Network Partitioning Effects on Ripple Transactions

Yoan Martin

Today's menu

- What is Ripple?
- Why is it interesting?
- Attacks
- Analysis

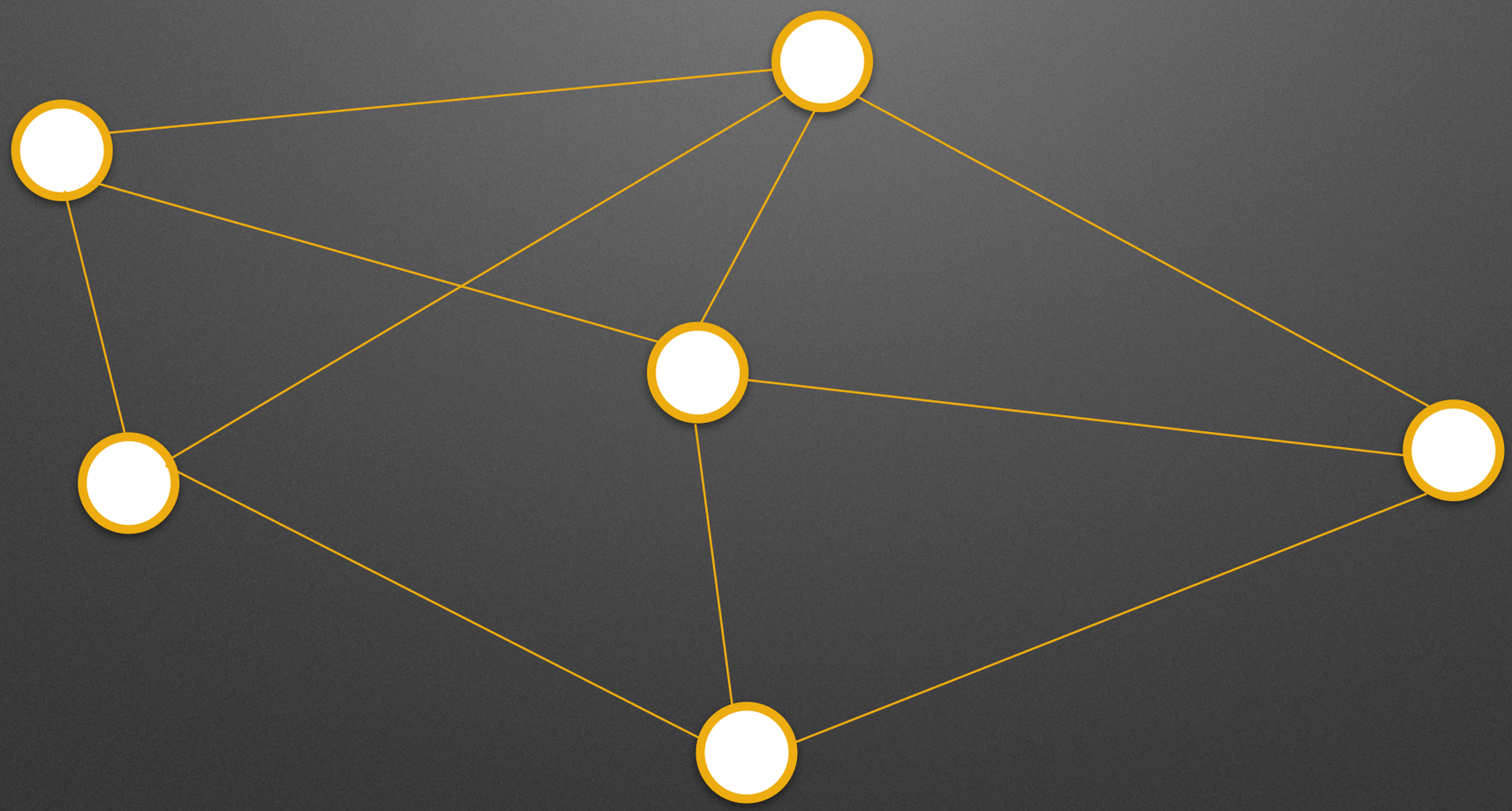
What is Ripple?

- Global Payments Network
- RippleNet vs XRP
- Gateway
  - Entry Point
  - Ripple Bank

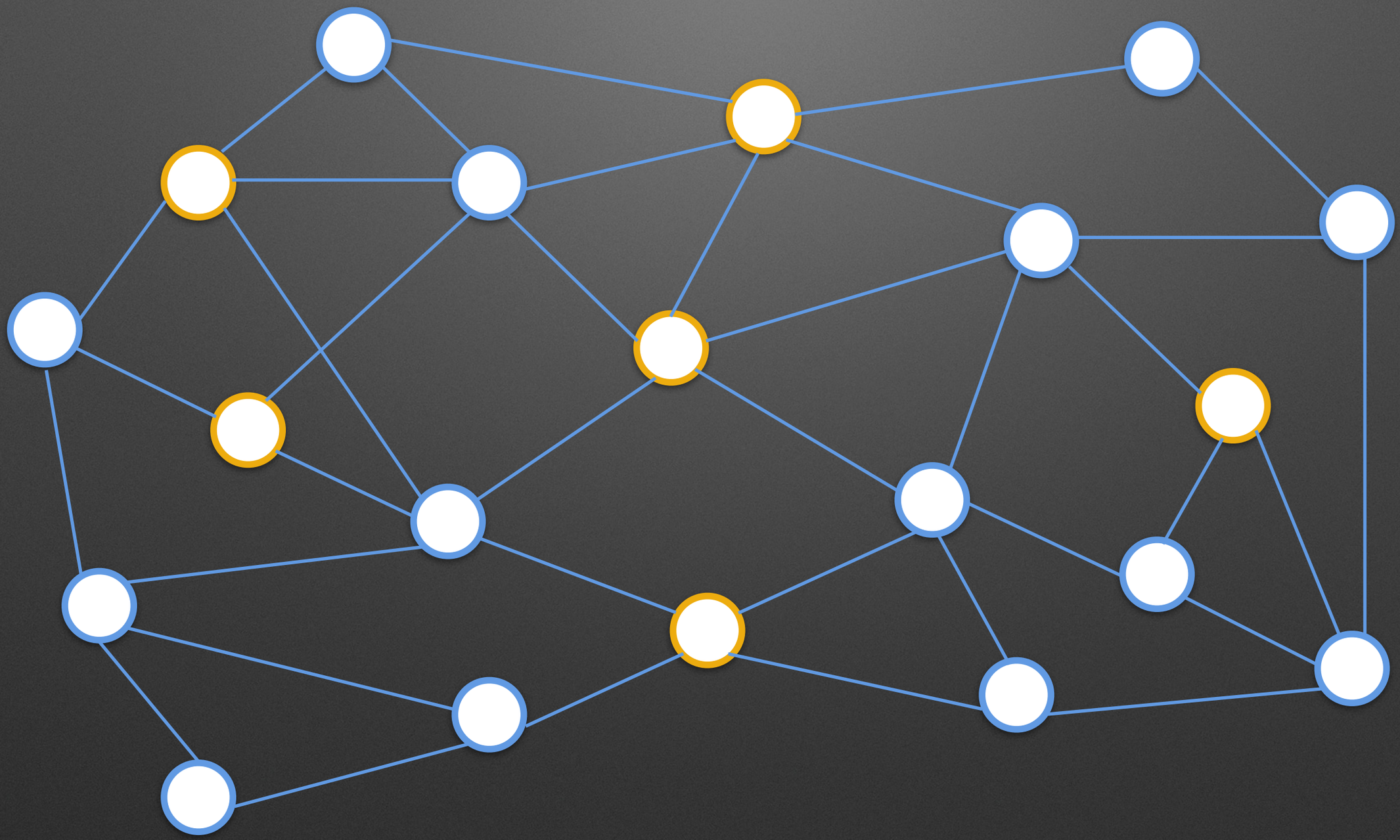
Why is it interesting?

- More than 200 financial institutions
- ~20’000’000 USD sent by hour
- Take place on internet

What is the network?



Network

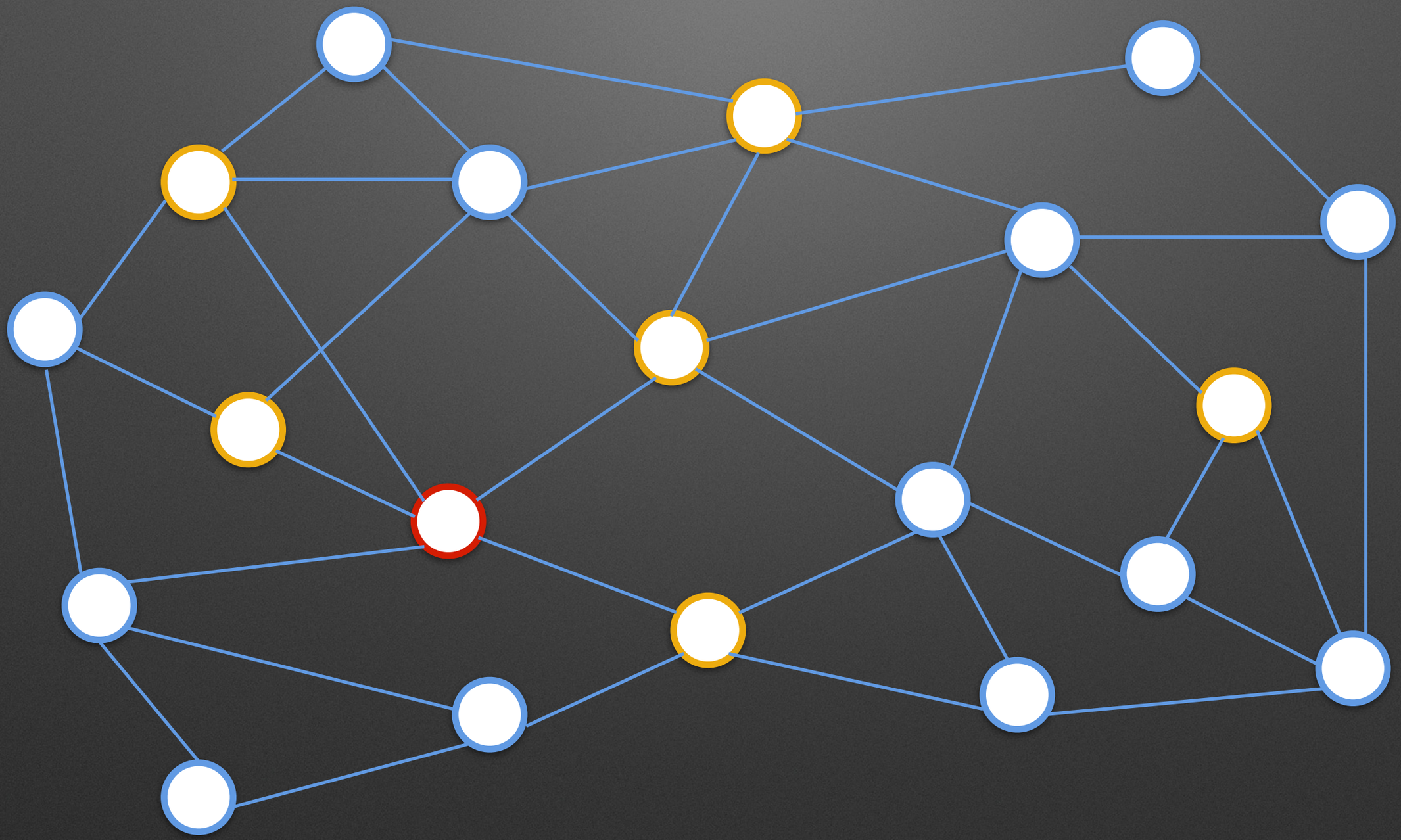


What is the network?

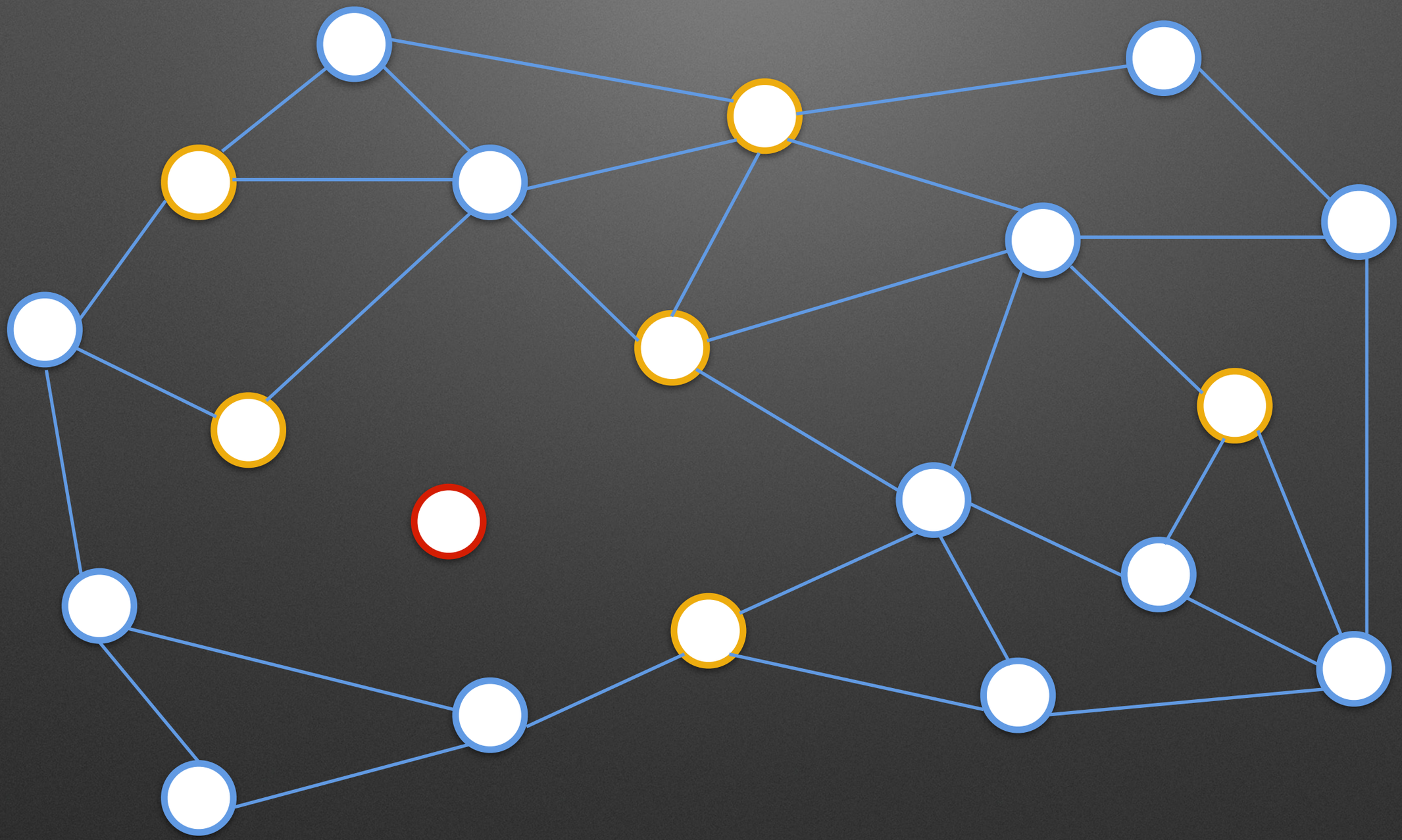
Attacks

- What if an AS is malicious?
- What can it do?
  - Dropping the traffic
  - BGP Hijacking

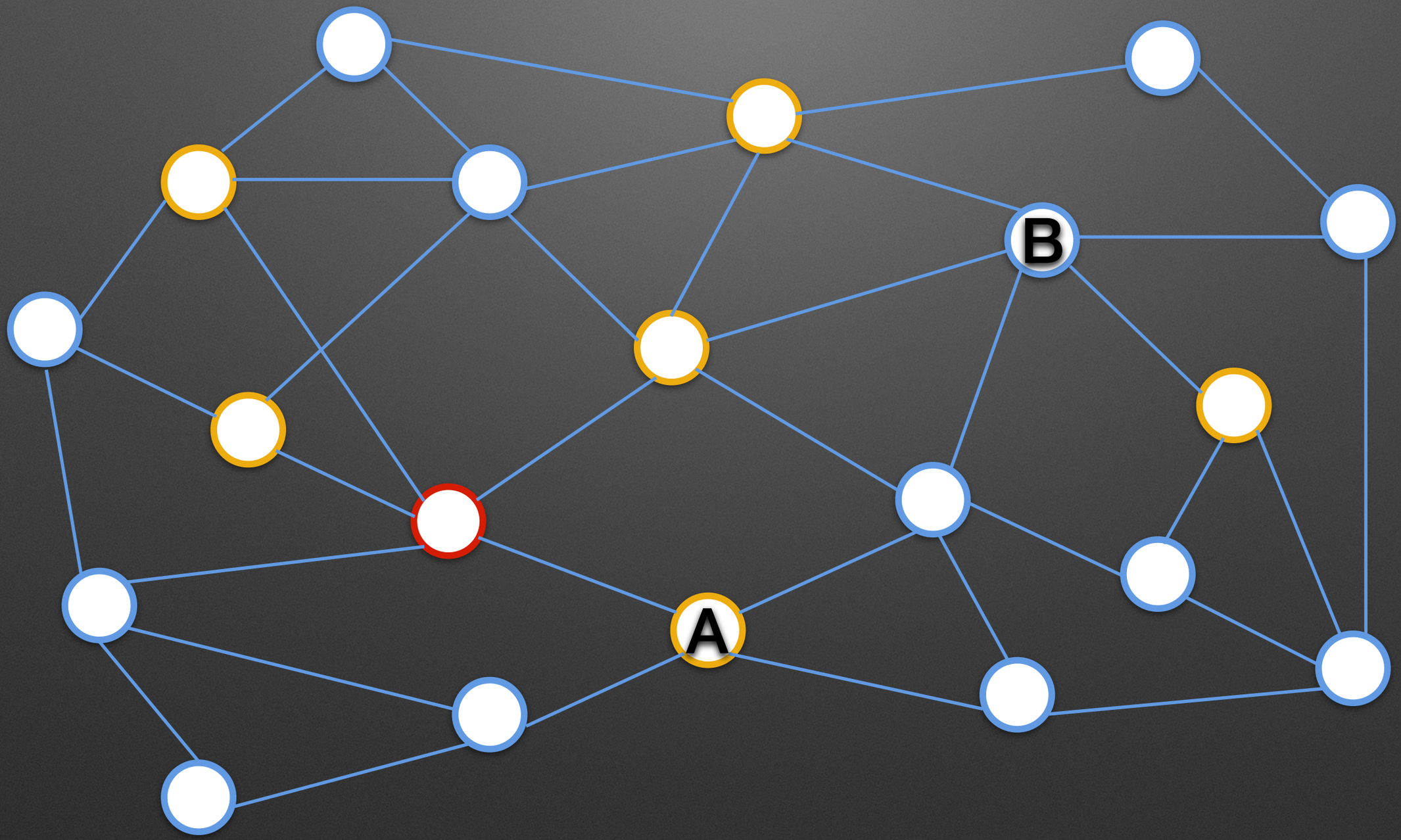
Traffic dropped



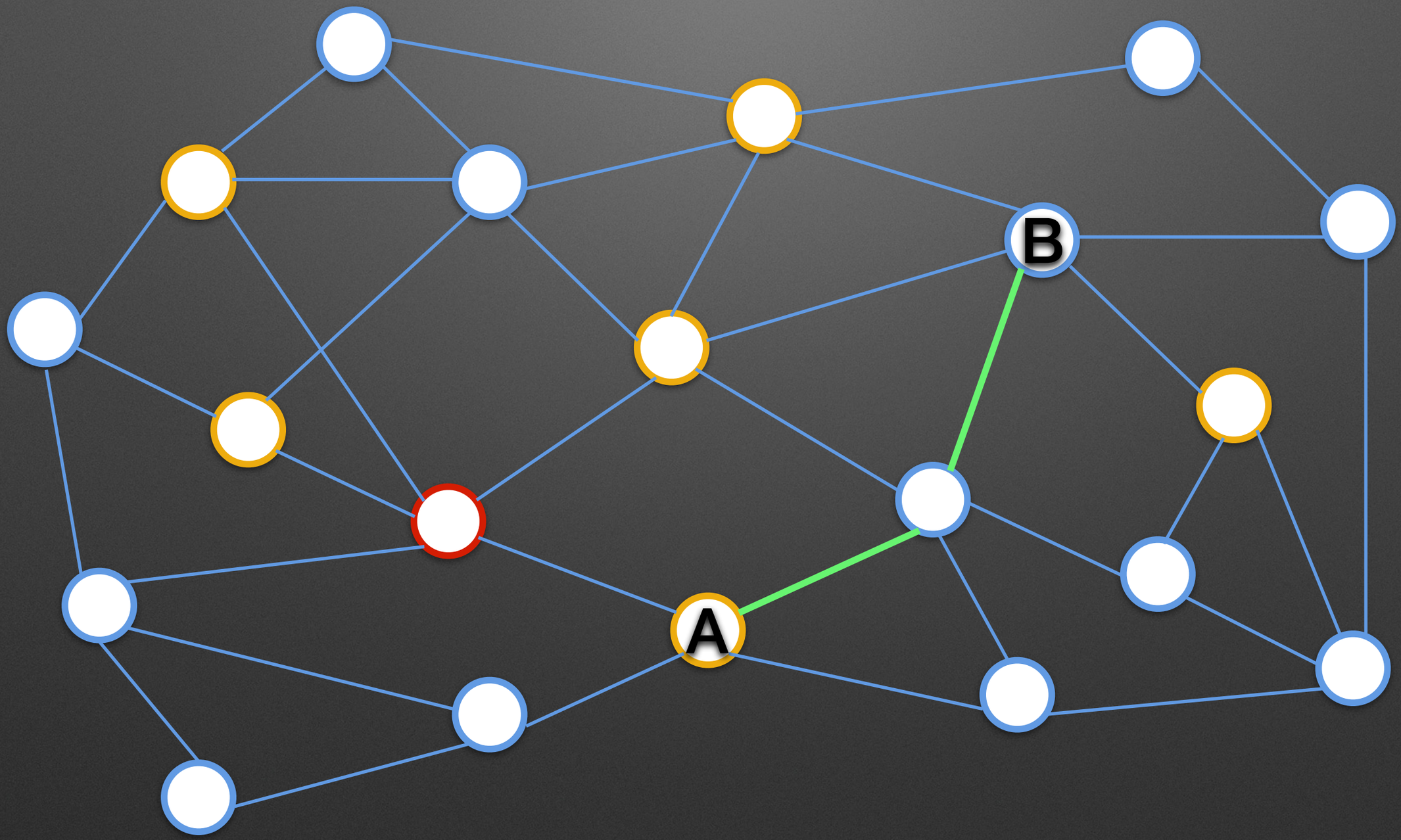
Traffic dropped



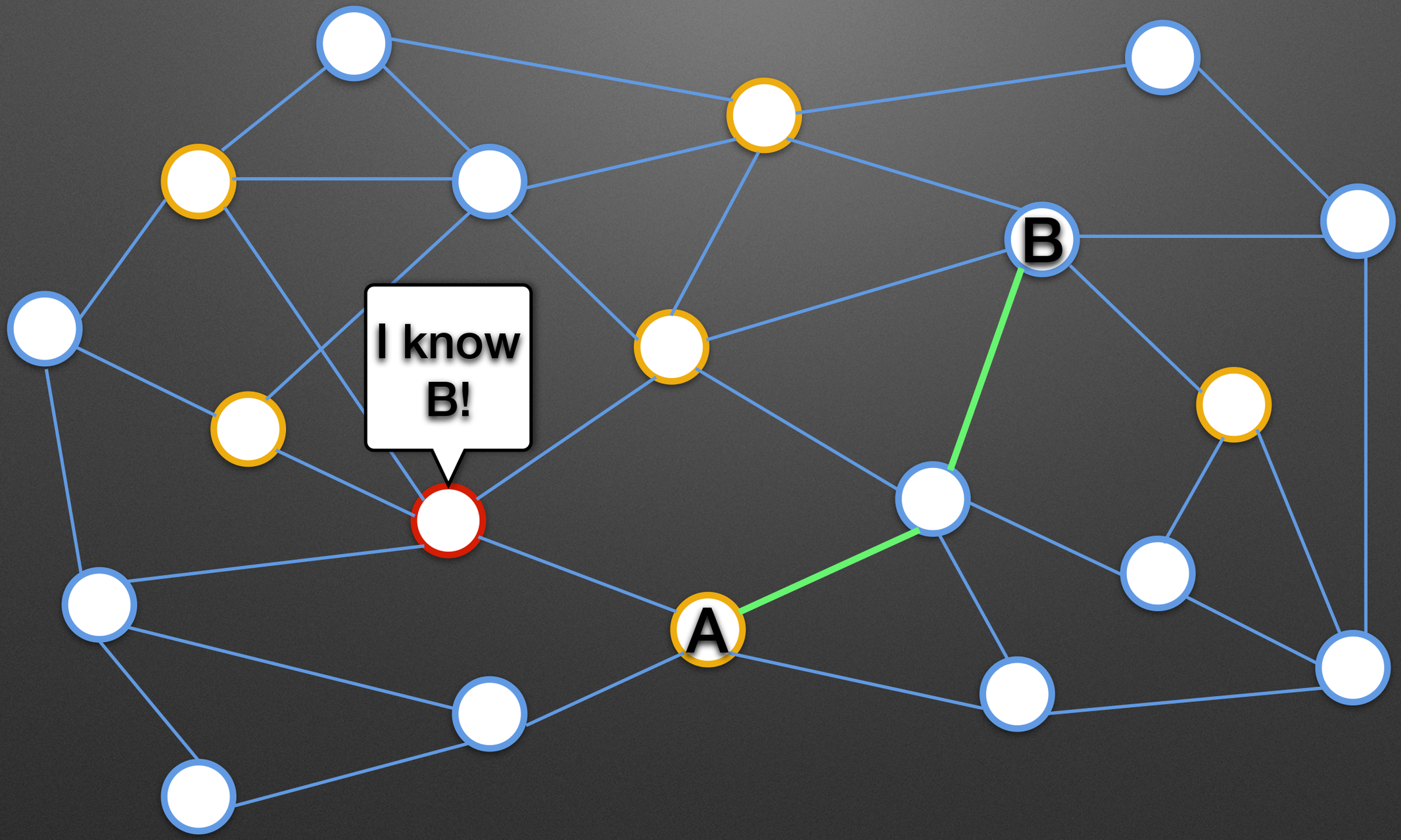
BGP Hijacking



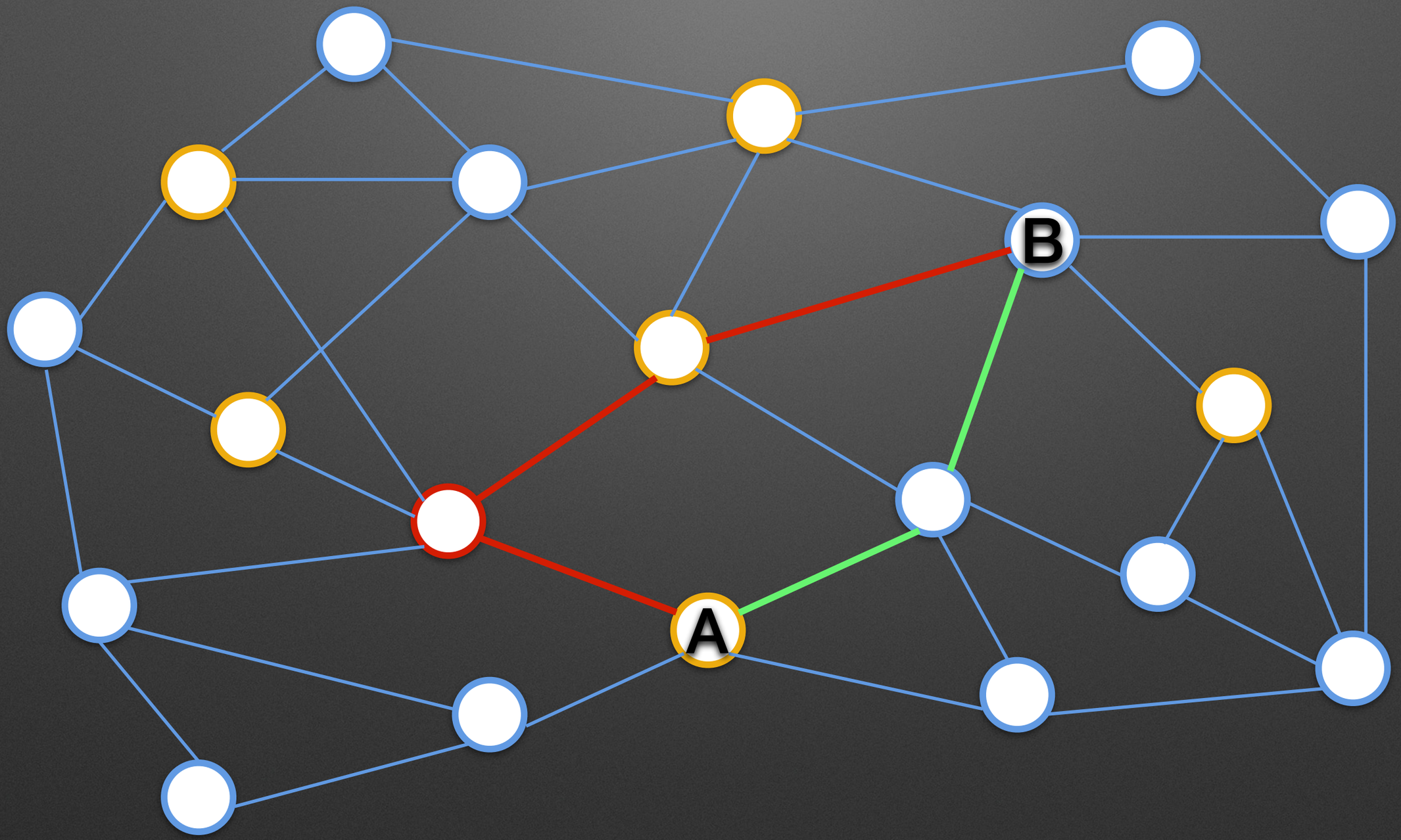
BGP Hijacking



BGP Hijacking



BGP Hijacking



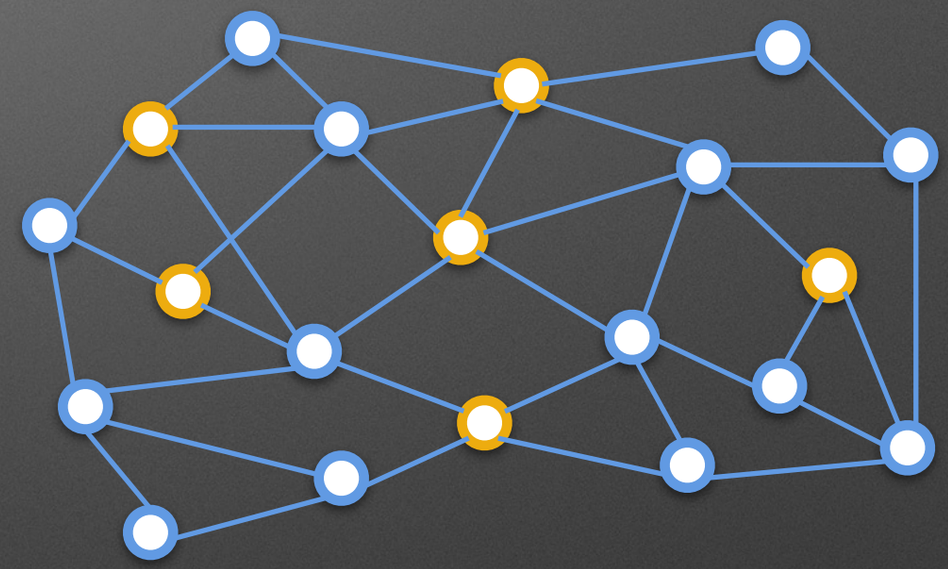
How to measure the effect?

- Build the Ripple Network
  - Ripple API
    - Caida
- Use previous transactions
- Replay transactions when an attack occurs

Build RippleNet

Ripple API,
Gateways data

AS relationships



AS

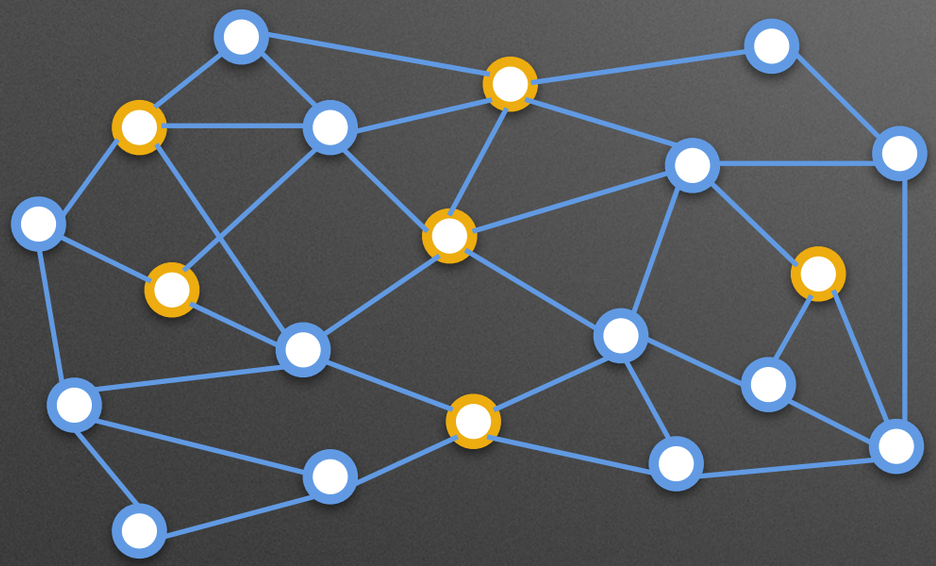
AS with a Gateway

Map Result

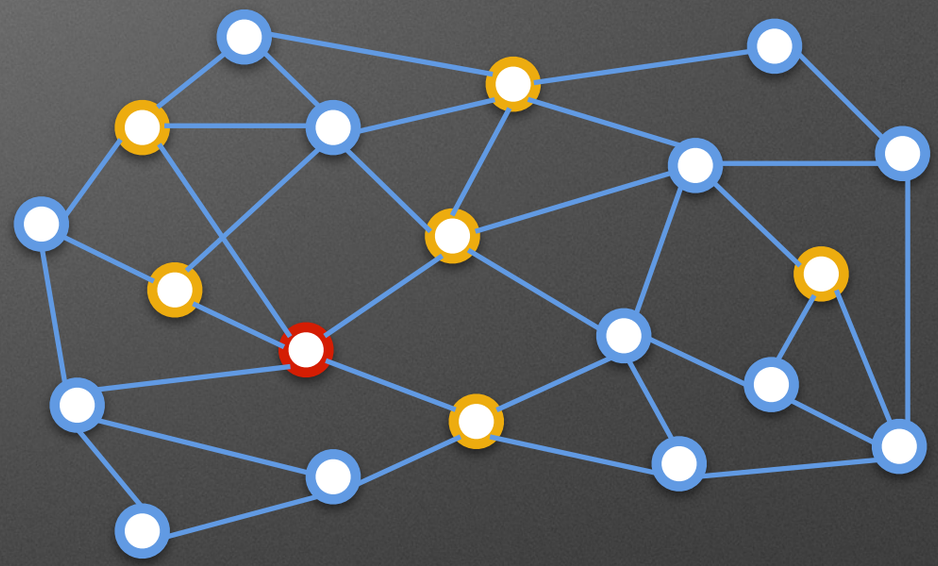
Transactions

- Account A sends 100 XRP to account B
- Some transactions have gateways data
  - Account A sends 100 XRP using Gateway G to B
  - Account B receives 100 XRP using Gateway H from A
- Keep only transactions with matching Gateways

Simulation : traffic dropped

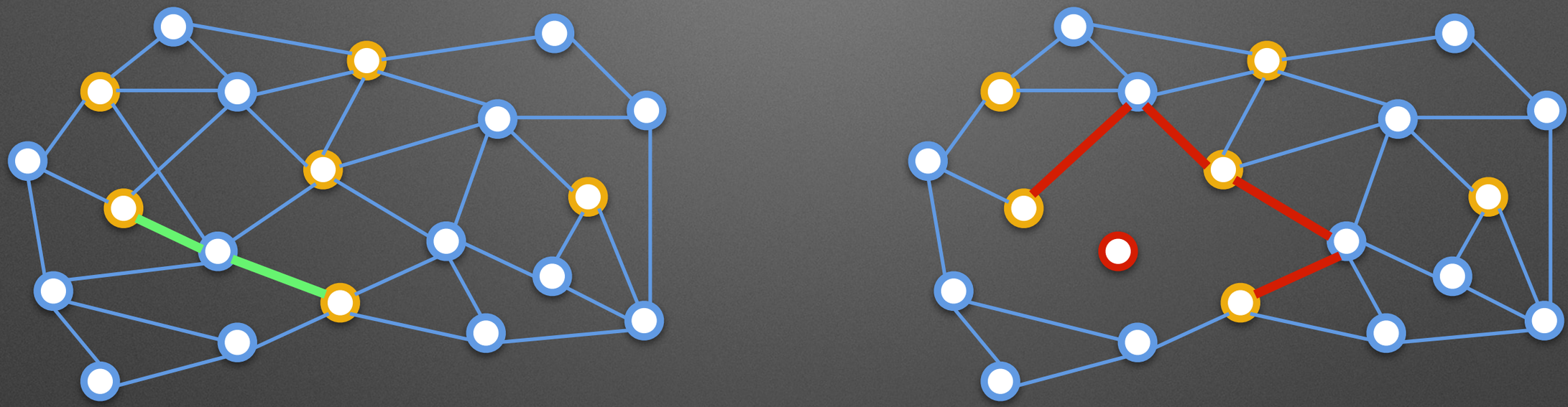


A sends 100 XRP to B
D sends 10 USD to A
C sends 4 EUR to B
…



A sends 100 XRP to B
D sends 10 USD to A
C sends 4 EUR to B
…

Simulation : traffic dropped

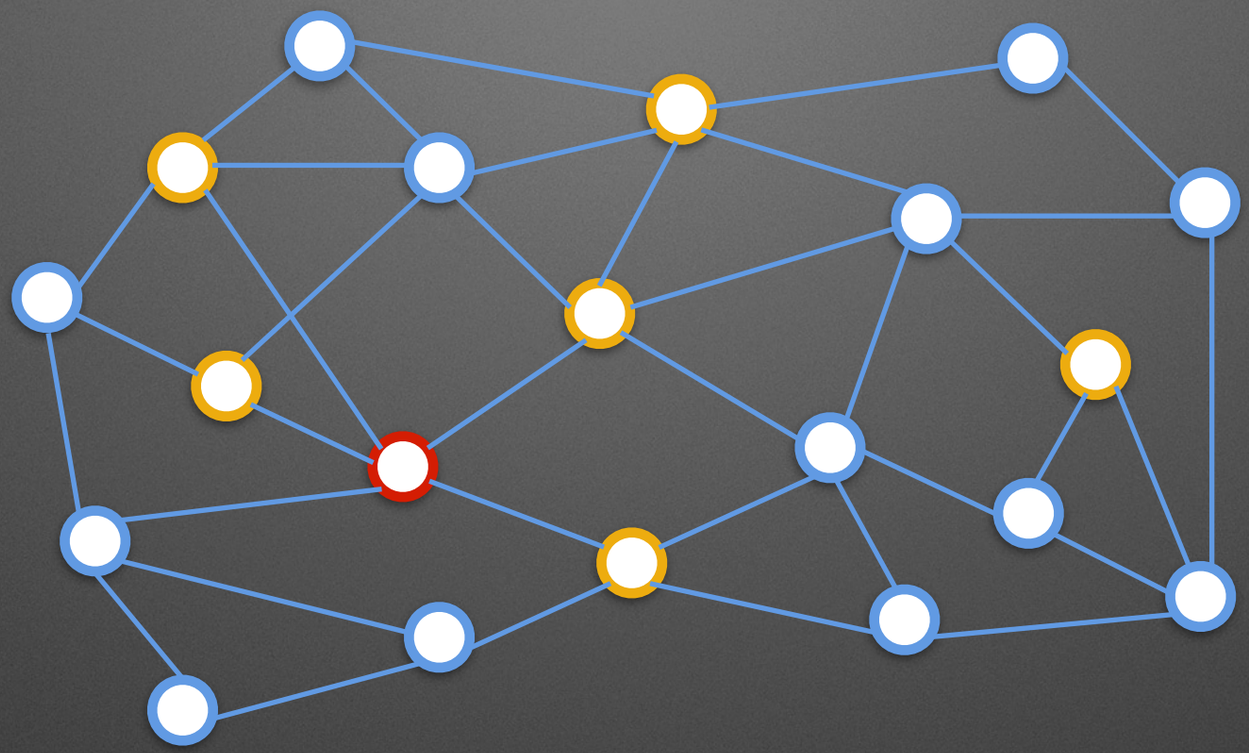


- If — == — , transaction is complete
- If — != — , transaction is rerouted
- If no ——— , transaction is lost

Example of results

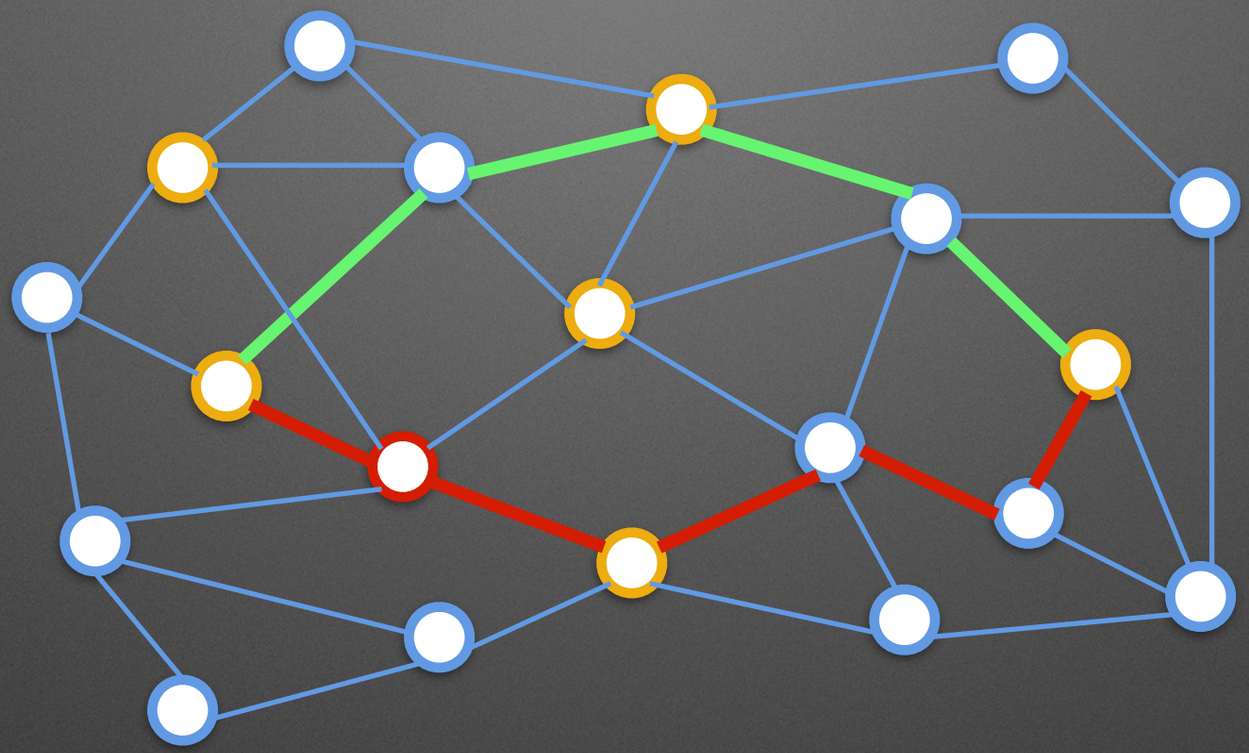
	Completed	Rerouted	Lost
Amazon	10%	10%	80%
AT&T	30%	20%	50%
China Telecom	60%	30%	10%
Swisscom	30%	30%	40%

Simulation: BGP Hijacking



A sends 100 XRP to B
D sends 10 USD to A
C sends 4 EUR to B
...

Simulation: BGP Hijacking



- If — == — , transaction is complete
- If — != — , transaction is rerouted

Example of results

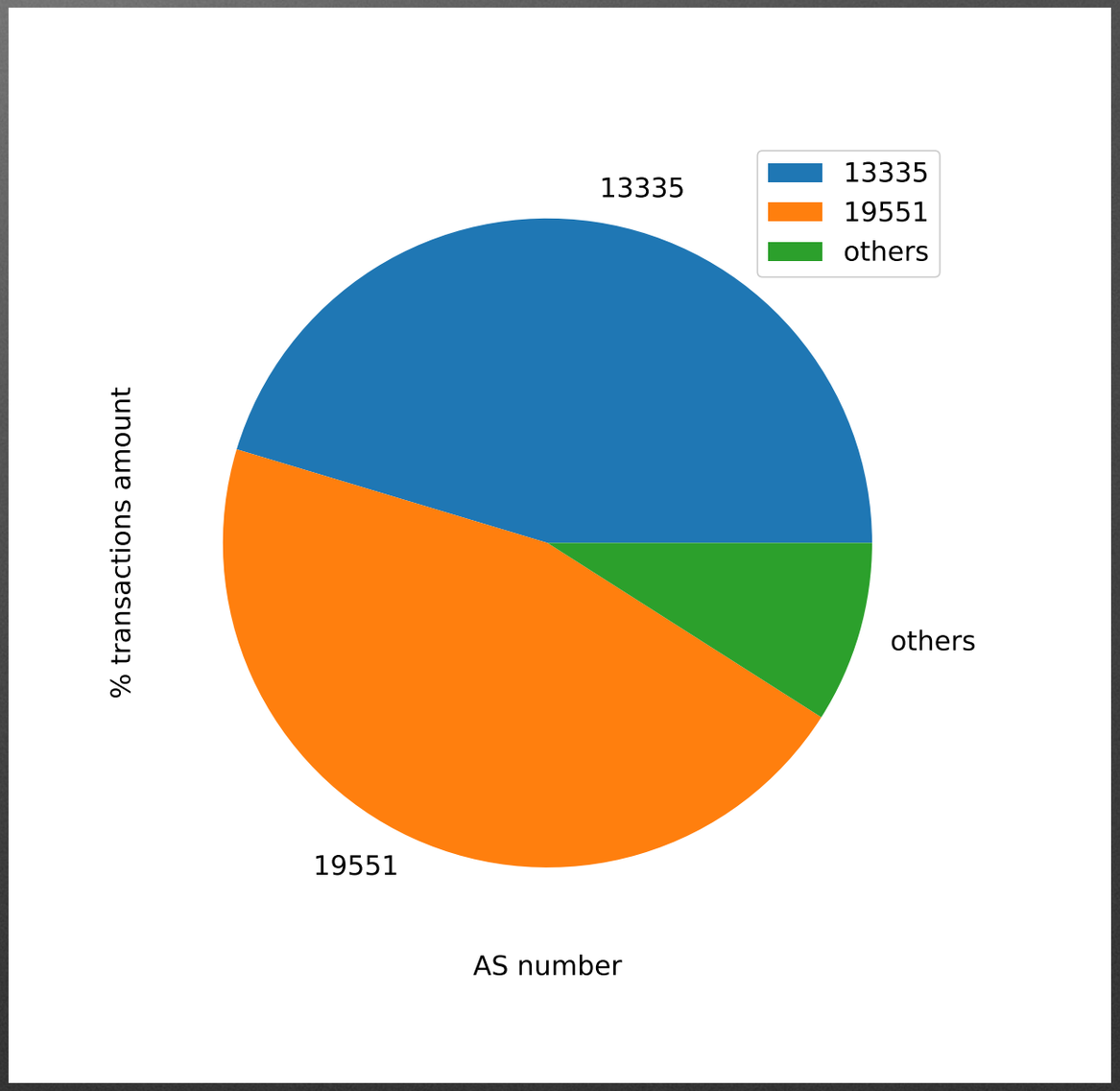
	Completed	Rerouted
Amazon	90%	10%
AT&T	60%	40%
China Telecom	20%	80%
Swisscom	30%	70%

Real Results

- Transactions analysis
- Which ASes are the most dangerous?
- What is the effect on the Ripple network?

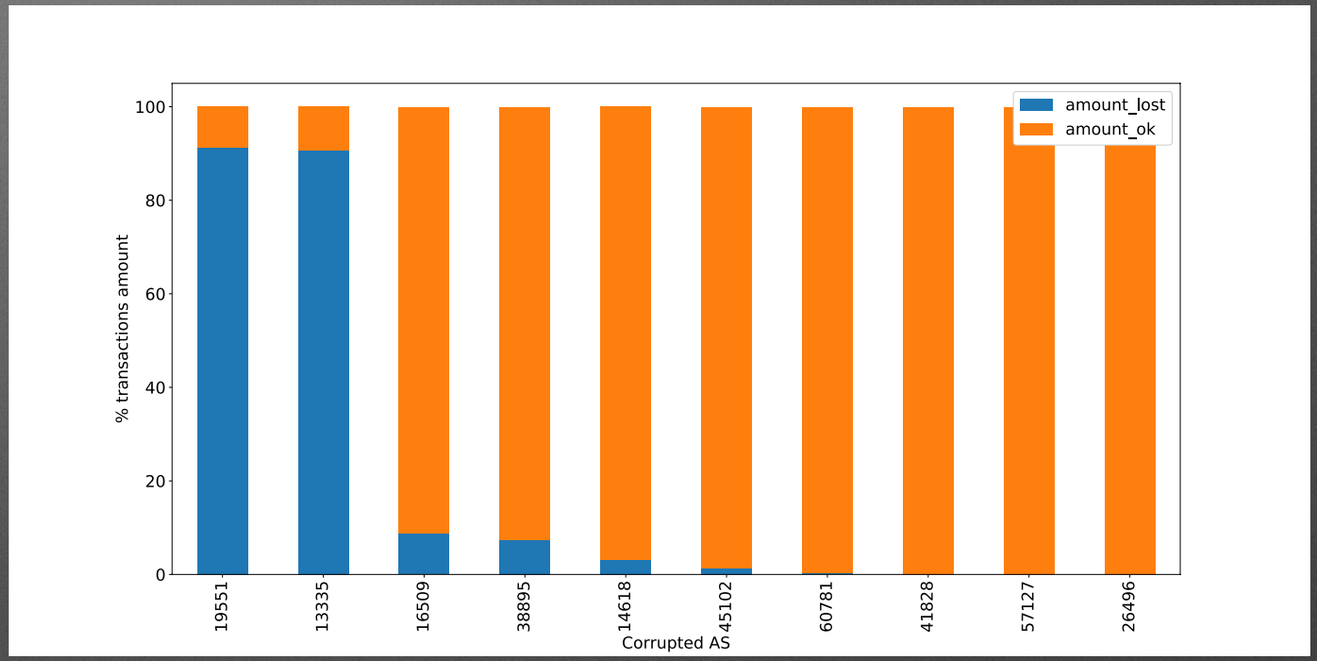
Transactions analysis

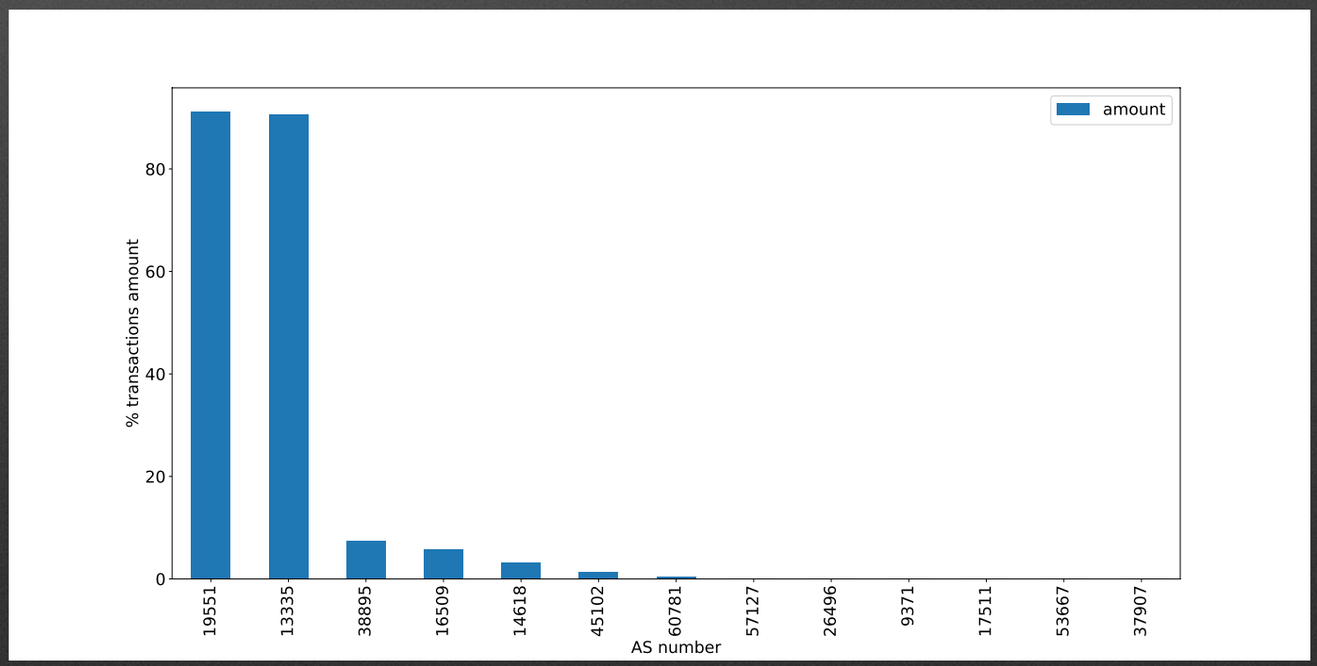
- % of transactions with AS as sender or receiver
- 13335 is Cloudflare (US)
- 19551 is Incapsula (US)



Which ASes are dangerous?
Traffic dropped

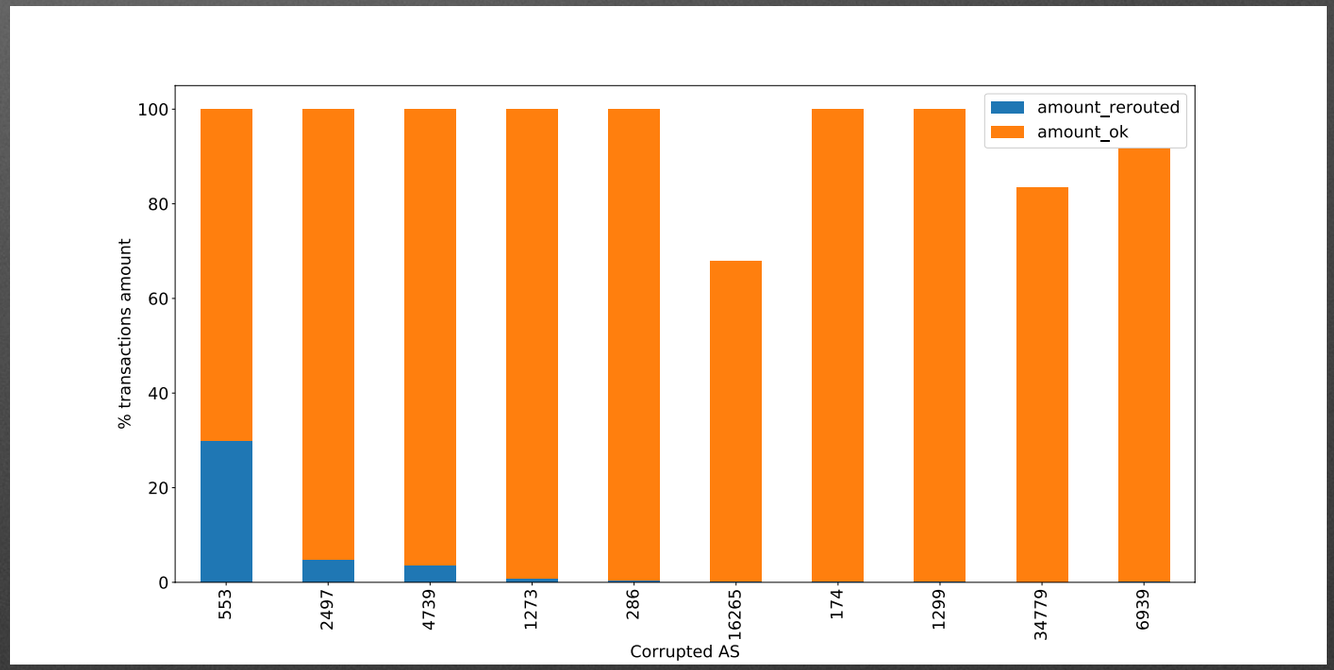
- % transactions lost corresponds to transactions distribution
- Lost if gateways in corrupted node
- Never lost if intermediaries
  - Always possible to find a path



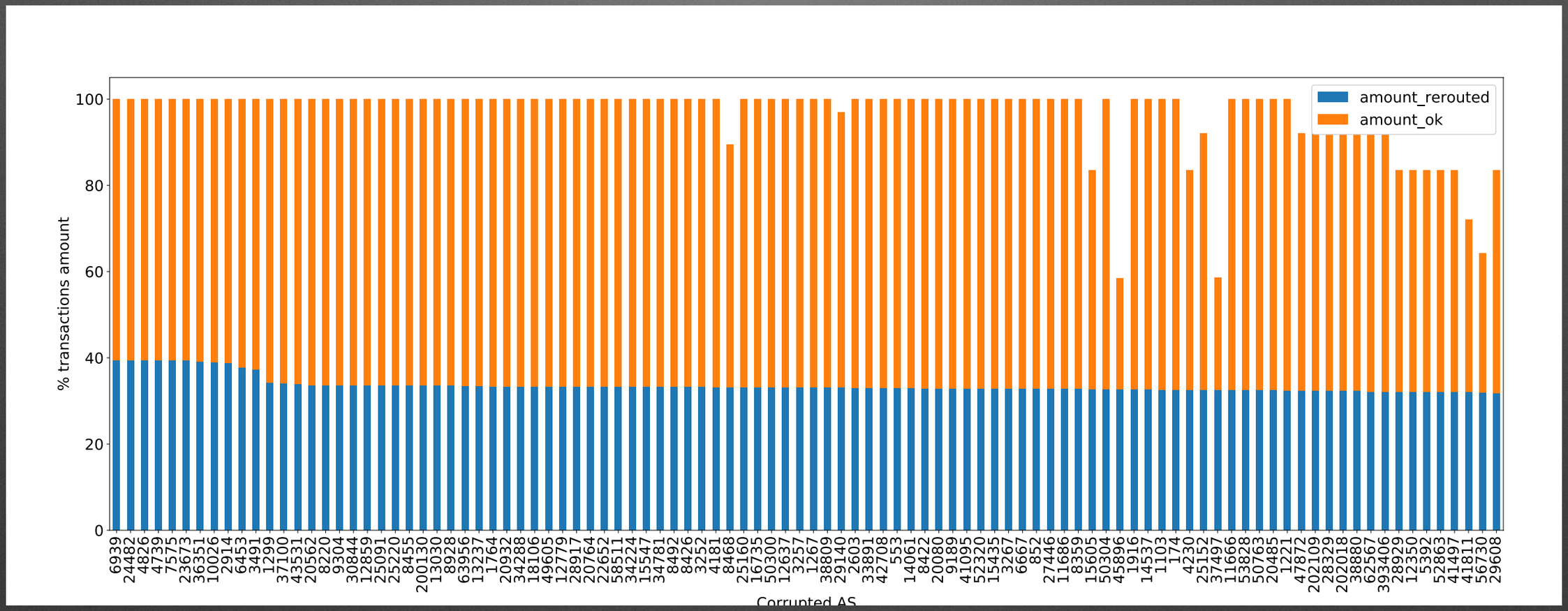


Which ASes are dangerous?
Traffic dropped

- Little % of rerouted transactions
- Certainly due to transactions distribution
- 553 is Belwue (DE)
  - Connections with 680 ISP
  - Switch, Swisscom



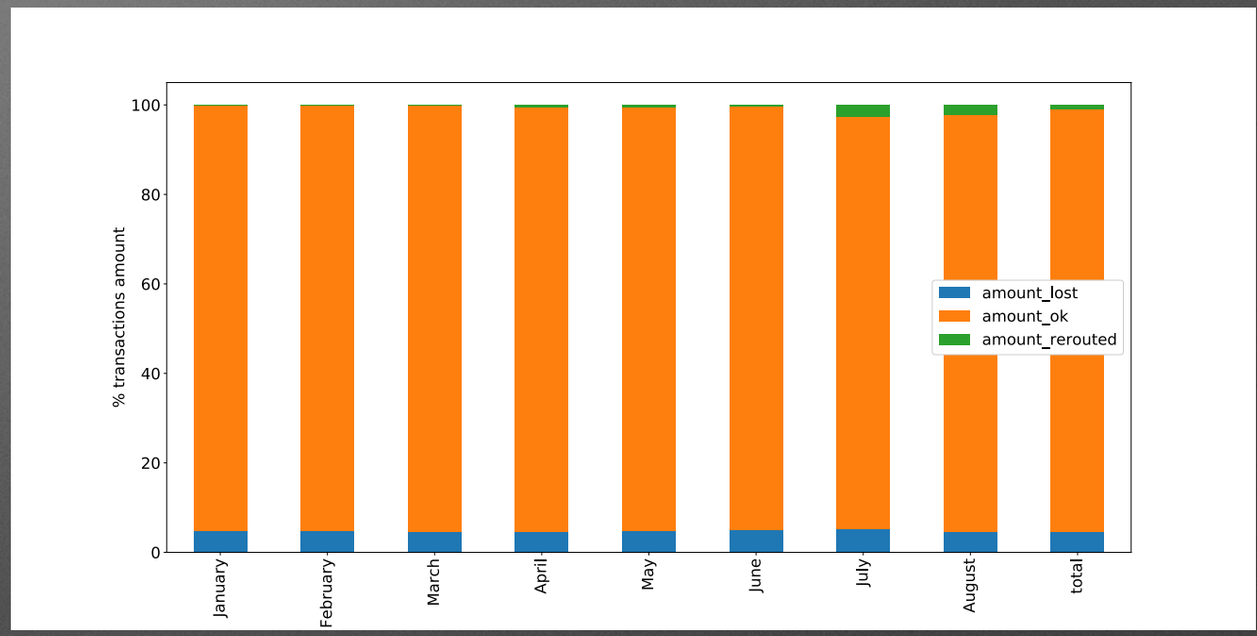
Which ASes are dangerous? BGP Hijacking

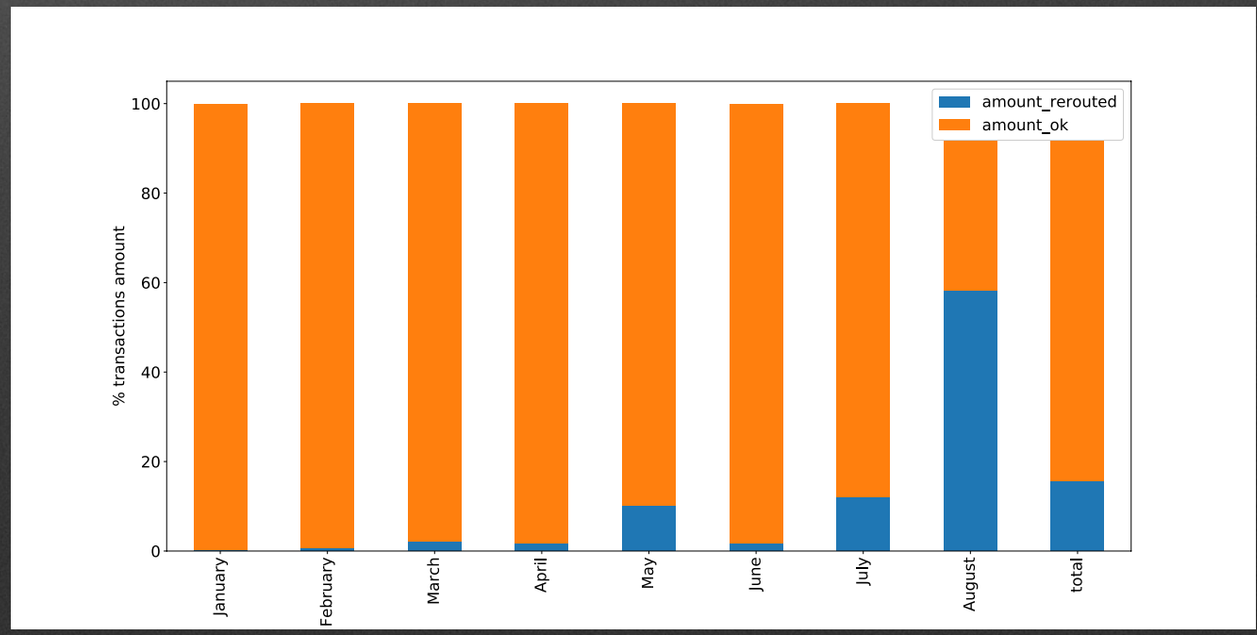


- Many ASes can corrupt the network
- Long list of ASes reach almost 40% of rerouted transactions

What is the effect on Ripple?

- Time analysis
- On average low effect



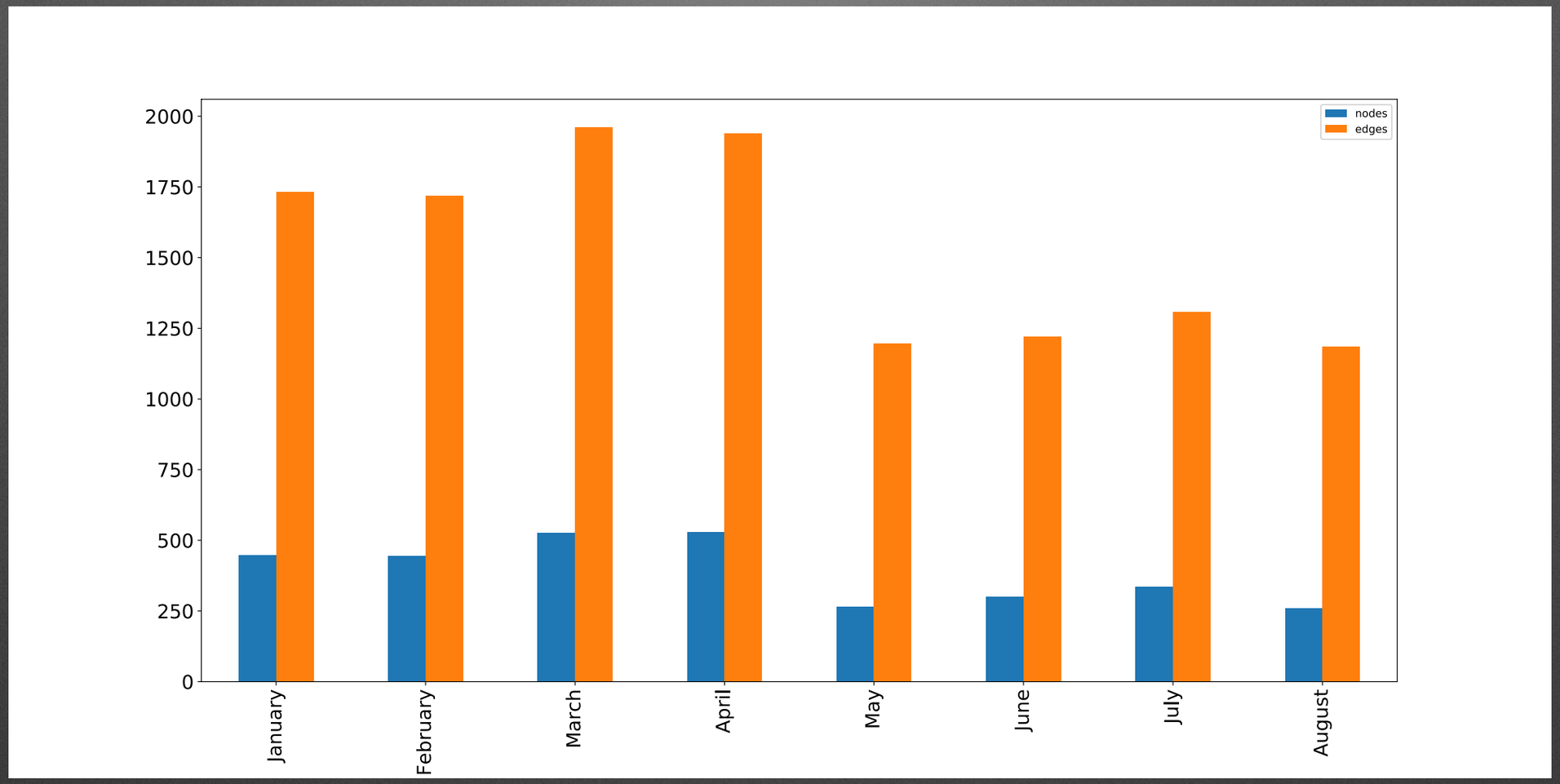


Conclusion

- Most of the transactions go through 2 ASes
  - Big impact if one of them is corrupted
- BGP Hijacking has more effect than traffic dropped
- Limitations of this analysis
  - Network only considers Gateways
  - Hence, only a few transactions are considered

Thank you for your attention

White gap?



In [36]:
```
for i in range(len(graphs_list)):
    print('16265 in {} : {}'.format(months[i],'16265' in graphs_list[i].nodes))
```

```
16265 in January : True
16265 in February : True
16265 in March : True
16265 in April : True
16265 in May : True
16265 in June : True
16265 in July : True
16265 in August : False
```

BGP Hijacking : August ?

In [43]:
```
for i in range(len(graphs_list)):
    print('Direct link for {} : {}'.format(months[i],graphs_list[i].has_edge('13335','19551')))
```

```
Direct link for January : True
Direct link for February : True
Direct link for March : True
Direct link for April : True
Direct link for May : True
Direct link for June : True
Direct link for July : True
Direct link for August : False
```