Technische Universität Berlin

EINSTEIN CENTER Digital Future

TOWARDS A DISTRIBUTED ROUTE SELECTION FOR PAYMENT CHANNEL NETWORKS

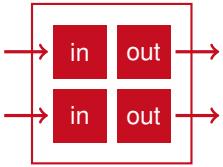
Elias Rohrer | Jann-Frederik Laß | Florian Tschorsch
Distributed Security Infrastructures

BITCOIN

first decentralized
digital currency

BITCOIN SCALABILITY

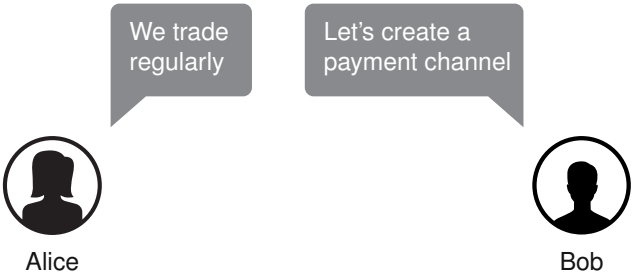
$$\frac{166\,\mathrm{B}/1\,\mathrm{MB}}{10\,\mathrm{min}} \approx 10\,\mathrm{tx/s}$$



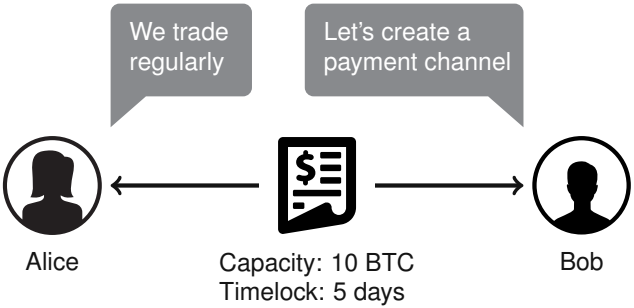
$$\frac{371\,\mathrm{B}/1\,\mathrm{MB}}{10\,\mathrm{min}} \approx 4\,\mathrm{tx/s}$$

VISA handles on average around 2,000 transactions per second (tps), so call it a daily peak rate of 4,000 tps. It has a peak capacity of around 56,000 transactions per second (2015)

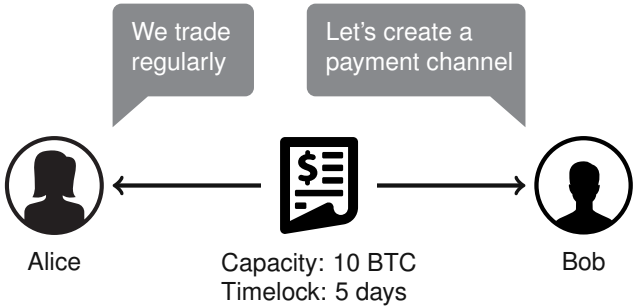
PAYMENT CHANNELS



PAYMENT CHANNELS

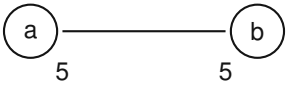


PAYMENT CHANNELS

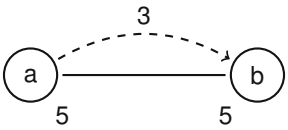


By using smart contracts and processing transactions off-chain, payment channels scale to high transaction rates

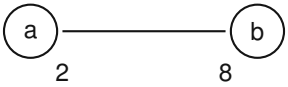
EXAMPLE: PAYMENT CHANNELS



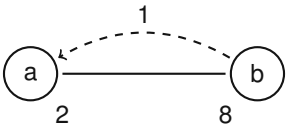
EXAMPLE: PAYMENT CHANNELS



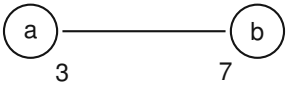
EXAMPLE: PAYMENT CHANNELS



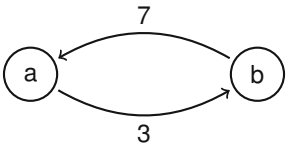
EXAMPLE: PAYMENT CHANNELS



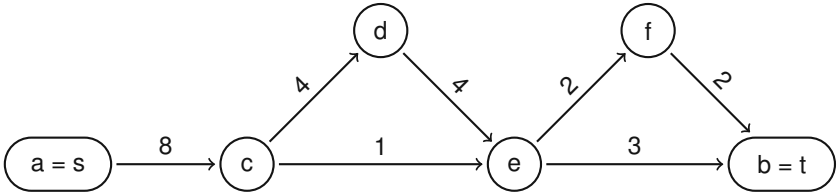
EXAMPLE: PAYMENT CHANNELS



EXAMPLE: PAYMENT CHANNELS

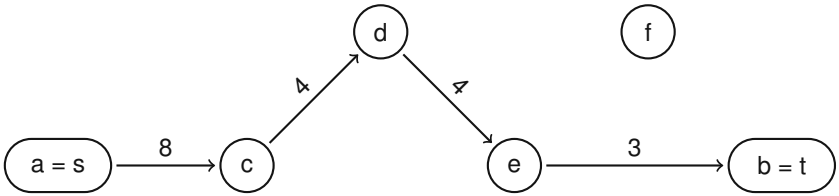


PAYMENT CHANNEL NETWORKS



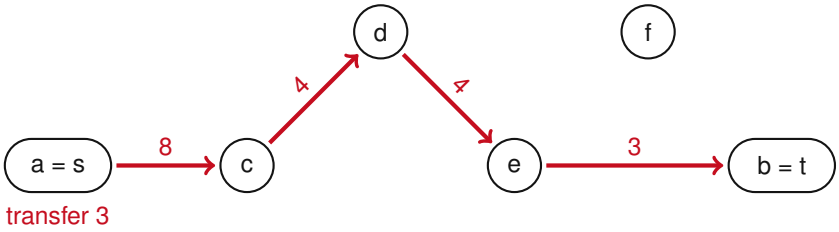
PAYMENT CHANNEL NETWORKS

Single-Path Routing



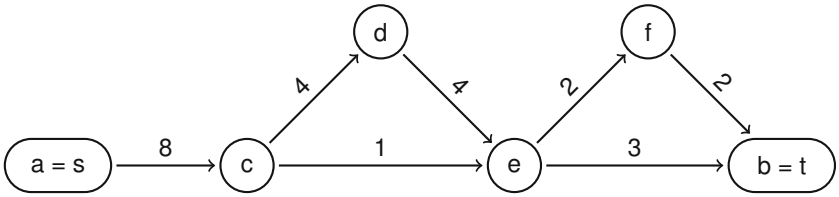
PAYMENT CHANNEL NETWORKS

Single-Path Routing



PAYMENT CHANNEL NETWORKS

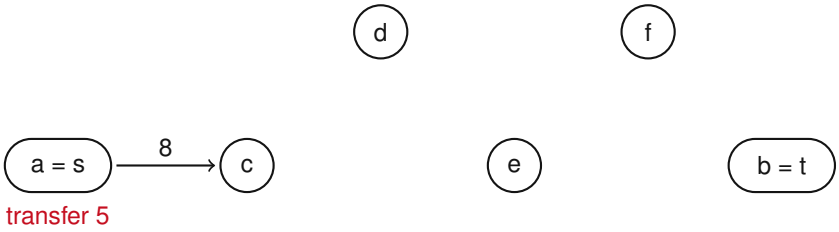
Single-Path Routing



transfer 5

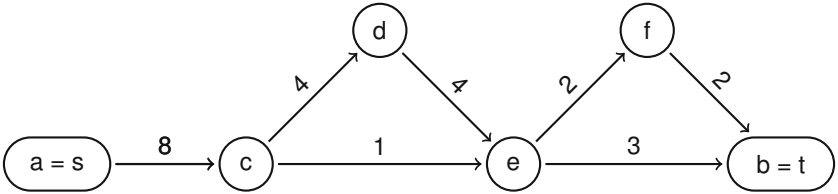
PAYMENT CHANNEL NETWORKS

Single-Path Routing



PAYMENT CHANNEL NETWORKS

Single-Path Routing



SINGLE-PATH ROUTING UNNECESSARILY LIMITS THE MAXIMUM TRANSFERABLE AMOUNT

PAYMENT CHANNEL NETWORKS

CONSIDER PAYMENT CHANNEL NETWORKS AS FLOW NETWORKS

In the following, we ...

- ... consider PCNs as flow networks, i.e., multi-path routing
- ... propose the push-relabel algorithm as a candidate
- ... develop an extension to enable distributed route selection

Elias Rohrer, Jann-Frederik Laß, and Florian Tschorsch. “Towards a Concurrent and Distributed Route Selection for Payment Channel Networks.” Data Privacy Management, Cryptocurrencies and Blockchain Technology. Springer, 2017. 411-419.

PUSH-RELABEL ALGORITHM

- algorithm for computing maximum flows
- uses local knowledge, i.e., good for distributed execution

  `push`: If the current node has excess flow, transfer it to a neighbor of smaller height (excess flows run “downhill” only)

  `relabel`: If no suitable neighbor exists, increase the node height
- eventually, only nodes *s* and *t* have excess flow, i.e., we found a maximum flow

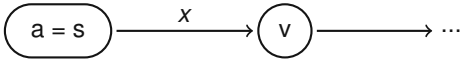
PUSH-RELABEL ALGORITHM

- algorithm for computing maximum flows
- uses local knowledge, i.e., good for distributed execution

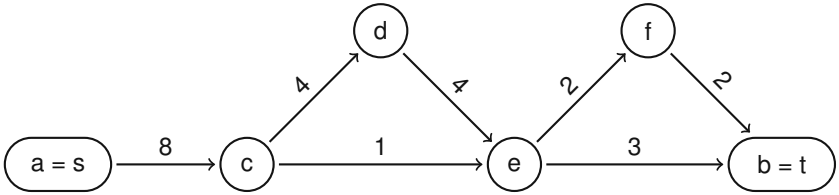
  `push`: If the current node has excess flow, transfer it to a neighbor of smaller height (excess flows run “downhill” only)

  `relabel`: If no suitable neighbor exists, increase the node height
- eventually, only nodes s and t have excess flow, i.e., we found a maximum flow

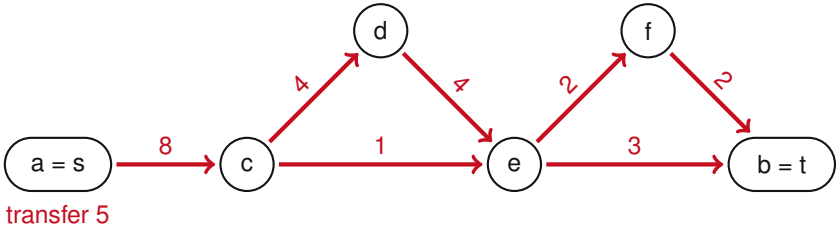
- adaptable to find feasible flows of volume x



MULTI-PATH ROUTING



MULTI-PATH ROUTING



DISTRIBUTED PATH SELECTION

With the Push-Relabel Algorithm

SEQUENTIAL EXECUTION

- only one instance of the algorithm at a time
- requires a coordinating central authority
- too slow for large networks

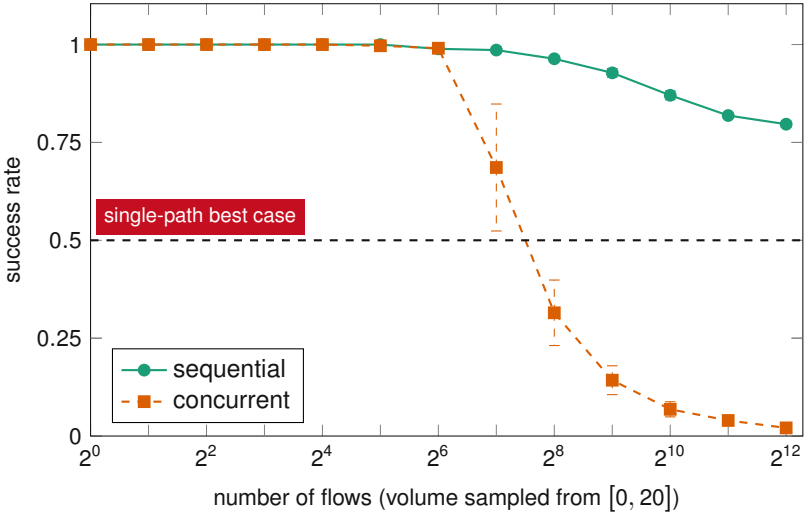
CONCURRENT EXECUTION

- distributed scenario, i.e., multiple flows are routed at the same time
- problem: simply executing multiple instances does not work, i.e., flows will *steal* capacity
- solution: *capacity locking*, i.e., account each flow volume independently while respecting the total channel capacity
- capacity locking is implemented as `locked-push`, which pushes a *specific* flow on an edge

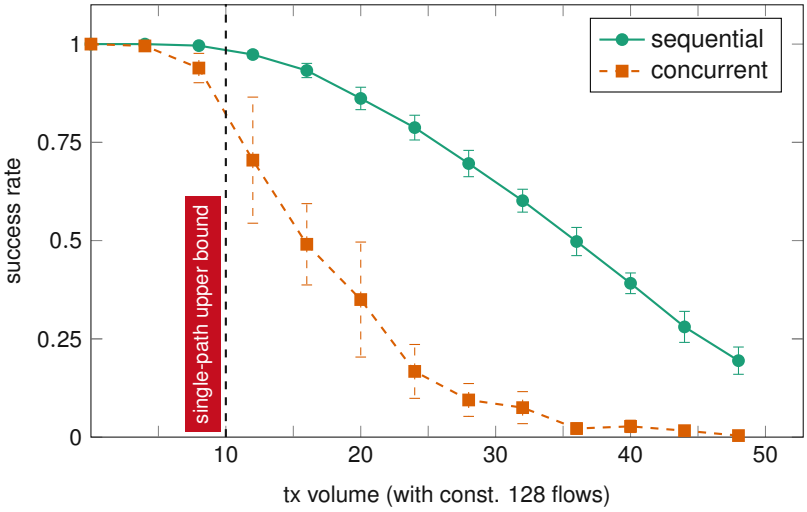
EVALUATION METHODOLOGY

- simulation for sequential and concurrent executions of the algorithm
- 10 randomly generated scenarios
  - Watts-Strogatz graph with $\beta = 0.5$, $n = 200$, $deg = 10$
  - capacities picked by uniform random sampling from $[0, 10]$
- how many flows of what size can we route?

NUMBER OF FLOWS



TRANSACTION VOLUME



Conclusion

- payment channels scale to high transaction rates
- single-path routing unnecessarily limits the transferrable amount

Conclusion

- payment channels scale to high transaction rates
- single-path routing unnecessarily limits the transferrable amount

- multi-path routes are needed to utilize available capacities
- therefore, consider payment channel networks as flow networks

Conclusion

- payment channels scale to high transaction rates
- single-path routing unnecessarily limits the transferrable amount

- multi-path routes are needed to utilize available capacities
- therefore, consider payment channel networks as flow networks

- we identified the push-relabel algorithm as a candidate for multi-path route selection
- we extended it to enable concurrent and distributed execution
- we showed that our algorithm is able to satisfy demands where single-path approaches fail