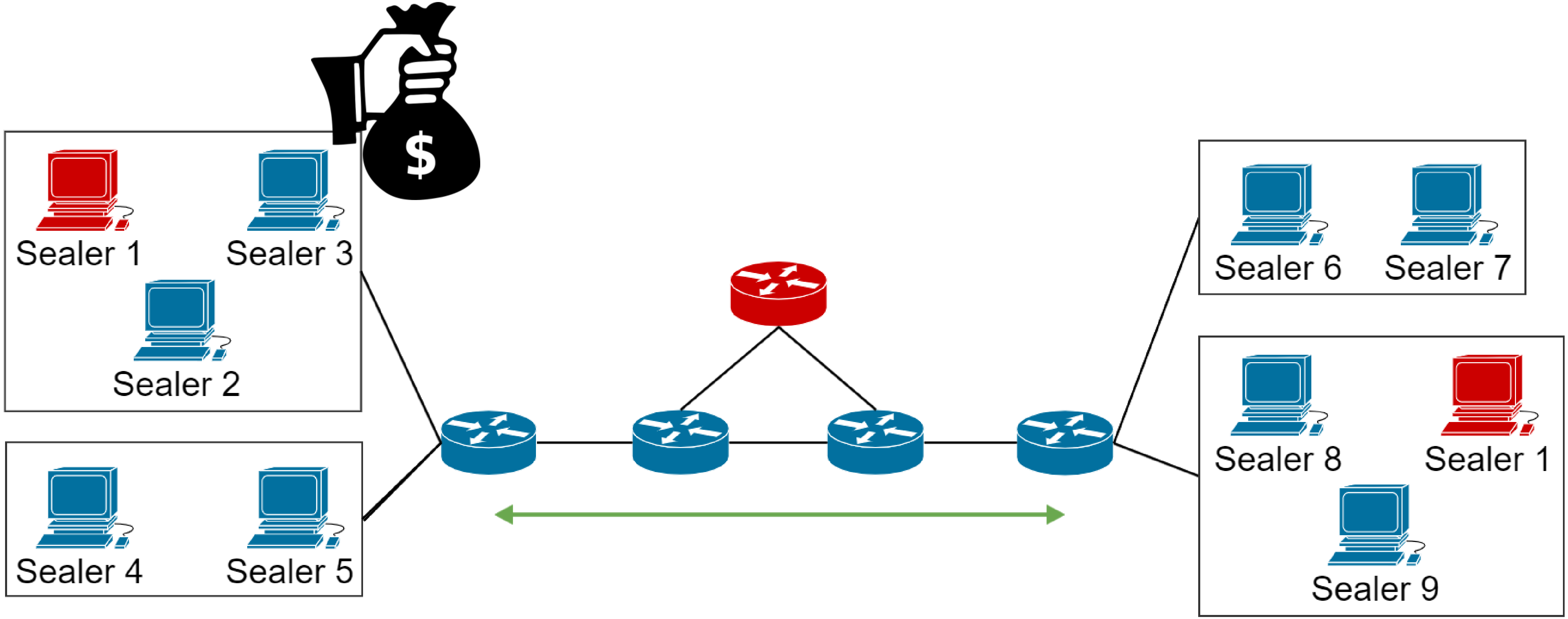
Ekparinya et al, "The Attack of the Clones against PoA"

The Cloning Attack

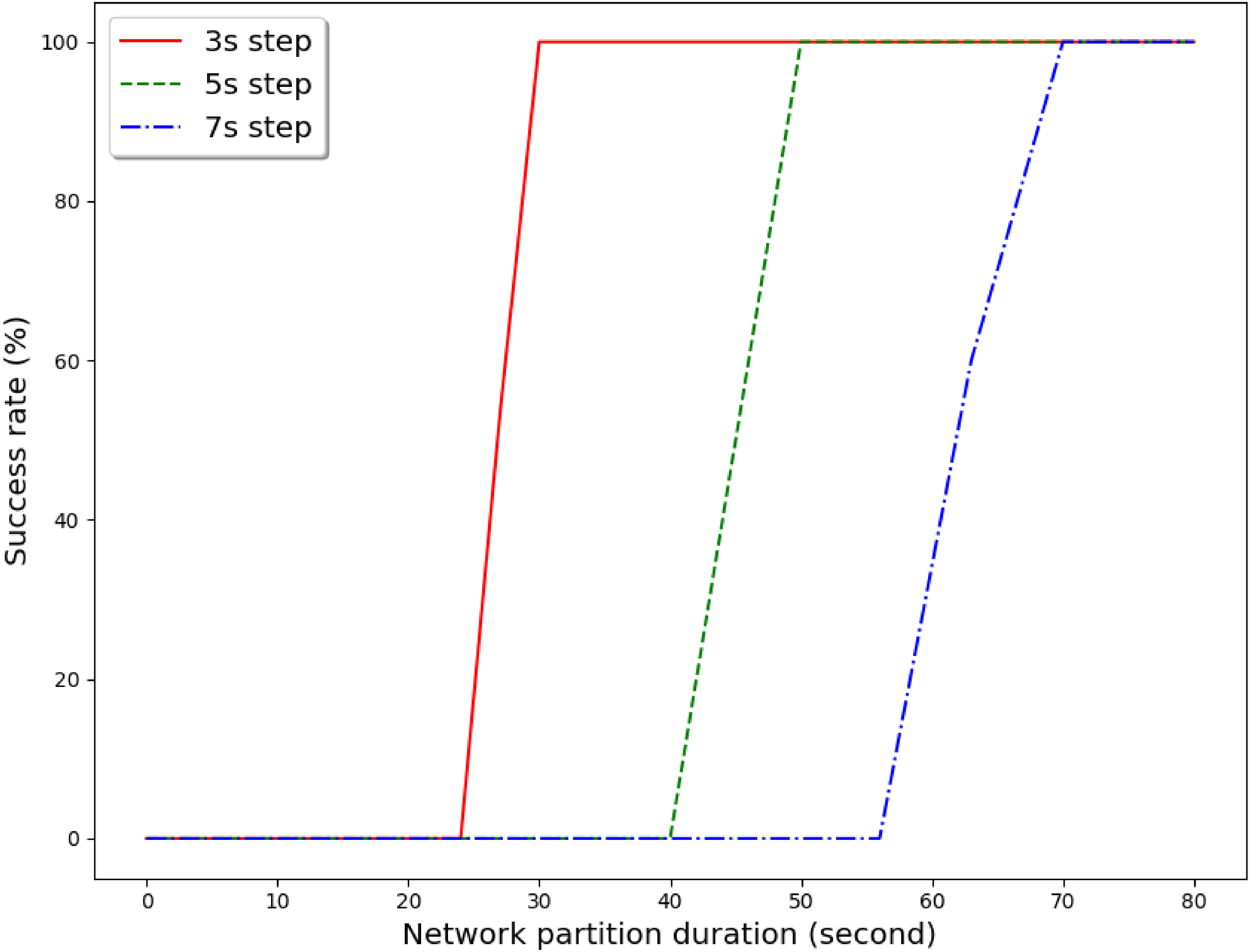


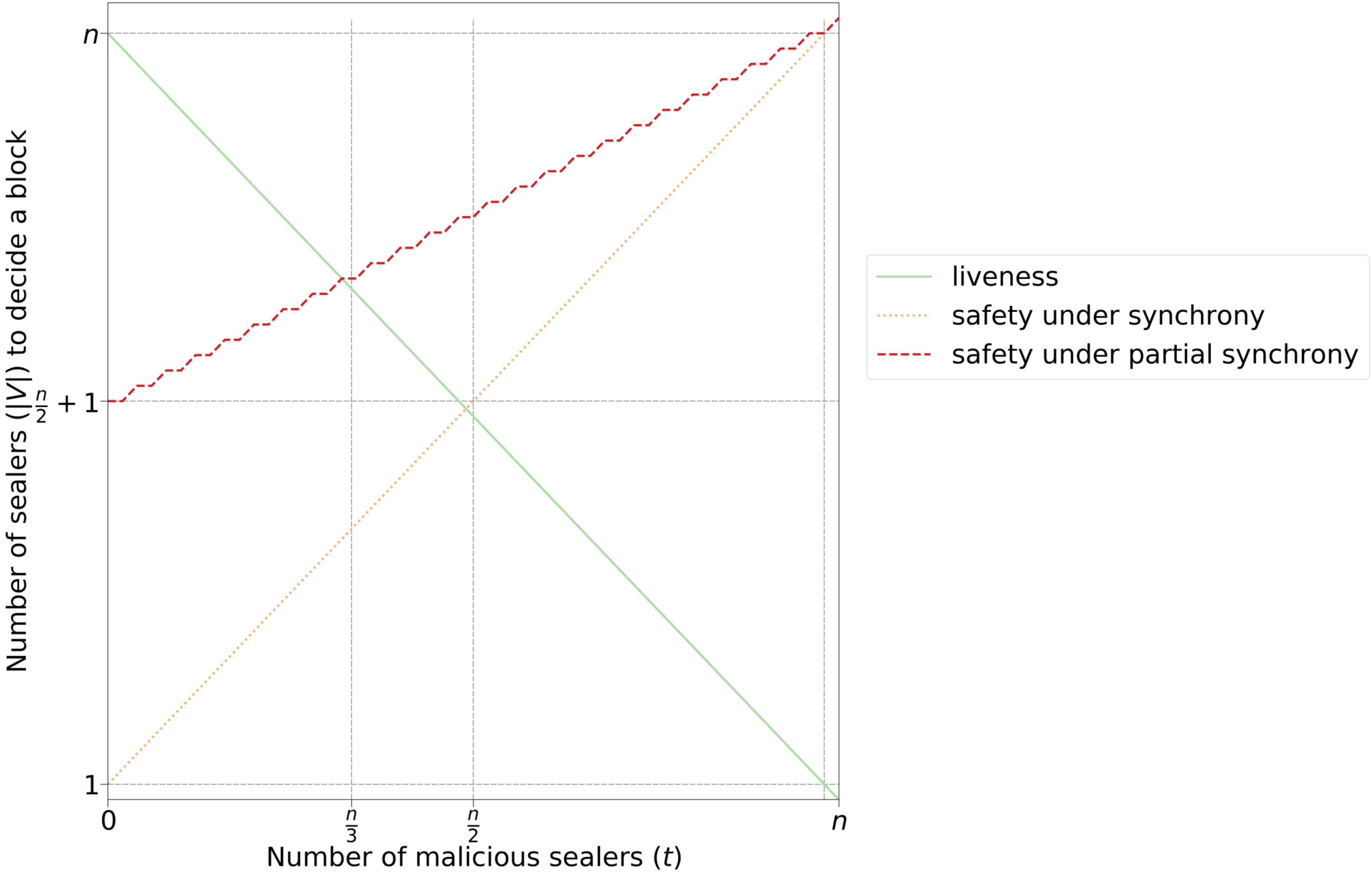
Ekparinya et al, "The Attack of the Clones against PoA"

The Cloning Attack

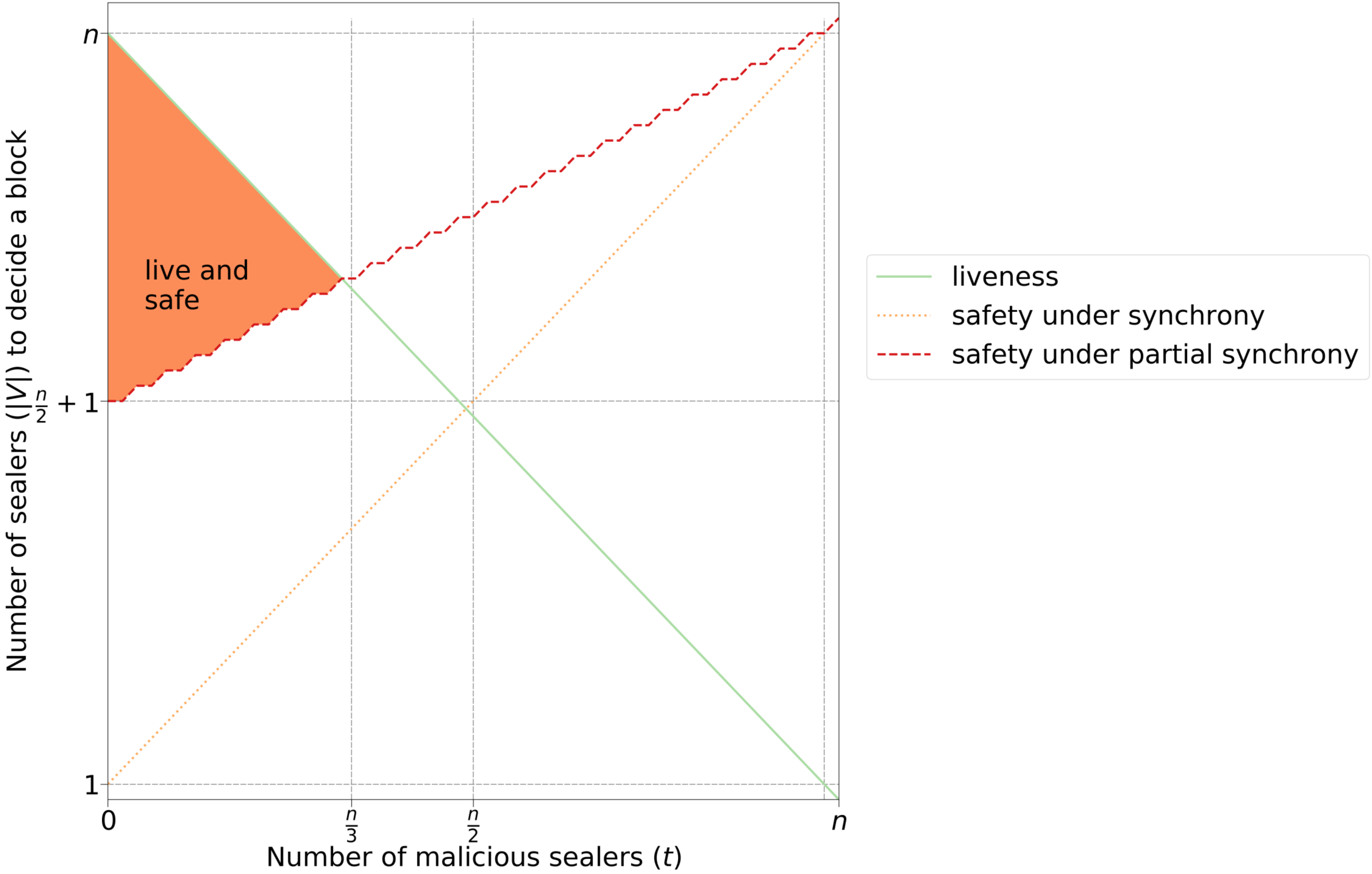


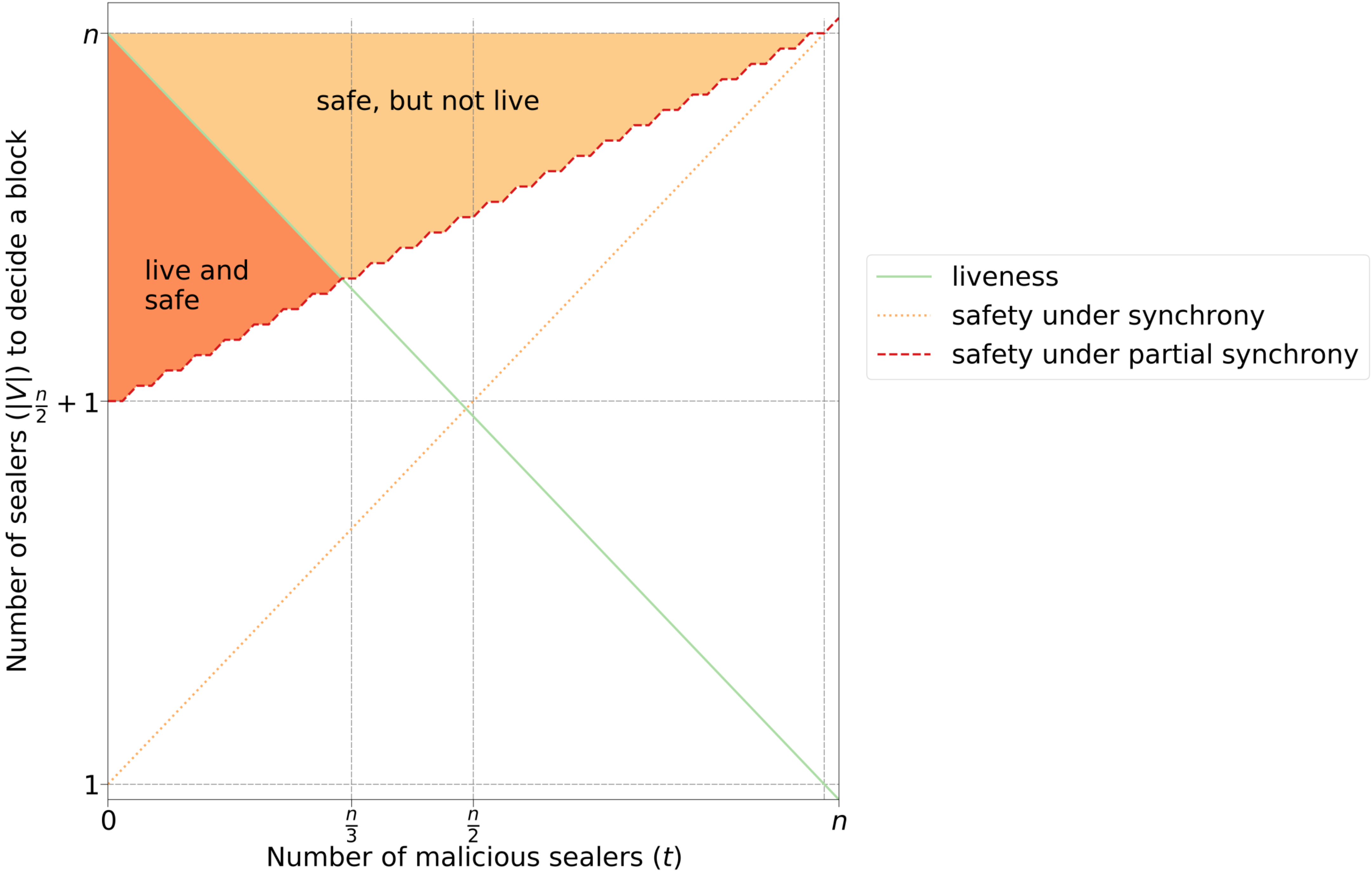
Ekparinya et al, "The Attack of the Clones against PoA"

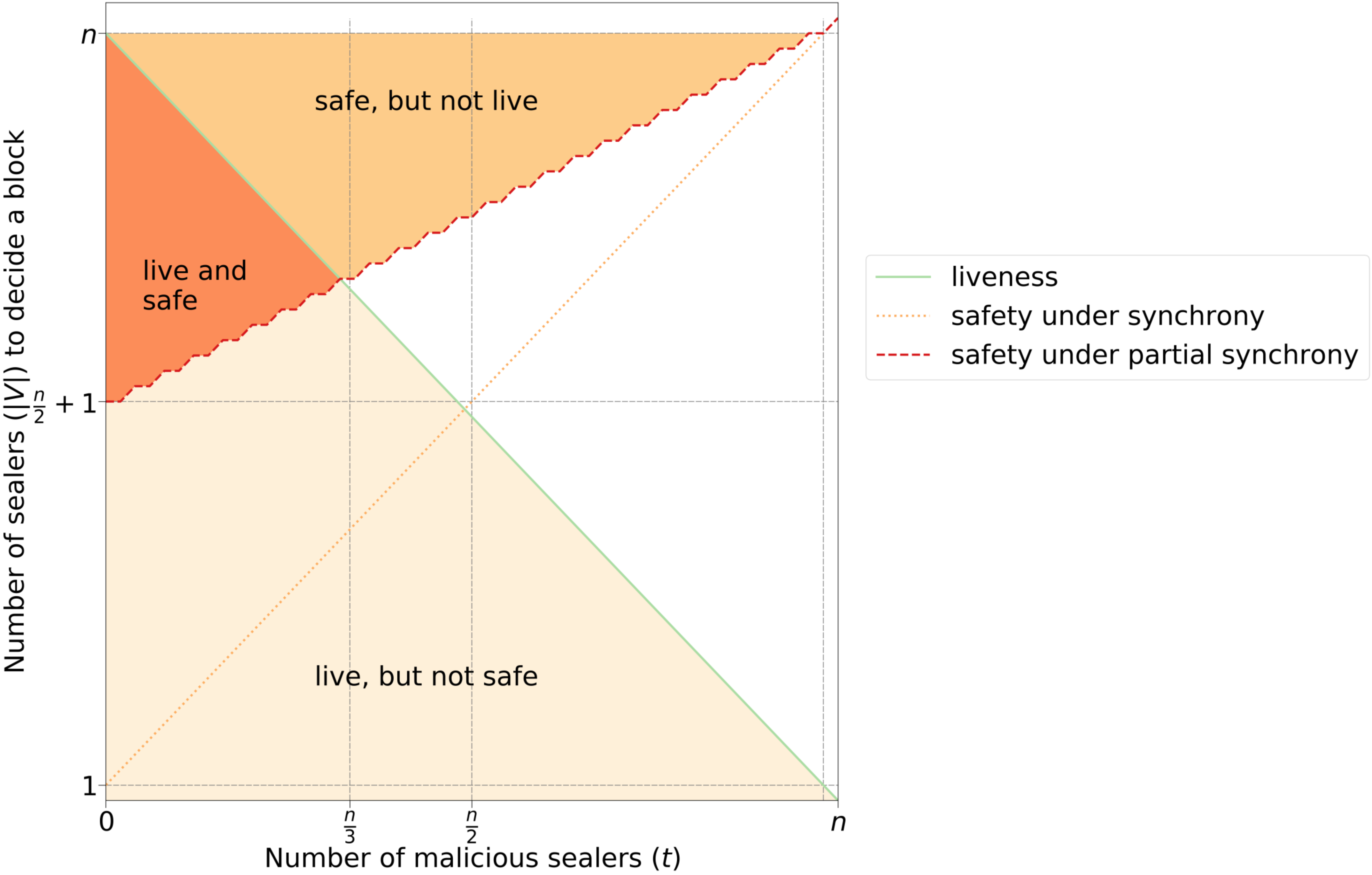

3s step
5s step
7s step
Success rate (%)
100
80
60
40
20
0
0
10
20
30
40
50
60
70
80
Network partition duration (second)

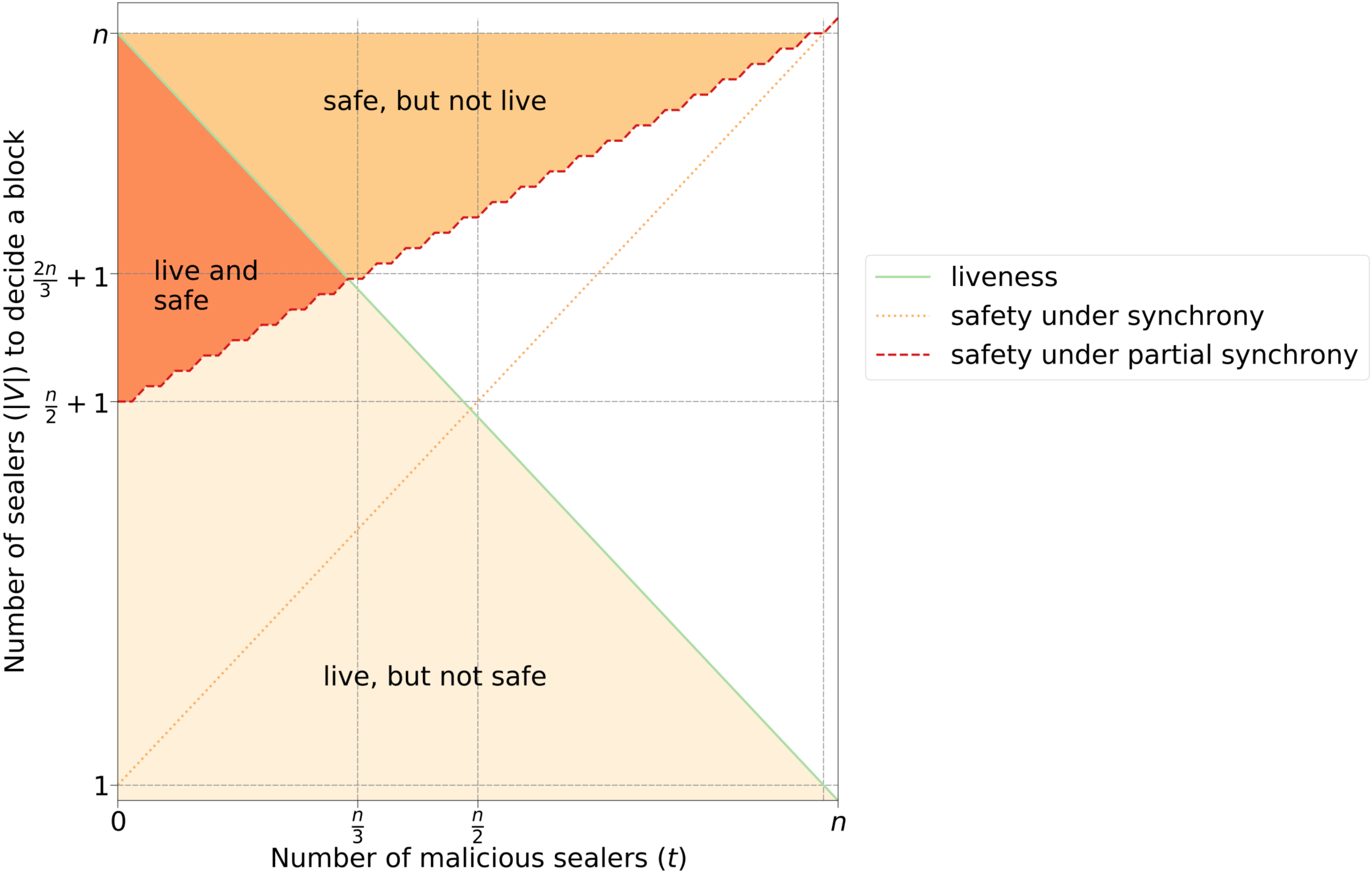


n
$\frac{n}{2}+1$
1
0
$\frac{n}{3}$
$\frac{n}{2}$
n
Number of sealers ($|V|$) to decide a block
Number of malicious sealers (t)
liveness
safety under synchrony
safety under partial synchrony


n
$\frac{n}{2}+1$
1
0
$\frac{n}{3}$
$\frac{n}{2}$
n
Number of sealers (|V|) to decide a block
Number of malicious sealers (t)
live and safe
liveness
safety under synchrony
safety under partial synchrony

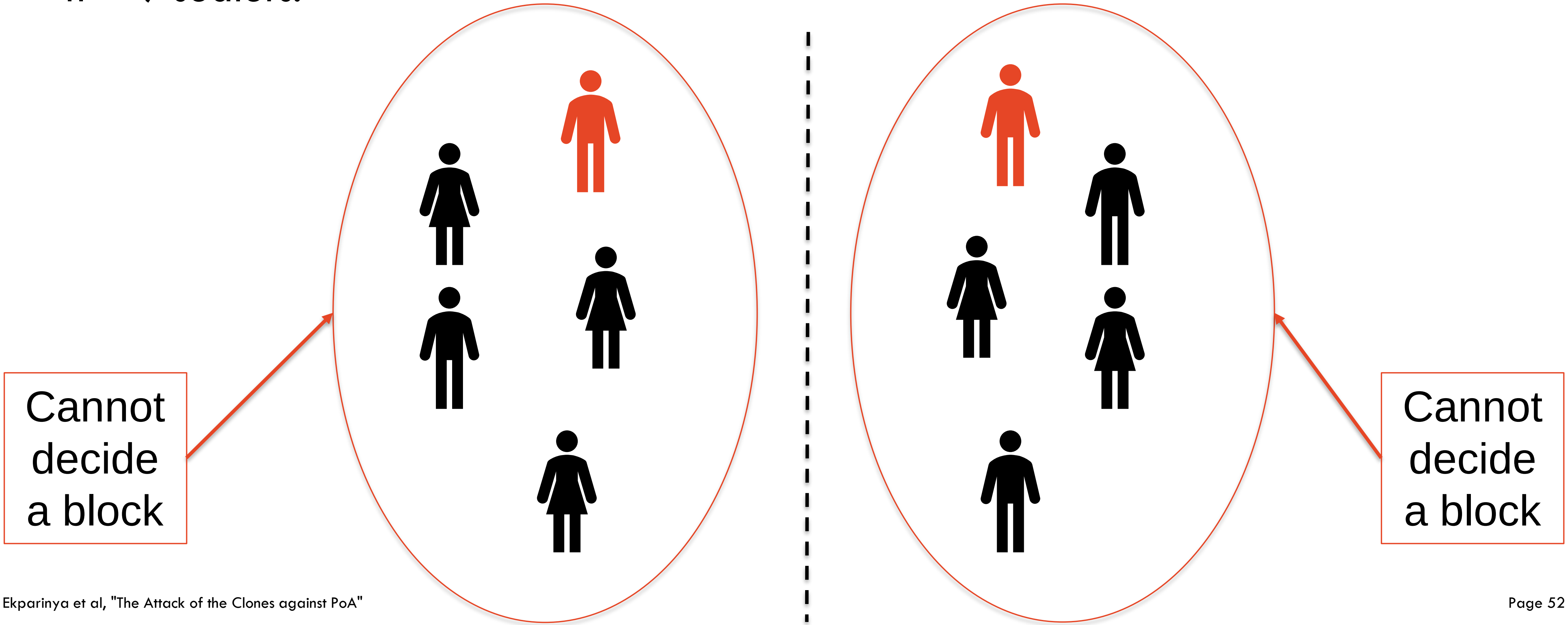

safe, but not live
live and safe
liveness
safety under synchrony
safety under partial synchrony
Number of sealers (|V|) to decide a block
n
$\frac{n}{2}+1$
1
0
$\frac{n}{3}$
$\frac{n}{2}$
n
Number of malicious sealers (t)


safe, but not live
live and safe
live, but not safe
liveness
safety under synchrony
safety under partial synchrony
Number of sealers (|V|) to decide a block
n
$\frac{n}{2}+1$
1
0
$\frac{n}{3}$
$\frac{n}{2}$
n
Number of malicious sealers (t)


n
$\frac{2n}{3}+1$
$\frac{n}{2}+1$
1
0
$\frac{n}{3}$
$\frac{n}{2}$
n
Number of sealers (|V|) to decide a block
Number of malicious sealers (t)
safe, but not live
live and safe
live, but not safe
liveness
safety under synchrony
safety under partial synchrony

Countermeasure

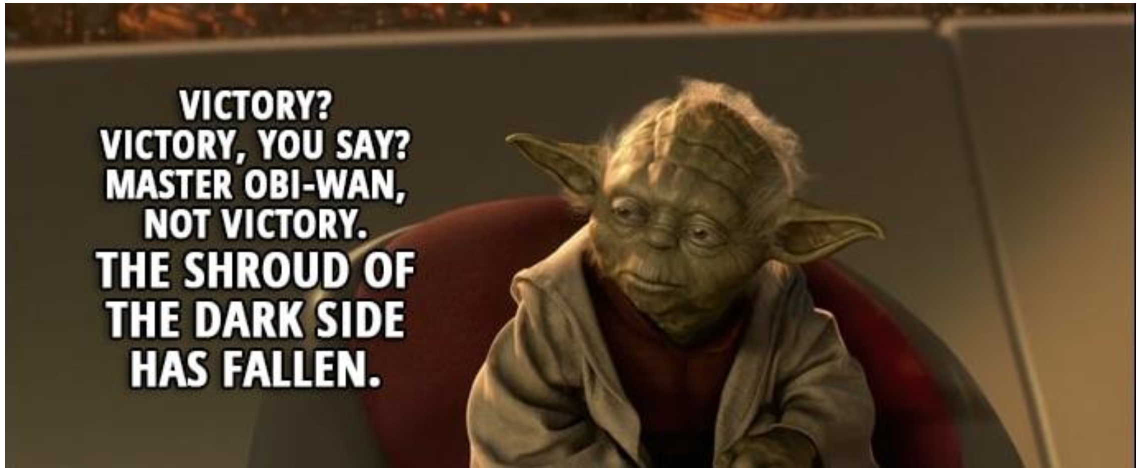
- The algorithm will be more resistant to the attack if it requires strictly more than two-thirds to decide a block as shown in the illustration below with n = 9 sealers.



Cannot decide a block

Cannot decide a block

Key takeaways



- With the attack of the Clones, it is possible to double spend in PoA/Ethereum.
- Provided sufficient network partition duration, the attacker can double spend with 100% success rate.
- To promote safety property in PoA/Ethereum: the higher number of required sealers, the higher resistance against the attack.
- The attack applies as well to Clique. The details can be found in paper.
- We exchanged with the security experts of geth and parity. The developers of xDai have already took this attack into account in their POSDAO consensus algorithm.

Ekparinya et al, "The Attack of the Clones against PoA"