Lecture 13: Layer 2 Scaling: Payment Channels

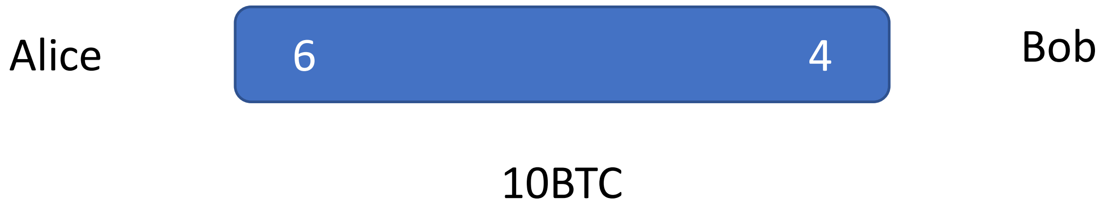
https://web3.princeton.edu/principles-of-blockchains/

Professor Pramod Viswanath
Princeton University

This lecture:
Layer 2 Scaling -- no need to change the consensus;
Payment channels; Scaling Bitcoin; Lightning network

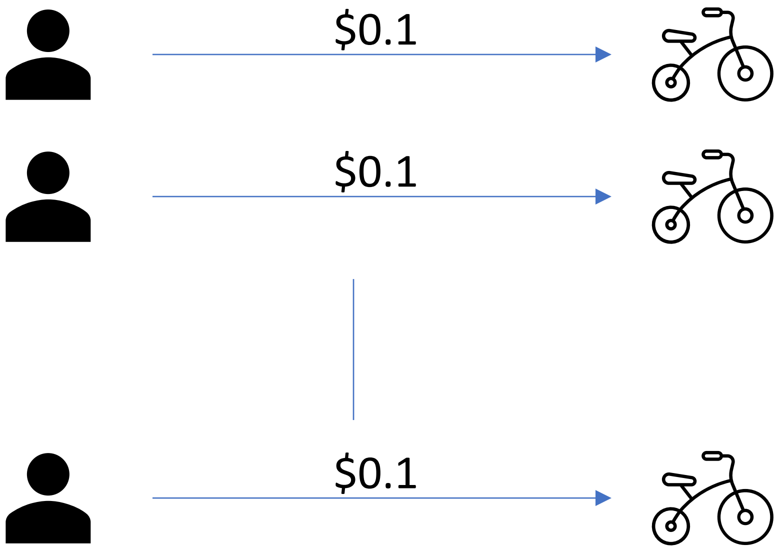
Payment channels vs Sidechains

- Sidechains:
  - Small set of nodes (managers) maintain a blockchain pegged to Ethereum
  - Resolve disputes on chain
- Payment channels:
  - Make payment off chain (participation only between parties involved in the transaction (and some others))
  - Only post transaction on-chain to start the channel and handle a dispute



Payment channels: One-way example

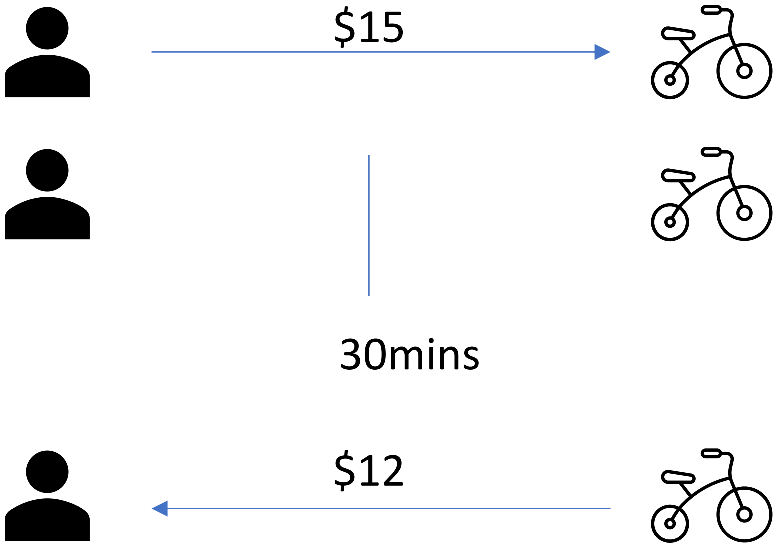
Use a bike sharing service: $0.1 per minute



$0.1

$0.1

$0.1



$15

30mins

$12

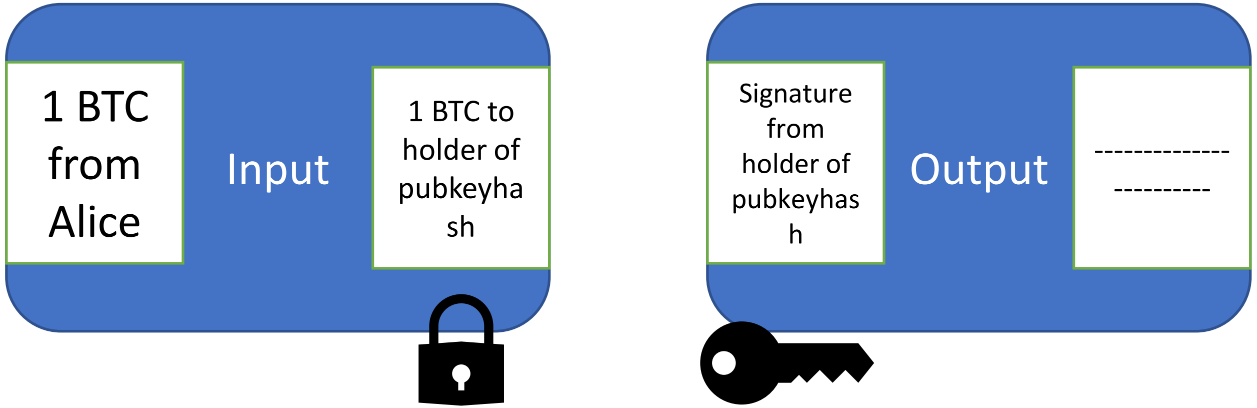
What if the user does not trust the bike to send back $12?
You need a collateral?

Locking and unlocking script: Pubkeyhash

```
<sig>
<pubkey>
__________
OP_DUP
OP_HASH160
<pubkeyhash?>
OP_EQUALVERIFY
OP_CHECKSIG
```

Redeeming transaction (Unlocking)

Referenced output transaction (UTXO input) (Locking)



1 BTC from Alice

Input

1 BTC to holder of pubkeyhash

Signature from holder of pubkeyhash

Output

Multisig

- Locking transaction has to be signed by k out of n pubkeys.
- Example: Requires transaction by Bob and Carol to unlock (2 out of 2)
    - Cannot be unlocked by signature of Bob or Carol alone

Hashlock

- Can be unlocked by the owner of a public key(Bob) and a secret
- Locking transaction has: Hash(secret) + pubkey
- Unlocking transaction should have secret and a signature by Bob

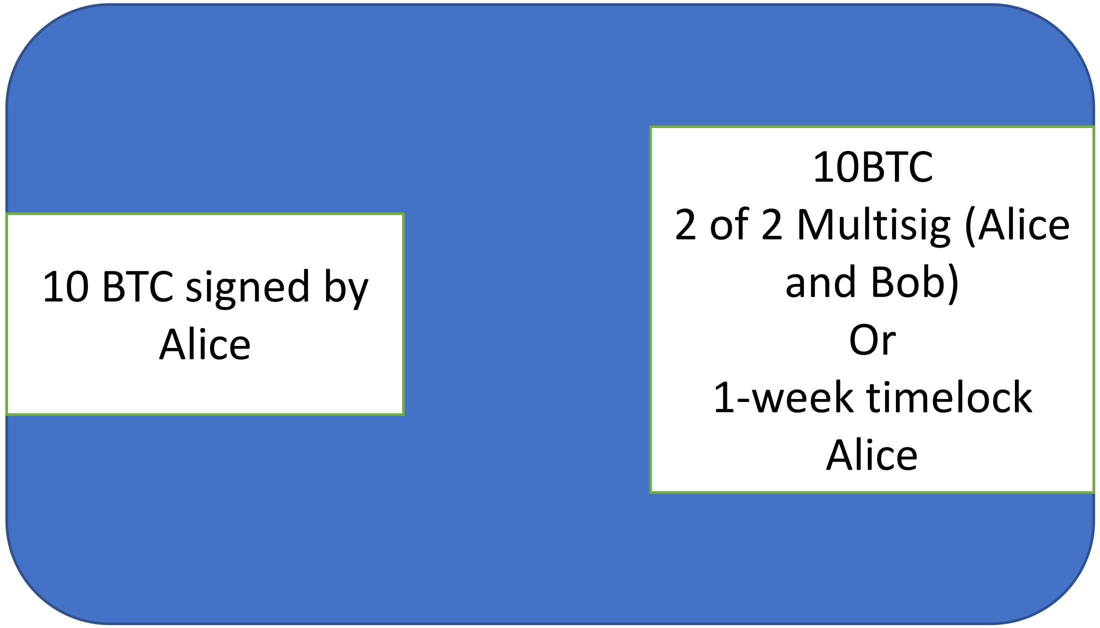
Timelock

- CLTV(CheckLockTimeVerify)
  - Pay to Bob after a certain blockheight
- CSV(Check sequence Verify)
  - Specific blocks after a CSV output is recorded in the blockchain

One-way payment channel

- Funding transaction
  - Creates the channel and is broadcast on the blockchain
- Commitment transactions
  - Intermediate transaction not typically posted on blockchain
- Closing transaction
  - Closes the channel, posted on blockchain
  - Cooperative or non-cooperative

Funding transaction



10 BTC signed by Alice

10BTC
2 of 2 Multisig (Alice and Bob)
Or
1-week timelock
Alice

Posted on blockchain

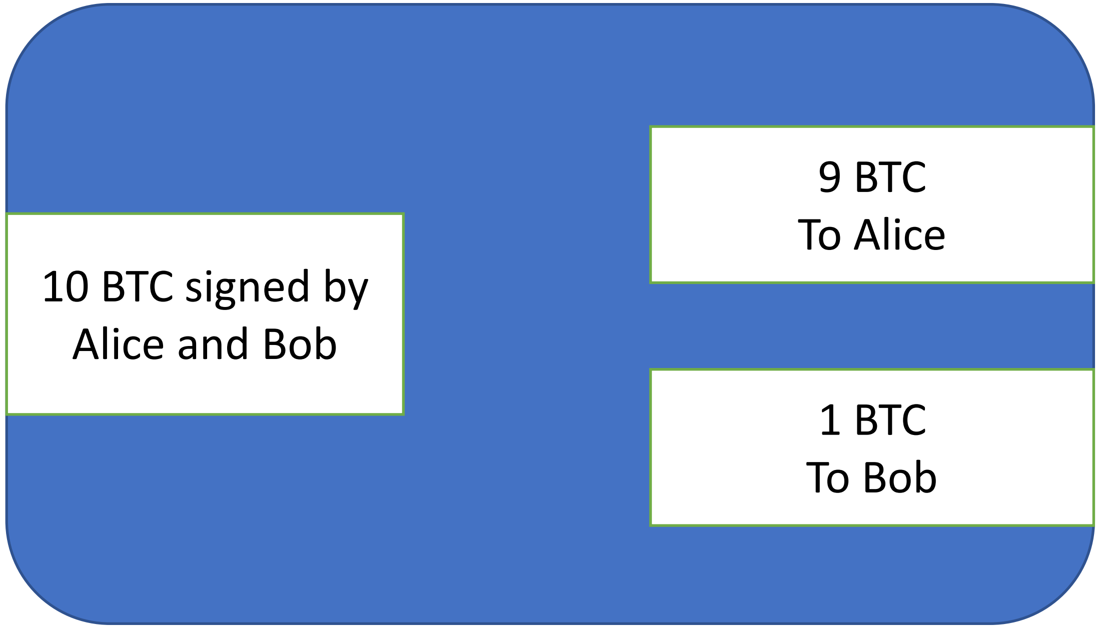
Alice

Bob

10BTC

O BTC

Commitment transactions

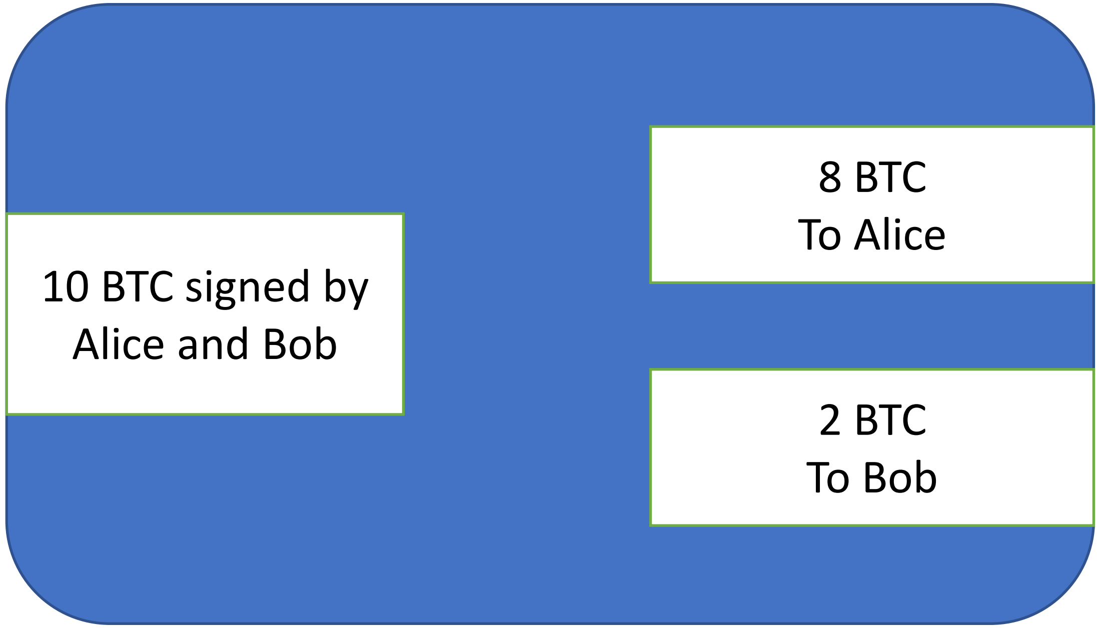


10 BTC signed by Alice and Bob

9 BTC
To Alice

1 BTC
To Bob

Not posted on blockchain
Held by Bob, signed by Alice



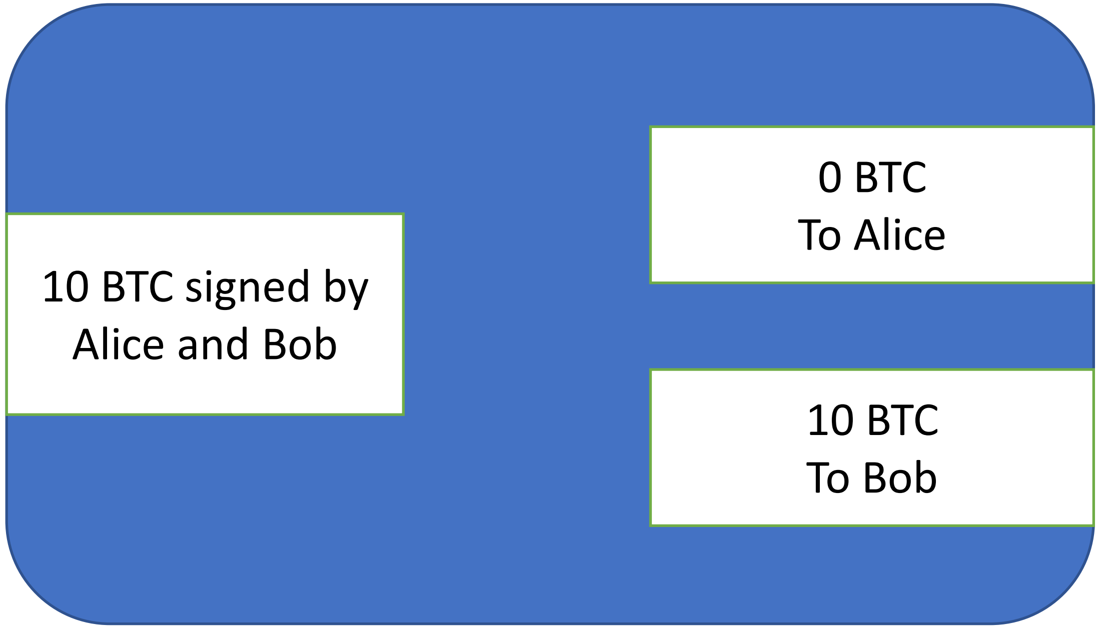
10 BTC signed by Alice and Bob

8 BTC
To Alice

2 BTC
To Bob

Not posted on blockchain
Held by Bob, signed by Alice

Closing transaction - cooperative



10 BTC signed by Alice and Bob

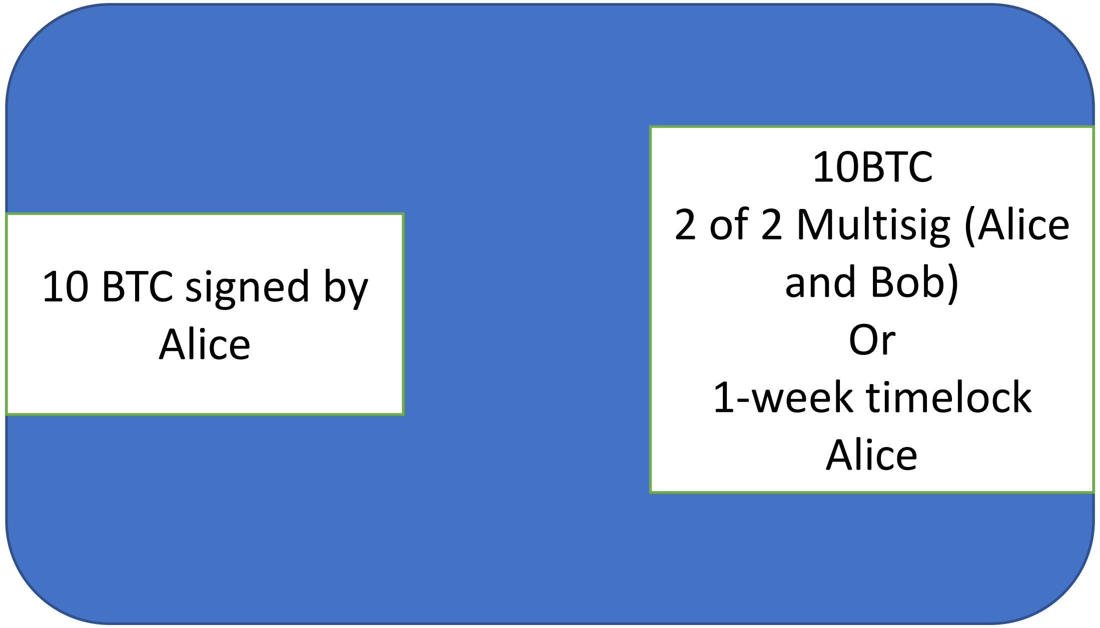
0 BTC To Alice

10 BTC To Bob

Bob posts on blockchain

Closing transaction – Non cooperative

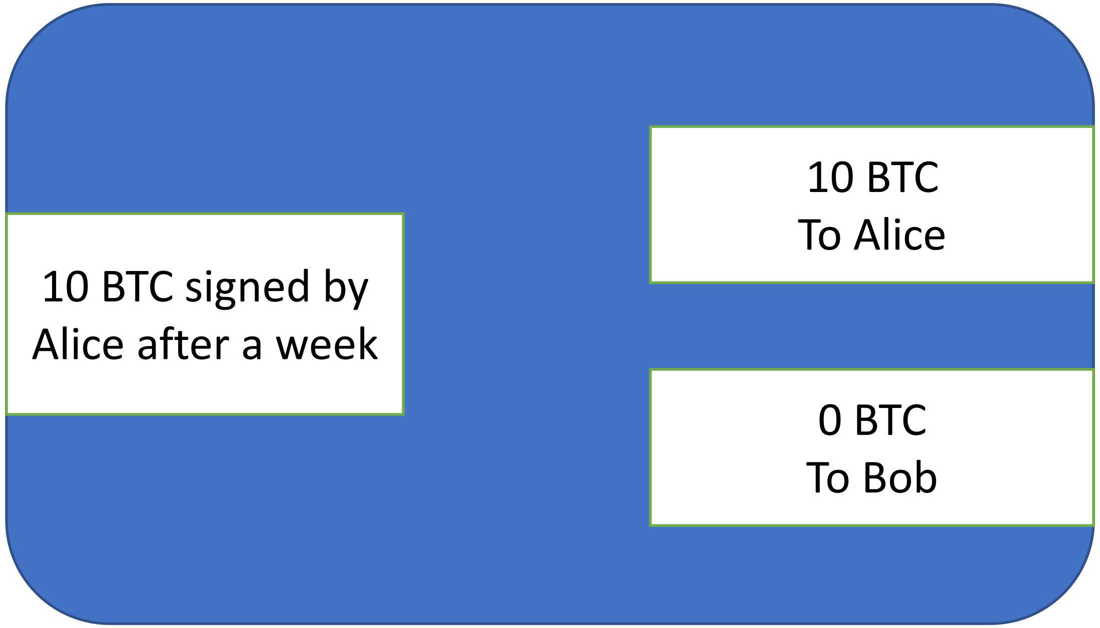
Bob is offline (non cooperative)



10 BTC signed by Alice

10BTC
2 of 2 Multisig (Alice and Bob)
Or
1-week timelock Alice

Funding transaciton



10 BTC signed by Alice after a week

10 BTC
To Alice

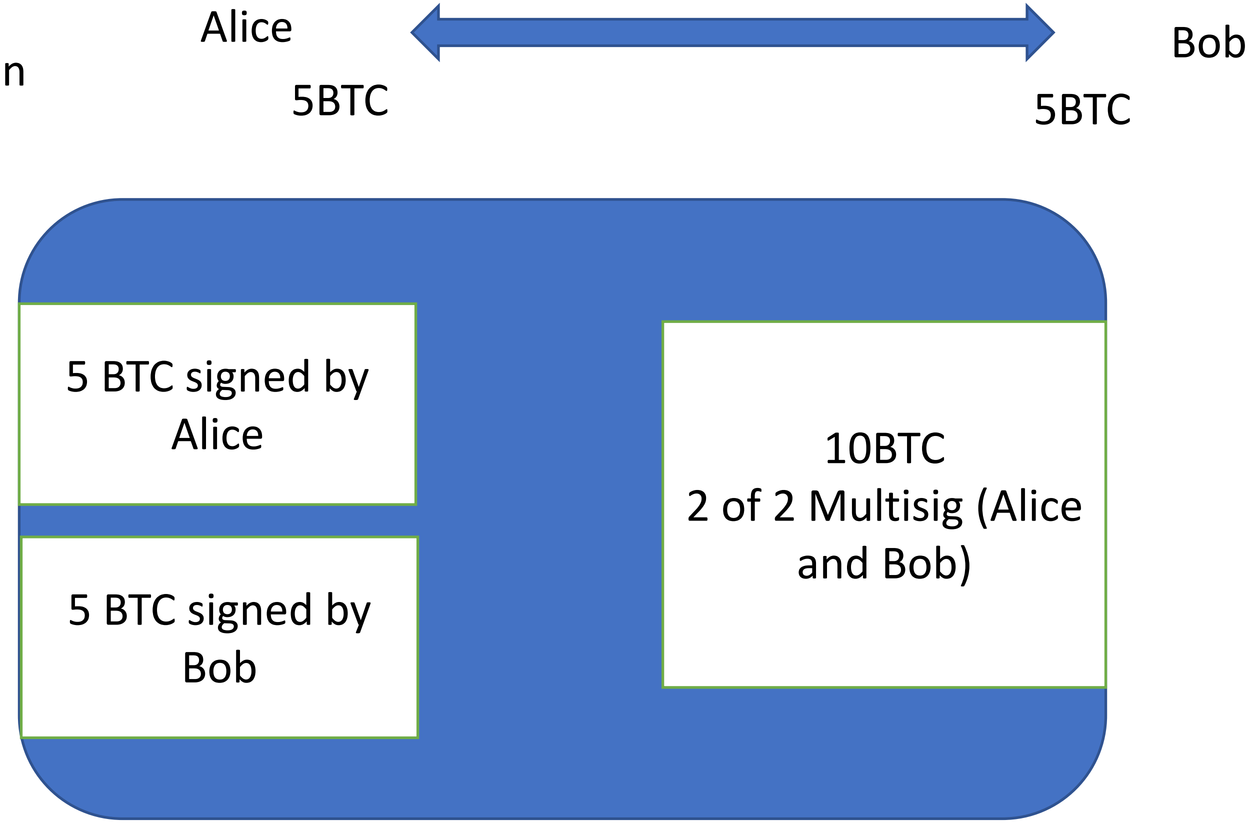
0 BTC
To Bob

Alice posts on blockchain

Bob has to redeem before a week

Two-way payment channel

Opening transaction



Alice

Bob

5BTC

5BTC

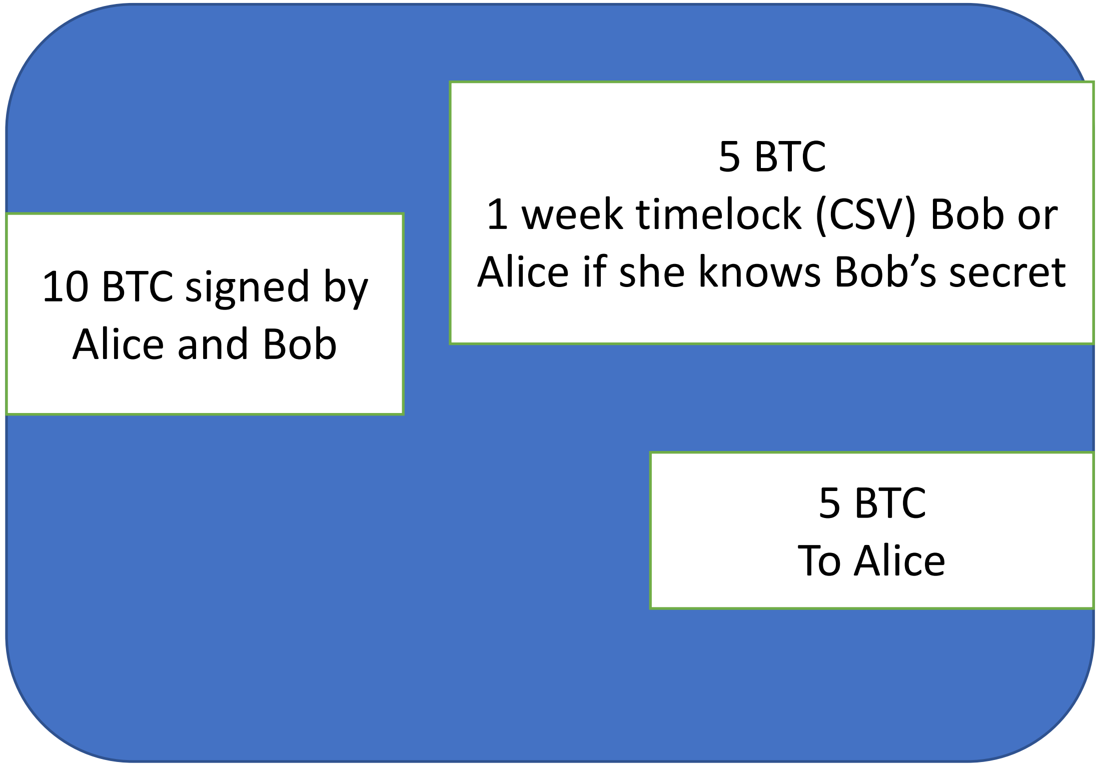
5 BTC signed by Alice

5 BTC signed by Bob

10BTC
2 of 2 Multisig (Alice and Bob)

Create secret and exchange hash(secret)
Not posted on blockchain
Not signed by both yet

Commitment transaction

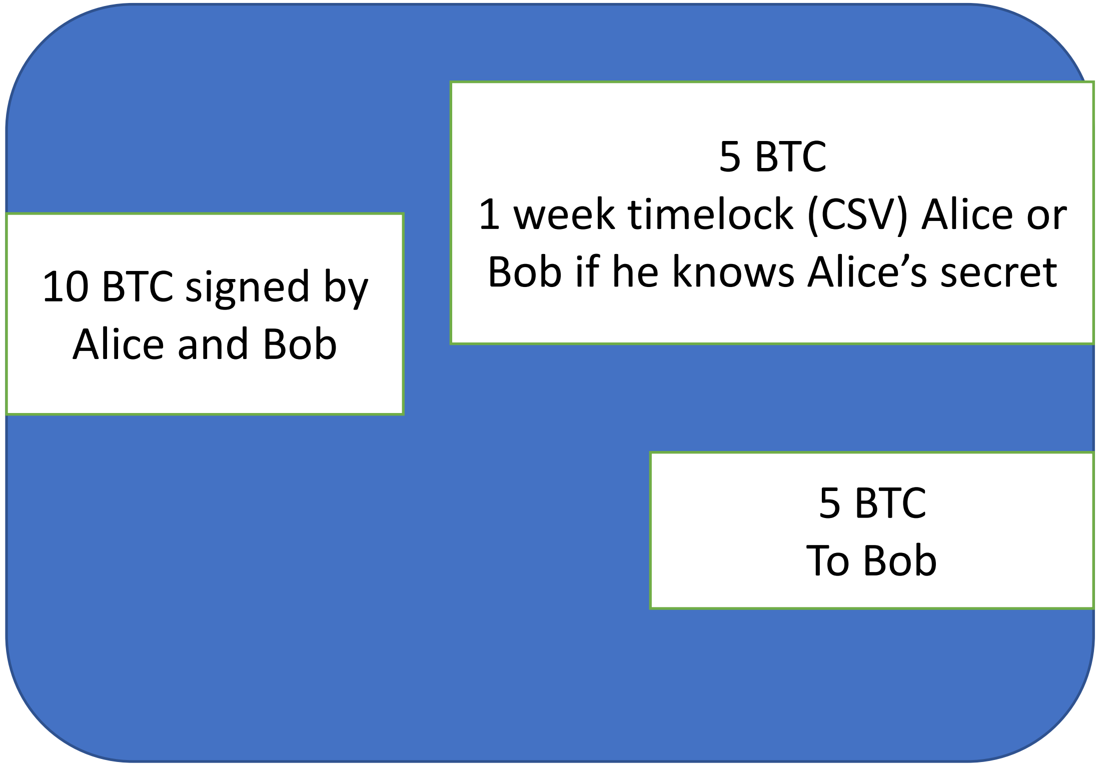


10 BTC signed by Alice and Bob

5 BTC
1 week timelock (CSV) Bob or Alice if she knows Bob’s secret

5 BTC
To Alice

Half signed by Alice, held by Bob



10 BTC signed by Alice and Bob

5 BTC
1 week timelock (CSV) Alice or Bob if he knows Alice’s secret

5 BTC
To Bob

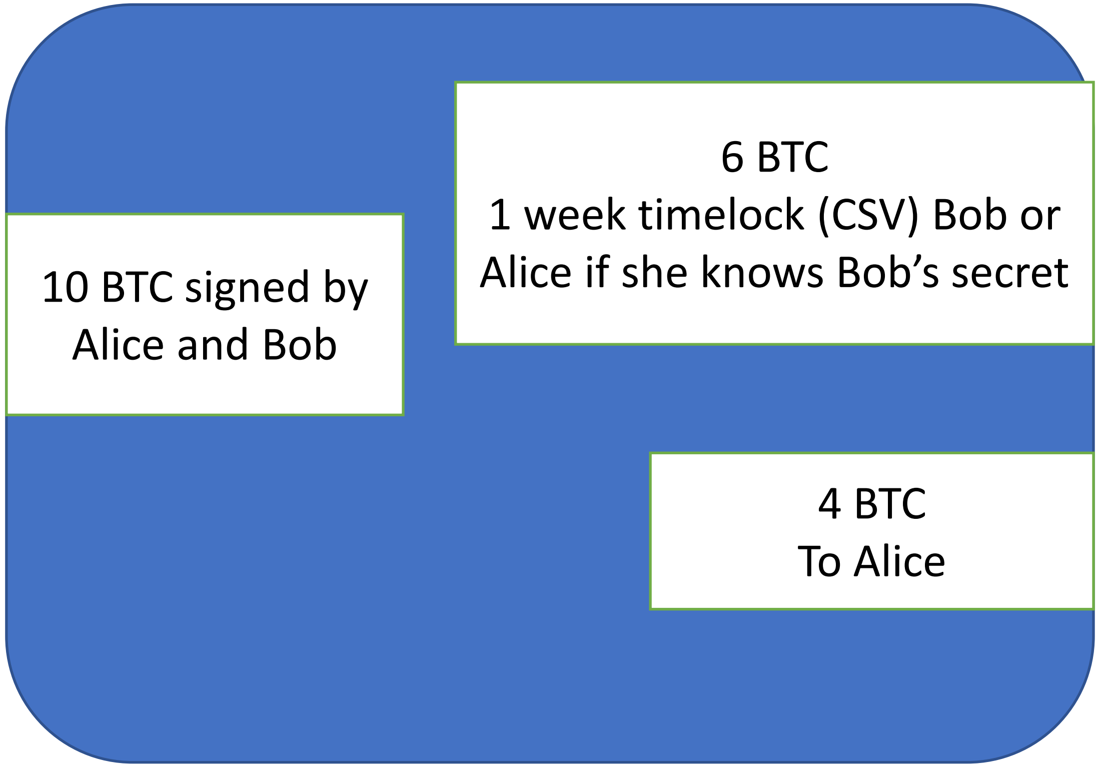
Half signed by Bob, held by Alice

Opening transaction broadcast

- On receiving half-valid commitment transactions, post the opening transaction on blockchain
- There is a way out if the other party does not cooperate
- Neither Alice nor Bob gain anything by posting commitment transactions

Commitment transactions

Let's say Alice wants to send 1 BTC to Bob



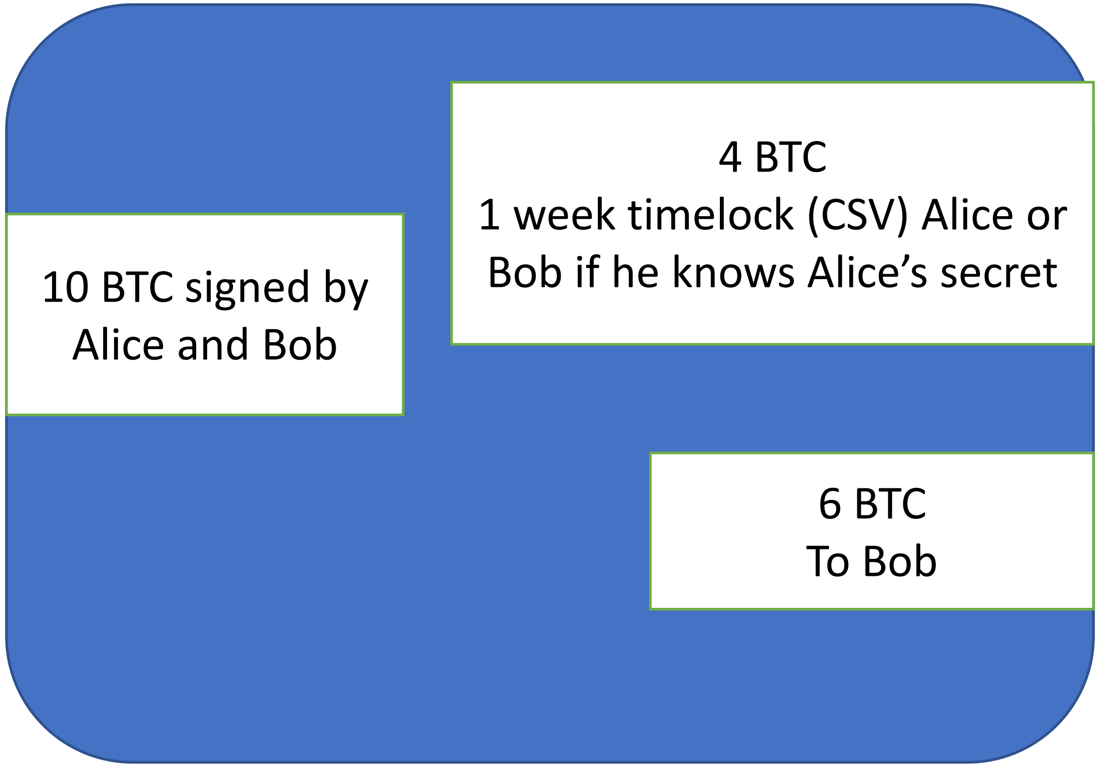
10 BTC signed by Alice and Bob

6 BTC
1 week timelock (CSV) Bob or Alice if she knows Bob's secret

4 BTC
To Alice

Half signed by Alice, held by Bob

Older secrets are exchanged, and new secrets are created (Why?)



10 BTC signed by Alice and Bob

4 BTC
1 week timelock (CSV) Alice or Bob if he knows Alice's secret

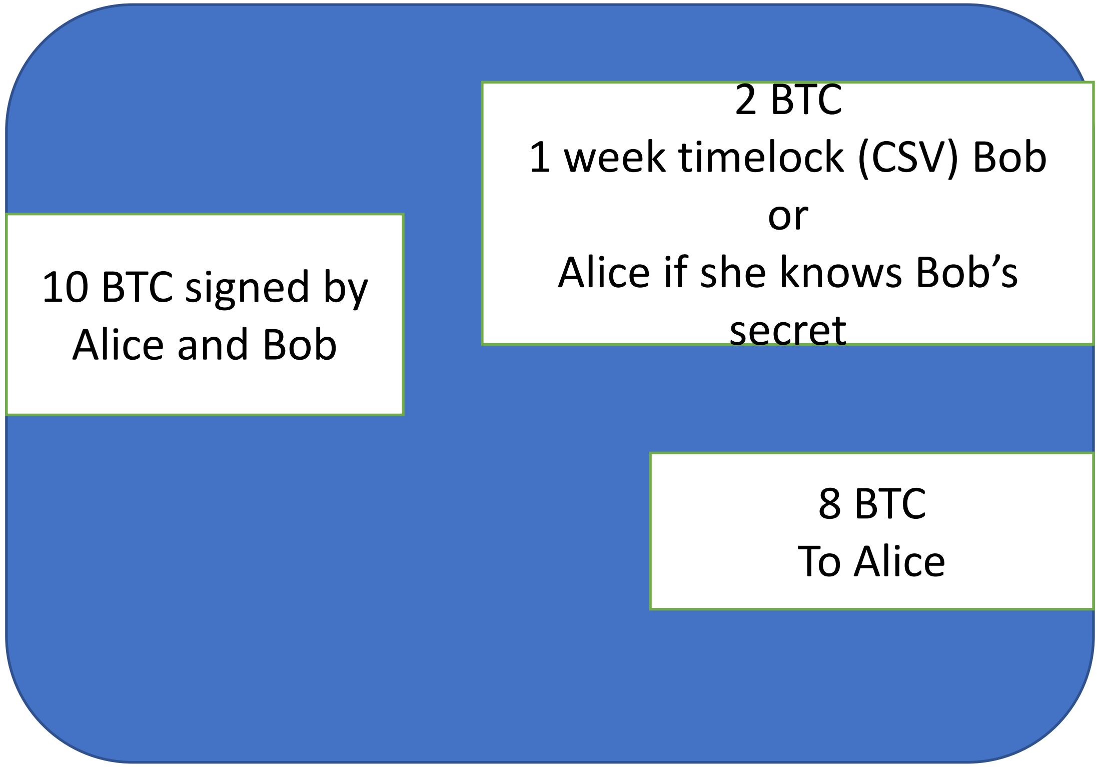
6 BTC
To Bob

Half signed by Bob, held by Alice

Ideally neither sign and broadcast your half of the transaction at all.

Commitment transaction

Let's say Bob wants to send 4 BTC to Alice



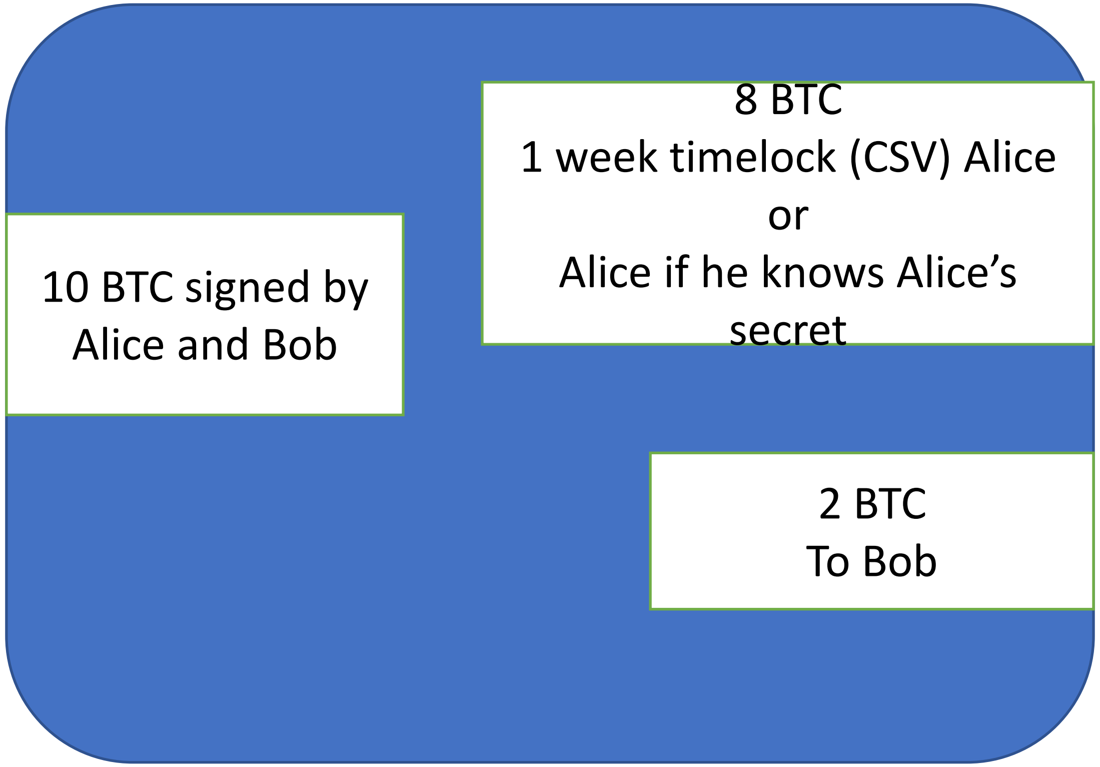
10 BTC signed by Alice and Bob

2 BTC
1 week timelock (CSV) Bob
or
Alice if she knows Bob's secret

8 BTC
To Alice

Half signed by Alice, held by Bob

Older secrets are exchanged, and new secrets are created (Why?)



10 BTC signed by Alice and Bob

8 BTC
1 week timelock (CSV) Alice
or
Alice if he knows Alice's secret

2 BTC
To Bob

Half signed by Bob, held by Alice

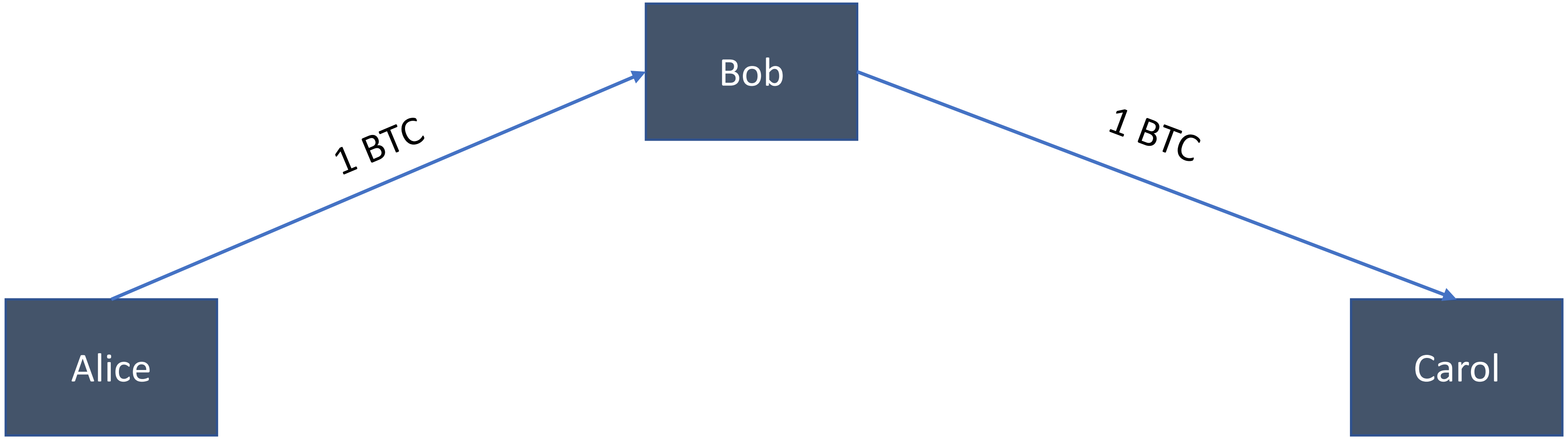
Closing transaction

- Close the channel by revealing *the latest* commitment transaction (non cooperative)
- Cooperative, create a transaction sending the settled balance to each party

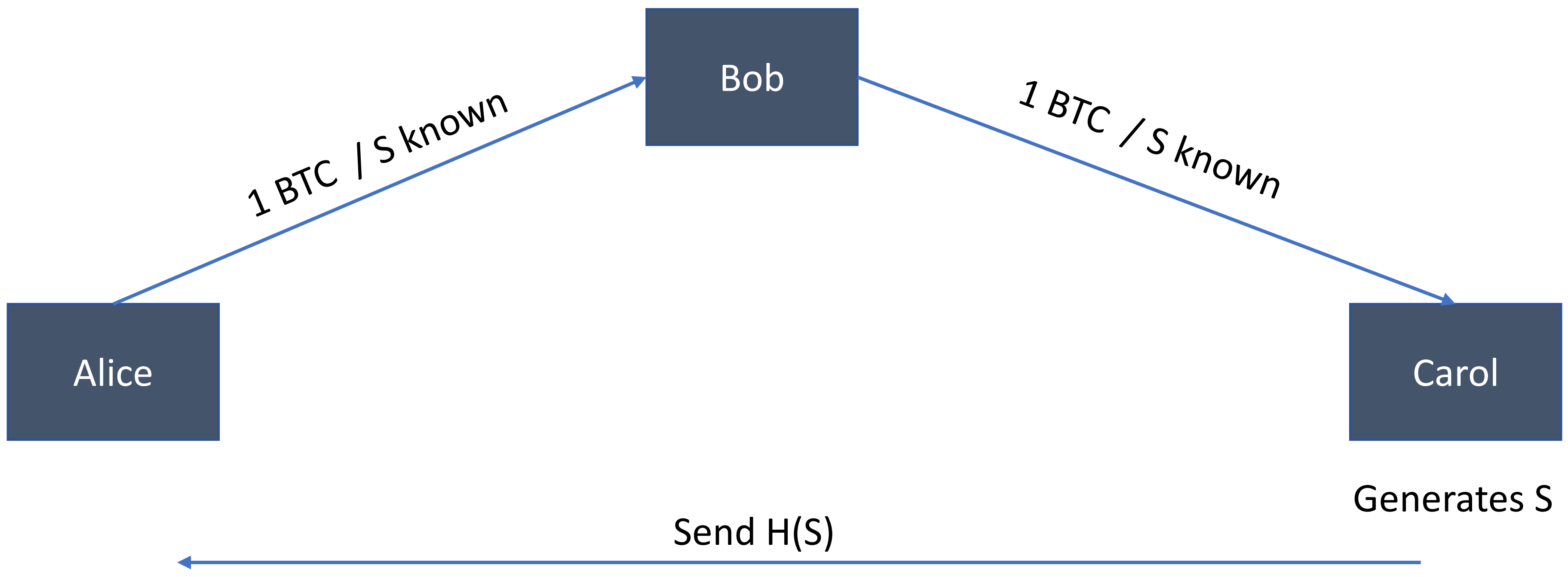
Channel to network: Multi-hop

- Alice wants to pay Carol
- Alice and Bob have a channel
- Bob and Carol have a channel
- Can we do payment over 2 hops?

Trusted multi hop payments - Trust Bob

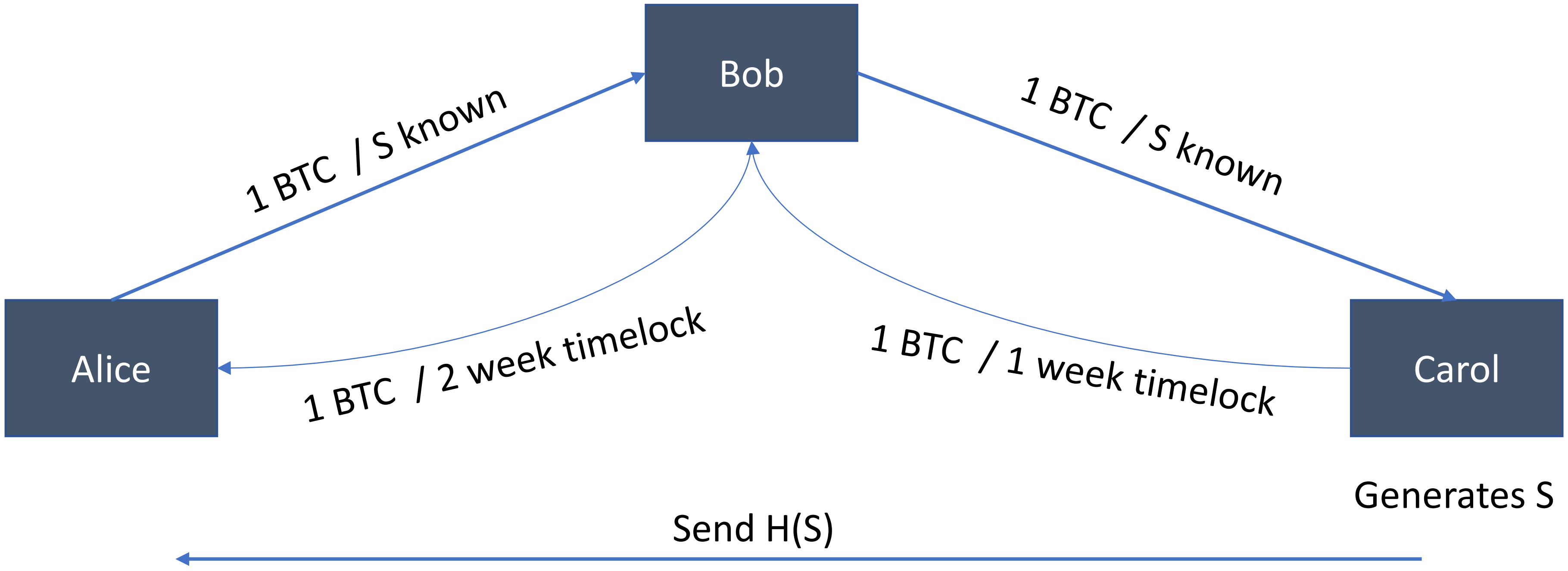


Trustless multi hop payments – Hashlock



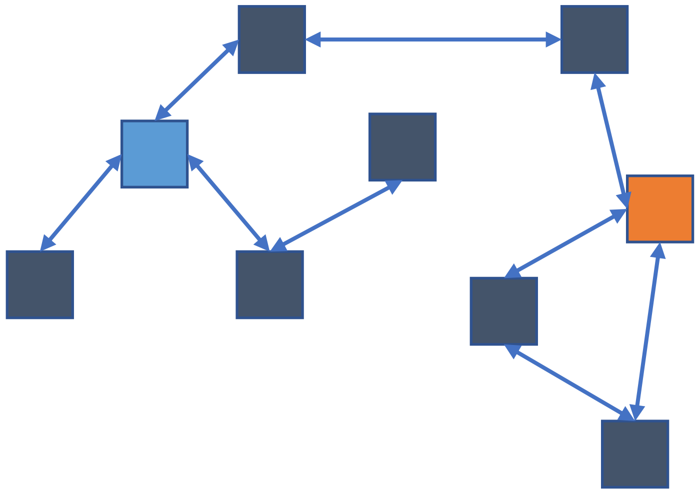
What if Carol does not release S? Alice -> Bob payment is locked

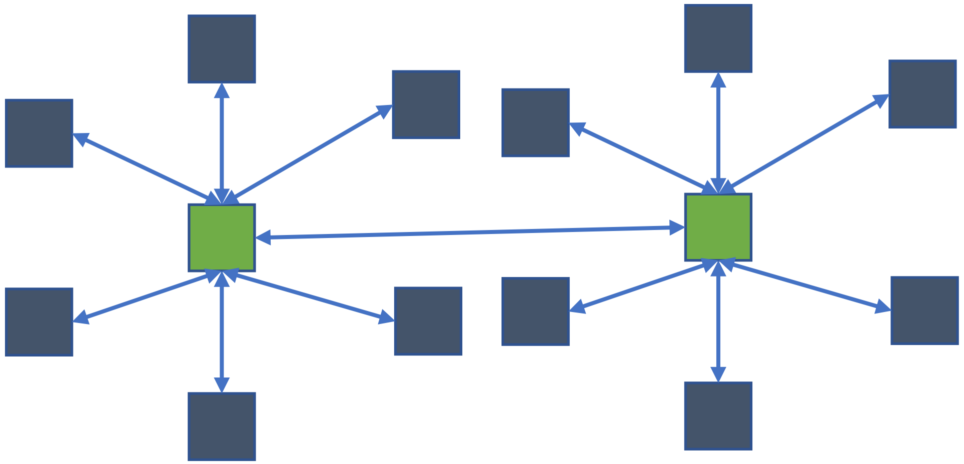
Trustless multi hop payments – Hashlock + Timelock



Payment network

- Multi hop payment channels + Routing
- Lightening network for bitcoin





Lightening network fee structure

- Base fee - 1 Satoshi per forward
- Fee rate – 0.5 Satoshi per million – 0.00005%
- Total fees = Amount*(Fee rate) + Base fee
- Current bitcoin on-chain transaction fee = 6600 Satoshi

Lightening network stats

- Total number of participating nodes ~ 20K
- Total number of channels ~ 85K
- Total capacity ~ USD 100M ~ 5K BTC
- Highest capacity node ~ 650 BTC

Source: 1ml.com, bitcoinvisuals.com/lightning

Pros

- High throughput
- Low latency
- Less fees

Cons

- Routing
  - Traffic based
  - Balance based
  - Centralization
- Nodes need to stay online
  - Watchtowers: Outsourcing
- Capital locked in channels