Attack Vectors

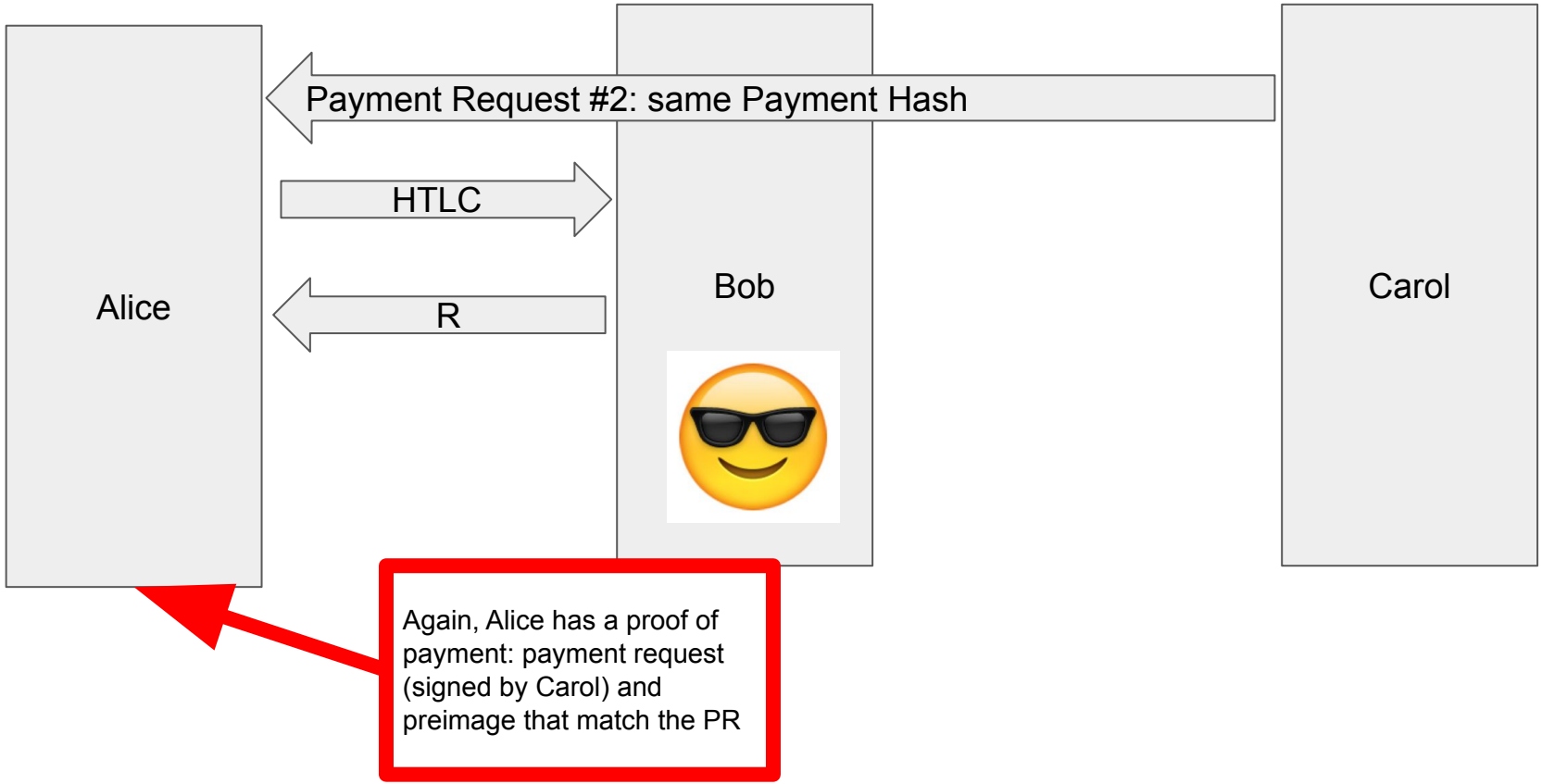
Chaincode LN Residency - NY 2019

Fabrice Drouin <fabrice.drouin@acinq.fr> - https://acinq.co/

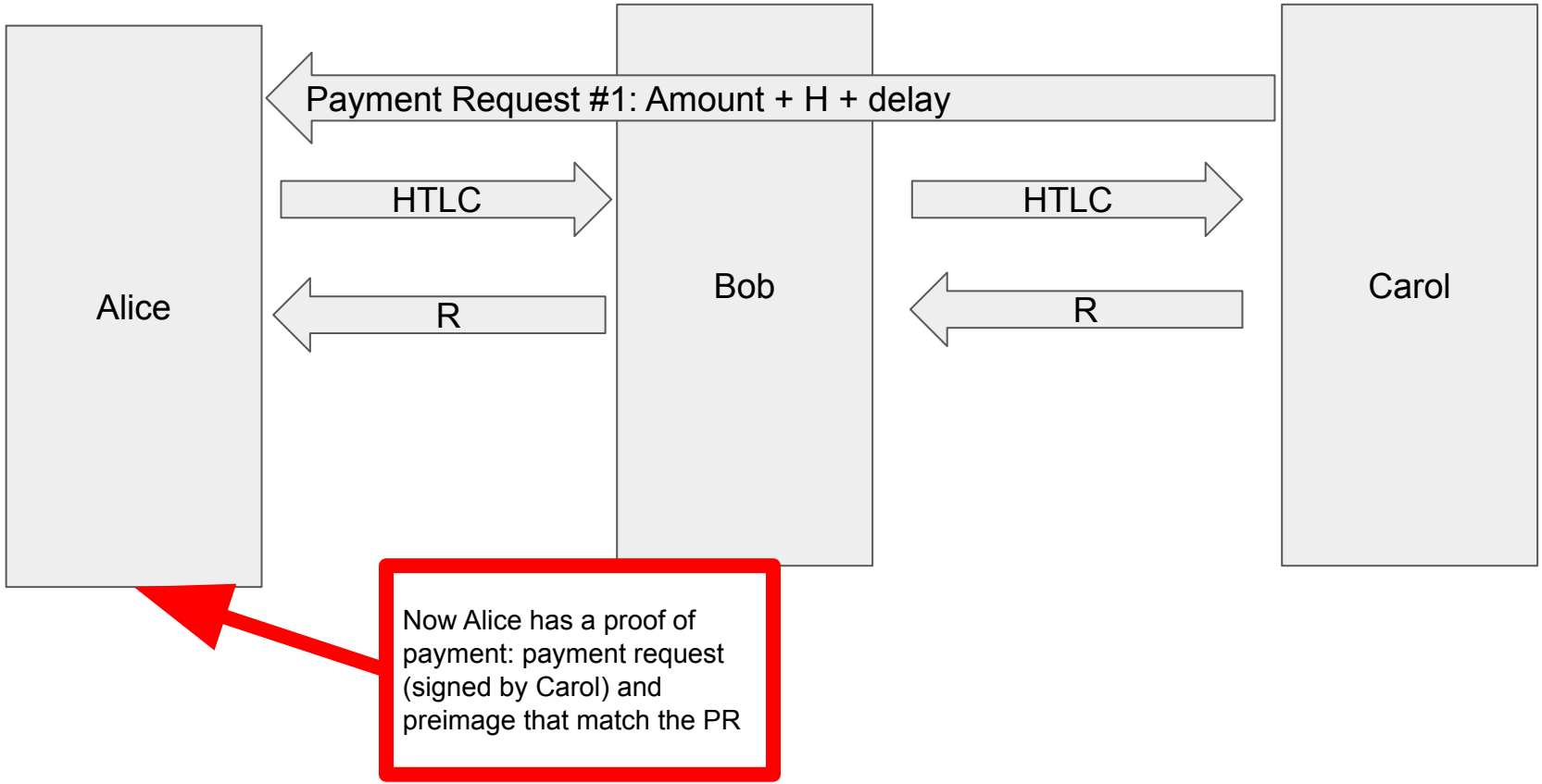
Denial Of Service

- TCP Connections
- Channel lock-up
  - Max pending amount
  - Max pending HTLC
- Resource Usage
  - Routing Table sync
  - Channel Range queries

Preimage reuse



Preimage reuse

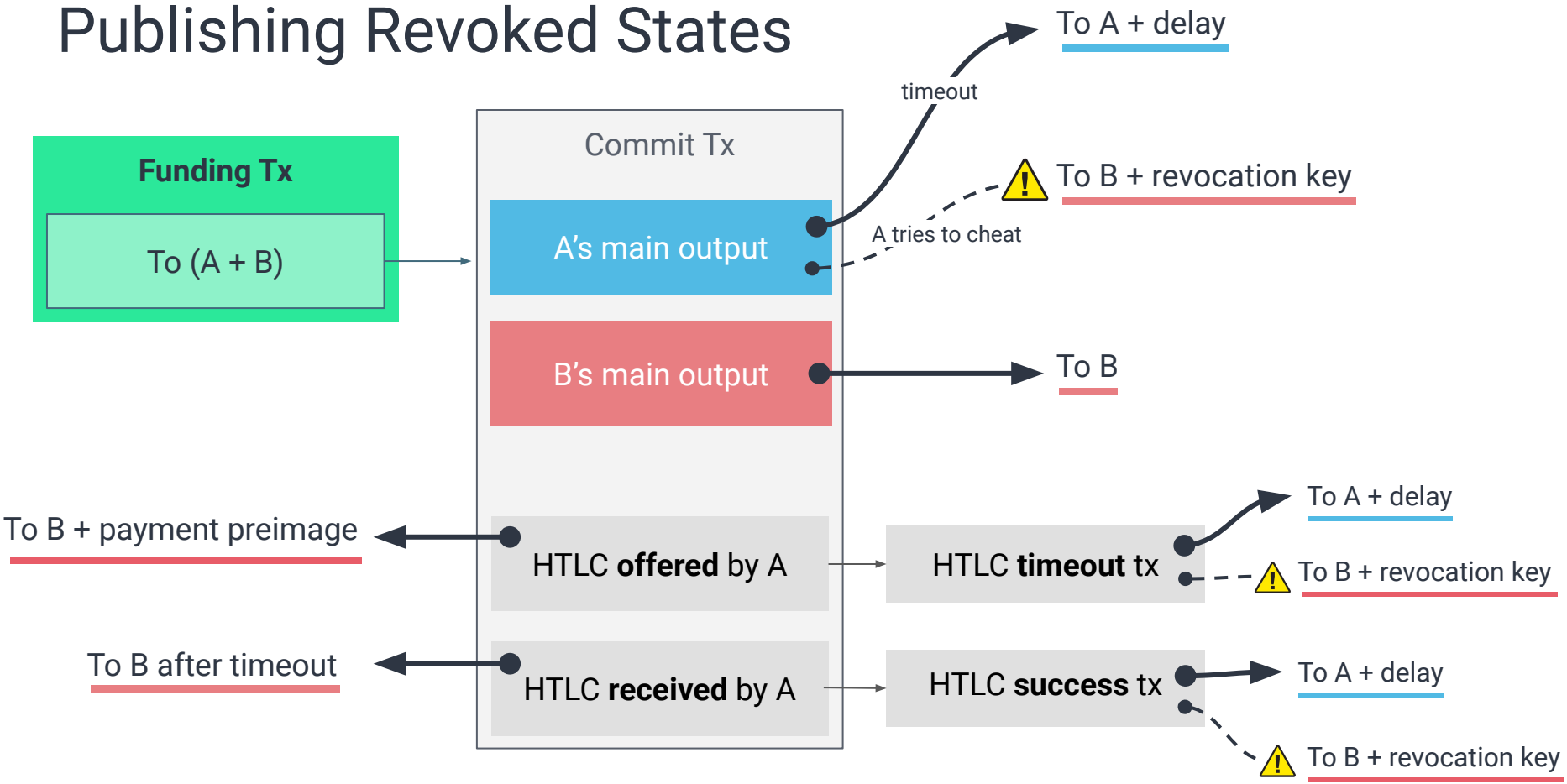


Probing Attacks

Goal: learn information about a payment destination

How ?

Publishing Revoked States



Publishing Revoked States

- Alice funded a channel to Bob
- She made a lot of payments, most of the funds are on Bob’s side
- What if she decides to publish an old commit tx ?
- If she does, there is a delay during which
  - She cannot spend her commit tx outputs
  - But Bob can spend them with the revocation secret he got from Alice

=> Bob must monitor the blockchain from time to time

funding tx is spent => check spending tx => publish penalty tx

Publishing Revoked States

Nodes have been using large CLTV delays (several days, up to 2 weeks)

=> Major UX PITA

What if Bob uses a mobile device that could get be offline for a long time ?

Watch Towers

- Watchtowers monitor the blockchain for Alice
- And publish a penalty tx when Bob tries to cheat
- Privacy issues !!
- Watch towers should not know what you’re doing, or even which channels they’re watching

Watch Towers

=> Each time a commit tx is revoked, you give them the penalty transaction for this commit tx, encrypted with the last 16 bytes of the txid.

index

encryption key

cbf2c70fe5f23e40a02141b01342b1b0537663316cfa878c6057f8336a24a789

Simple design, easy to implement, but you need to store an ever-growing amount of opaque binary data…

=> How to incentivize Watch Towers ?

Watch Towers

Is the “Penalty Tx” idea really that good ?

Most, if not all “cheating attempts” were actually people who mistakenly restored an old state…

=> Eltoo

“Lightning Node” Attack Surface

- OS + Network Stack
- Clients ?
  - “Remote Control” Nodes
- Usual Suspects
  - Buffer overflows
  - Fuzzing
- Onchain Wallet
  - Used only to create funded transactions
  - “Cold” storage, external wallet etc… => How to automate channel opening ?

“Lightning Node” Attack Surface

- LN Wallet
  - Receiving funds => fine
  - Sending funds ?
  - Relaying funds ?
    - Must check that there is a matching incoming payment
- “HSM” ?
  - Not that useful if just blindly signing
  - “Smart HSM” means implementing parts of LN in the HSM...

“Eclipse” Attack