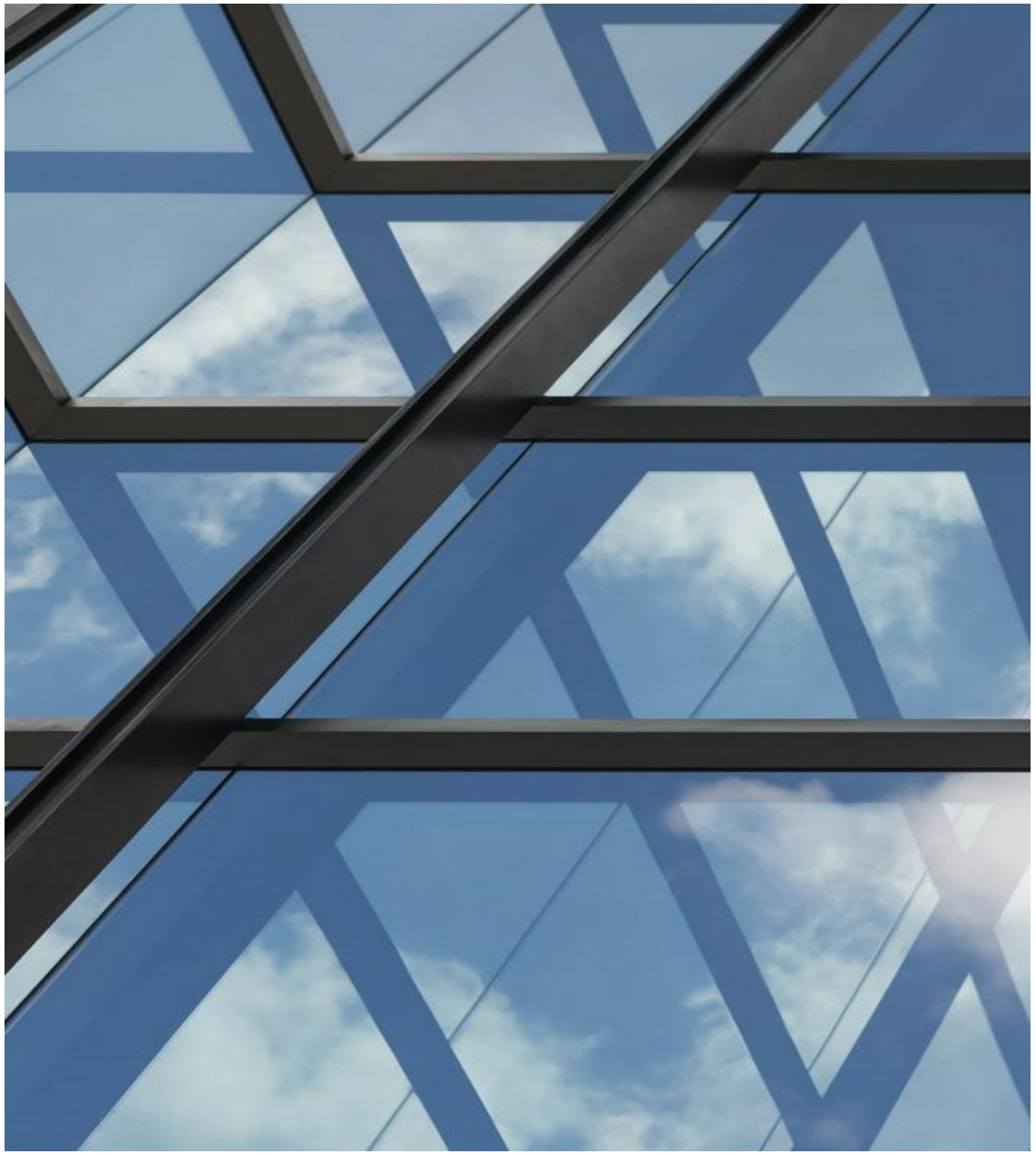
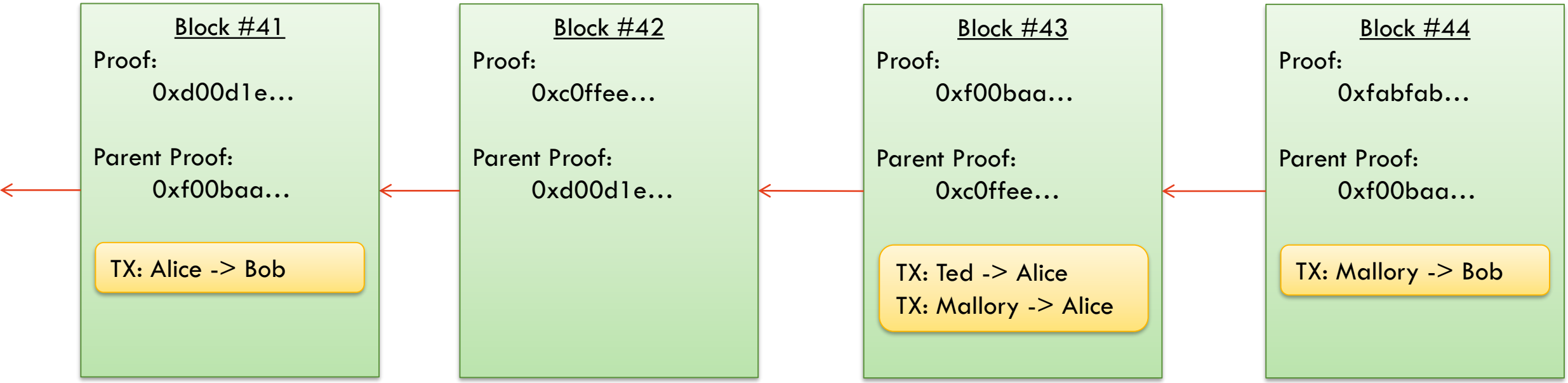
How to Hack Blockchain Systems

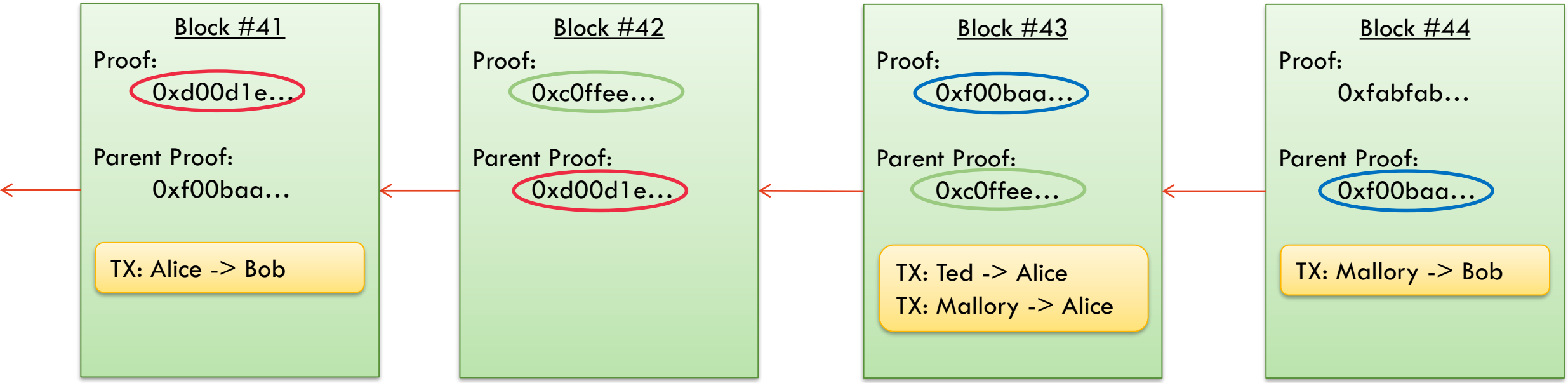
Parinya Ekparinya
Vincent Gramoli
Guillaume Jourjon



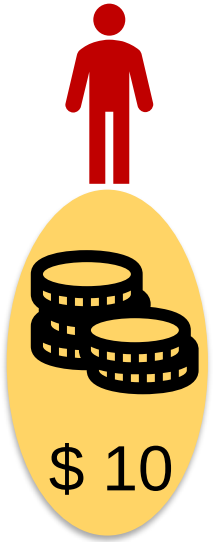
Blockchain

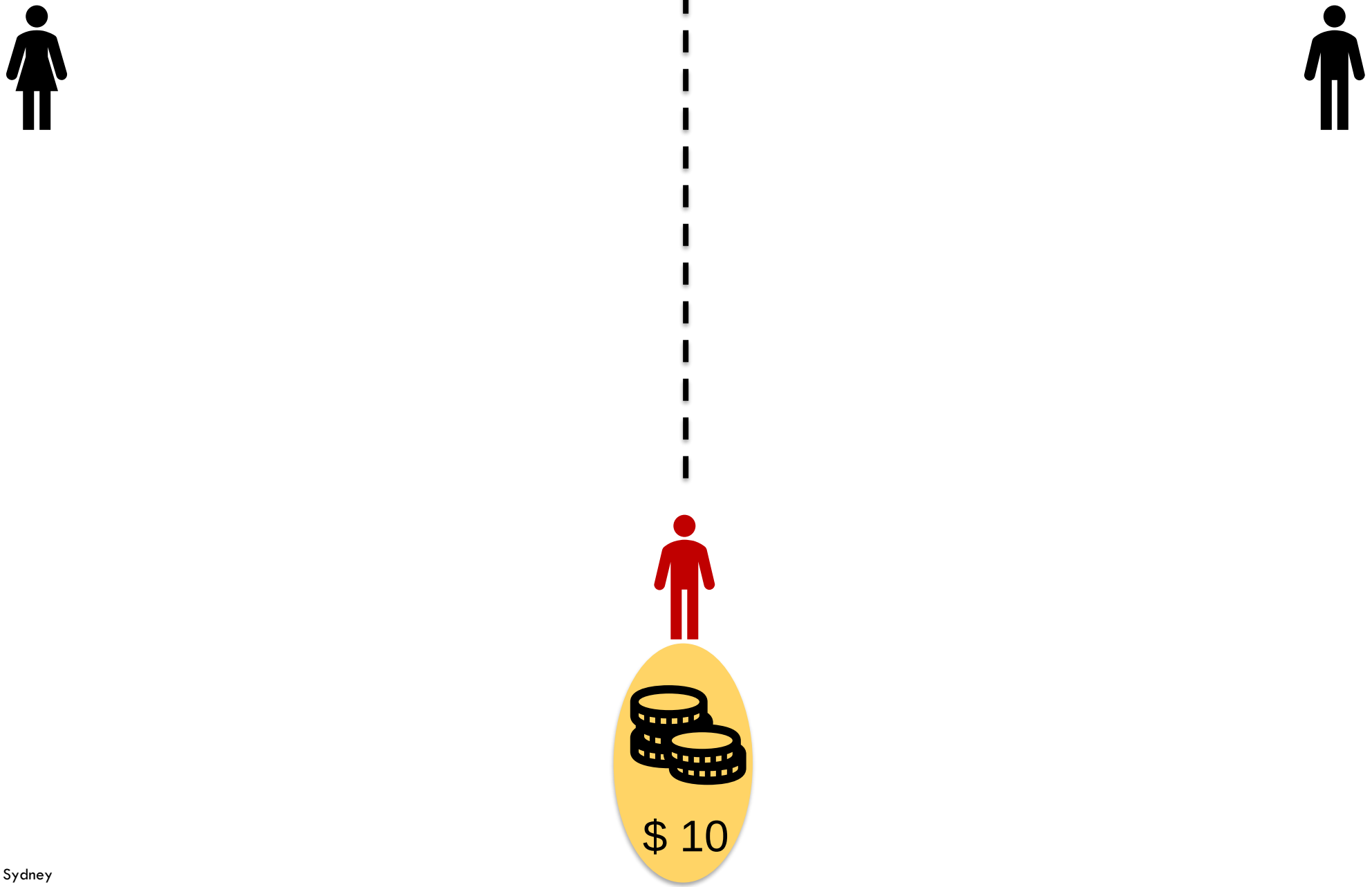

Block #41
Proof:
0xd00d1e...
Parent Proof:
0xf00baa...
TX: Alice -> Bob
Block #42
Proof:
0xc0ffee...
Parent Proof:
0xd00d1e...
Block #43
Proof:
0xf00baa...
Parent Proof:
0xc0ffee...
TX: Ted -> Alice
TX: Mallory -> Alice
Block #44
Proof:
0xfabfab...
Parent Proof:
0xf00baa...
TX: Mallory -> Bob

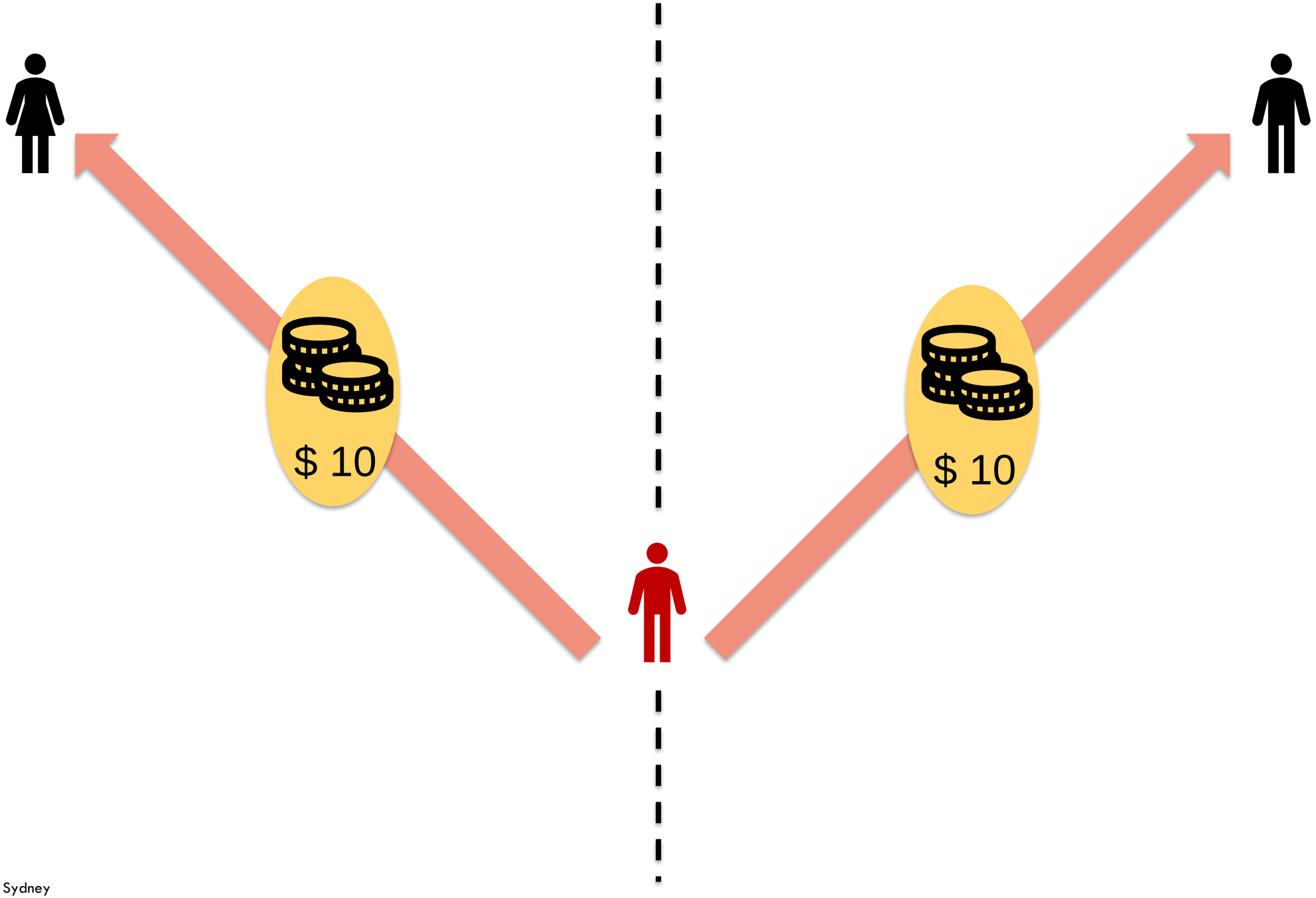
Blockchain


Block #41
Proof:
0xd00d1e...
Parent Proof:
0xf00baa...
TX: Alice -> Bob
Block #42
Proof:
0xc0ffee...
Parent Proof:
0xd00d1e...
Block #43
Proof:
0xf00baa...
Parent Proof:
0xc0ffee...
TX: Ted -> Alice
TX: Mallory -> Alice
Block #44
Proof:
0xfabfab...
Parent Proof:
0xf00baa...
TX: Mallory -> Bob


Insert
Home
Page Up
End
Page Down

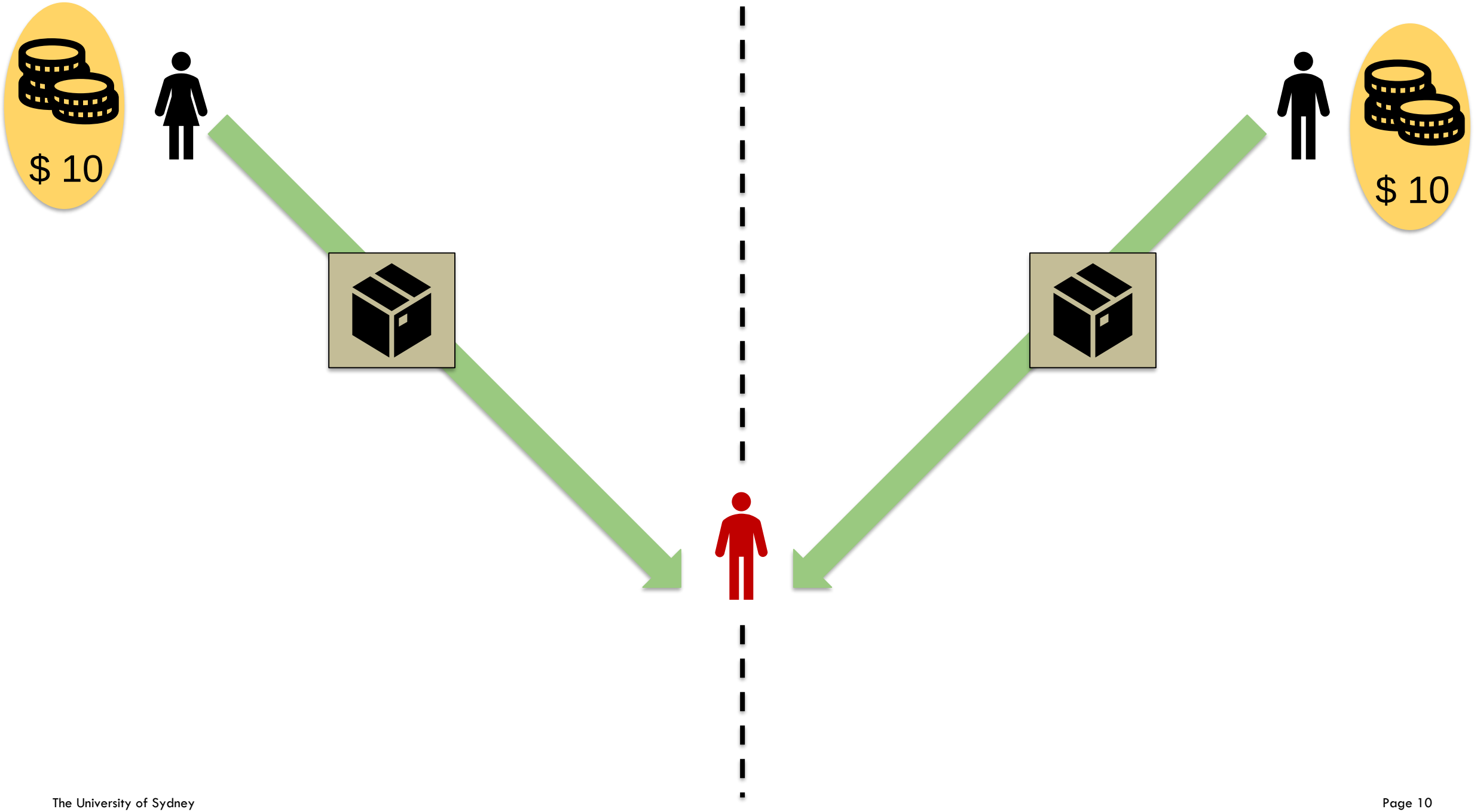

$ 10

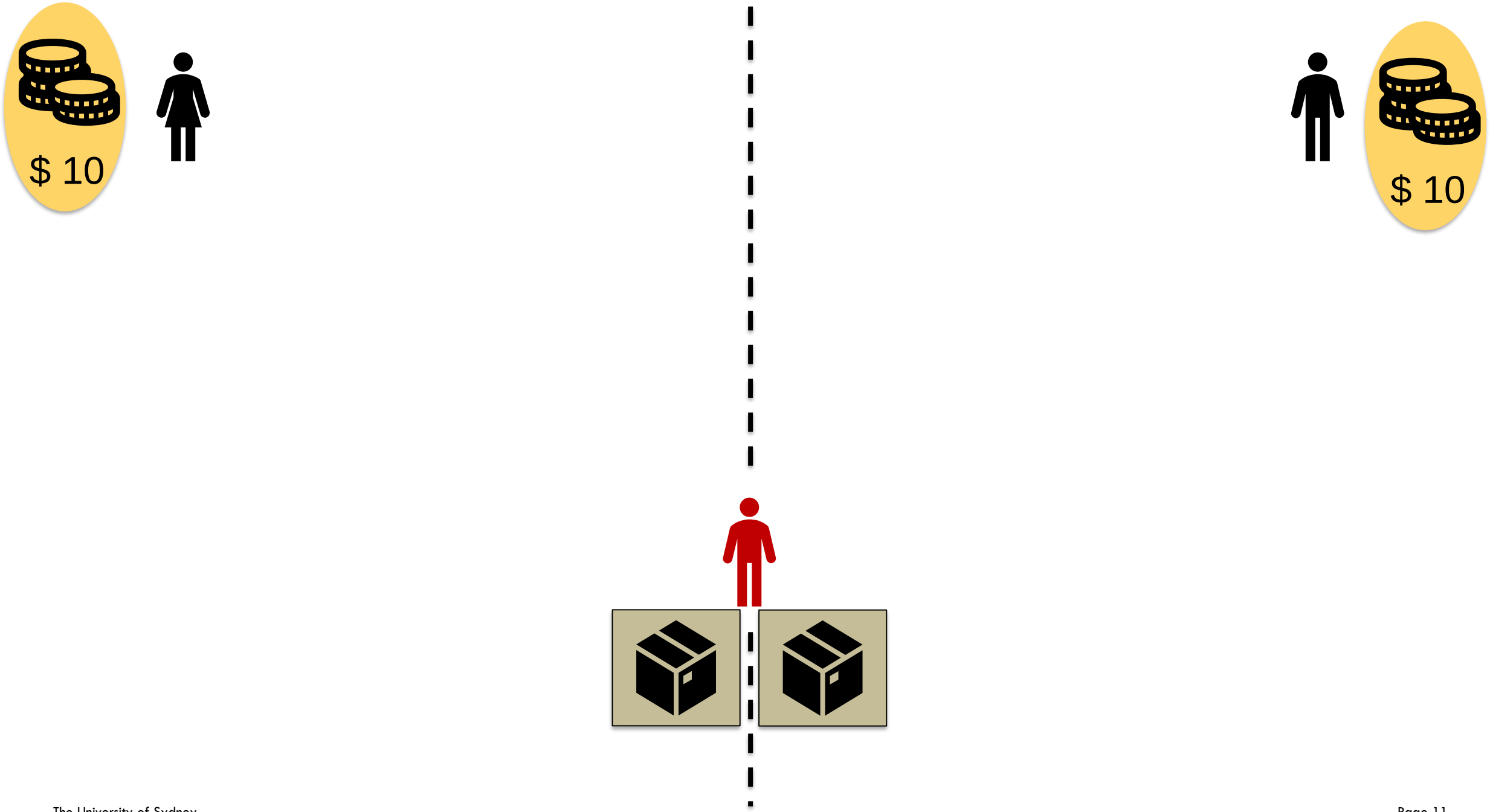

$ 10


$ 10
$ 10


$ 10

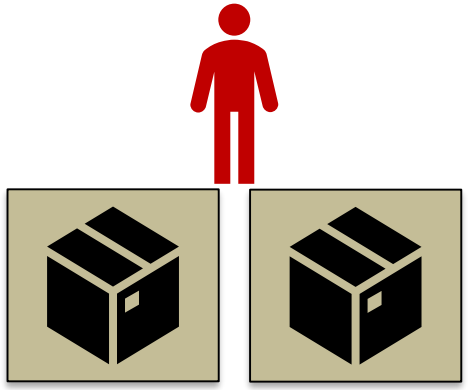

$ 10


$ 10
$ 10


$ 10
$ 10

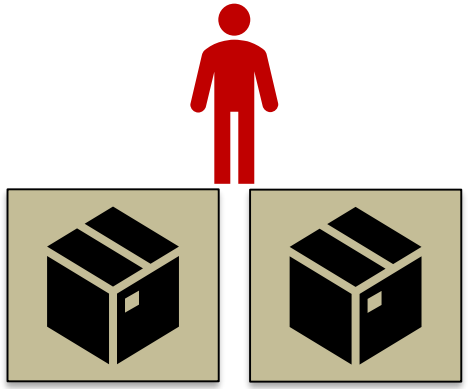

$ 10


$ 10




$ 10


What da
h…



Q: is it possible to double spend on Ethereum with network attacks?

Approaches to study …

- Goals:
  1. How the blockchain system decide a block?
  2. How the blockchain system resolve fork?

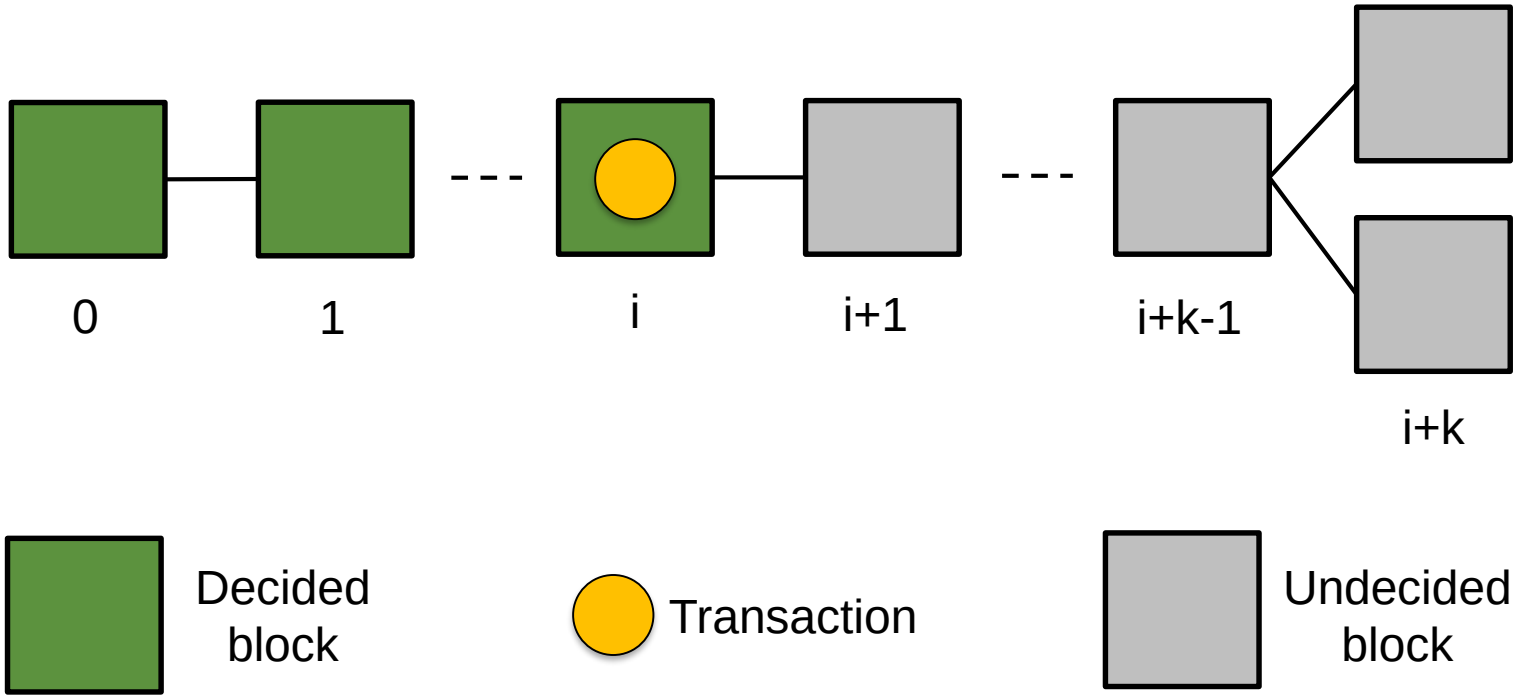
Approaches to study …

- Goals:
  1. How the blockchain system decide a block?
  2. How the blockchain system resolve fork?

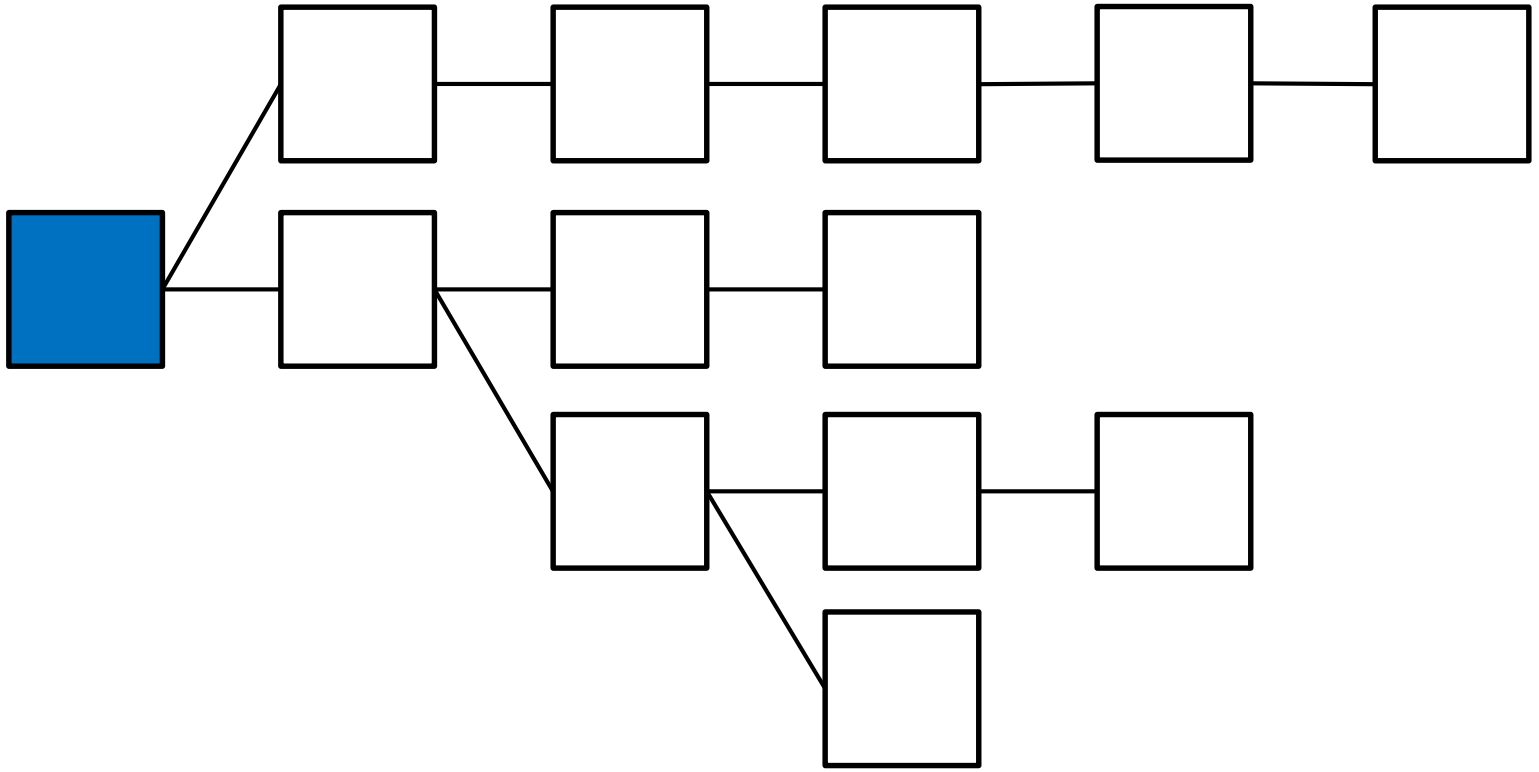
- Reading the documentation
  - Scattered and un-organised information:
    website, wiki, github, issue tracker, yellow paper ☺, etc.
  - Lack of necessary information
  - Intention ≠ Actual implementation
- Reading the code !!
- Running it for real because the devil is in the detail …

Decided Blocks and Committed Transactions in PoW/Ethereum

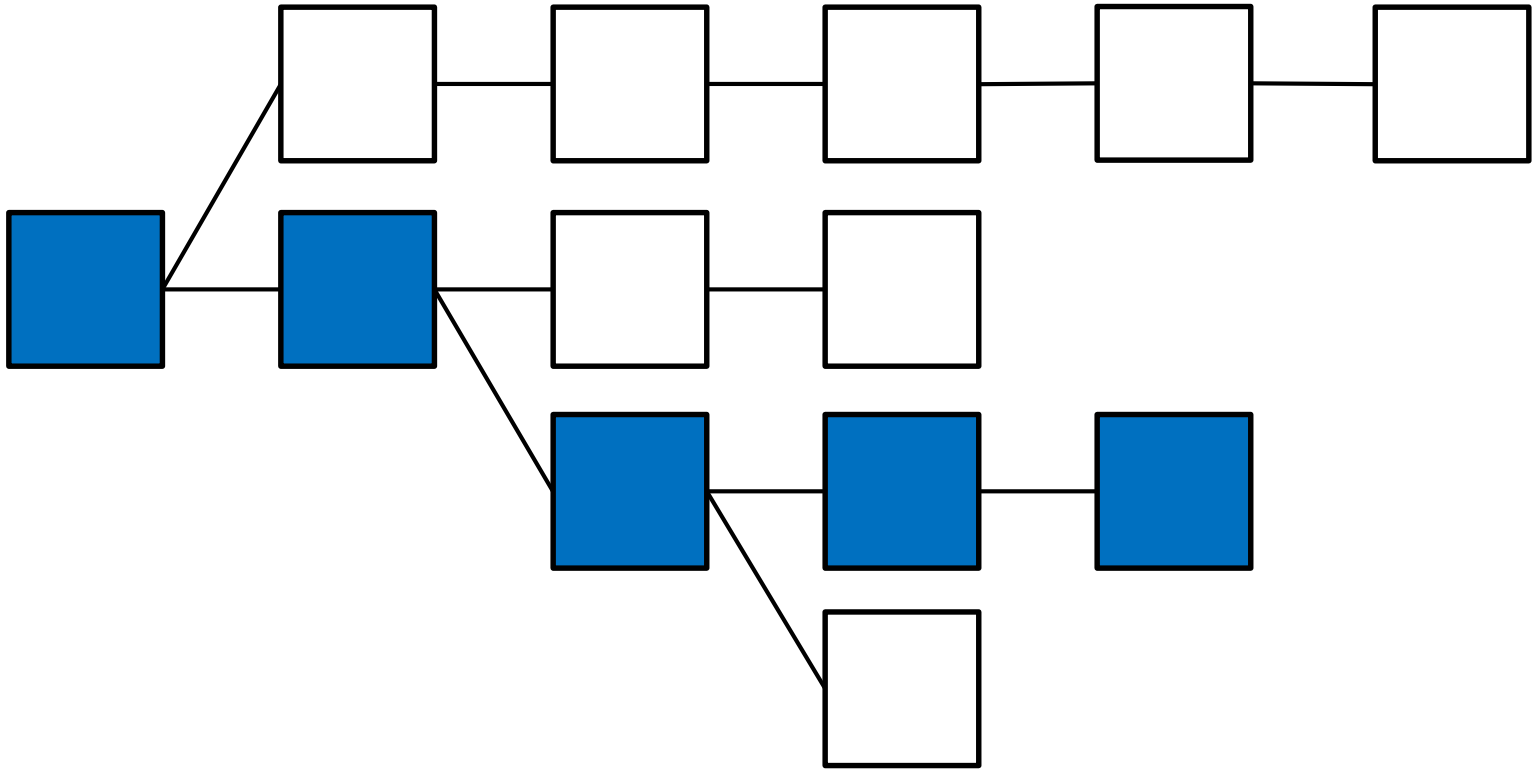
- Given a blockchain with parameter k, a block at index i is *decided* when the chain depth reaches i+k
- A transaction is *committed* if it belongs to a decided block



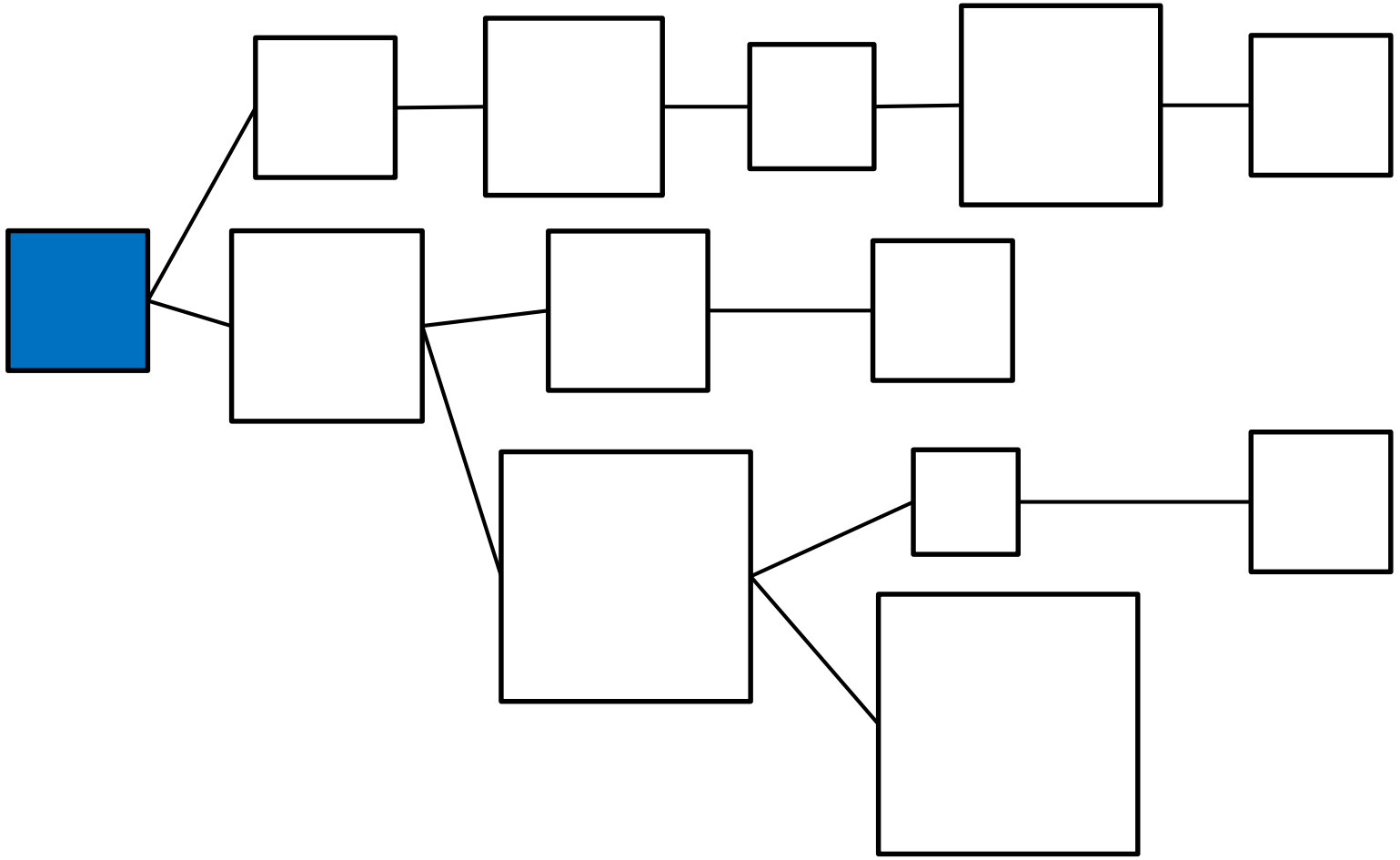
Expected Branch Selection in PoW/Ethereum: GHOST



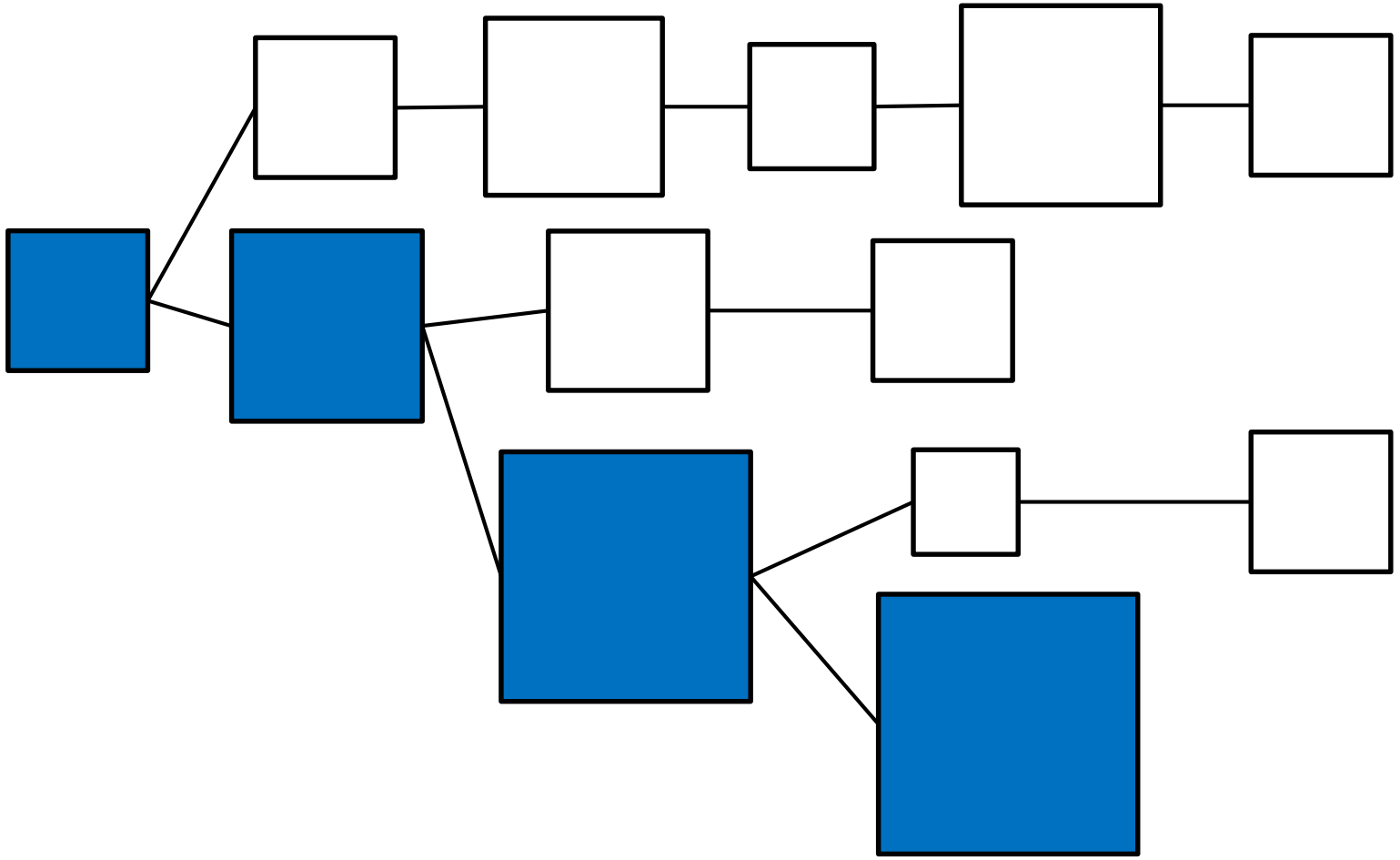
Expected Branch Selection in PoW/Ethereum: GHOST



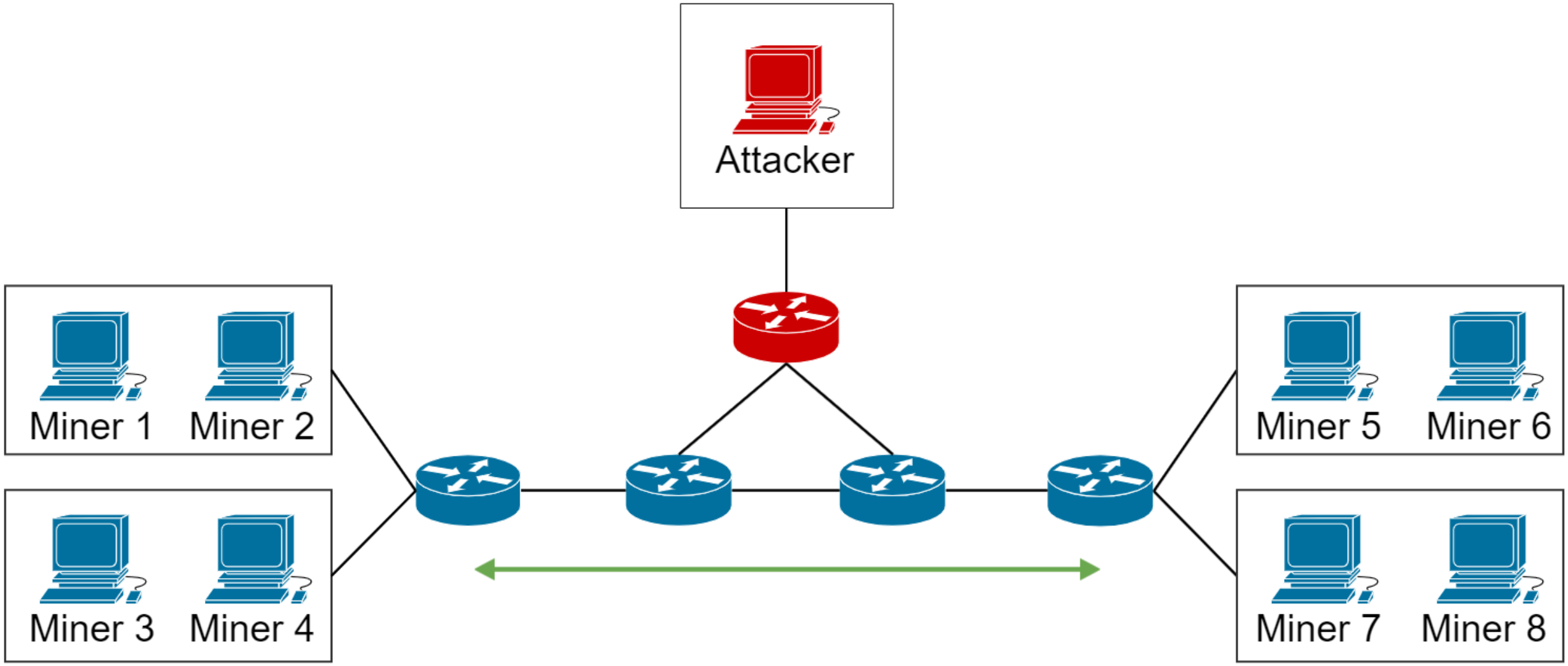
Actual Branch Selection in PoW/Ethereum: Highest total difficulty



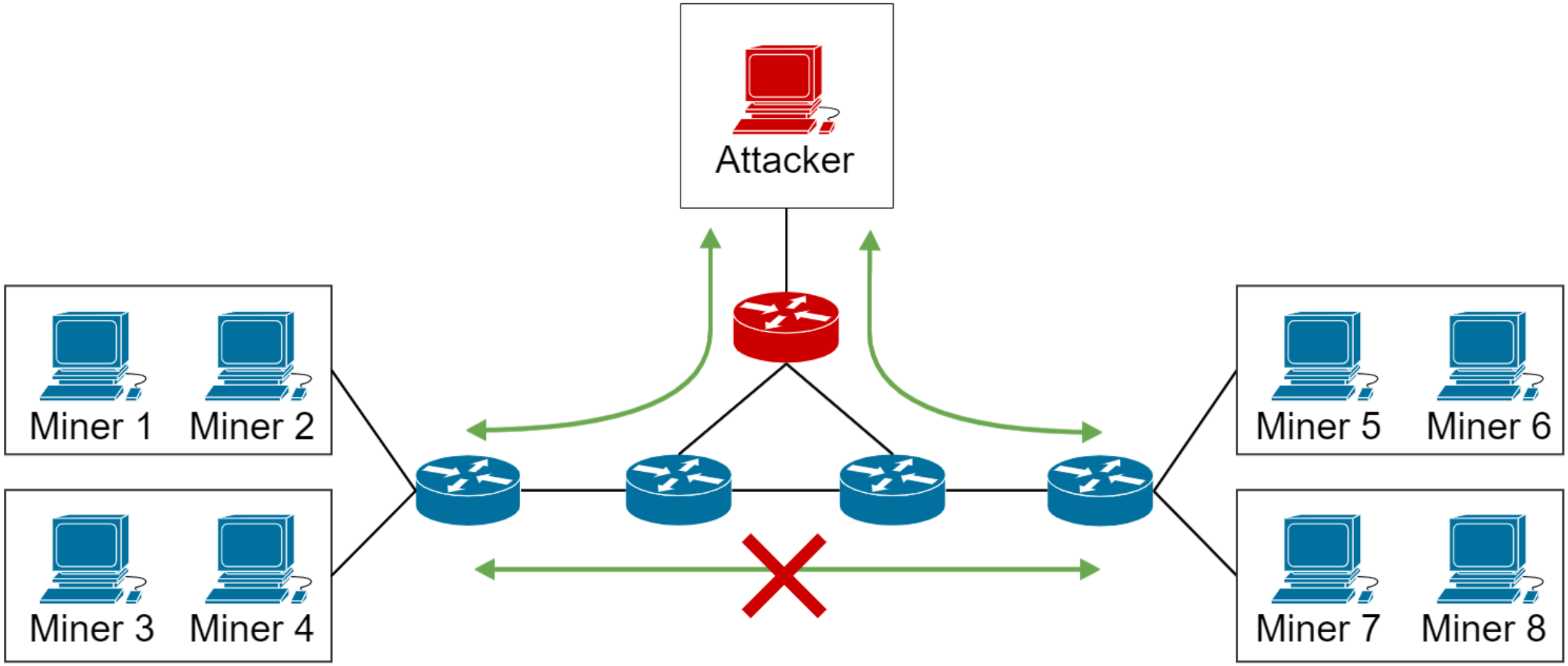
Actual Branch Selection in PoW/Ethereum: Highest total difficulty



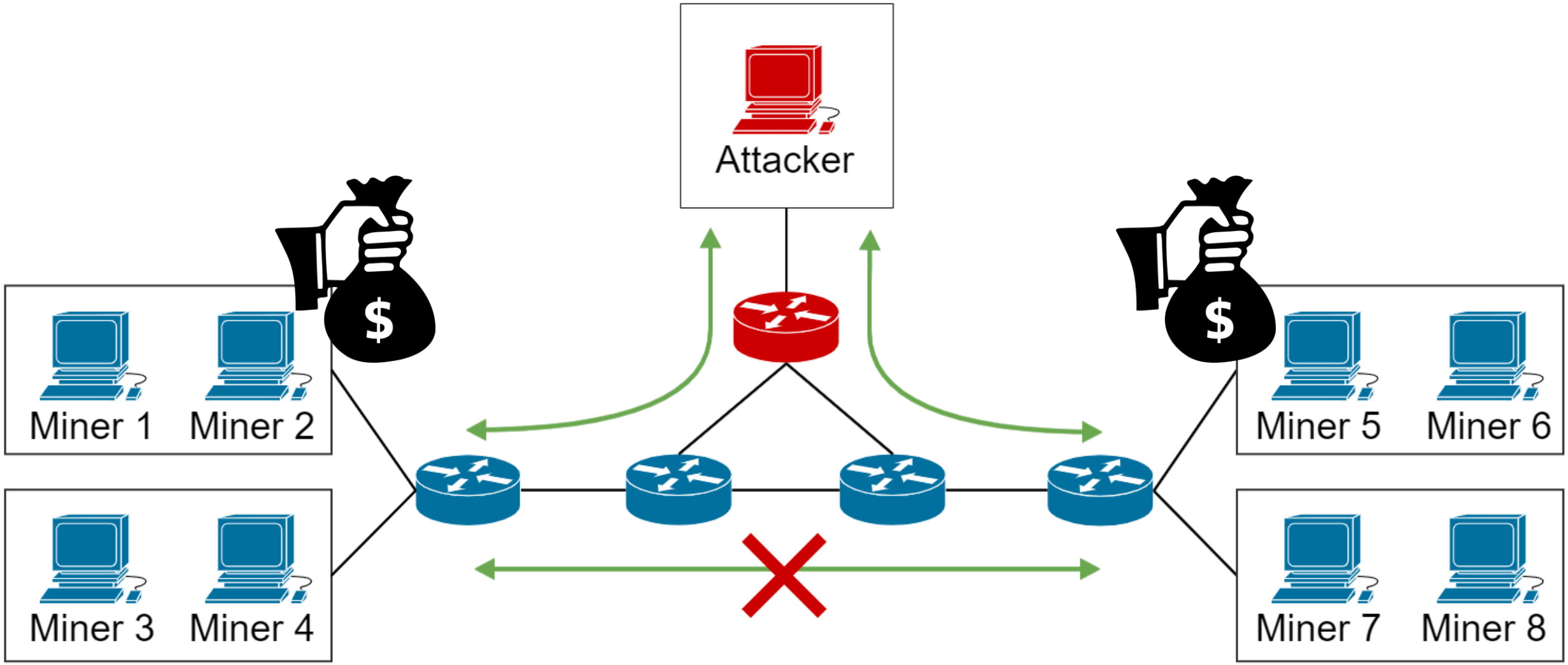
Example 1: Man-in-the-middle Attack aaainst PoW



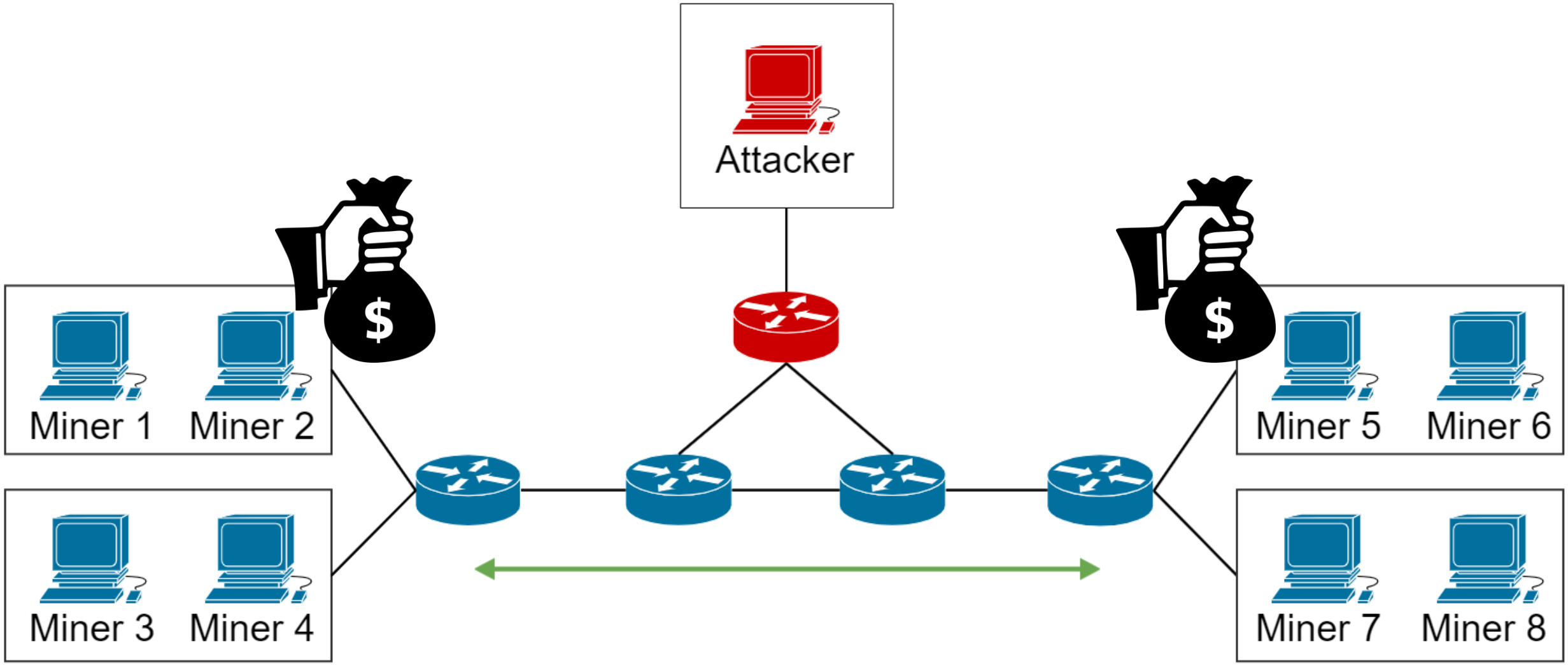
Example 1: Man-in-the-middle Attack aaainst PoW



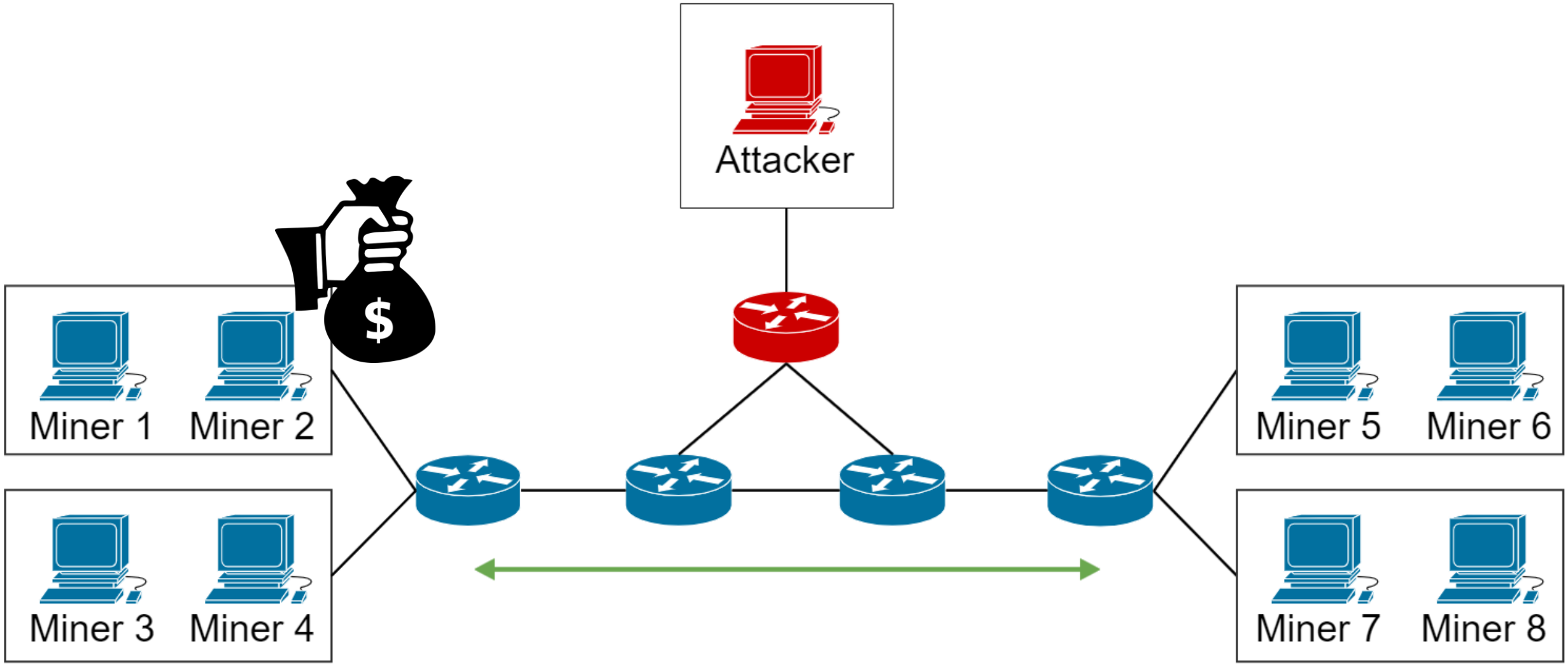
Example 1: Man-in-the-middle Attack aaainst PoW



Example 1: Man-in-the-middle Attack aaainst PoW

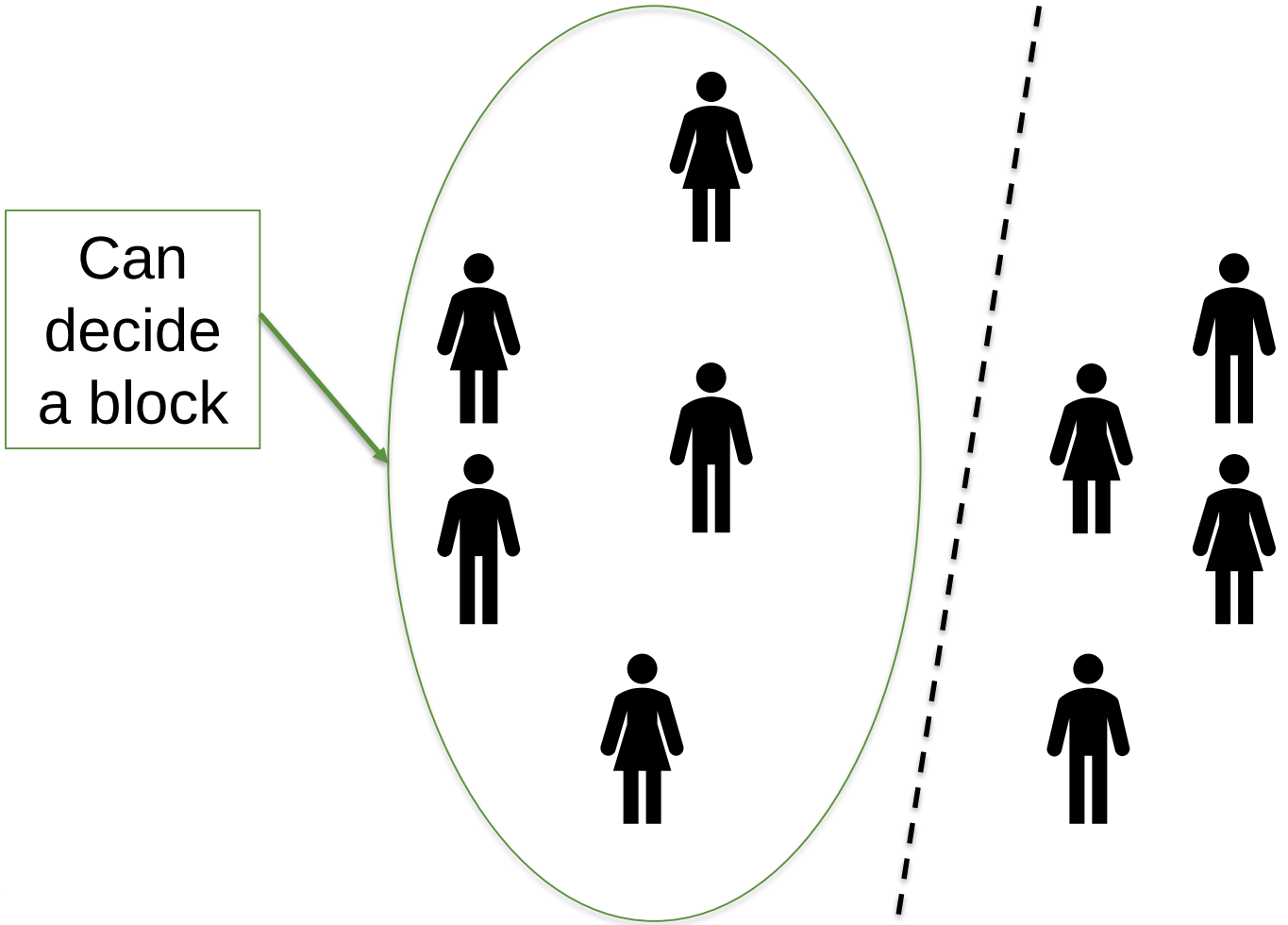


Example 1: Man-in-the-middle Attack aaainst PoW

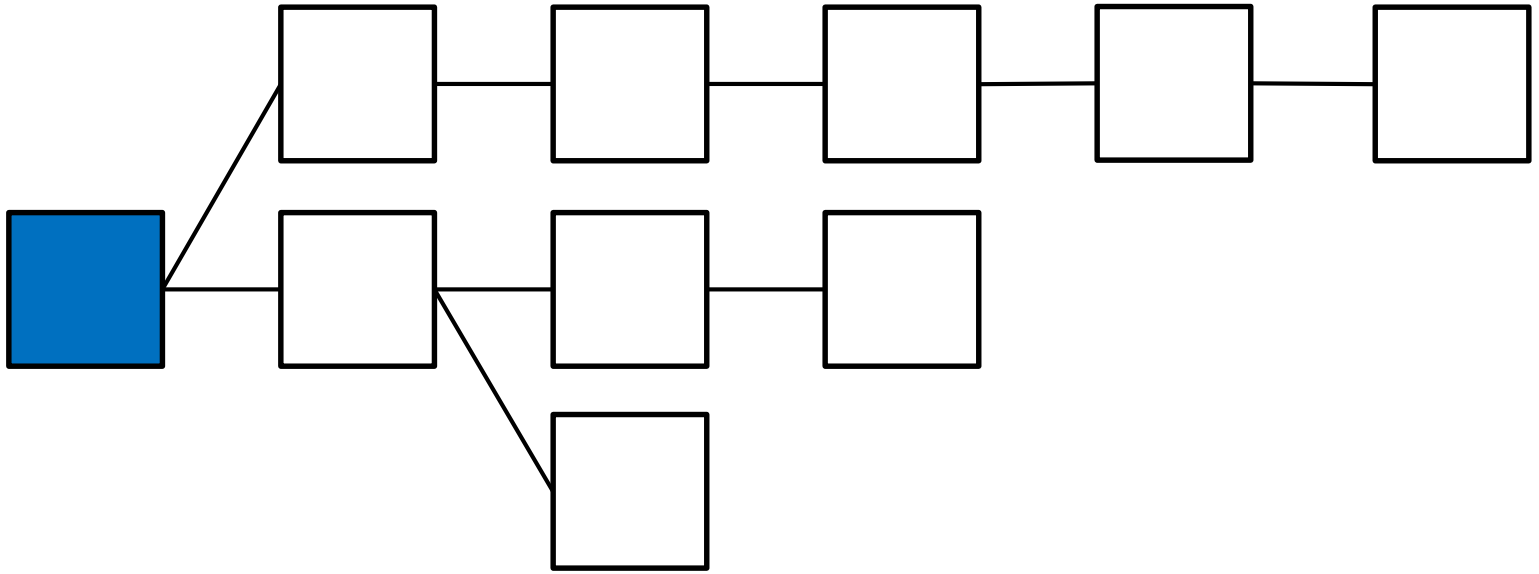


Decided Blocks and Committed Transactions in AuRa PoA/Ethereum

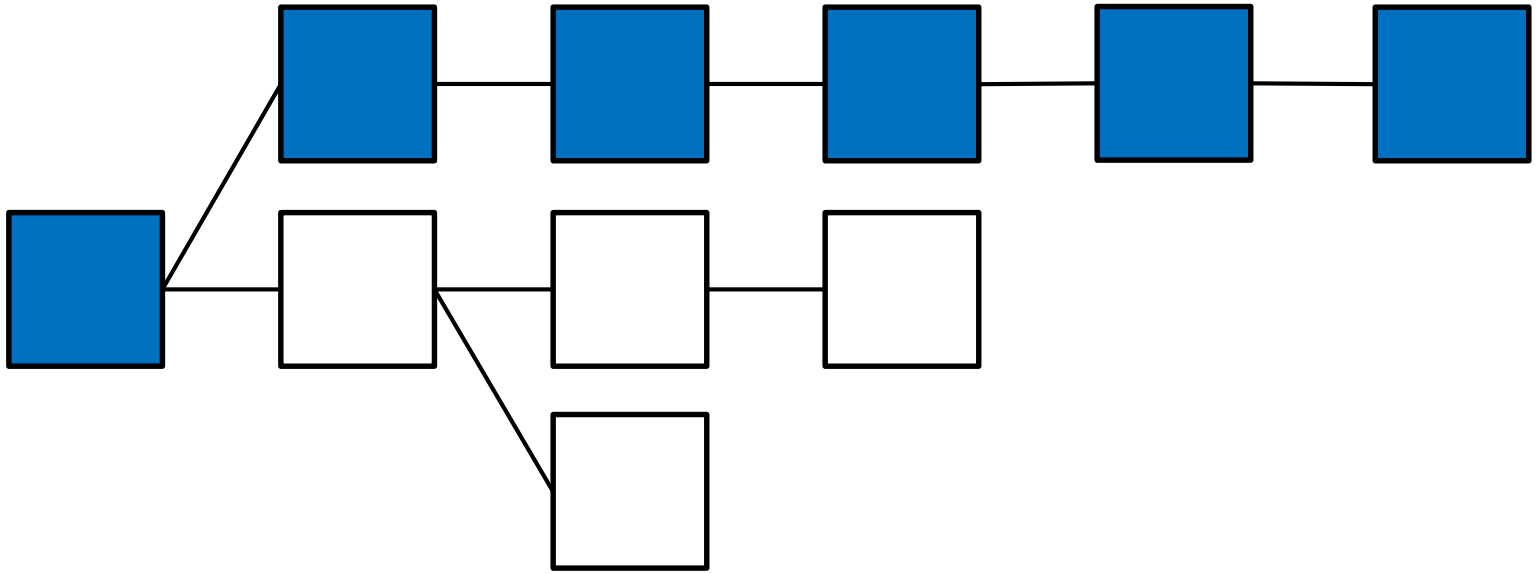
– A decision requires strictly more than half, only one partition may decide blocks



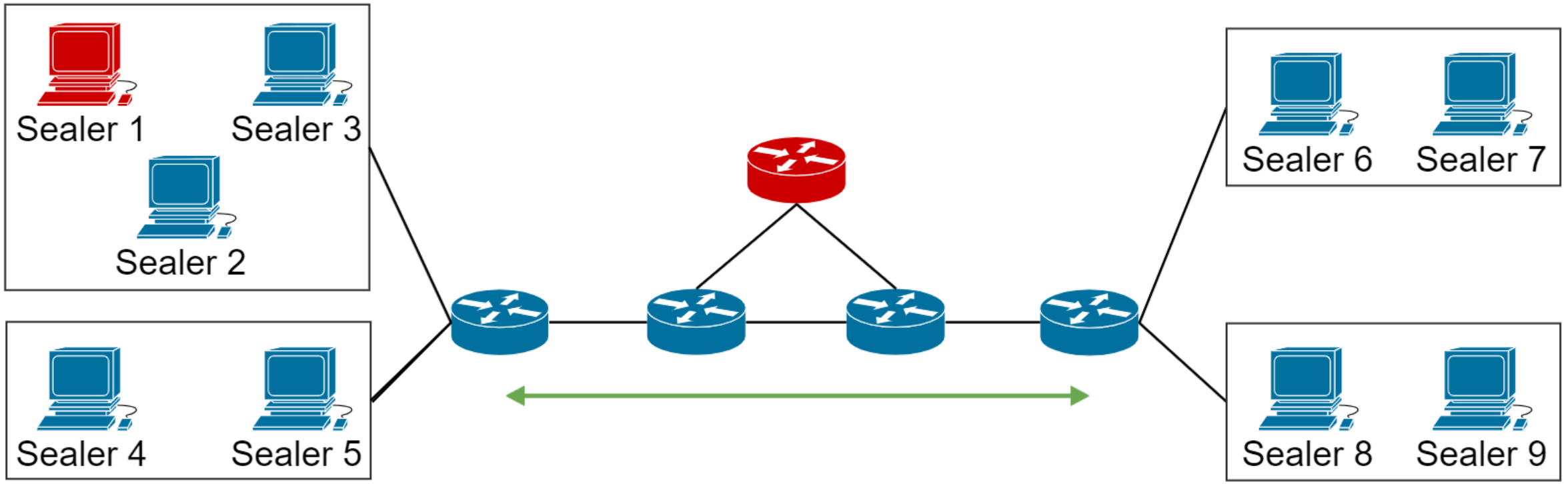
Branch Selection in AuRa PoA/Ethereum : Longest branch



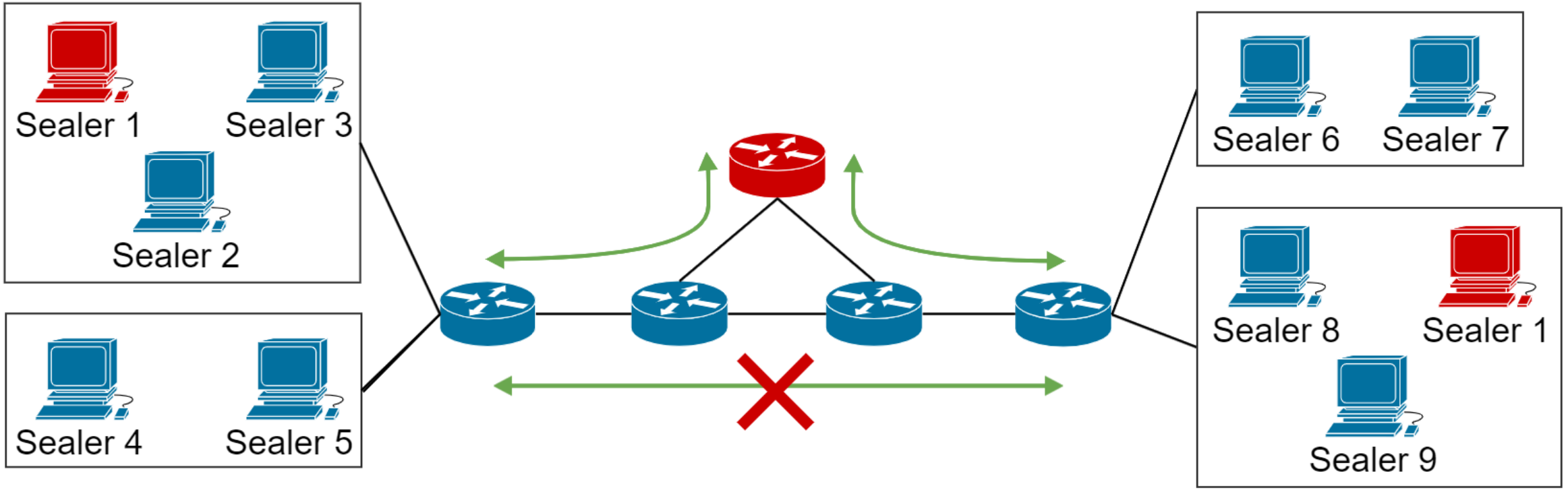
Branch Selection in AuRa PoA/Ethereum : Longest branch



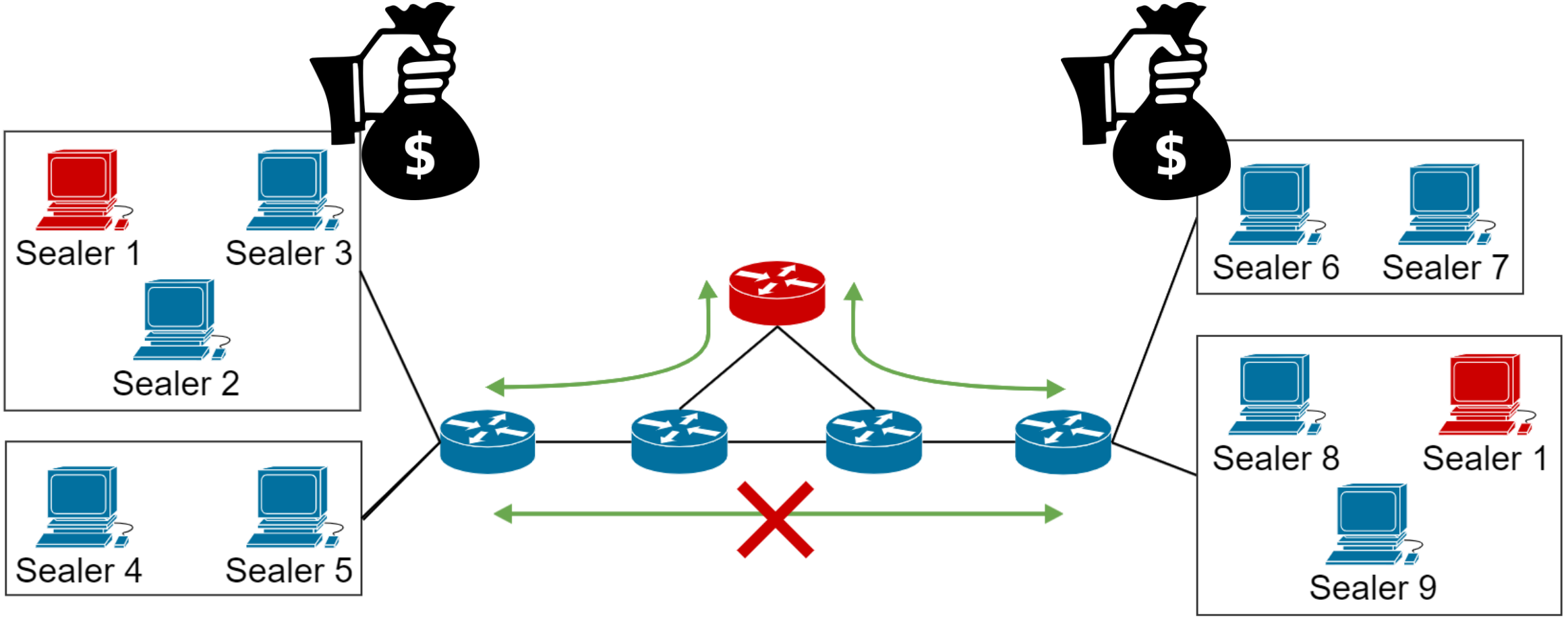
Example 2: The Cloning Attack against PoA



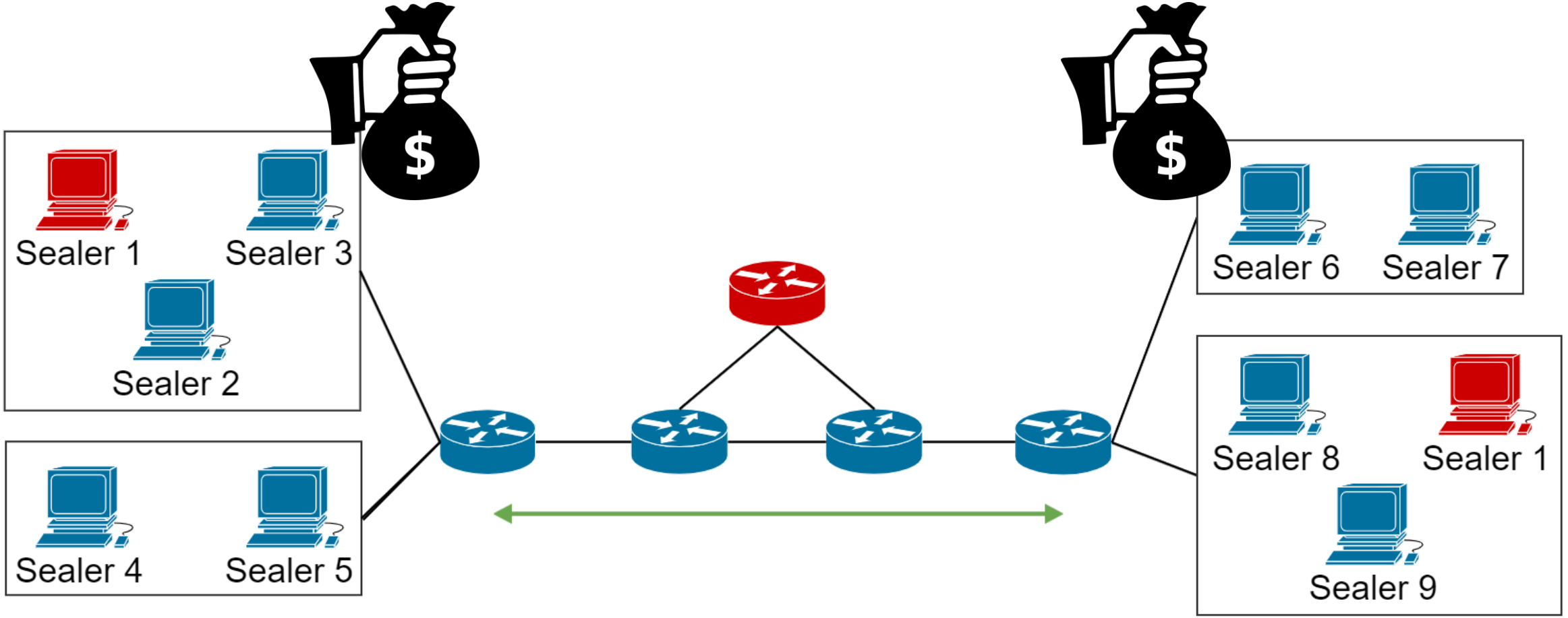
Example 2: The Cloning Attack against PoA



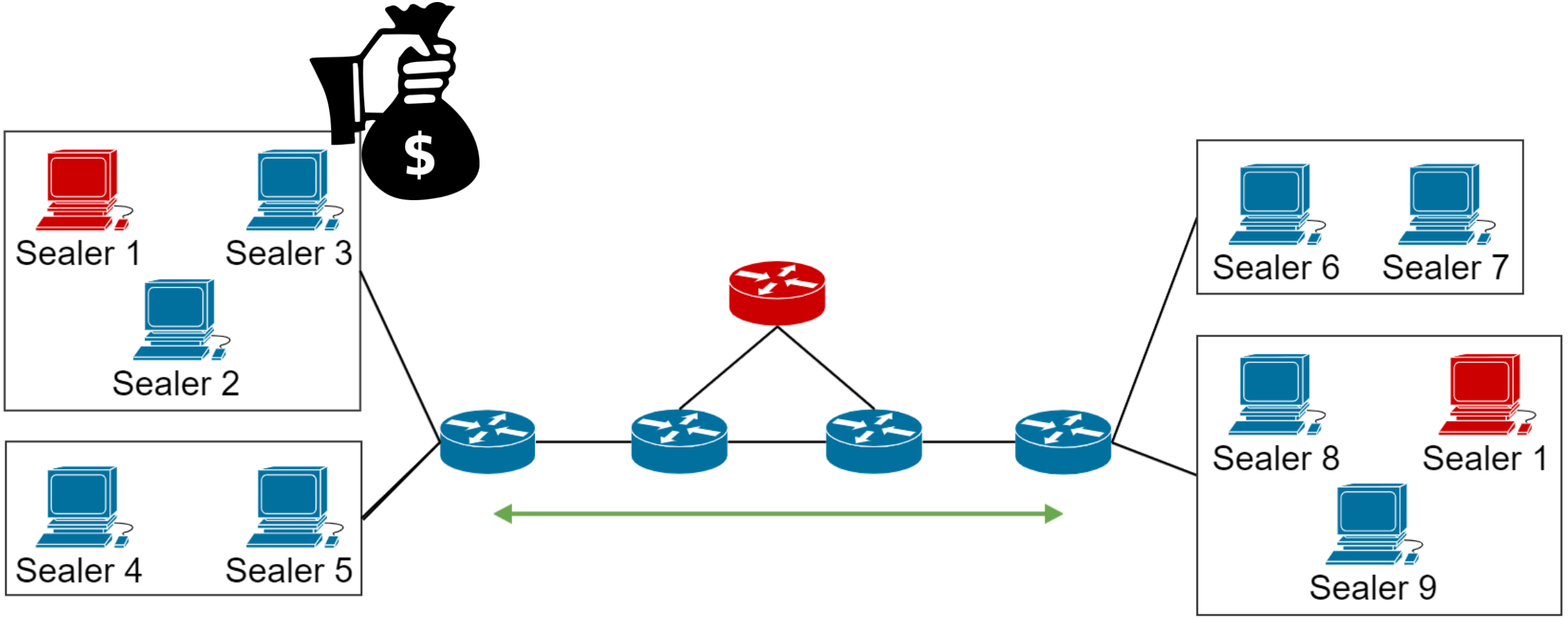
Example 2: The Cloning Attack against PoA



Example 2: The Cloning Attack against PoA



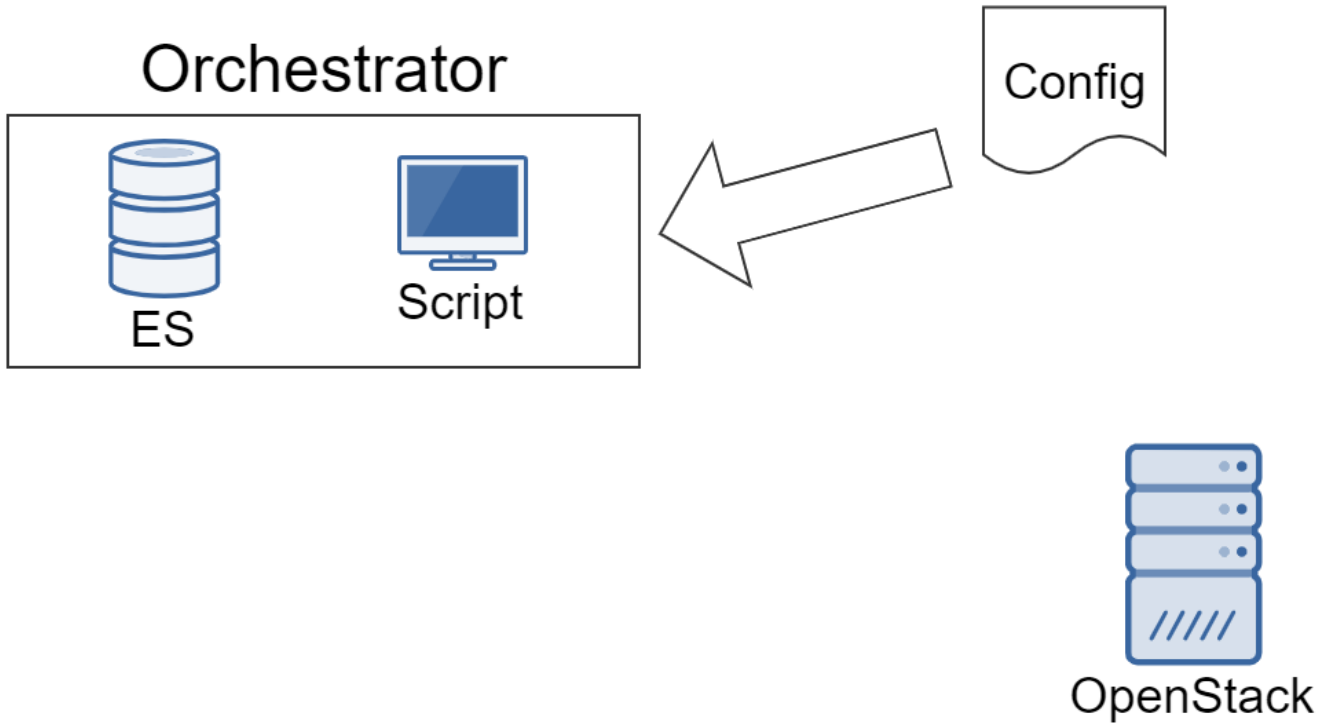
Example 2: The Cloning Attack against PoA



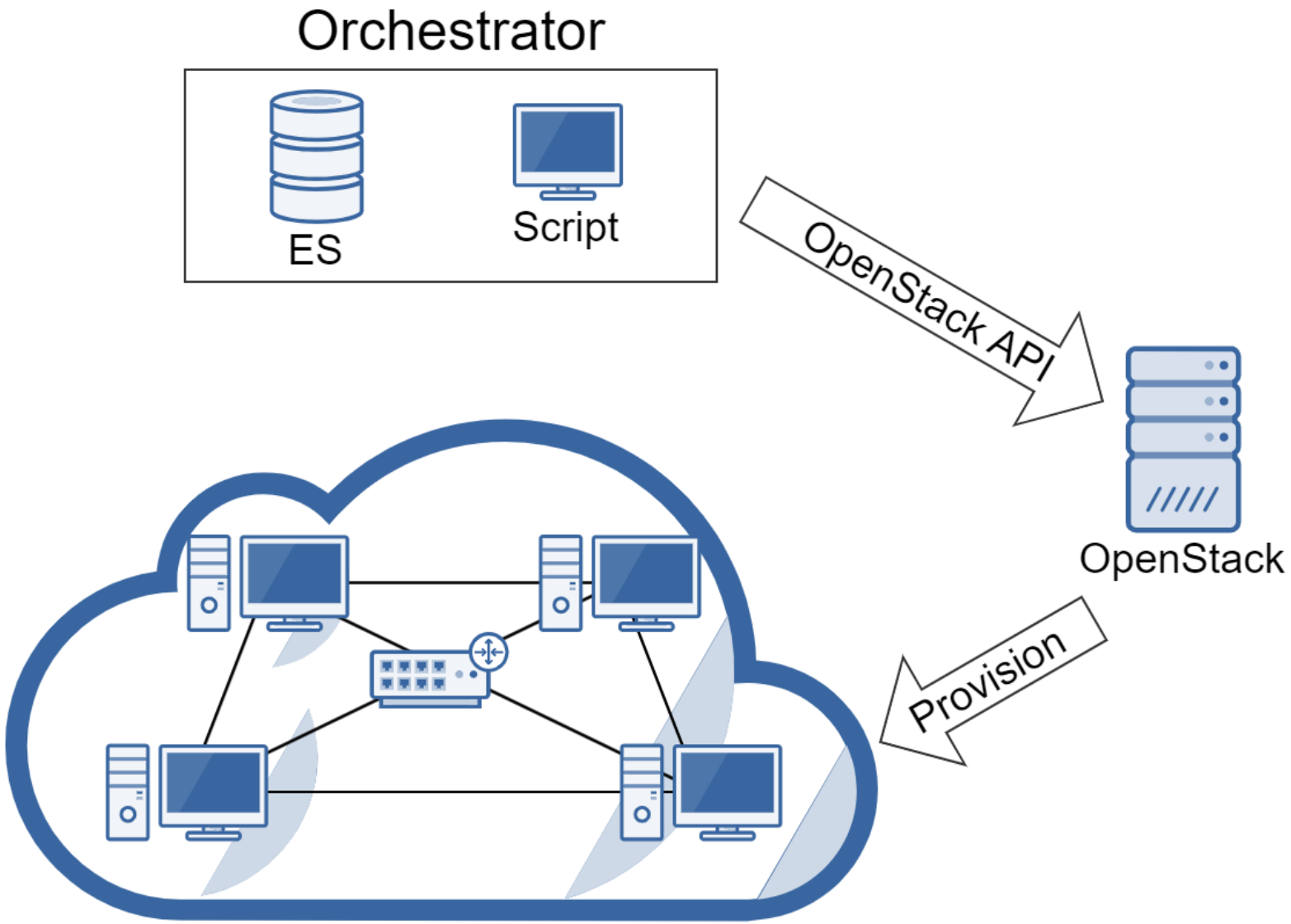
The requirements for the experiments

– Control over computing resources	➢ OpenStack Private Cloud
– Network control and isolation	➢ Virtual switches, Virtual routers (Quagga) and VLAN
– Highly automated	➢ OpenStack API and Ethereum API
– Robust data collection	➢ Elasticsearch

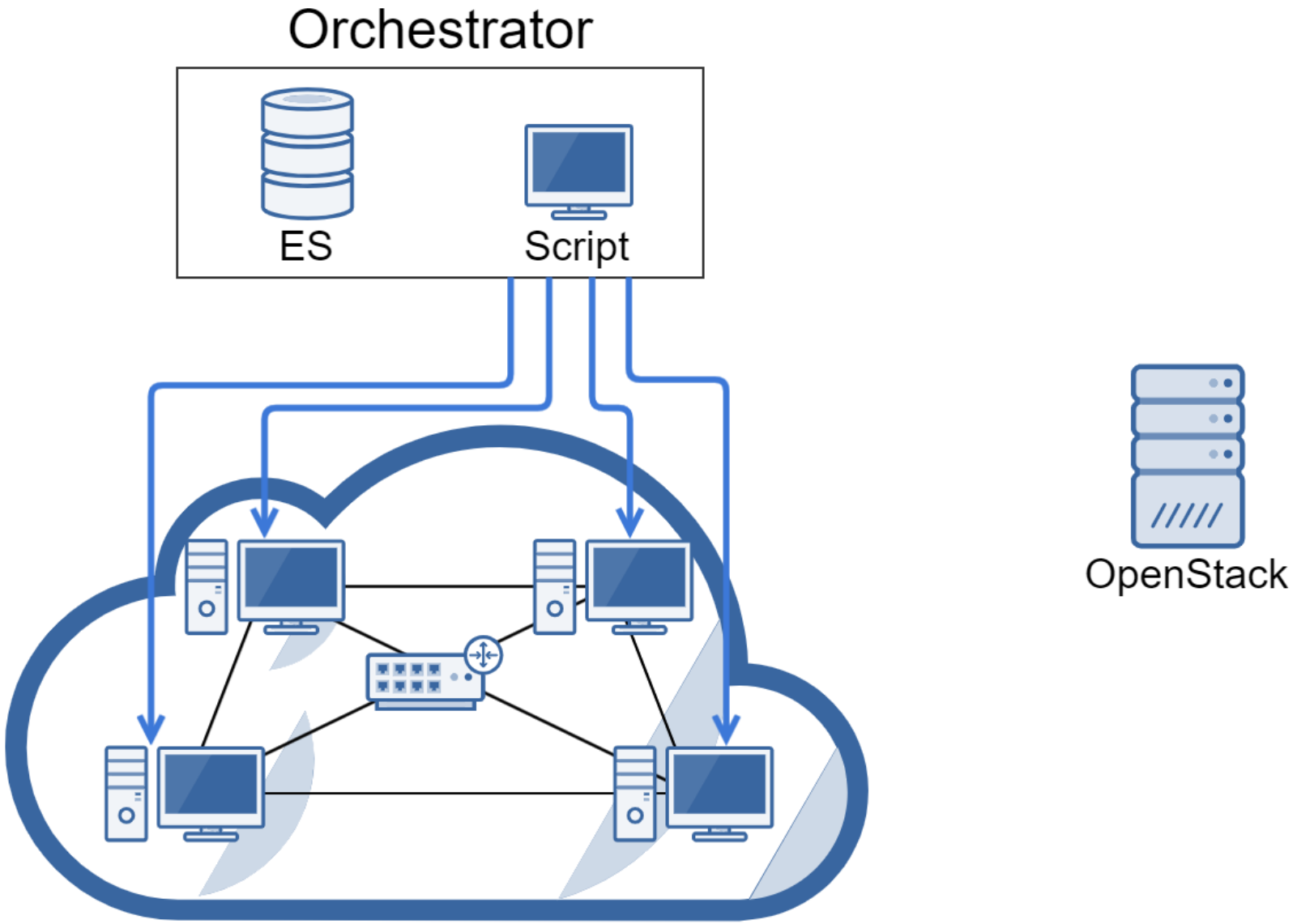
Testbed Provisioning



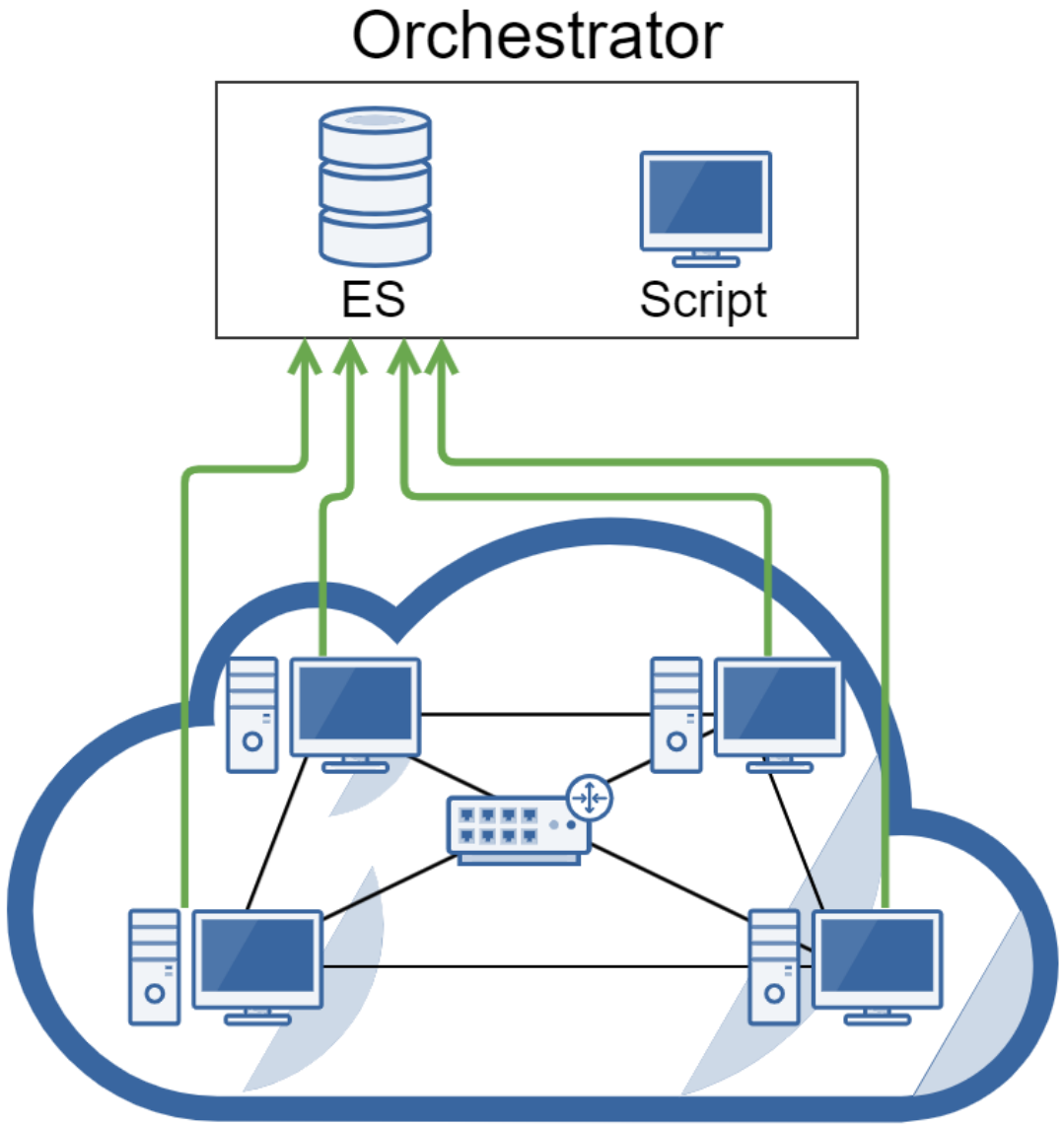
Testbed Provisioning



Testbed Provisioning



Testbed Provisioning



Time for Discussions !!

THE UNIVERSITY OF SYDNEY