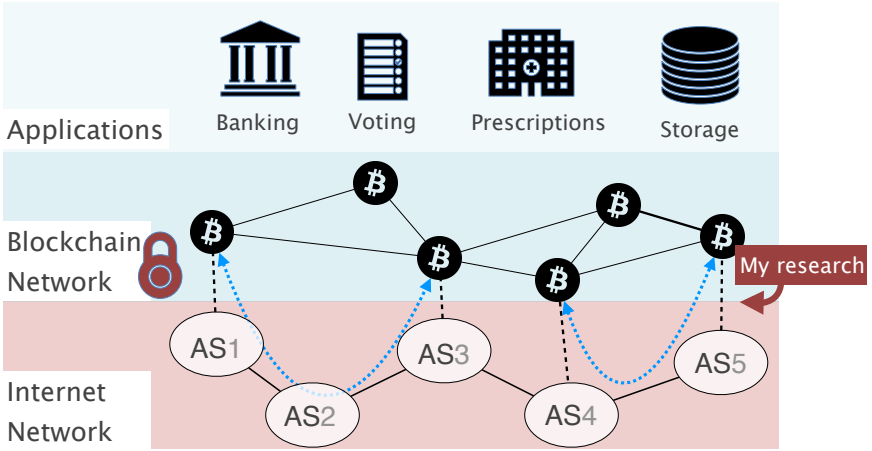
Routing Security for Blockchain Systems

Maria Apostolaki

My research is on the intersection of Networks and Blockchain

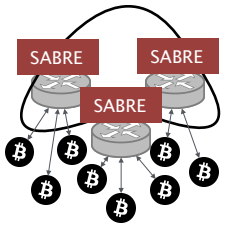


	Partitioning attack [1]	Delay Attack [1]	Perimeter Attack [4]
What:	Splits the Bitcoin network in two disjoint components	Delays the propagation of blocks to regular clients	Maps a client's transactions with their real-world identity
So what:	Double-spending Revenue loss Denial of Service	Zero-confirmation attack Mining power waste	Reveal transaction history Mass surveillance companies
Practicality	Any AS in the Internet can create a 50/50 partition by hijacking <100 IP prefixes	67% of clients can be eclipsed from at least 2 attackers for most of their up-time	40% of the clients can be deanonymized by ≥3 ASes with 90% accuracy

Routing attacks have network- & application-level enablers

- Few Internet networks intercept most of the Bitcoin traffic.
- Few Internet networks host most of the Bitcoin mining power.
- Traffic is unencrypted traffic and without integrity guarantees.
- There is no cross-layer visibility.
- Performance-oriented design choices work against security.

SABRE [2] relay network can protect the Bitcoin network from partitioning



SABRE is a relay network working alongside the Bitcoin network.

SABRE's node functionality is split between software & hardware.

SABRE nodes cannot be partitioned or DDoSed.

Routing attacks beyond Bitcoin

- The Partitioning and the Perimeter attacks generalize to other Blockchain systems.
- Routing attacks are also dangerous to other Internet services such as anonymity systems (Tor) and certificate authorities [3].
- There is a need for more secure routing protocols and network-level defenses.

References

[1] Hijacking Bitcoin: Routing Attacks on Cryptocurrencies. S&P '17

[2] SABRE: Protecting Bitcoin against Routing Attacks NDSS '19

[3] Securing Internet Applications from Routing Attacks CACM, to appear

[4] Routing Attacks on Cryptocurrencies Anonymity Under Submission