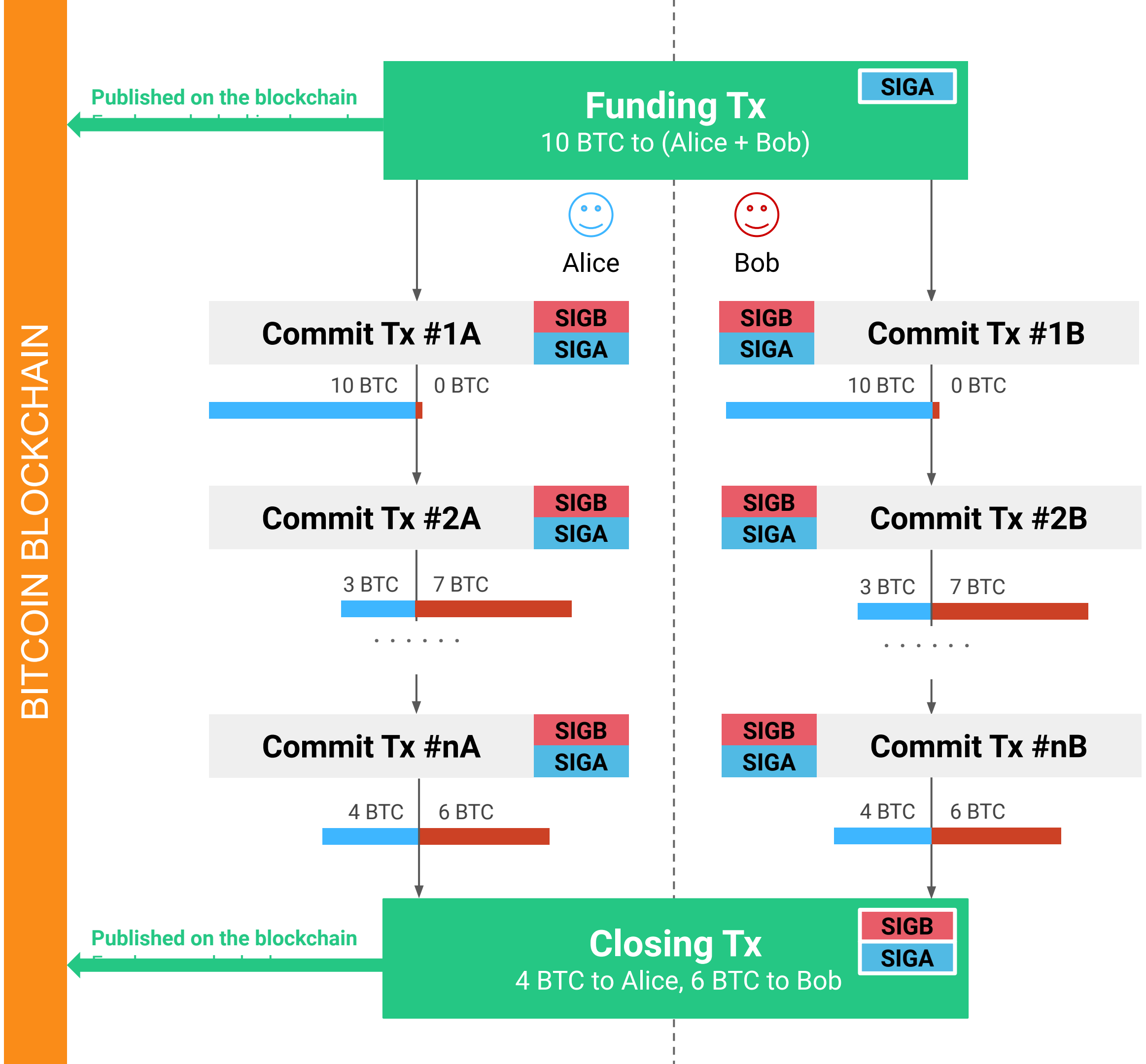
Payment Model

Chaincode LN residency - NY 2019

Context

- Channel = Funding Tx + Commit Tx
- Funding Tx: confirmed, on chain tx that sends to A + B
- Commit Tx: unpublished but publishable tx that spends the funding t



OPEN

First tx is published on the blockchain.
Funds are “locked” in the channel

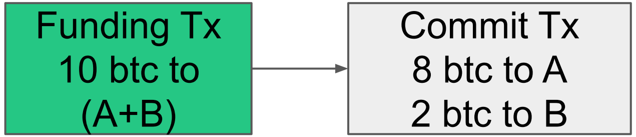
UPDATE

Publishable (signed by both parties) but **not published**!

CLOSE

Last tx is published on the blockchain.
Funds are “unlocked”

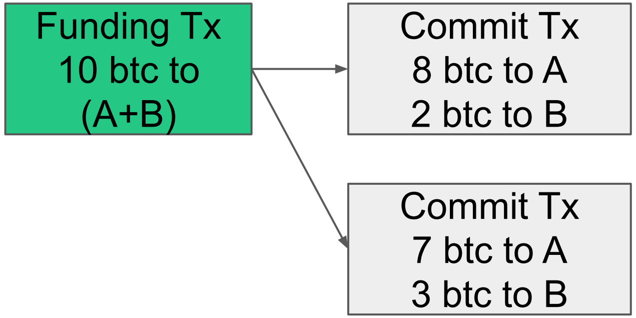
Context



Funding Tx
10 btc to
(A+B)

Commit Tx
8 btc to A
2 btc to B

Context



Funding Tx
10 btc to
(A+B)

Commit Tx
8 btc to A
2 btc to B

Commit Tx
7 btc to A
3 btc to B

Payment Model: HTLC

Hash **T**imed**L**ocked **C**ontract

- I will pay you if you give me the **preimage of a hash**
- If you don’t give it to me I get my money back **after a delay**

Payment Model: HTLC

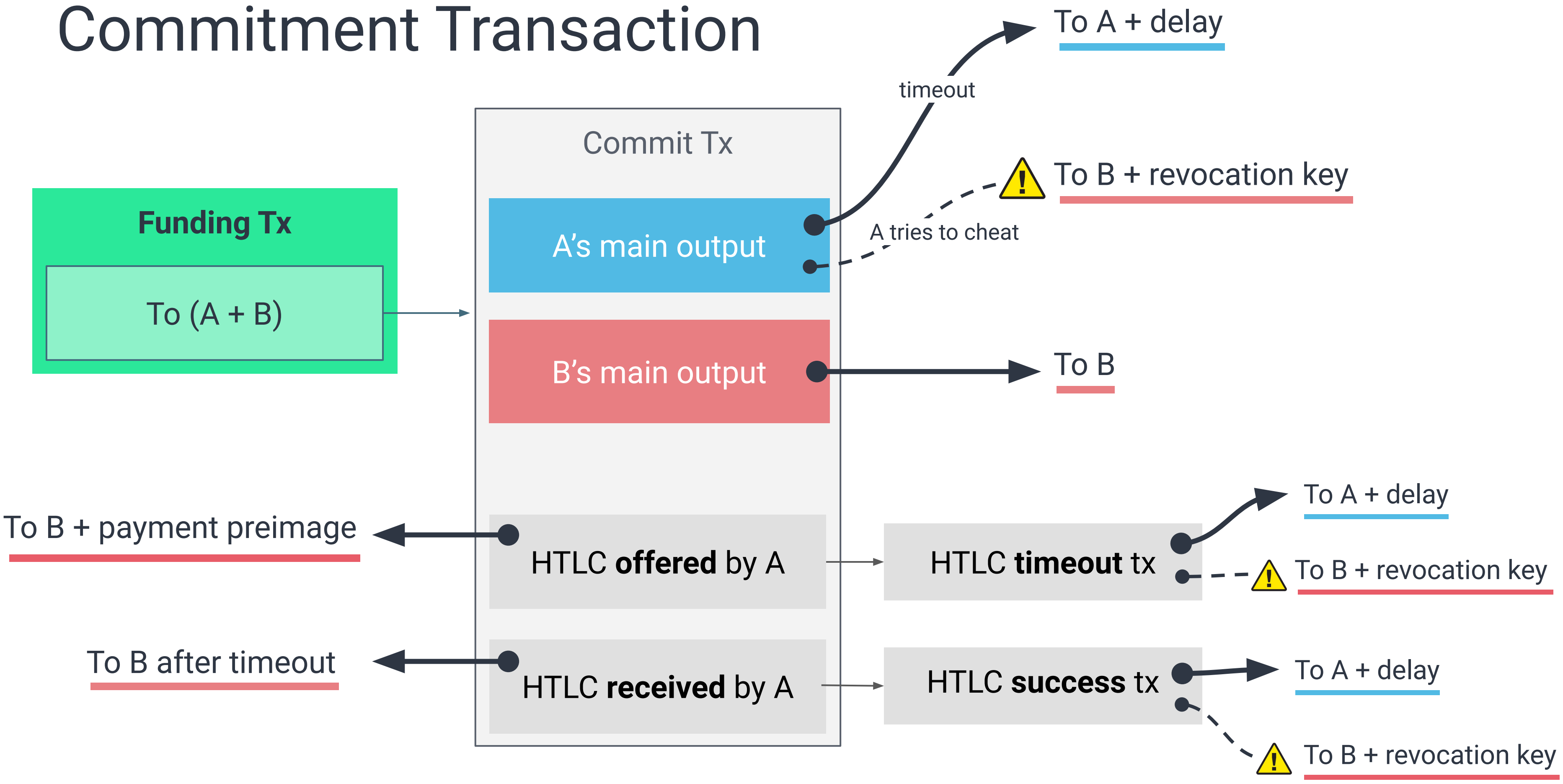
Hash **T**imed**L**ocked **C**ontract

- I will pay you if you give me the **preimage of a hash**
- If you don’t give it to me I get my money back **after a delay**

BIP99 HTLC:

```
OP_IF
      [HASHOP] <digest> OP_EQUALVERIFY OP_DUP OP_HASH160 <seller pubkey hash>
OP_ELSE
      <num> [TIMEOUTOP] OP_DROP OP_DUP OP_HASH160 <buyer pubkey hash>
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
```

Commitment Transaction



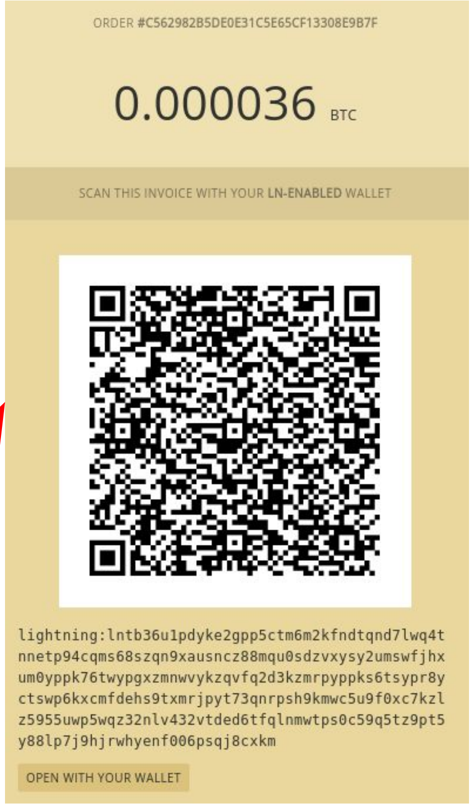
Payment Request

Payment Model: **Hashed Time Locked Contract (HTLC)**

- I will pay you for the preimage of **hash**
- I you don’t reply, I get my money back **after a delay**

Lighting Payment Request: Amount + Hash + Delay

Description = 1 Espresso Coin Panna, 1 Scala Chip Frappuccino
H = c2f7adaac99b5609b7df702ab9cf2b096b806e1a3c040994dde427811cfb071f
NodeId = 035b55e3e08538afeef6ff9804e3830293eec1c4a6a9570f1e96a478dad1c86fed
Amount = 3600000 MilliSatoshis
Timestamp = 1514890568



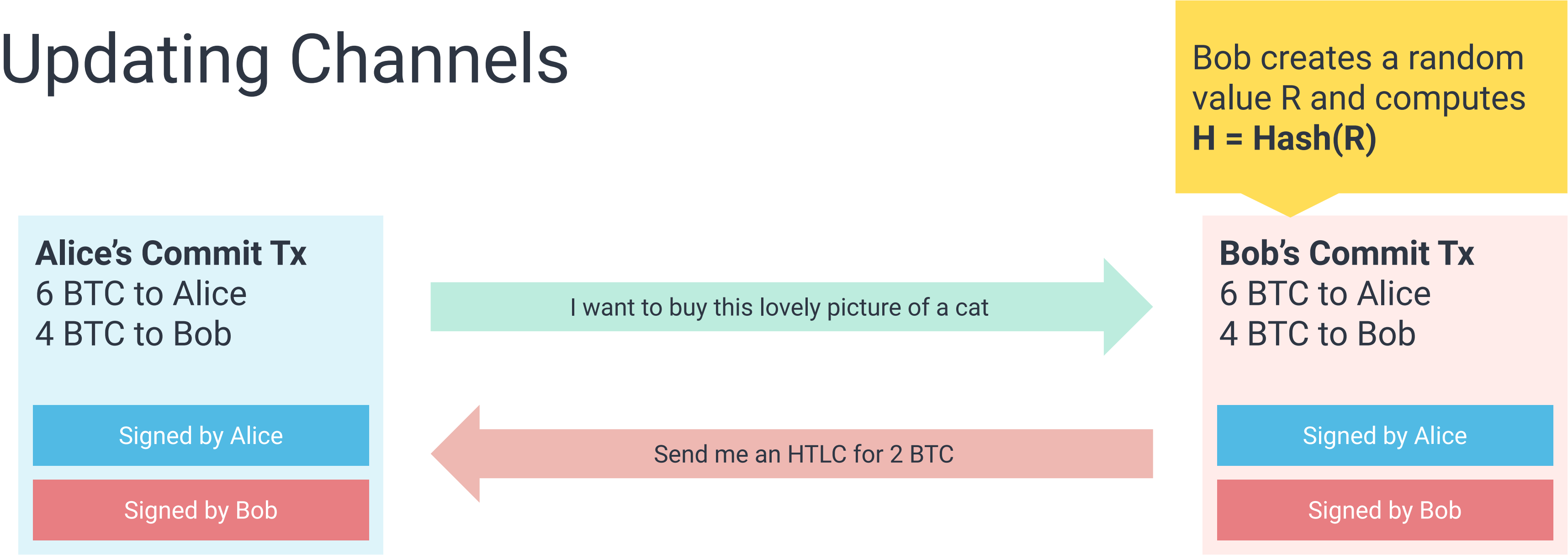
ORDER **#C562982B5DE0E31C5E65CF13308E9B7F**

0.000036 BTC

SCAN THIS INVOICE WITH YOUR **LN-ENABLED** WALLET

```
lightning:lntb36u1pdyke2gpp5ctm6m2kfndtqnd7lwq4t
nnetp94cqms68szqn9xausncz88mqu0sdzvxysy2umswfjhx
um0yppk76twypgxzmnwvykzqvfq2d3kzmrpyppks6tsypr8y
ctswp6kxcmfdehs9txmrjpyt73qnrpsh9kmwc5u9f0xc7kzl
z5955uwp5wqz32nlv432vtded6tfqlnmwtps0c59q5tz9pt5
y88lp7j9hjrwhyenf006psqj8cxkm
```

Updating Channels



Bob creates a random value R and computes **H = Hash(R)**

Alice's Commit Tx
6 BTC to Alice
4 BTC to Bob

Signed by Alice

Signed by Bob

I want to buy this lovely picture of a cat

Send me an HTLC for 2 BTC

Bob's Commit Tx
6 BTC to Alice
4 BTC to Bob

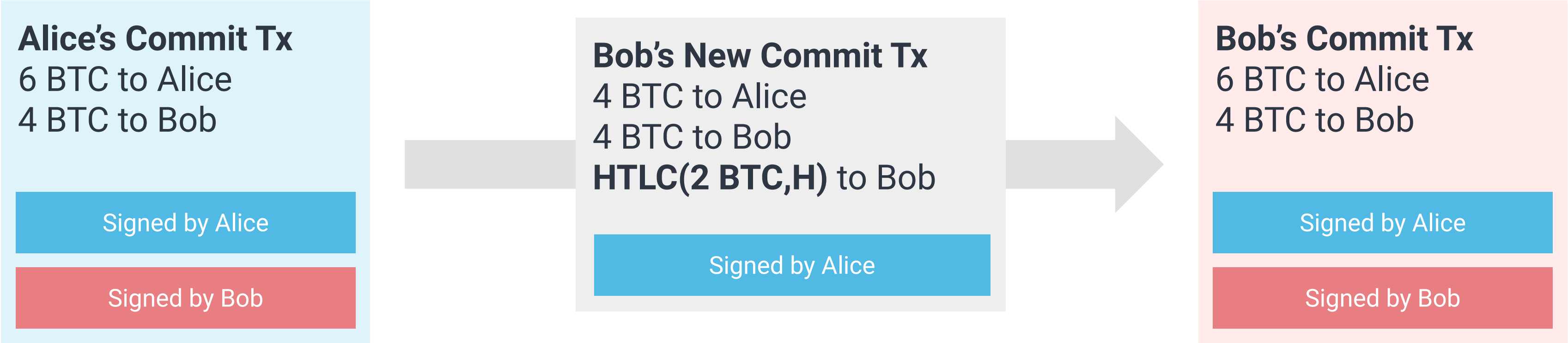
Signed by Alice

Signed by Bob

- Alice wants **to buy a picture** of a cat from Bob
- Bob says "**send me an HTLC** for 2 BTC redeemable **with the preimage of H**"
- This dialog happens **off-band** (web pages, QR codes, …..)

Updating Channels

exchanging signatures



Alice's Commit Tx
6 BTC to Alice
4 BTC to Bob

Signed by Alice

Signed by Bob

Bob's New Commit Tx
4 BTC to Alice
4 BTC to Bob
HTLC(2 BTC,H) to Bob

Signed by Alice

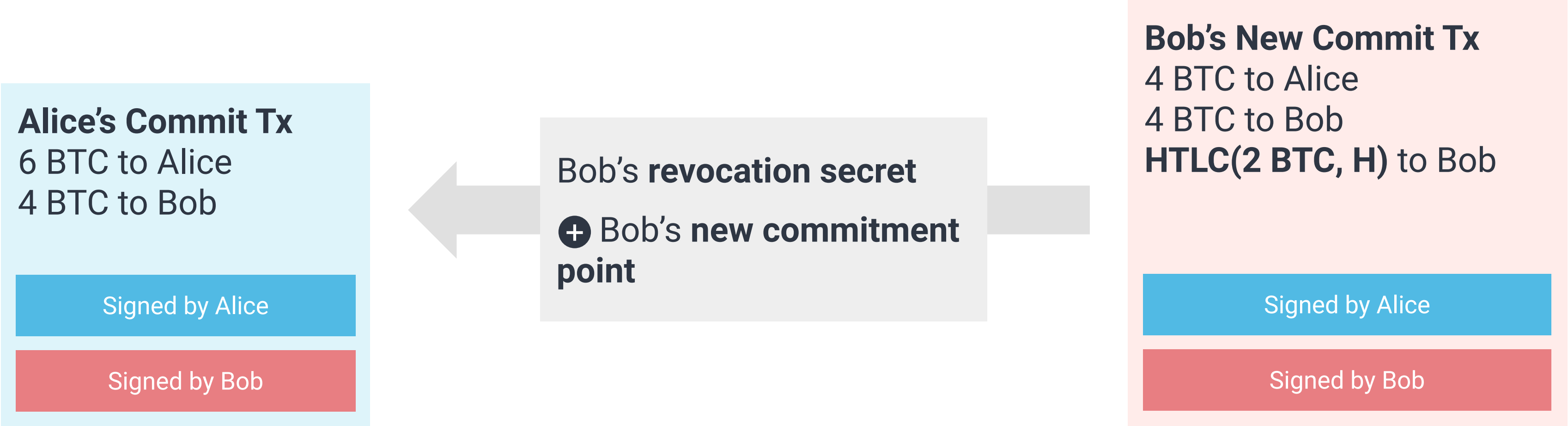
Bob's Commit Tx
6 BTC to Alice
4 BTC to Bob

Signed by Alice

Signed by Bob

- Alice creates a **new Commit Tx for Bob**, which includes the HTLC
- Alice signs Bob's new Commit Tx and send it to Bob

exchanging signatures



Alice's Commit Tx
6 BTC to Alice
4 BTC to Bob

Signed by Alice

Signed by Bob

Bob's **revocation secret**

⊕ Bob's **new commitment point**

Bob's New Commit Tx
4 BTC to Alice
4 BTC to Bob
HTLC(2 BTC, H) to Bob

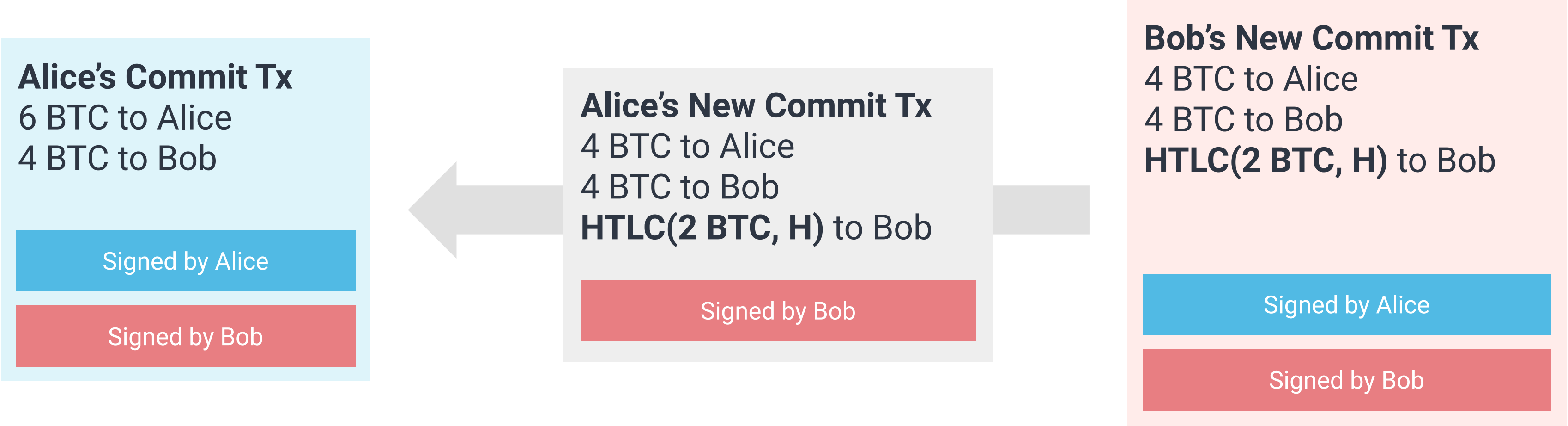
Signed by Alice

Signed by Bob

- Bob checks that **Alice's signature is valid**.
- Bob now has a **valid new commit tx** that includes the HTLC
- Bob replies with the **revocation secret for his old commitment tx**
- Alice checks that the **revocation secret is valid**. Bob cannot publish his old tx anymore

Updating Channels

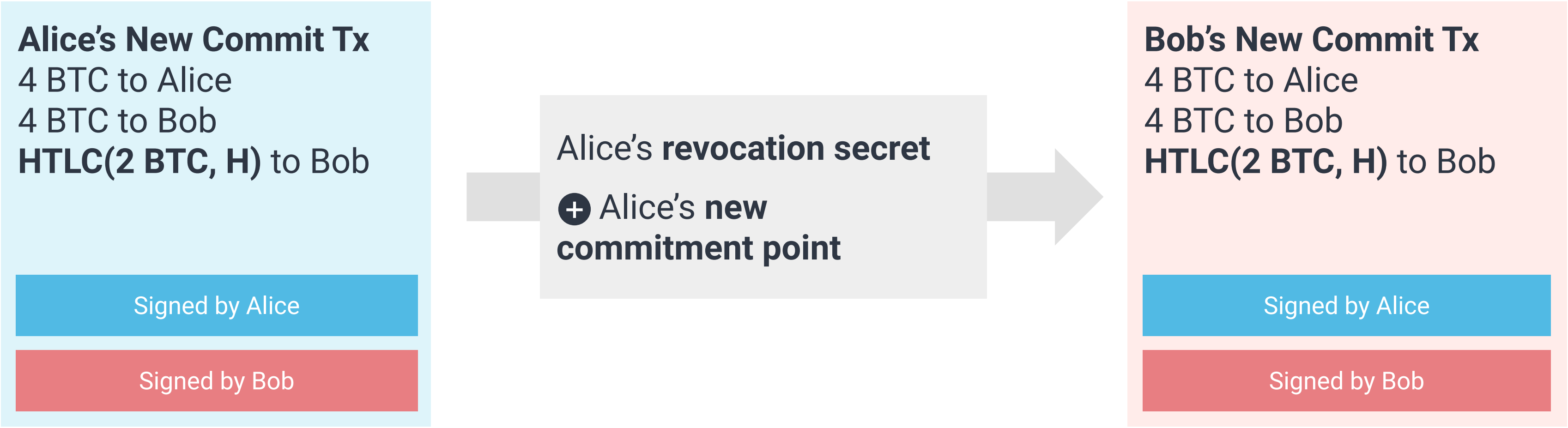
exchanging signatures



- Bob creates a **new Commit Tx for Alice**, which includes the HTLC
- Bob signs Alice's new Commit Tx and send it to Alice

Updating Channels

exchanging signatures



Alice's New Commit Tx
4 BTC to Alice
4 BTC to Bob
HTLC(2 BTC, H) to Bob

Signed by Alice

Signed by Bob

Alice's **revocation secret**

⊕ Alice's **new commitment point**

Bob's New Commit Tx
4 BTC to Alice
4 BTC to Bob
HTLC(2 BTC, H) to Bob

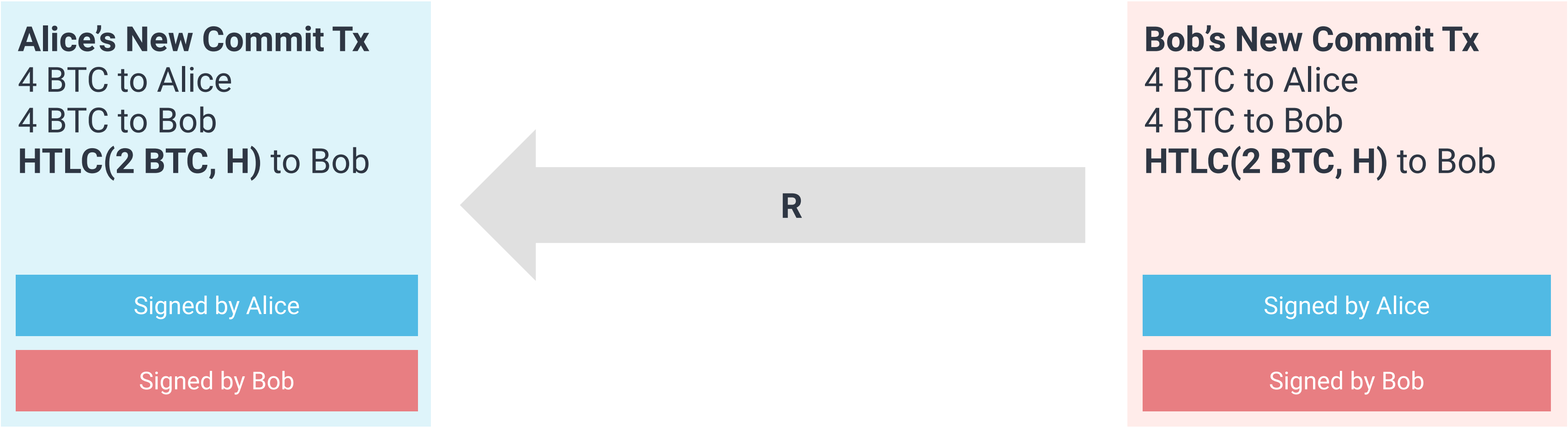
Signed by Alice

Signed by Bob

- Alice checks that **Bob's signature is valid**.
- Alice now has a valid new commit tx that **includes the HTLC**
- Alice replies with the **revocation secret for his old commitment tx**
- Bob checks that the **revocation secret is valid**. Alice cannot publish her old tx anymore

Updating Channels

fulfilling HTLCs



Alice's New Commit Tx
4 BTC to Alice
4 BTC to Bob
HTLC(2 BTC, H) to Bob

Signed by Alice

Signed by Bob

R

Bob's New Commit Tx
4 BTC to Alice
4 BTC to Bob
HTLC(2 BTC, H) to Bob

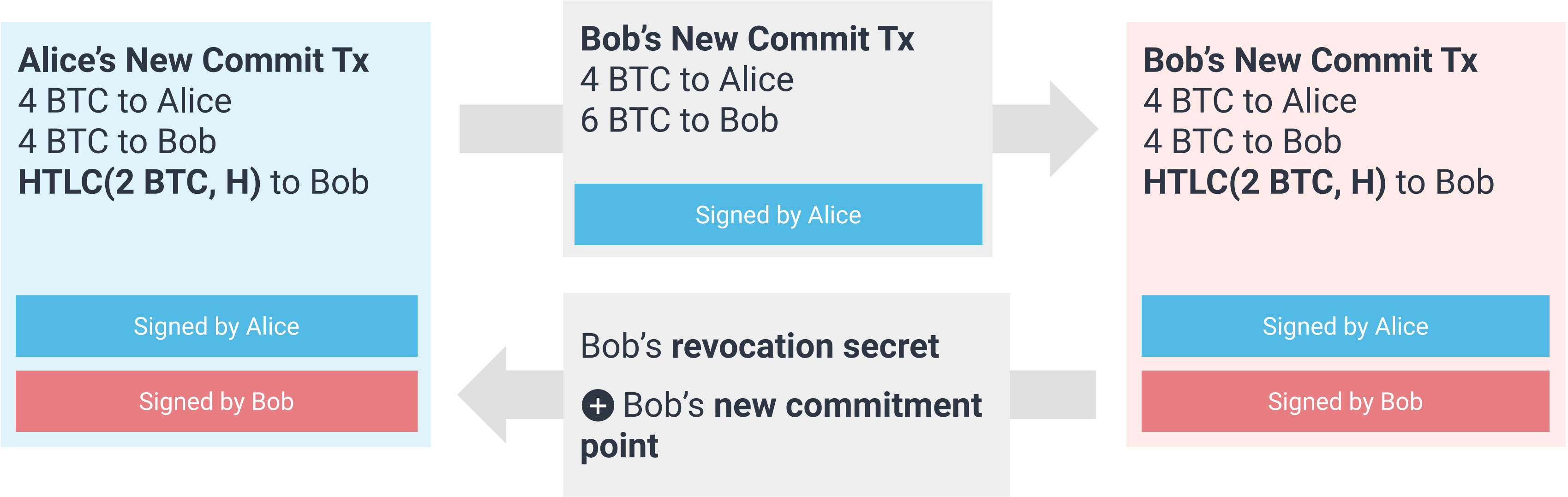
Signed by Alice

Signed by Bob

- Bob sends **R** to Alice
- Alice checks that **Hash(R) == H**

Updating Channels

exchanging signatures



Alice's New Commit Tx
4 BTC to Alice
4 BTC to Bob
HTLC(2 BTC, H) to Bob

Signed by Alice

Signed by Bob

Bob's New Commit Tx
4 BTC to Alice
6 BTC to Bob

Signed by Alice

Bob's New Commit Tx
4 BTC to Alice
4 BTC to Bob
HTLC(2 BTC, H) to Bob

Signed by Alice

Signed by Bob

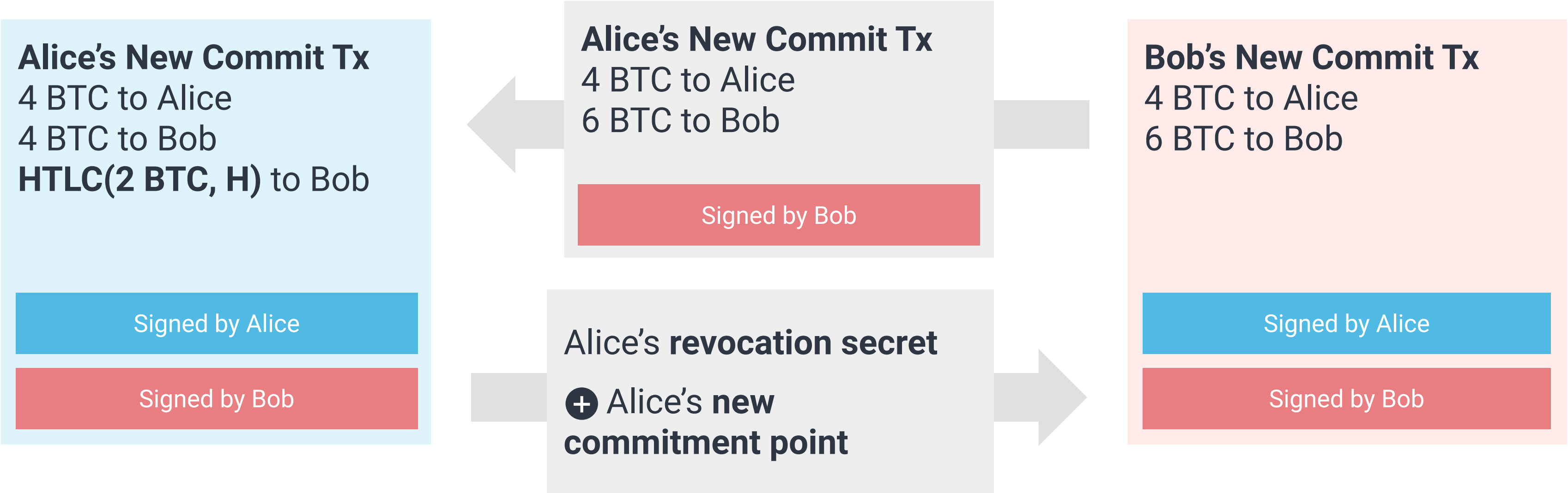
Bob's **revocation secret**

+ Bob's **new commitment point**

- Alice create a new Commit Tx for Bob which **updates his balance and sends her signature to Bob**
- Bob checks the signature and **replies with his revocation secret**

Updating Channels

exchanging signatures



Alice's New Commit Tx
4 BTC to Alice
4 BTC to Bob
HTLC(2 BTC, H) to Bob

Signed by Alice

Signed by Bob

Alice's New Commit Tx
4 BTC to Alice
6 BTC to Bob

Signed by Bob

Alice's **revocation secret**

⊕ Alice's **new commitment point**

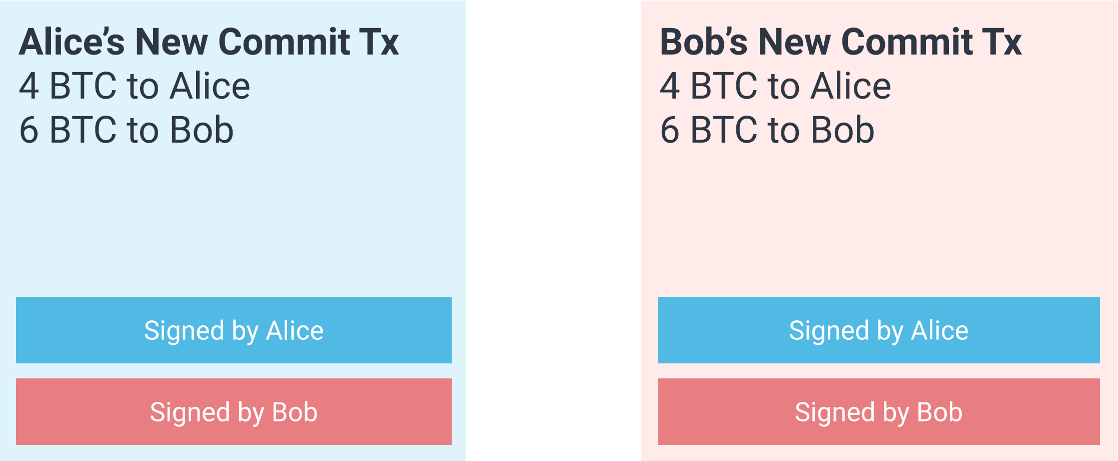
Bob's New Commit Tx
4 BTC to Alice
6 BTC to Bob

Signed by Alice

Signed by Bob

- Bob creates a **new Commit Tx for Alice**, with updated balances
- Bob signs Alice's new Commit Tx and send it to Alice
- Alice checks the signature and **replies with her revocation secret**

fully signed commit tx



Alice’s New Commit Tx
4 BTC to Alice
6 BTC to Bob

Signed by Alice

Signed by Bob

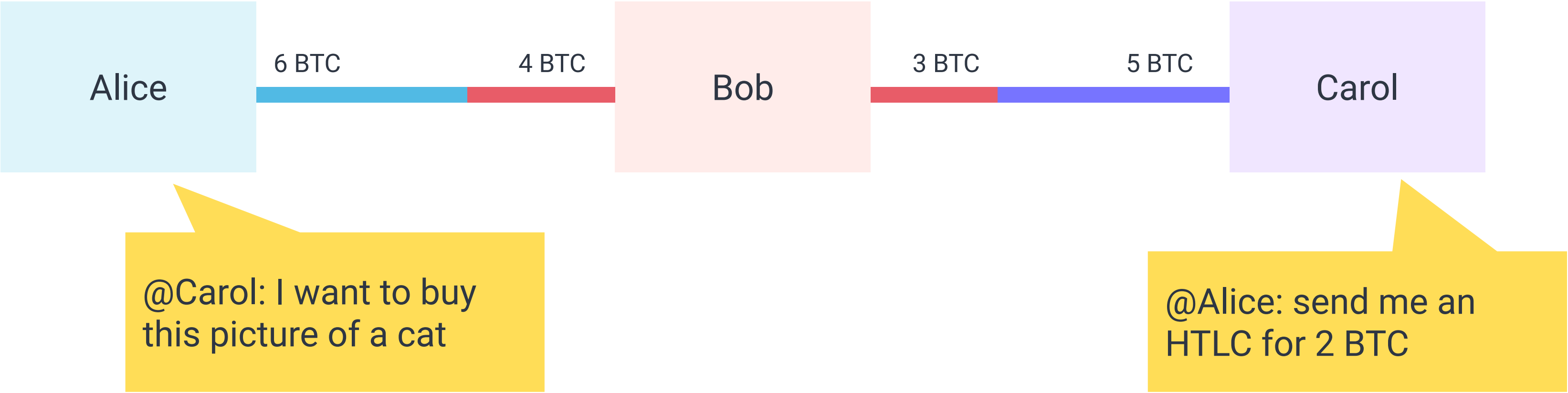
Bob’s New Commit Tx
4 BTC to Alice
6 BTC to Bob

Signed by Alice

Signed by Bob

Alice and Bob now have **fully signed commit tx with updated channel balances**

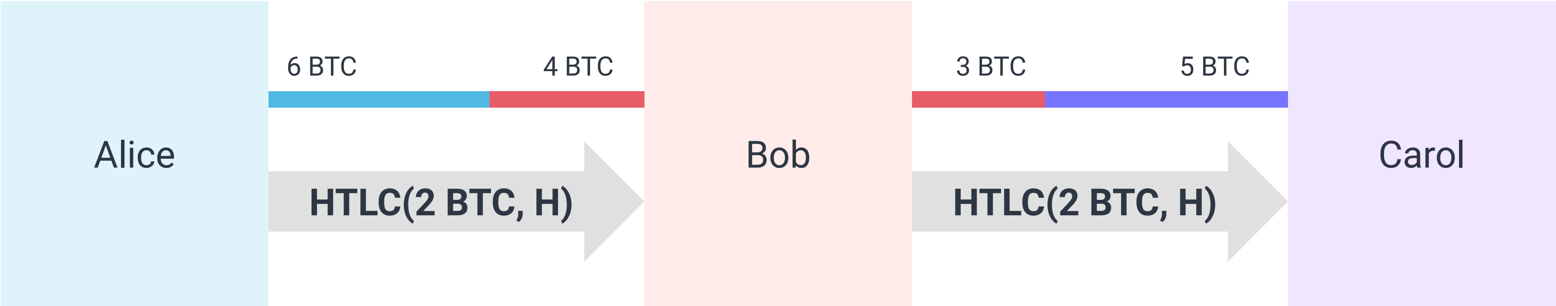
Multi-Hop Payments


Alice
6 BTC
4 BTC
Bob
3 BTC
5 BTC
Carol
@Carol: I want to buy this picture of a cat
@Alice: send me an HTLC for 2 BTC

Carol tells Alice to send her an HTLC for 2 BTC redeemable for the preimage of H

Multi-Hop Payments

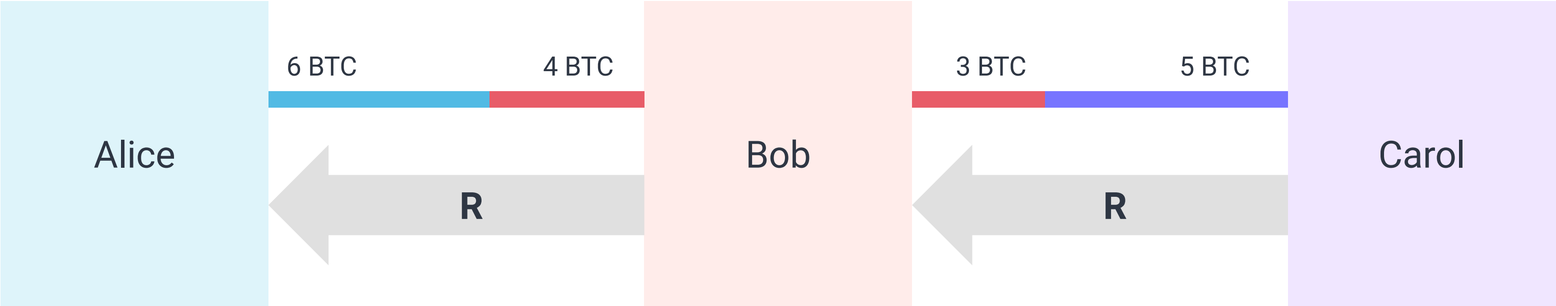
forward HTLC



Alice sends an HTLC to Bob and ask him to **forward the same HTLC** to Carol

Multi-Hop Payments

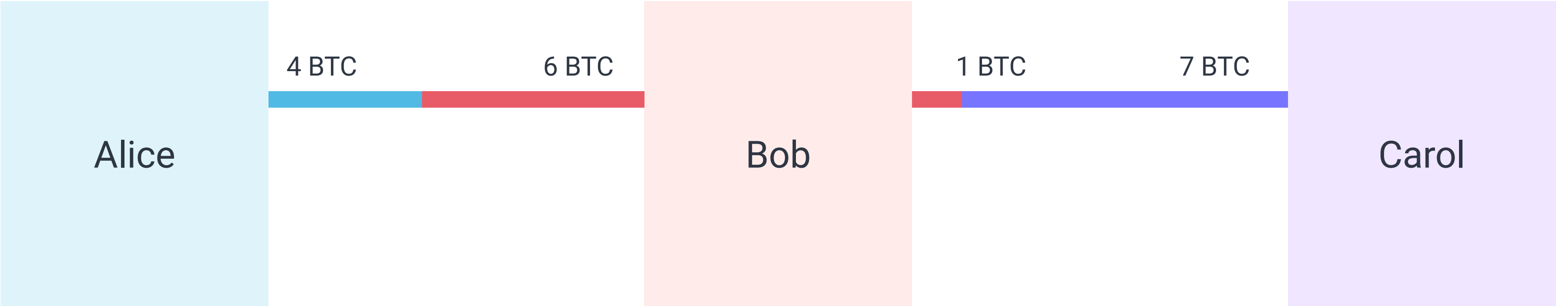
forward Preimage



- Carol sends the Payment Preimage to Bob
- Bob forwards the Payment Preimage to Alice

Multi-Hop Payments

update balance



- Alice, Bob and Carol have **updated their balances**
- Bob **still has 7 BTC** (but Bob might ask for a small fee to relay payments)

Limitations

- What happens if you reuse a payment hash ?
- H and R are the same in all hops
  - Bad for privacy
  - Can be improved if we switch to using signatures instead of Preimage/Hash