

# Deanonymizing Ethereum Validators: The P2P Network Has a Privacy Issue

Yann Vonlanthen • ETH Zürich

# Deanonymizing Ethereum Validators: The P2P Network Has a Privacy Issue

Yann Vonlanthen • ETH Zürich



**Lioba Heimbach**  
ETH Zurich



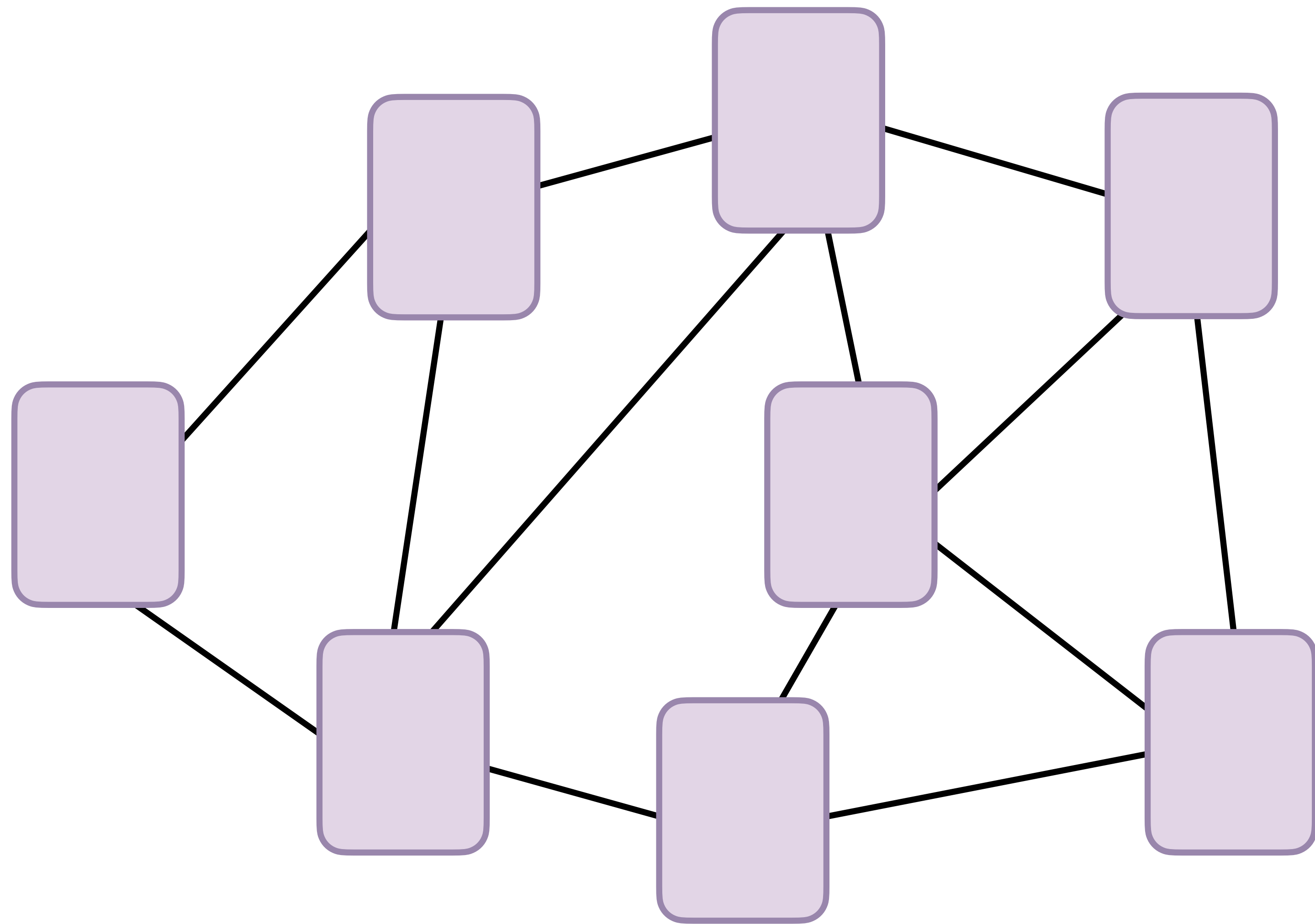
**Juan Villacis**  
University of Bern

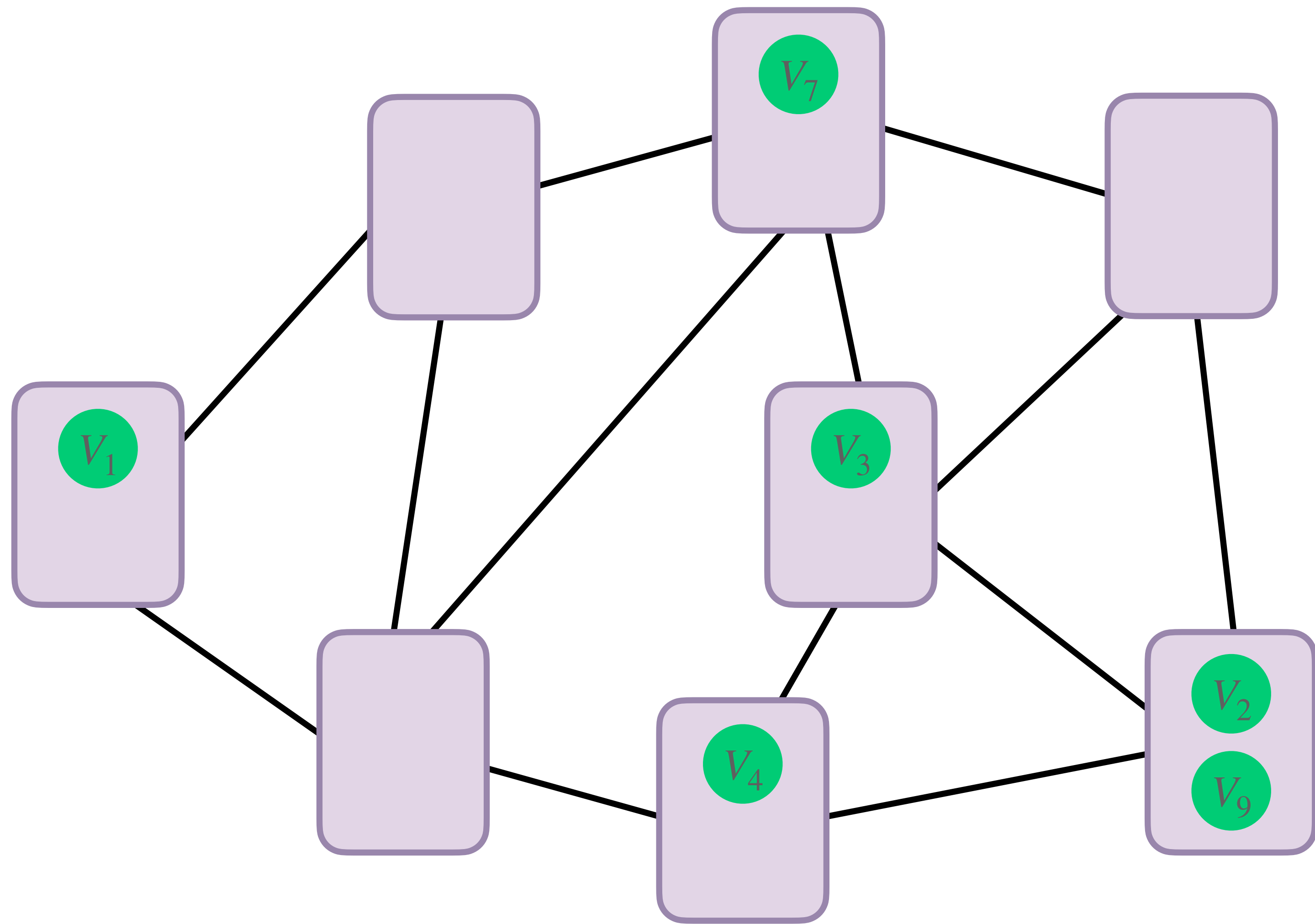


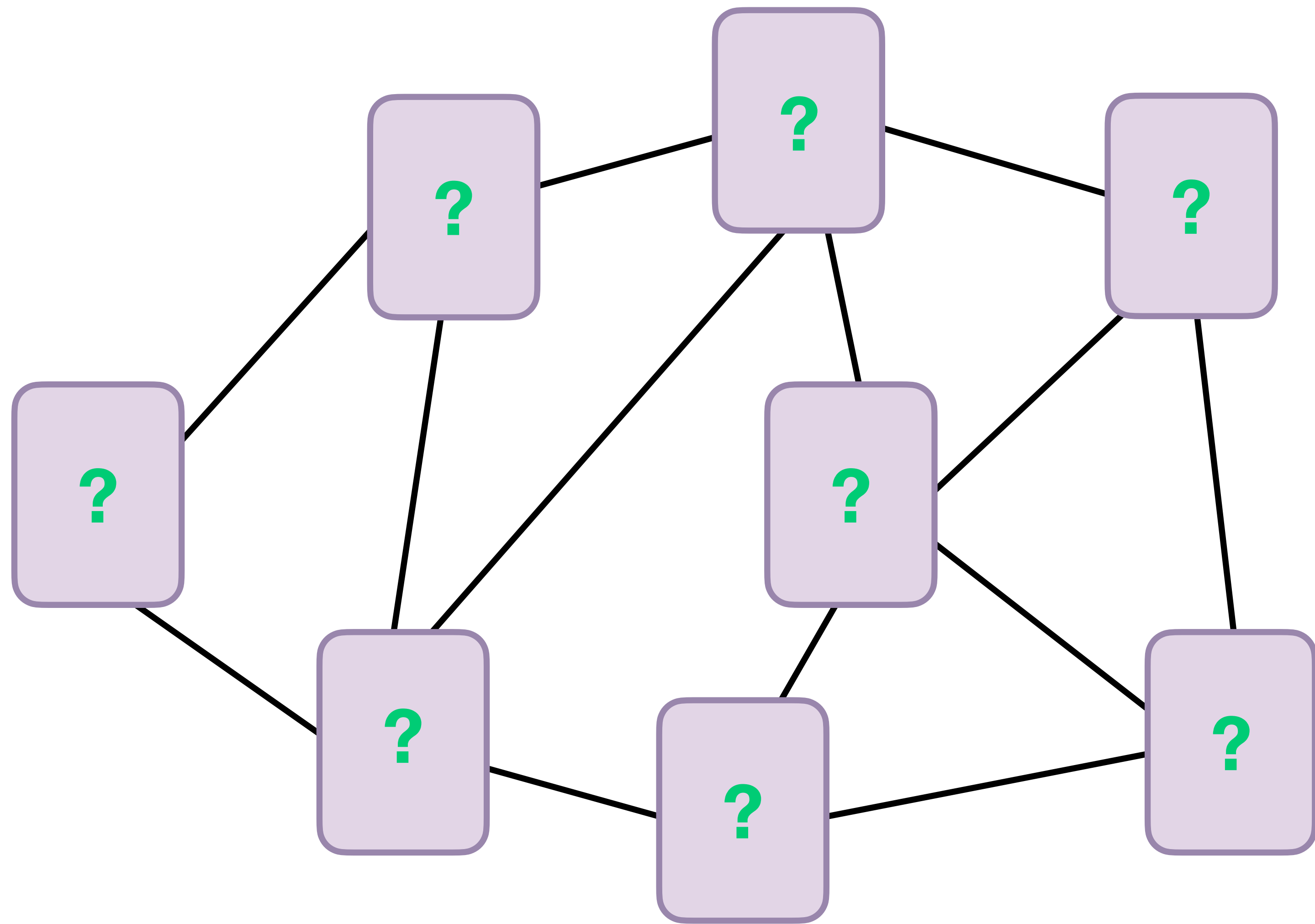
**Dr. Lucianna Kiffer**  
IMDEA Networks



**Prof. Roger Wattenhofer**  
ETH Zurich

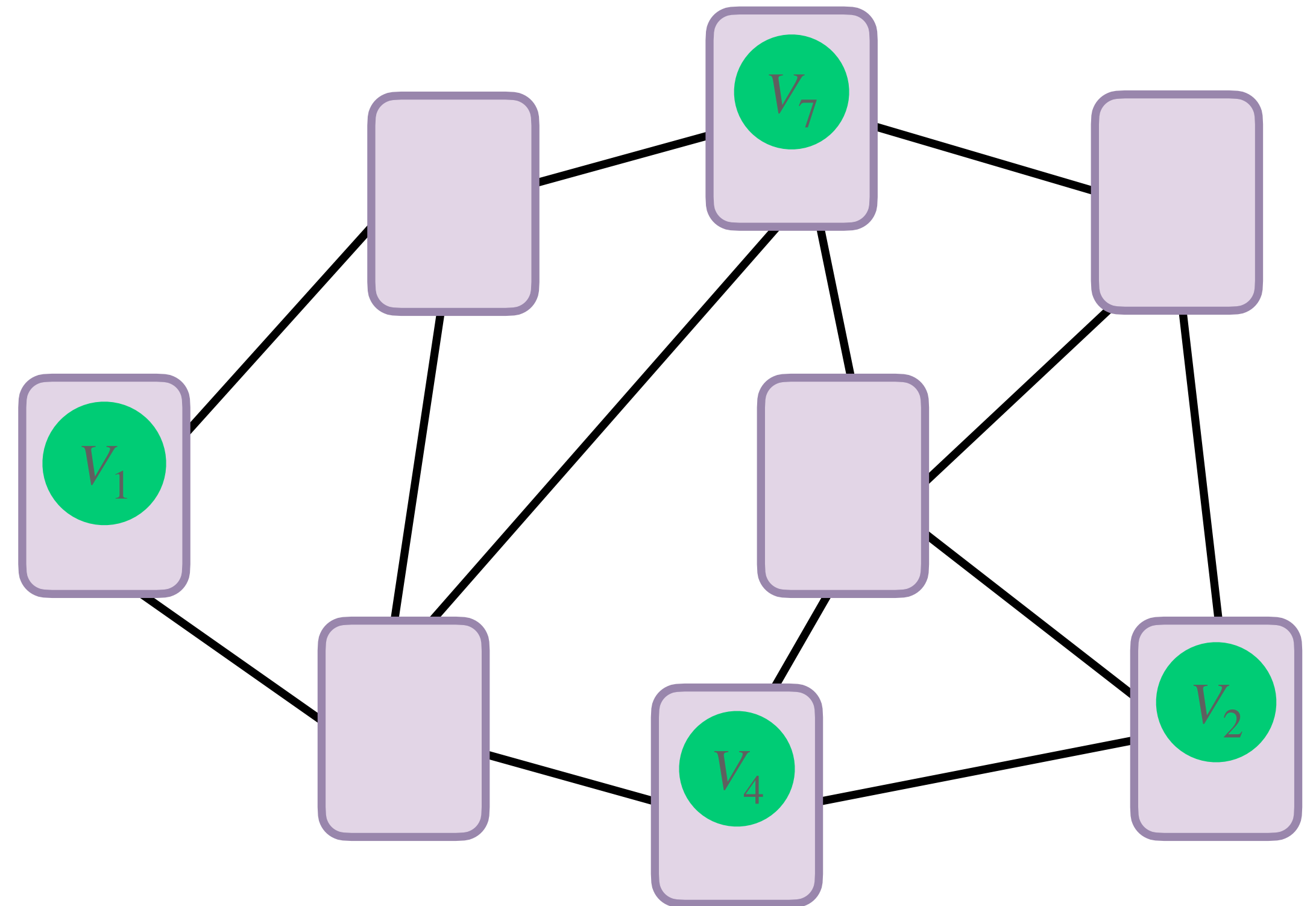
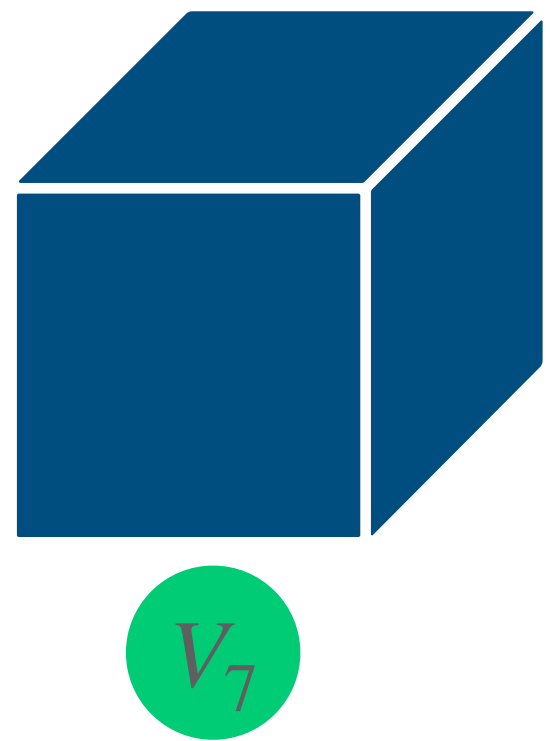




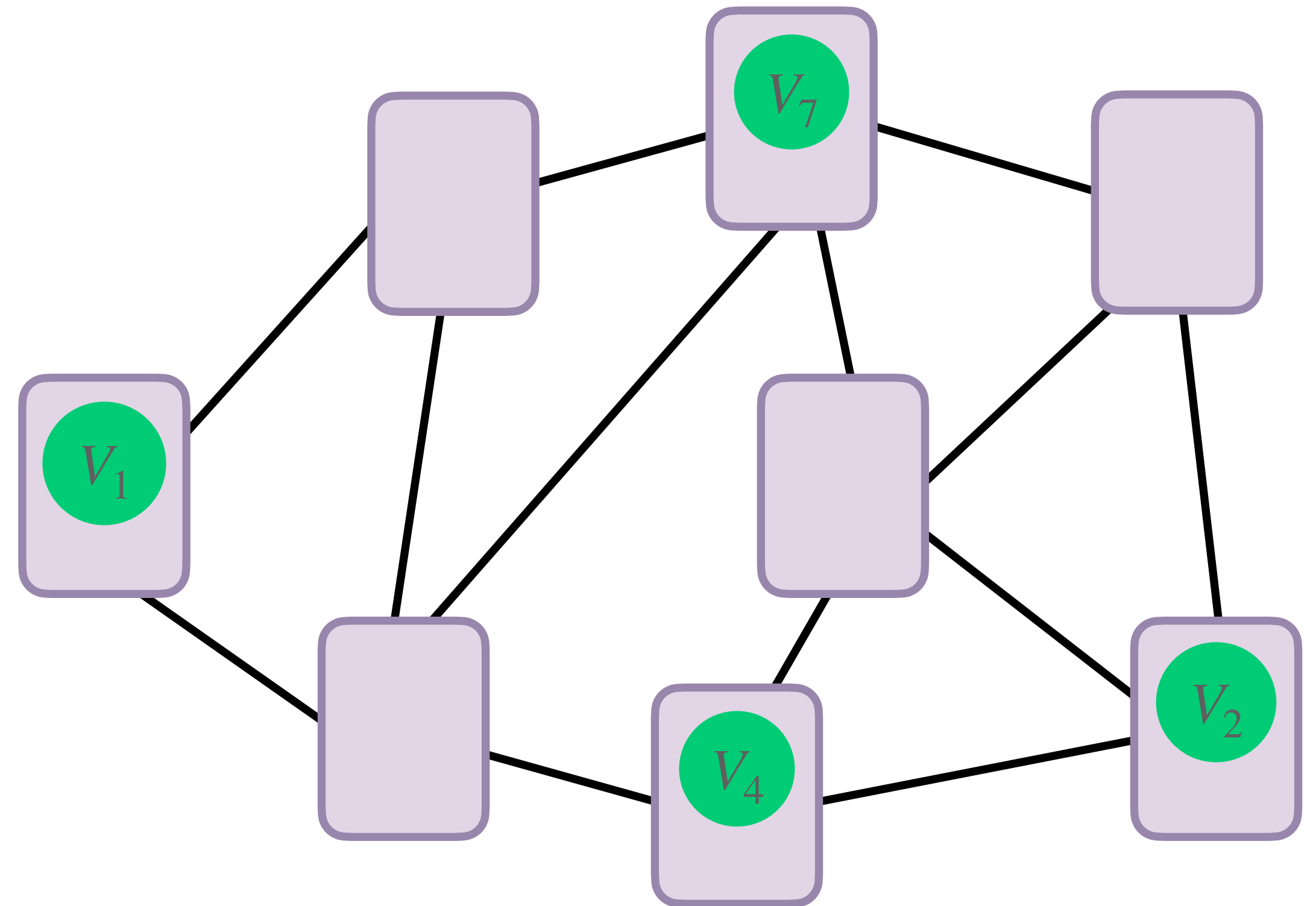
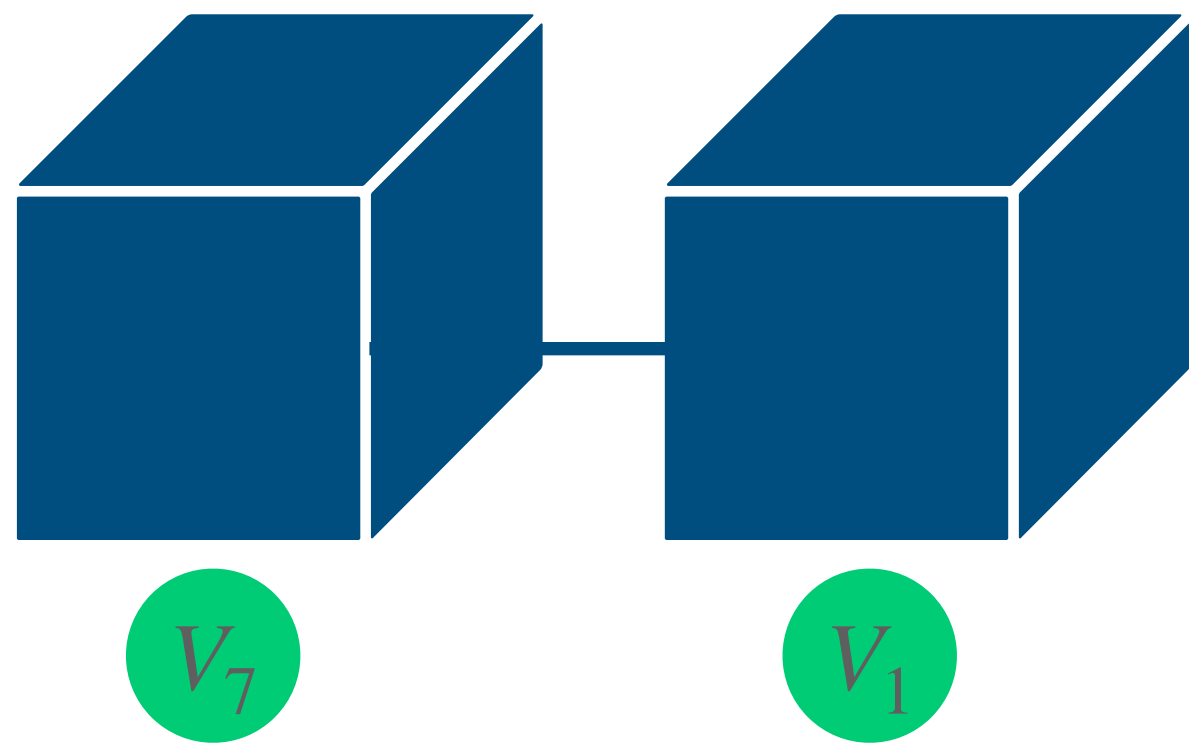


**Why does anonymity matter?**

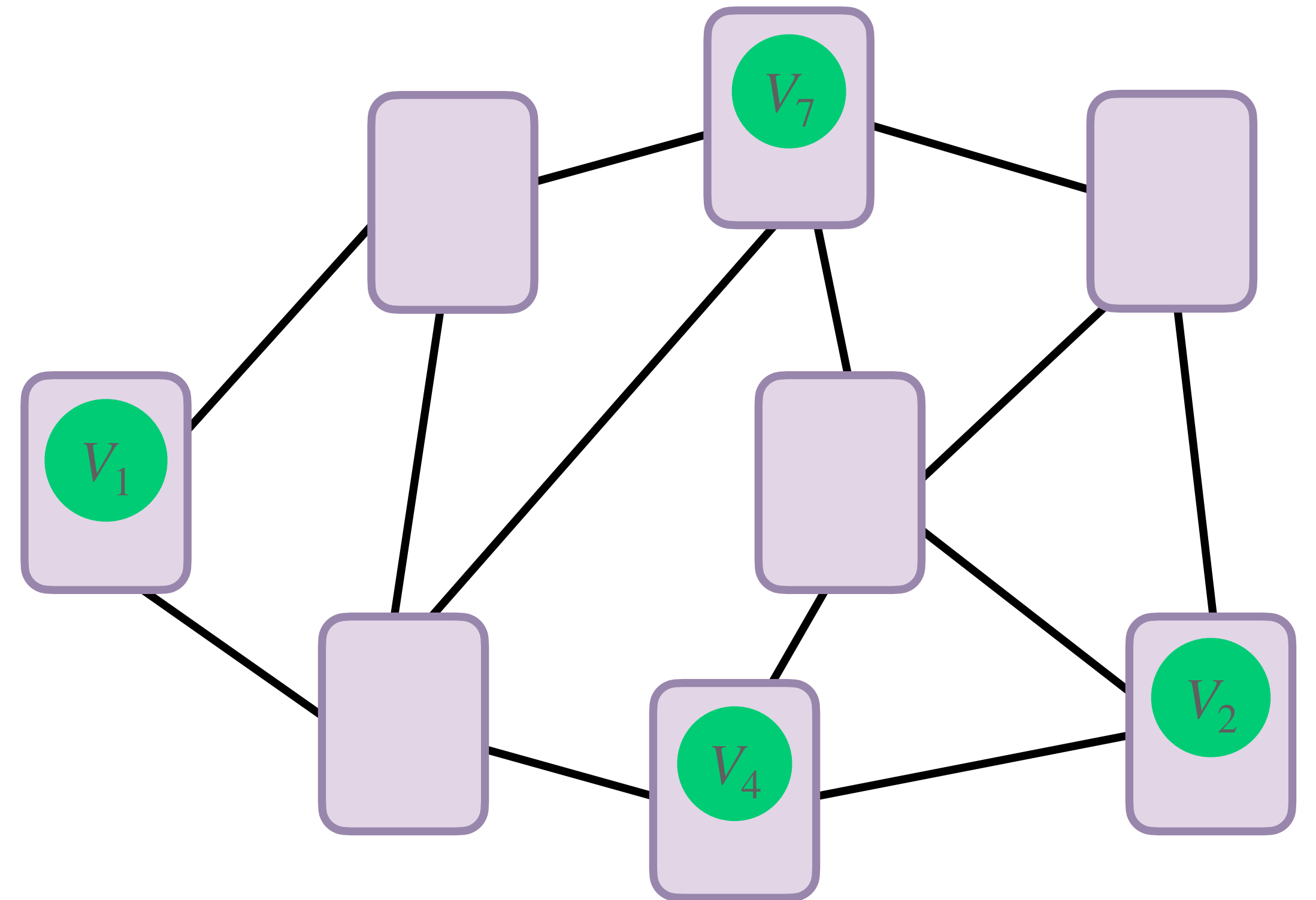
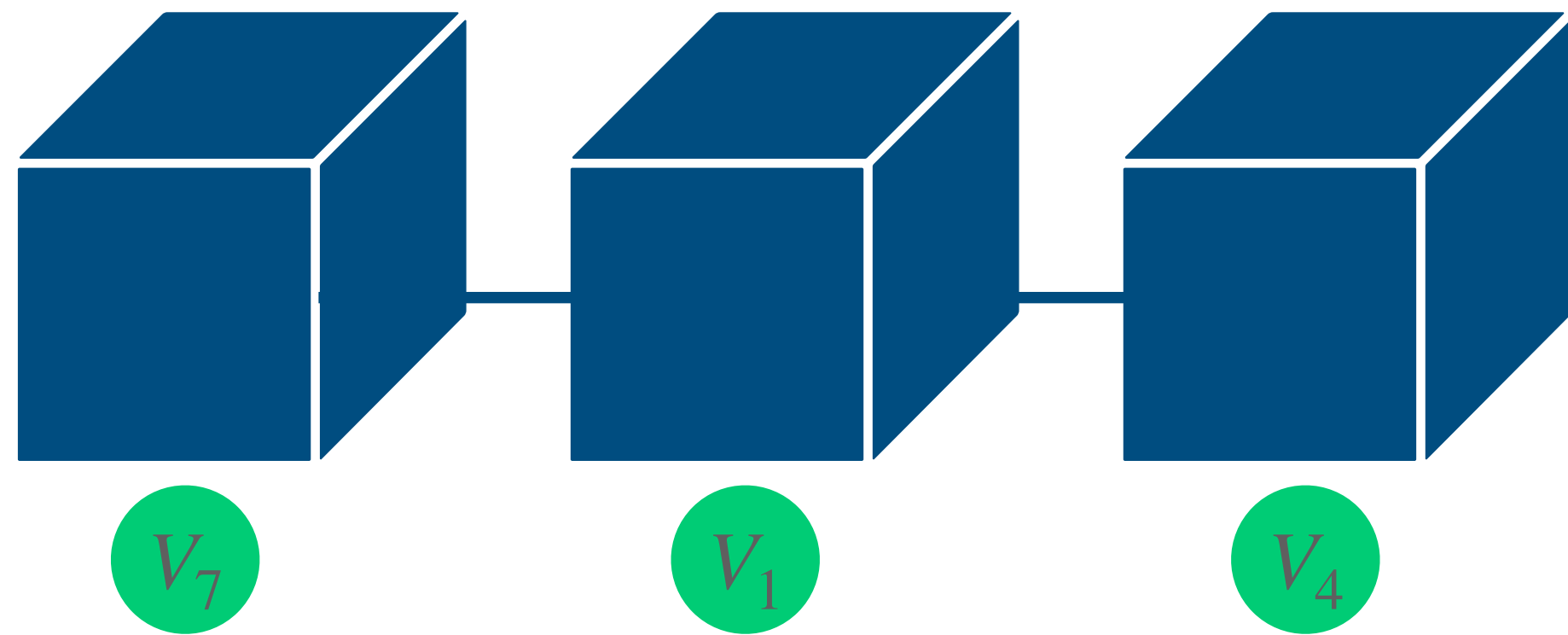
# Why does anonymity matter?



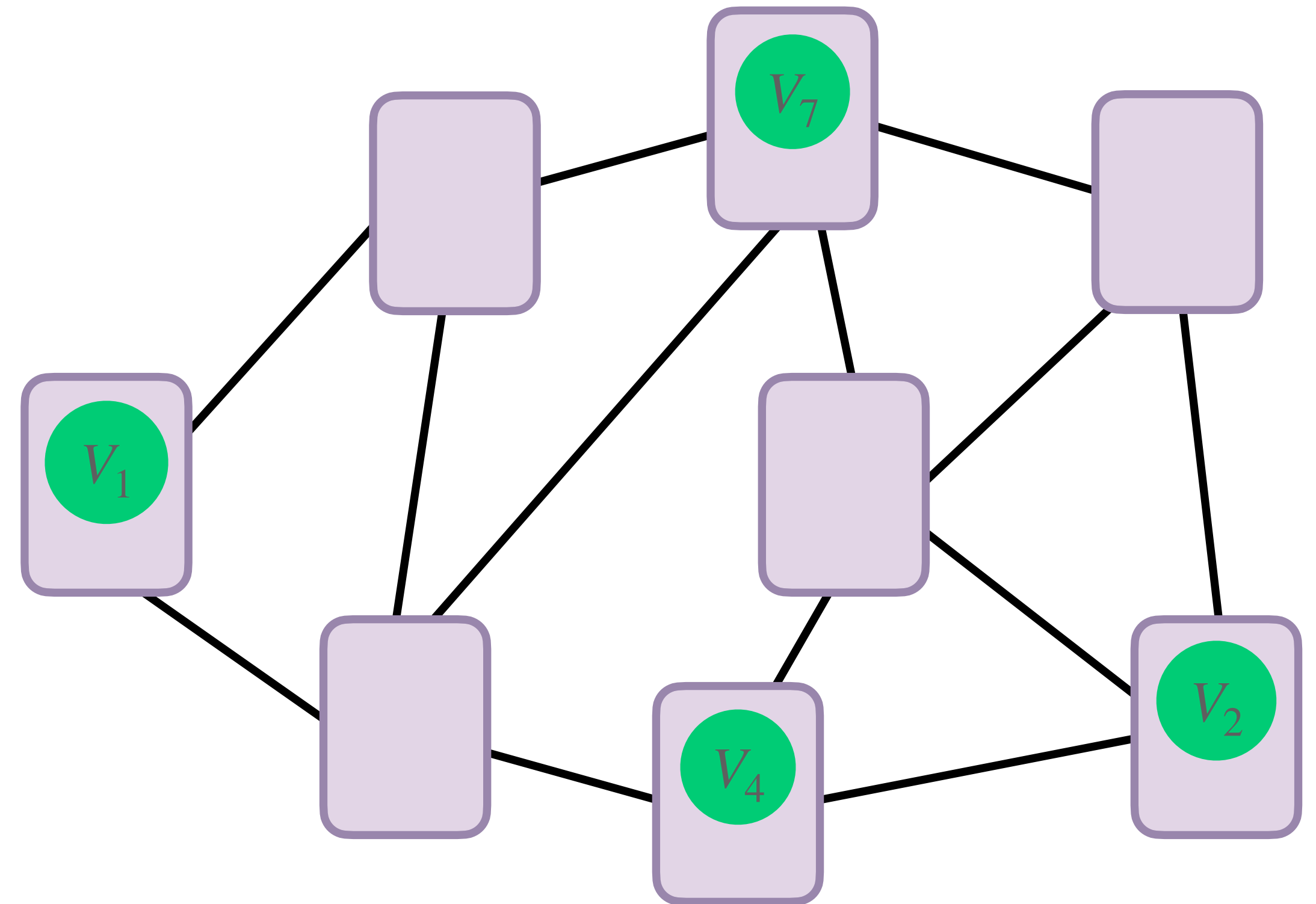
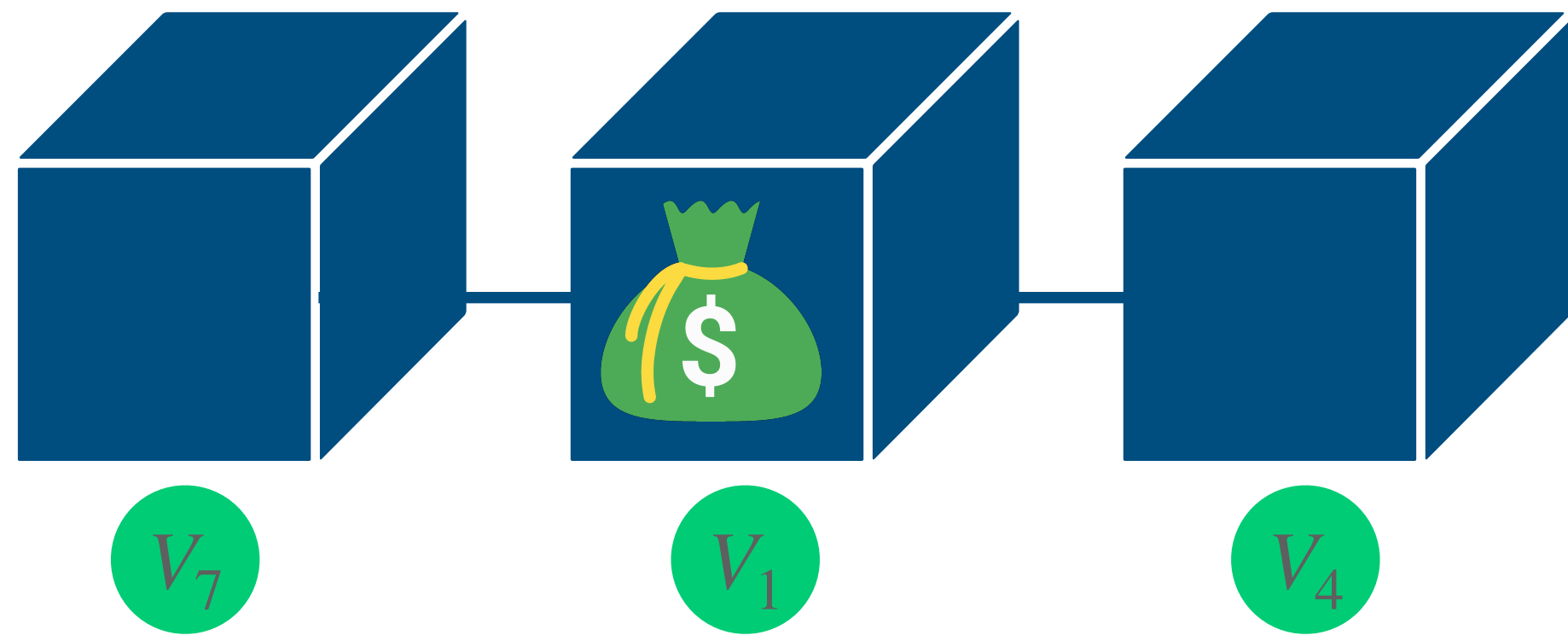
# Why does anonymity matter?



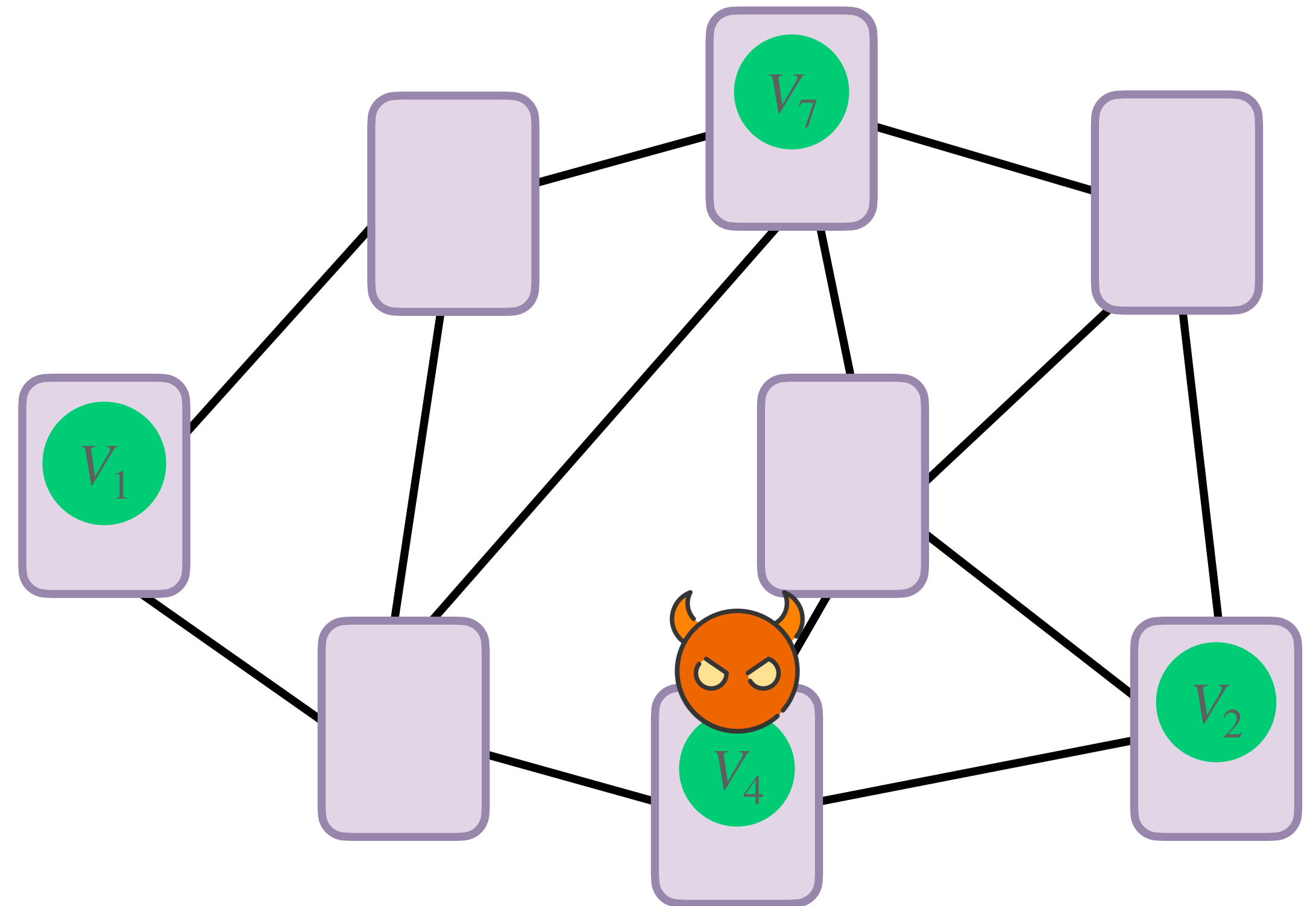
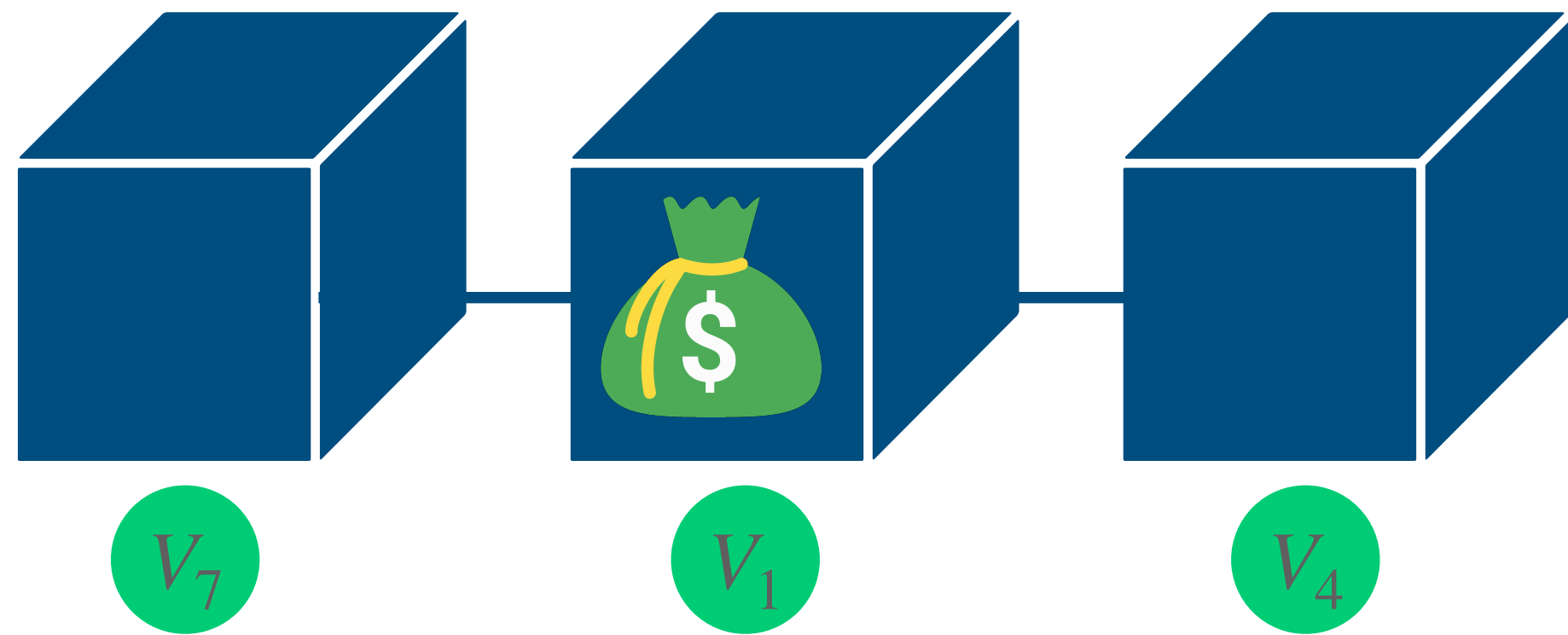
# Why does anonymity matter?



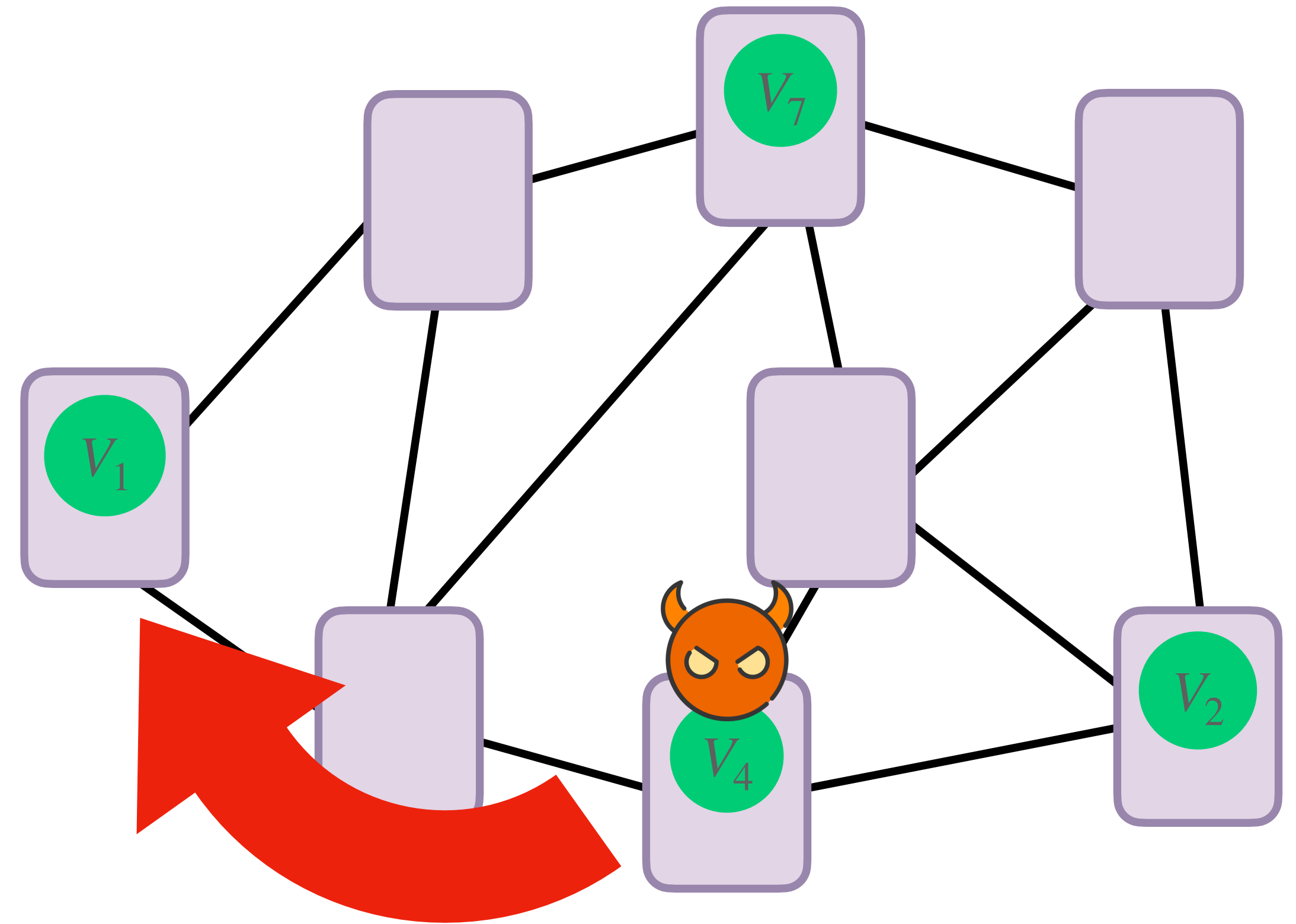
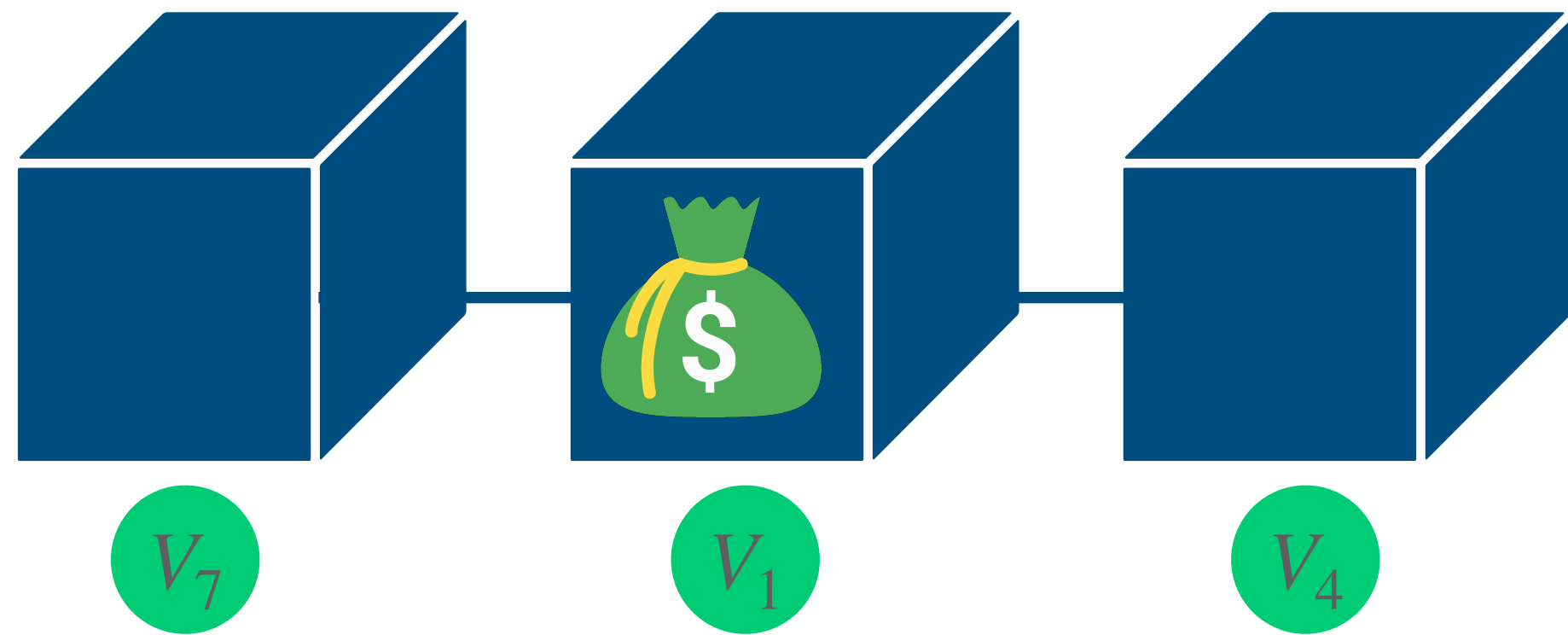
# Why does anonymity matter?



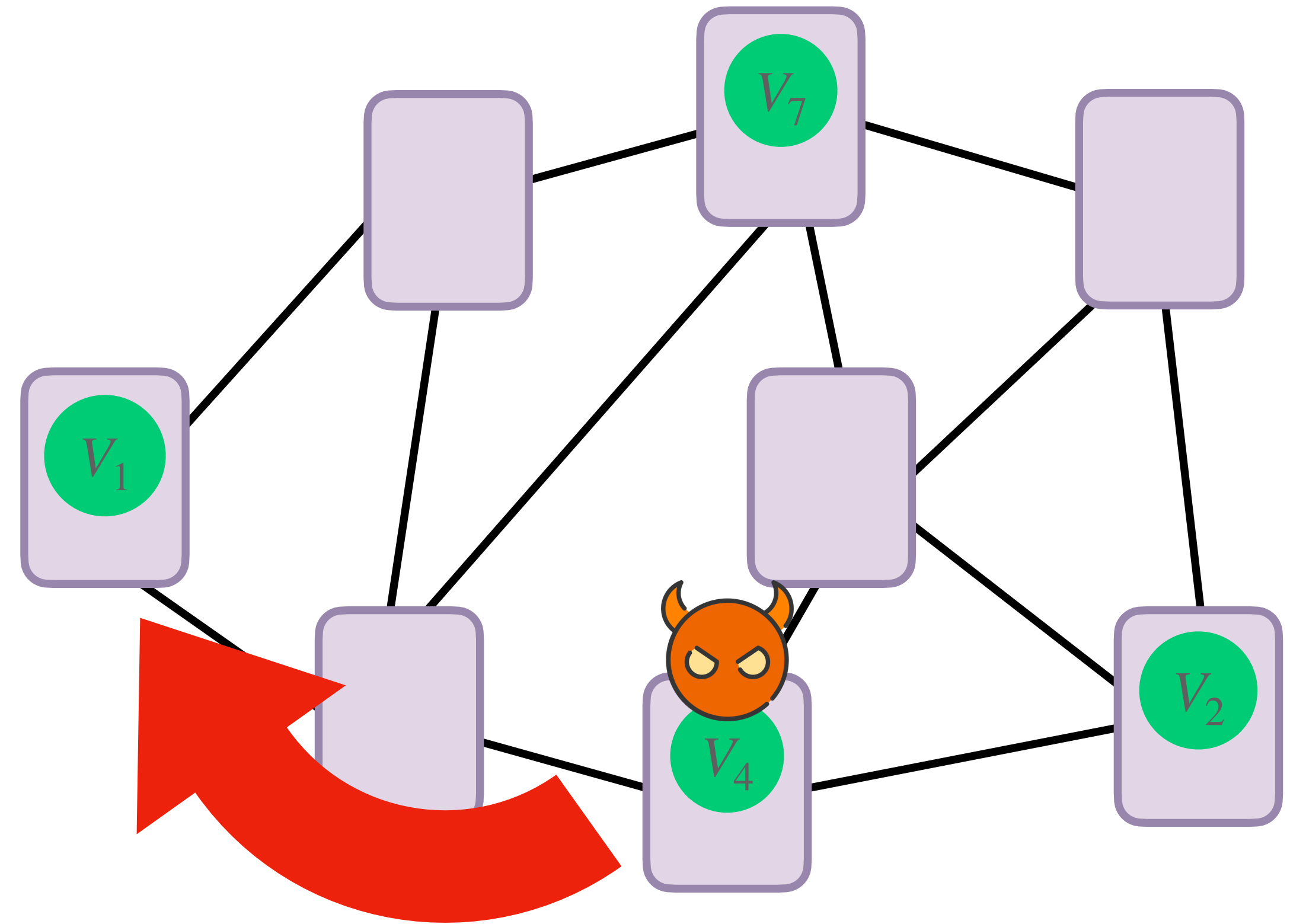
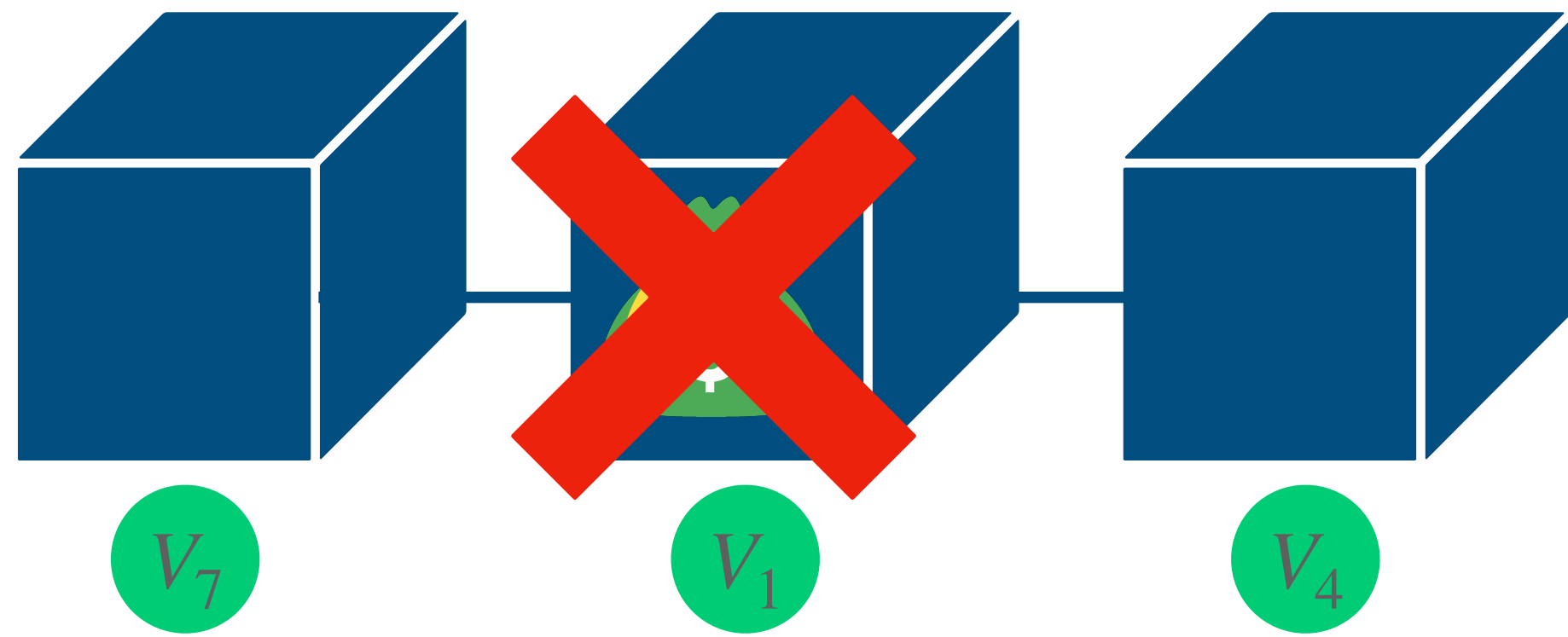
# Why does anonymity matter?



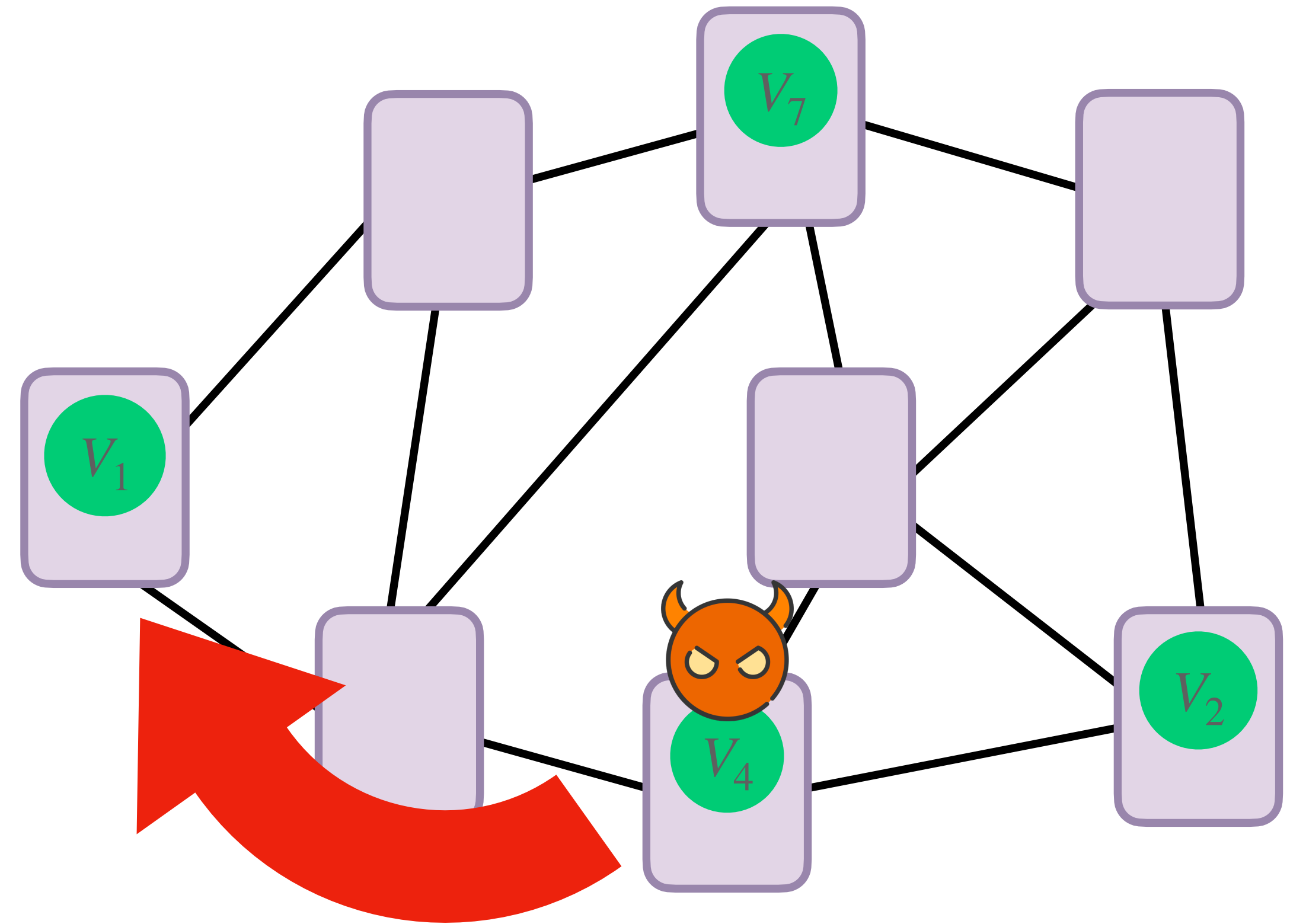
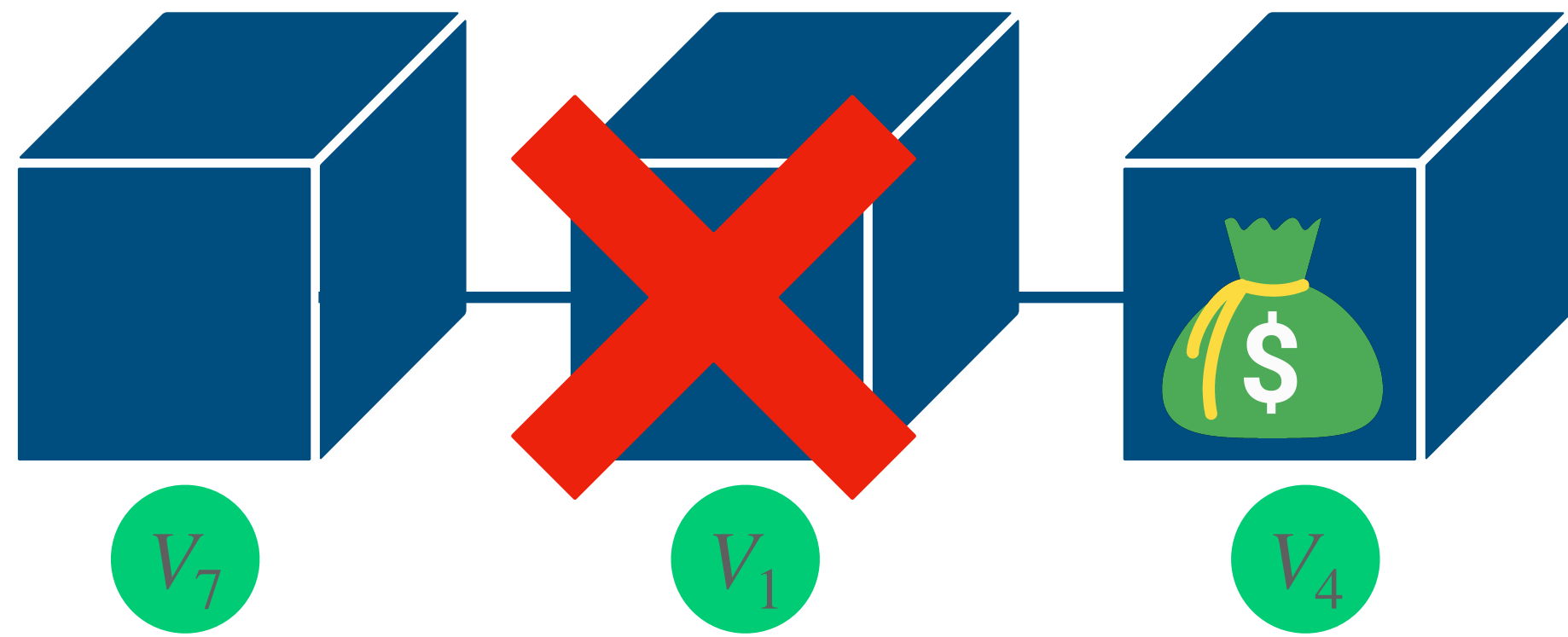
# Why does anonymity matter?



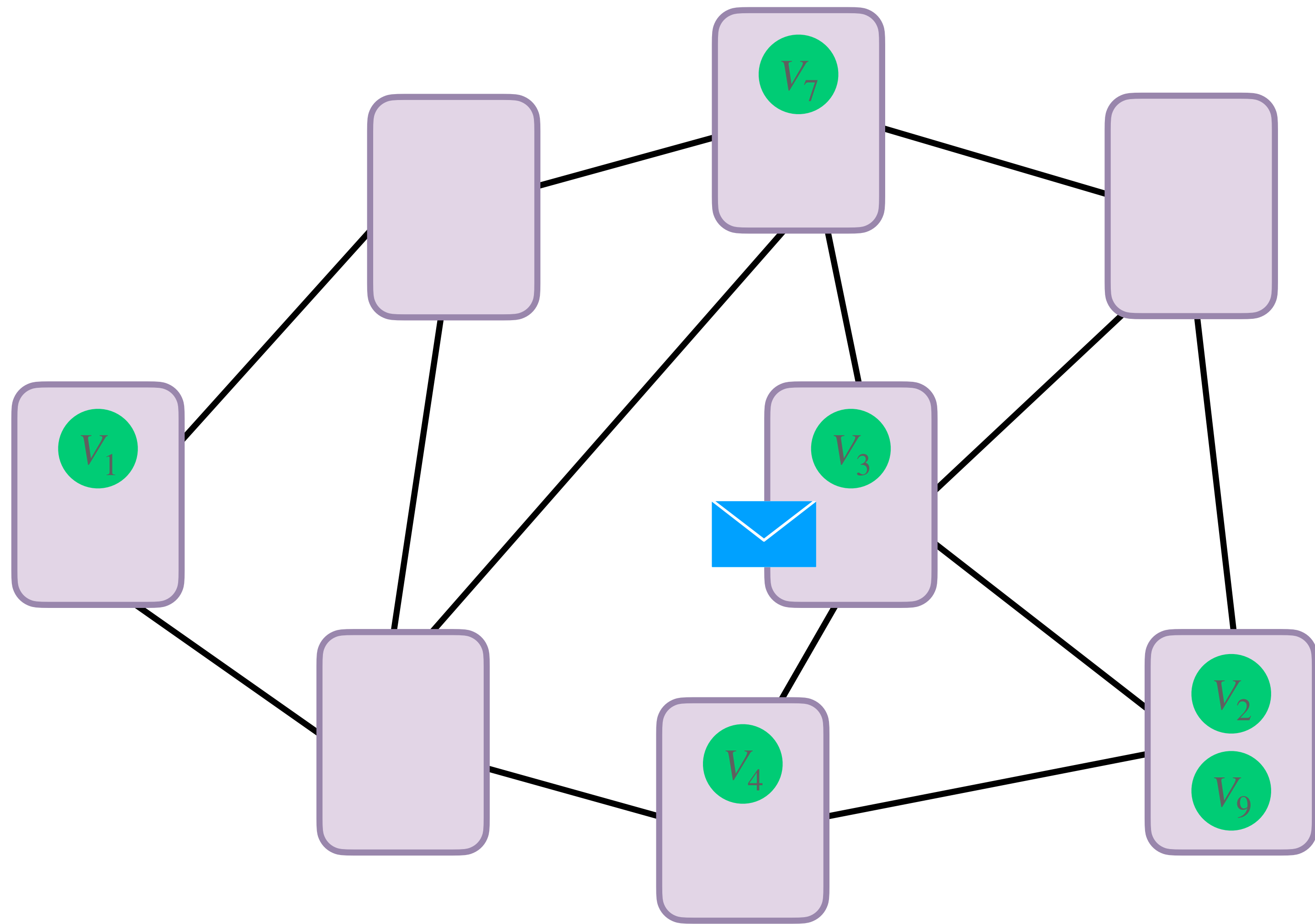
# Why does anonymity matter?



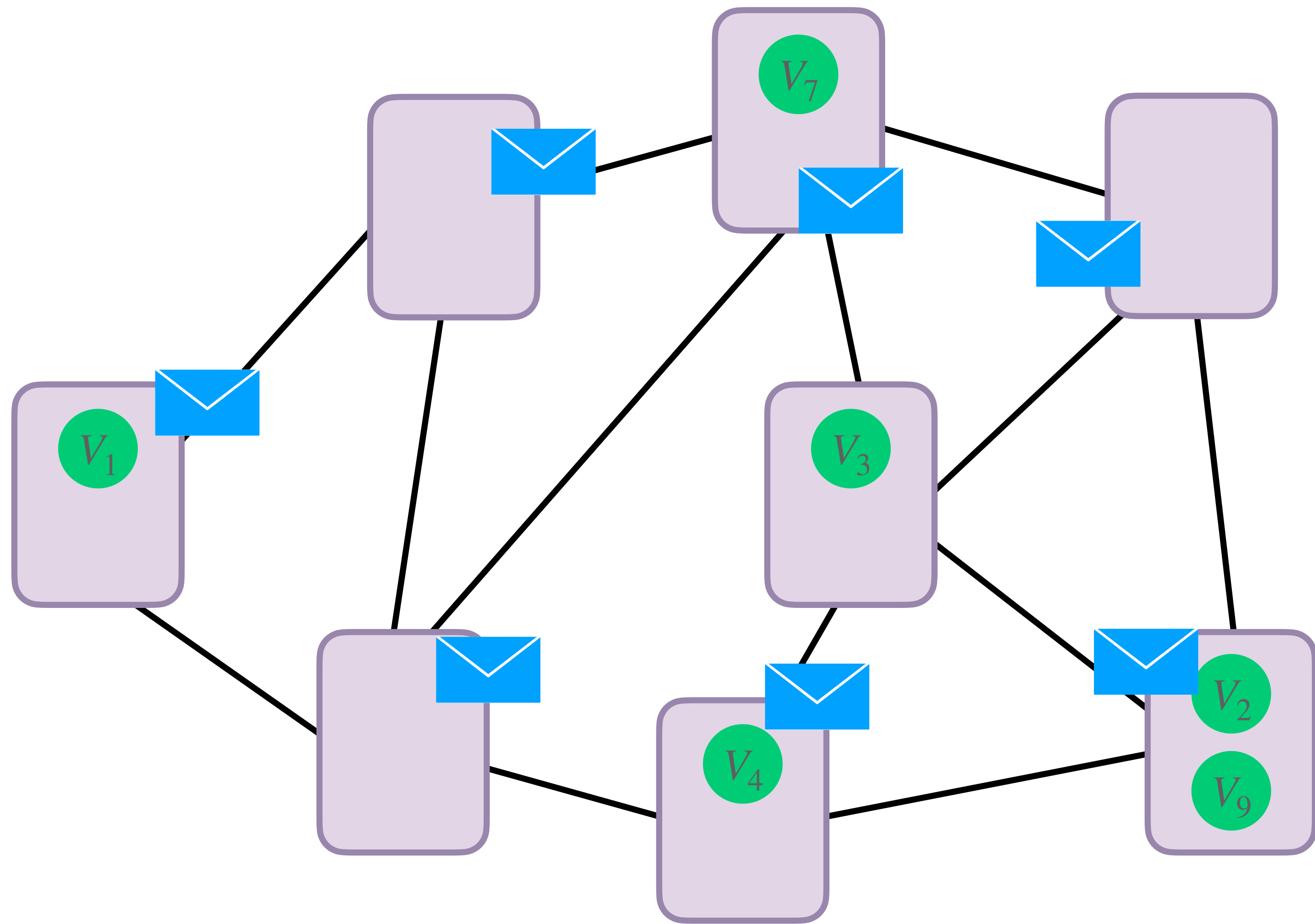
# Why does anonymity matter?

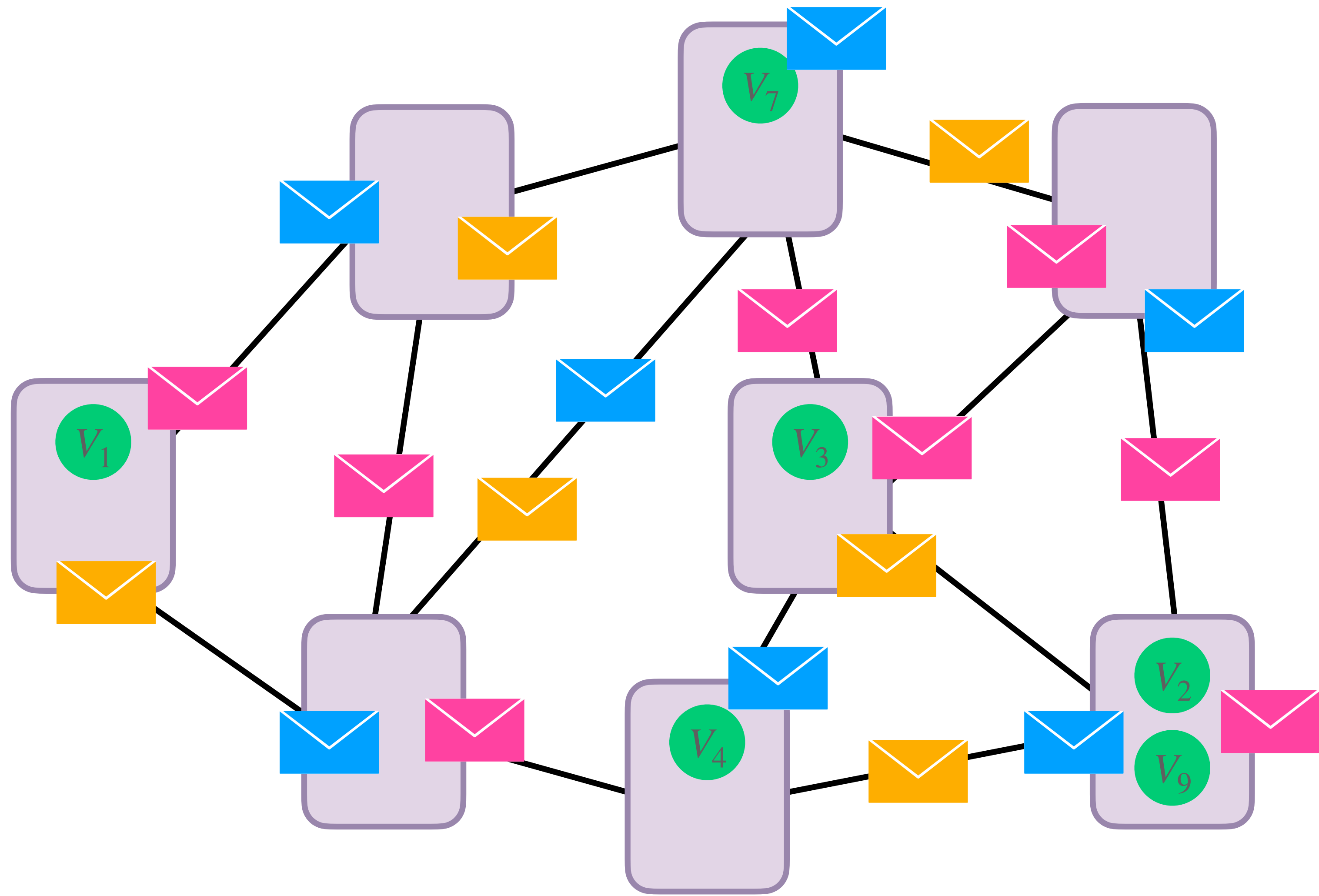


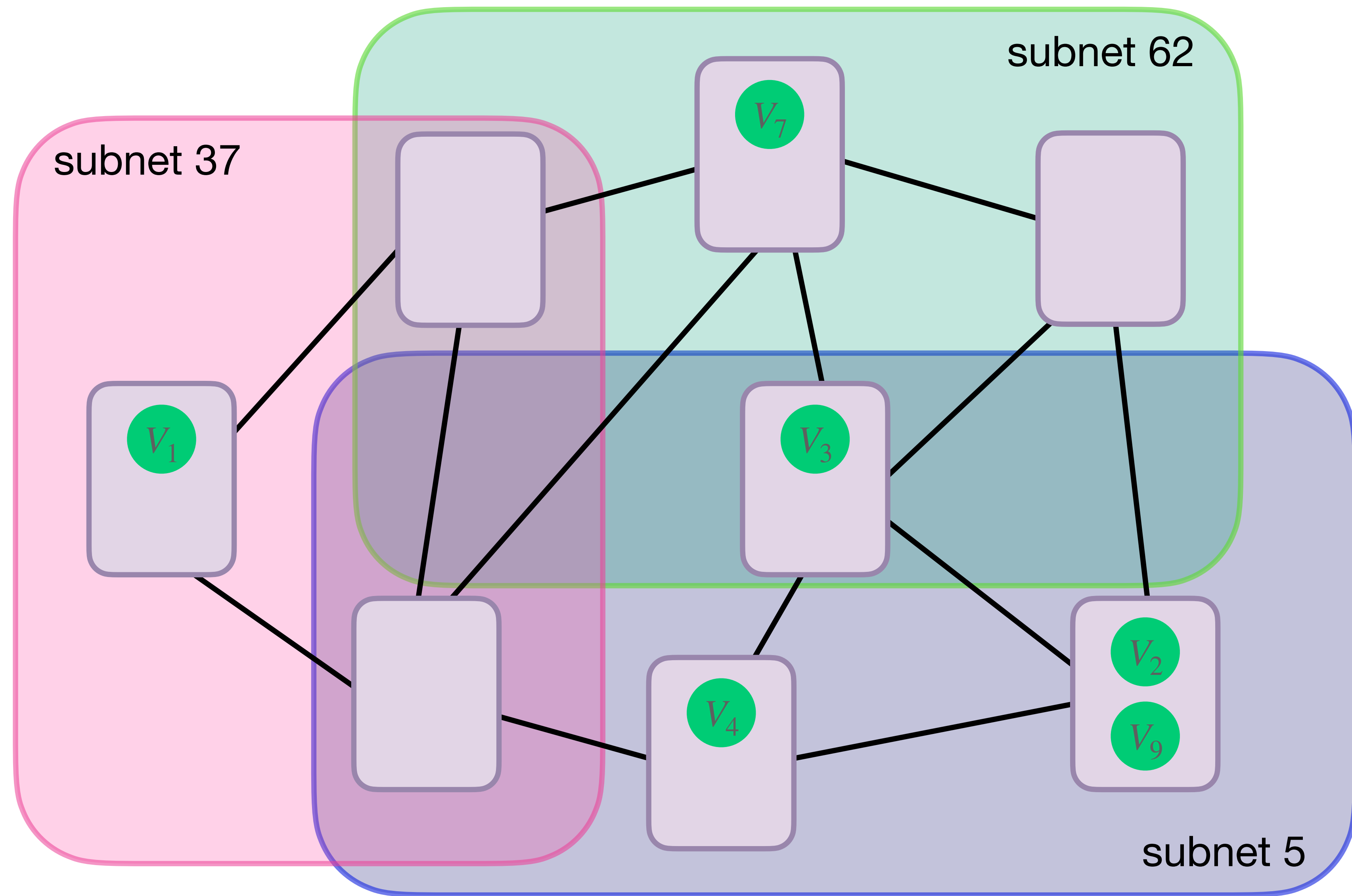
# Ethereum Network Layer

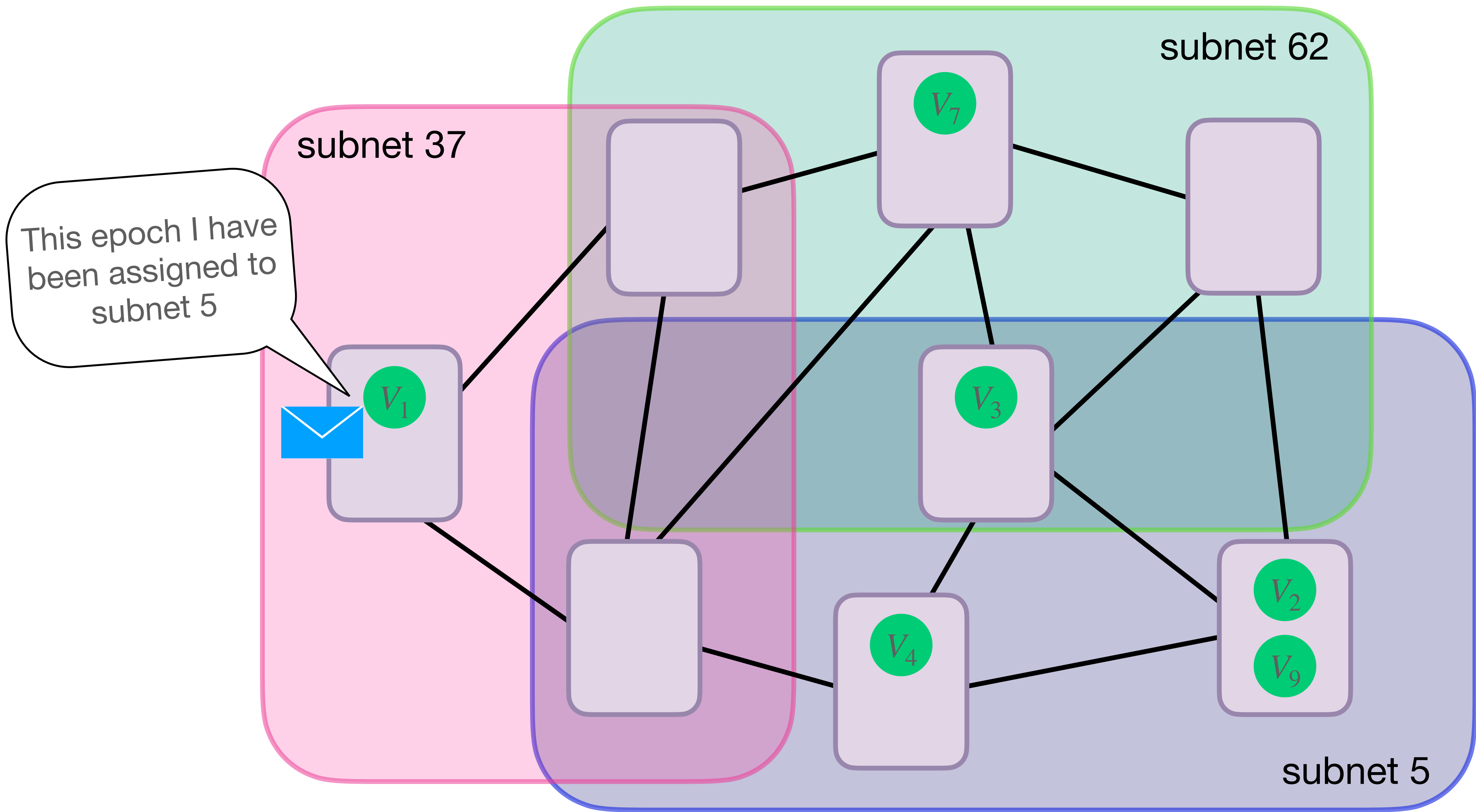


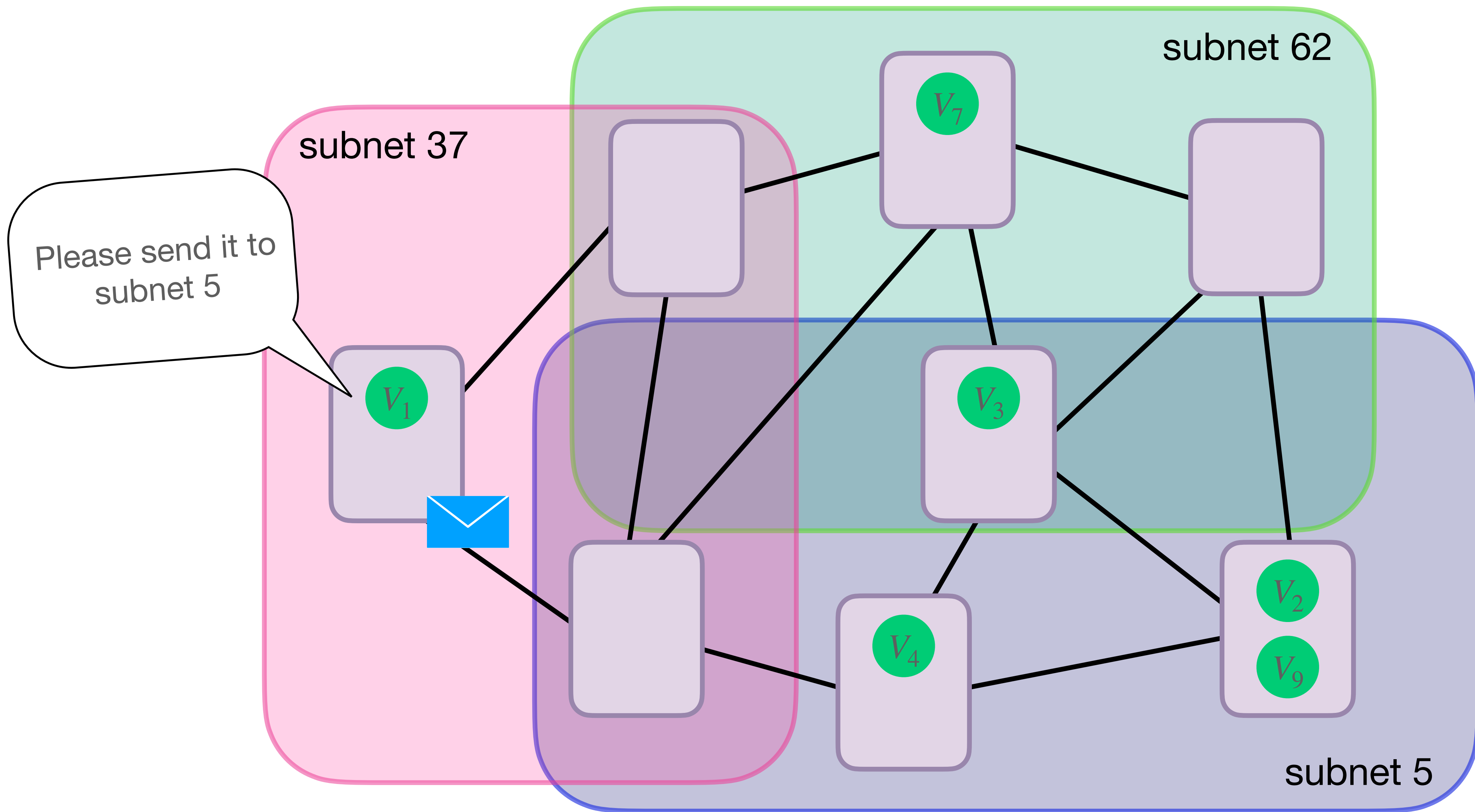


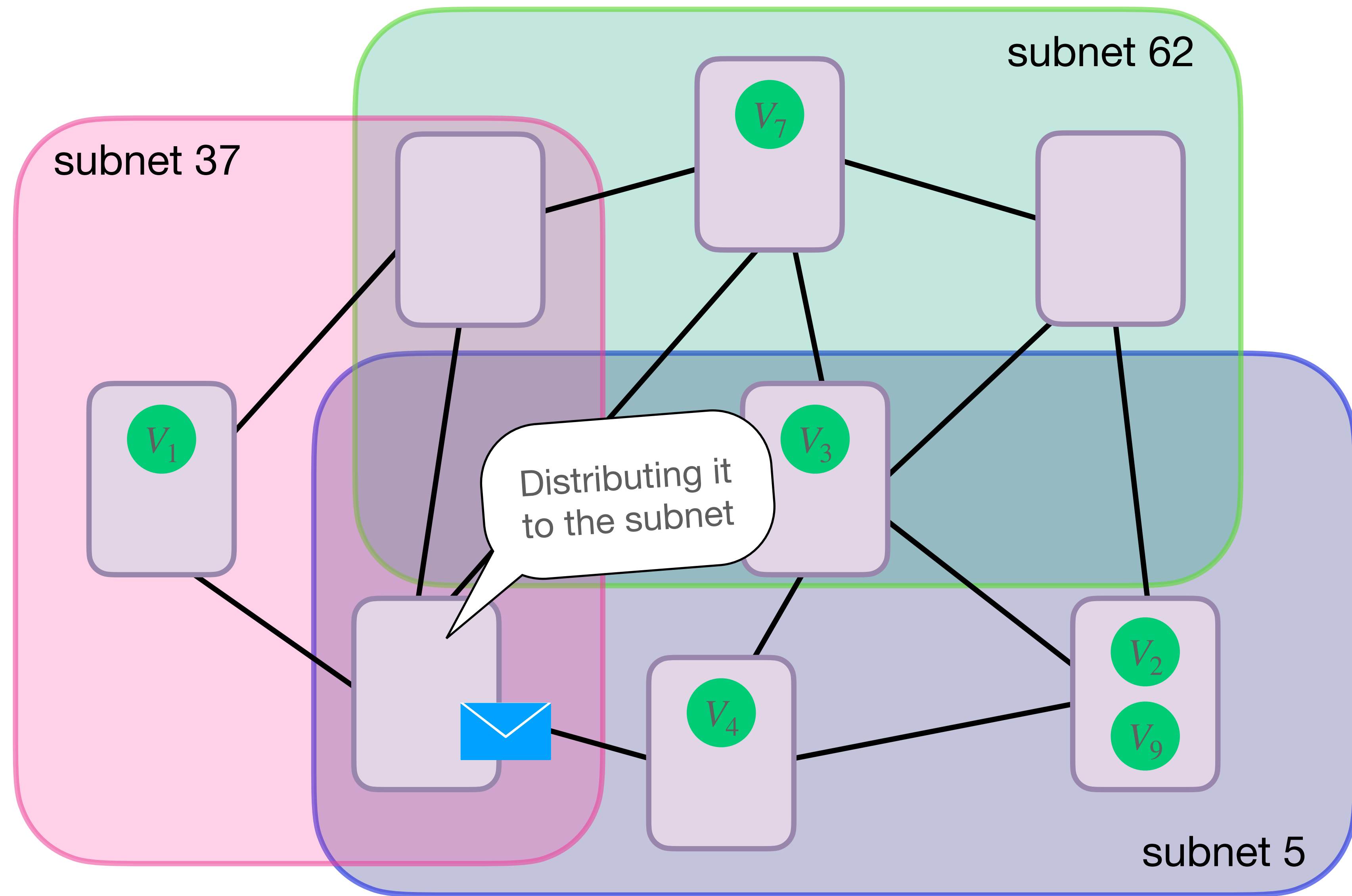


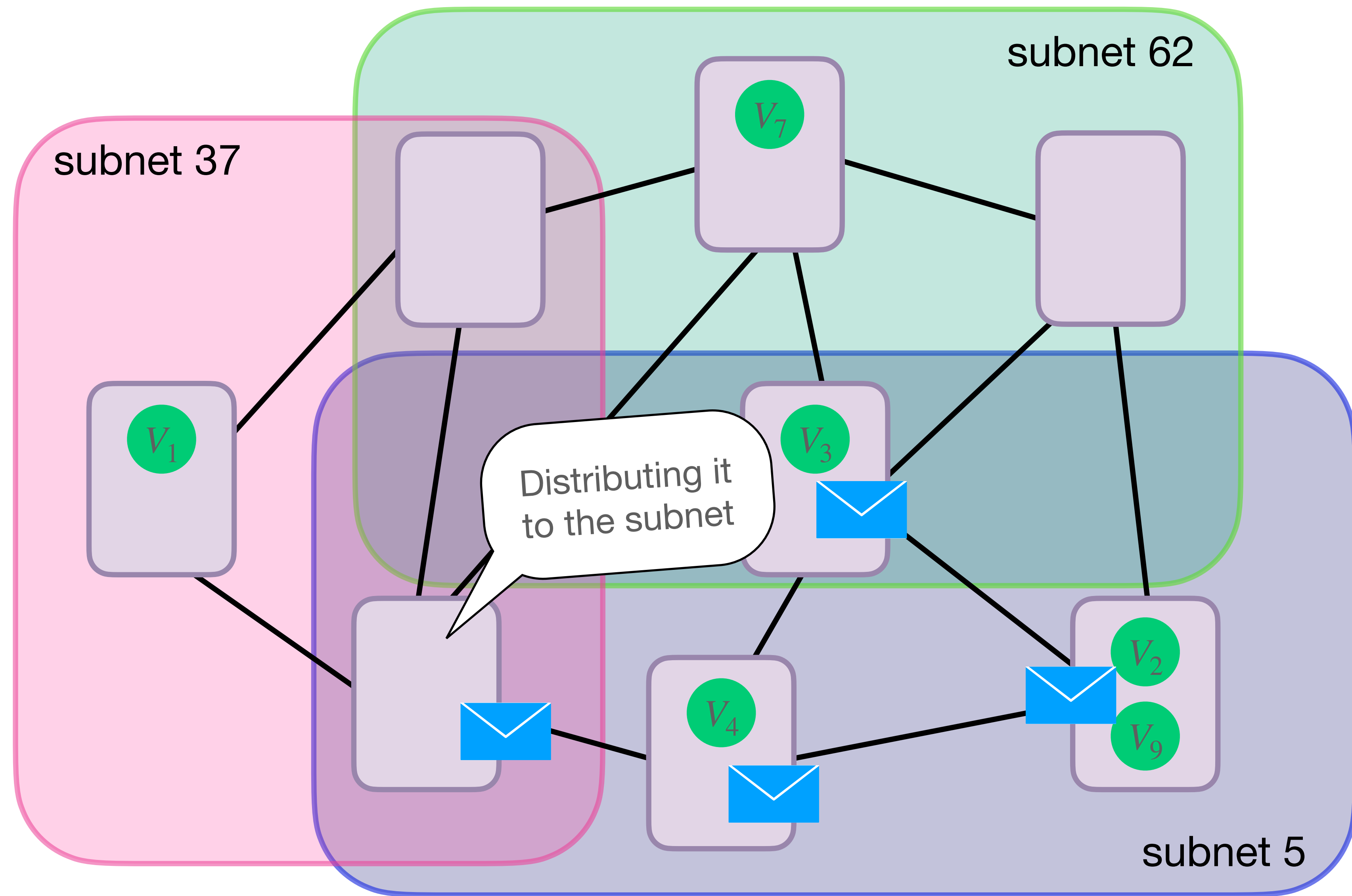


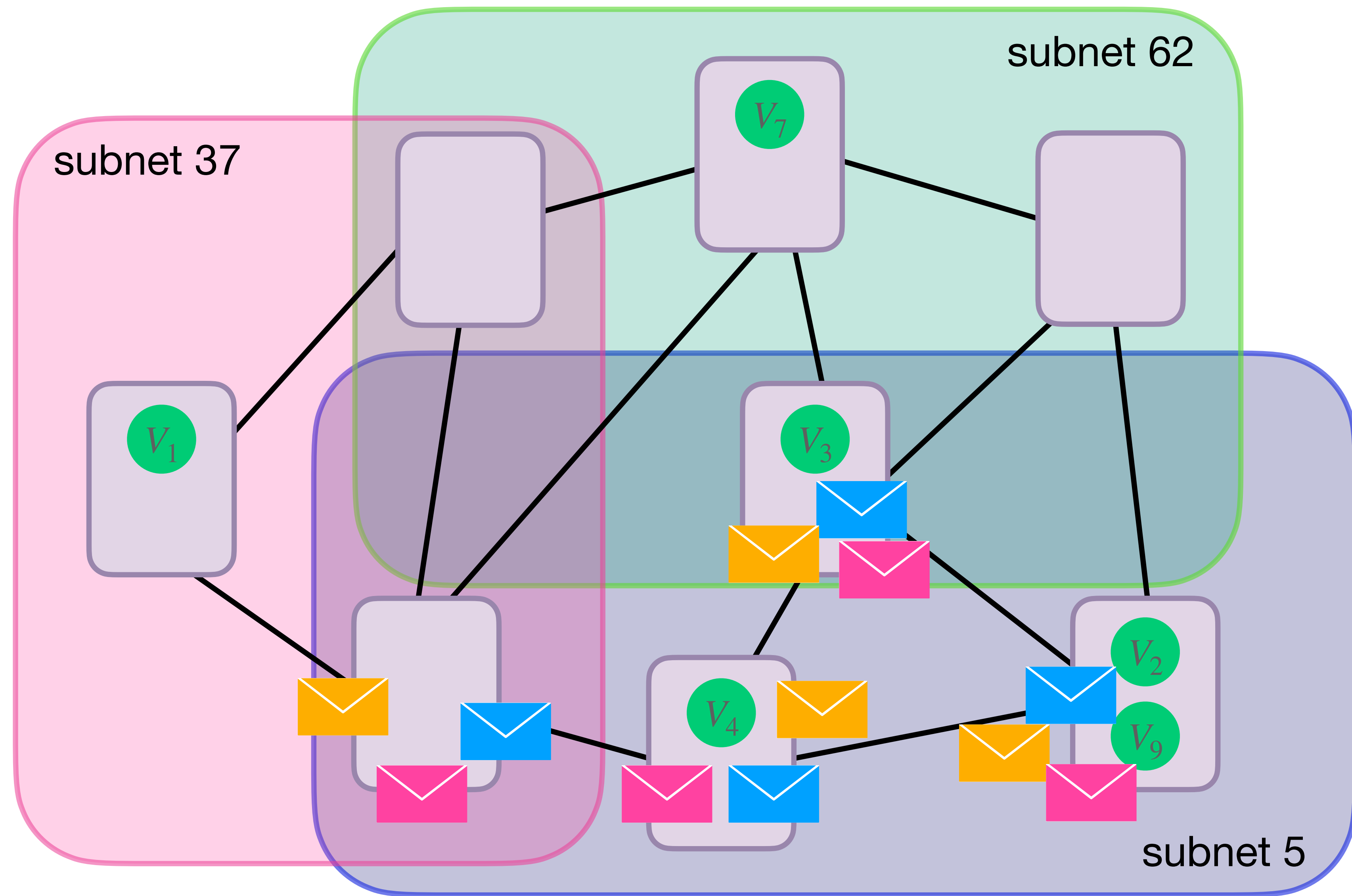


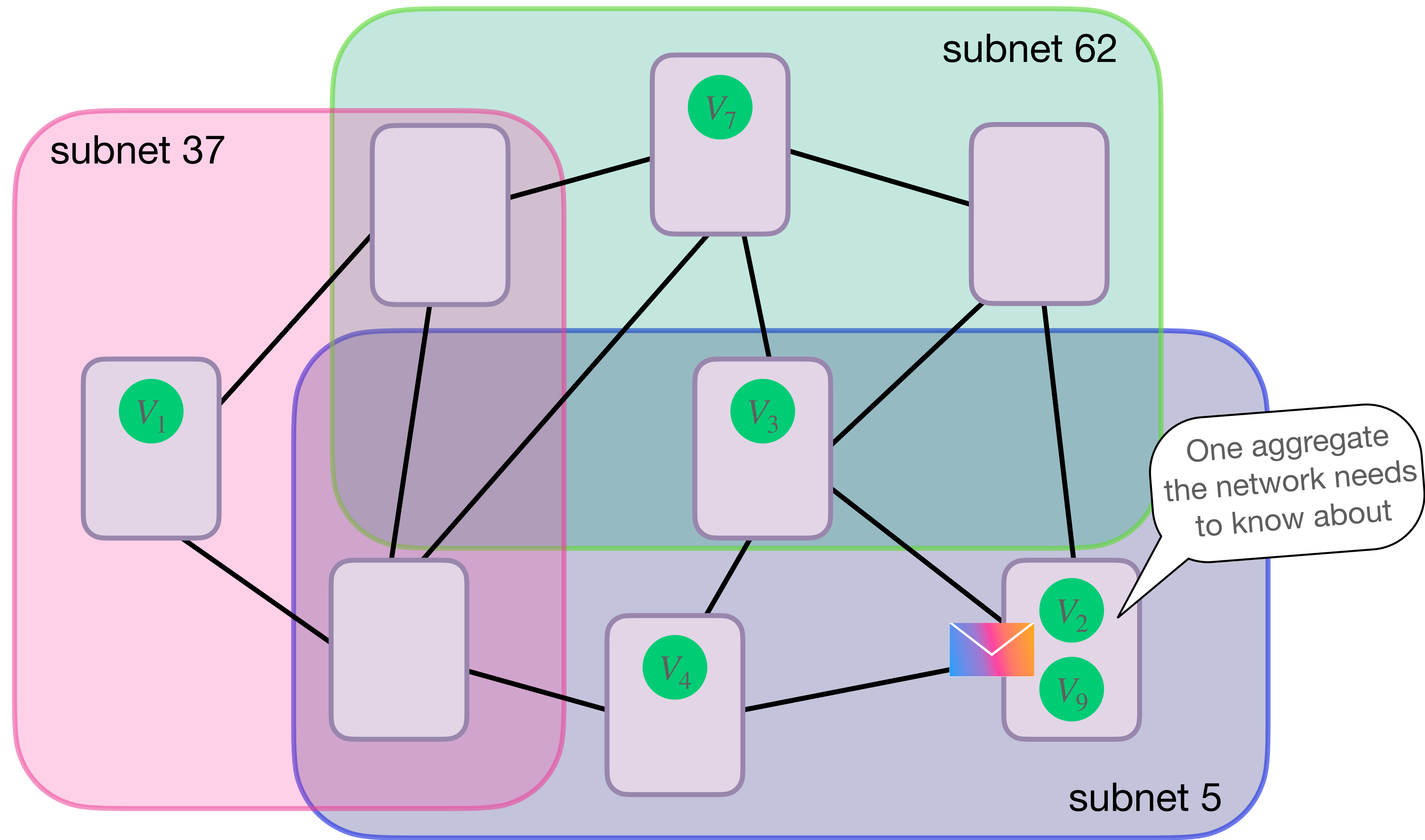


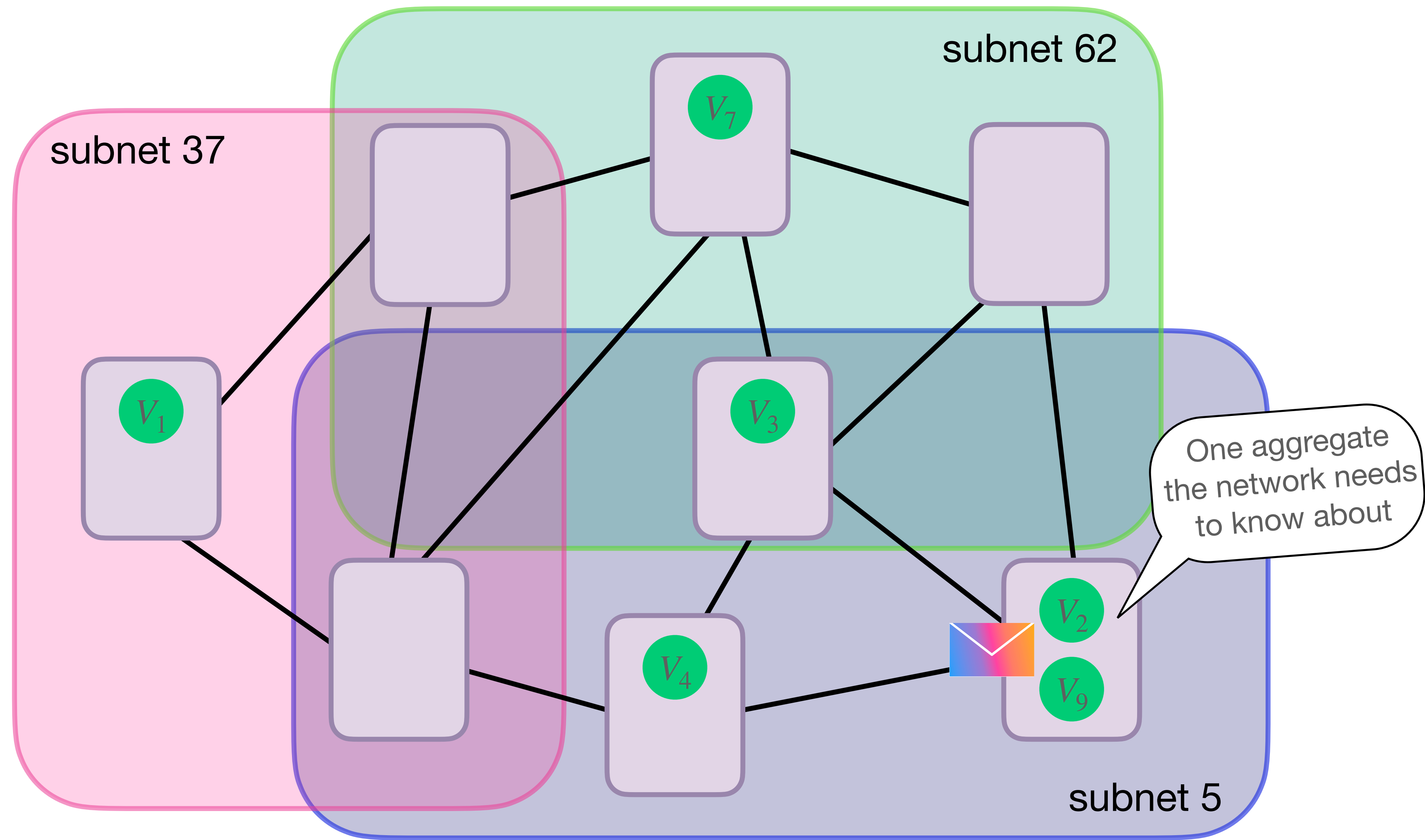






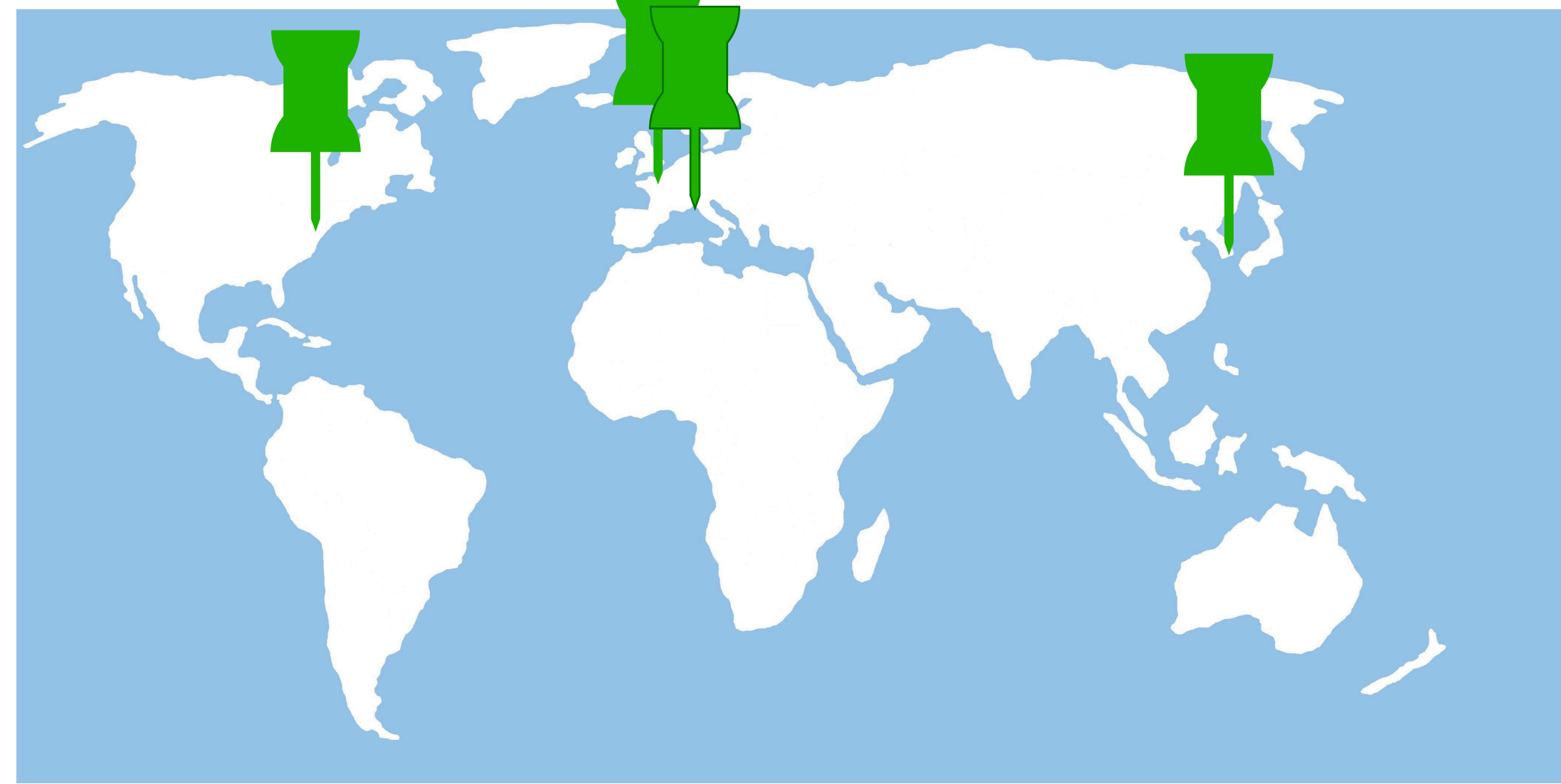


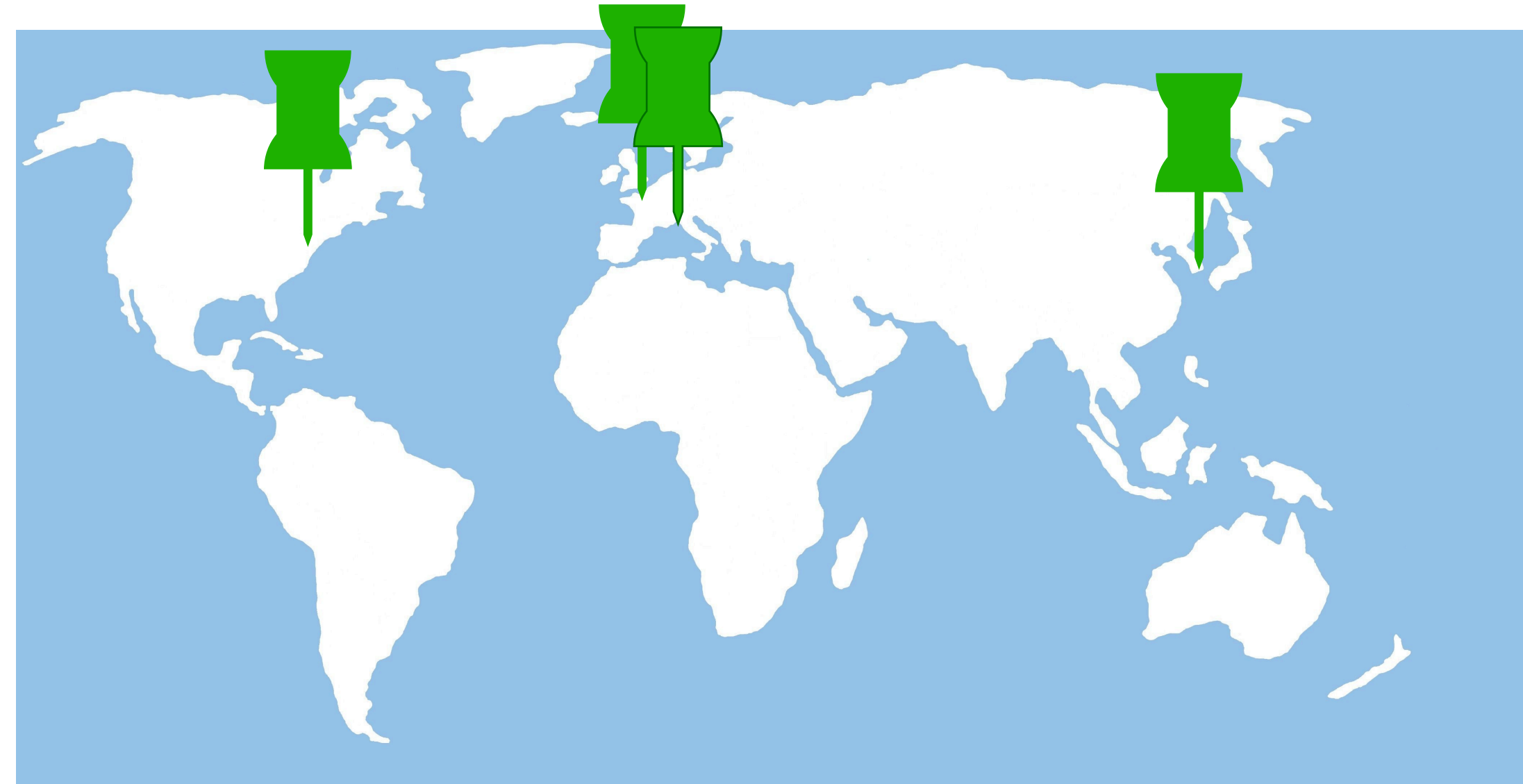




**Do we give up privacy as a tradeoff for lower network load?**







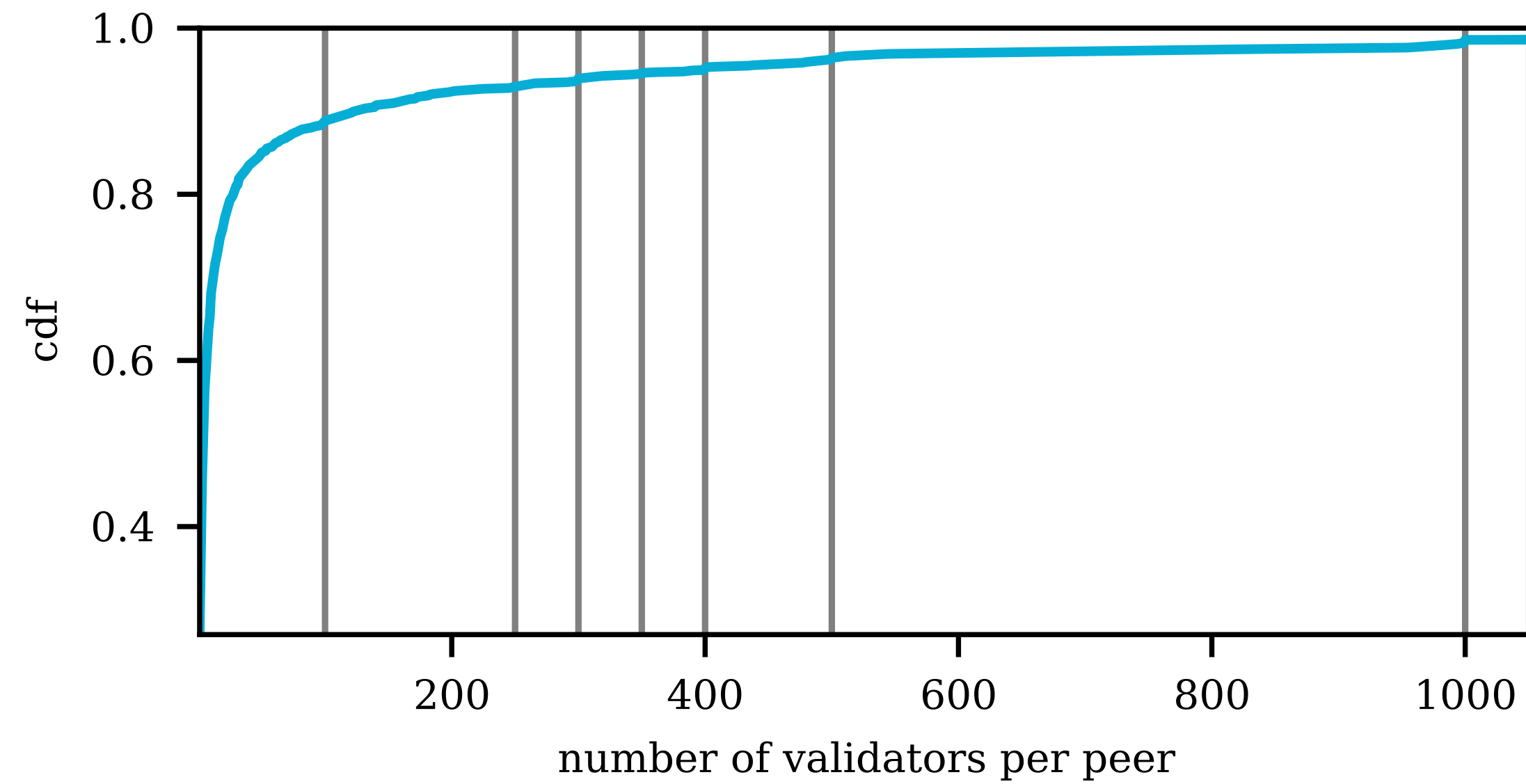
**161'057**

**validators were deanonymized.**

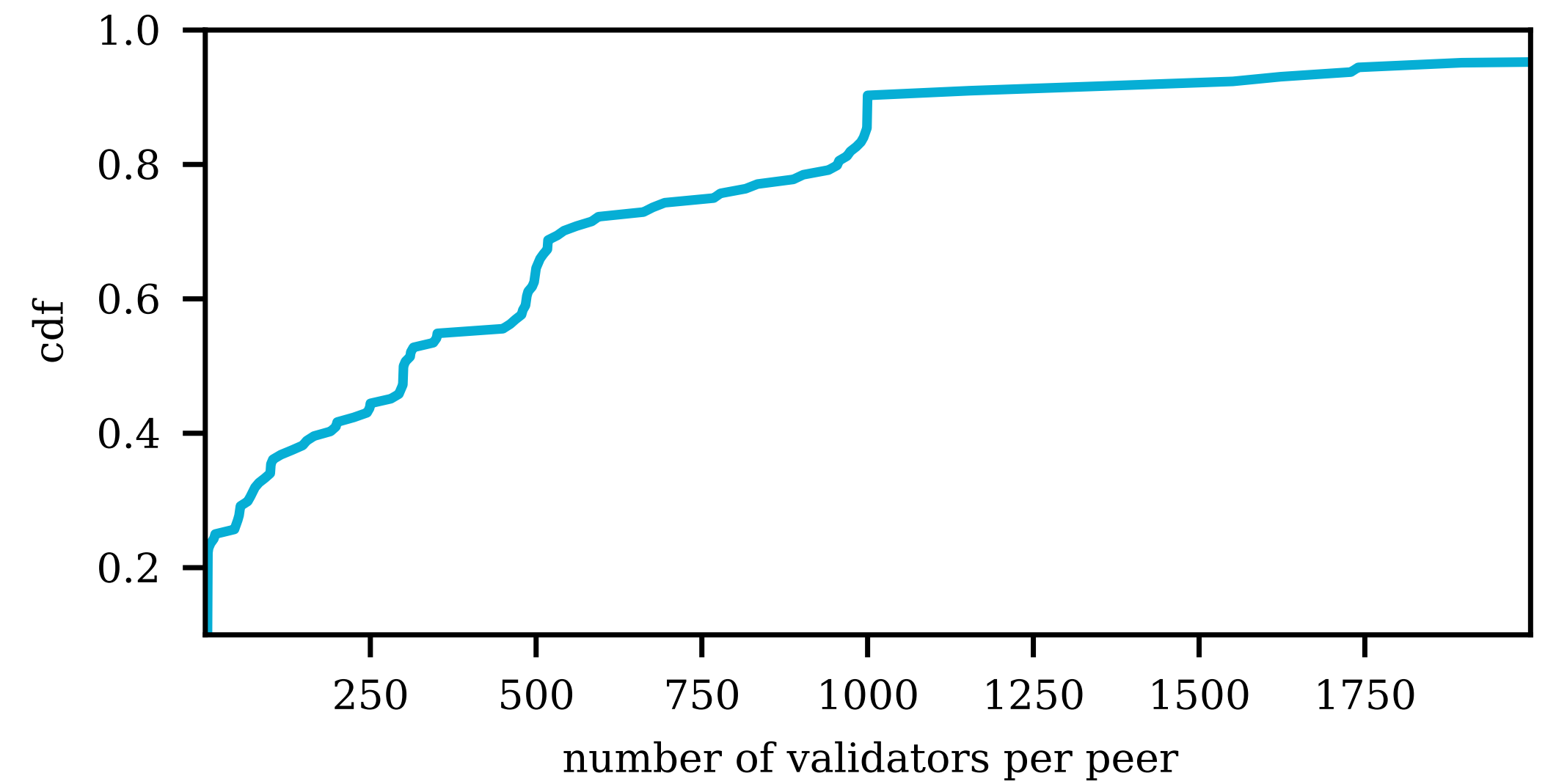
# Take-Aways

# Validators per Peer

## Overall

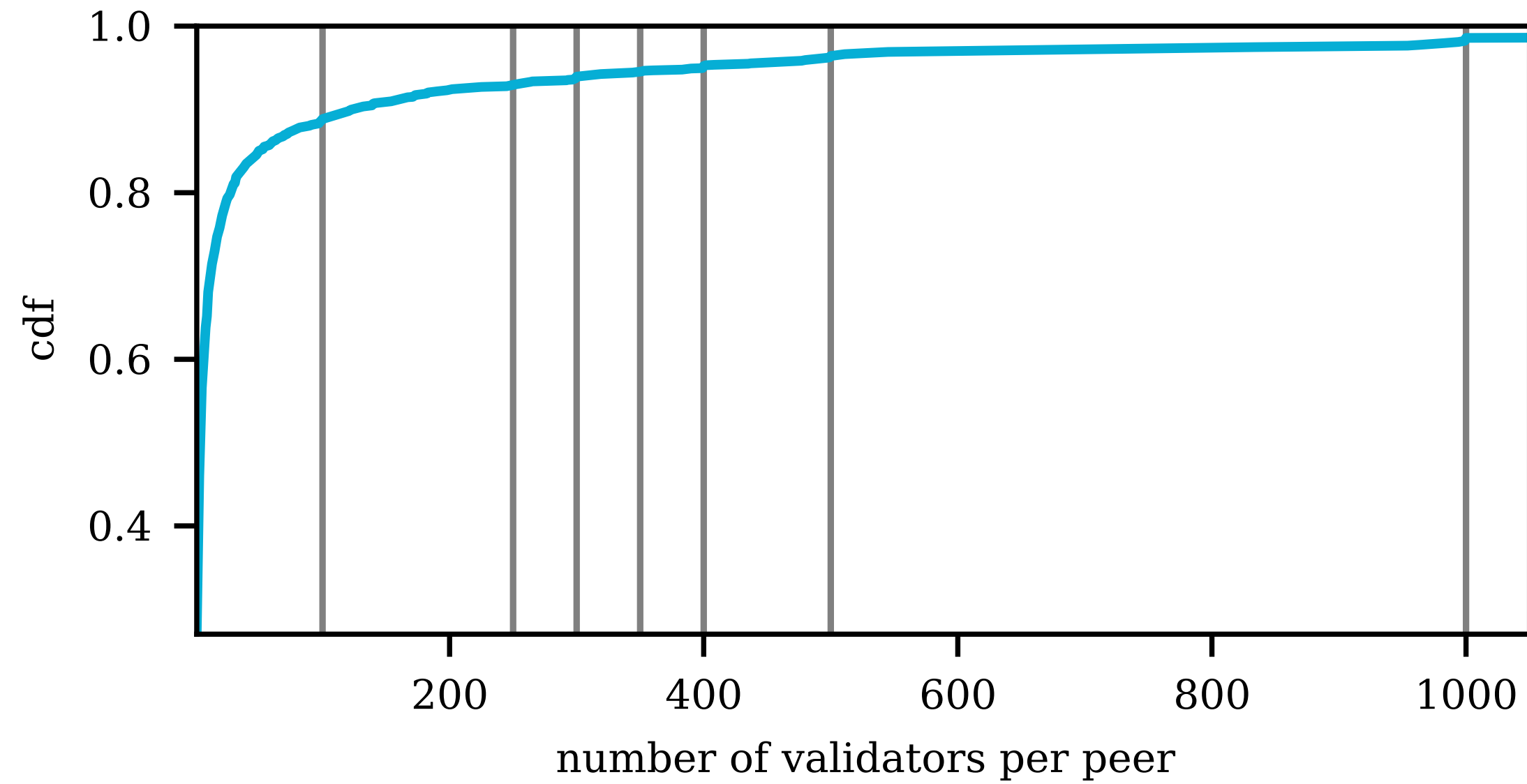


## Five Largest Staking Pools

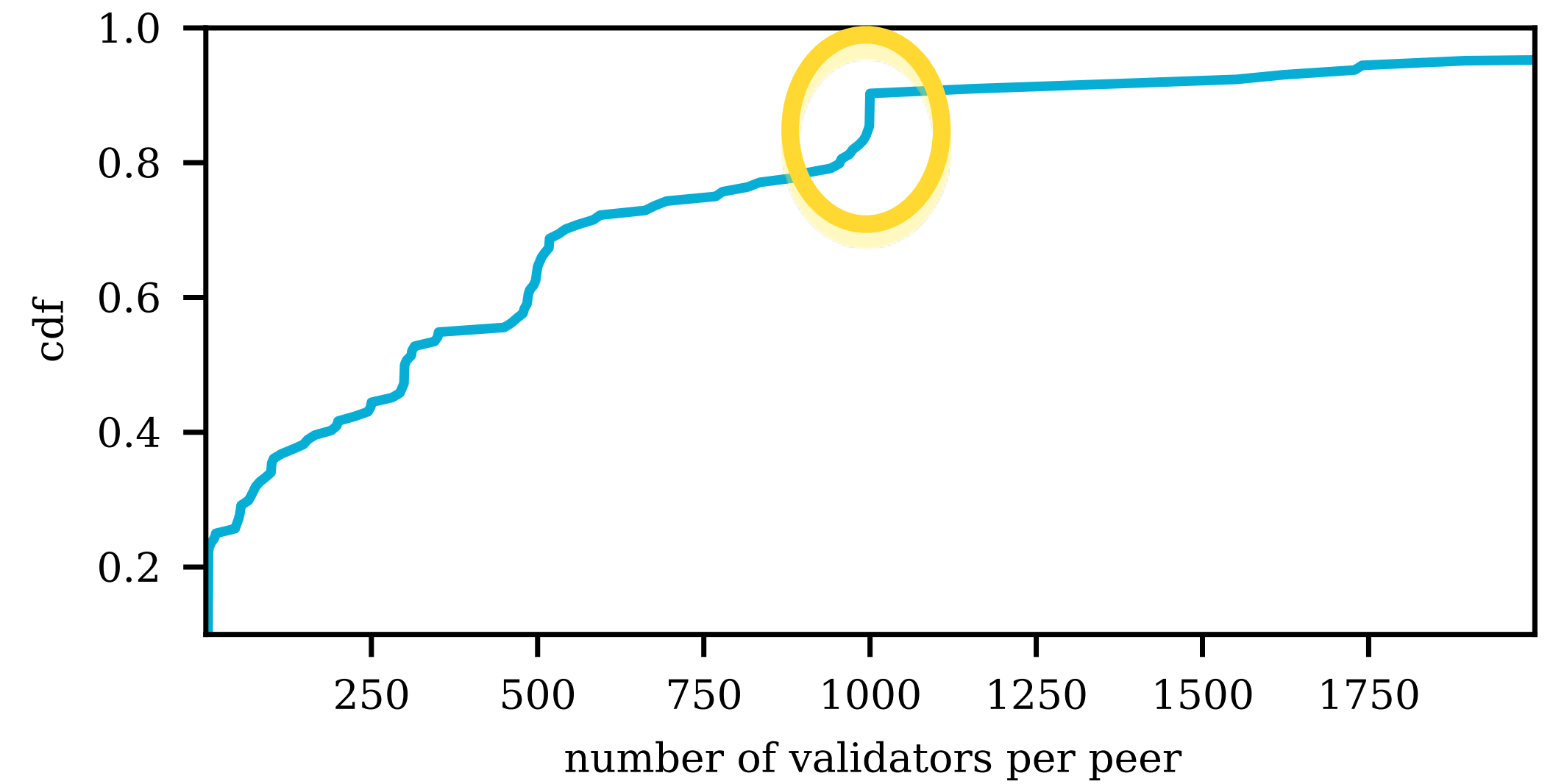


# Validators per Peer

## Overall

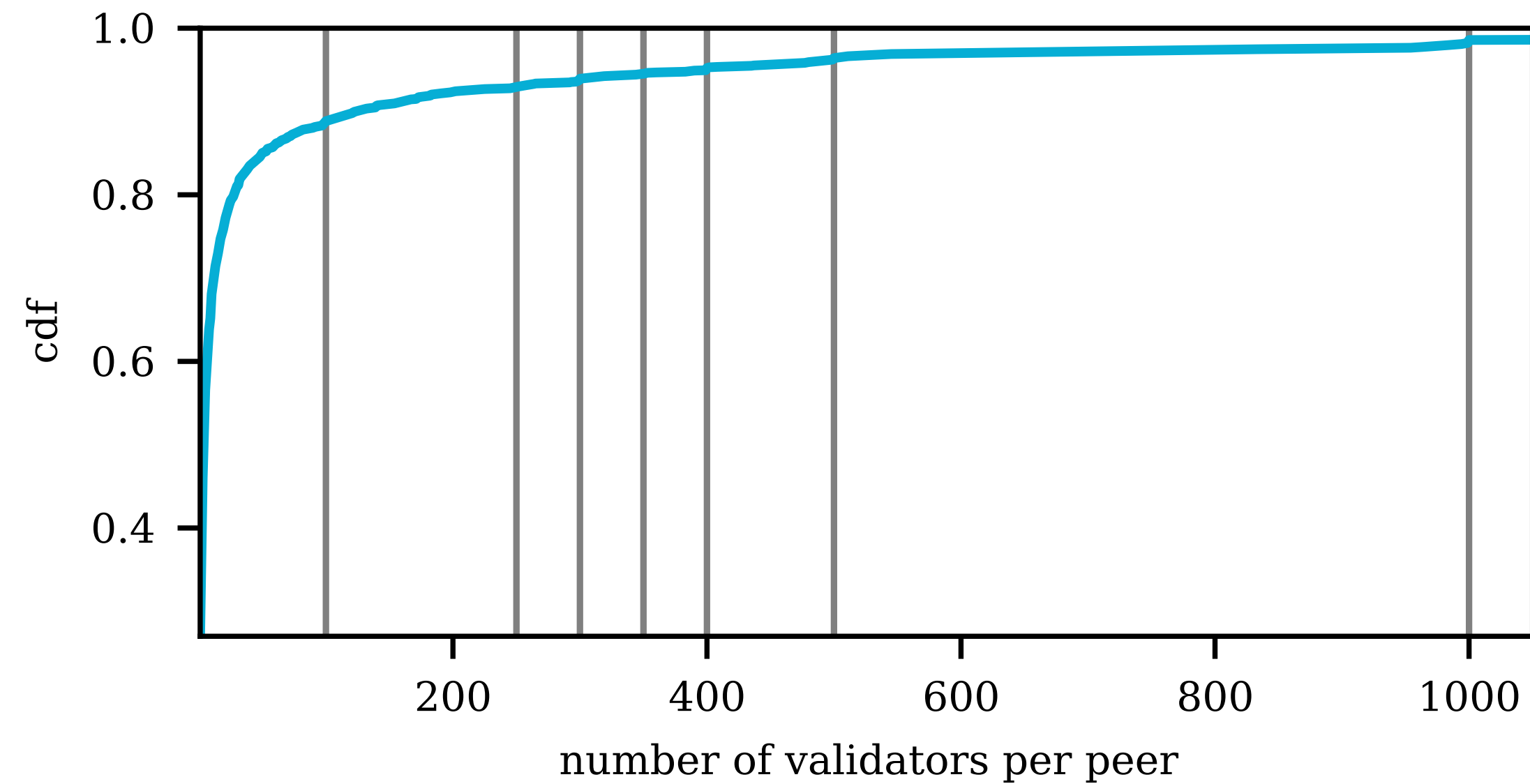


## Five Largest Staking Pools

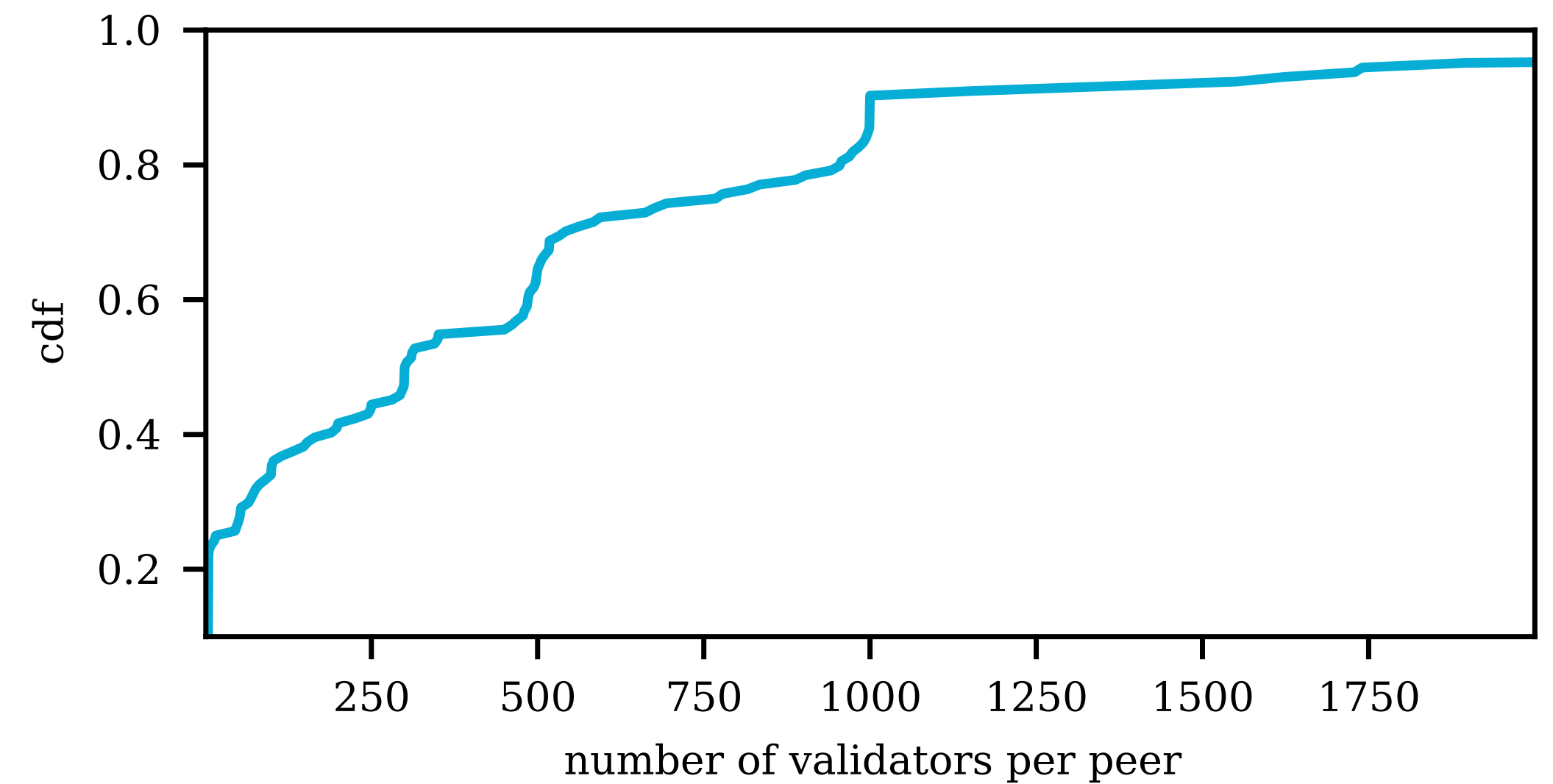


# Validators per Peer

## Overall



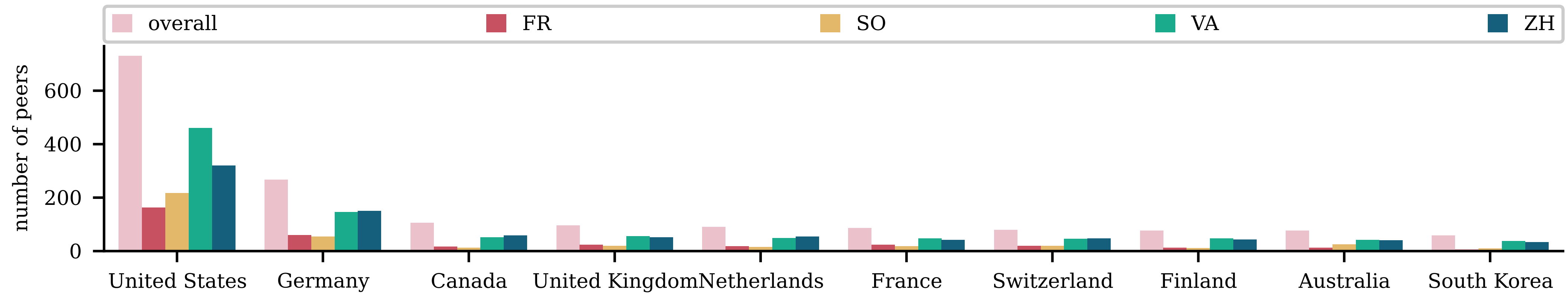
## Five Largest Staking Pools



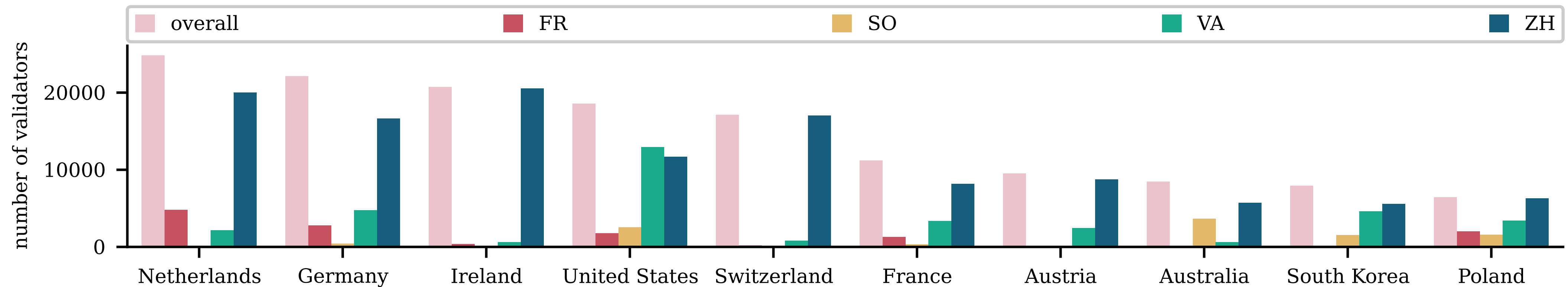
Most Validators on Single Peer: 19'390

# Location

## Peers



## Validators



# Thanks!

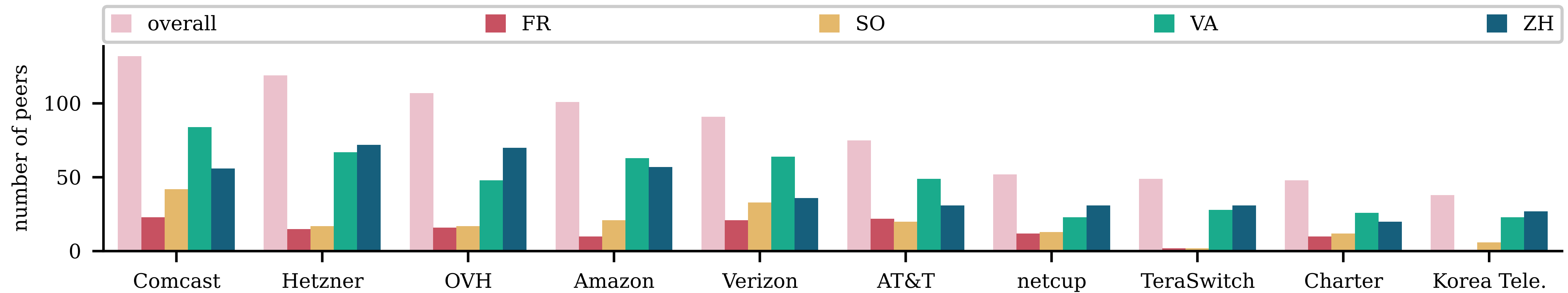


@yannvon

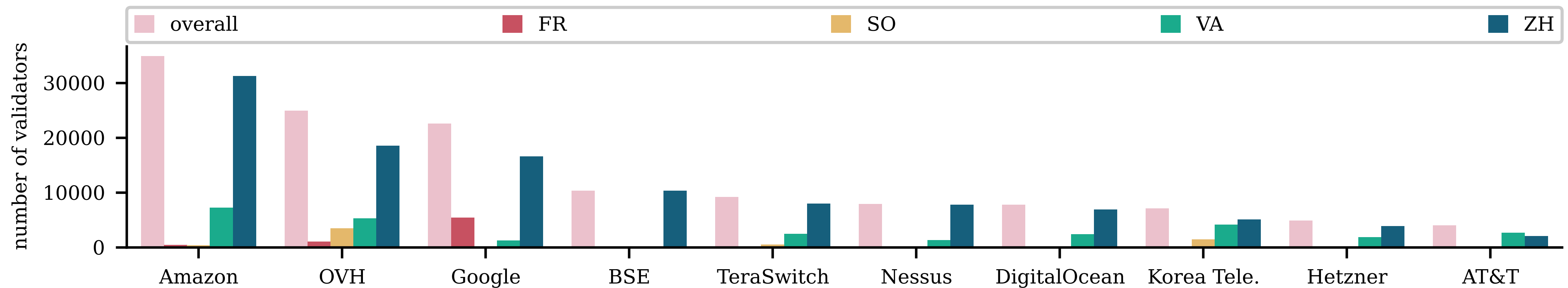


# Organizations

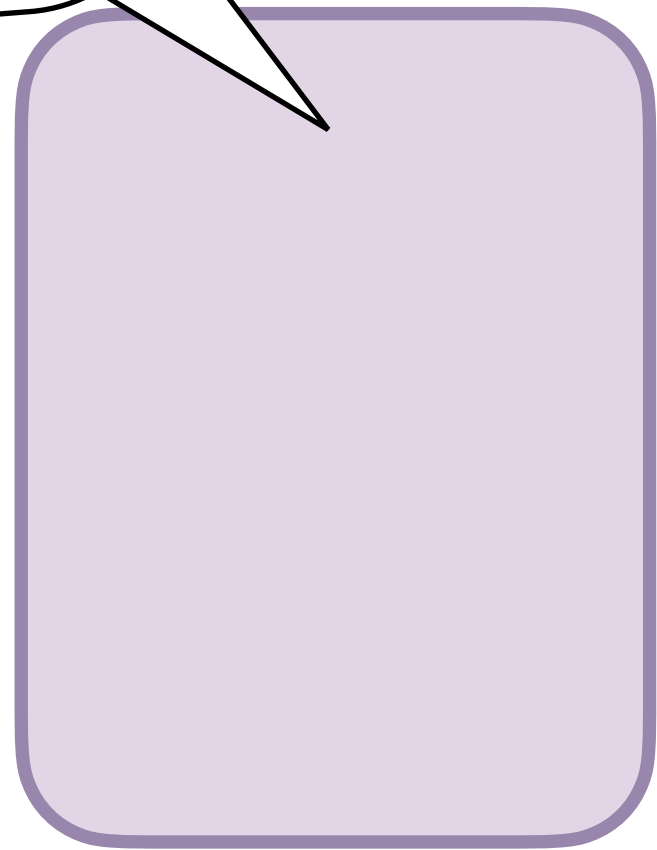
## Peers



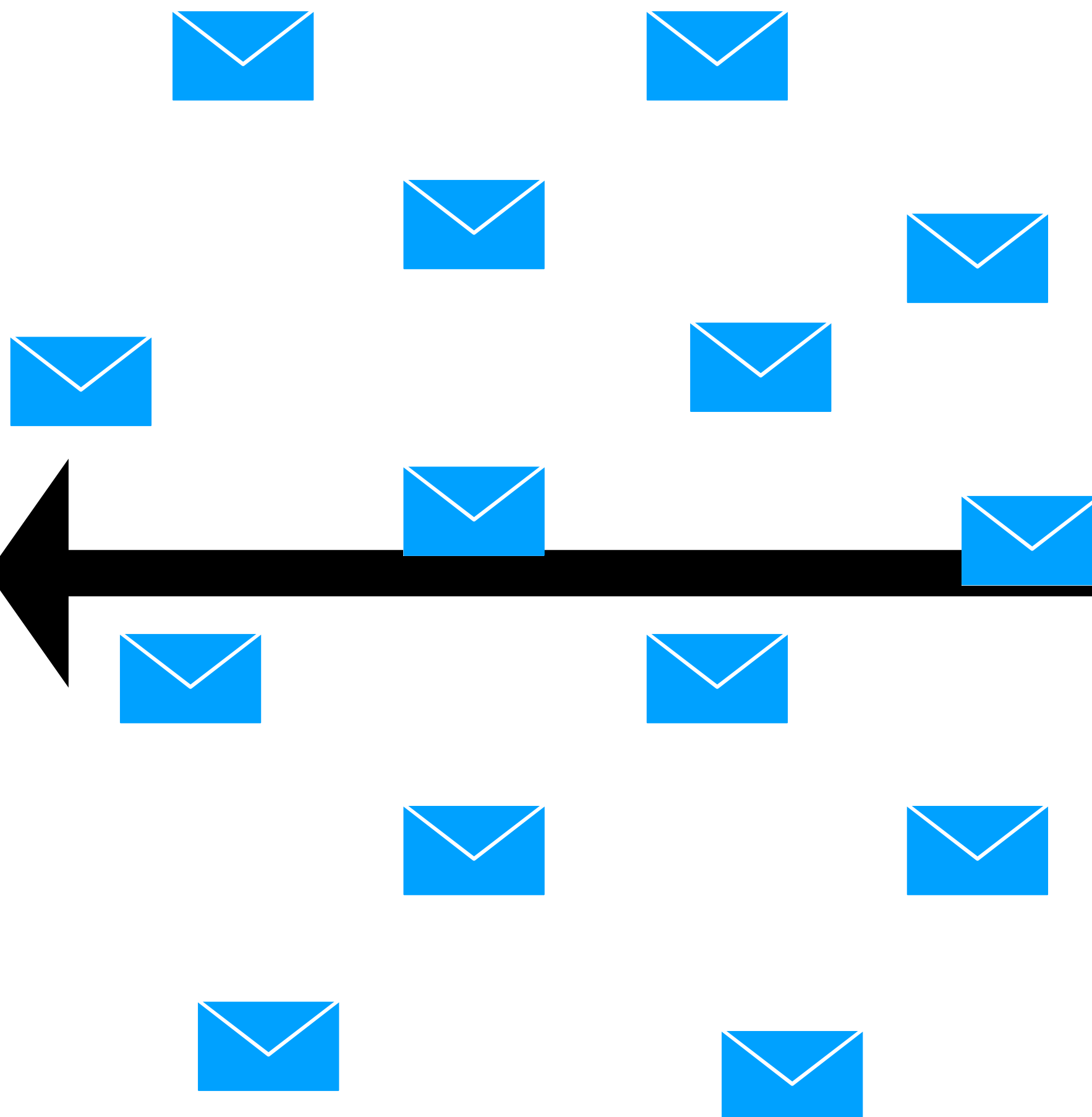
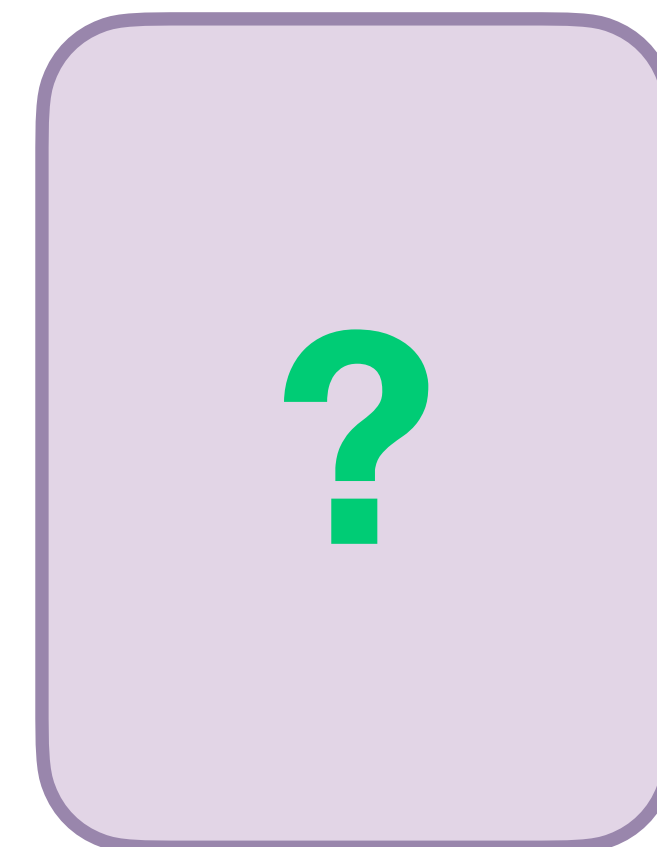
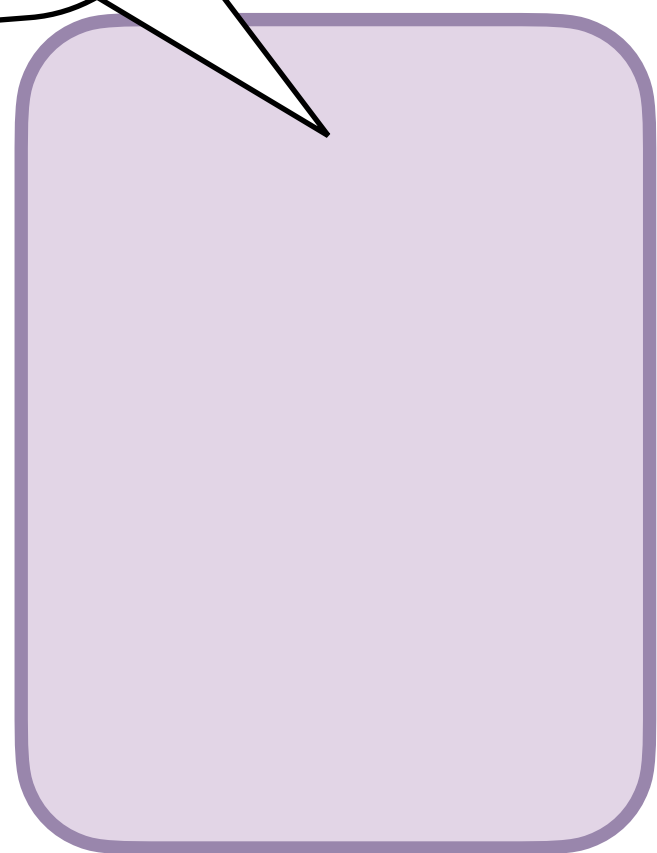
## Validators



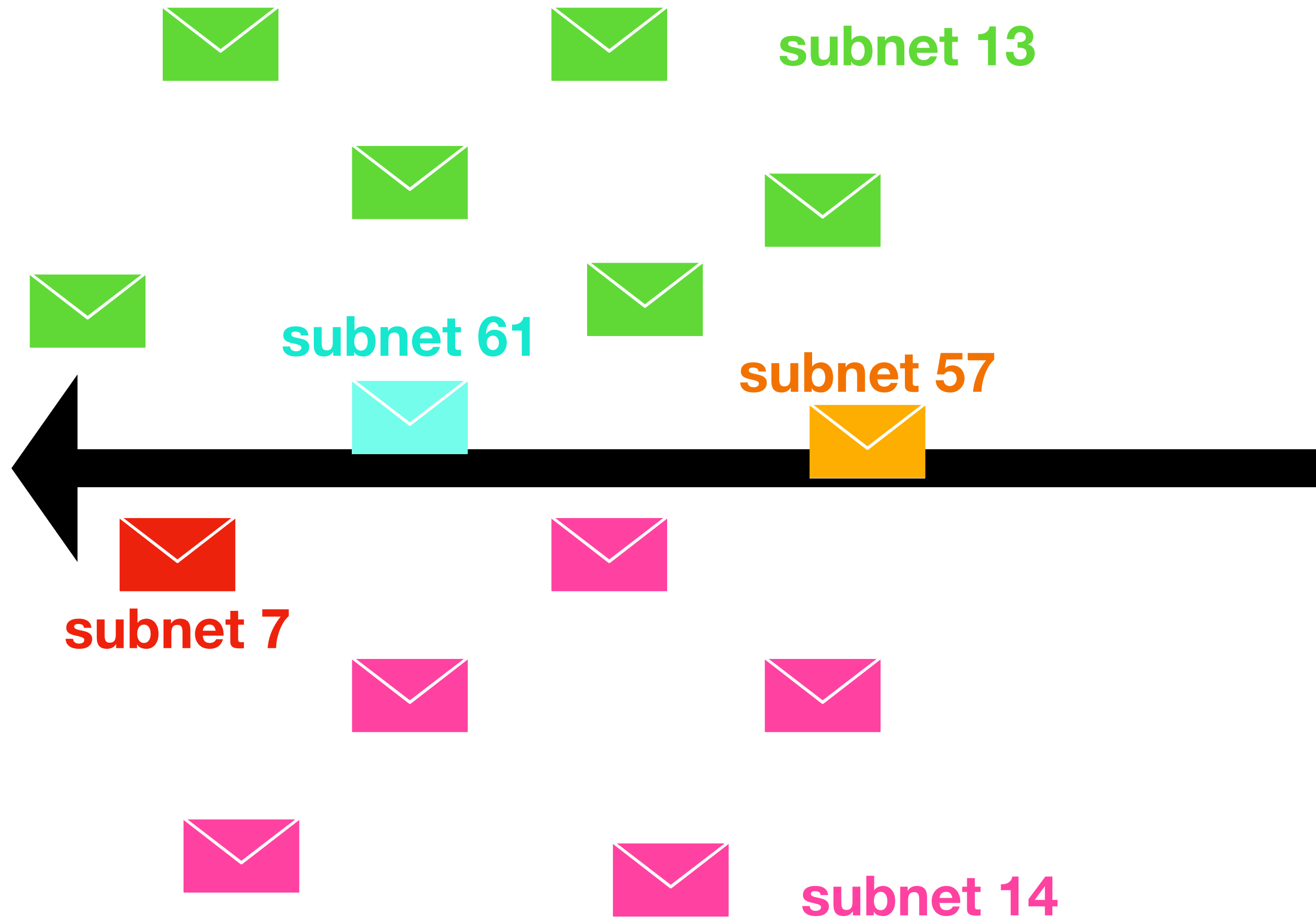
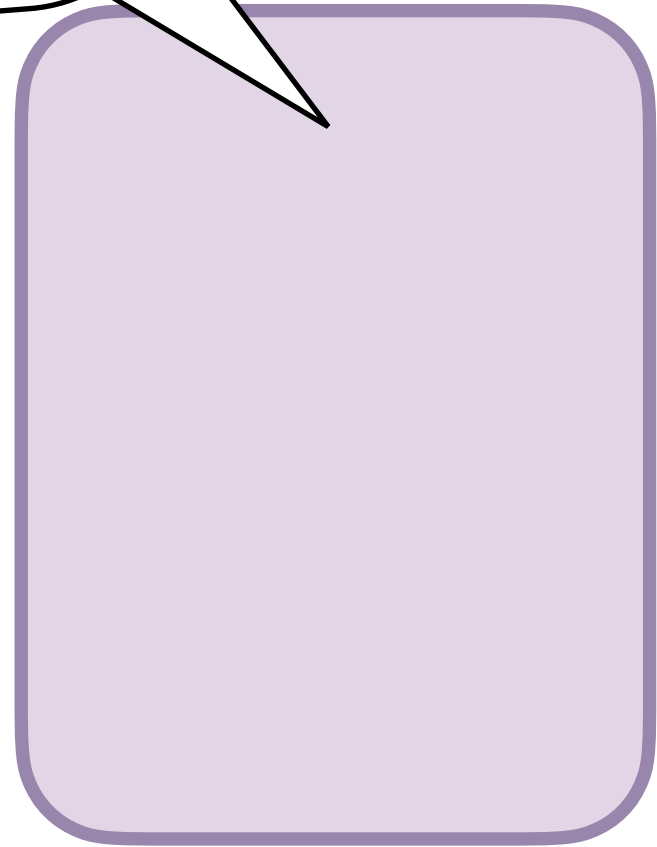
I am in  
all subnets!



I am in all subnets!

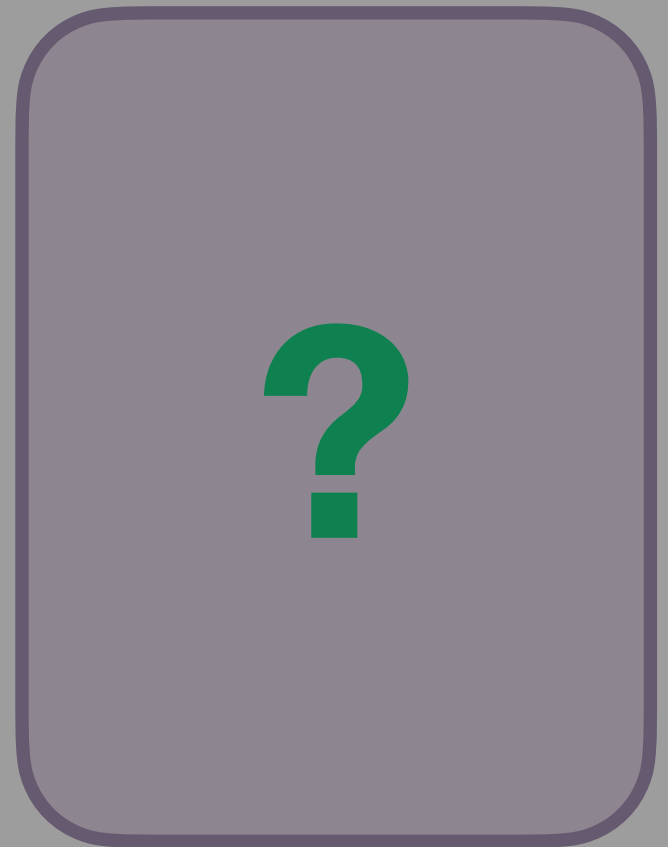
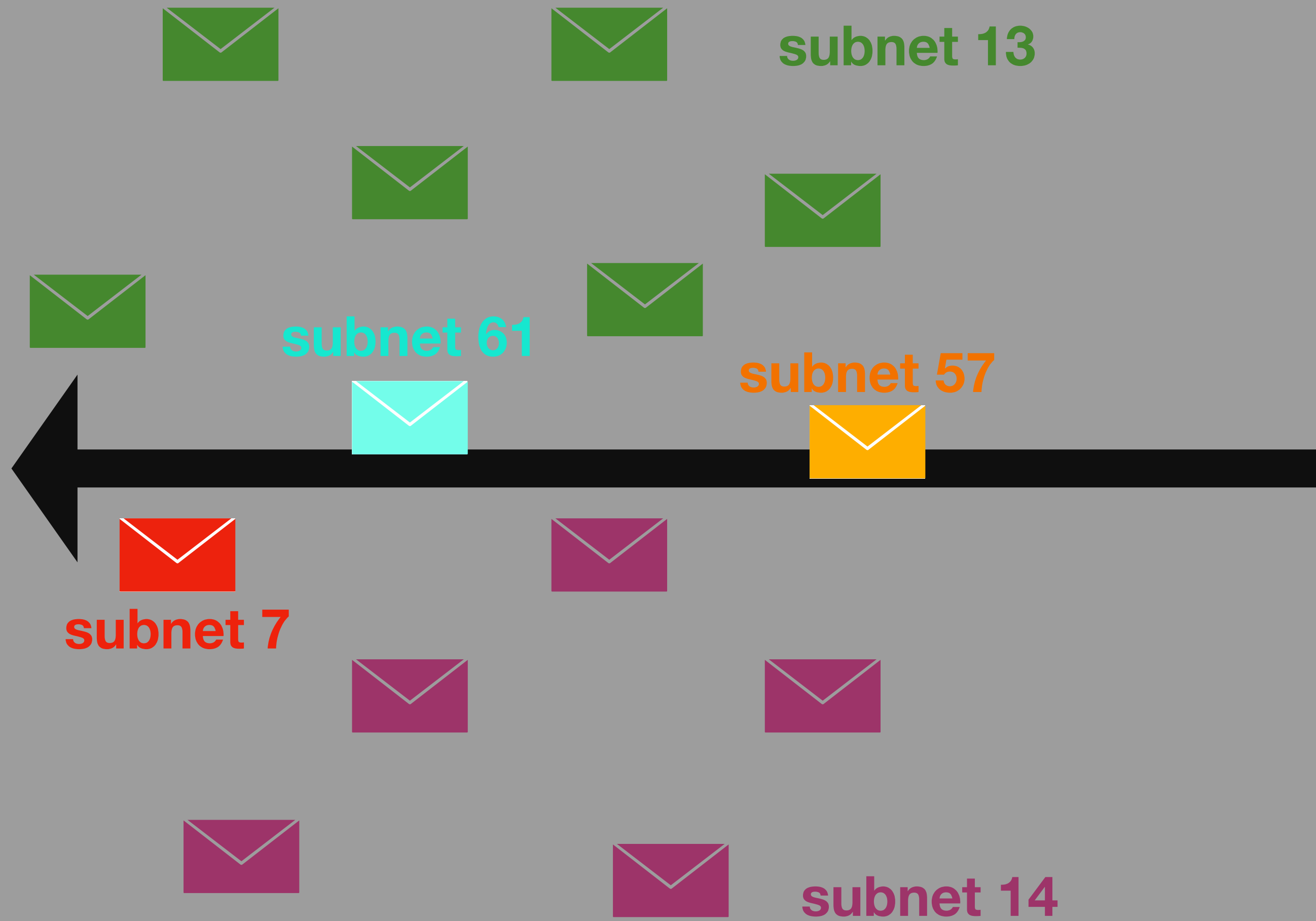
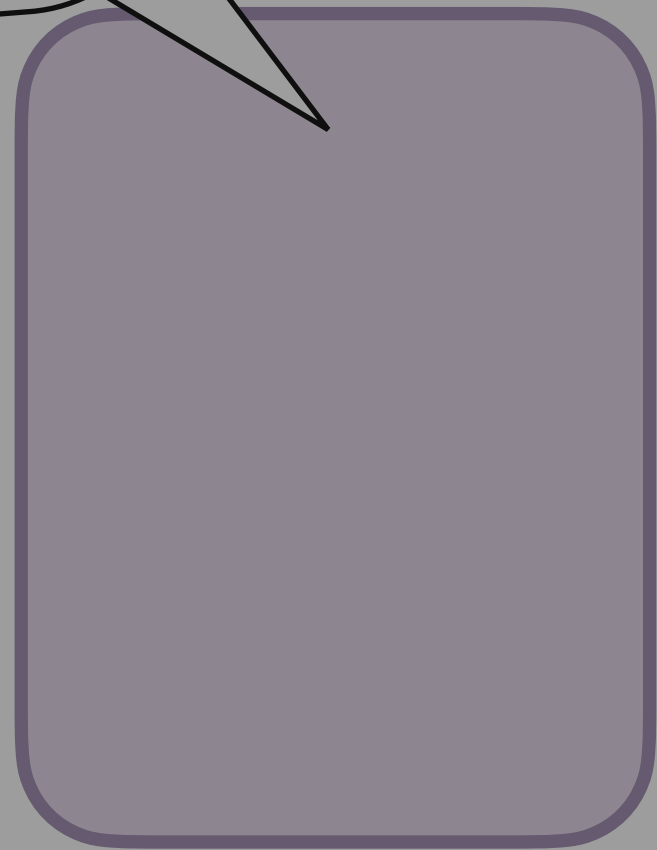


I am in all subnets!



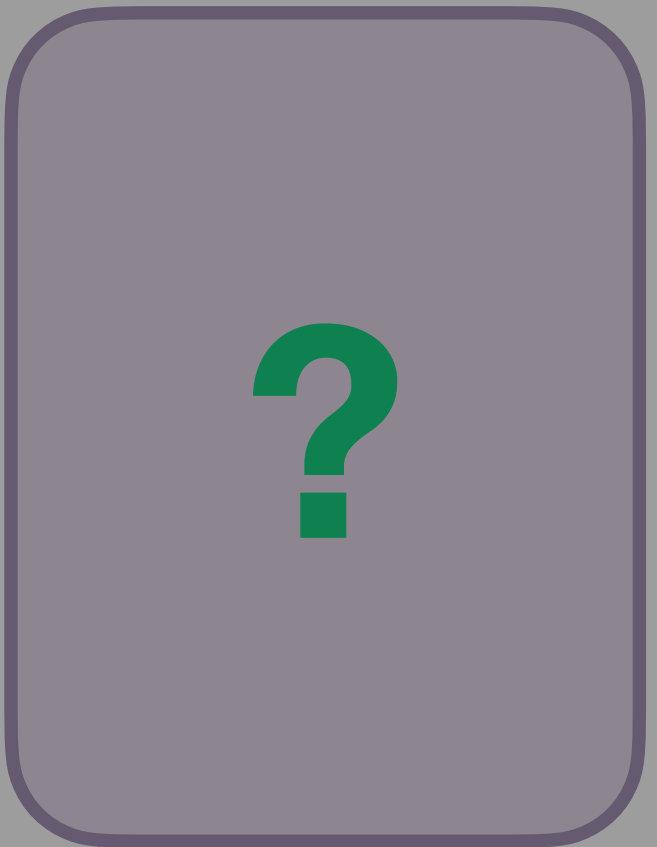
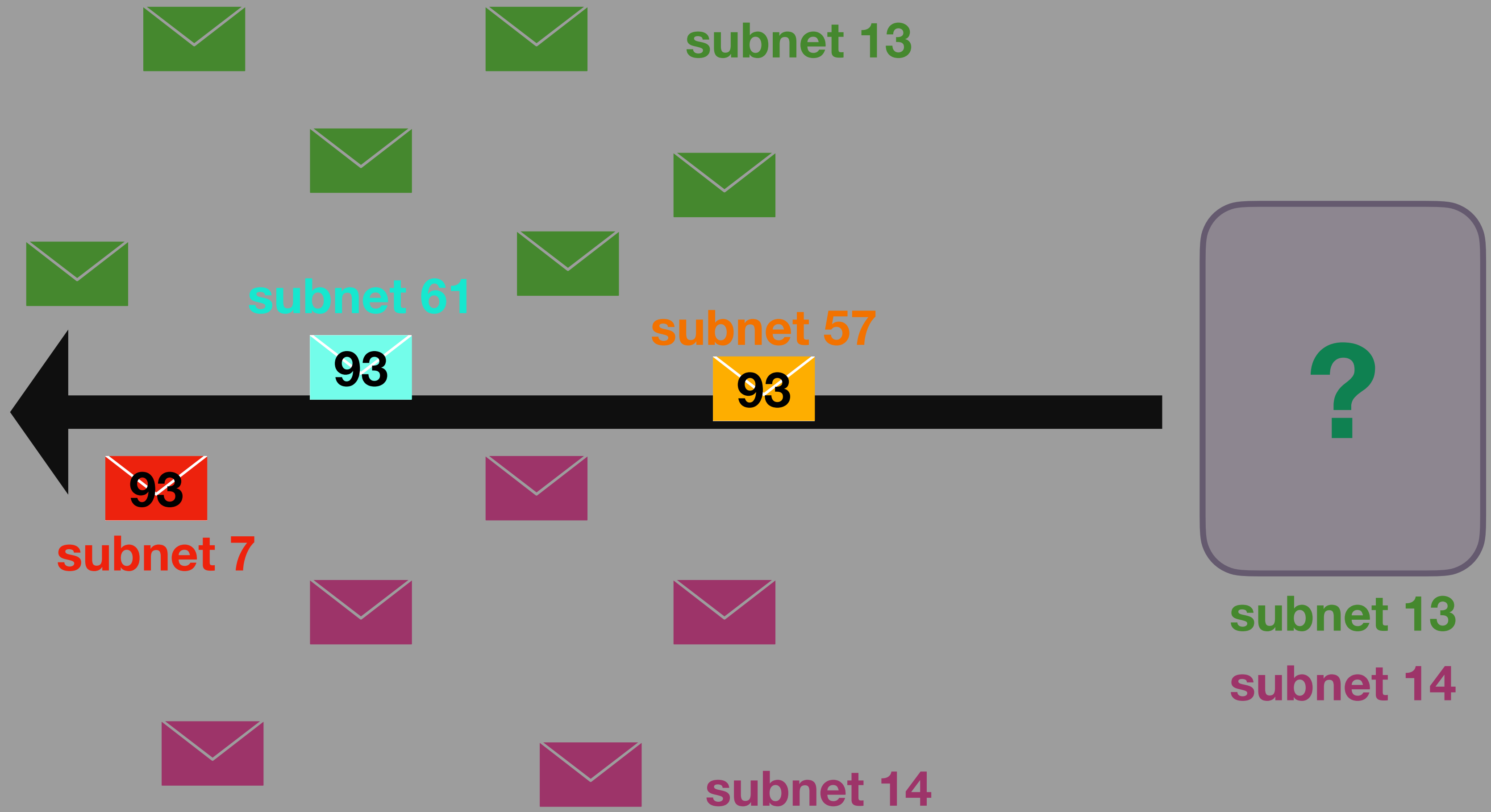
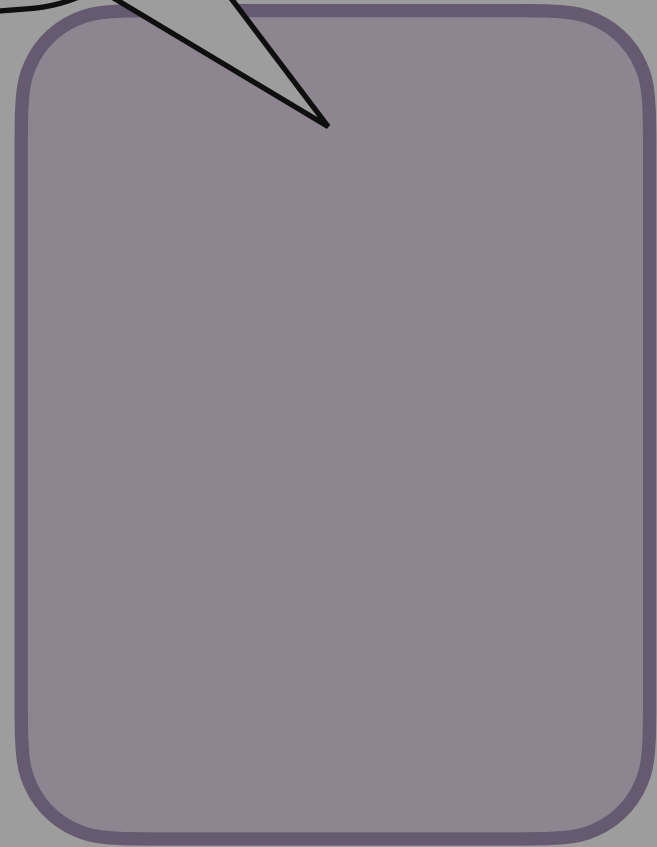
subnet 13  
subnet 14

I am in all subnets!



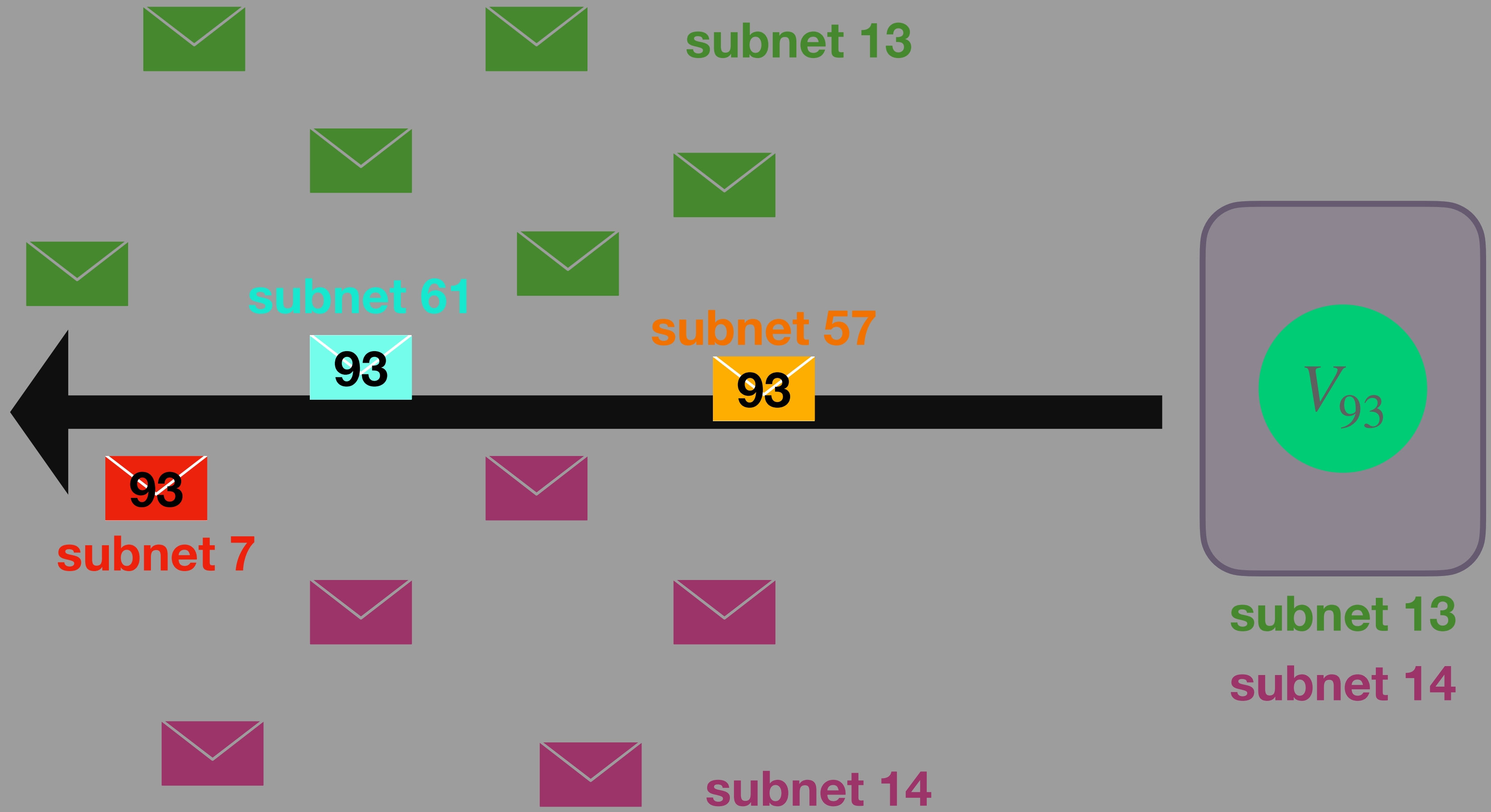
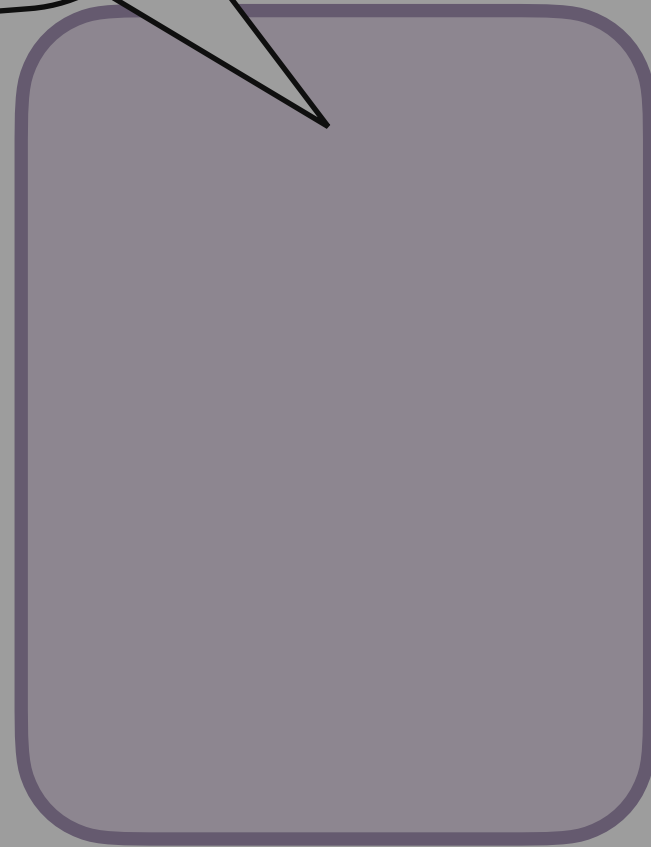
subnet 13  
subnet 14

I am in all subnets!



subnet 13  
subnet 14

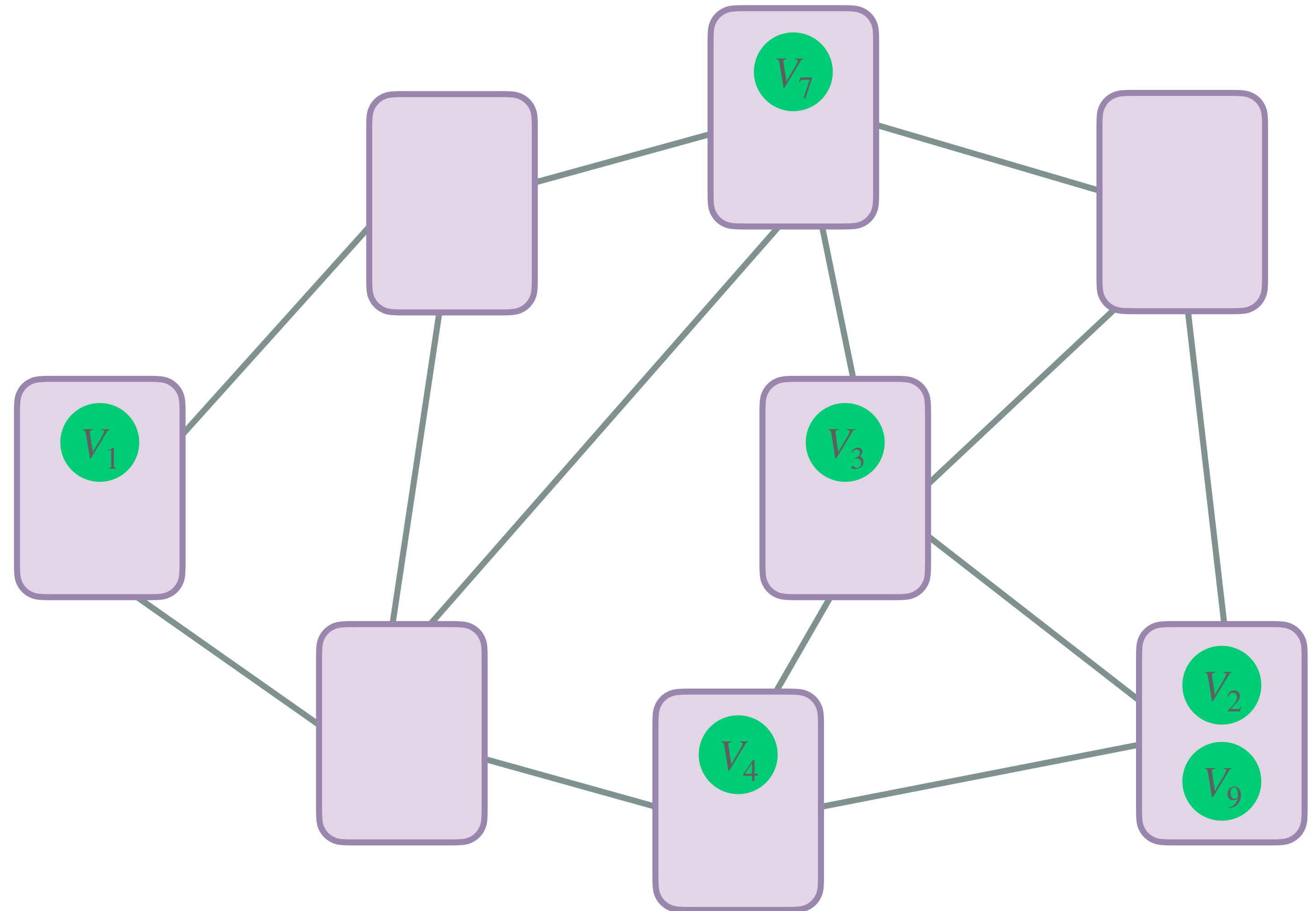
I am in all subnets!



# Mitigations

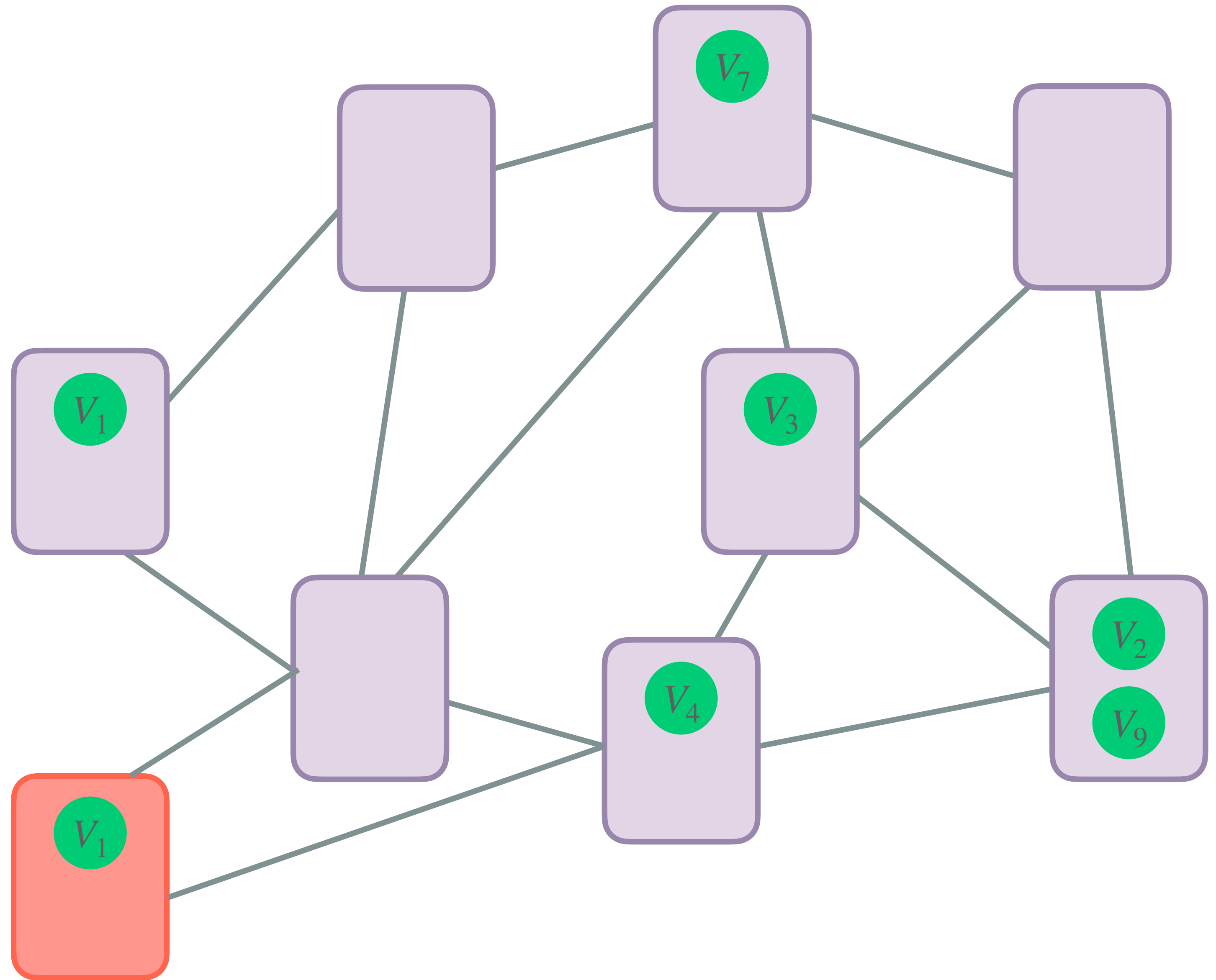
# Mitigations

## Additional Nodes



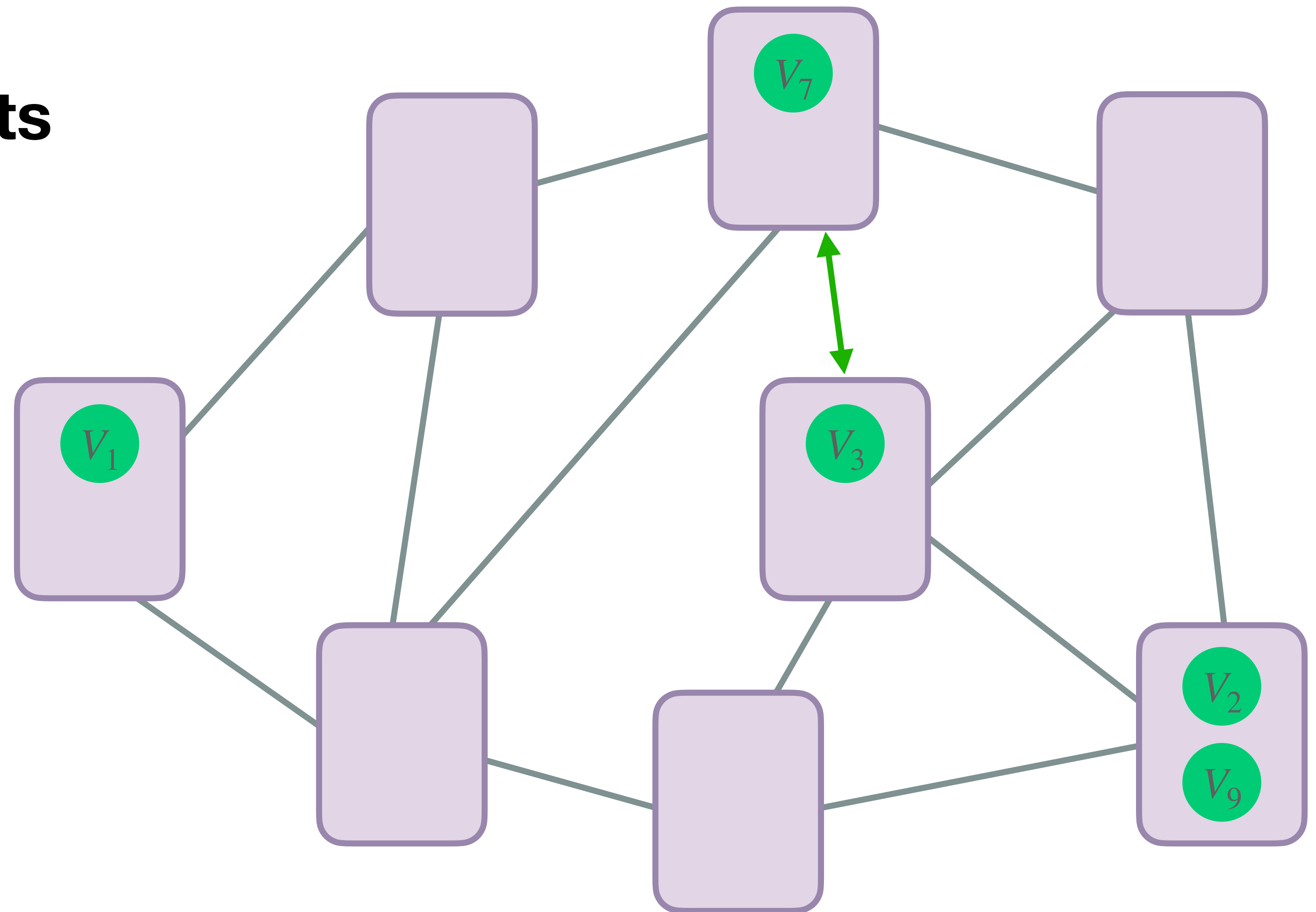
# Mitigations

## Additional Nodes



# Mitigations

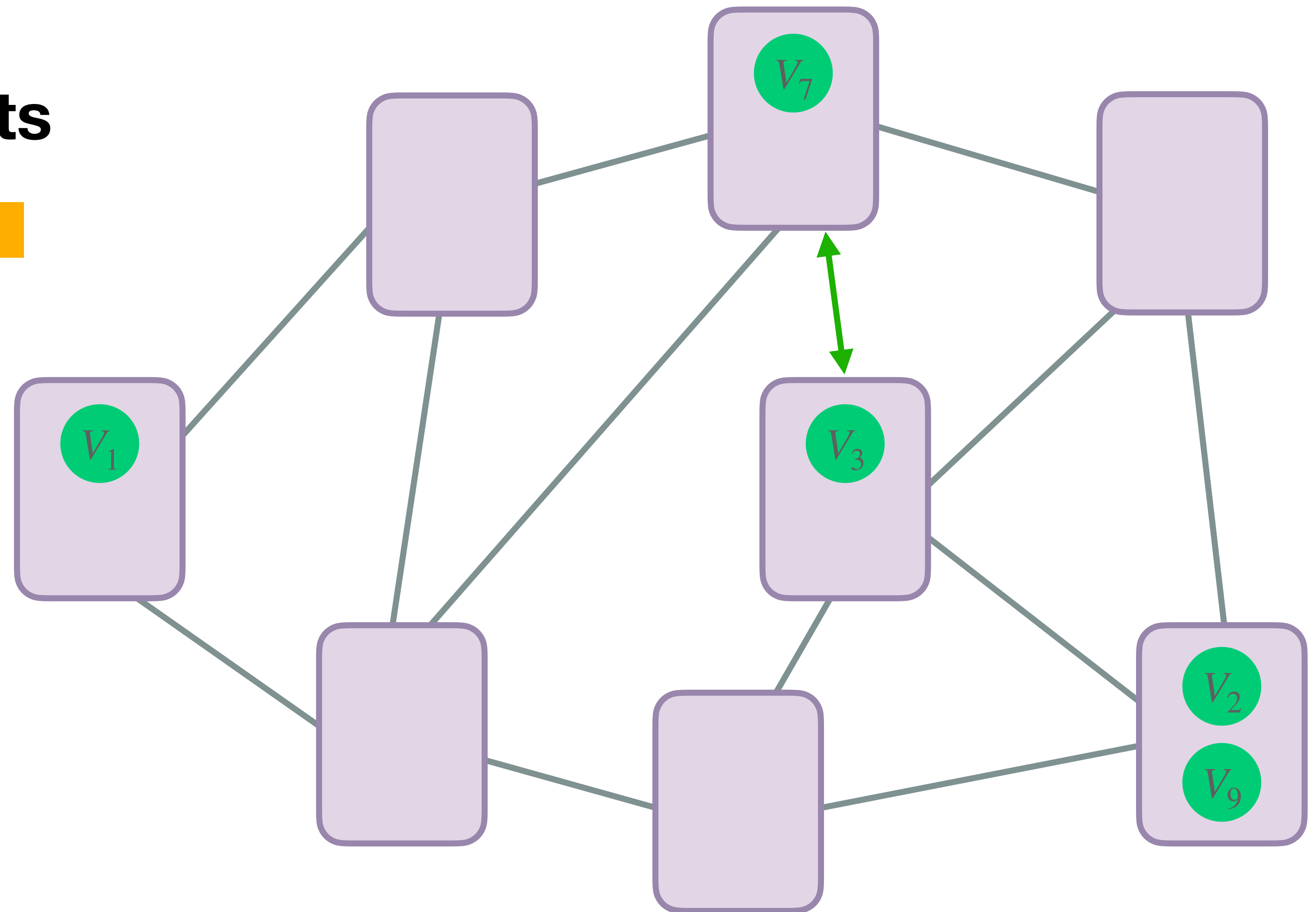
## Private Peering Agreements



# Mitigations

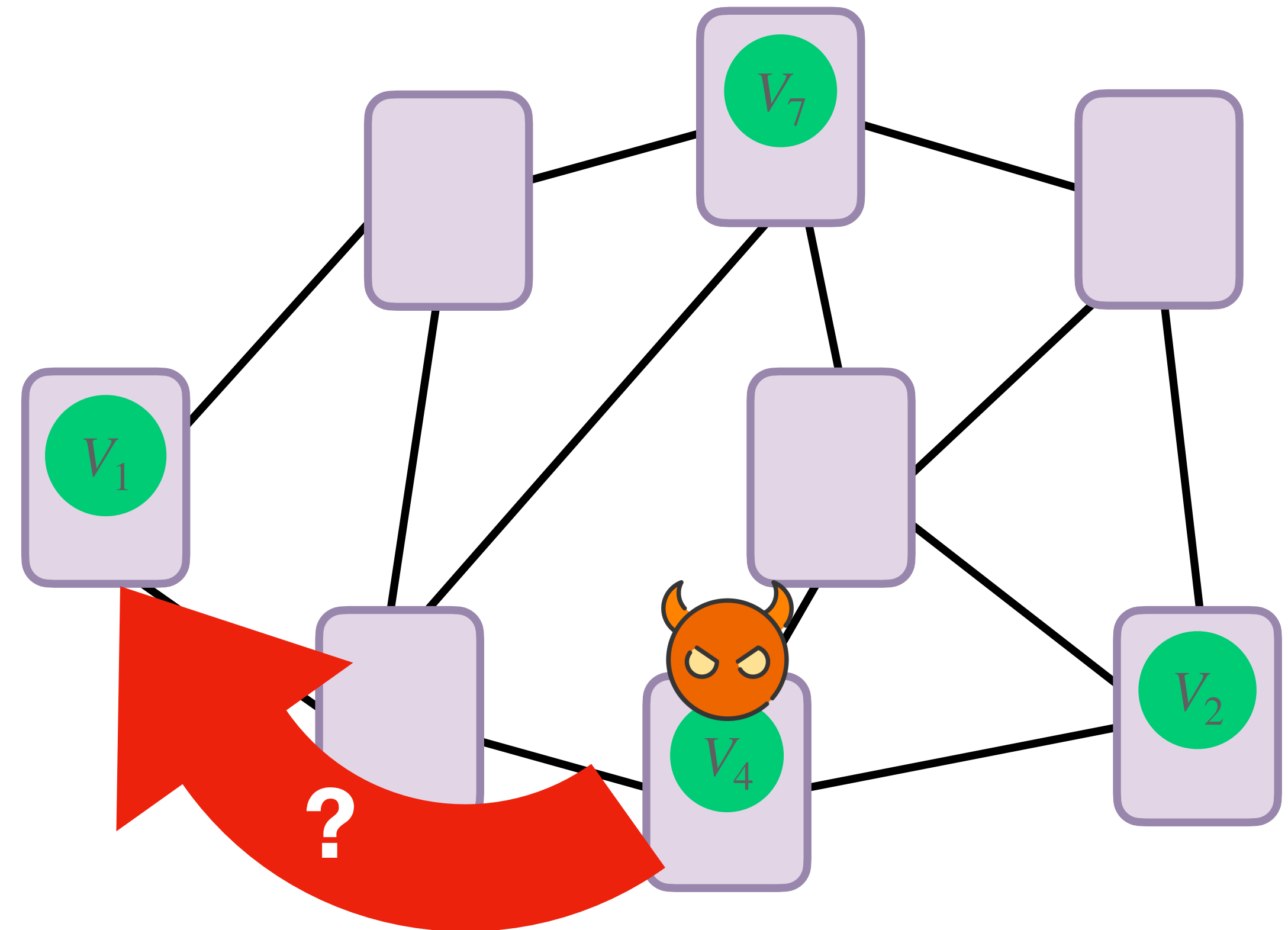
## Private Peering Agreements

k-Anonymity



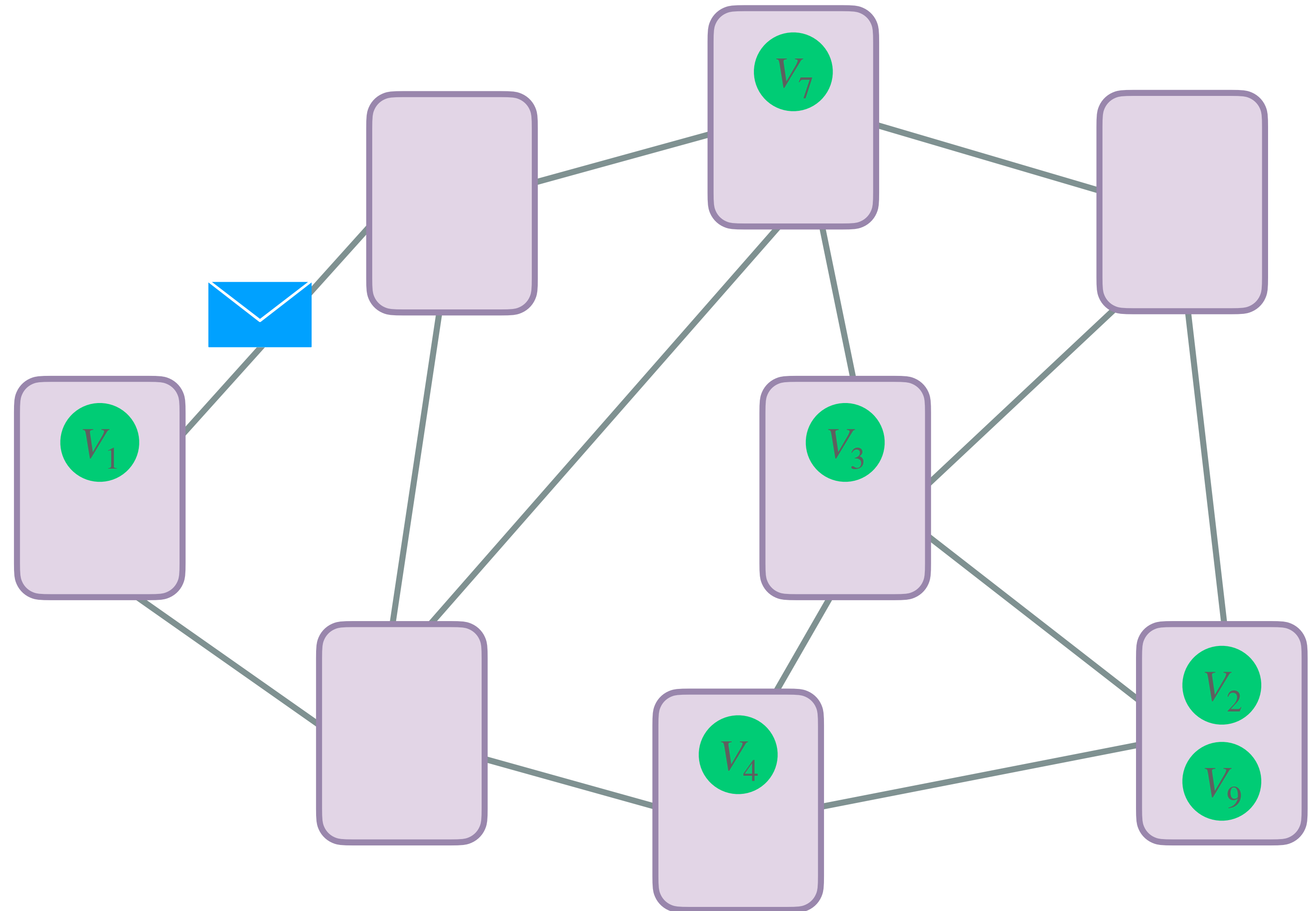
# Mitigations

## Secret Leader Election



# Mitigations

## Anonymous Broadcast



# Mitigations

## DoS Prevention

