VerLoc: Verifiable Localization in Decentralized Systems

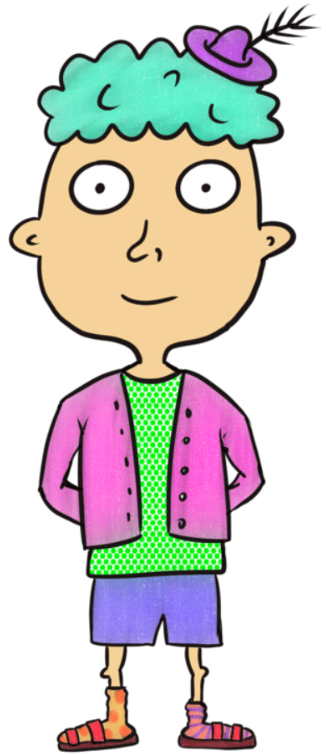
Claudia Diaz, imec-COSIC KU Leuven, Nym Technologies SA
Katharina Kohls, Radboud Universiteit Nijmegen

Radboud University

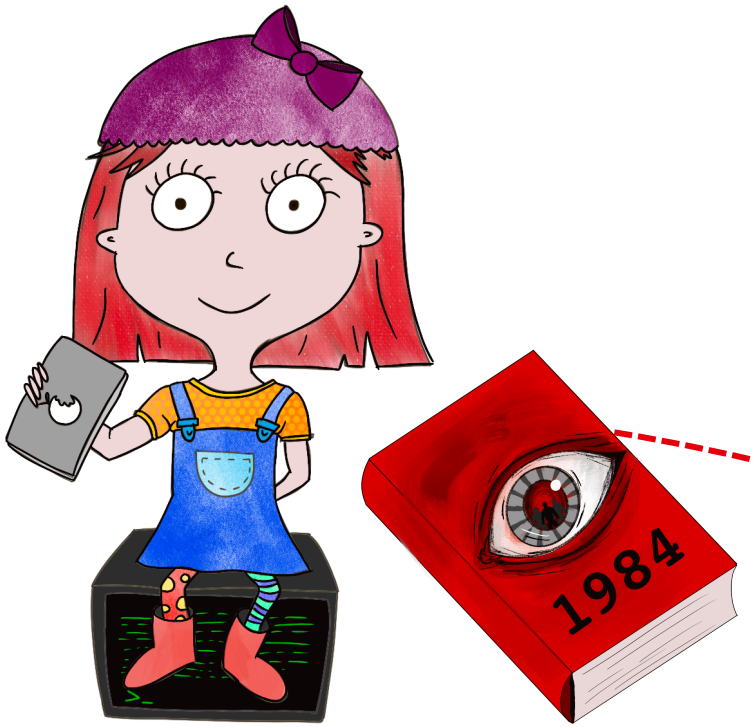
I want to send you this super special edition of 1984!

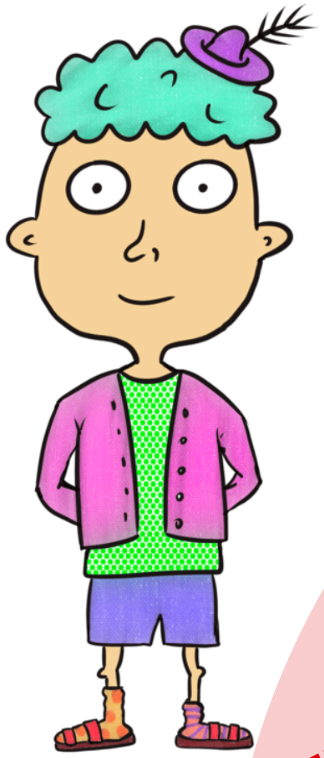
I want to send you this super special edition of 1984!

Send it to socks guy, he'll send it over to me.

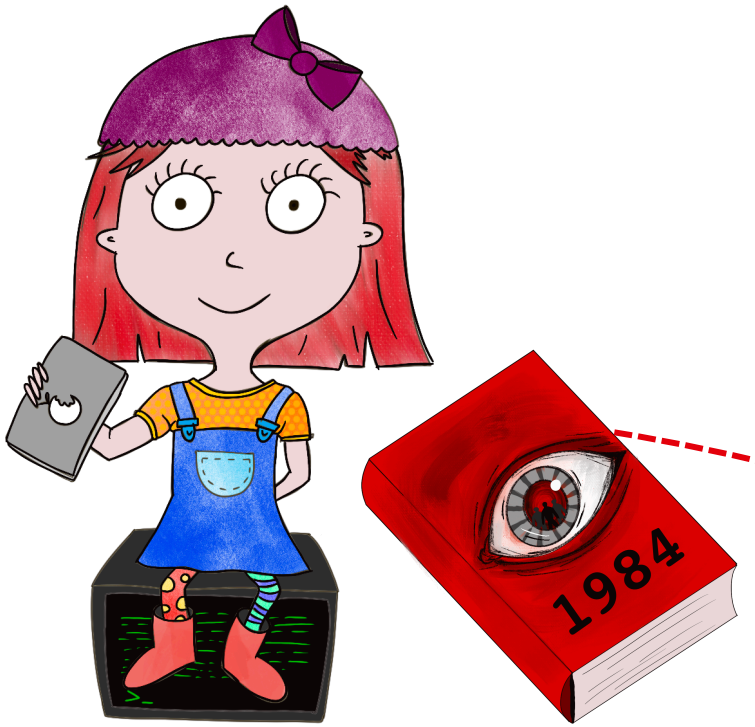


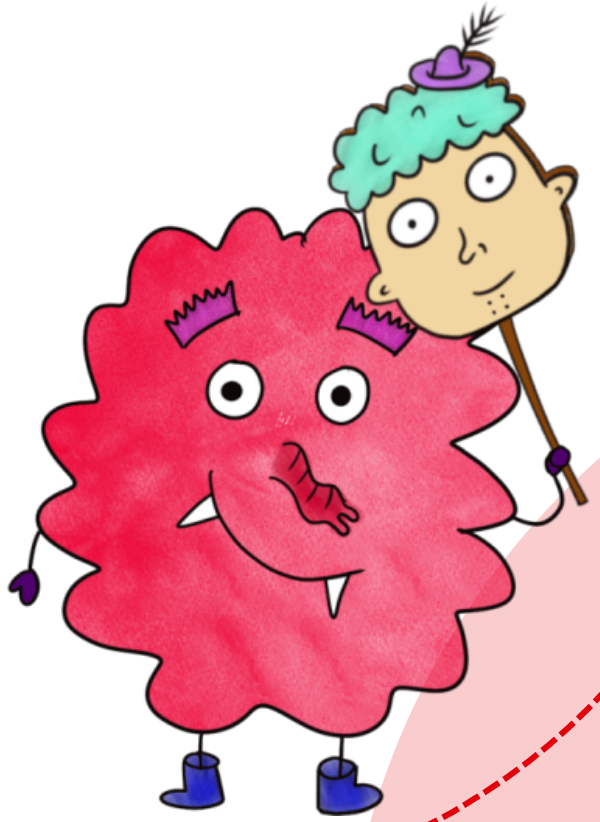
They need me because the book might get lost on the way. Evil town doesn‘t like it…

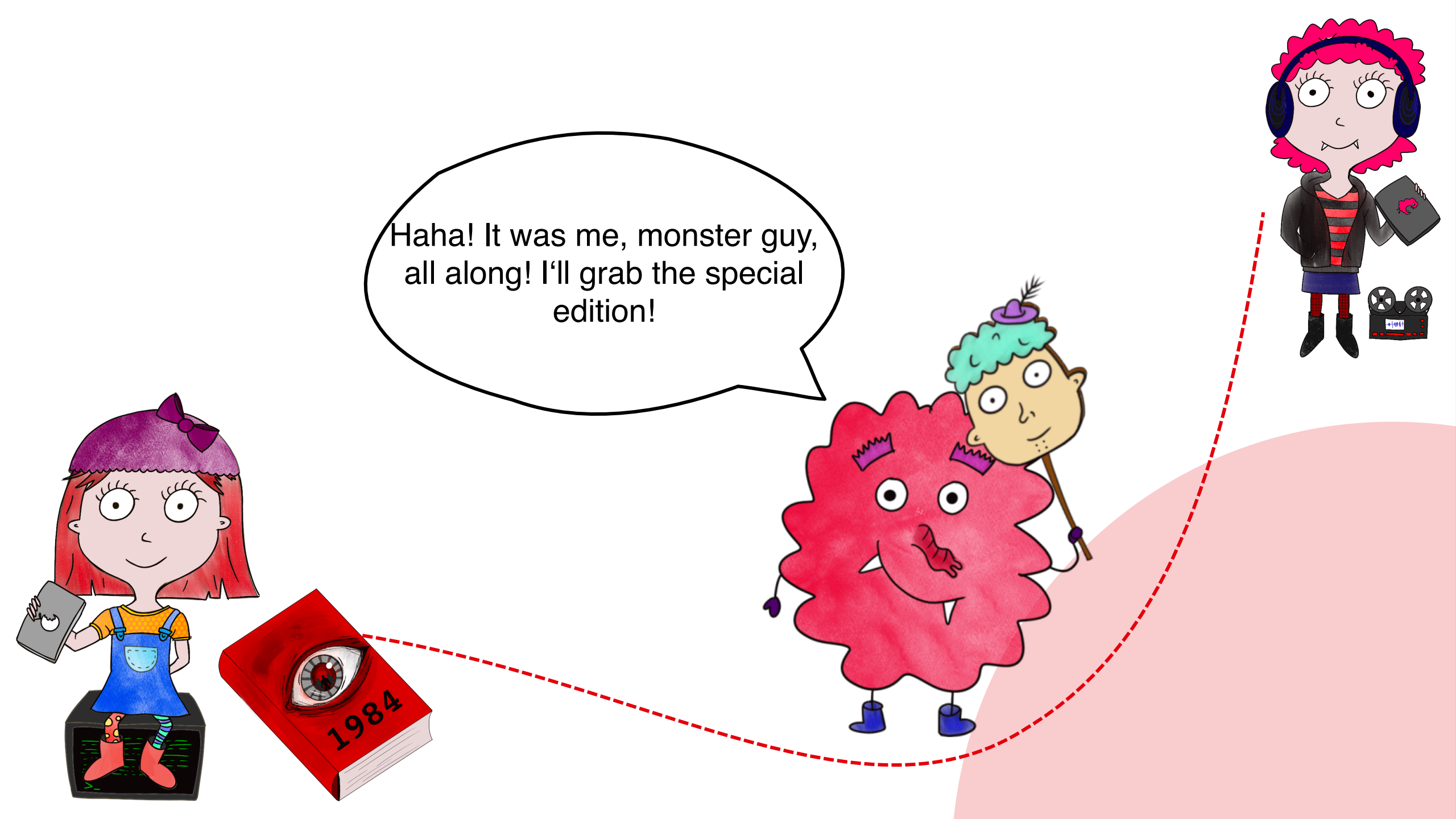




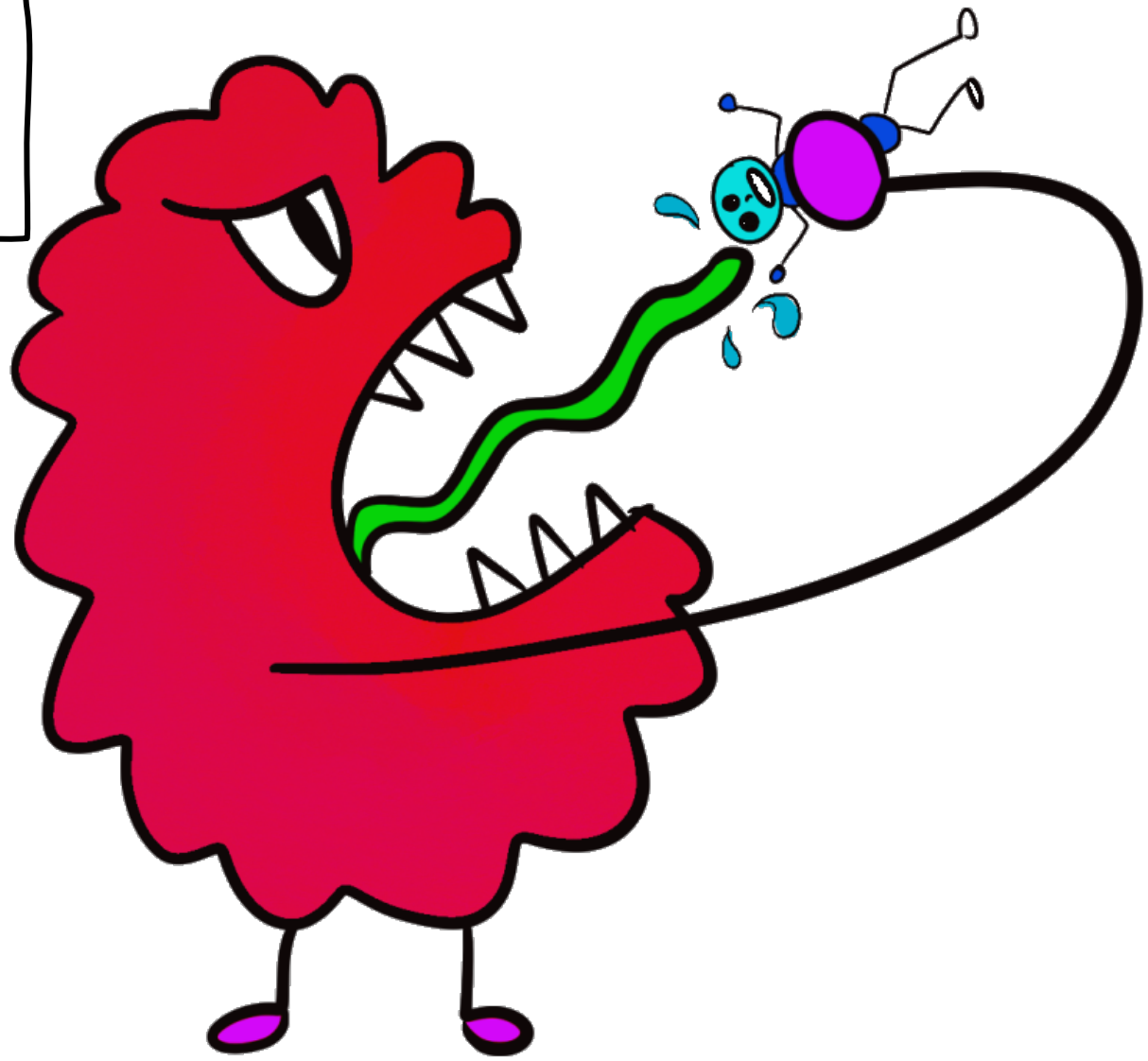
In the meantime…






Haha! It was me, monster guy, all along! I'll grab the special edition!
1984

Oh no!
Monster guy wins again!

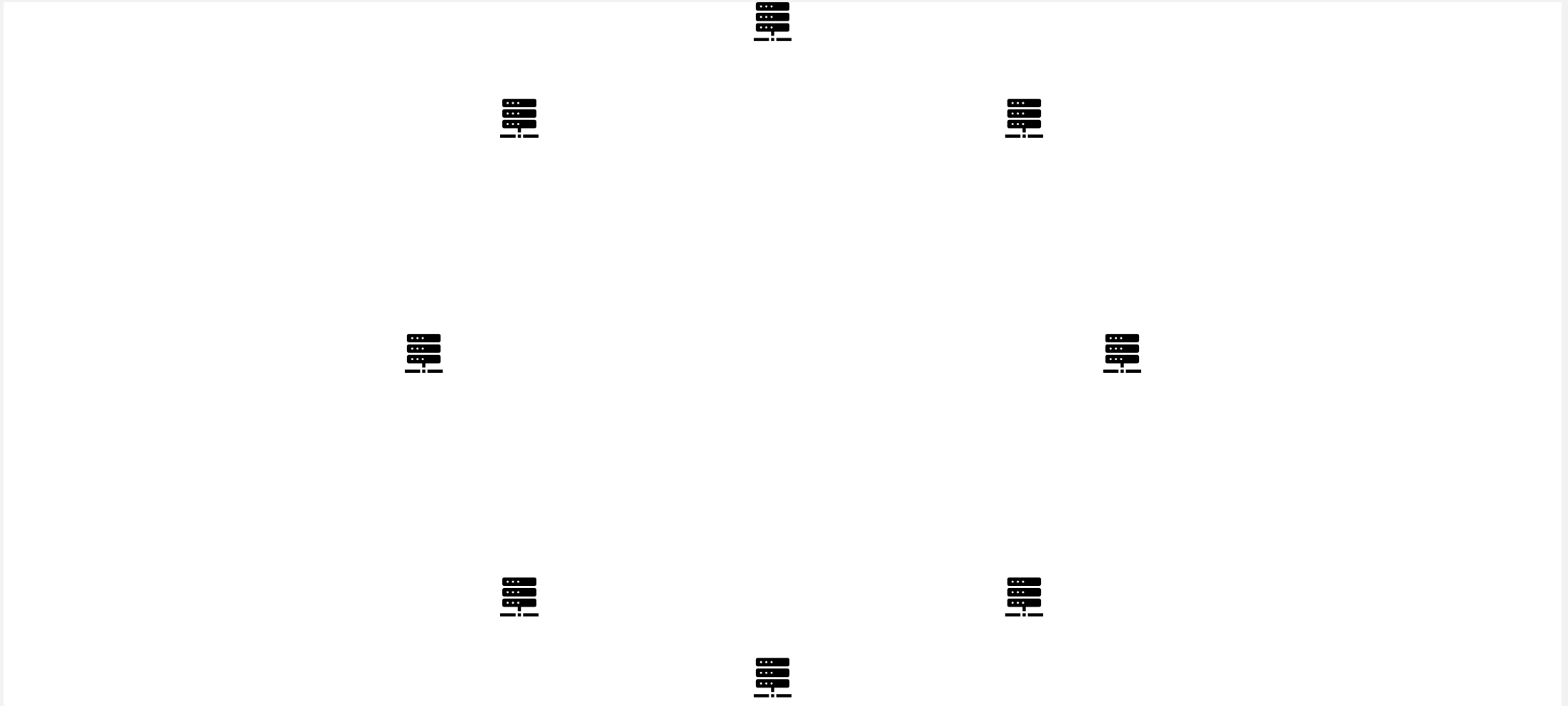


MOTIVATION

WORLDWIDE TRUST

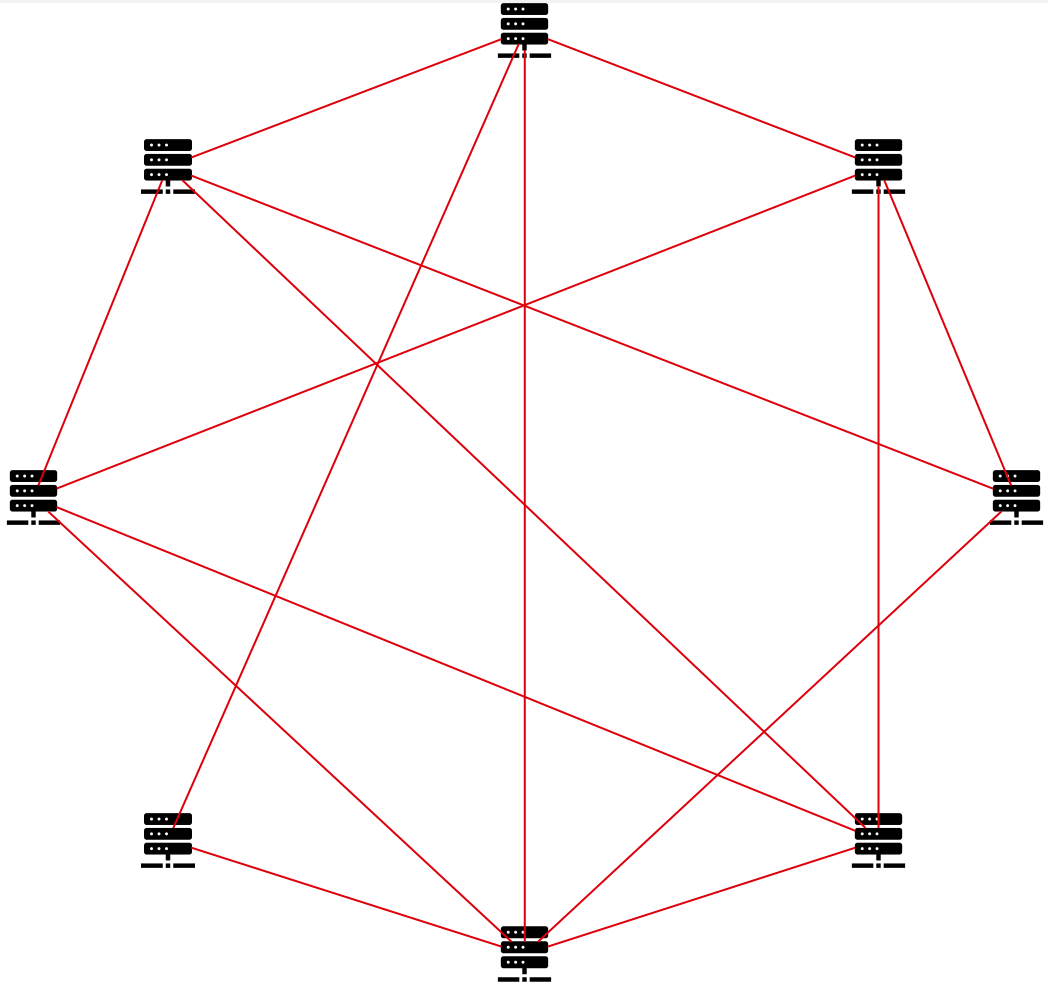
MOTIVATION

WORLDWIDE TRUST



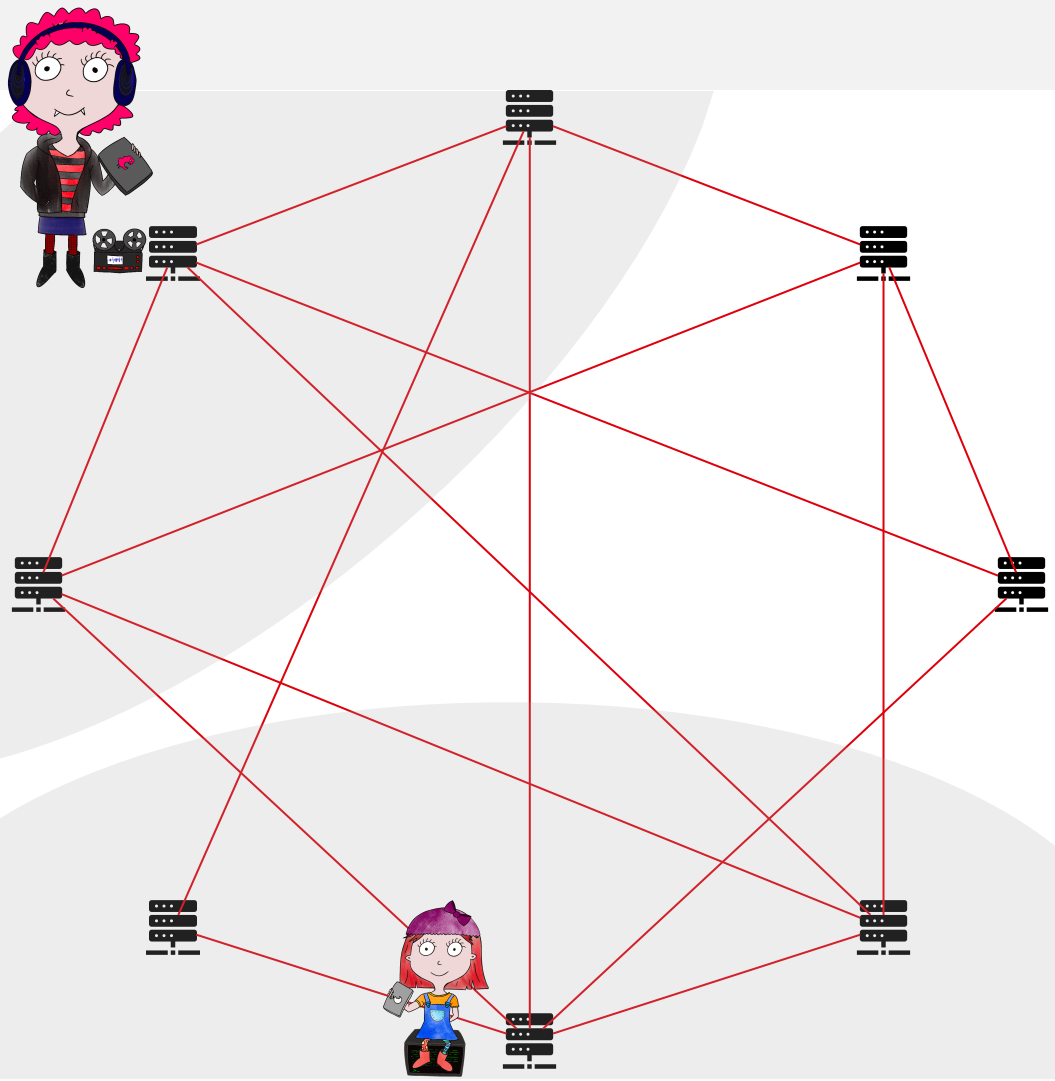
MOTIVATION

WORLDWIDE TRUST



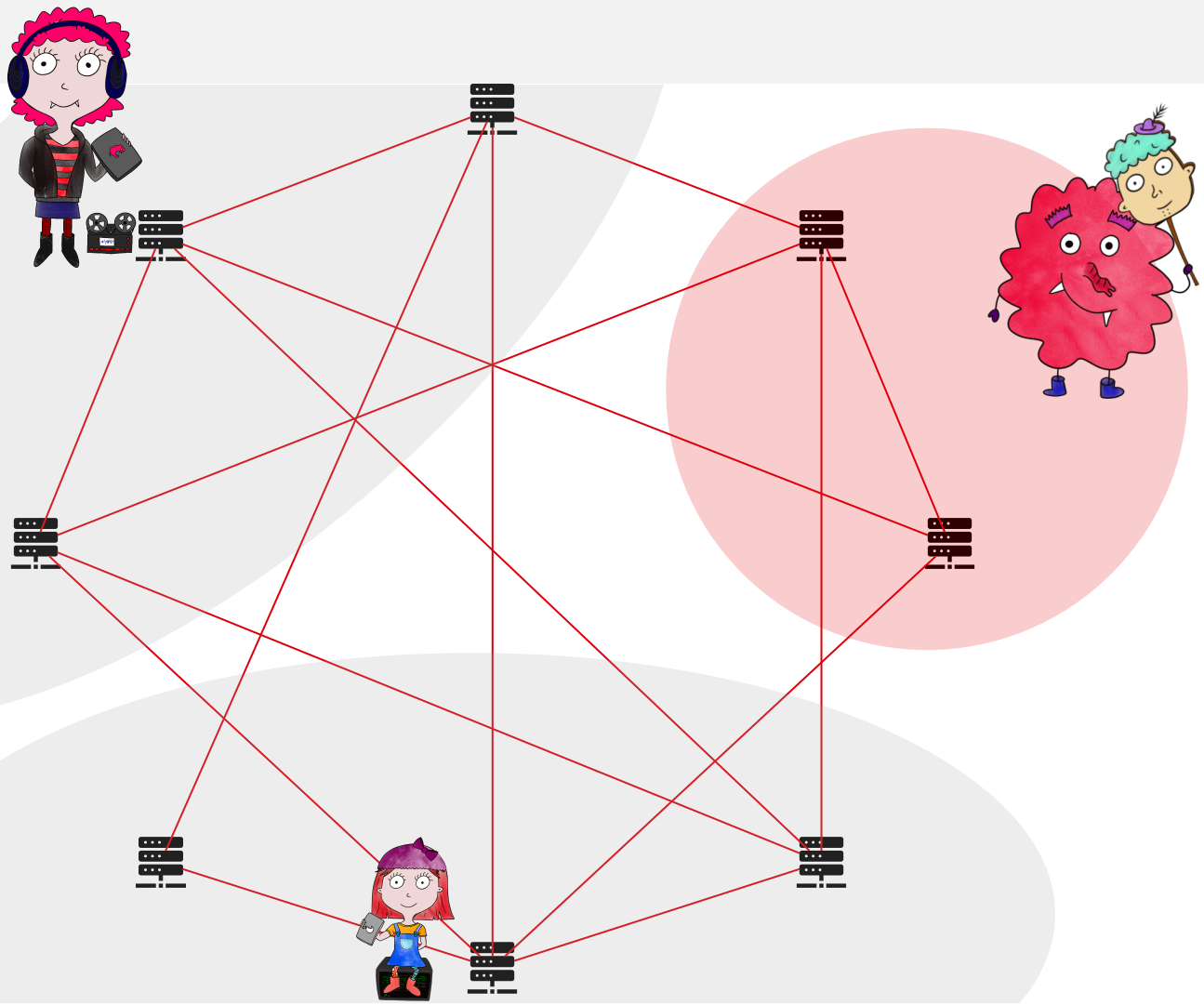
MOTIVATION

WORLDWIDE TRUST



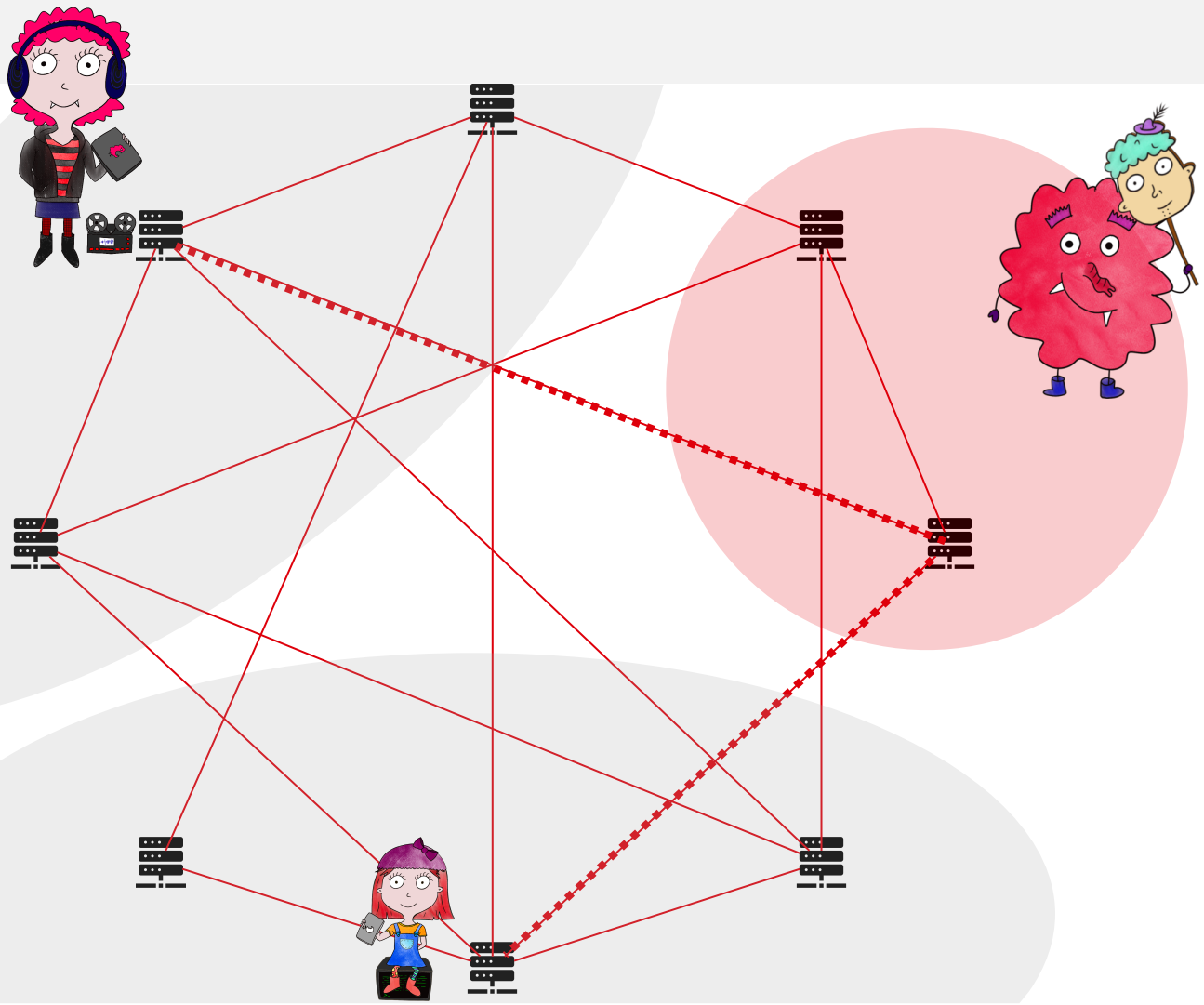
MOTIVATION

WORLDWIDE TRUST



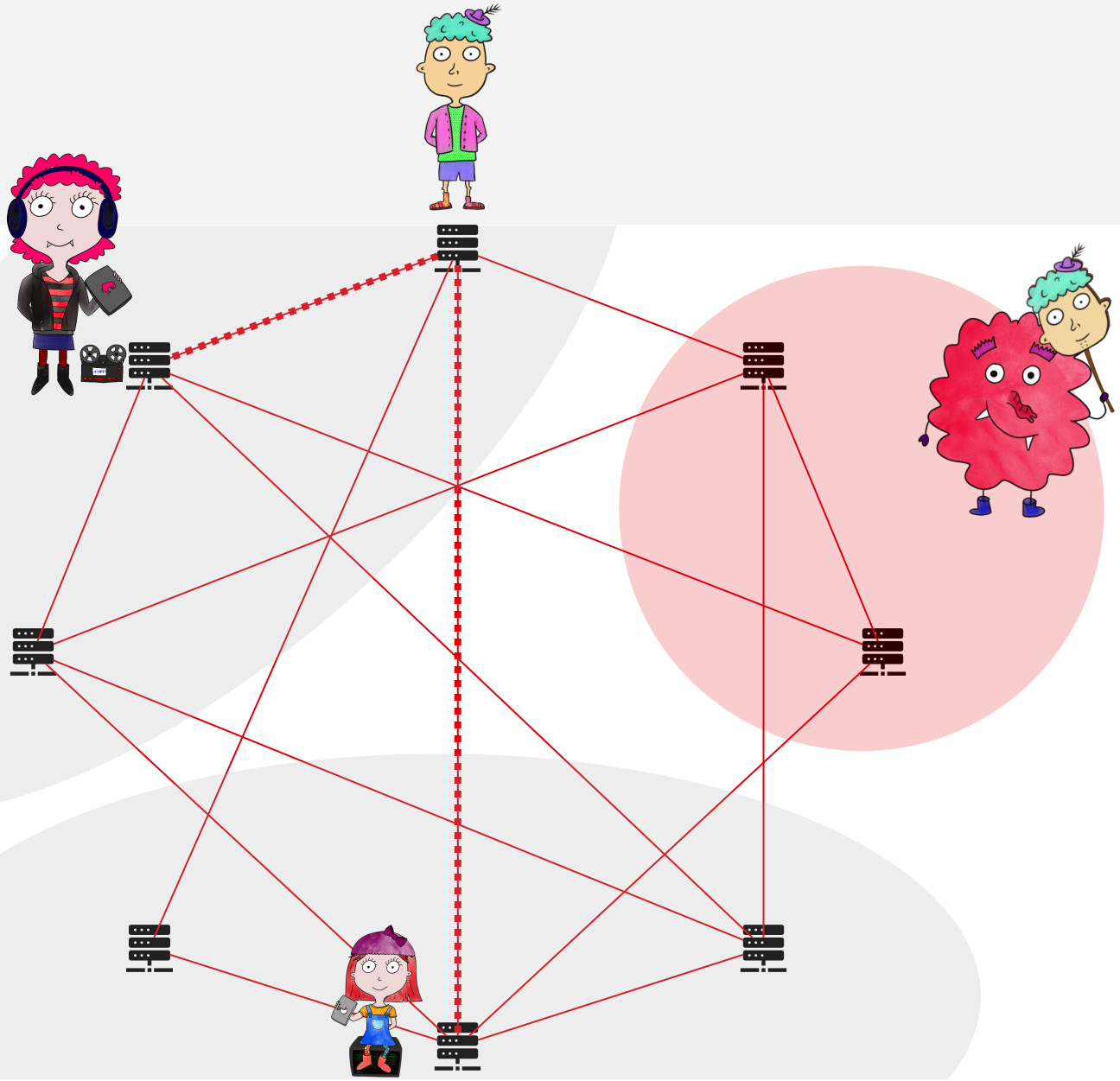
MOTIVATION

WORLDWIDE TRUST



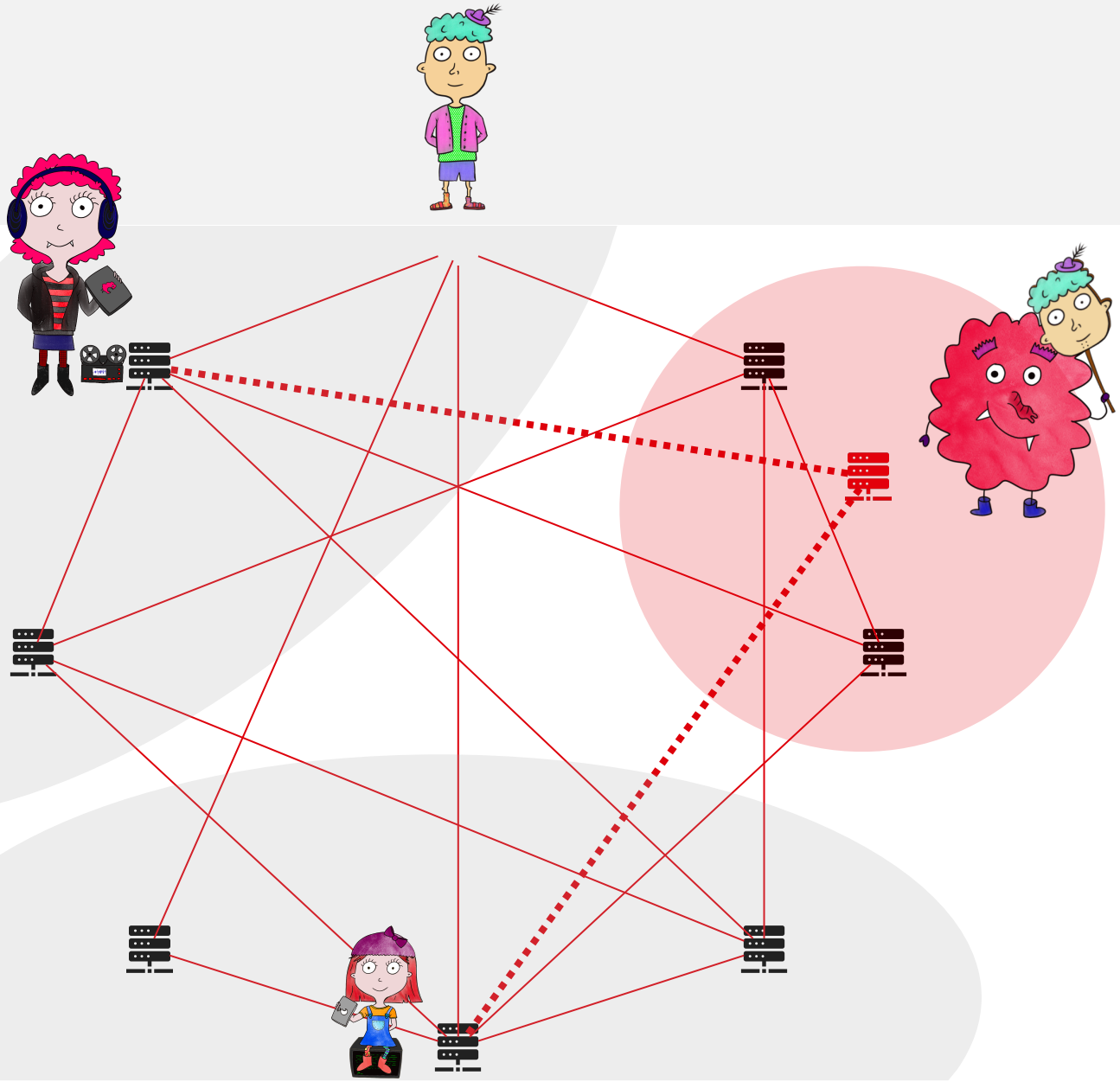
MOTIVATION

WORLDWIDE TRUST



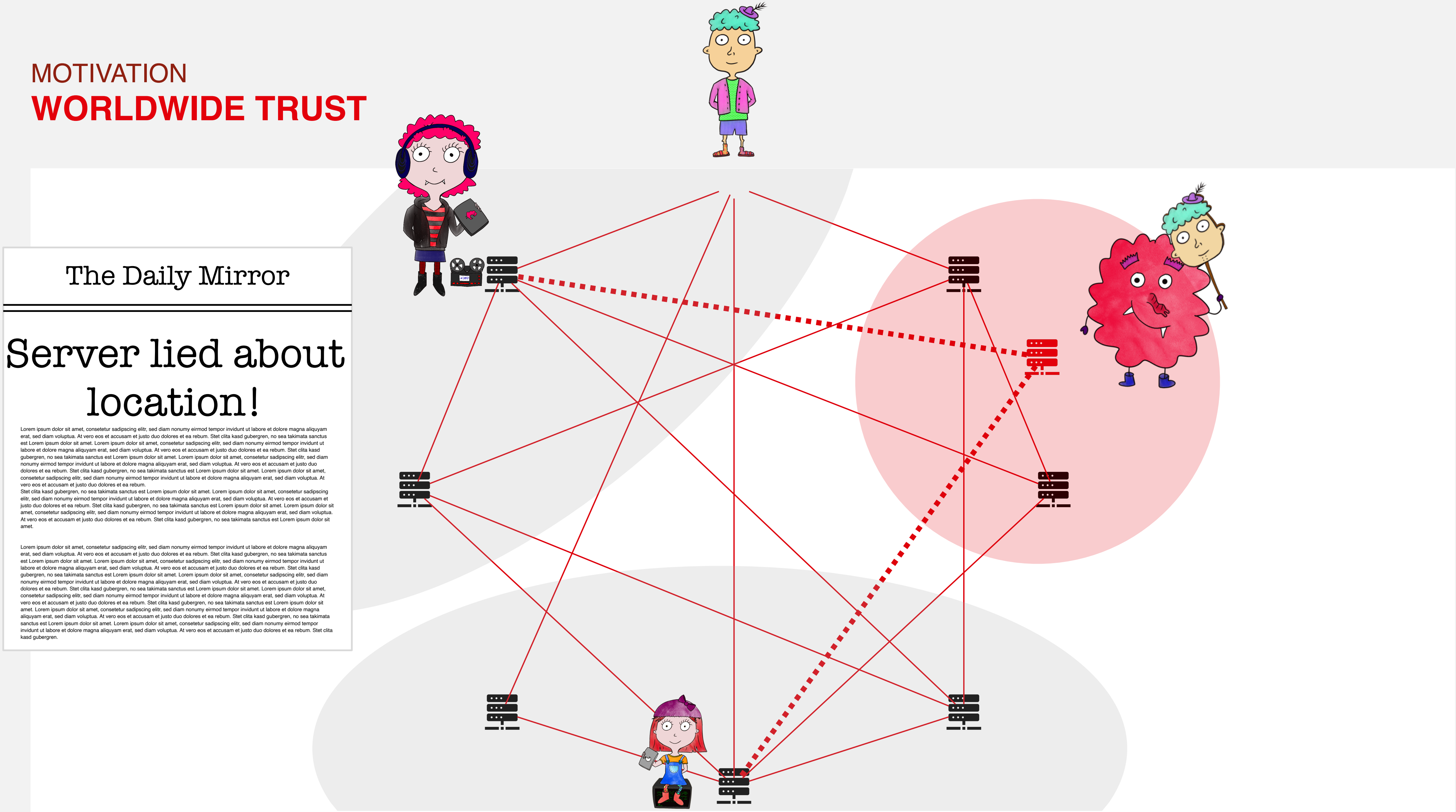
MOTIVATION

WORLDWIDE TRUST



MOTIVATION

WORLDWIDE TRUST



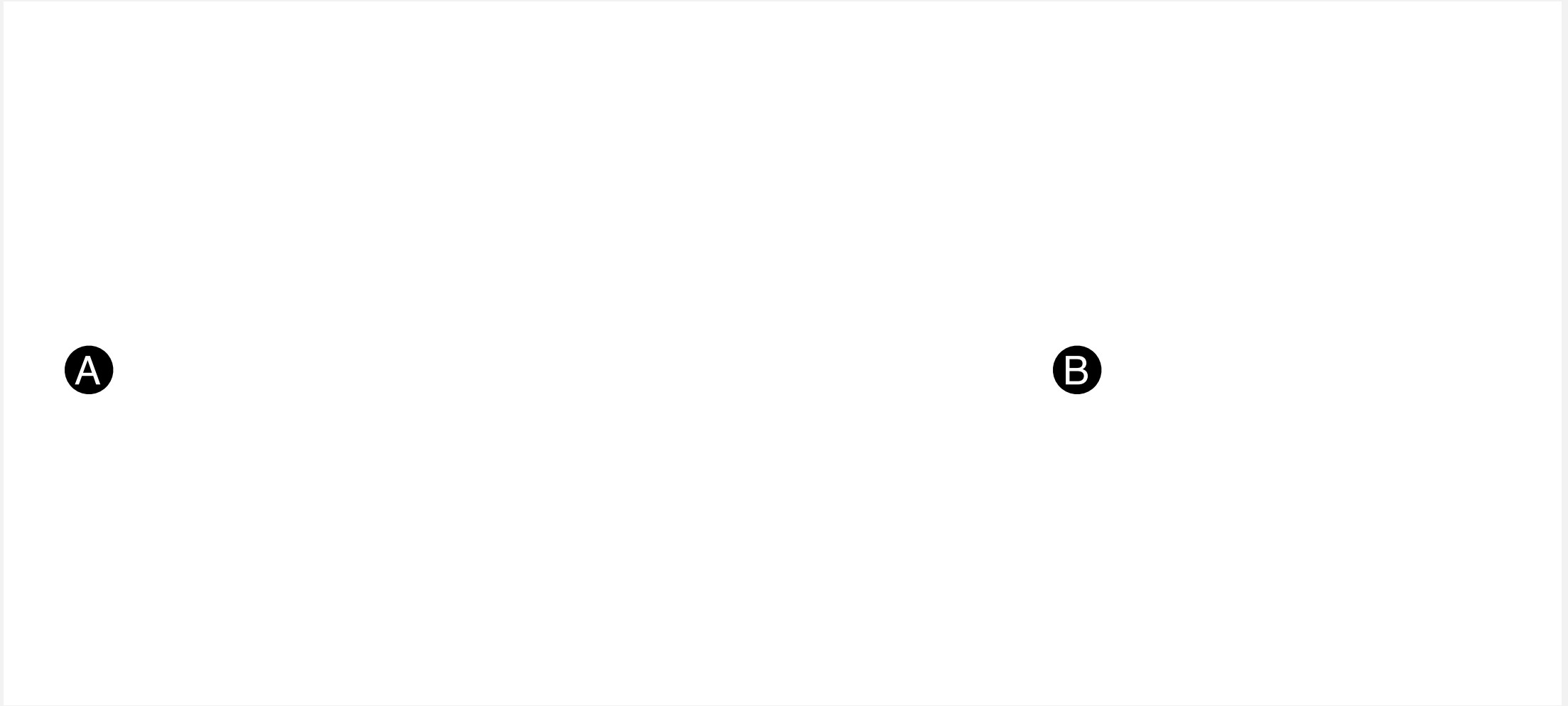
HOW CAN WE ACHIEVE THIS?

TODO:

1. **Localize** nodes (please no overhead)
2. **Verify** the results (prepare for trouble)
3. **Decentralize** all the things

TODO 1: LOCALIZE NODES

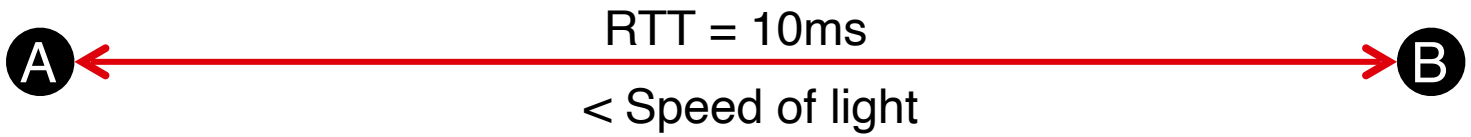
SPEED * TIME = DISTANCE



TODO 1: LOCALIZE NODES

SPEED * TIME = DISTANCE

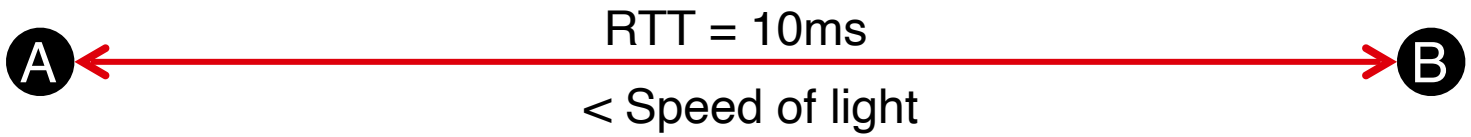
```
ping google.com                                                    ⌥⌘1
→  ~ ping google.com
PING google.com (142.251.39.110): 56 data bytes
64 bytes from 142.251.39.110: icmp_seq=0 ttl=115 time=17.655 ms
64 bytes from 142.251.39.110: icmp_seq=1 ttl=115 time=5.889 ms
64 bytes from 142.251.39.110: icmp_seq=2 ttl=115 time=7.468 ms
64 bytes from 142.251.39.110: icmp_seq=3 ttl=115 time=20.249 ms
64 bytes from 142.251.39.110: icmp_seq=4 ttl=115 time=5.580 ms
64 bytes from 142.251.39.110: icmp_seq=5 ttl=115 time=5.851 ms
64 bytes from 142.251.39.110: icmp_seq=6 ttl=115 time=5.735 ms
64 bytes from 142.251.39.110: icmp_seq=7 ttl=115 time=31.046 ms
64 bytes from 142.251.39.110: icmp_seq=8 ttl=115 time=78.711 ms
```



TODO 1: LOCALIZE NODES

SPEED * TIME = DISTANCE

$$speed * time = distance$$



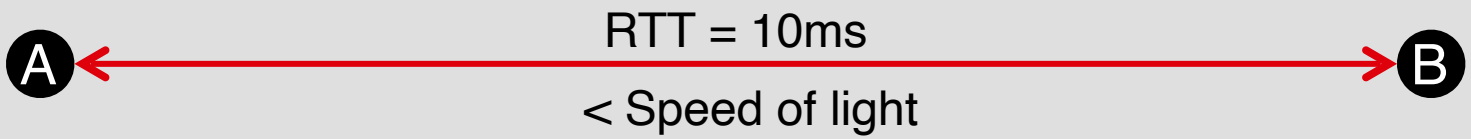

```
ping google.com                                                    ⌥⌘1
→  ~ ping google.com
PING google.com (142.251.39.110): 56 data bytes
64 bytes from 142.251.39.110: icmp_seq=0 ttl=115 time=17.655 ms
64 bytes from 142.251.39.110: icmp_seq=1 ttl=115 time=5.889 ms
64 bytes from 142.251.39.110: icmp_seq=2 ttl=115 time=7.468 ms
64 bytes from 142.251.39.110: icmp_seq=3 ttl=115 time=20.249 ms
64 bytes from 142.251.39.110: icmp_seq=4 ttl=115 time=5.580 ms
64 bytes from 142.251.39.110: icmp_seq=5 ttl=115 time=5.851 ms
64 bytes from 142.251.39.110: icmp_seq=6 ttl=115 time=5.735 ms
64 bytes from 142.251.39.110: icmp_seq=7 ttl=115 time=31.046 ms
64 bytes from 142.251.39.110: icmp_seq=8 ttl=115 time=78.711 ms
```

TODO 1: LOCALIZE NODES

SPEED * TIME = DISTANCE

$$speed * time = distance$$

$$c * 10ms = 2998km$$

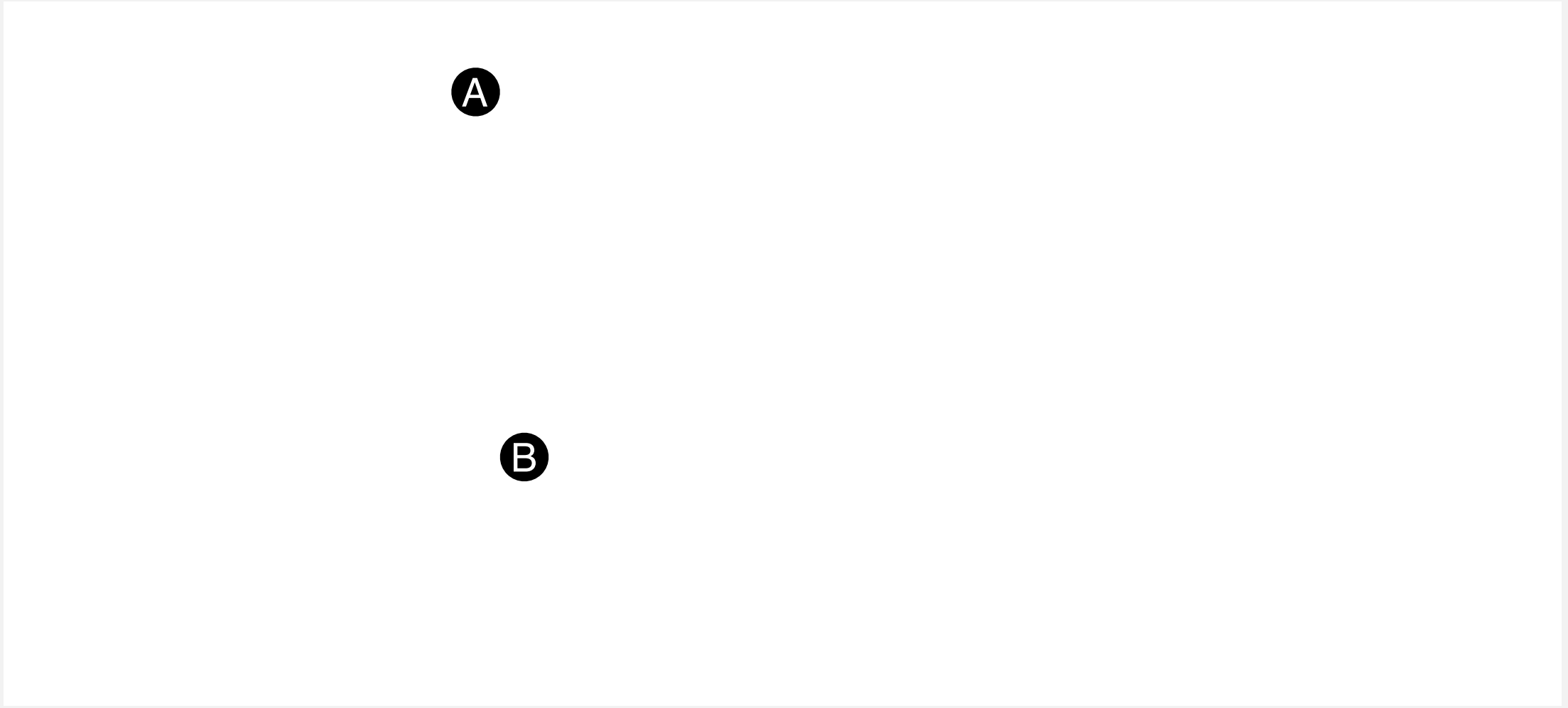


ping google.com ⌥⌘1

```
→  ~ ping google.com
PING google.com (142.251.39.110): 56 data bytes
64 bytes from 142.251.39.110: icmp_seq=0 ttl=115 time=17.655 ms
64 bytes from 142.251.39.110: icmp_seq=1 ttl=115 time=5.889 ms
64 bytes from 142.251.39.110: icmp_seq=2 ttl=115 time=7.468 ms
64 bytes from 142.251.39.110: icmp_seq=3 ttl=115 time=20.249 ms
64 bytes from 142.251.39.110: icmp_seq=4 ttl=115 time=5.580 ms
64 bytes from 142.251.39.110: icmp_seq=5 ttl=115 time=5.851 ms
64 bytes from 142.251.39.110: icmp_seq=6 ttl=115 time=5.735 ms
64 bytes from 142.251.39.110: icmp_seq=7 ttl=115 time=31.046 ms
64 bytes from 142.251.39.110: icmp_seq=8 ttl=115 time=78.711 ms
```

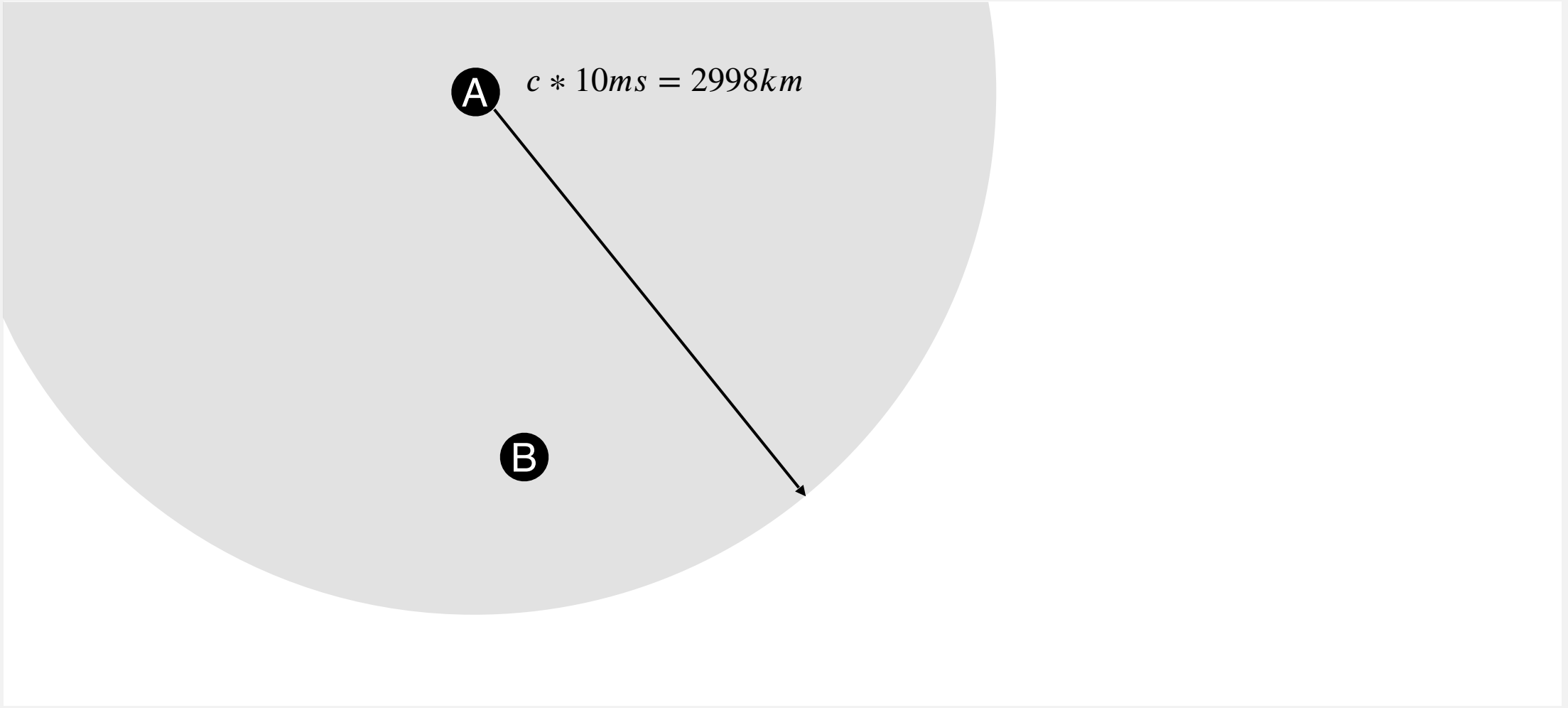
TODO 1: LOCALIZE NODES

TIMING-BASED LOCALIZATION



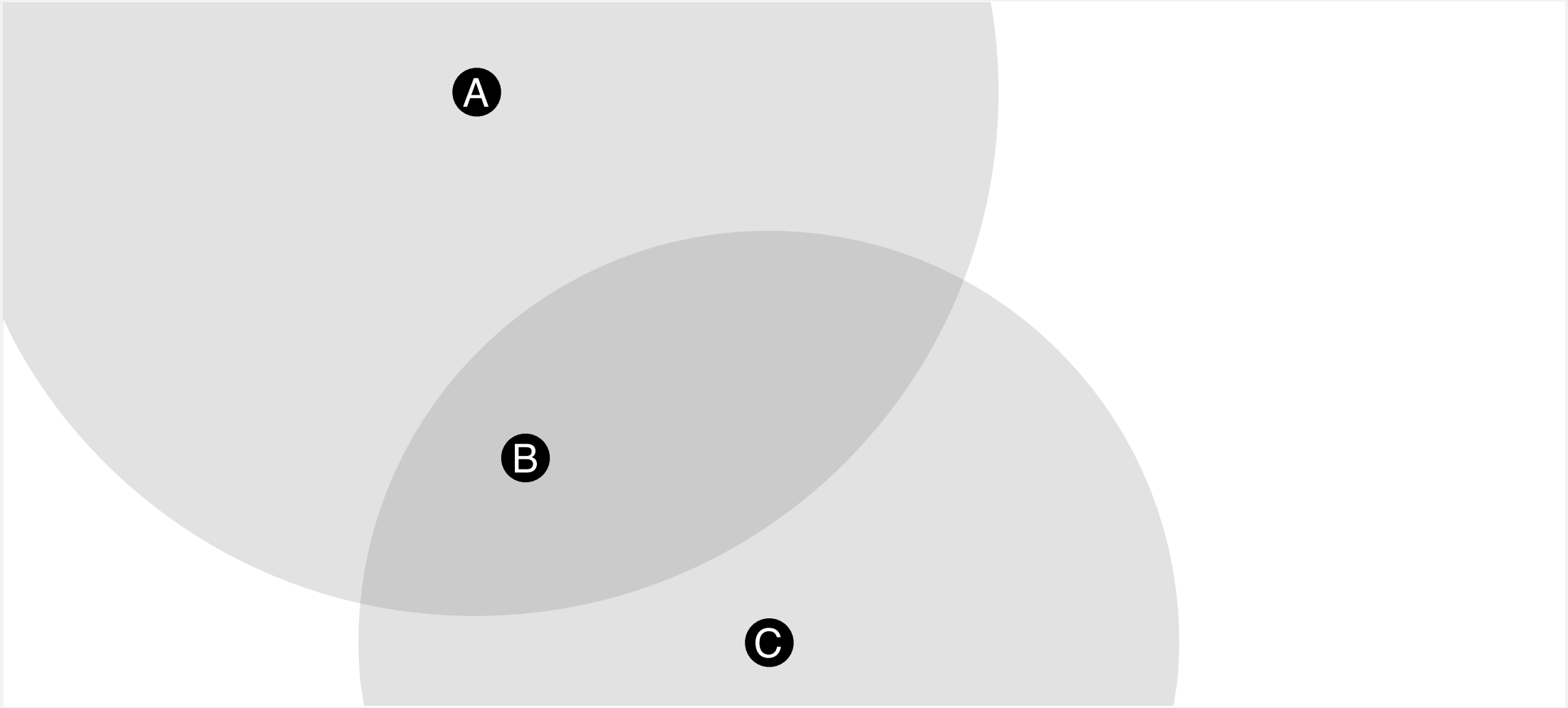
TODO 1: LOCALIZE NODES

TIMING-BASED LOCALIZATION



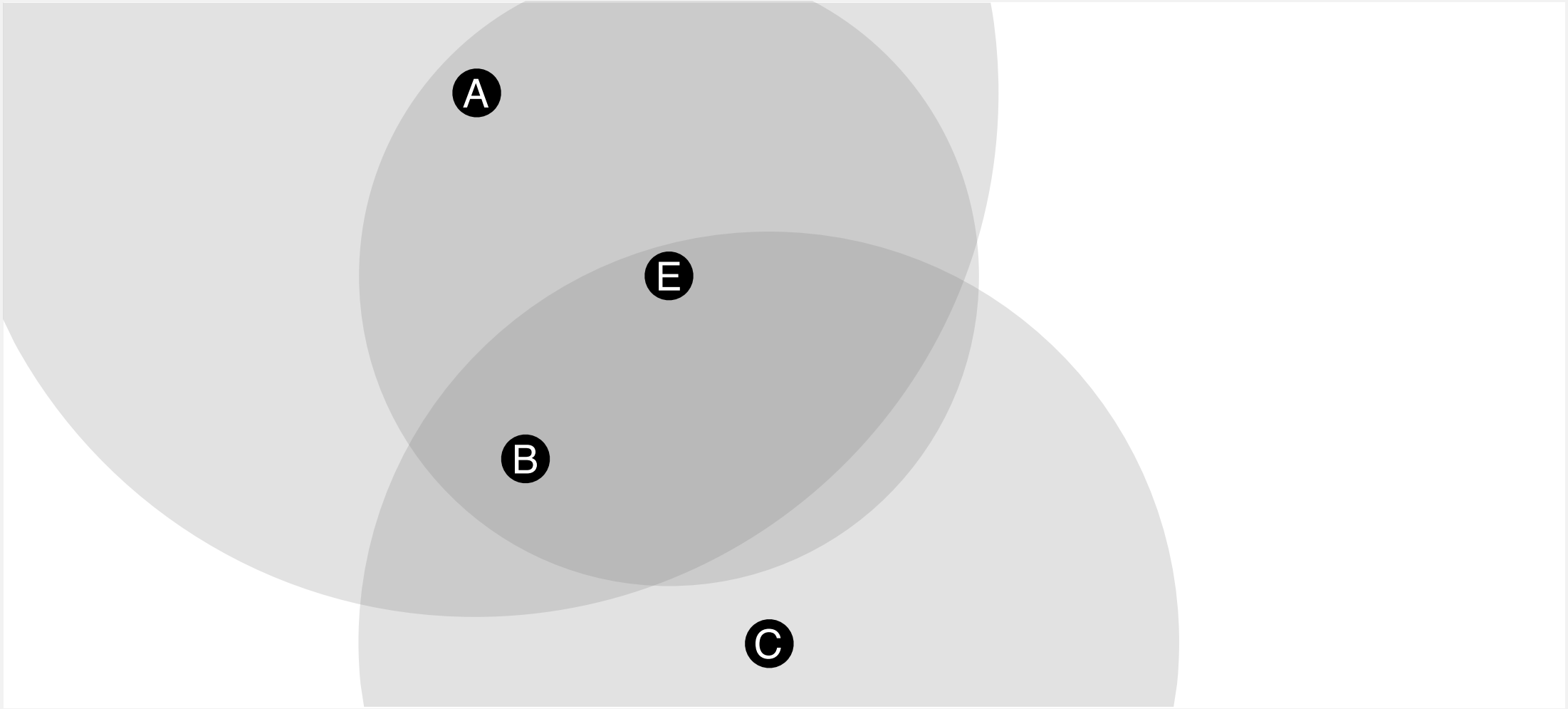
TODO 1: LOCALIZE NODES

TIMING-BASED LOCALIZATION



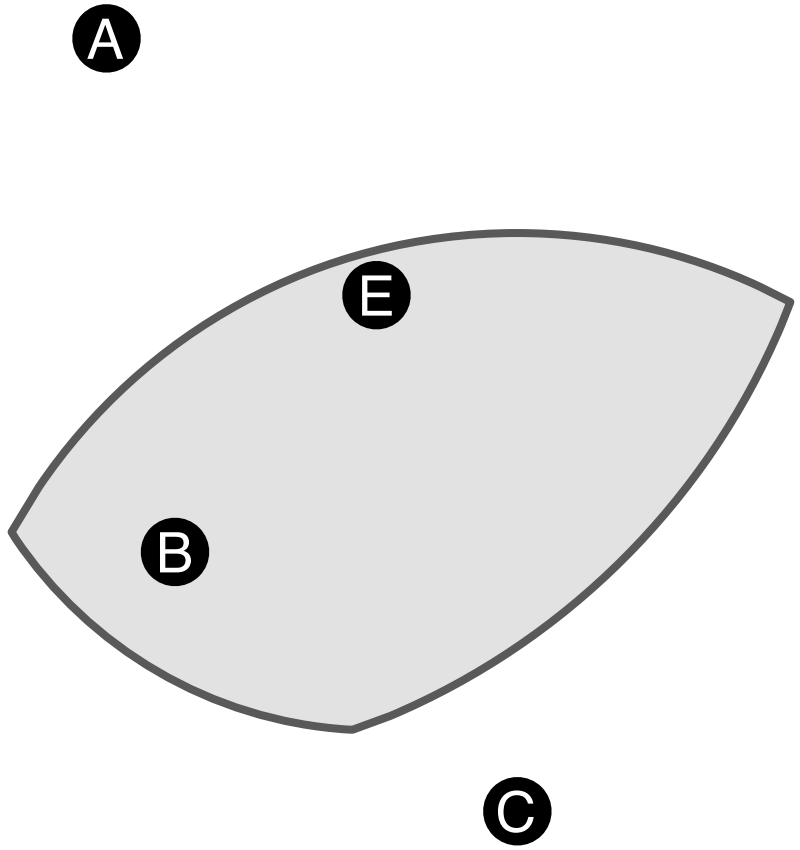
TODO 1: LOCALIZE NODES

TIMING-BASED LOCALIZATION



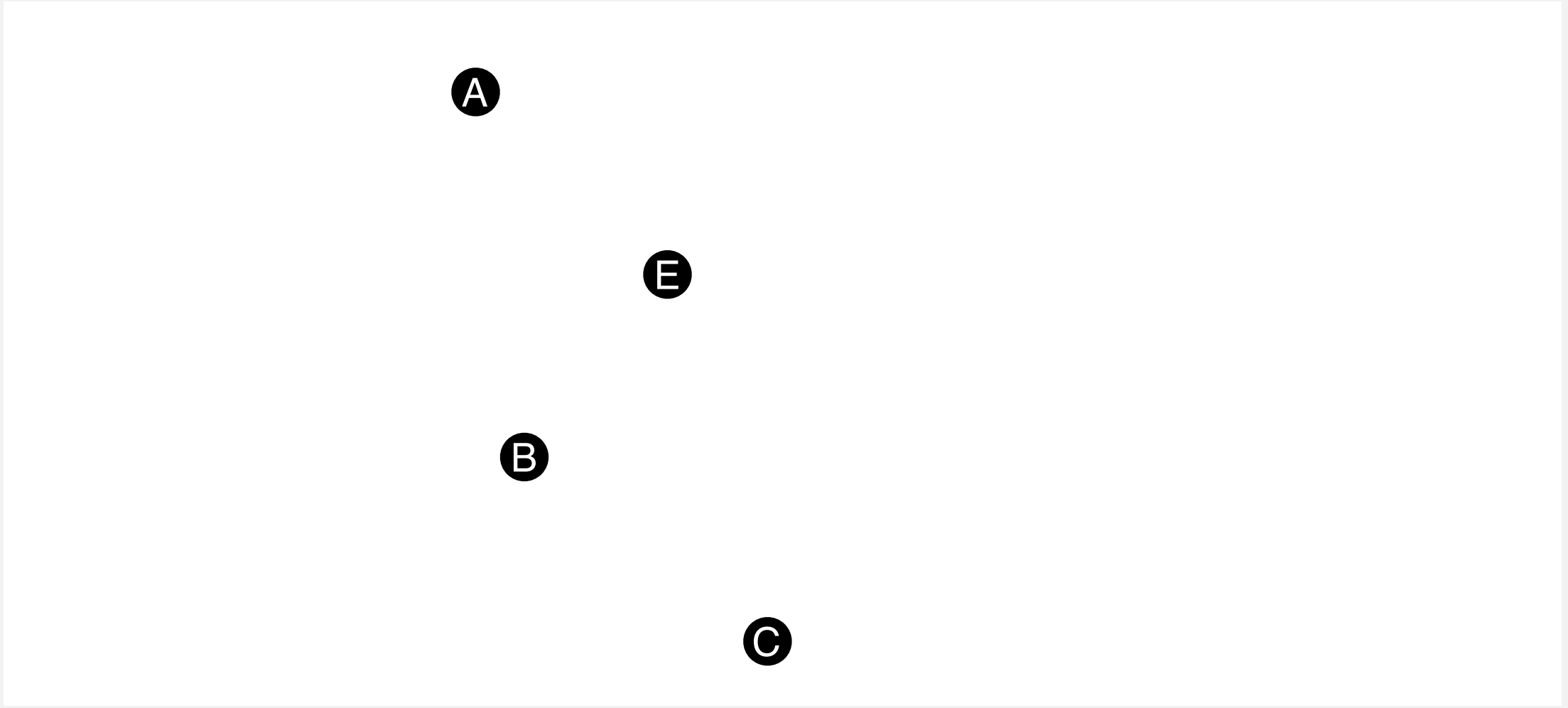
TODO 1: LOCALIZE NODES

TIMING-BASED LOCALIZATION



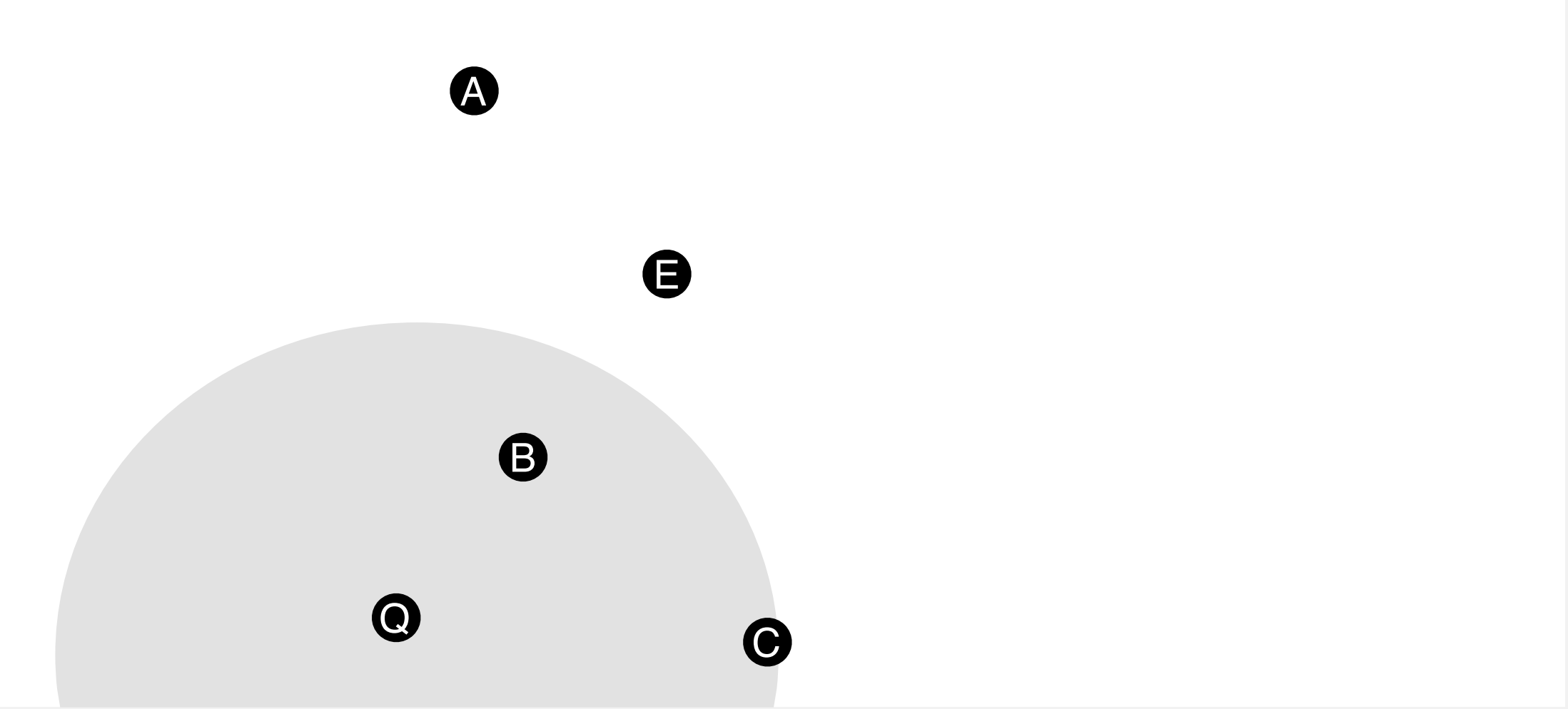
TODO 1: LOCALIZE NODES

TIMING-BASED LOCALIZATION



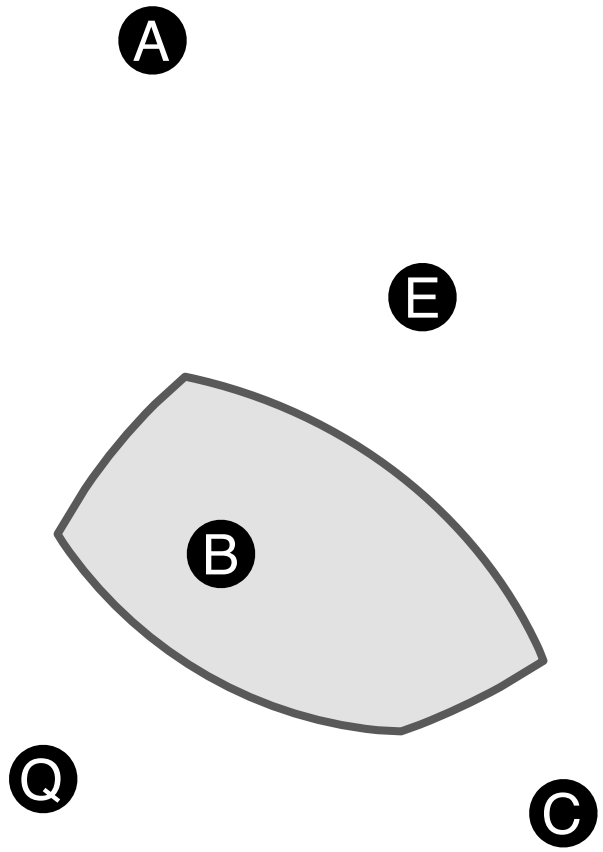
TODO 1: LOCALIZE NODES

TIMING-BASED LOCALIZATION



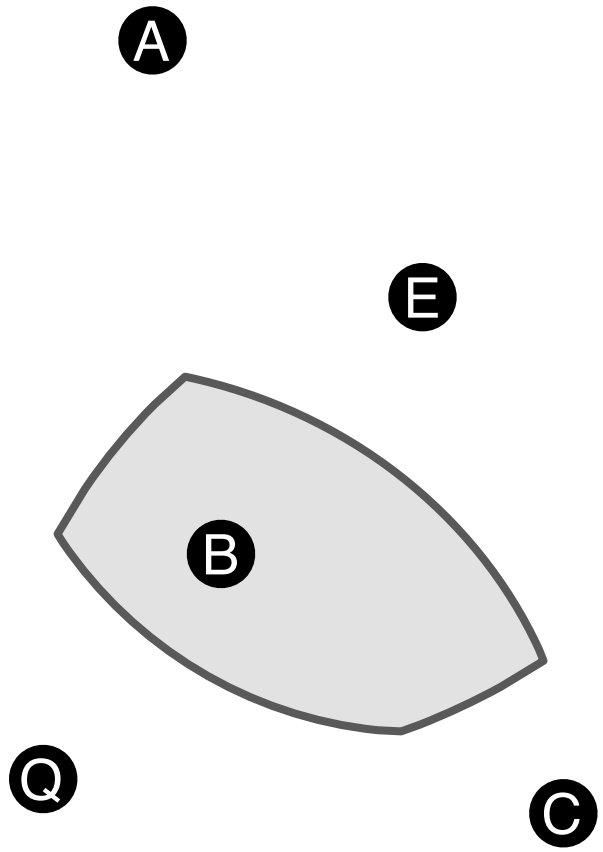
TODO 1: LOCALIZE NODES

TIMING-BASED LOCALIZATION



TODO 1: LOCALIZE NODES

TIMING-BASED LOCALIZATION



Estimate area

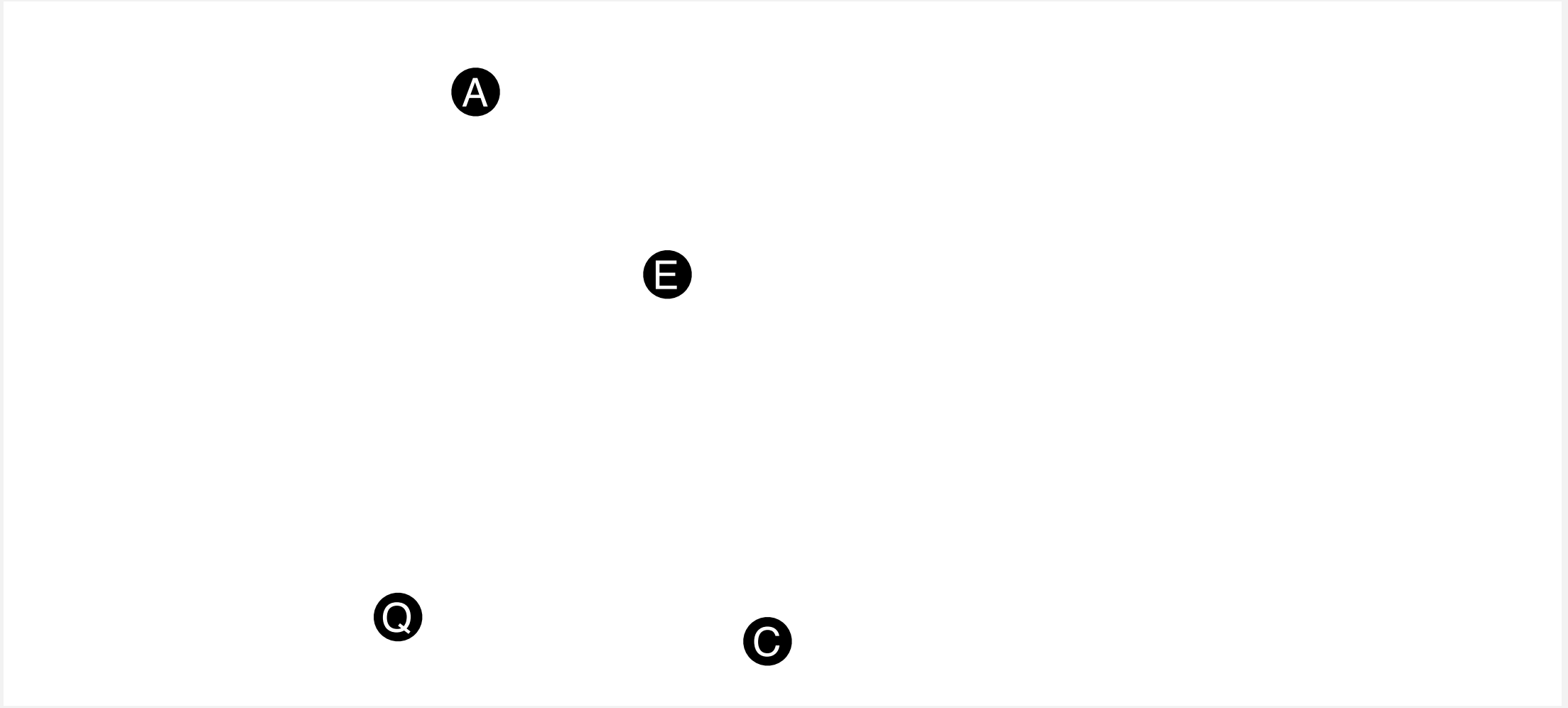
VERIFICATION AND MALICIOUS NODES

TODO:

1. **Localize** nodes (yes, no overhead!)
2. **Verify** the results (prepare for trouble)
3. **Decentralize** all the things

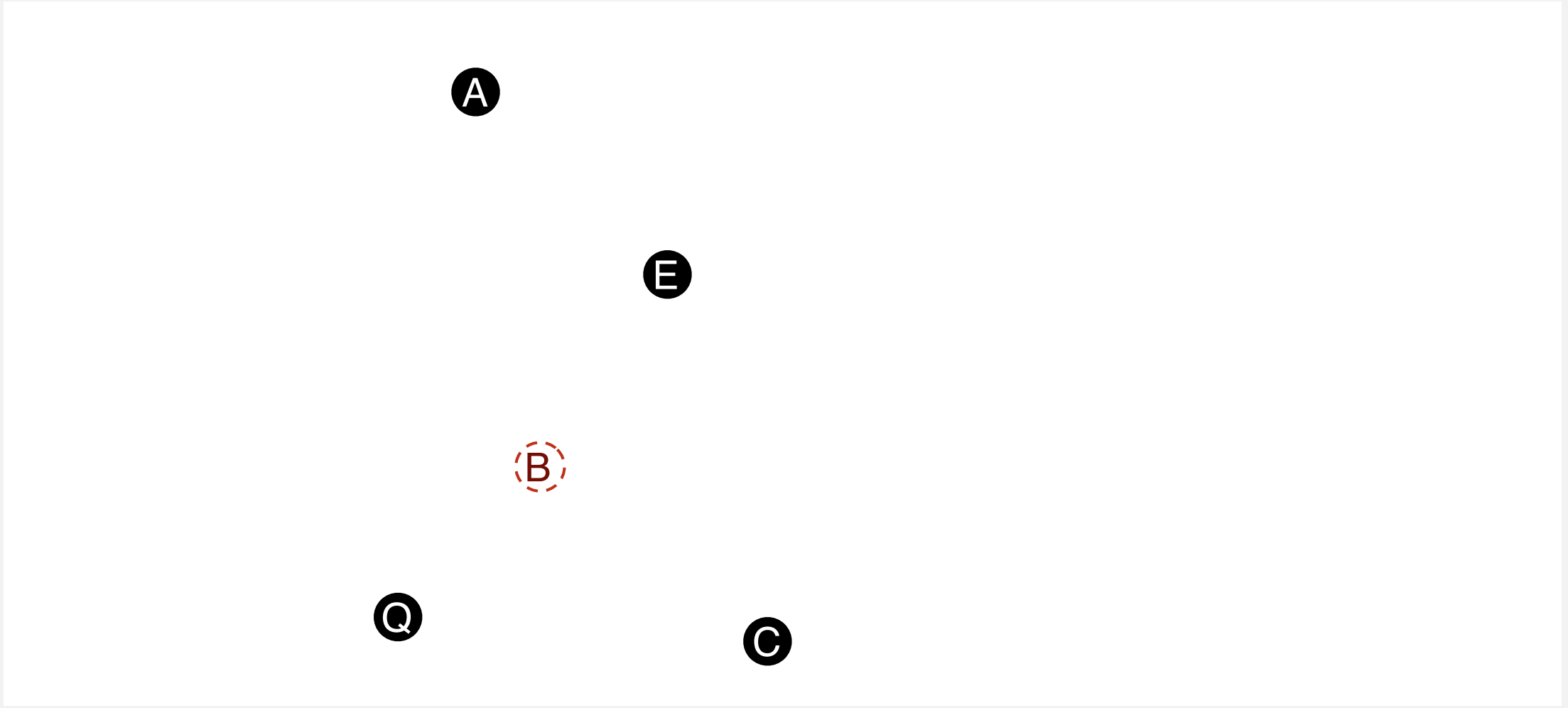
TODO 2: VERIFY RESULTS

CLAIMING FALSE LOCATIONS



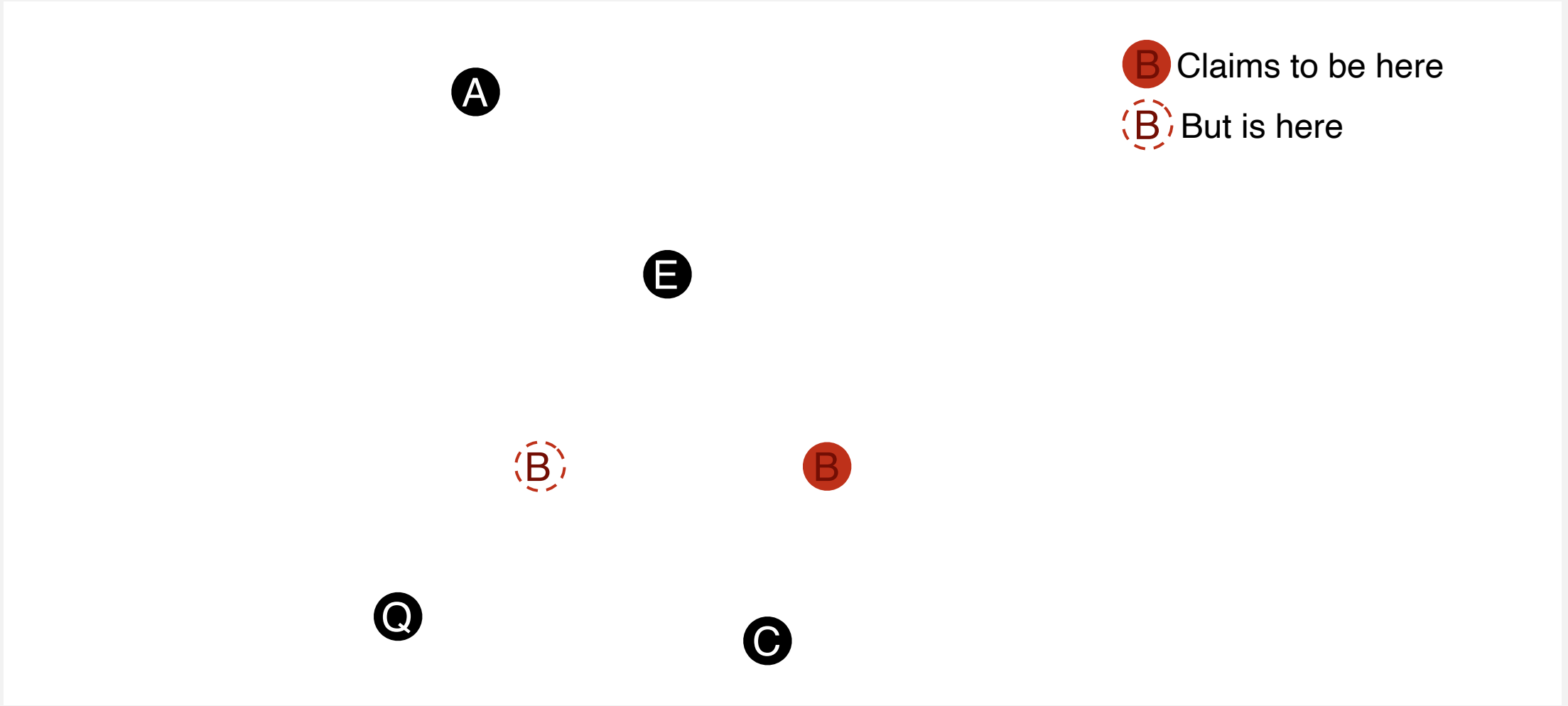
TODO 2: VERIFY RESULTS

CLAIMING FALSE LOCATIONS



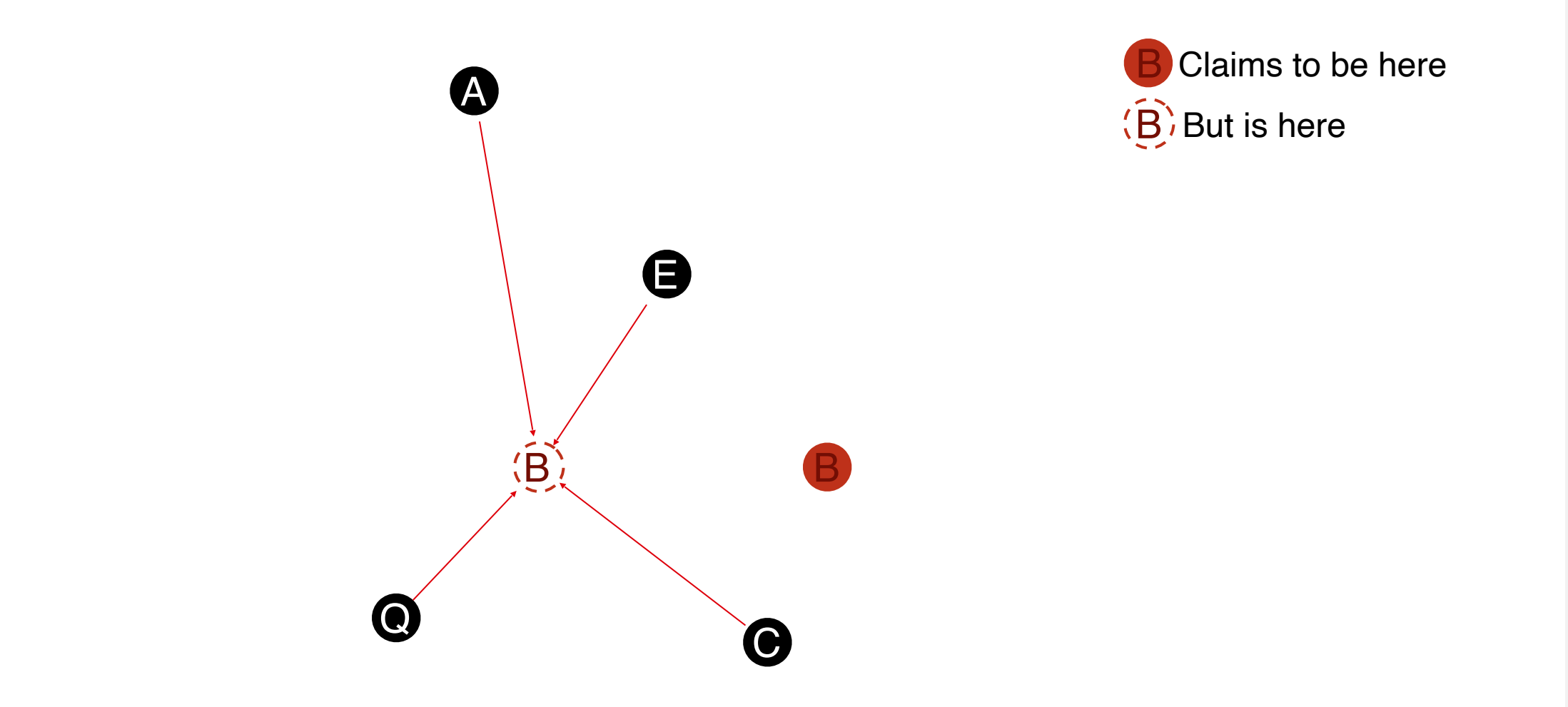
TODO 2: VERIFY RESULTS

CLAIMING FALSE LOCATIONS



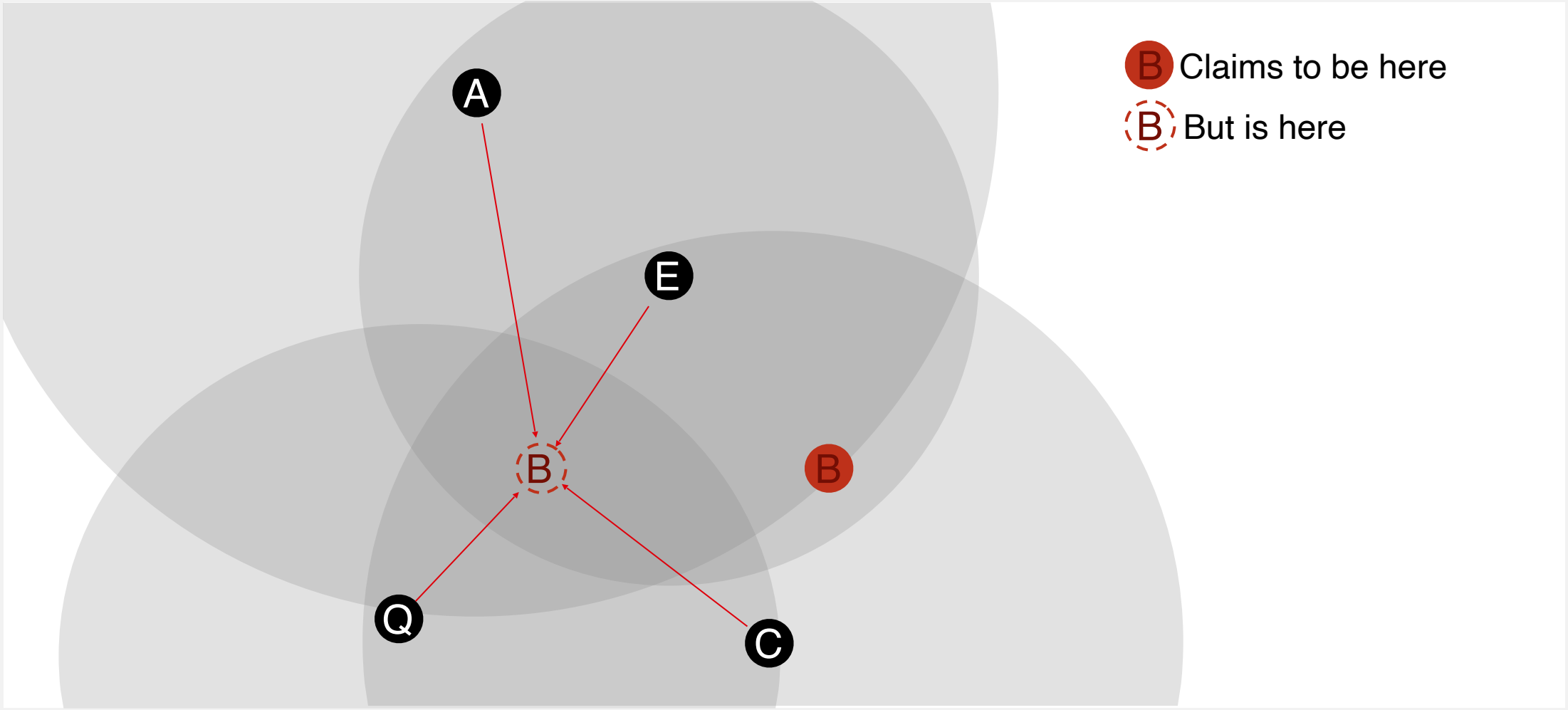
TODO 2: VERIFY RESULTS

CLAIMING FALSE LOCATIONS



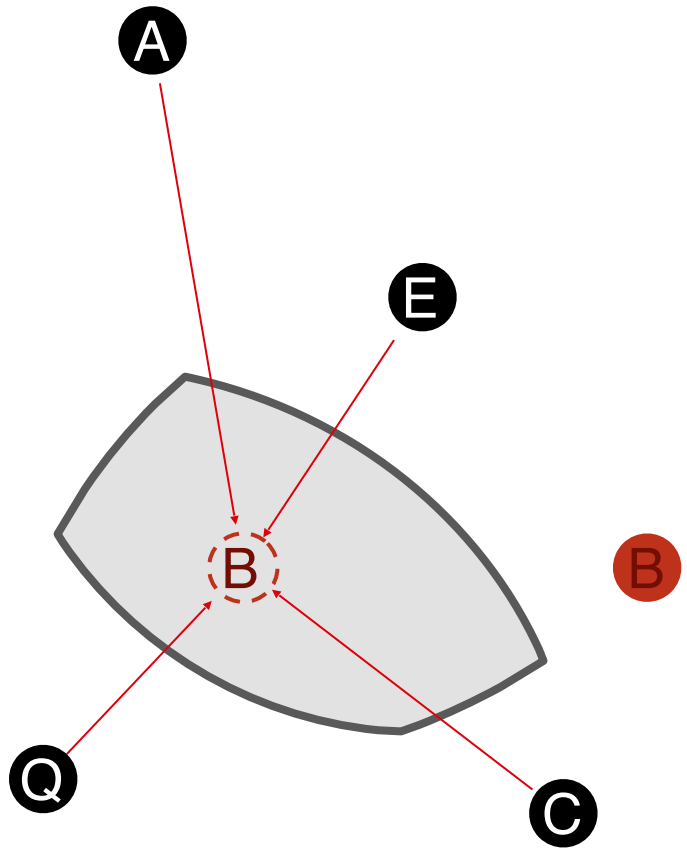
TODO 2: VERIFY RESULTS

CLAIMING FALSE LOCATIONS



TODO 2: VERIFY RESULTS

CLAIMING FALSE LOCATIONS

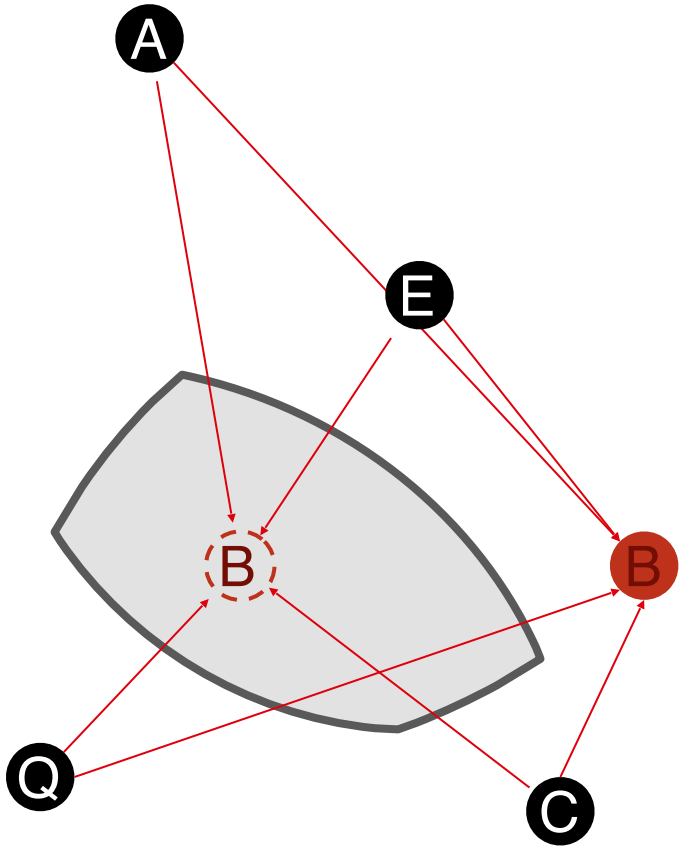


B Claims to be here

B But is here

TODO 2: VERIFY RESULTS

CLAIMING FALSE LOCATIONS

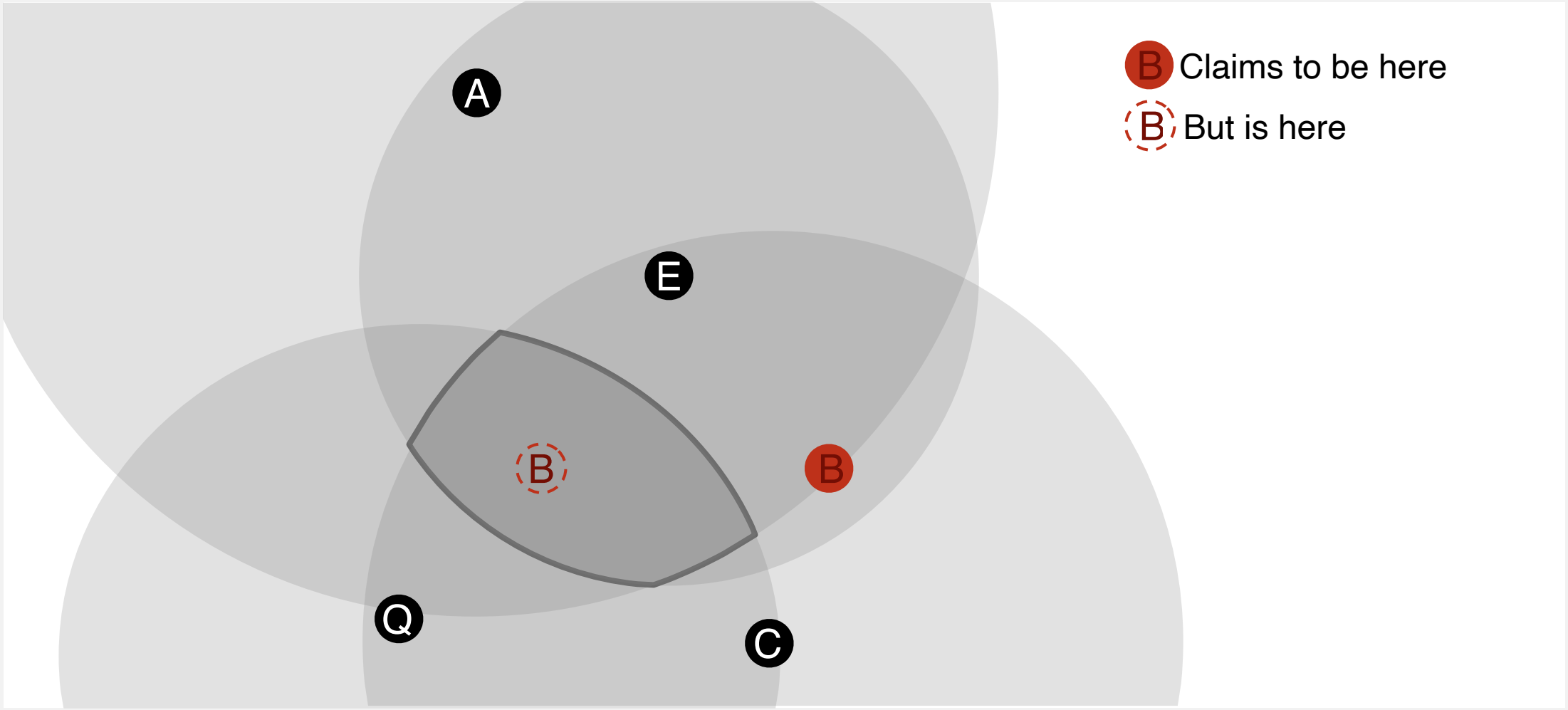


B Claims to be here

B But is here

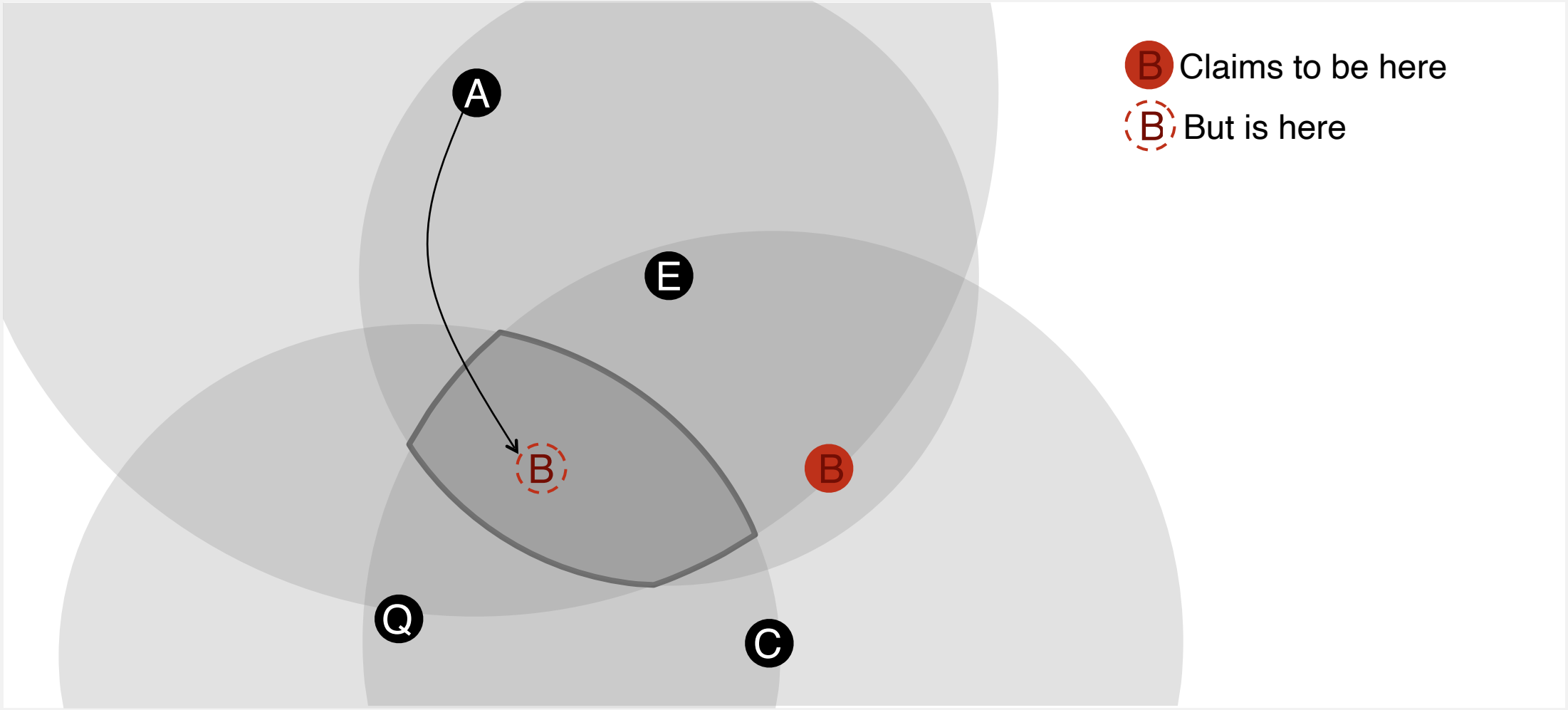
TODO 2: VERIFY RESULTS

MANIPULATE THE MEASUREMENTS



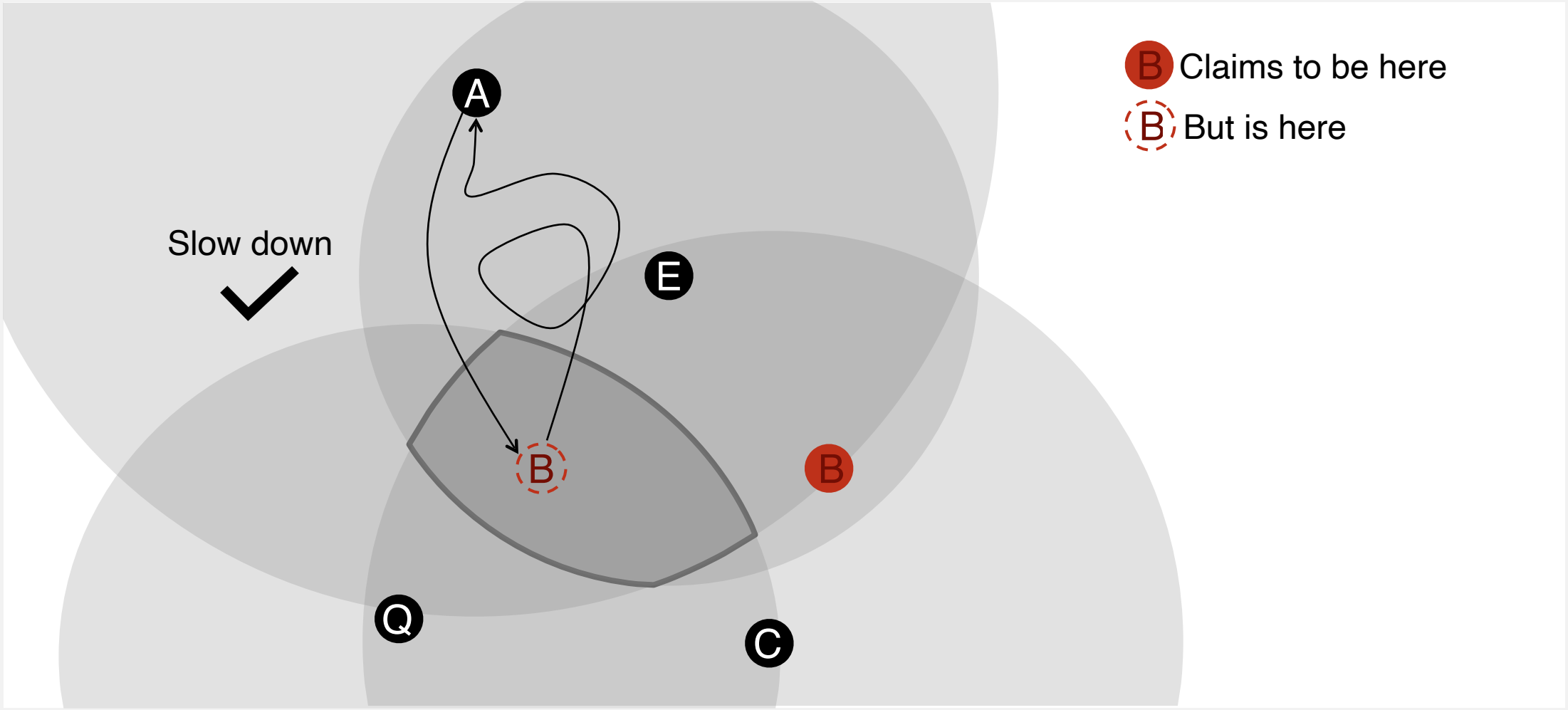
TODO 2: VERIFY RESULTS

MANIPULATE THE MEASUREMENTS



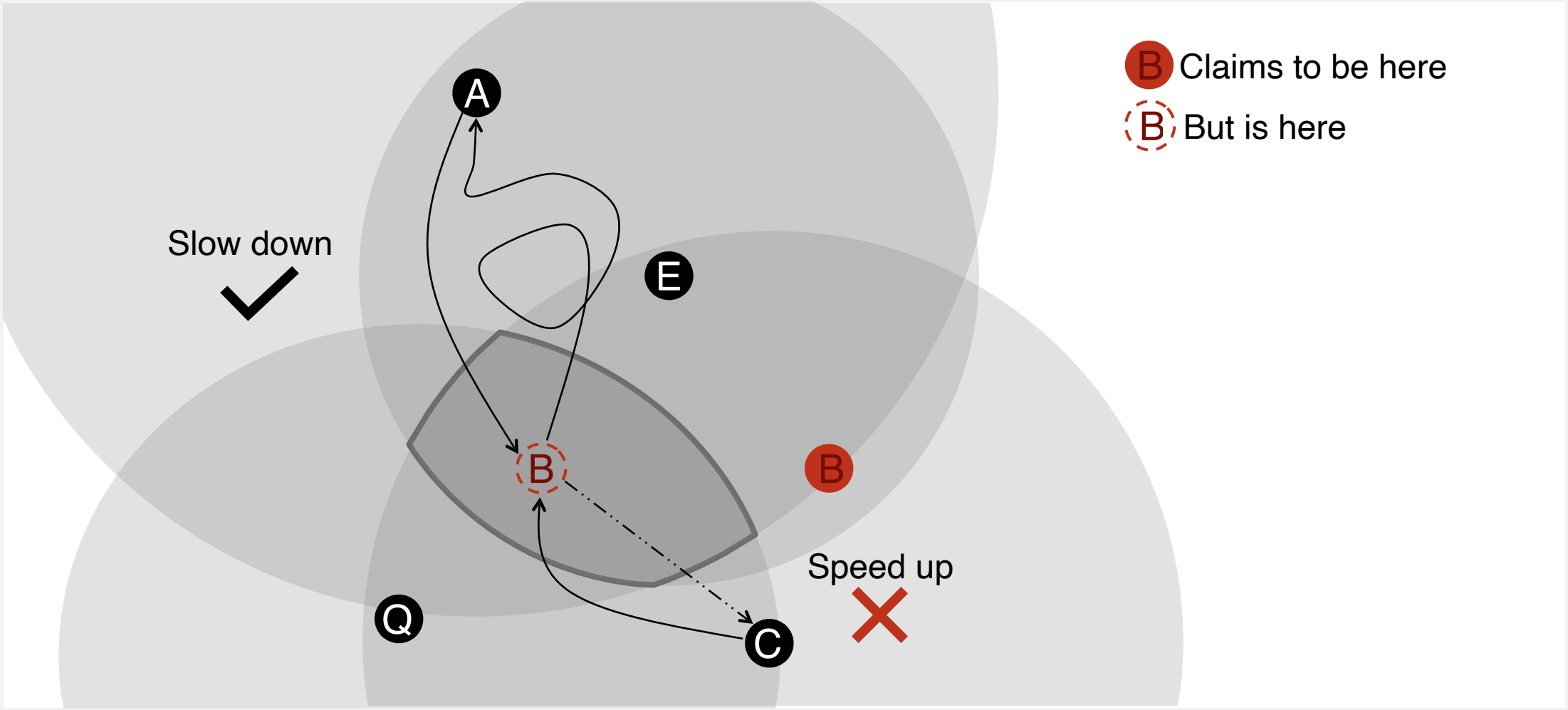
TODO 2: VERIFY RESULTS

MANIPULATE THE MEASUREMENTS



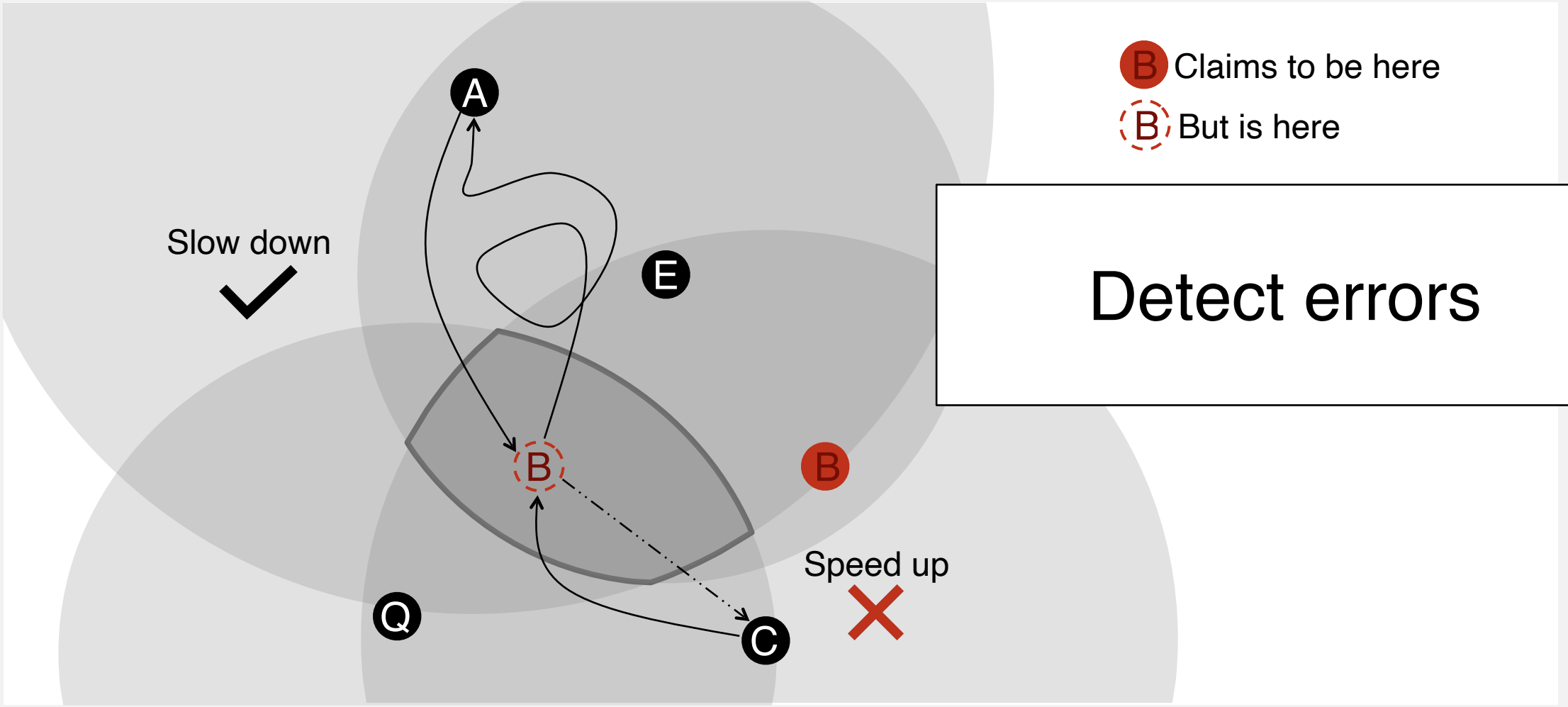
TODO 2: VERIFY RESULTS

MANIPULATE THE MEASUREMENTS



TODO 2: VERIFY RESULTS

MANIPULATE THE MEASUREMENTS



TODO 2: VERIFY RESULTS

VERIFICATION AND MALICIOUS NODES

Done:

1. **Localize:** RTT measurements
2. **Verify:** Estimate vs. claim
3. **Decentralize**: Broadcast channel

This is never going to work, real networks are too noisy…

PROTOTYPE

Localization Error: **60km**

CONCLUSION

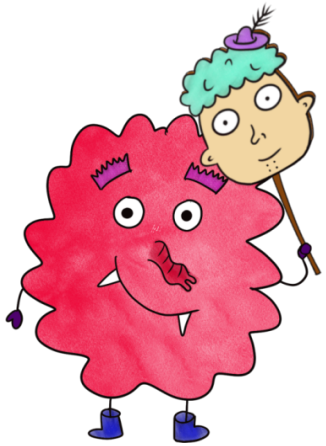
LESSONS LEARNED

CONCLUSION

LESSONS LEARNED

Problem Statement

- Node locations matter
- You can lie
- Let’s verify the claims!

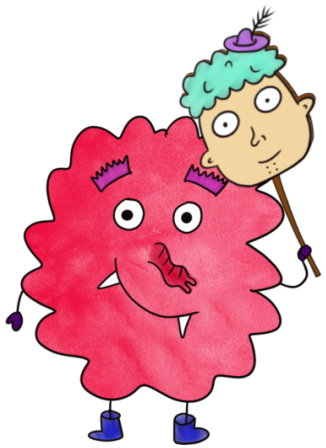


CONCLUSION

LESSONS LEARNED

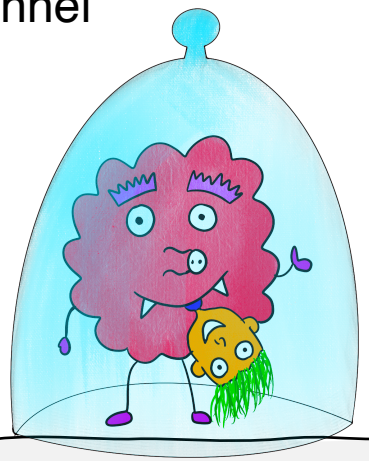
Problem Statement

- Node locations matter
- You can lie
- Let's verify the claims!



Goals

1. **Localize**: RTT and estimated areas
2. **Verify**: Robust estimation versus claim
3. **Decentralize**: Broadcast channel

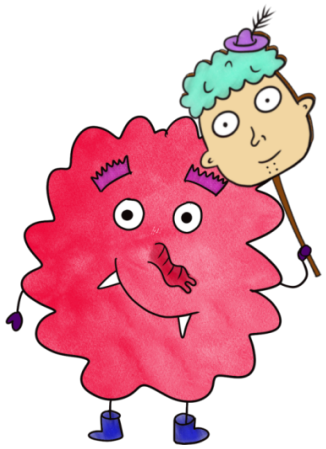


CONCLUSION

LESSONS LEARNED

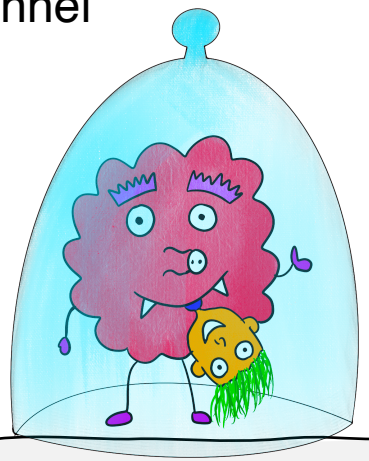
Problem Statement

- Node locations matter
- You can lie
- Let's verify the claims!



Goals

1. **Localize**: RTT and estimated areas
2. **Verify**: Robust estimation versus claim
3. **Decentralize**: Broadcast channel



Prototype

- Nym network
- Verify claimed locations of nodes
- 60km location error with noisy real-world data