OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

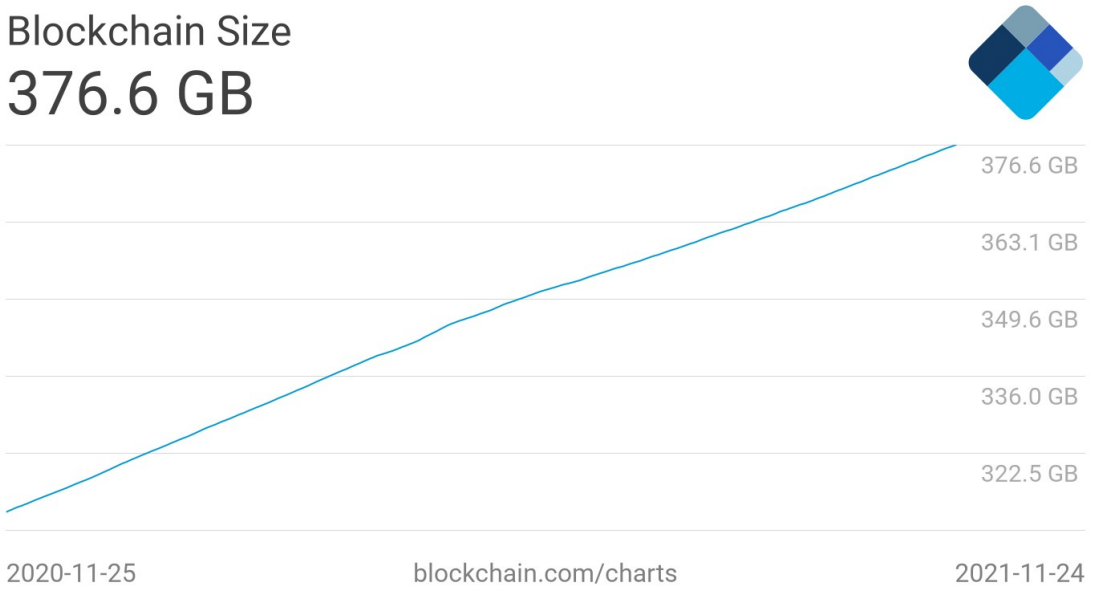
Layer 2 Solutions - Payment Channels

Thomas Bocek

25.11.2021

Scalability Solutions

- Blockchains grow linearly
- Solutions
  - 1. First Layer Scalability Solutions (on-chain)
    - Sharding (distribute storage)
    - Improve protocol (SegWit, Taproot, Rollups)
  - 2. Second Layer Scalability Solutions (off-chain)
    - State Channels (payment channels)
      - Lightning Network
    - Sidechains / Blockchain Interoperability



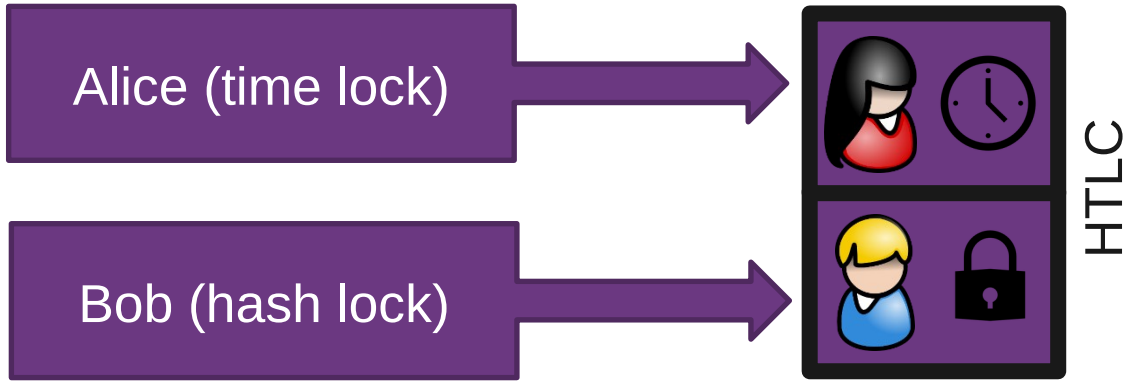
OST

Recap: Hashed Time-Locked Contracts

- Building block for cross-chain atomic swaps and payment ch.
- Hash time lock:
  - store hashed secret – publicly stored in a smart contract
  - unlock – only if secret is provided (publicly) before timeout

Or

  - unlock – after timeout



Hash time lock (HTLC)

Hash lock to Bob

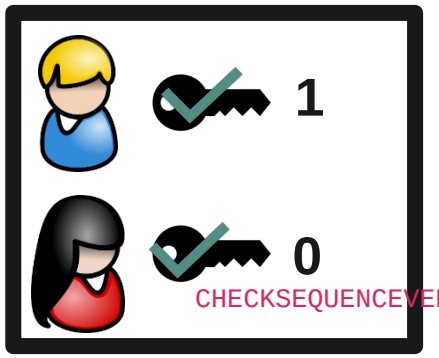
Time lock to Alice

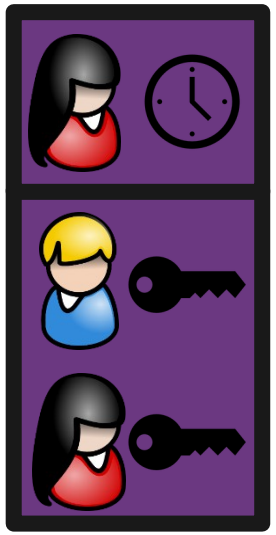
```
OP_IF
  OP_SIZE
  AddInt64(secretSize)
  OP_EQUALVERIFY
  OP_SHA256
  AddData(secretHash)
  OP_EQUALVERIFY)
  OP_DUP
  OP_HASH160
  AddData(pkhThem[:])
OP_ELSE
  AddInt64(locktime)
  OP_CHECKLOCKTIMEVERIFY
  OP_DROP
  OP_DUP
  OP_HASH160
  AddData(pkhMe[:])
OP_ENDIF
OP_EQUALVERIFY
OP_CHECKSIG
```


OST

Direct Payment Channel with 2-of-2 Multisig Contracts

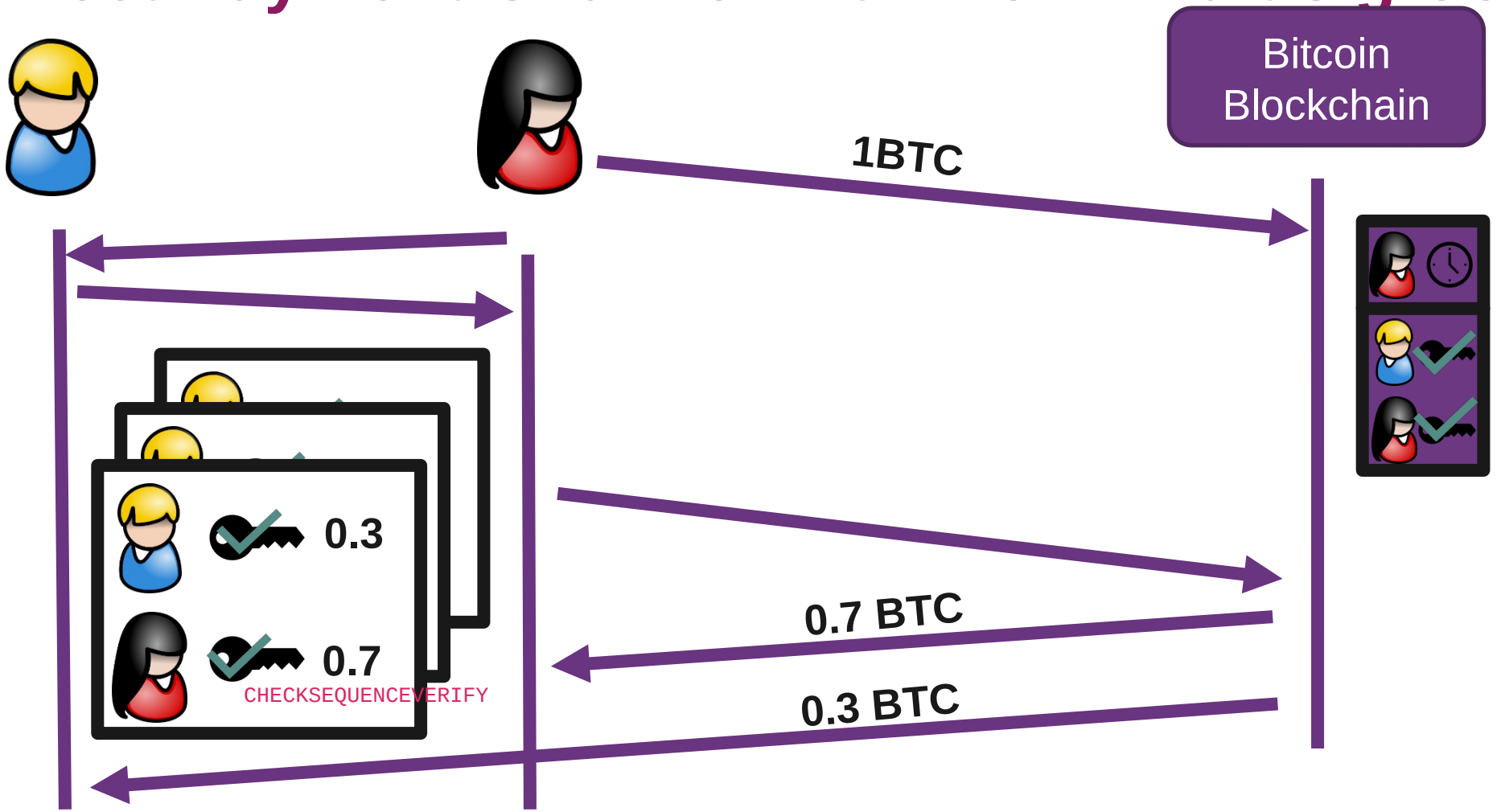
- Open a payment channel between Alice and Bob
  - 1 BTC of Alice to Locked Multisig
  - 2-of-2 multisig
    - Initial offchain TX
  - Bob does nothing





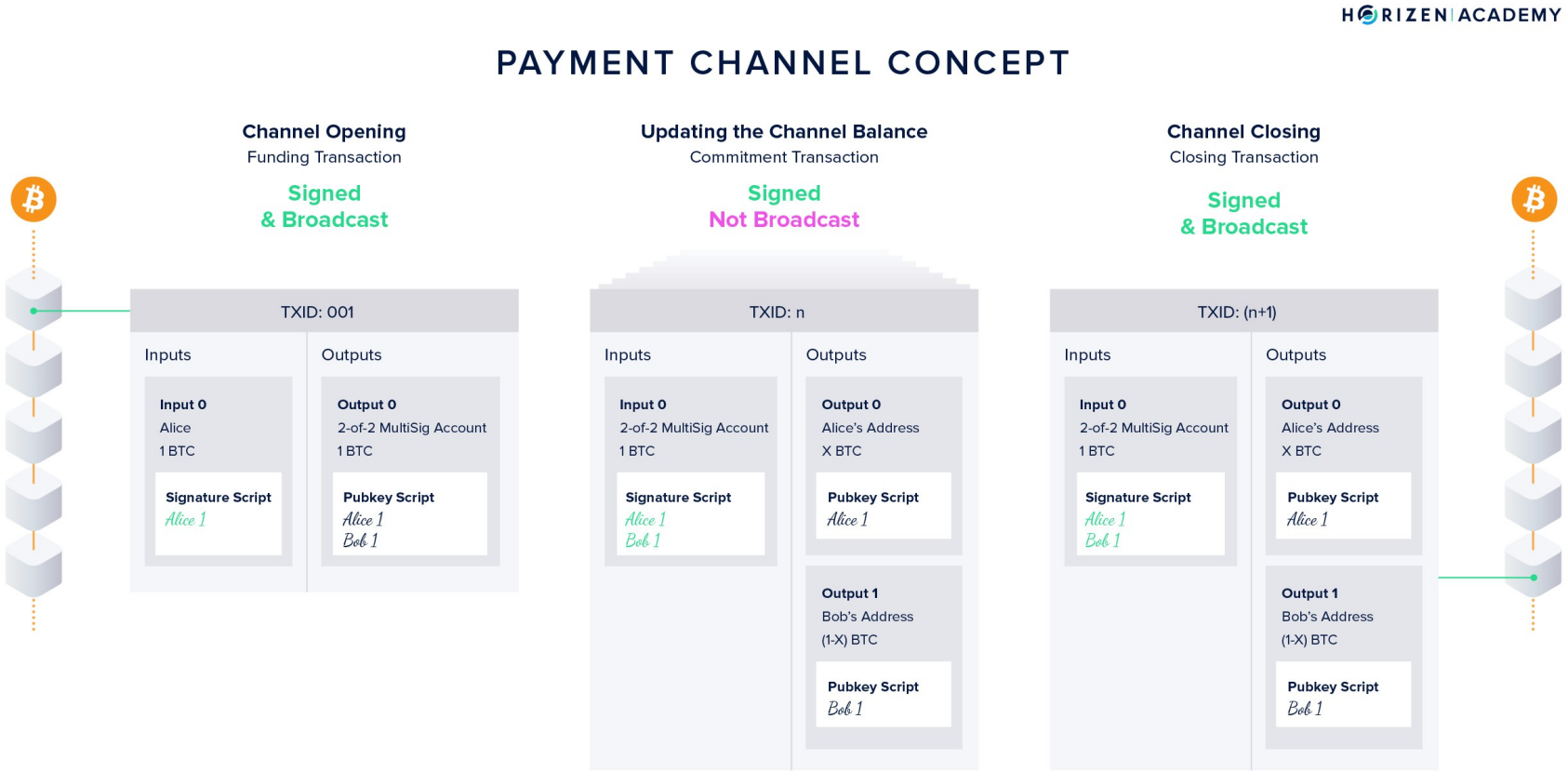
OST

Direct Payment Channel with 2-of-2 Multisig Contracts



OST

Other View on Direct Payment Channels

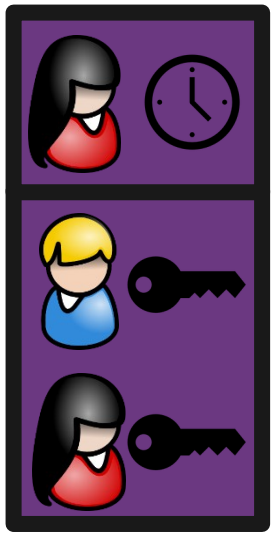


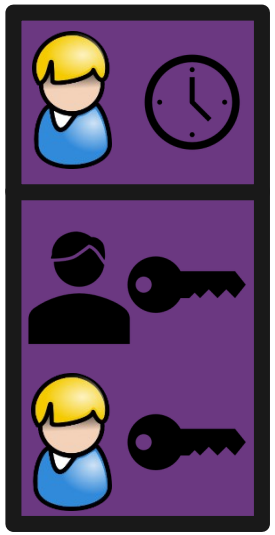
https://academy.horizen.io/technology/expert/state-and-payment-channels/

OST

Indirect Payment Channel with HTLC

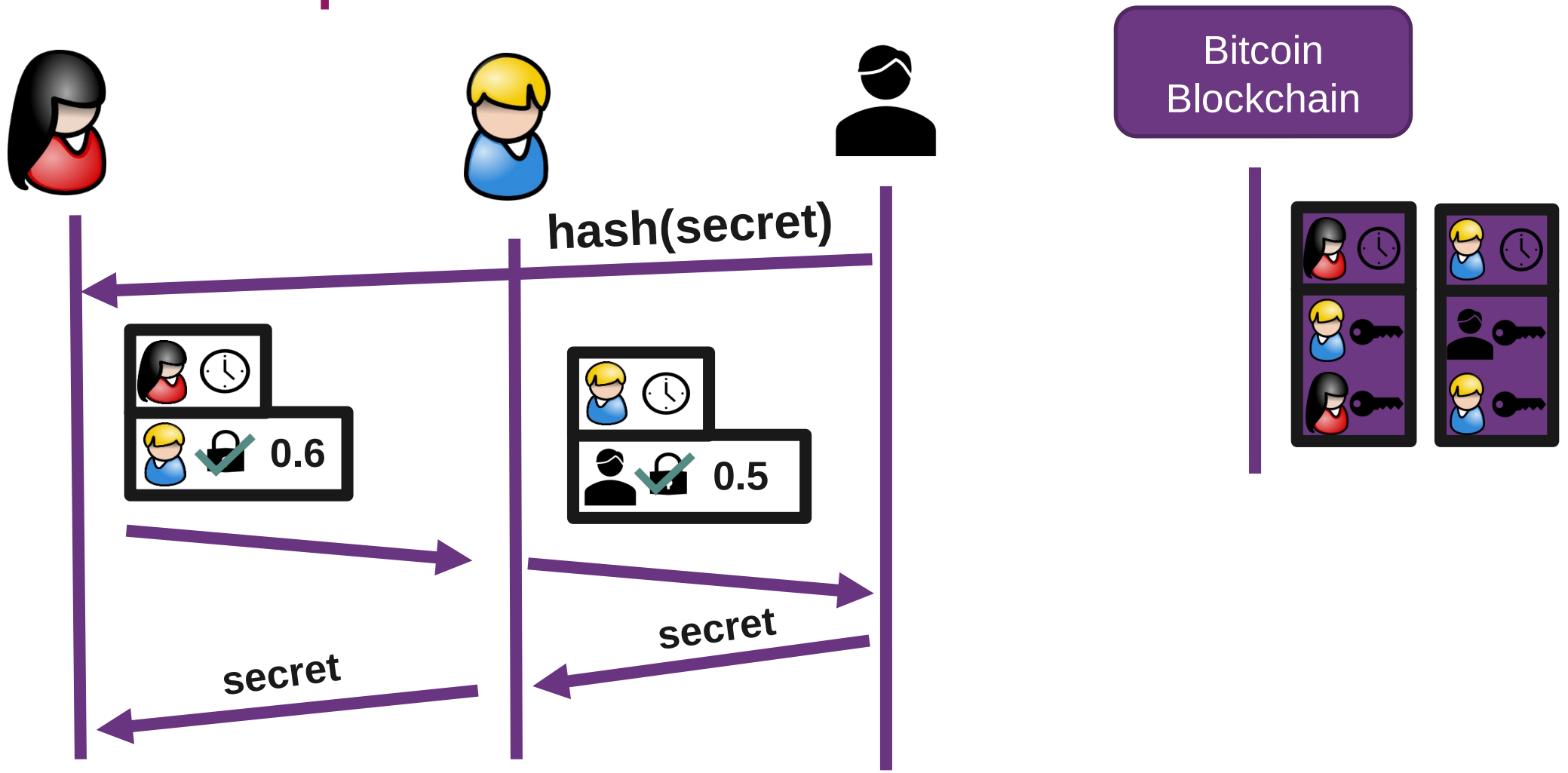
- Now we are ready to open a payment channel between Alice and Bob and Charlie
  - 1 BTC lockup, Alice – Bob, Bob – Charlie
  - Alice wants to send 0.5 BTC to Charlie (no direct channel)





OST

Atomic Swaps - Alice needs to reveal secret to redeem 1 BTC



OST

Other View on Indirect Payment Channels

https://medium.com/softblocks/lightning-network-in-depth-part-2-htlc-and-payment-routing-db46aea445a8