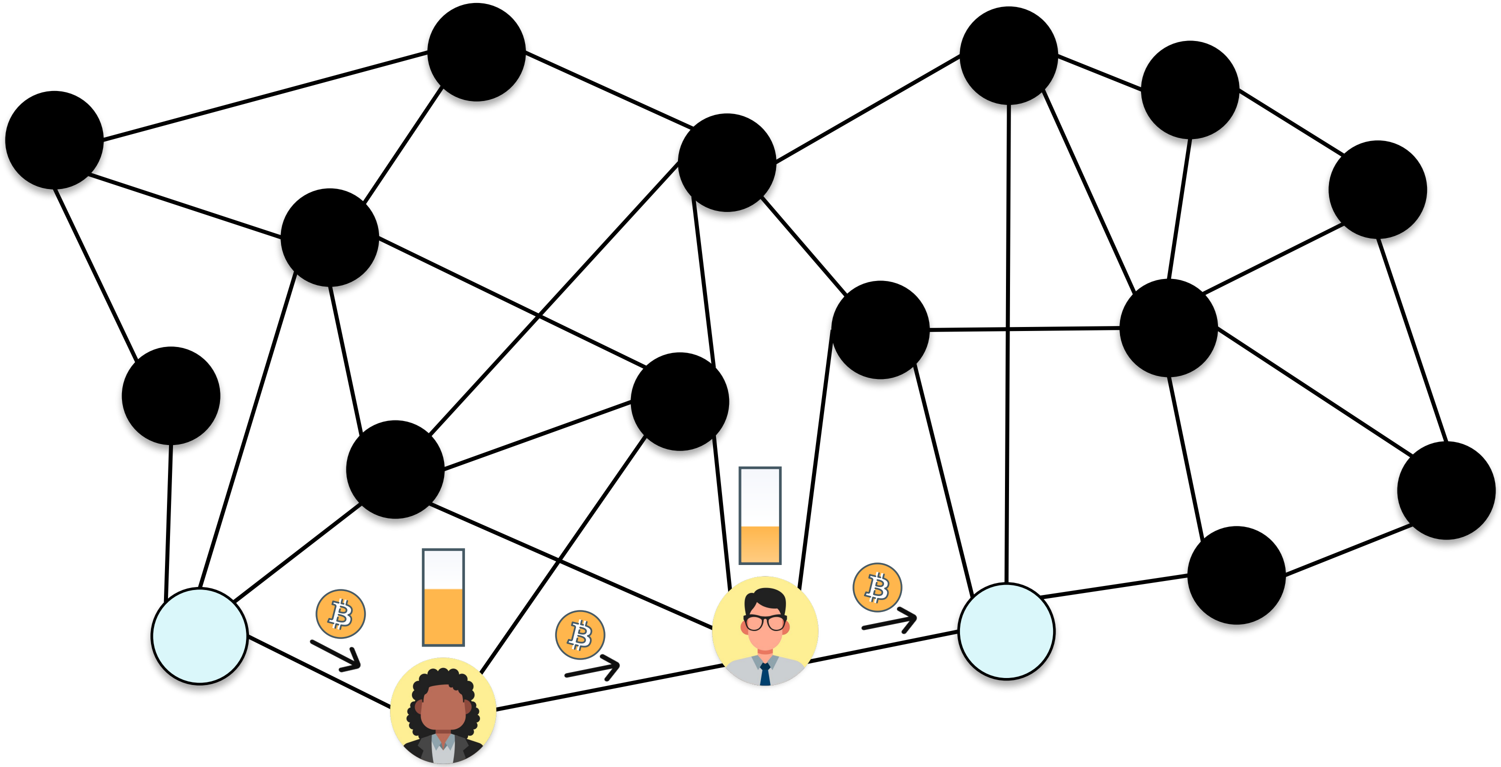
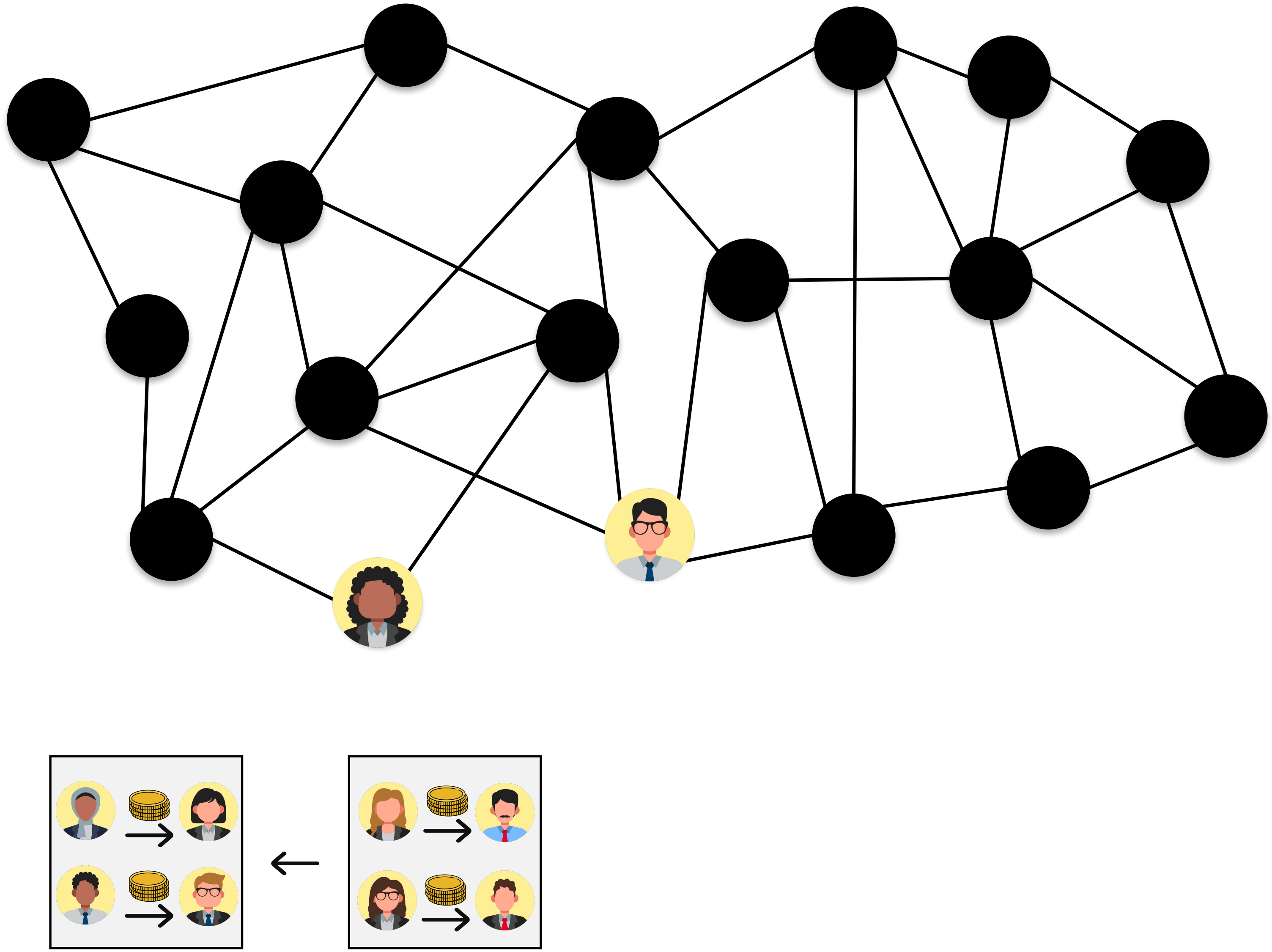
On the Lifecycle of a Lightning Network Payment Channel



Florian Grötschla, Lioba Heimbach, Severin Richner and Roger Wattenhofer
ETH Zurich

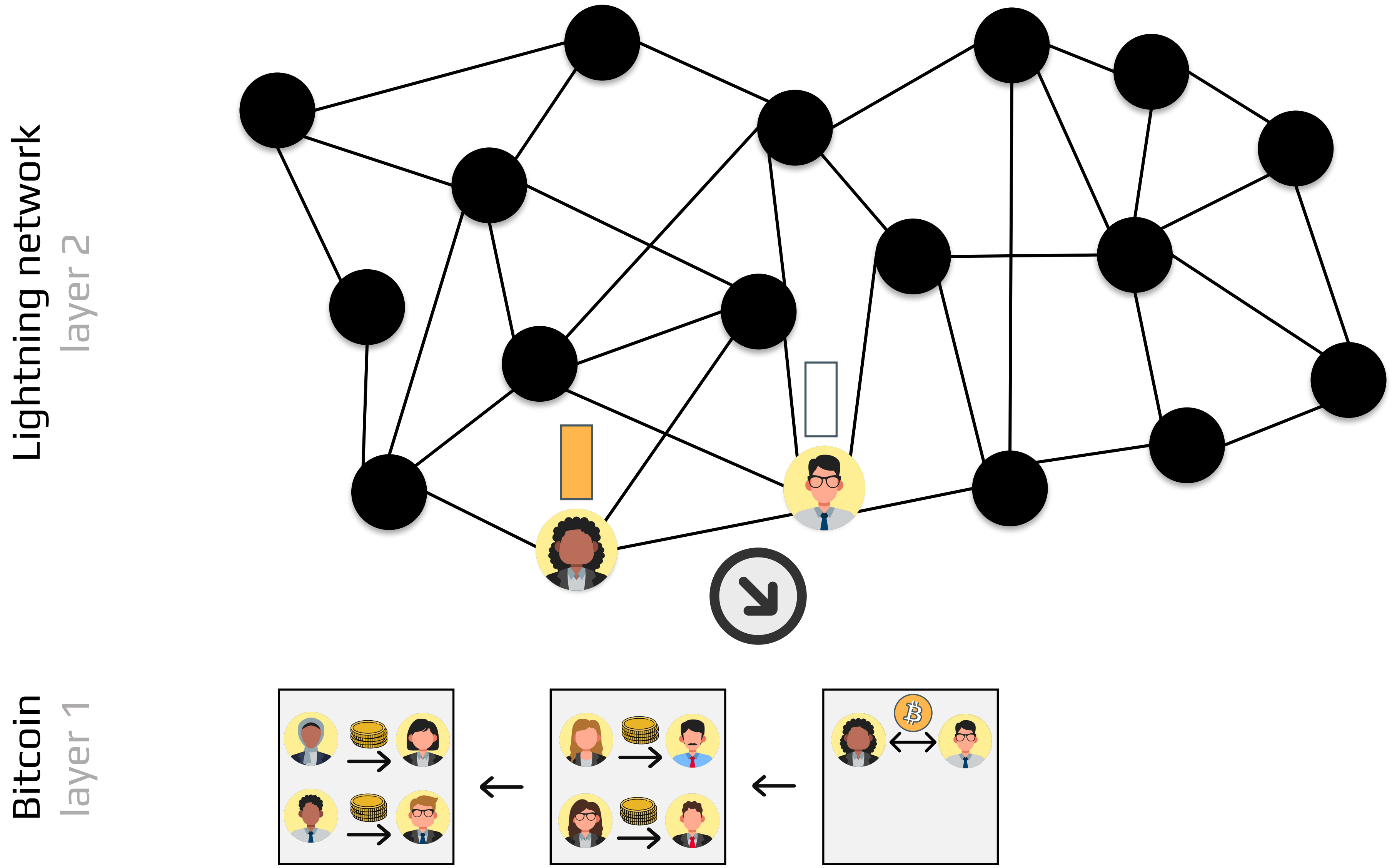
Payment channels



Lightning network
layer 2

Bitcoin
layer 1

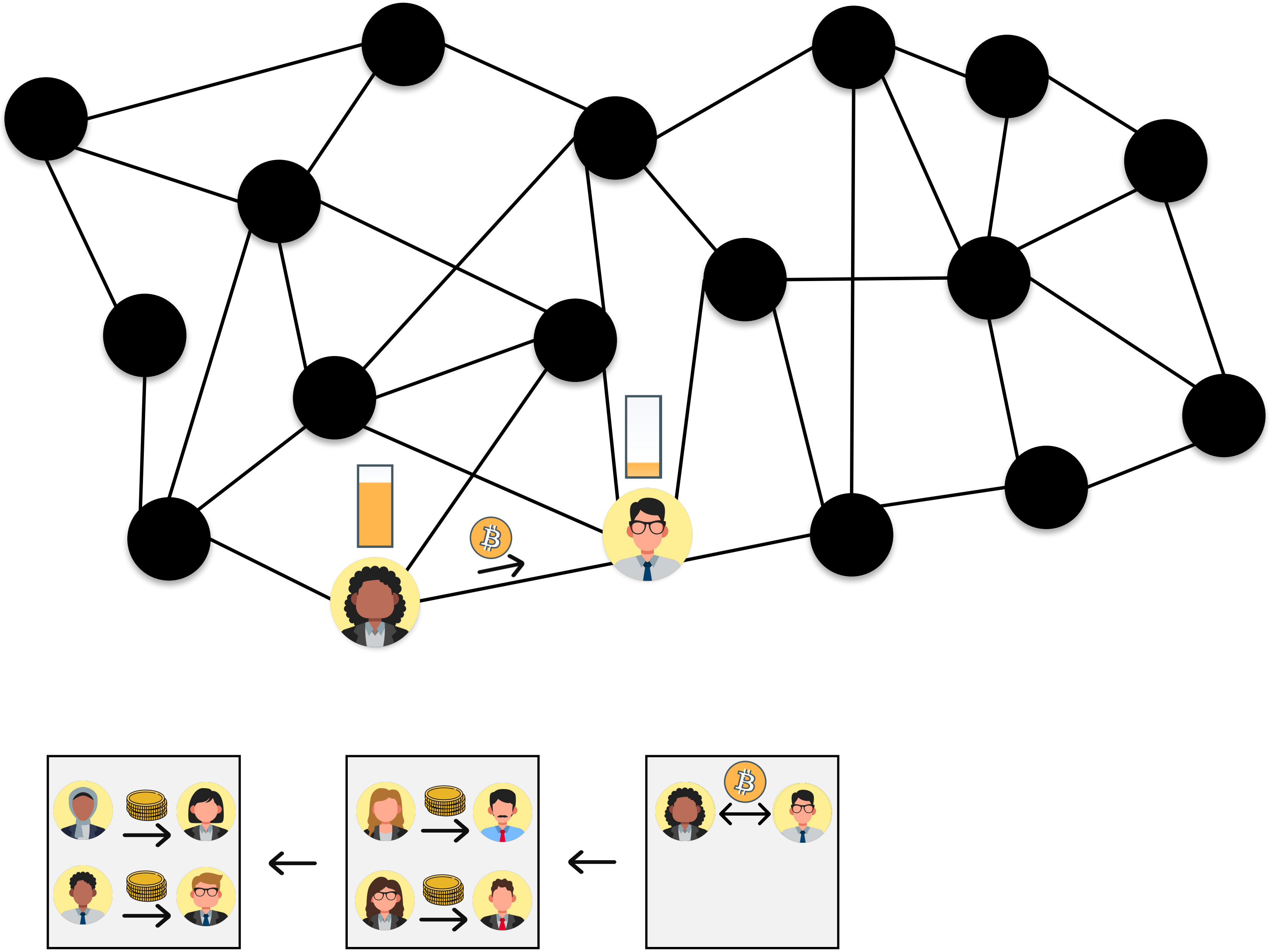
Payment channels – channel opening



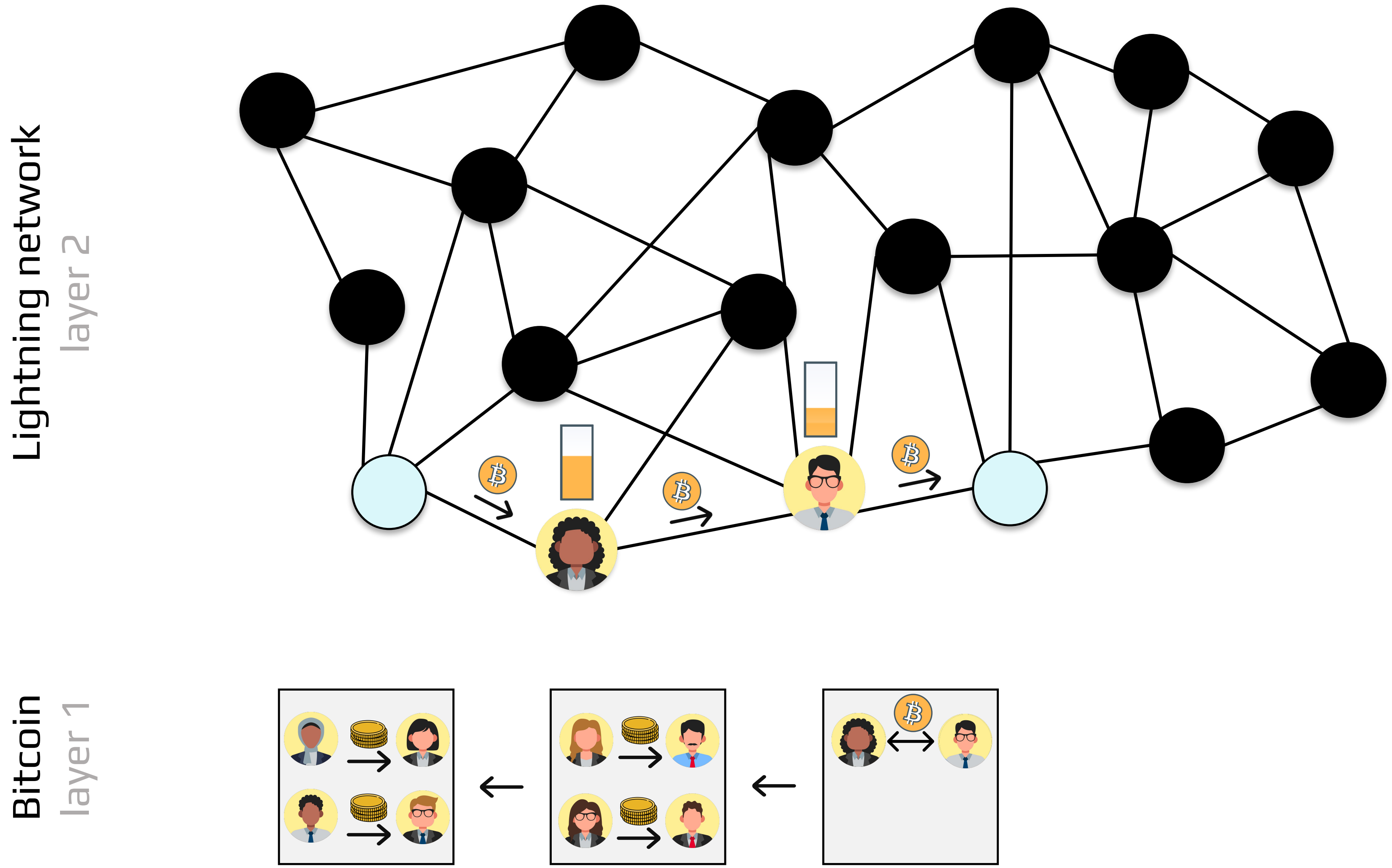
Payment channels – channel lifetime

Lightning network
layer 2

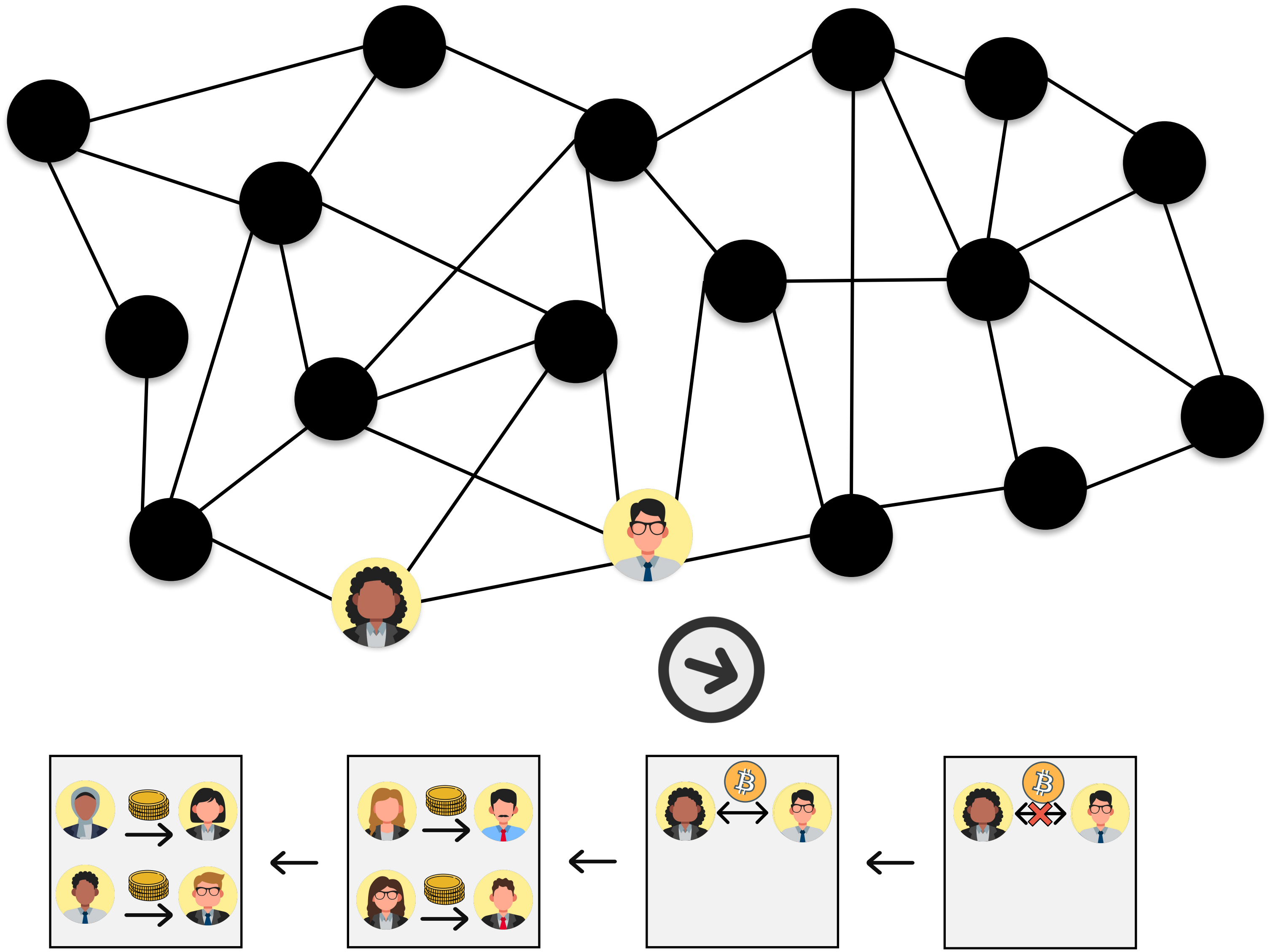
Bitcoin
layer 1



Payment channels – channel lifetime



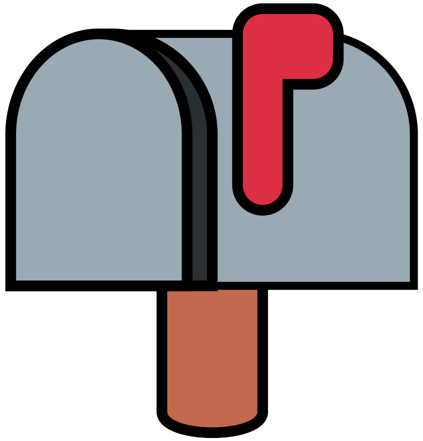
Payment channels – channel closing



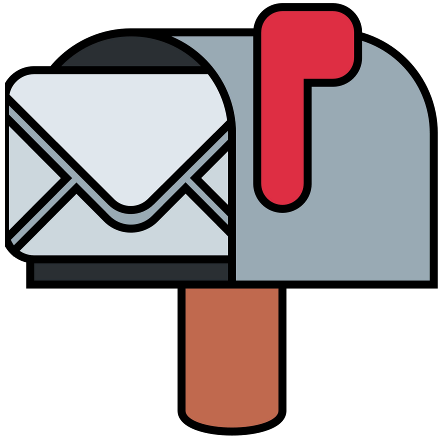
Lightning network
layer 2

Bitcoin
layer 1

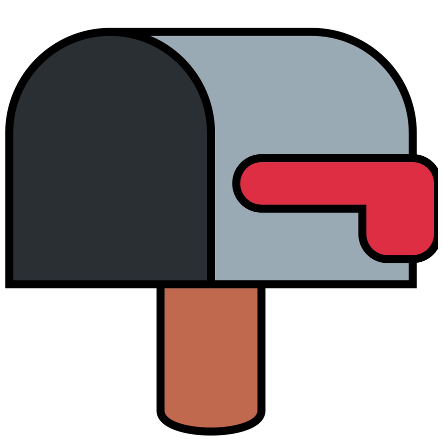
Lifecycle of a Channel



opening



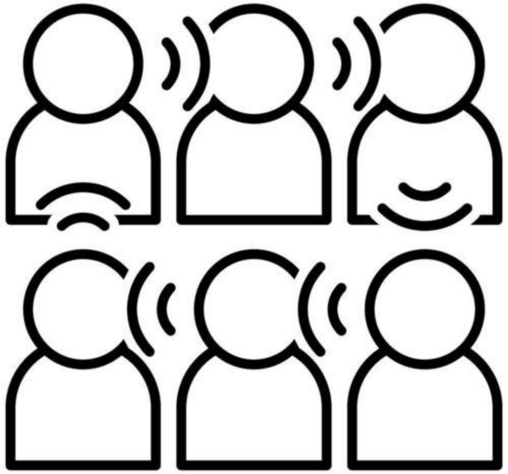
lifetime



closing

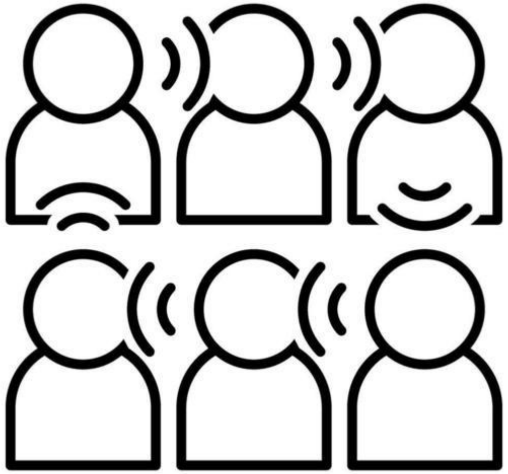
Data collection

gossip data



Data collection

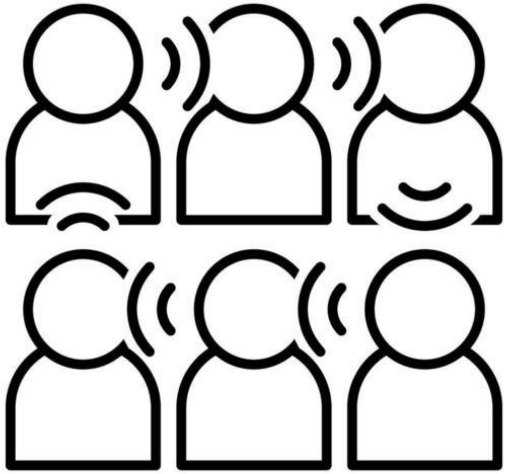
gossip data



- channel announcements
- node announcements
- channel updates (fees, ...)

Data collection

gossip data

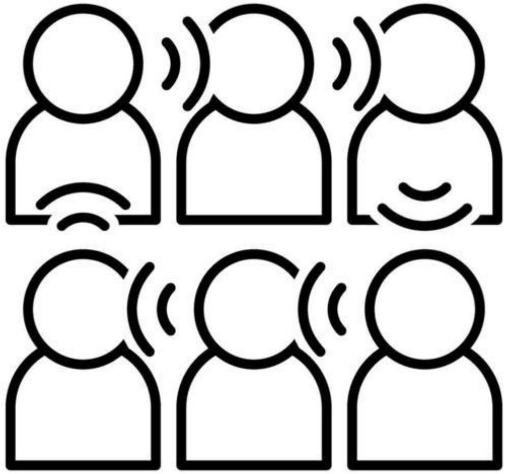


- channel announcements
- node announcements
- channel updates (fees, ...)

Bitcoin data

Data collection

gossip data



- channel announcements
- node announcements
- channel updates (fees, ...)

Bitcoin data

- private channel detection
- channel closing classification

Methodology

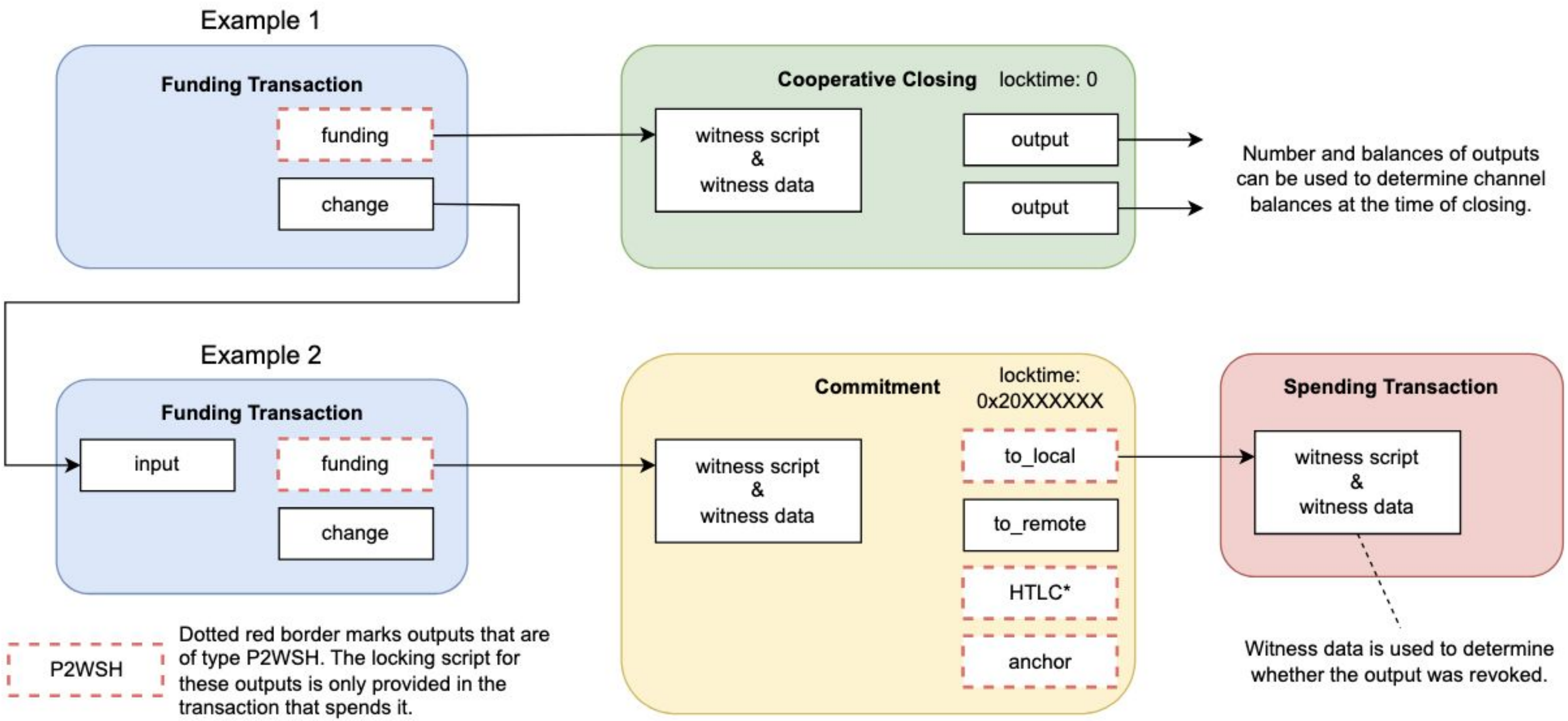
Private Channels

Many channels remain unannounced.
We adopt heuristics from Kappos et al. to identify likely private channels.

On-chain Analysis

- Trace funding transactions to their spending outputs.
- Distinguish closing types (commitment, cooperative, etc.)
- Classify output roles (local, remote, HTLCs, change)

Transaction flow

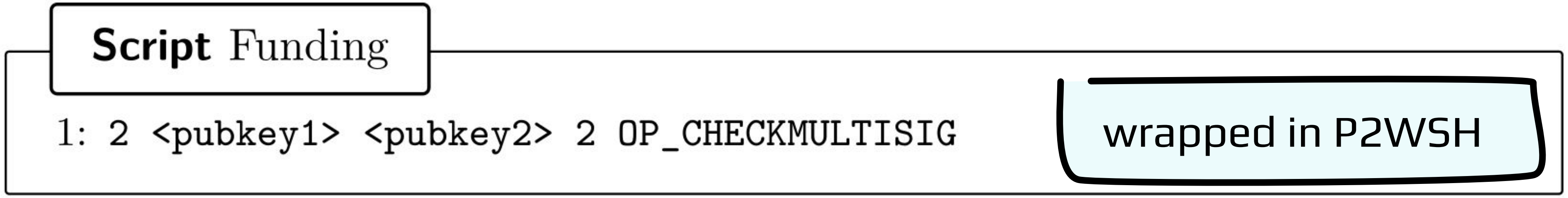


Number and balances of outputs can be used to determine channel balances at the time of closing.

Witness data is used to determine whether the output was revoked.

Dotted red border marks outputs that are of type P2WSH. The locking script for these outputs is only provided in the transaction that spends it.

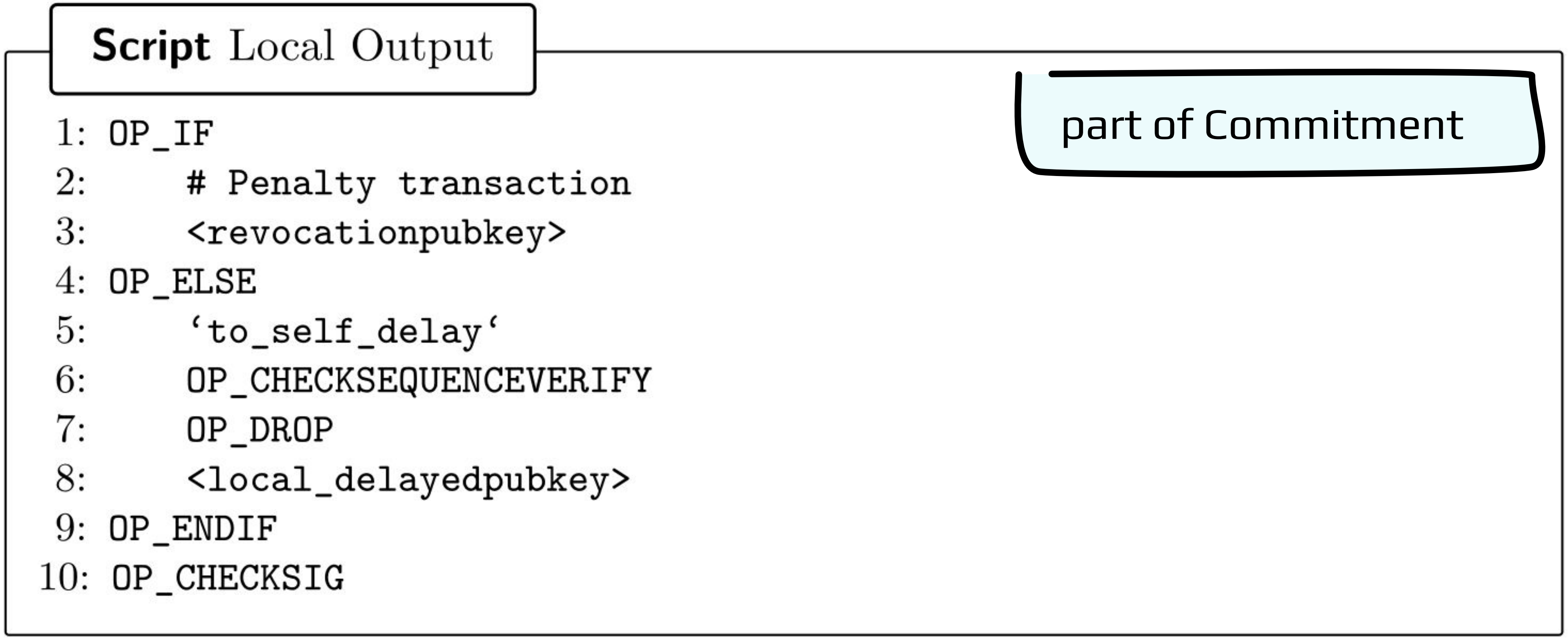
Scripts



Script Funding

```
2 <pubkey1> <pubkey2> 2 OP_CHECKMULTISIG
```

wrapped in P2WSH

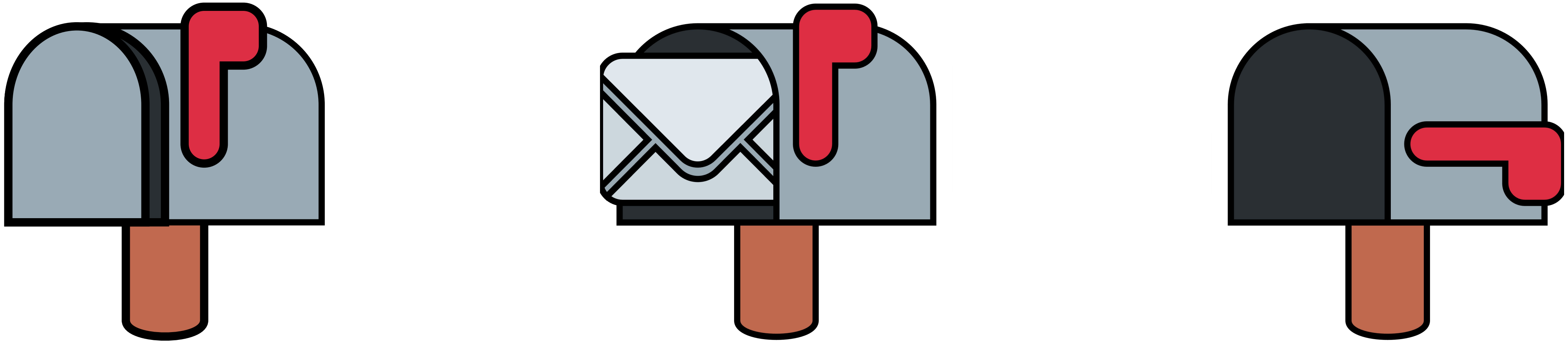


Script Local Output

```
OP_IF
    # Penalty transaction
    <revocationpubkey>
OP_ELSE
    ‘to_self_delay‘
    OP_CHECKSEQUENCEVERIFY
    OP_DROP
    <local_delayedpubkey>
OP_ENDIF
OP_CHECKSIG
```

part of Commitment

Lifecycle of a Channel

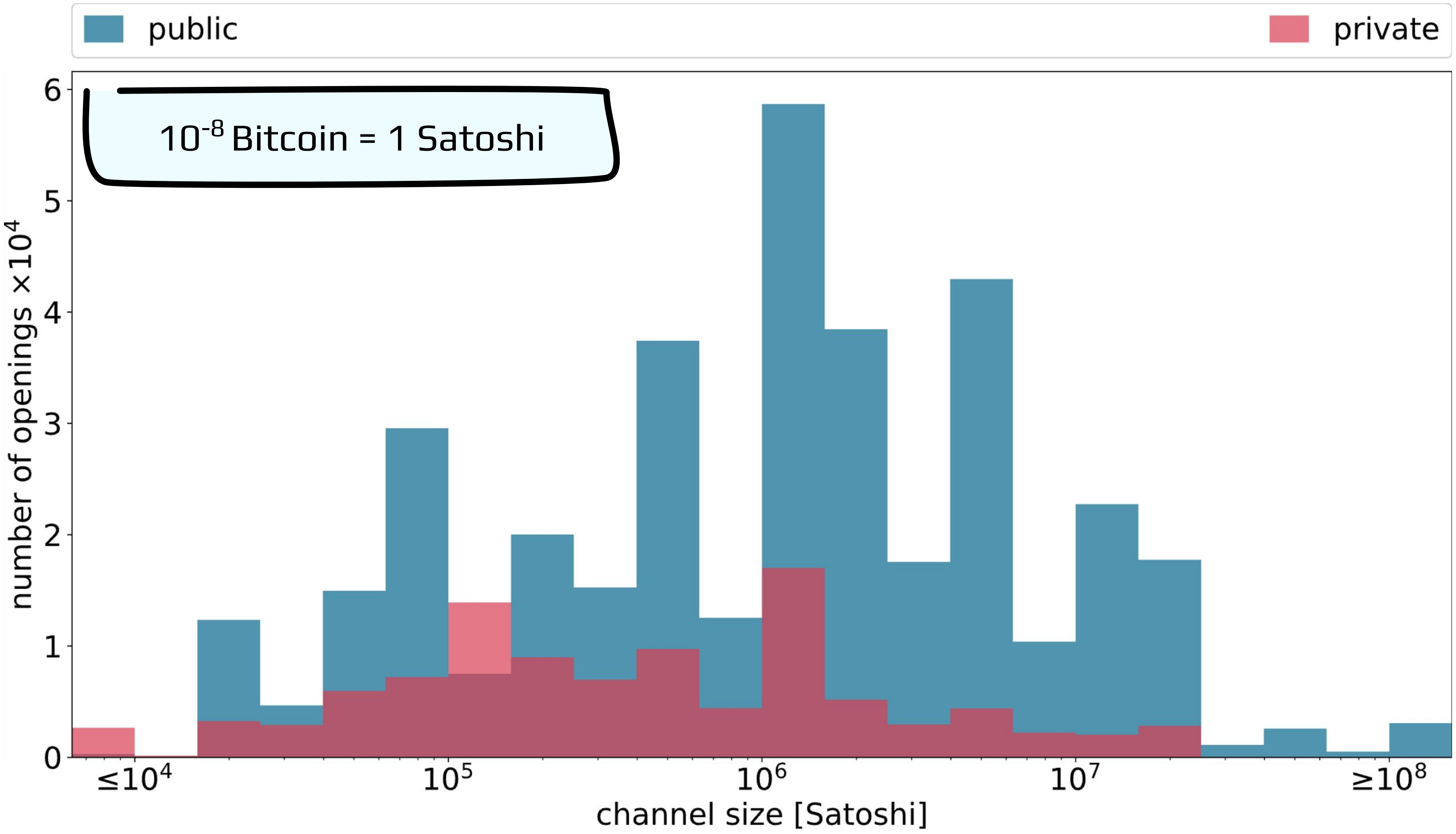


opening

lifetime

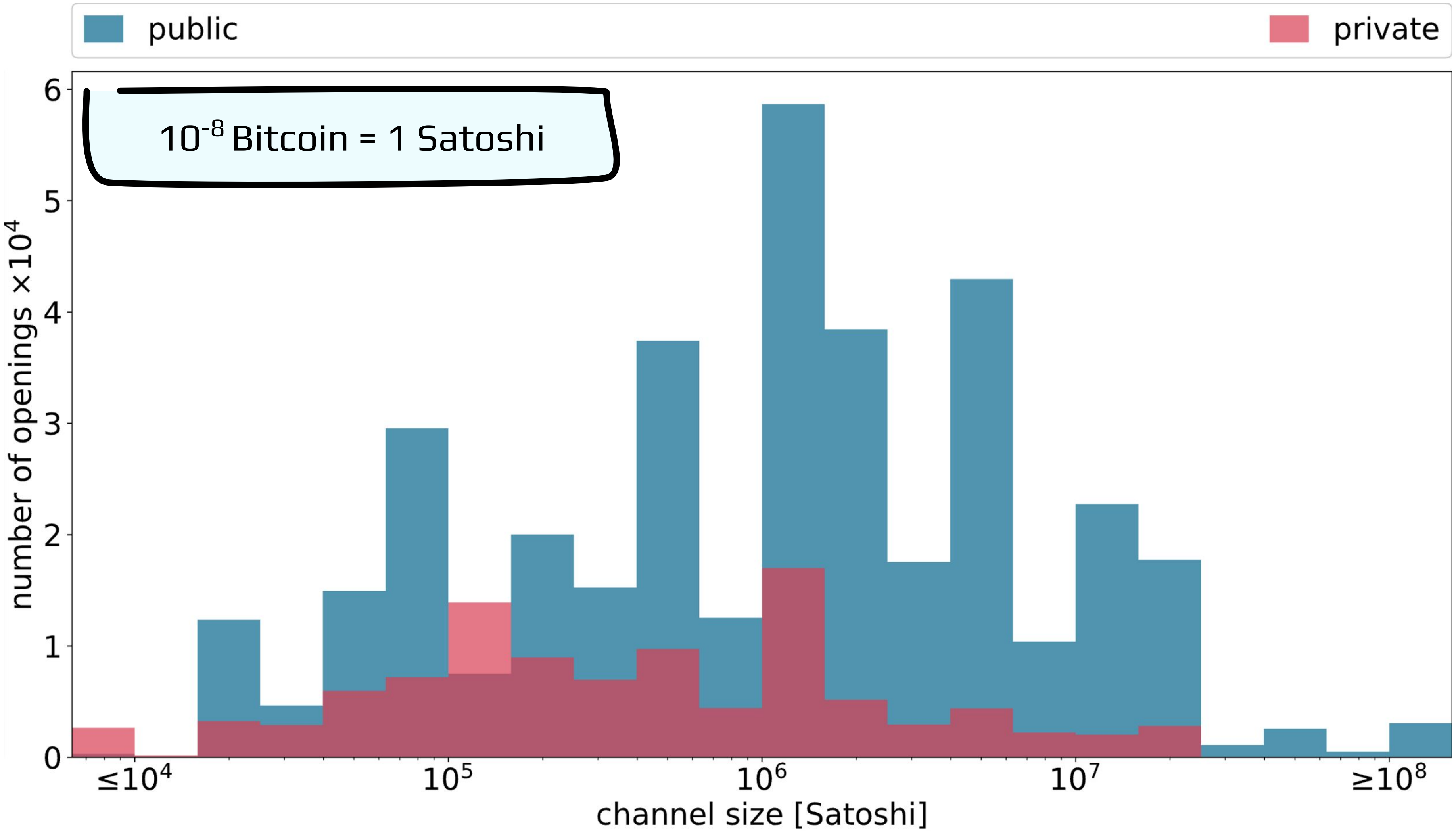
closing

Public channels tend to have a greater capacity than private channels



10^{-8} Bitcoin = 1 Satoshi

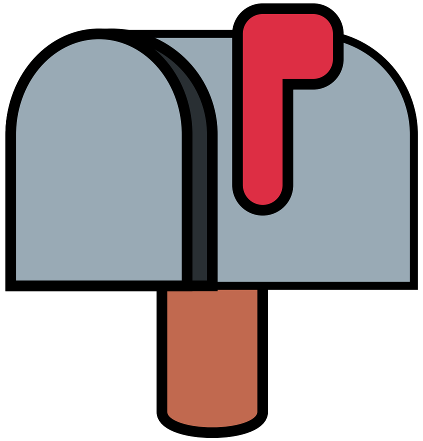
Public channels tend to have a greater capacity than private channels



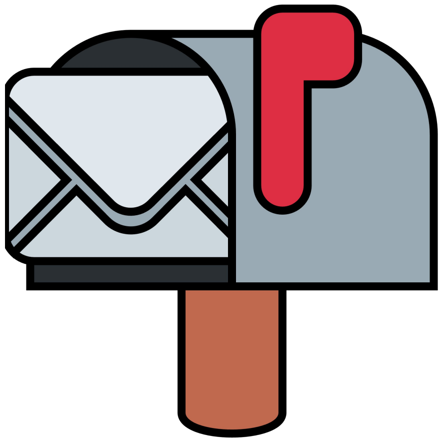
10^{-8} Bitcoin = 1 Satoshi

median channel size ≈ $1000

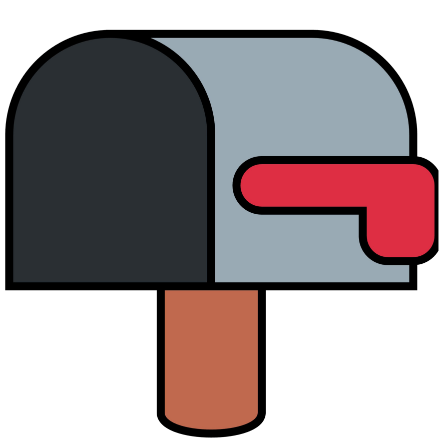
Lifecycle of a Channel



opening

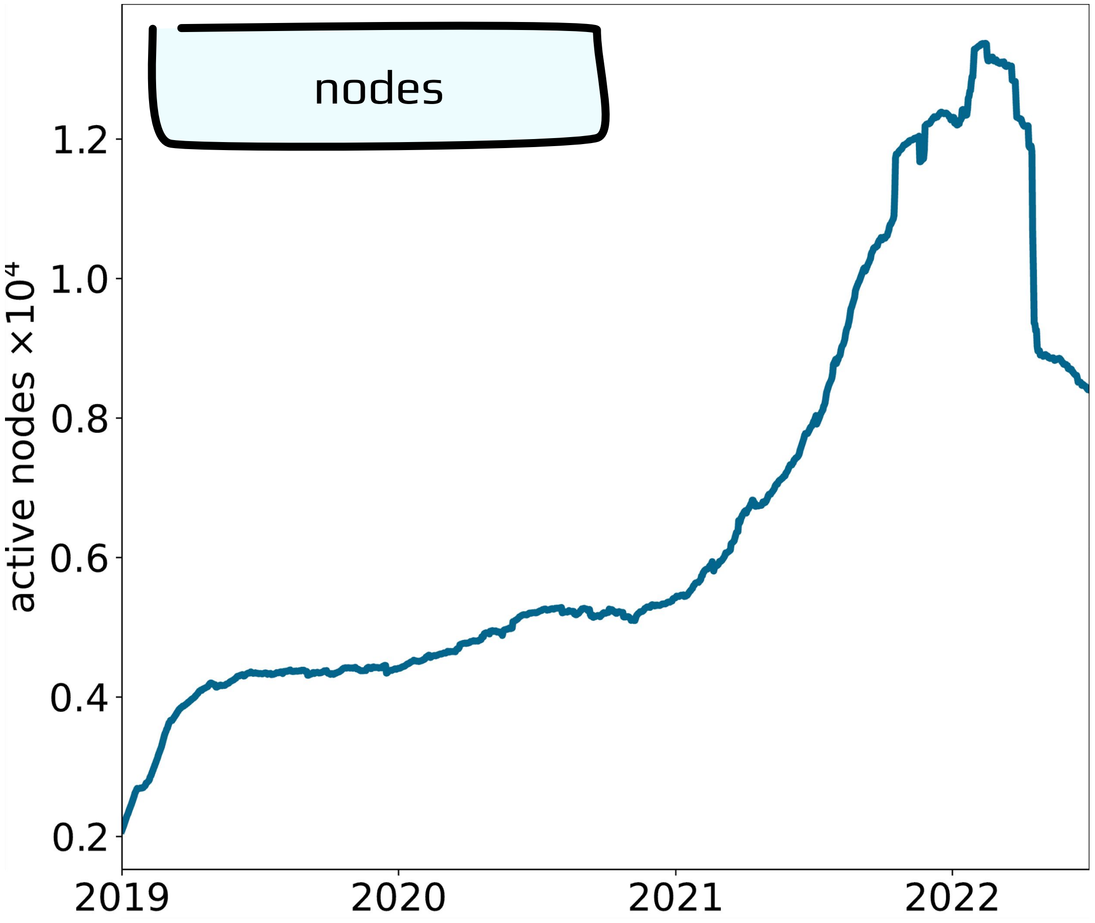


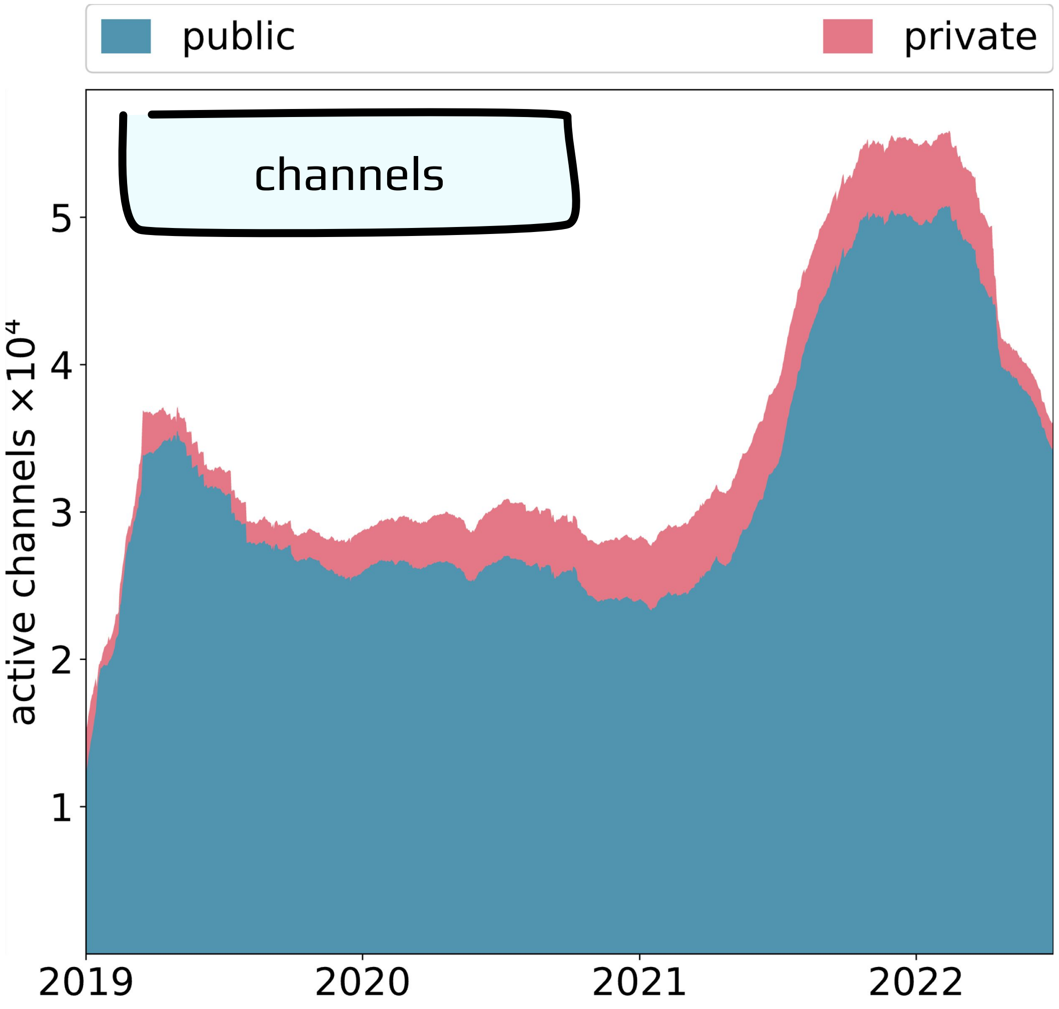
lifetime



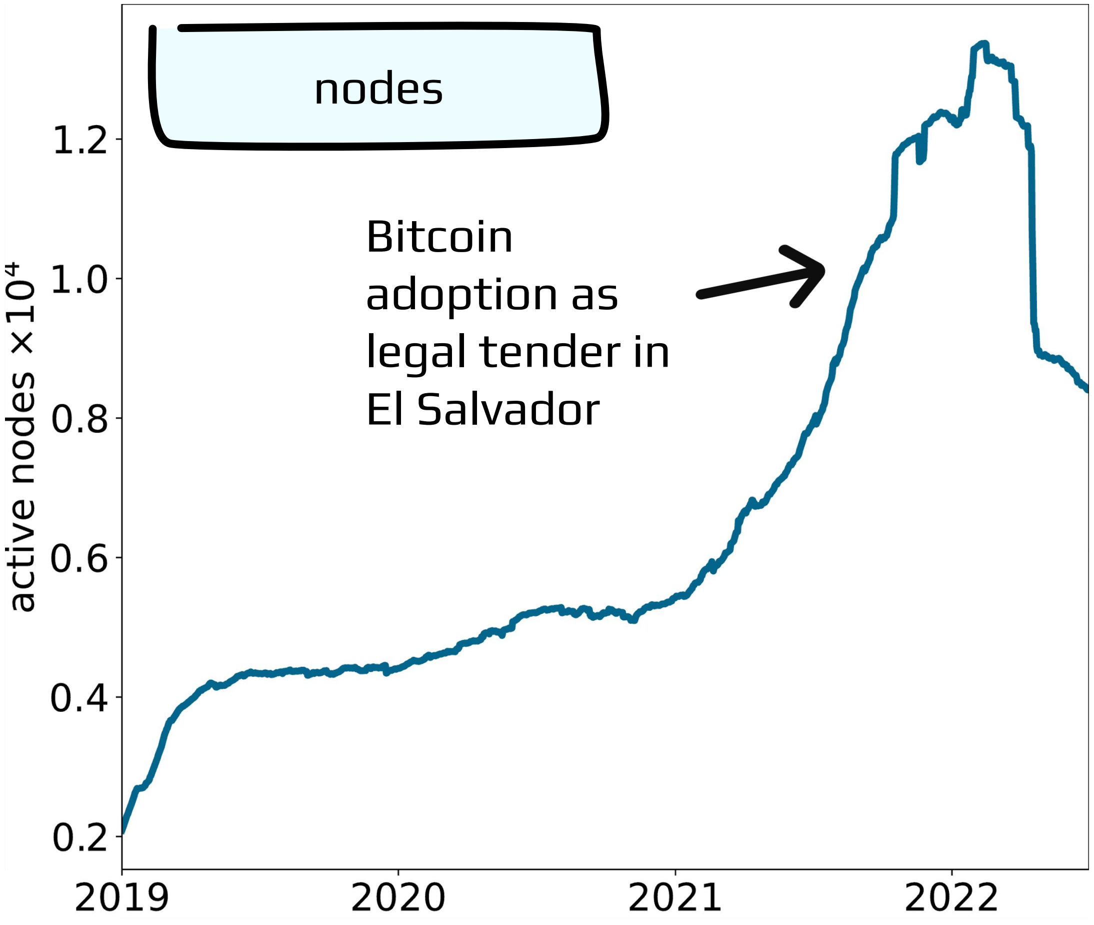
closing

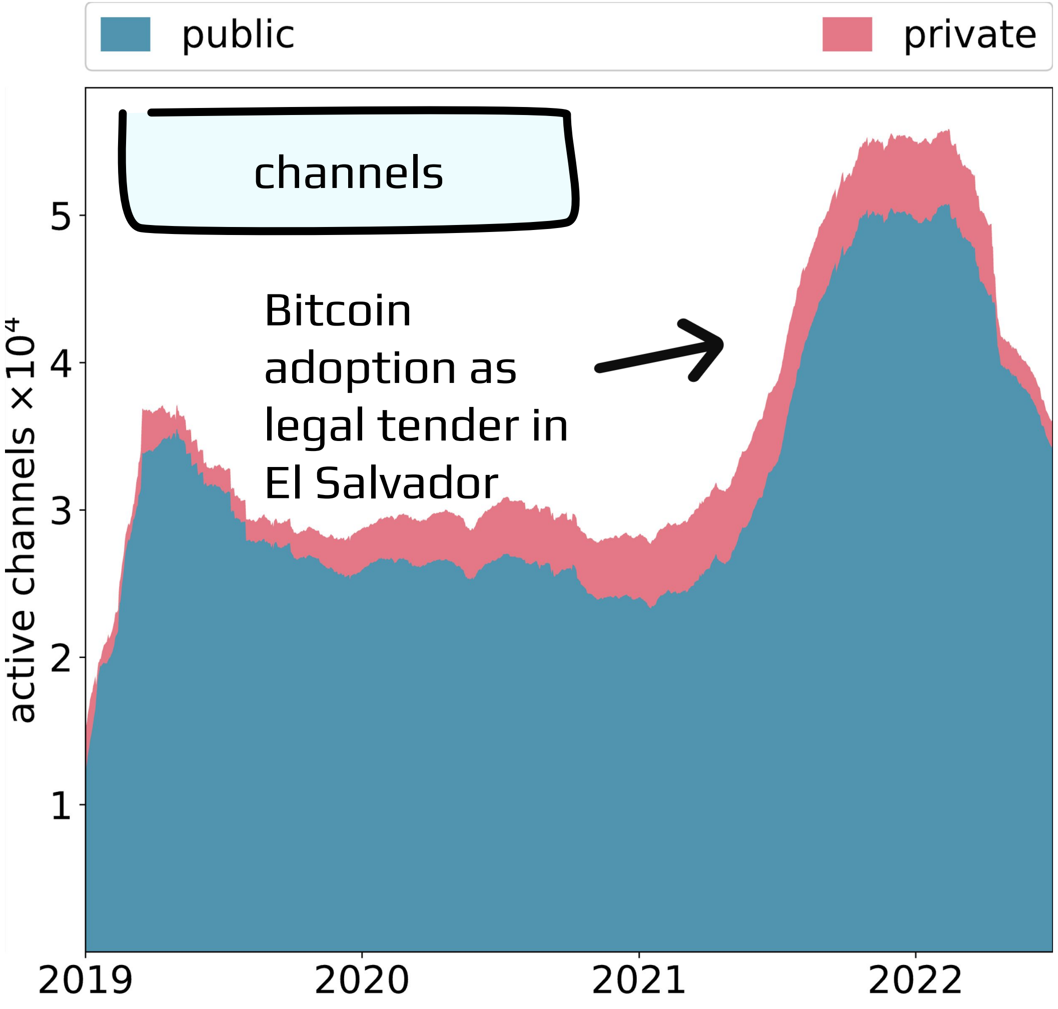
The Lightning network size is generally increasing



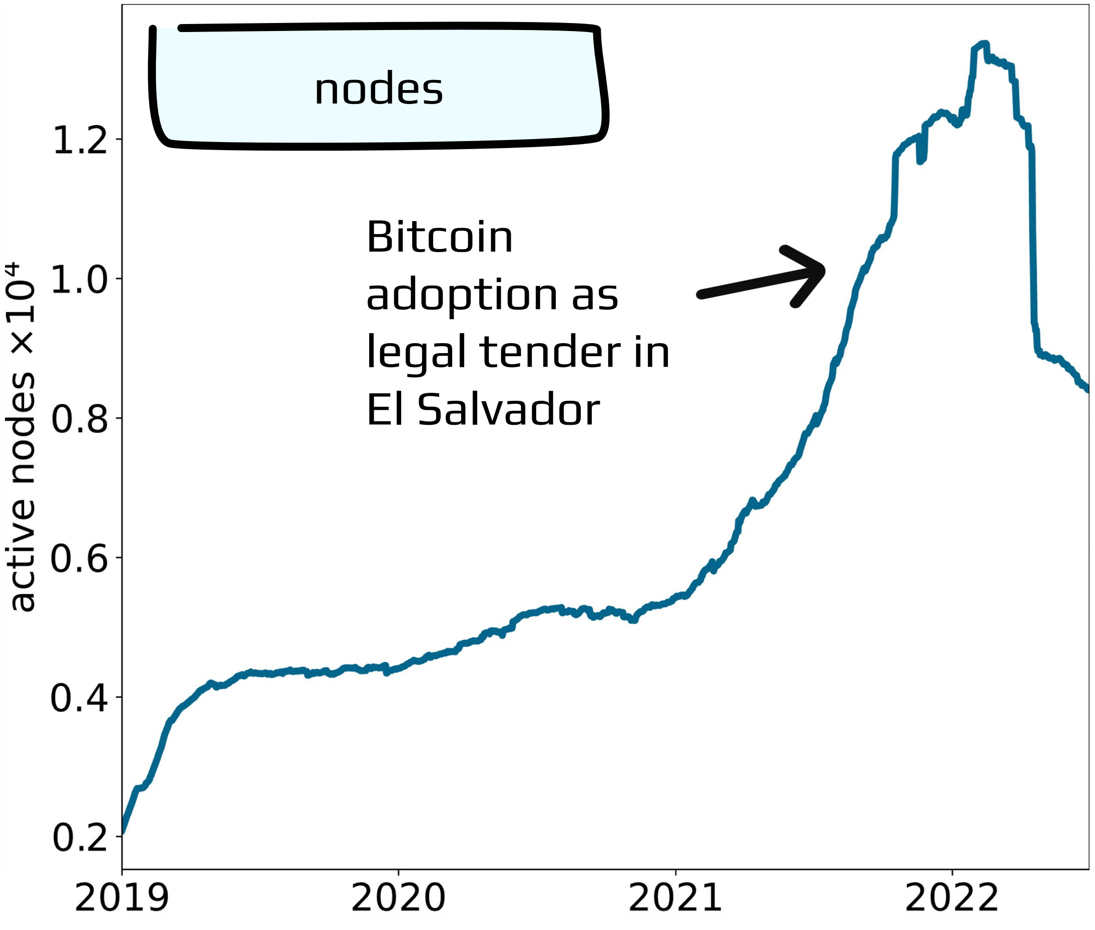


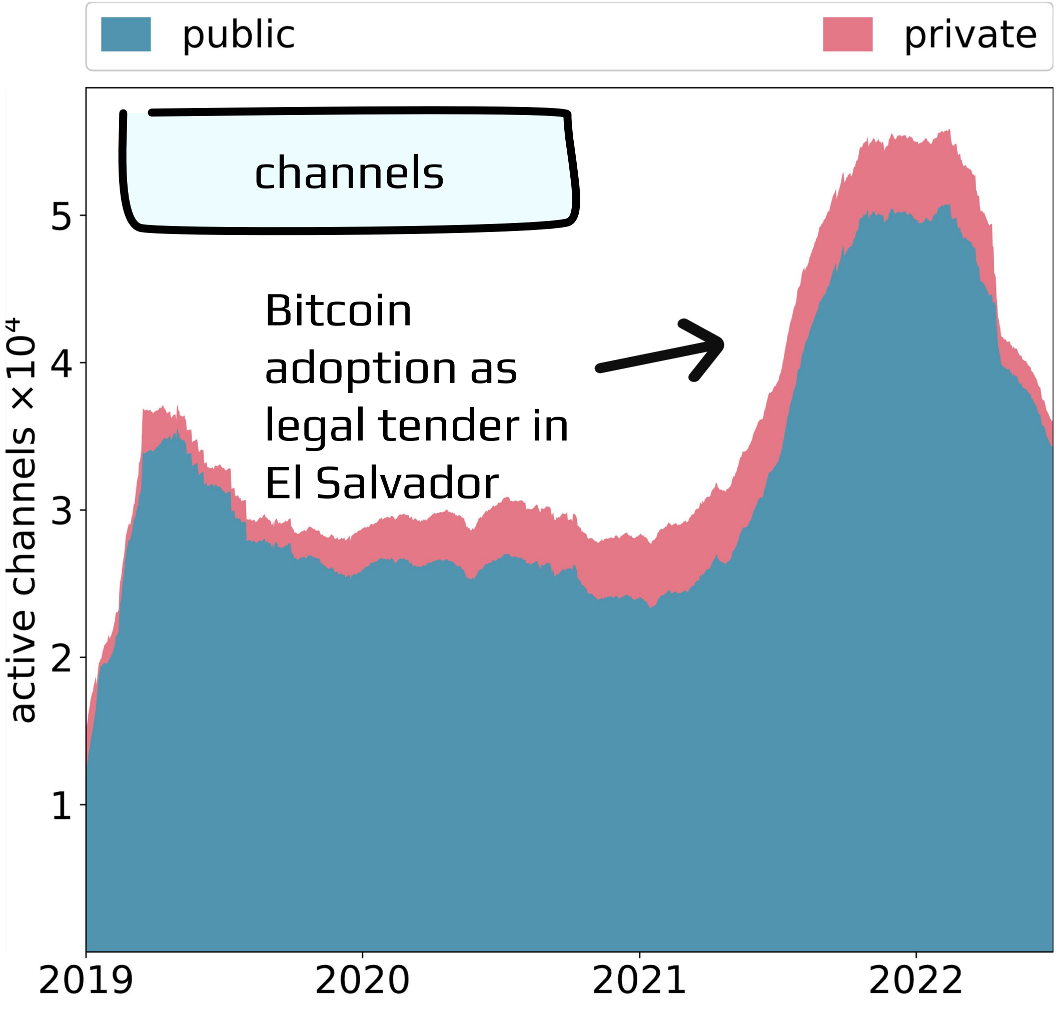
The Lightning network size is generally increasing



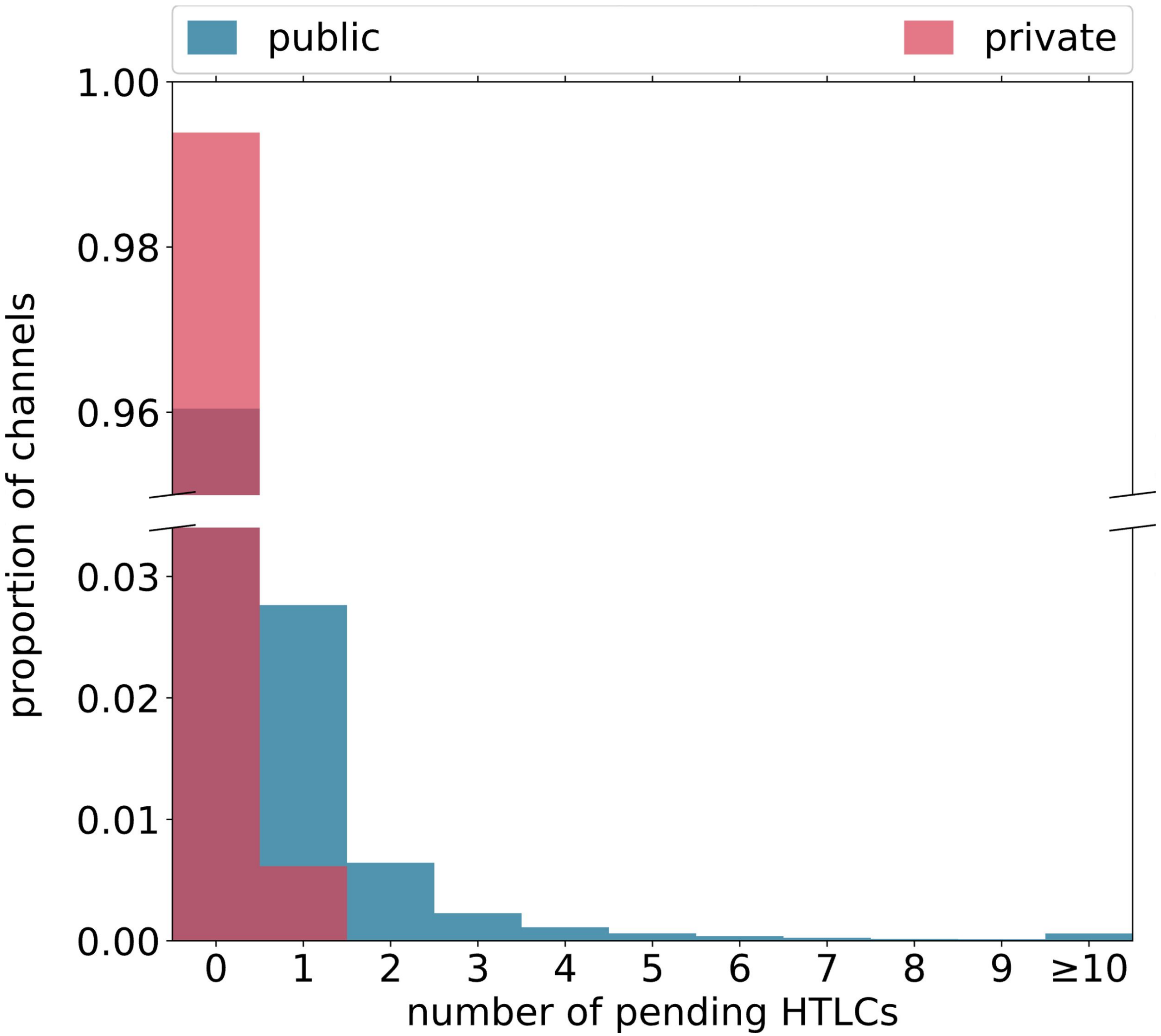


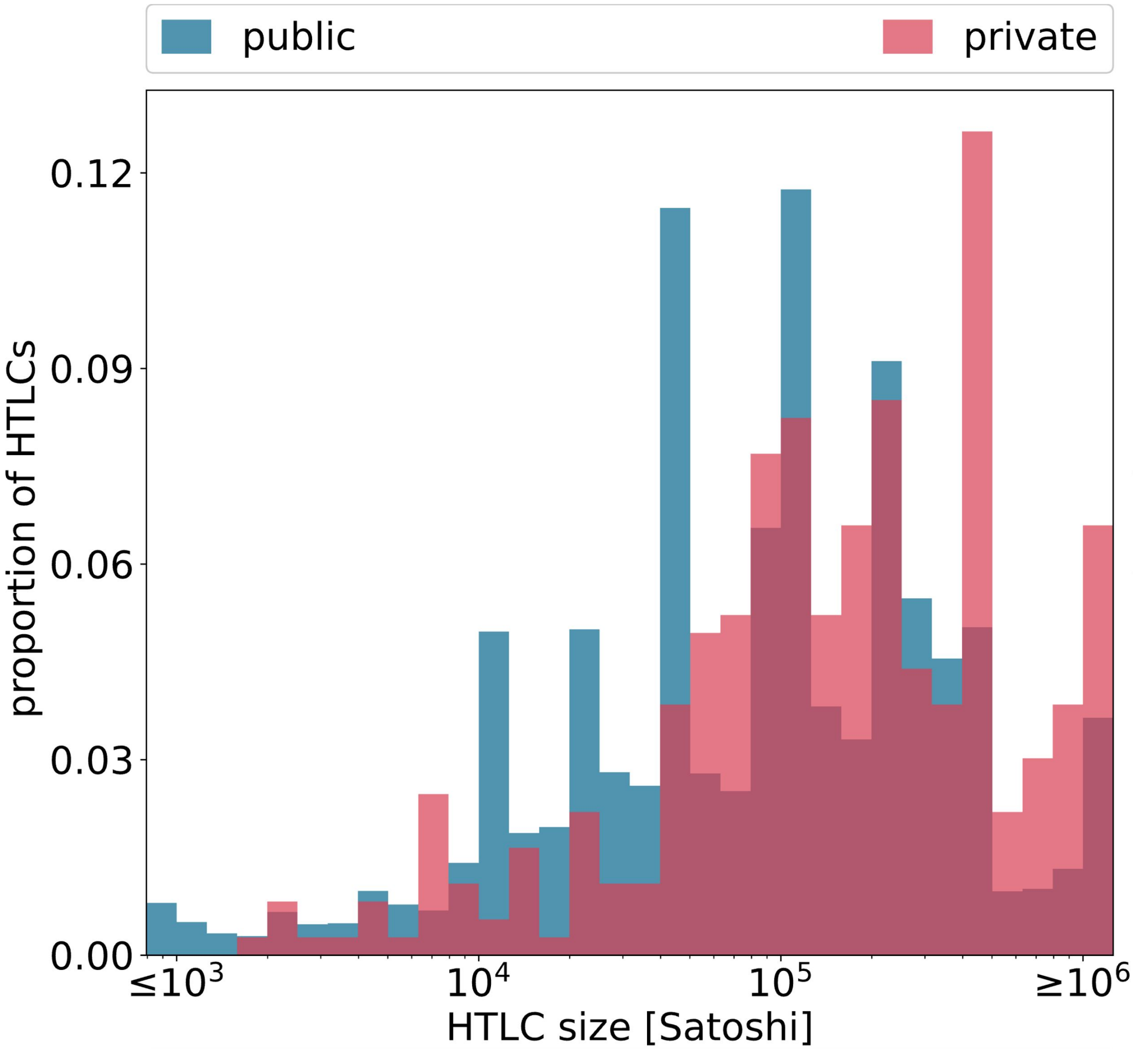
The Lightning network size is generally increasing but has been decreasing lately



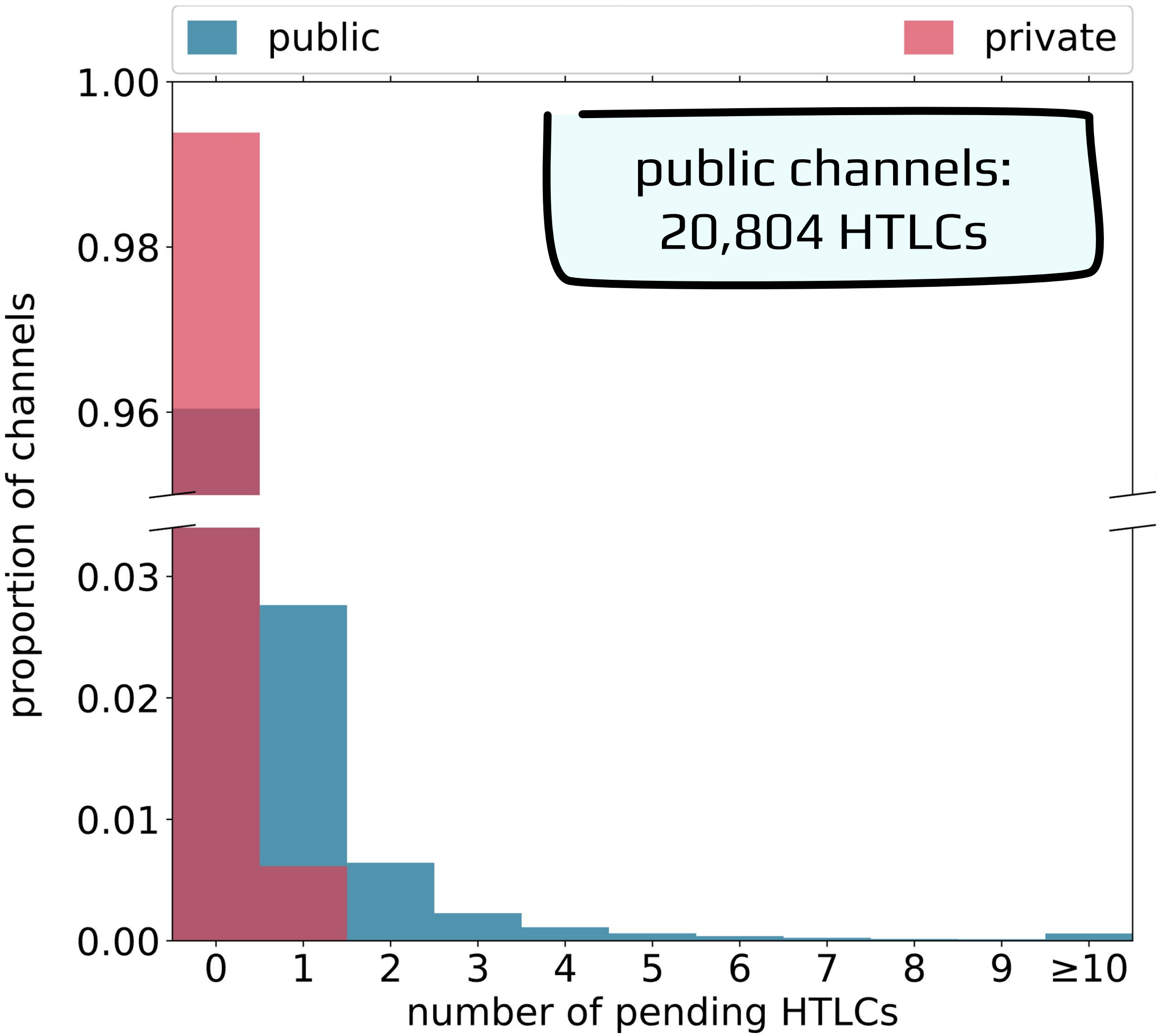


Pending HTLCs represent unconfirmed transactions (single- and multi-hop)

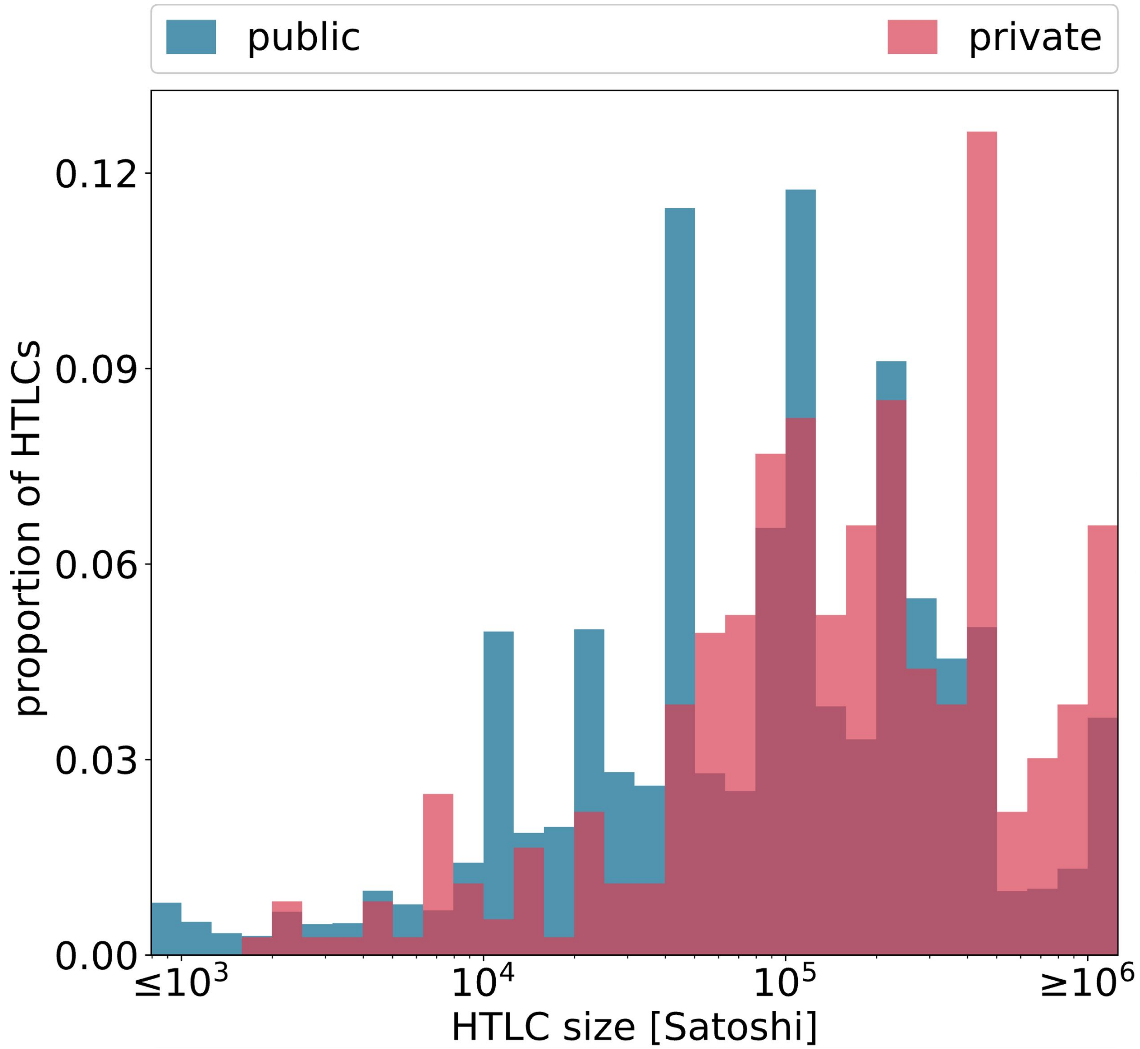




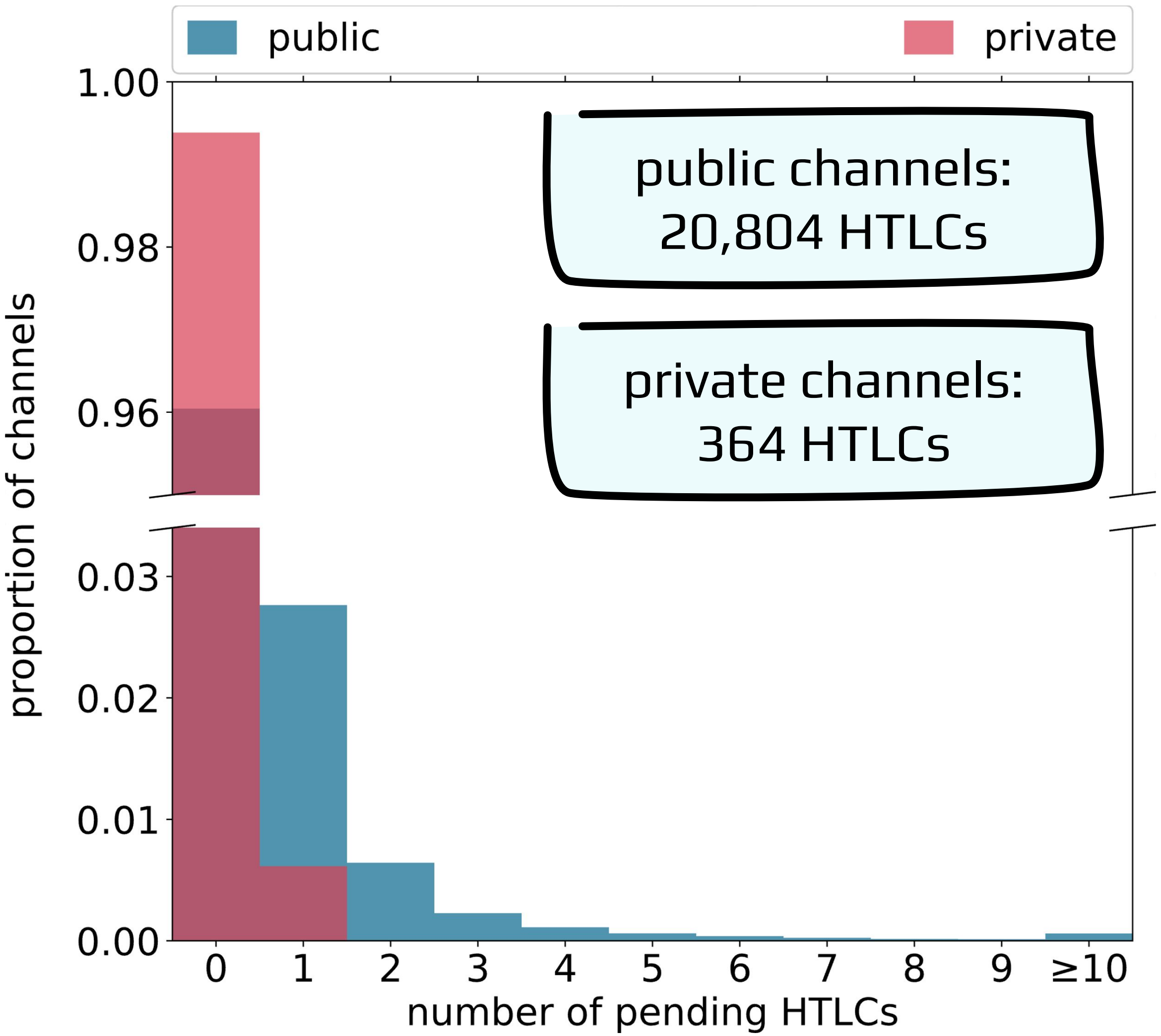
Pending HTLCs represent unconfirmed transactions (single- and multi-hop)



public channels:
20,804 HTLCs

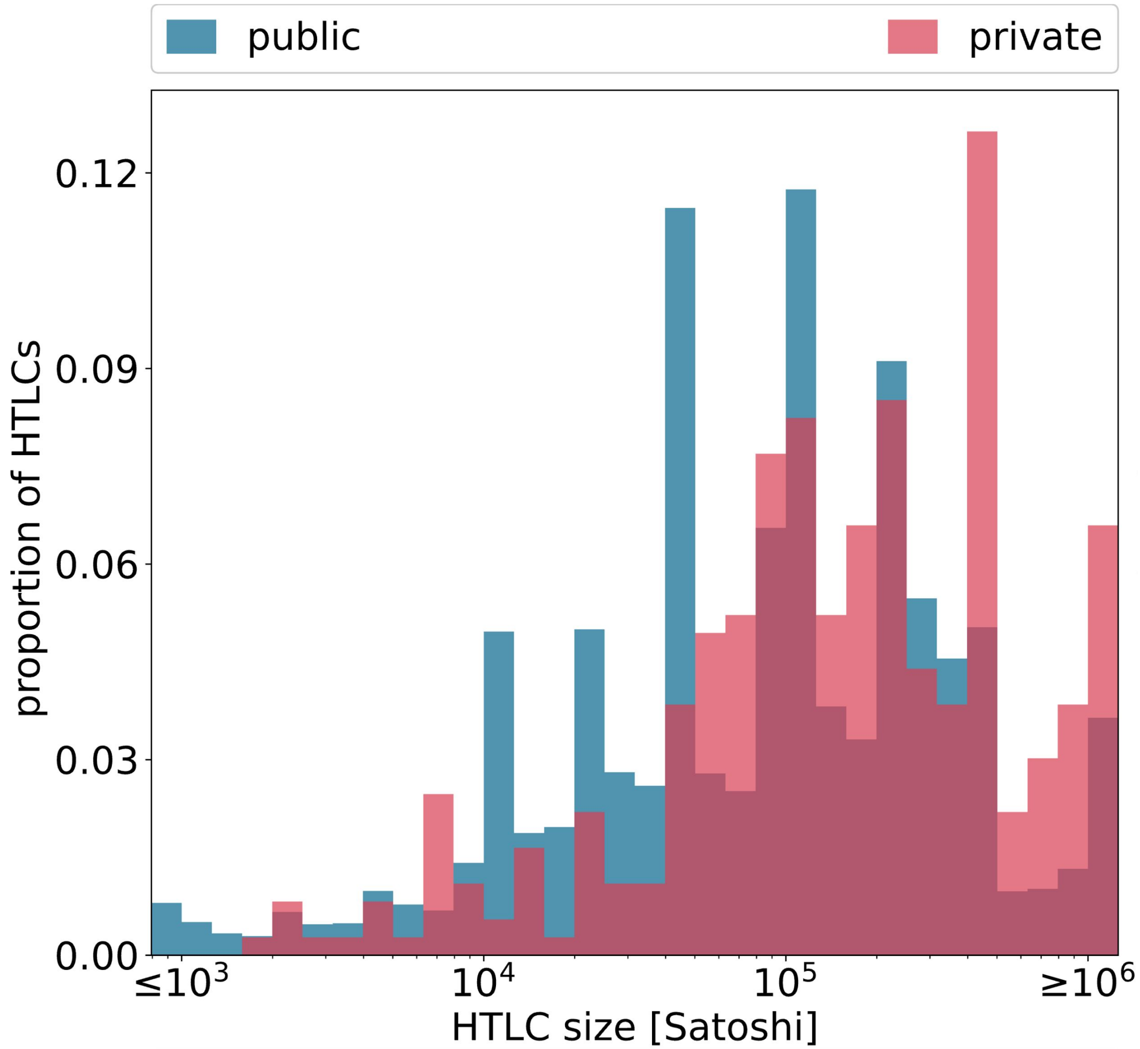


Pending HTLCs represent unconfirmed transactions (single- and multi-hop)

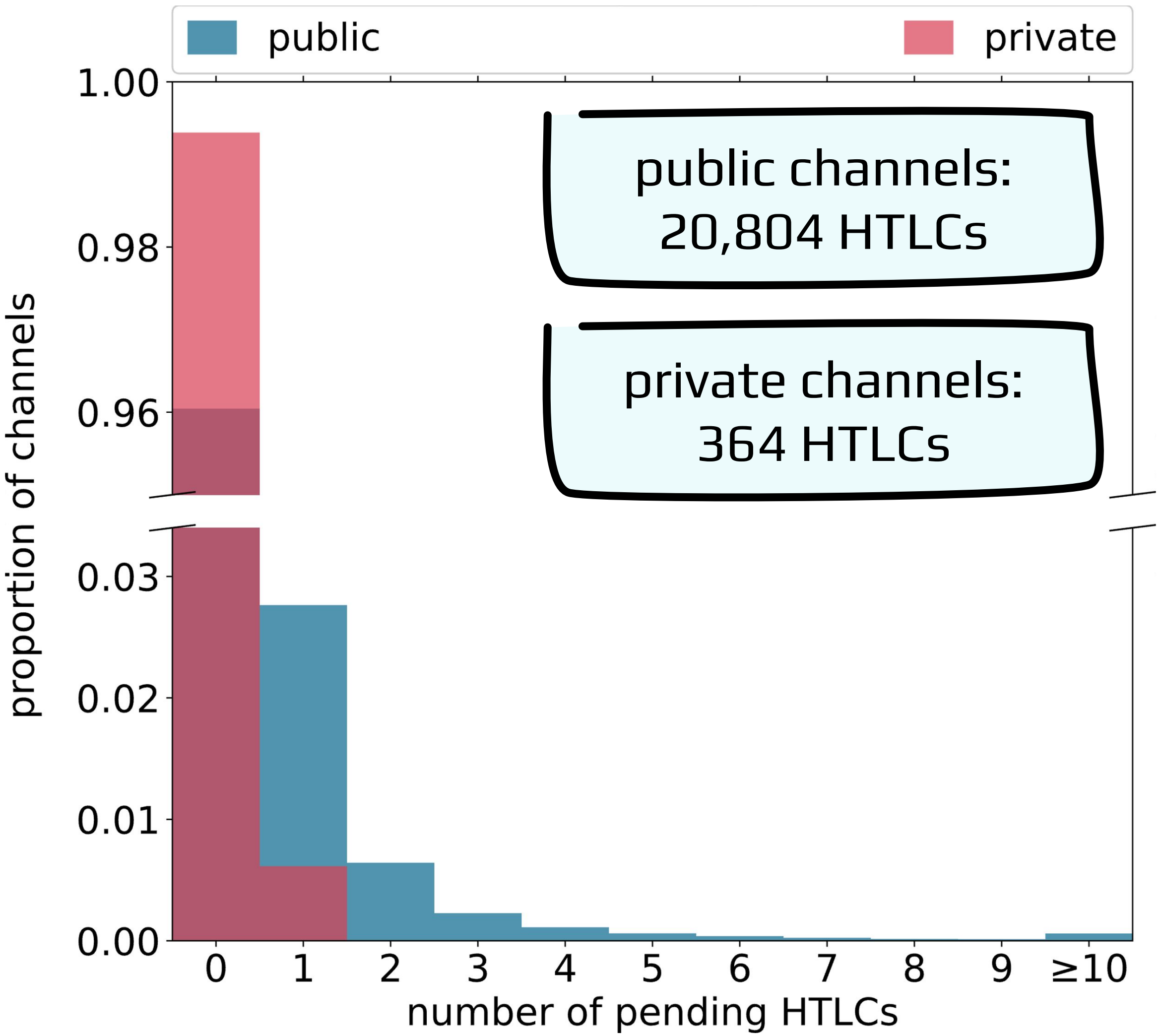


public channels:
20,804 HTLCs

private channels:
364 HTLCs

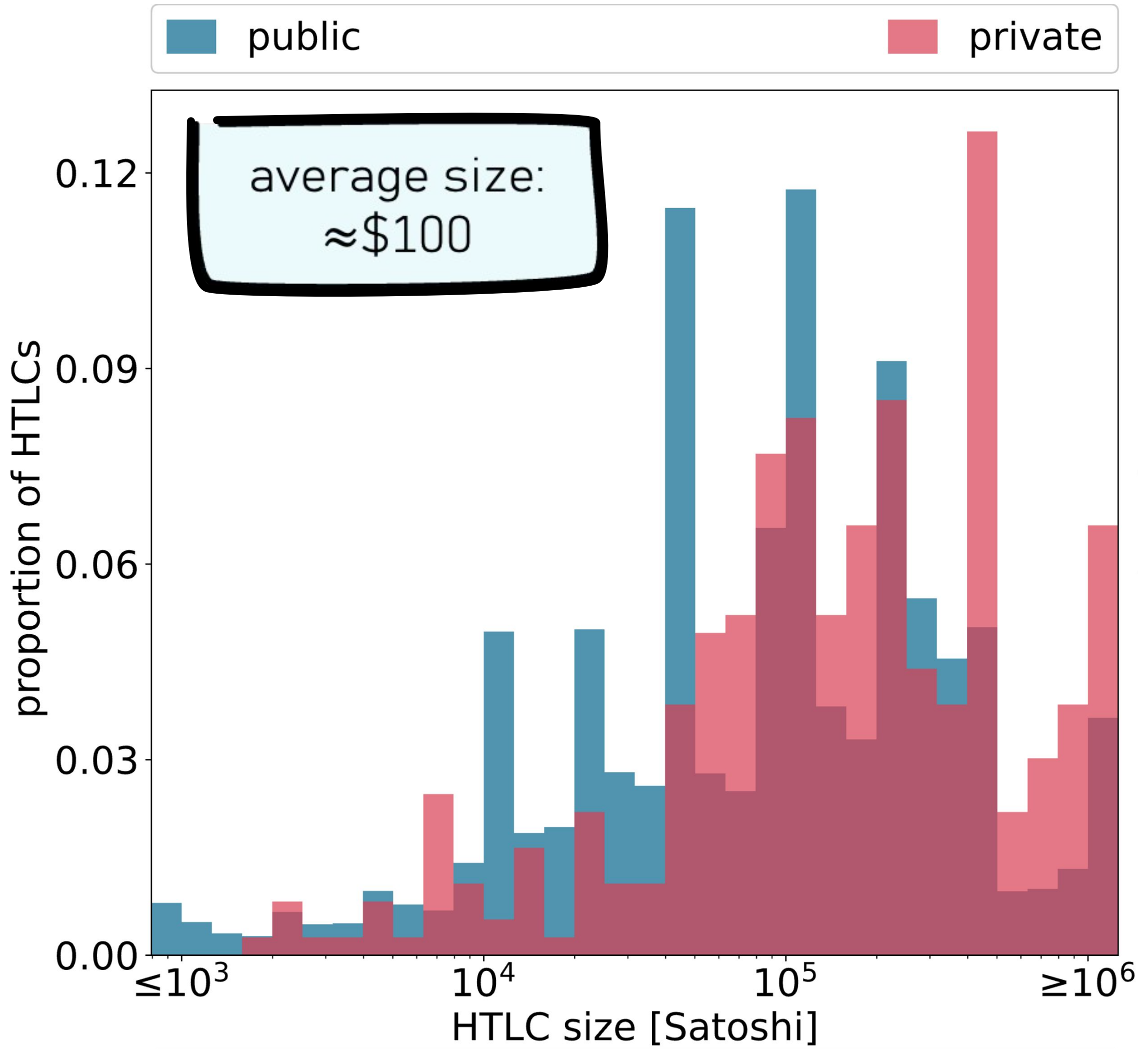


Pending HTLCs represent unconfirmed transactions (single- and multi-hop)



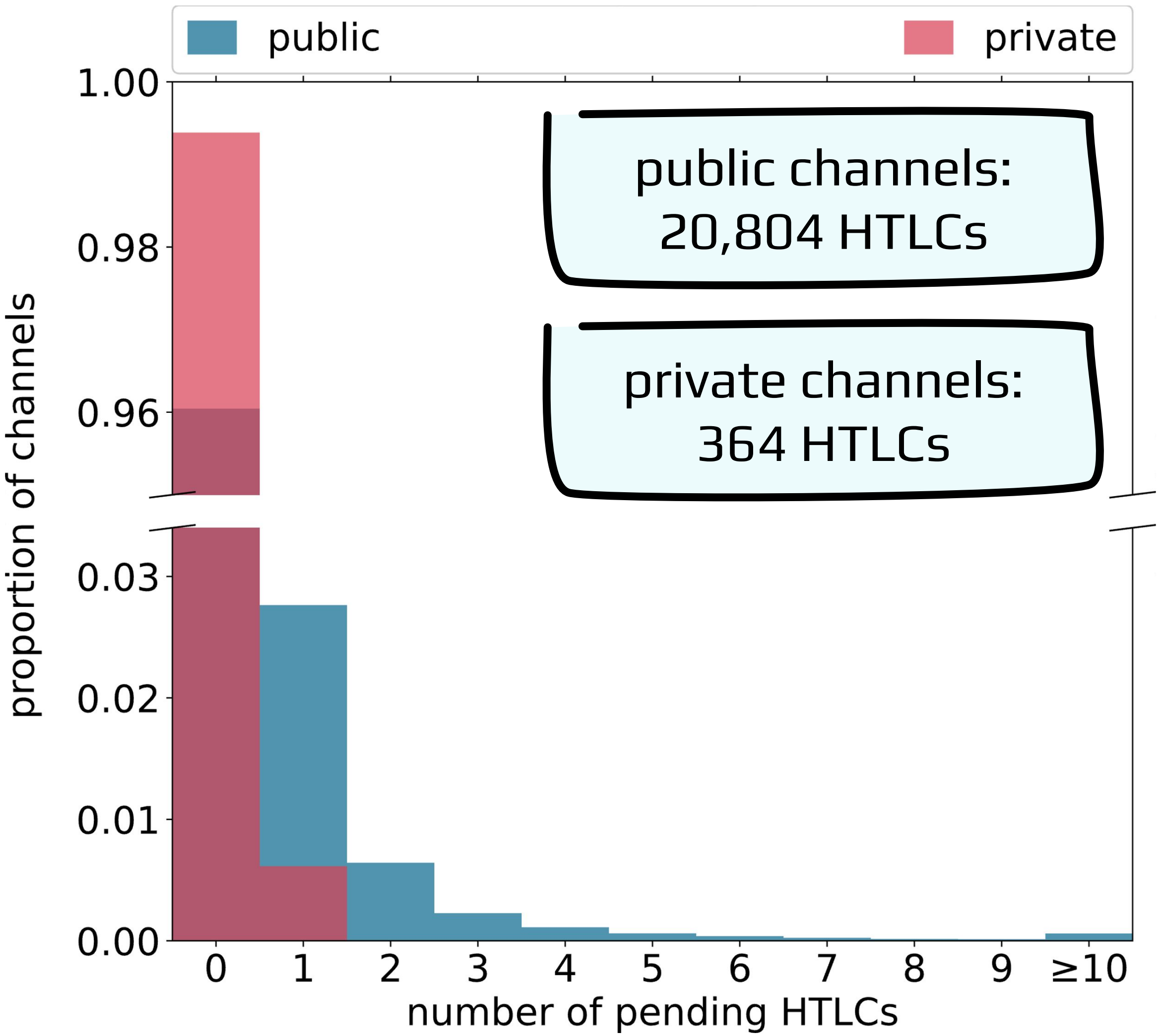
public channels:
20,804 HTLCs

private channels:
364 HTLCs



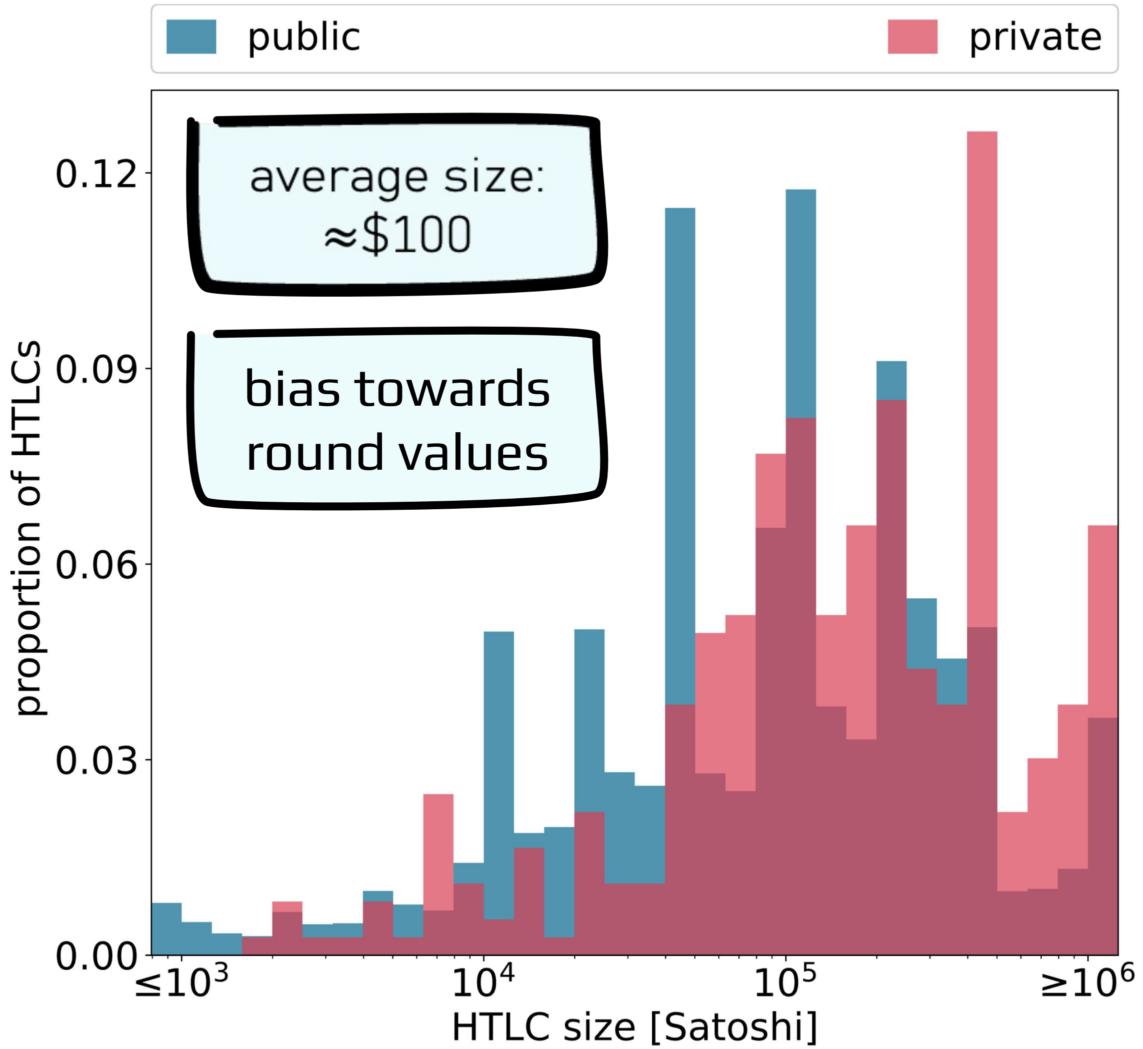
average size:
≈$100

Pending HTLCs represent unconfirmed transactions (single- and multi-hop)



public channels:
20,804 HTLCs

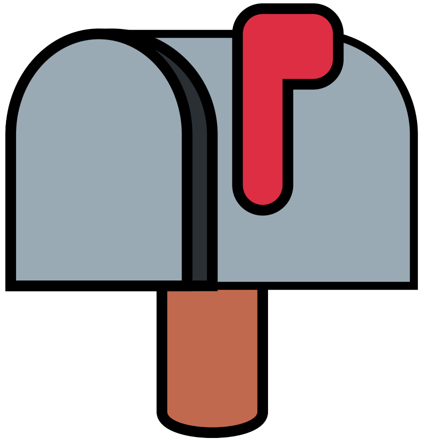
private channels:
364 HTLCs



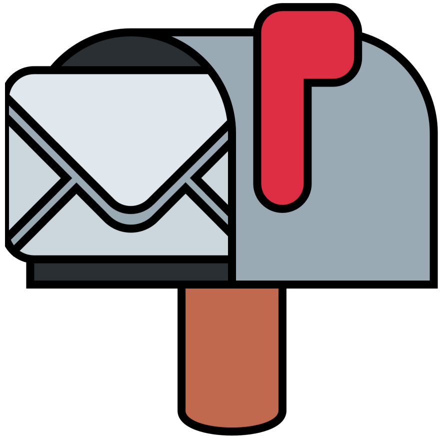
average size:
≈$100

bias towards
round values

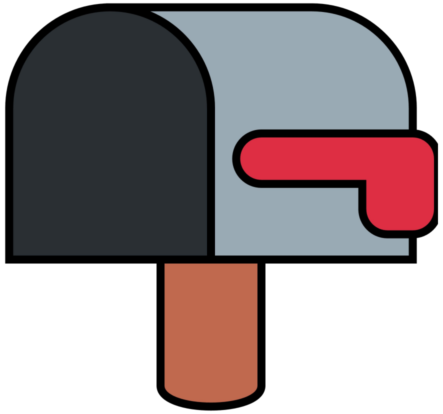
Lifecycle of a Channel



opening

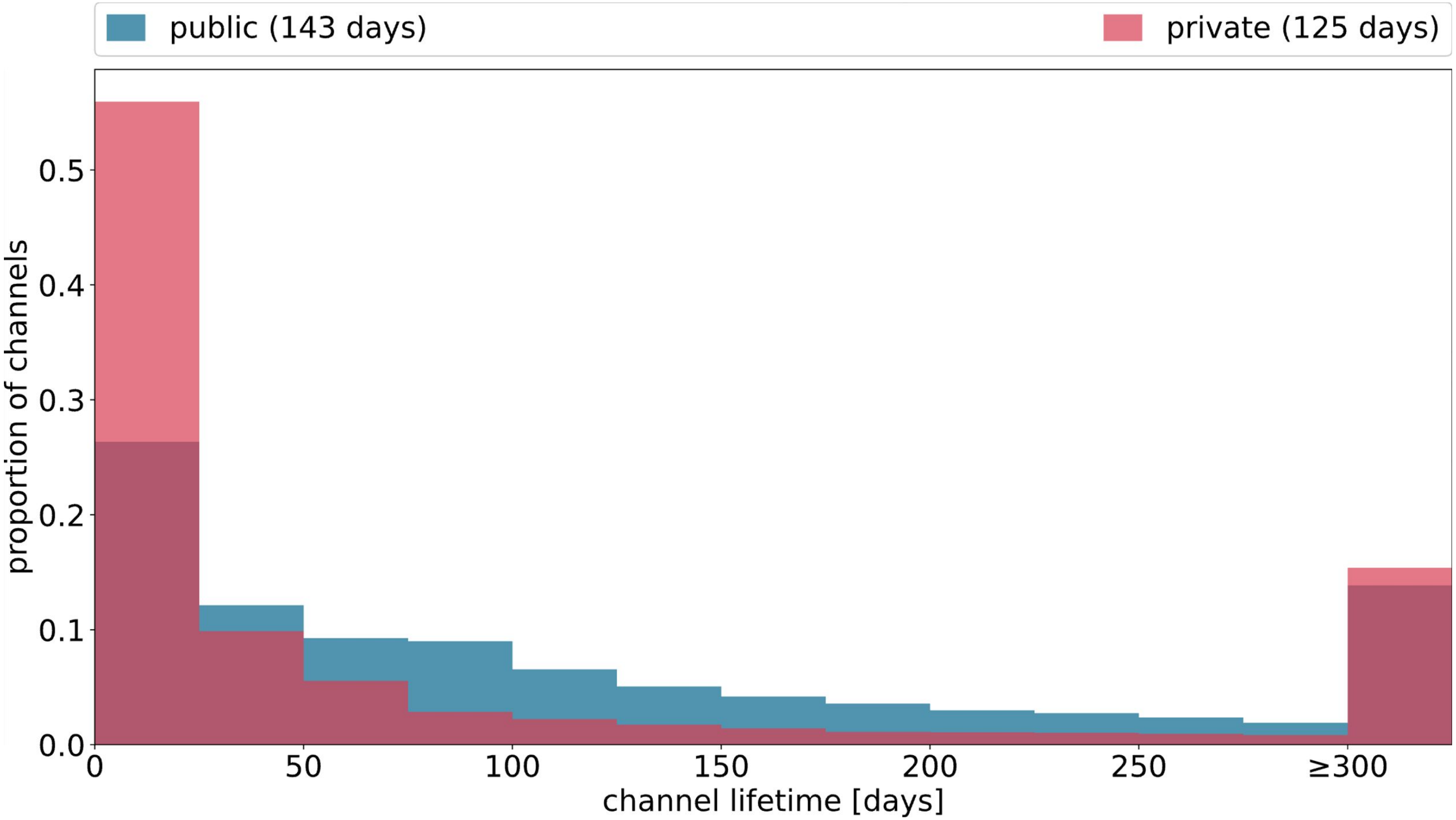


lifetime

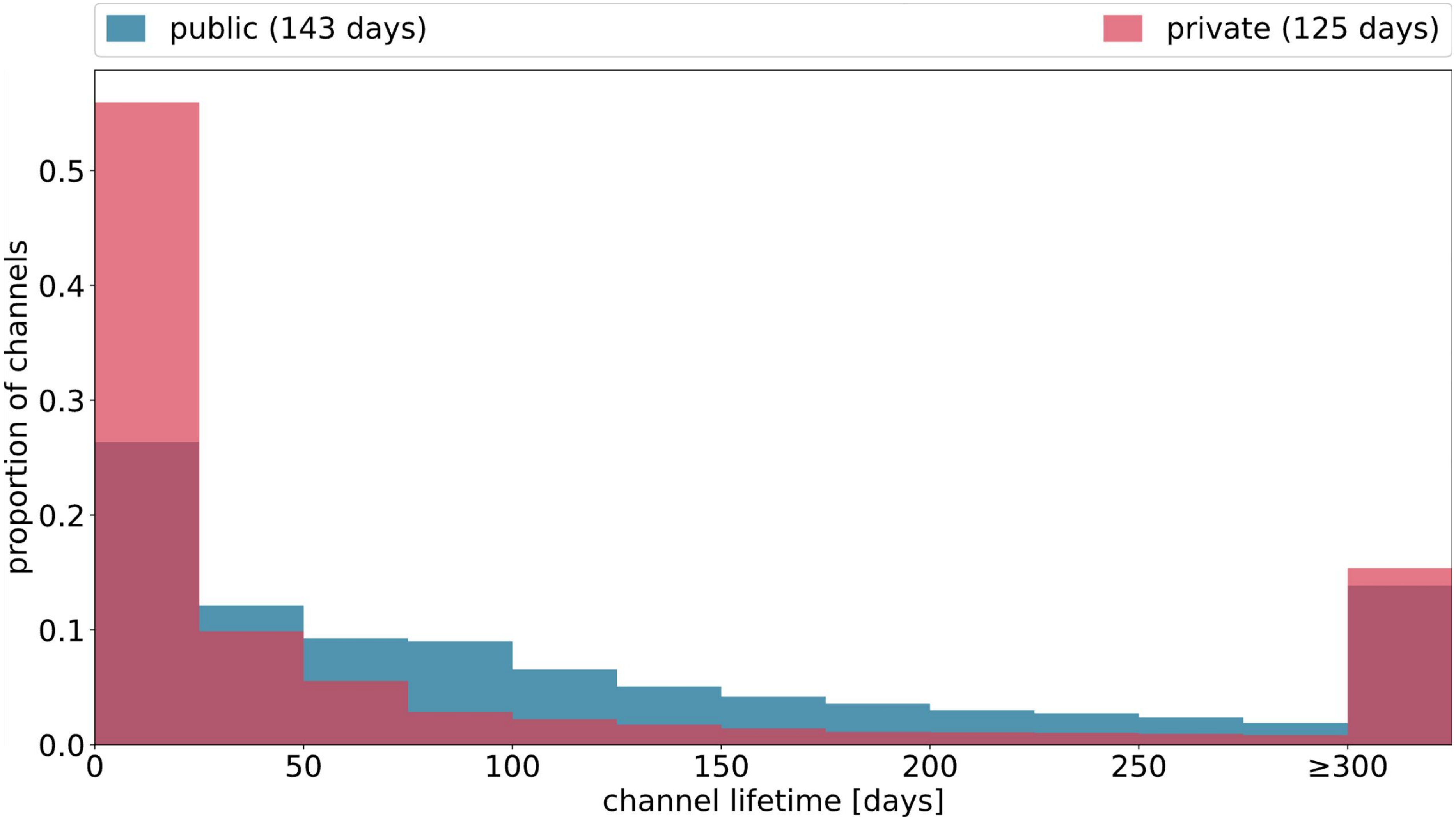


closing

Public channels have longer lifetimes than private channels

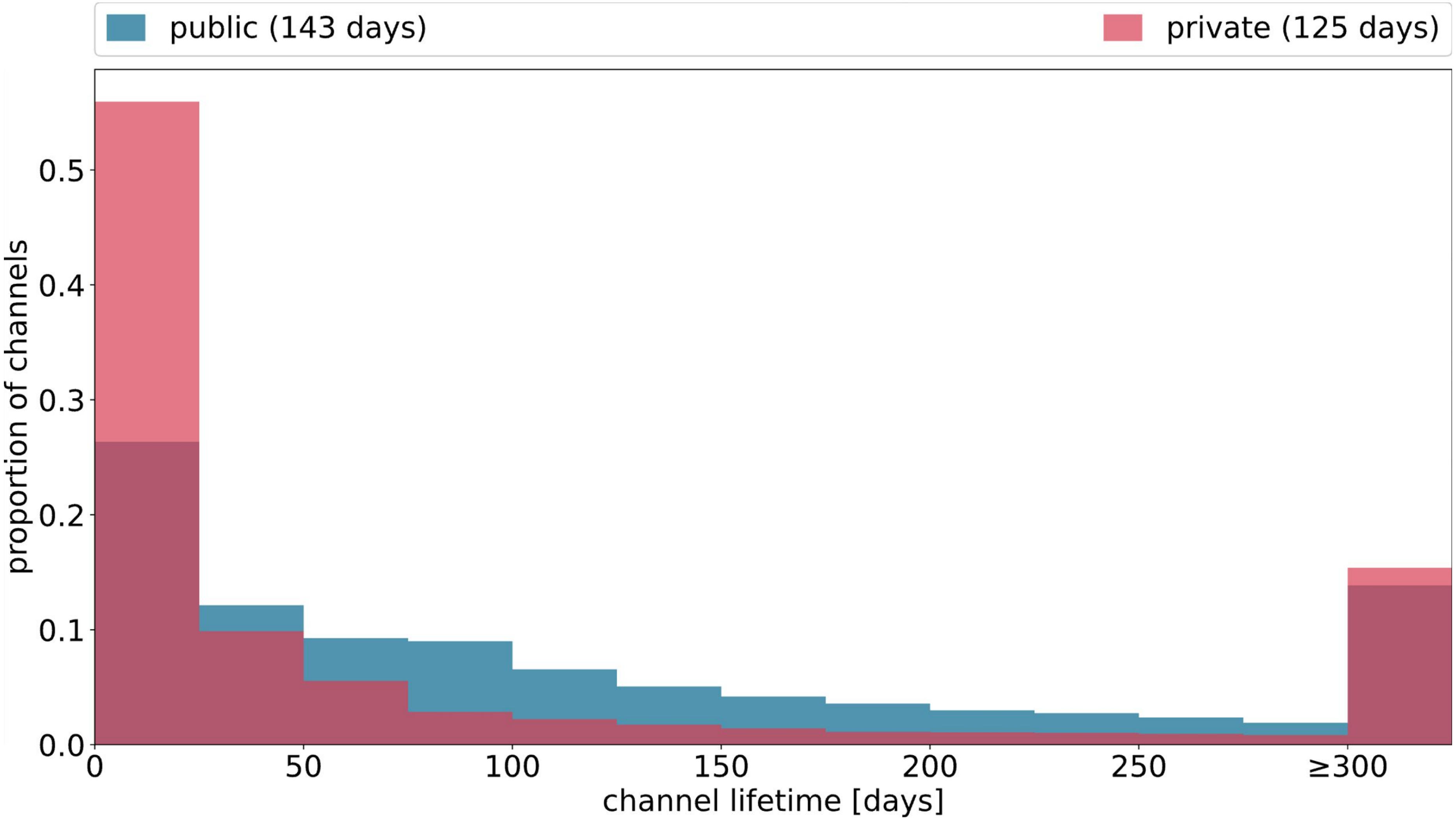


Public channels have longer lifetimes than private channels



public channels:
143 days

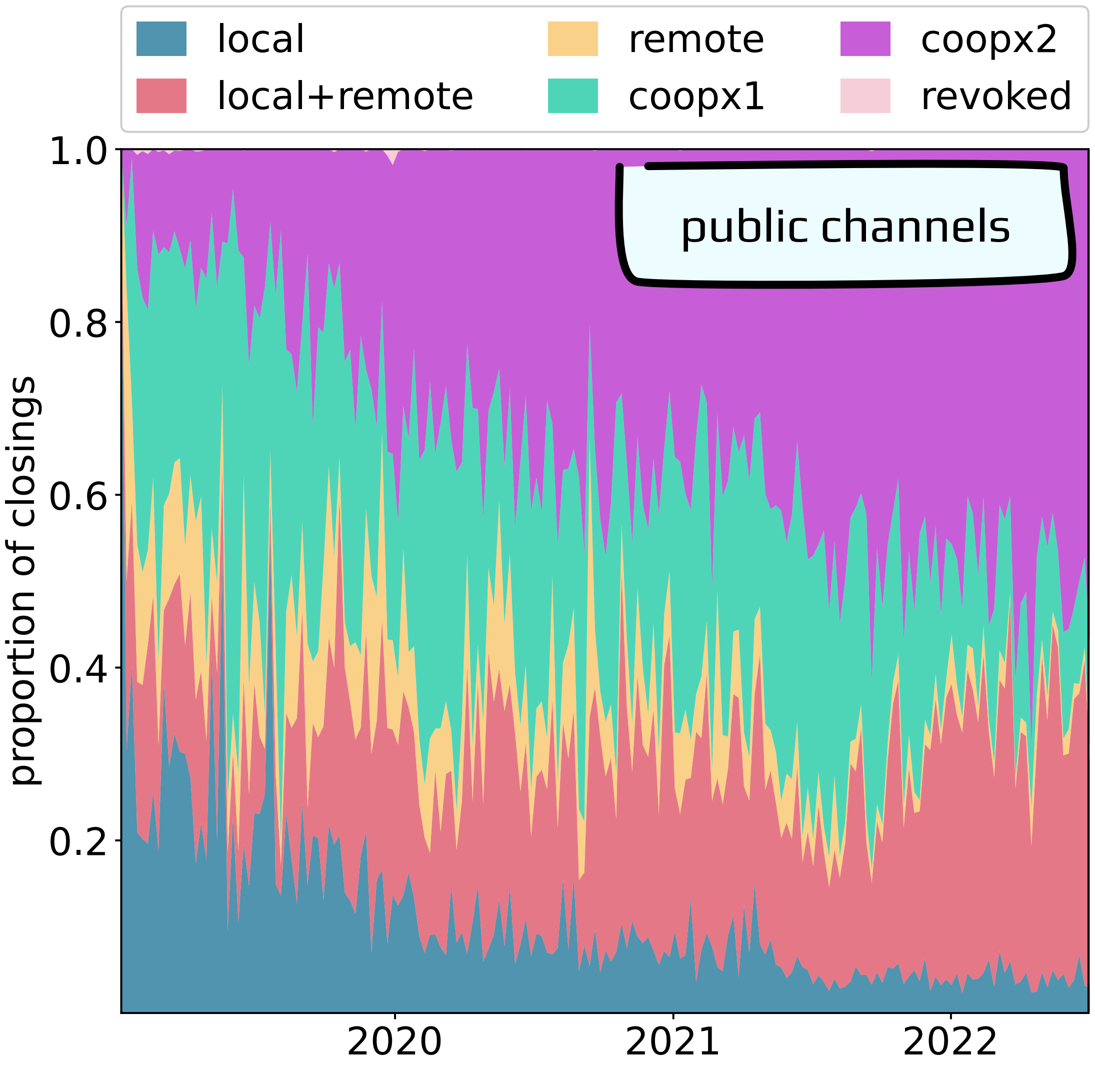
Public channels have longer lifetimes than private channels

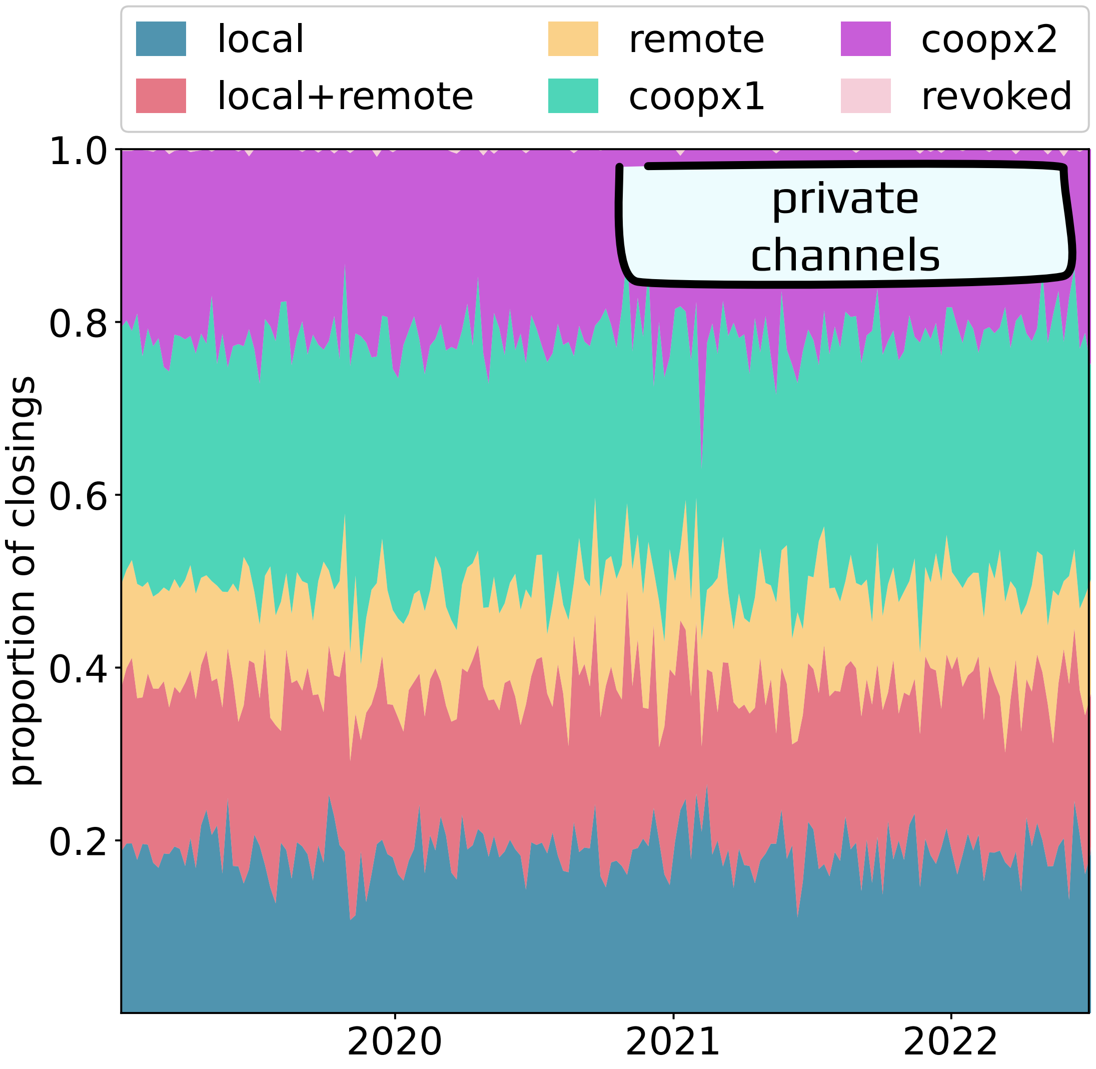


public channels:
143 days

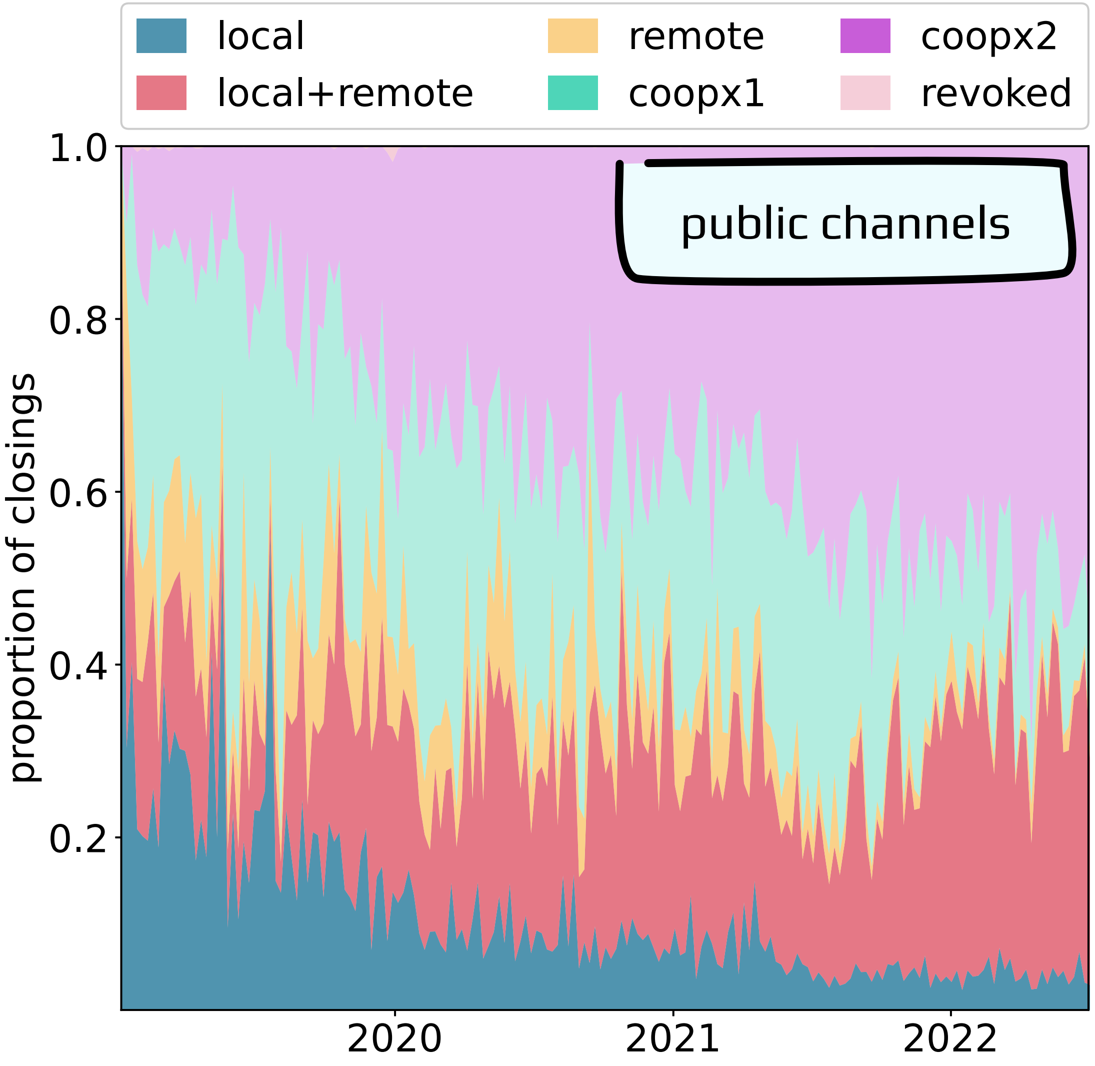
private channels:
125 days

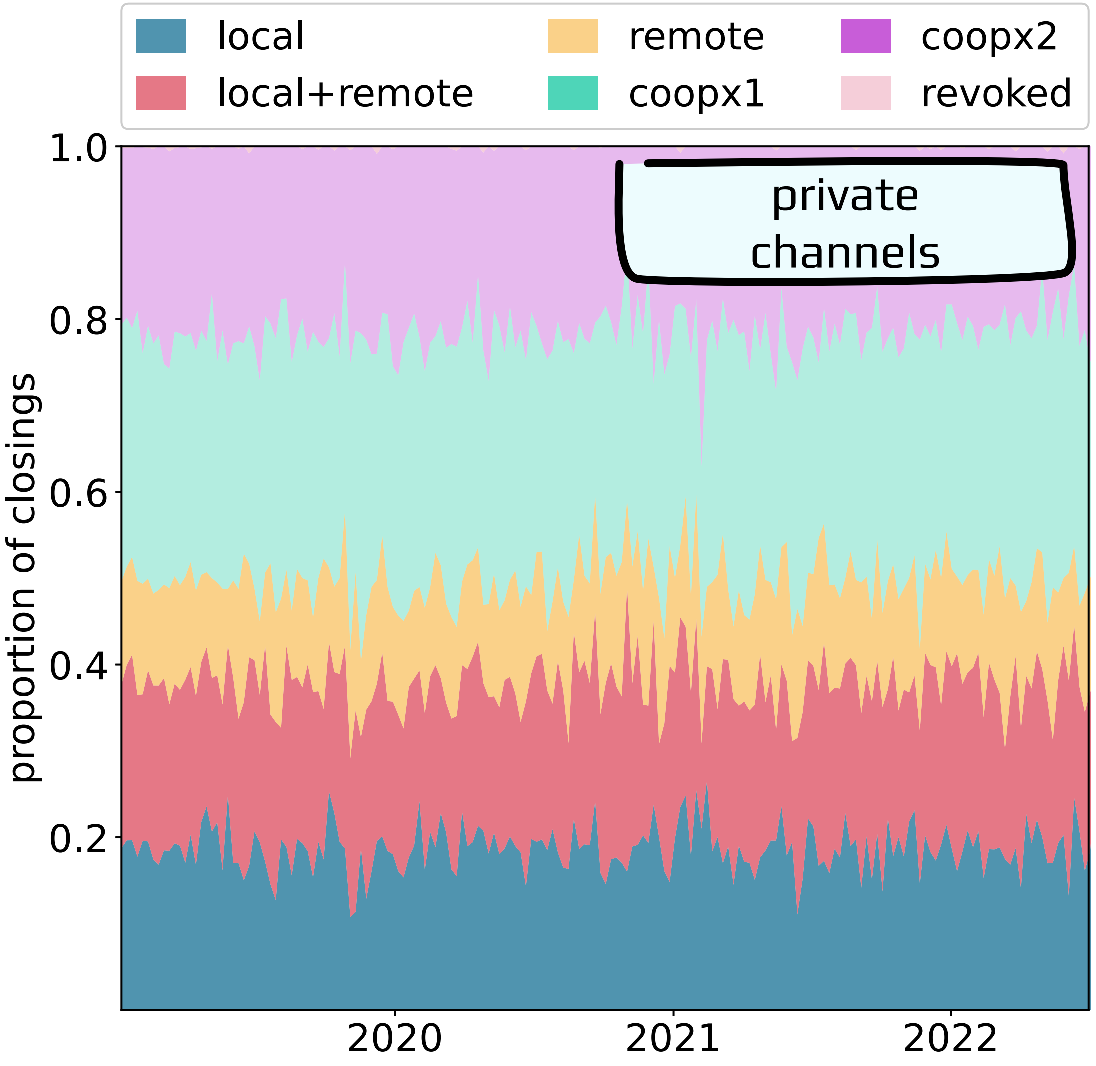
Channel closing outputs


public channels

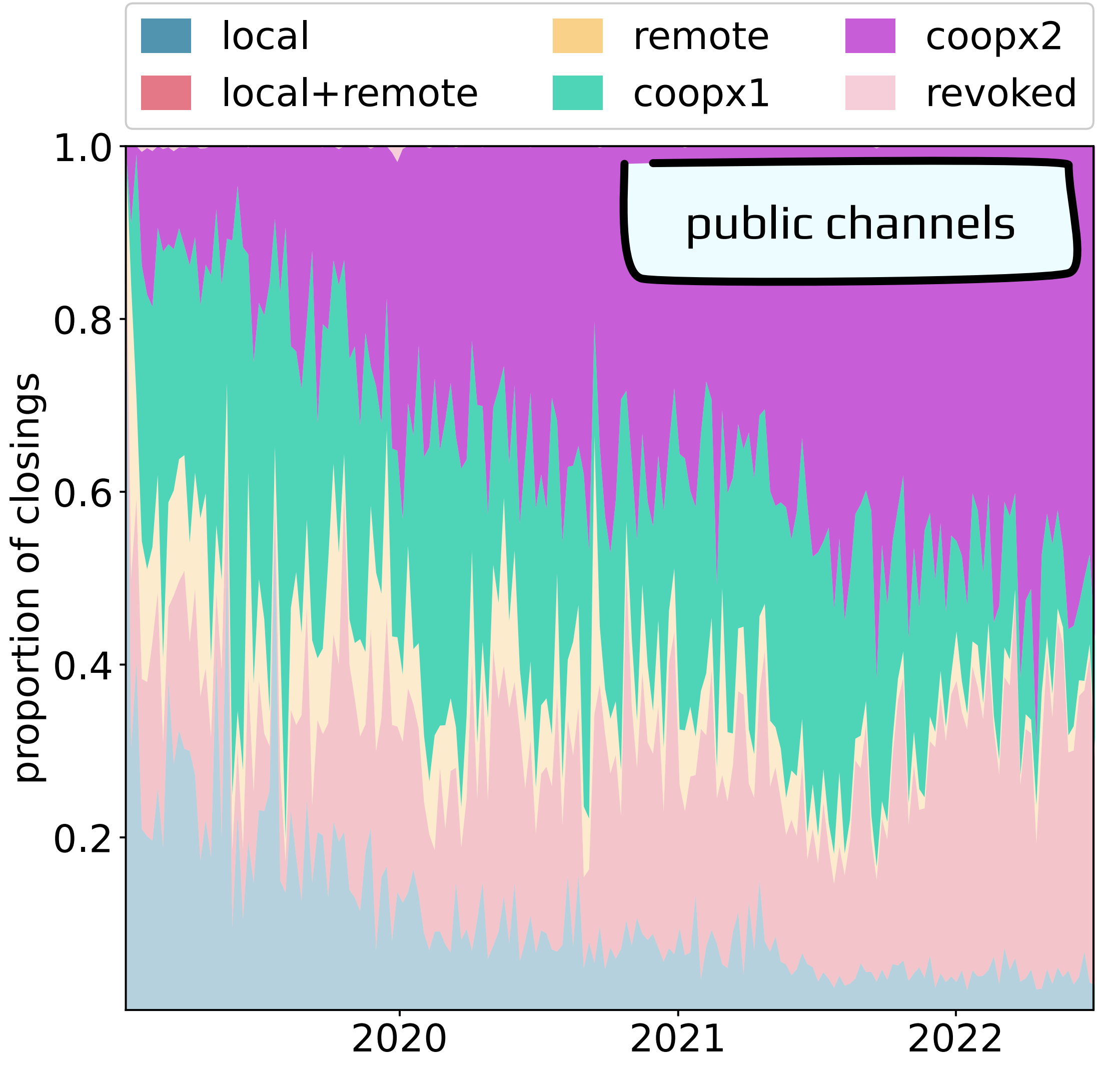

private channels

Channel closing outputs: unilateral closing

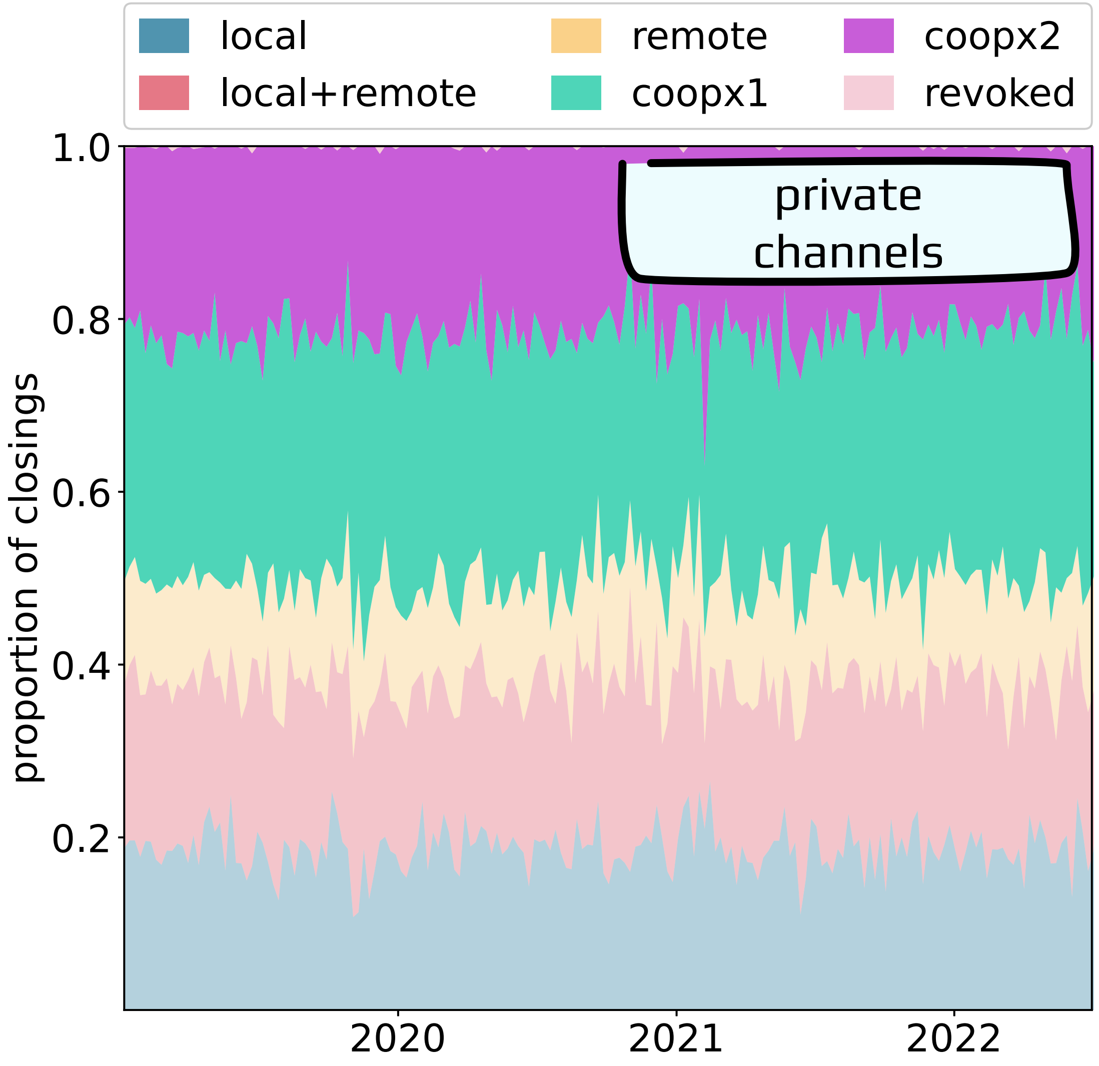




Channel closing outputs: cooperative closing



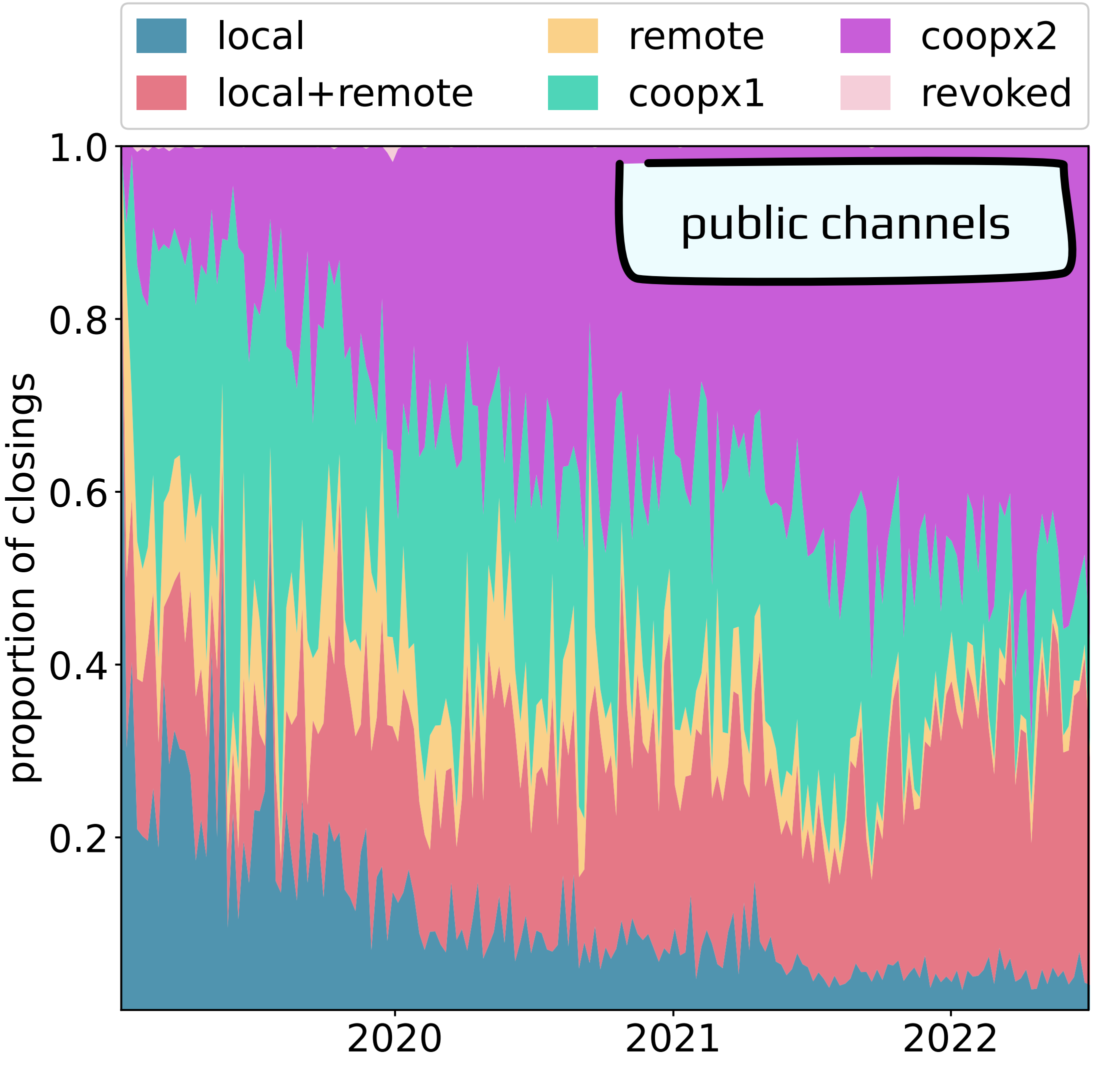
public channels

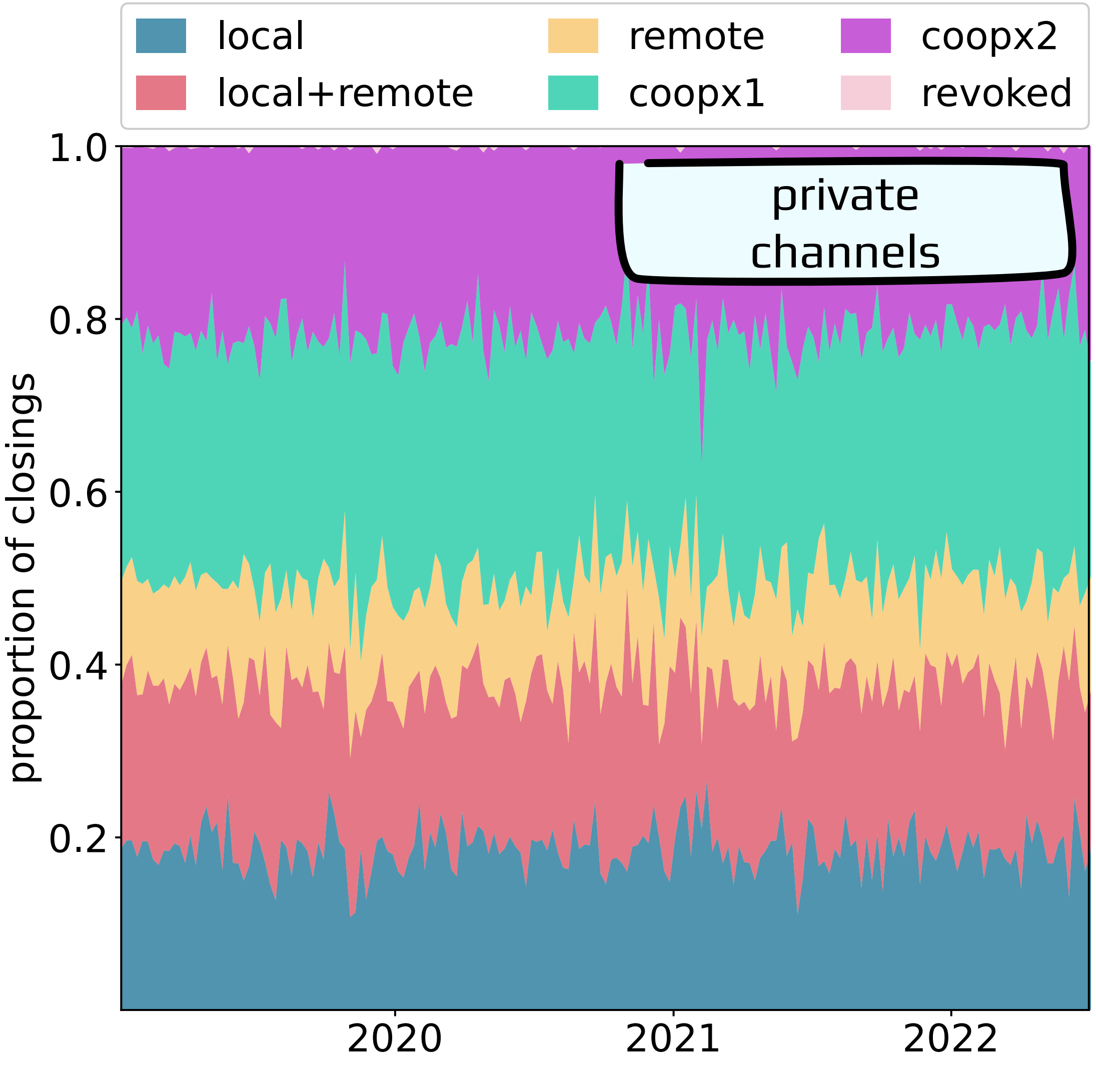


private channels

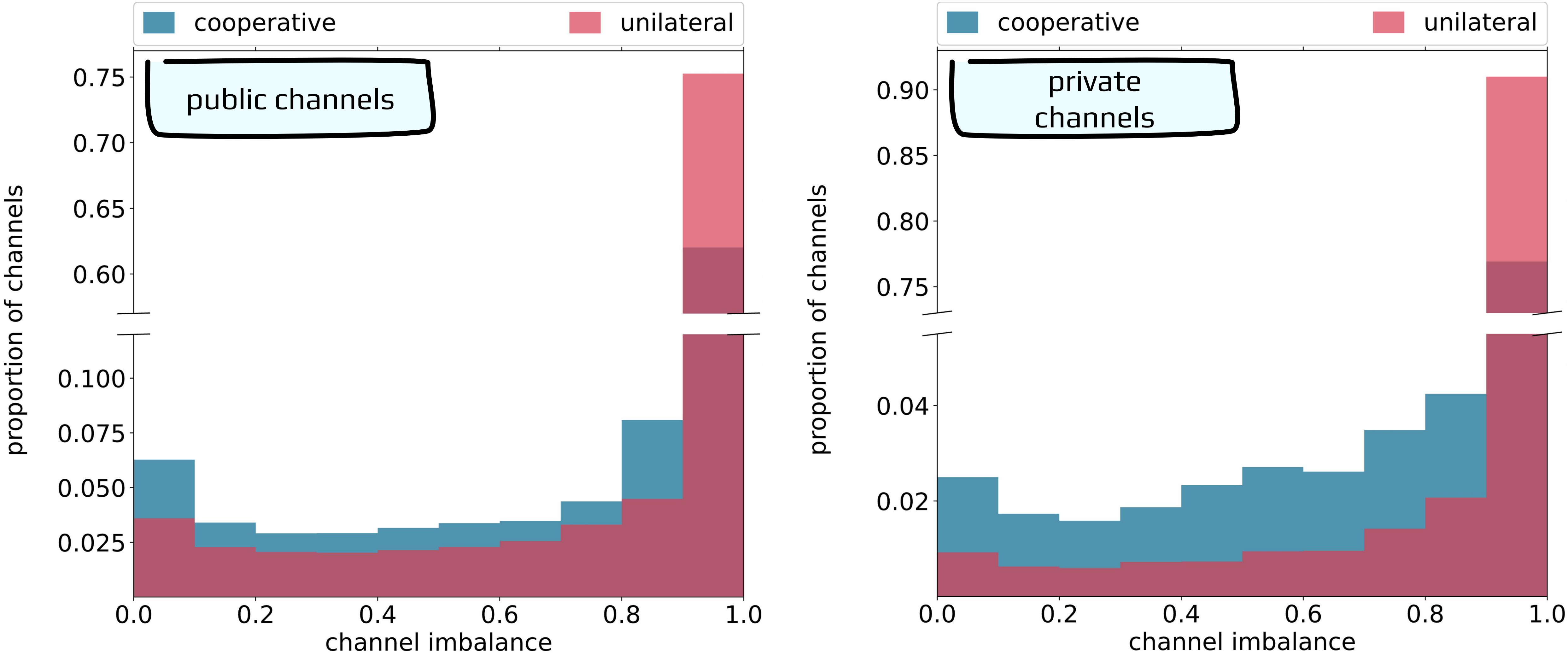
Channel closing outputs

revocations are extremely rare

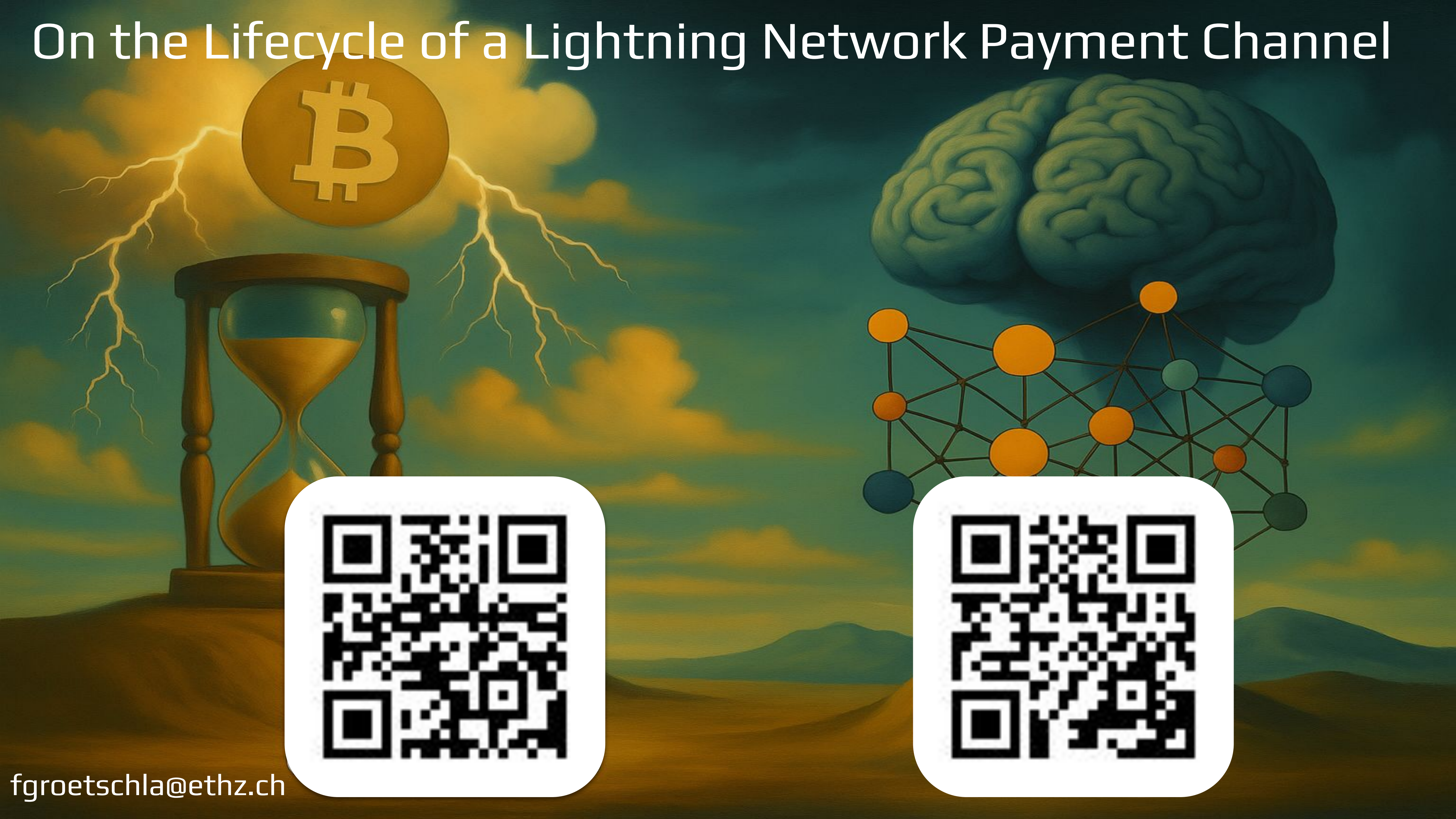




Channels are highly unbalanced at closing, especially unilaterally closed channels



On the Lifecycle of a Lightning Network Payment Channel



fgroetschla@ethz.ch