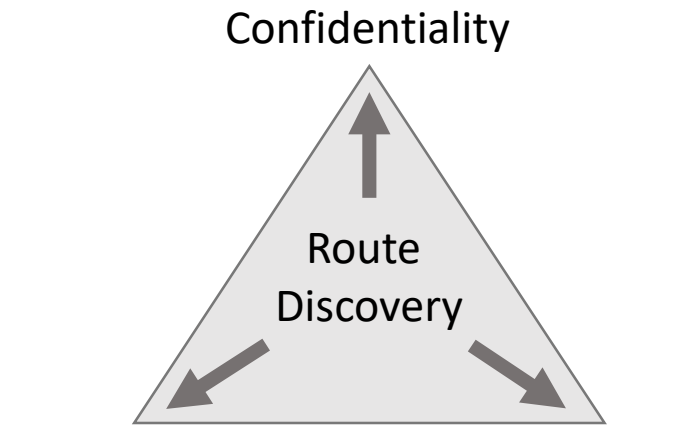
On Search Friction of Route Discovery in Off-chain Networks

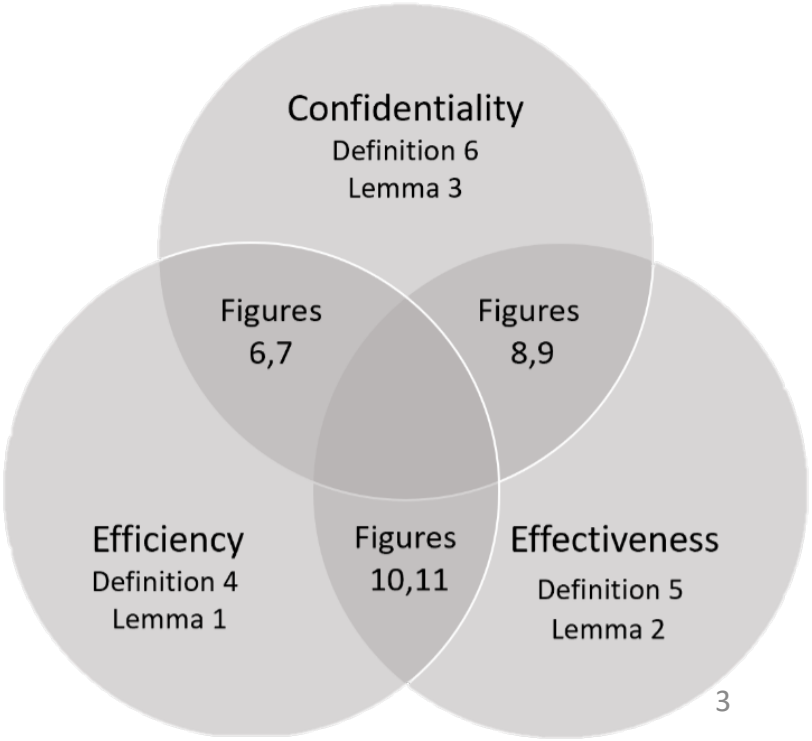
Saar Tochner
The Hebrew University
saart@cs.huji.ac.il

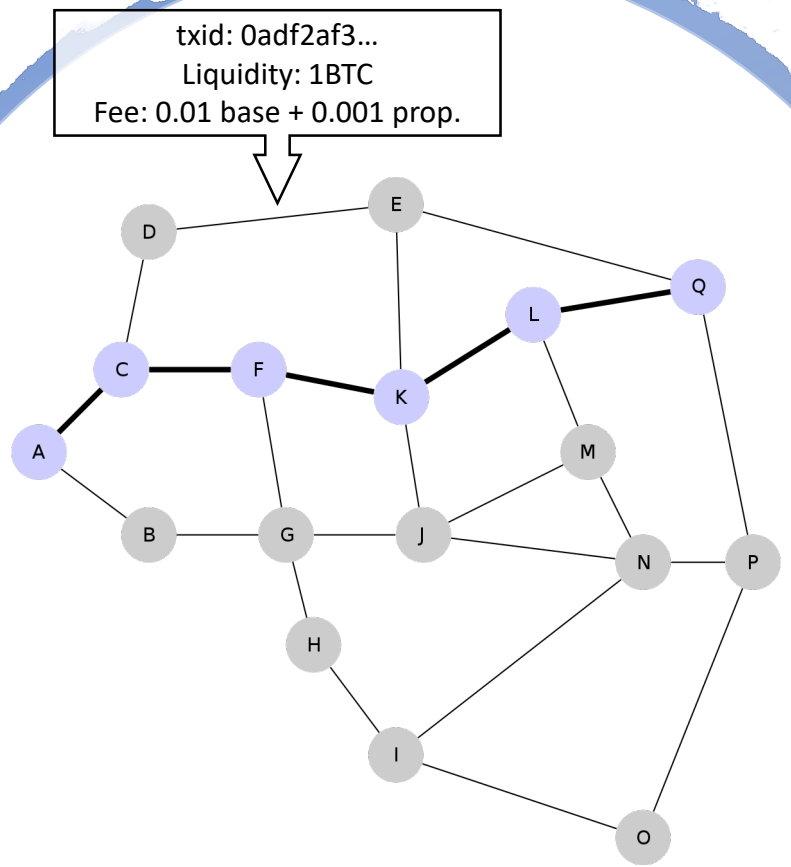
Stefan Schmid
University of Vienna
stefan_schmid@univie.ac.at


Confidentiality
Route
Discovery
Effectiveness
Efficiency

Agenda

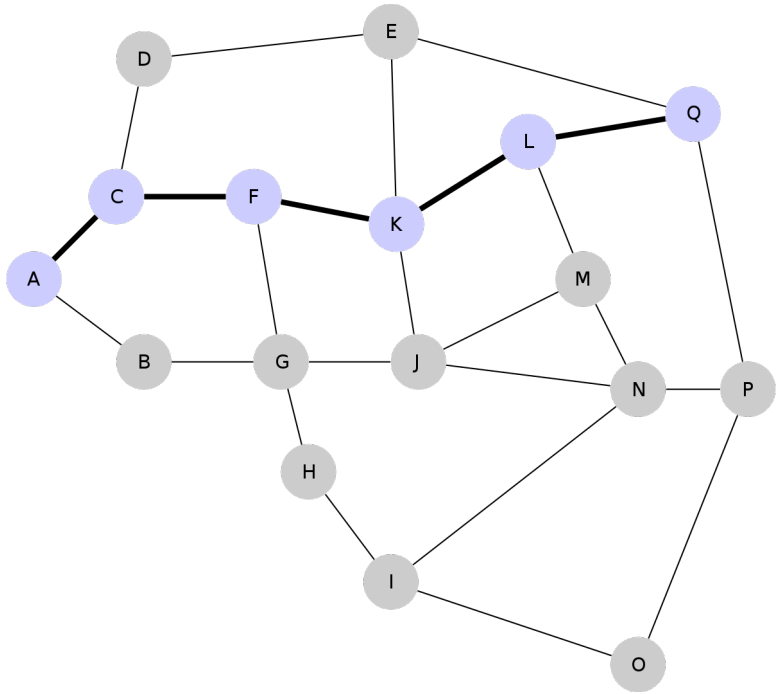
- The Lightning network
- The problem of scale
- Route Discovery Algorithm (RDA)
- Confidentially-Efficiency-Effectiveness
- Results





The Lightning Network

- Solution to Bitcoin's scalability issue
- Channel – locked liquidity between two parties
- Route – list of channels from source to target
- Transaction – atomic swap of liquidities across route
- Channel's fee – the cost that the owner demands to use it in a transaction
- Routing algorithm – choose the best route



The Problem of Scale

- How to choose a route?
  - High number of channels
  - Frequent changes
  - Mobile users
- Trampoline nodes
  - Selfishness

Definitions

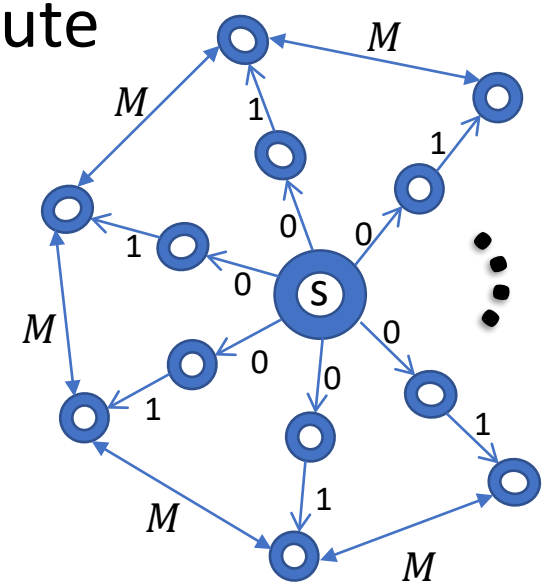
- **q-RDA** - route discovery algorithm that performs at most q queries to trampoline nodes and returns the best-found route or nothing
- **Efficiency** – $\frac{Weight\ of\ R}{Minimal\ weight\ of\ s \rightarrow t}$ for a route R from s to t
- **Effectiveness** - the number of queries which have to be issued to successfully execute a given transaction
- **Confidentiality** (Leak Rate) – how many more nodes will learn about the existence of this transaction compared to source routing

Analytical Results

- There is no perfect RDA:
  For every RDA there exists a topology in which the RDA is as bad as we want in Efficiency, Effectiveness and Confidentiality

- Example with low efficiency: If there are q+1 direct neighbors, then any q-RDA struggles to find an efficient route

- Examples with better measurements:
  Cliques, Scale-free networks

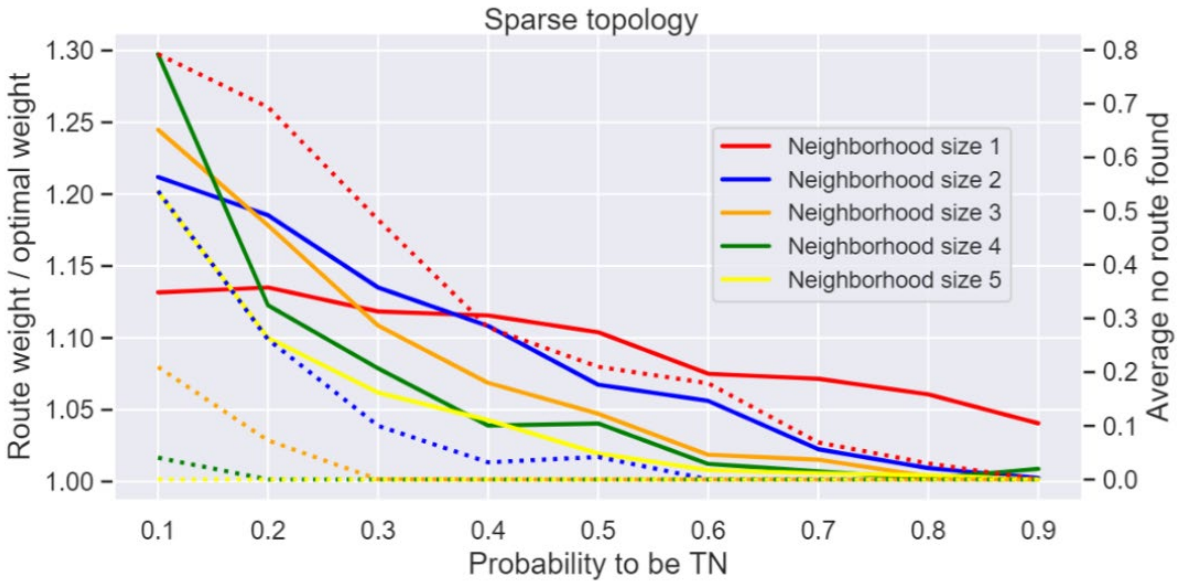


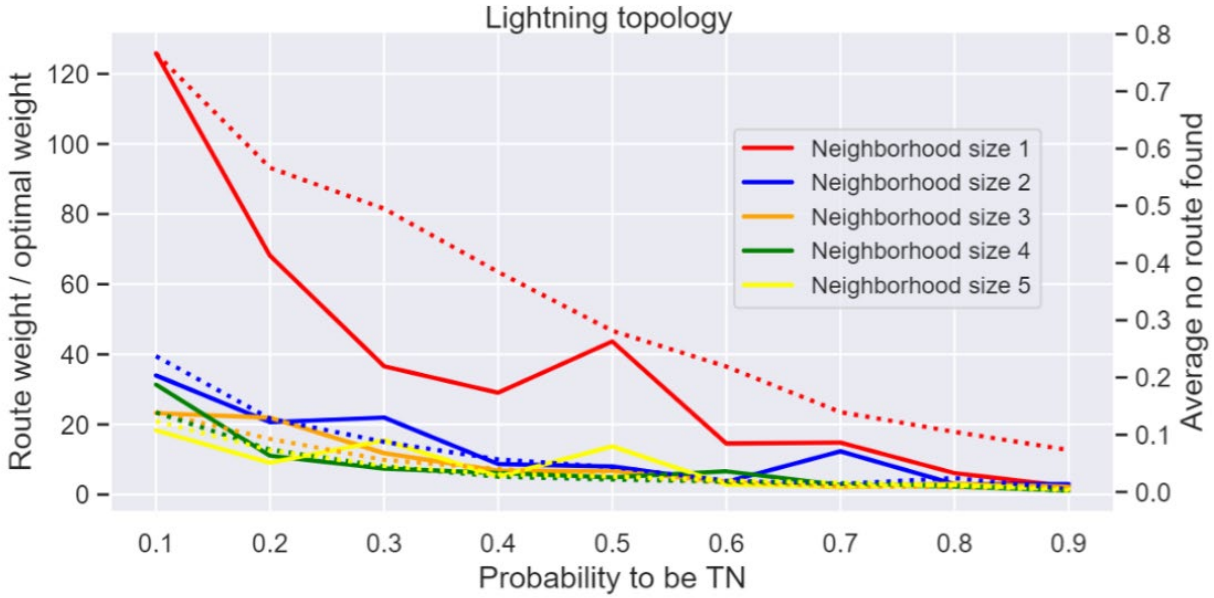
Empirical Evaluations

- Topologies:
  - The Lightning network (March. 24th 2020)
  - Sparse topology – nodes in a circle, with 2 outgoing links: to the next node and to a random node

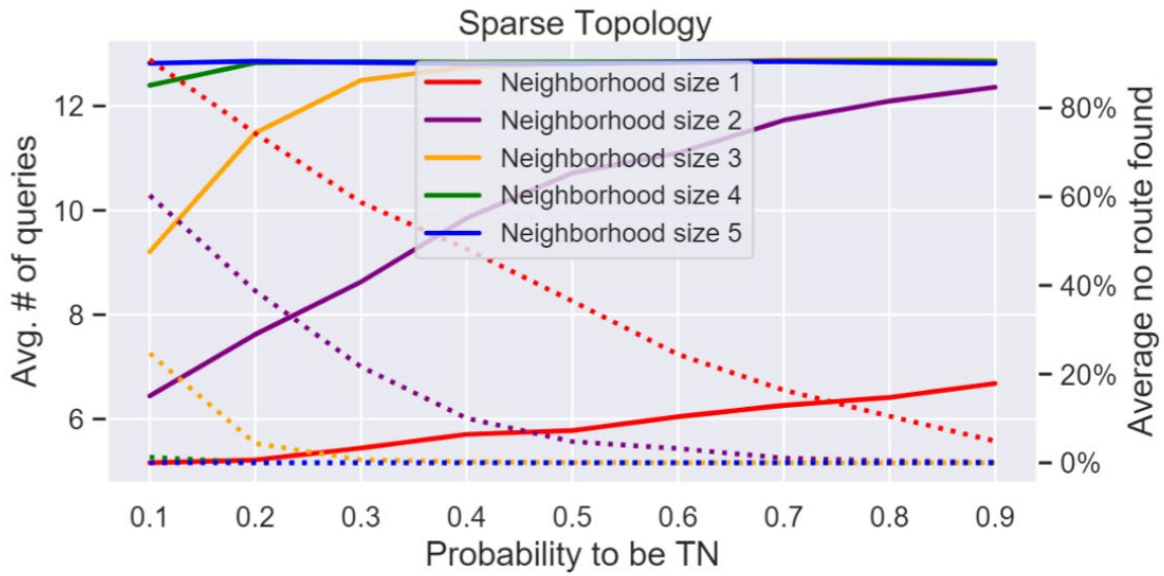
- Transactions Distributions:
  - Every pair performs a single transaction (uniform)
  - Power-law “activity level”

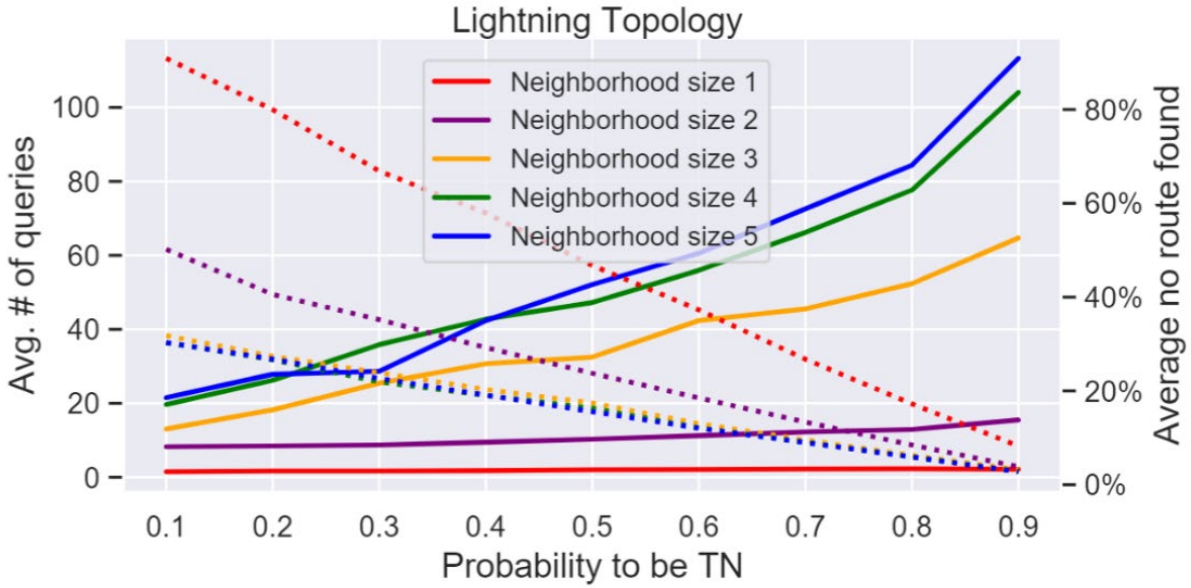
Efficiency-Confidentiality Tradeoff



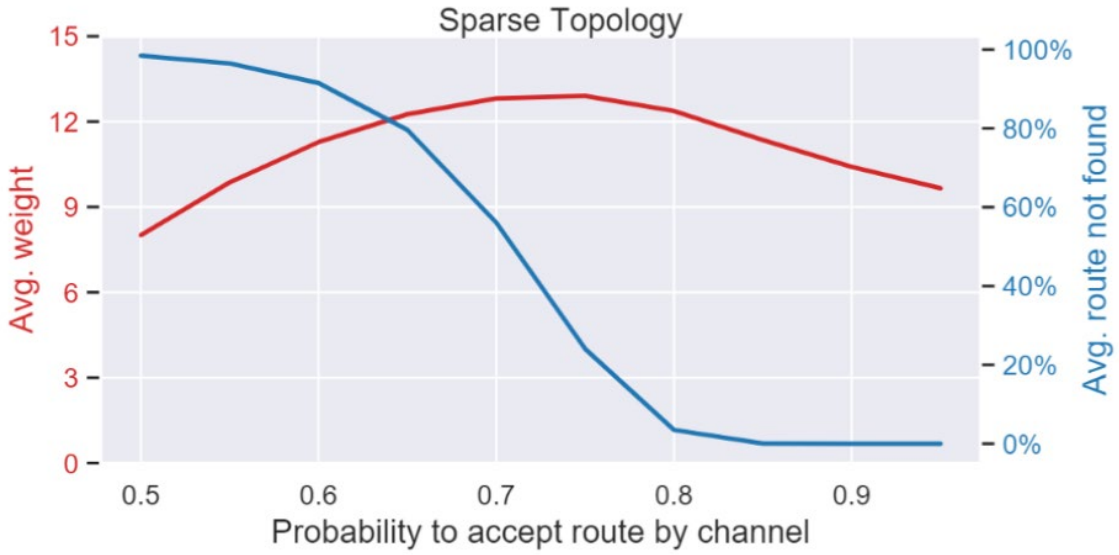


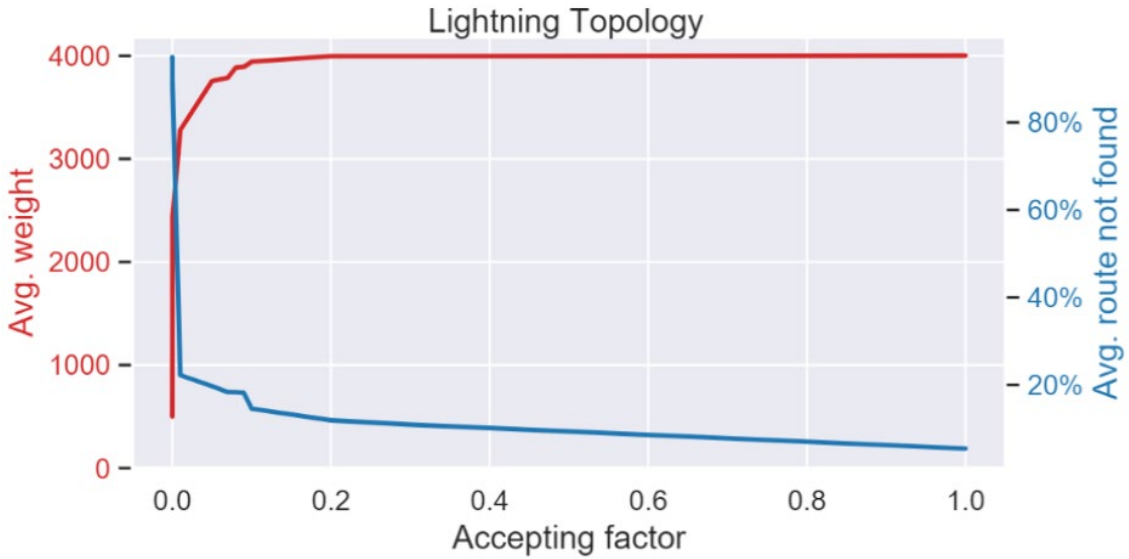
Effectiveness-Confidentiality Tradeoff



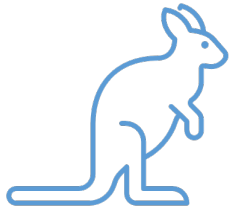


Effectiveness-Efficiency Tradeoff

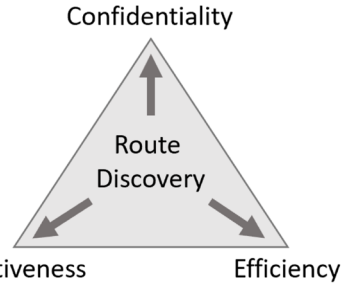




Take-aways



Trampoline nodes



Routing tradeoffs

Selfish Incentives

Questions?

Saar Tochner- saart@cs.huji.ac.il
Stefan Schmid - stefan_schmid@univie.ac.at

https://medium.com/blockchains-huji/routing-with-selfish-information-sharing-6ade69235531