Bitcoin: Programming the Future of Money

Topics in Computer Science - ITCS 4010/5010, Spring 2025

Dr. Christian Kümmerle

Lecture 26

Lightning Network

The content of this class is based on Chapter 1 and 3 of the book “Mastering the Lightning Network” by Andreas M. Antonopoulos, Olaoluwa Osuntokun and René Pickhardt, available at https://github.com/lnbook/lnbook.

UNIVERSITY OF NORTH CAROLINA CHARLOTTE

Proof-of-Stake

RECAP: PROOF-OF-WORK VS. PROOF-OF-STAKE

Advantages of PoS:

- Less energy consumption
- Lower latency possible / better finality guarantees
- Recovery from 51% attacks / punishment of bad actors within protocol possible

Disadvantages of PoS (vs. PoW):

- Significant additional complexity -> Possibility of bugs, lack of transparency
- Additional attack vectors (e.g., due to possibility of “costless simulation”, cf. Long-Range Attack)
- Less established proof record/ history (Bitcoin’s PoW works since 2009)
- Stronger trust assumptions
- (Possibly problematic) economic implications from how consensus works / protocol changes are implemented.

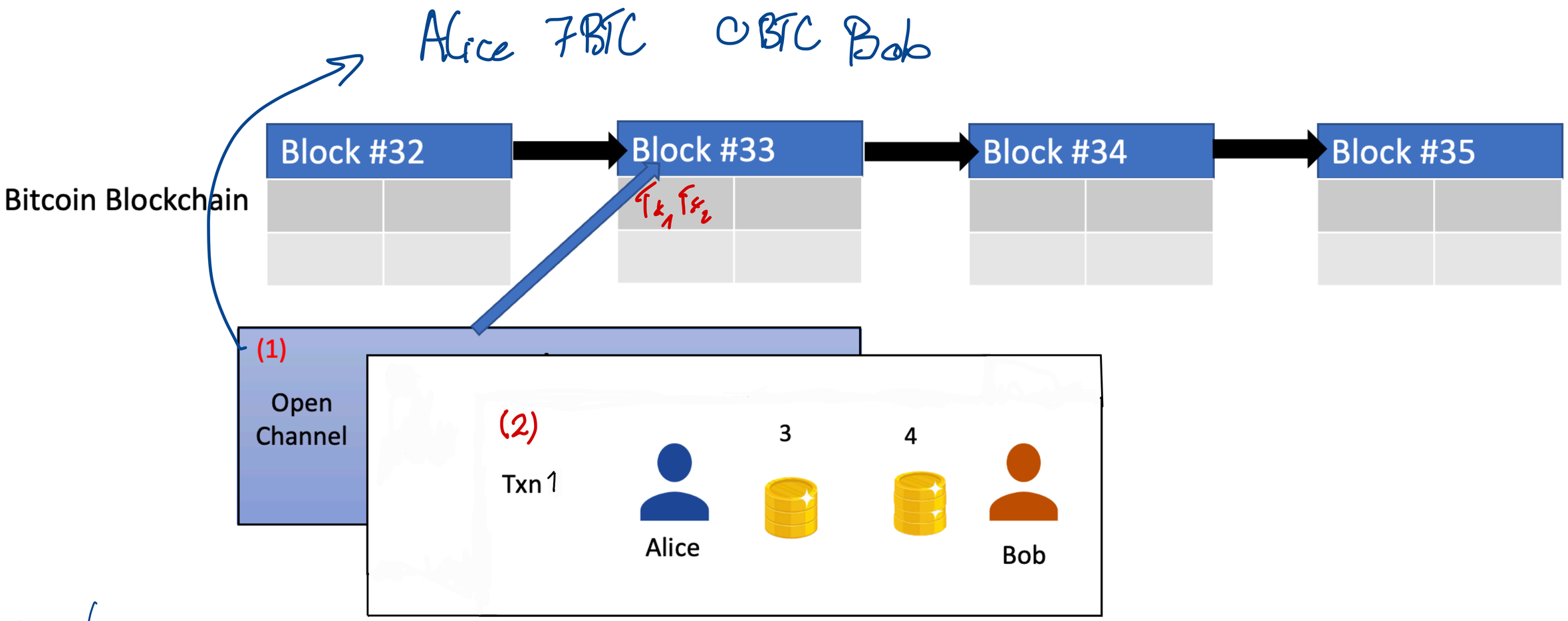
The Lightning Network

MAJOR LIMITATIONS OF THE BITCOIN PROTOCOL

Limitations within the Bitcoin protocol that challenge the ability of bitcoin (the monetary unit) to “global money”:

- **Scalability: Can the network ever support the global demand for transactions?**
  3000-4000 Tx’s per block, one block per 10 minutes (on average):
  Bitcoin Tx/sec: 3500*6 / (60*60) ≈ 6 Tx/sec
- **Latency: Each transaction needs to ≈10 minutes (or 20, 30, …) to be reliably settled.**
- **Privacy: All transactions are visible to everyone.**

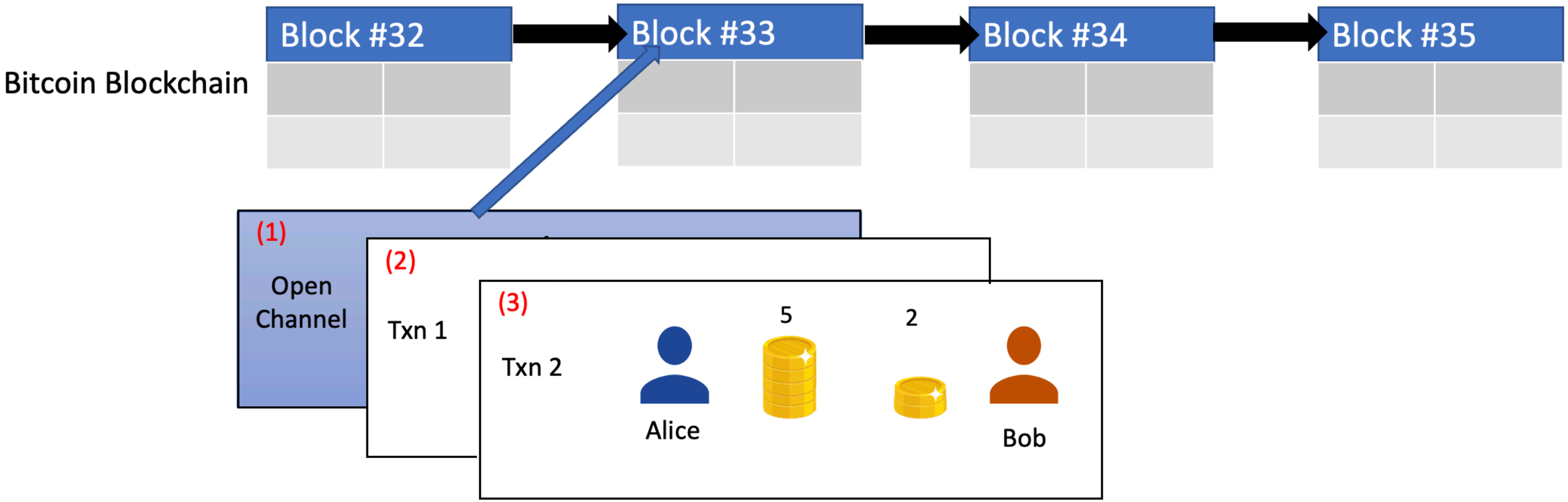
PAYMENT CHANNELS IN THE LIGHTNING NETWORK



Example:

- Alice creates a so-called "payment channel" with Bob through a "funding transaction" in block #33, in which Alice allocates 7 BTC to this channel.
- Alice sends 4 BTC of these 7 BTC to Bob, the remaining balance of hers is 3 BTC.
- Note: If Bob can obtain a cryptographic proof from Alice that this "change of balances" has occured, this might not need to be included as a blockchain transaction.

PAYMENT CHANNELS IN THE LIGHTNING NETWORK



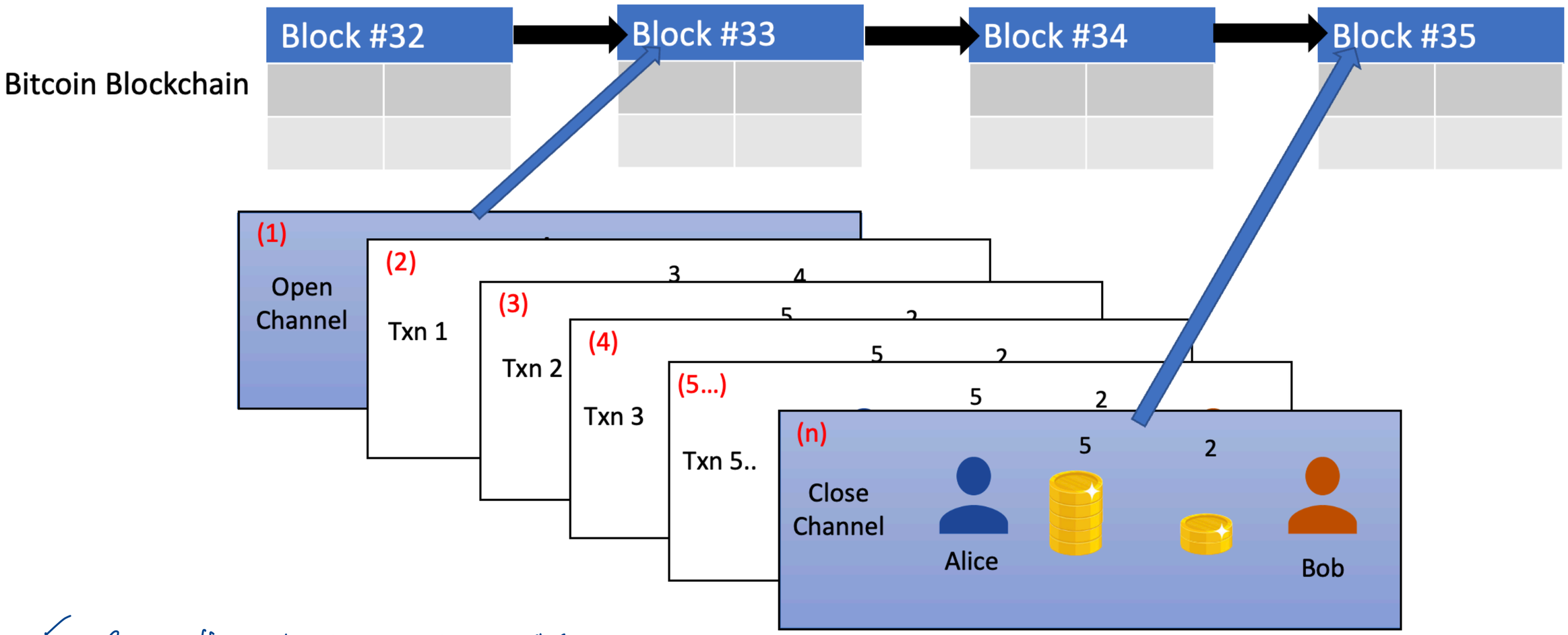
- Bob can also send coins to Alice within the payment channel, for example 2 BTC.
- If he does that, the channel balance is updated from

Alice	Bob
3 BTC	4 BTC

to

Alice	Bob
5 BTC	2 BTC

PAYMENT CHANNELS IN THE LIGHTNING NETWORK



▷ Finally, the balance between Alice and Bob can be settled through a "closing transaction" which pays the corresponding amounts to address held by Alice and Bob, respectively (here: 5 BTC & 2 BTC).

Brief Overview:

- Proposed in 2016 by Joseph Poon and Tadge Drjya
- 2018-2019: First mature implementations

- A peer-to-peer “second layer” network designed to address Bitcoin’s scalability challenges, facilitating **cost-effective** and **instantaneous** transactions
- Based on “bidirectional payment channels”
- Ability of users to unilaterally withdraw funds
- Supported by major Bitcoin / cryptocurrency exchanges
- It is NOT another alternative cryptocurrency

FEATURES OF THE LIGHTNING NETWORK

- Users can send/receive BTC payments instantaneously and w/ low cost
- Payments with LN are finally settled
- Privacy feature:
  - Channel opening/closing transactions are public
  - Payments within LN are transmitted between nodes which only have very partial information about the payments
  - Unlike for on-chain transactions, LN payment information does need to be stored forever.

↳ Using Tor-like onion routing

USE CASES FOR THE LIGHTNING NETWORK

- Consumers: Small retail purchases (cup of coffee)
- Merchants: Ability to reduce proprietary transaction fees of networks like Visa/Mastercard
- Software Services Business: Can receive smaller, reccurring, pay-per-use payments, cross-border
- Online Micropayments between individuals:
  - → Tipping in social media: Twitter/X, Nostr (decentralized social media protocol)
  - → Content Creators

FEATURES AND PROPERTIES OF PAYMENT CHANNELS IN LN

Communication requirements:

- Each participant of a Lightning Network payment channel needs to be online, i.e., reachable over the internet
- Transaction speed not bounded by block time/frequency, but by internet speed.

Public knowledge about payment channel: (List not complete...)

- Committed channel capacity (in example above: 7 BTC)
- Fees charged by channel operators to route third-party payments

Communicated through gossip in LN

Private knowledge —"— (only know to both channel nodes):

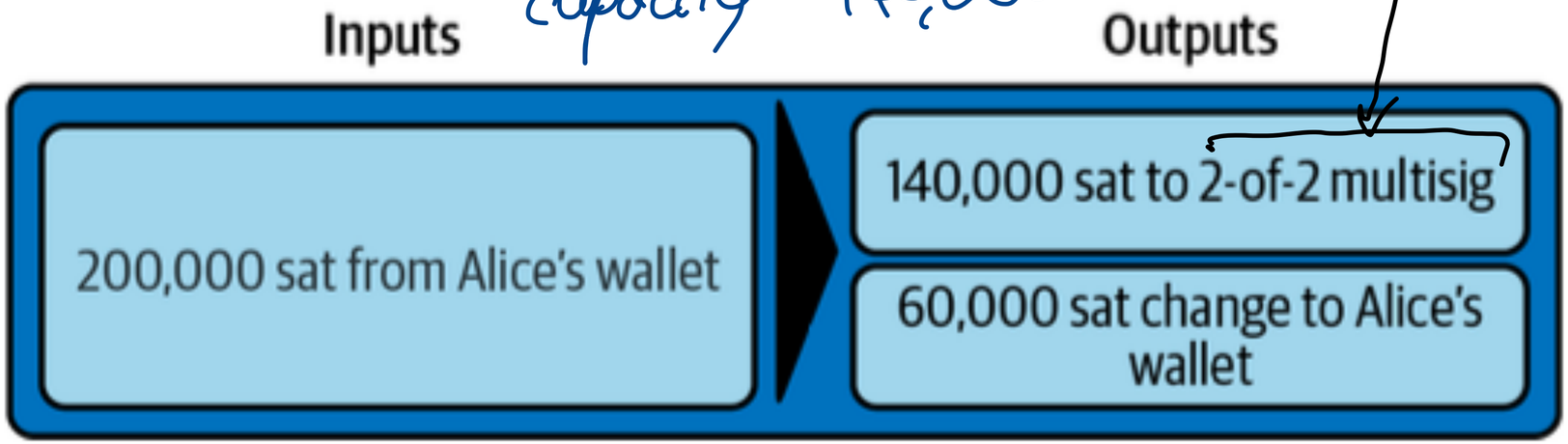
- Current balance of both channel nodes (*)
- But: Either node can use cryptographic proof of changes in balances to resolve dispute with node partner on Bitcoin blockchain without trust in honesty of node partner.

(*) Final balance after closing of channel will be public.

FUNDING AND COMMITMENT TRANSACTIONS

Alice uses UTXO of 200,000 sats to "fund" a payment channel of capacity 140,000 sats

with, e.g., Bob

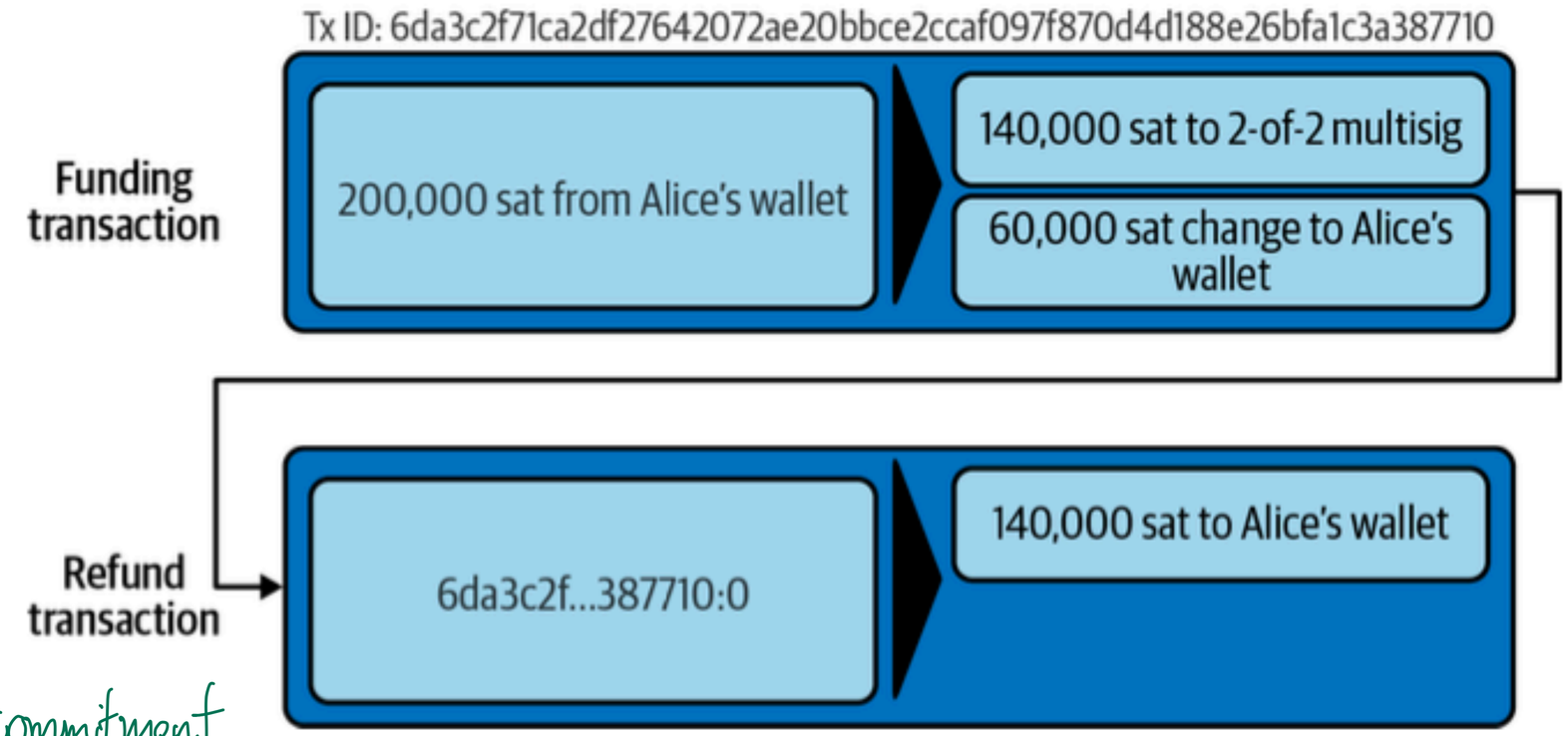


corresponds to a payment channel opening

FUNDING AND COMMITMENT TRANSACTIONS

broadcast to the Bitcoin network

signed, but not yet broadcast



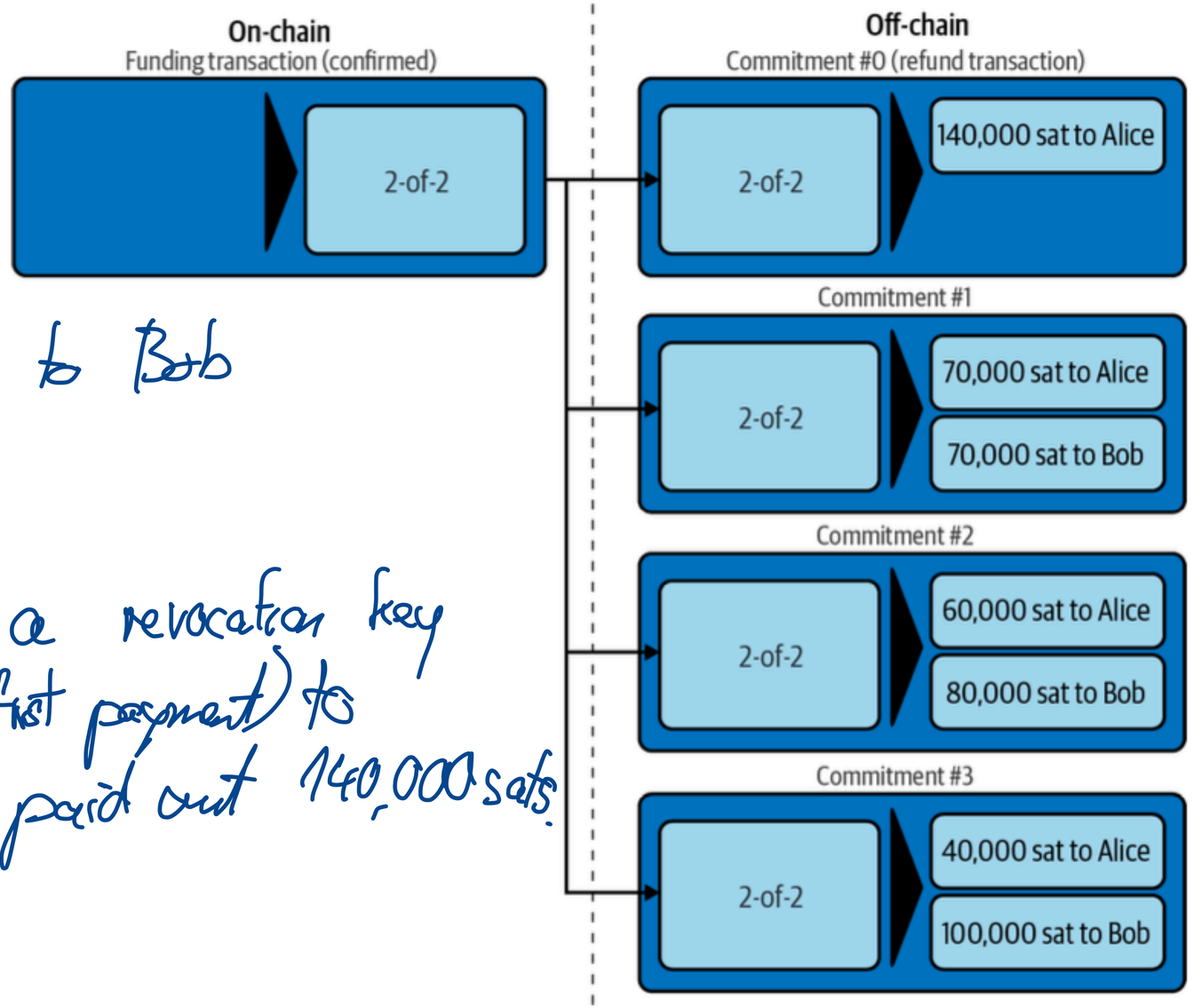
"commitment transaction"

Alice will broadcast this transaction only if no payments have occured within the payment channel, and if Alice does want to use the funds for something else.

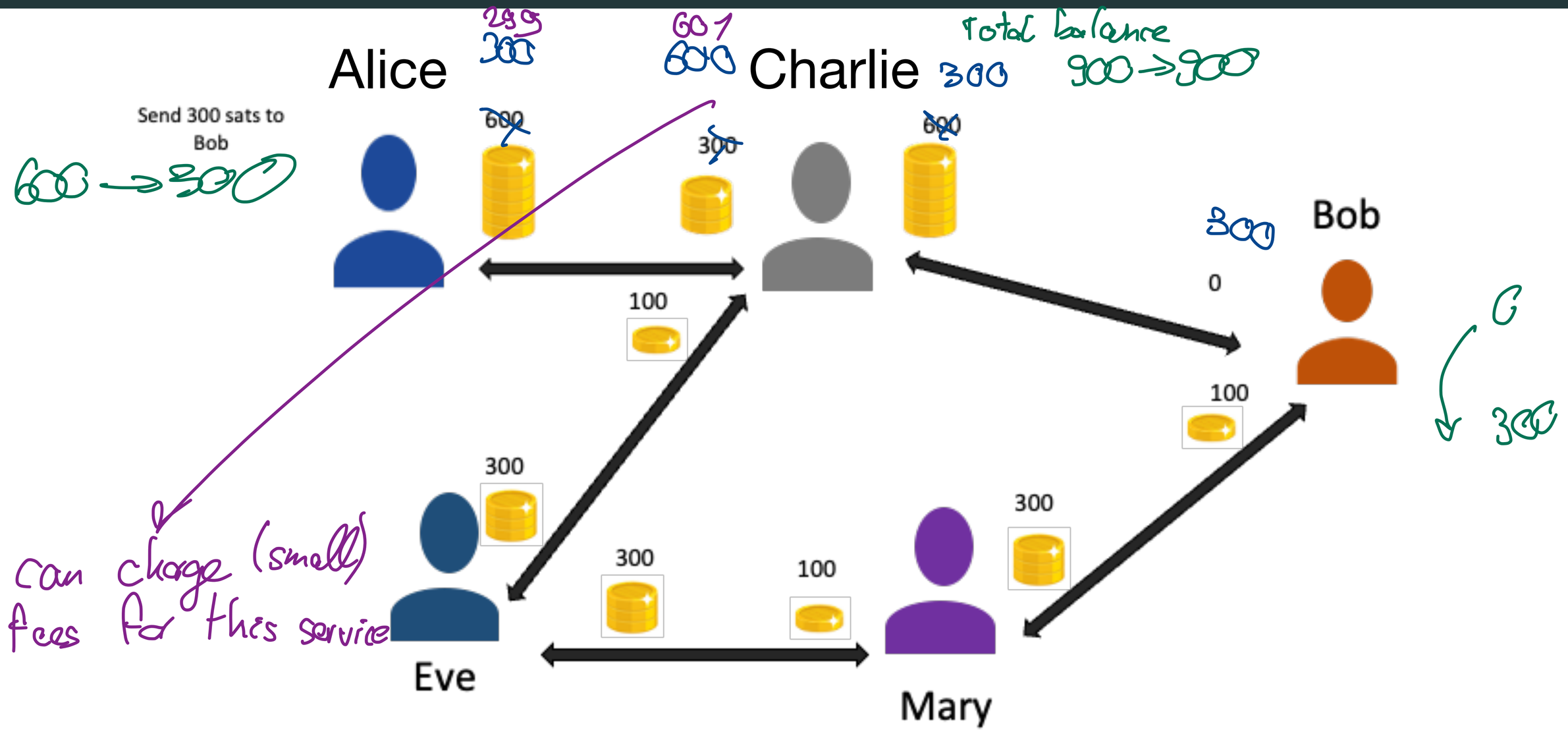
FUNDING AND COMMITMENT TRANSACTIONS

Q: What if Alice just publishes (*) after having paid 70,000 sats to Bob within channel?

↳ Bob is able to use a revocation key (shared by Alice to Bob after first payment) to prevent Alice from being paid out 140,000 sats.



ROUTING IN THE LIGHTNING NETWORK

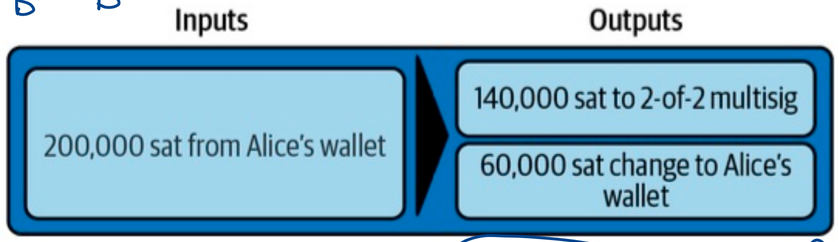


THE PAYMENT CHANNEL PROTOCOL: BASICS

The protocol needs to make sure that at no step, Alice needs to trust Bob or Bob needs to trust Alice to be honest.

Steps to create payment channel (PC) between Alice and Bob of capacity 140k sats (funded by Alice):

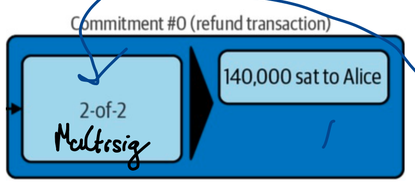
1. Alice creates private/public key pair (e_A, P_A) and informs Bob that she wants create PC.
2. Bob creates private/public key pair (e_B, P_B) and agrees w/ request. Sends P_B to Alice.
3. Alice creates funding transaction (e.g.,



) with locking script of 2-of-2 multisig:

$2 \langle P_A \rangle \langle P_B \rangle 2$ CHECKMULTISIG

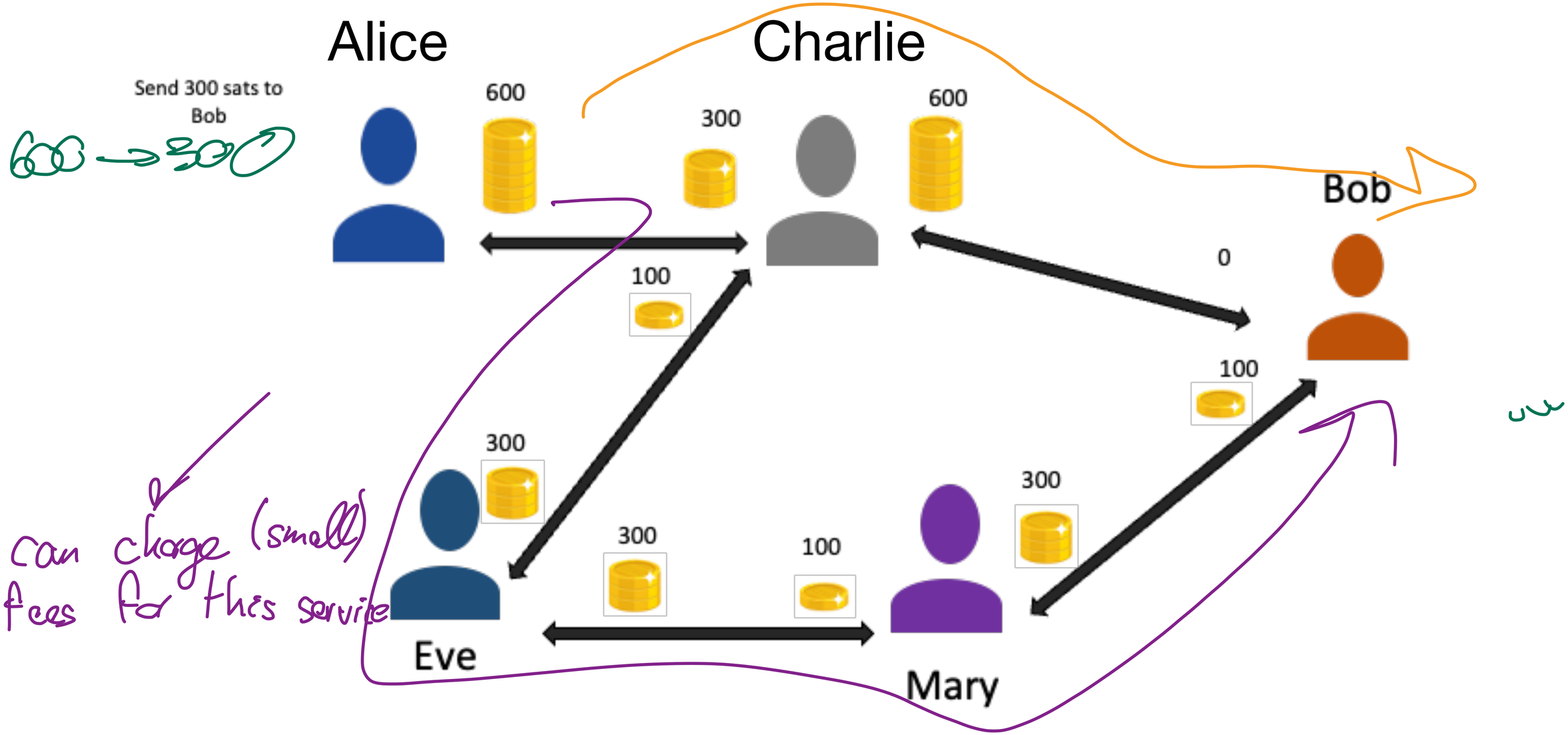
4. Alice provides her signature (corresponding to P_A) of commitment transaction



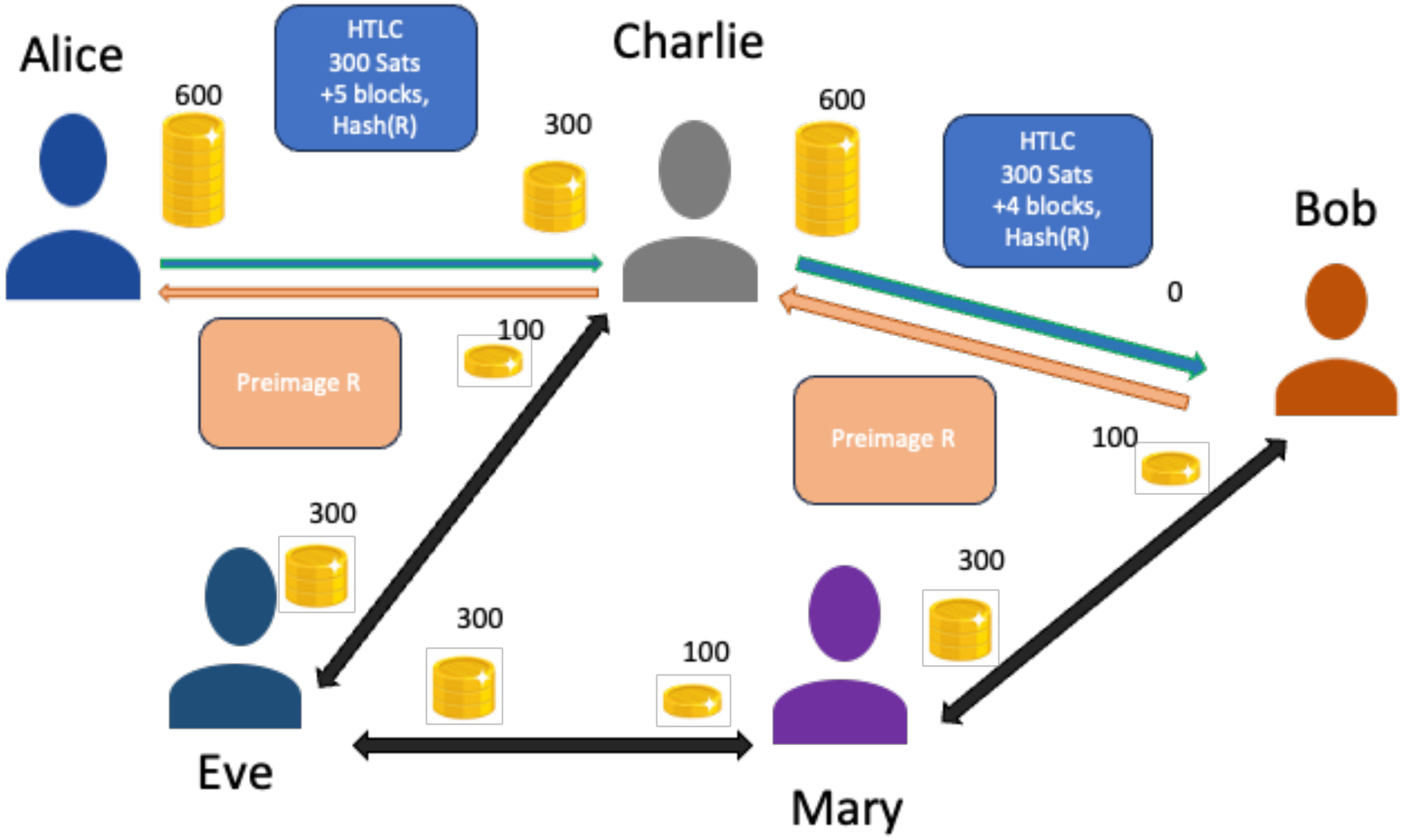
sends signature to Bob.
5. Bob sends his signature of the commitment Tx (corresponding to P_B) to Alice.
6. Alice publishes funding Tx to mempool.

Note: ▷ After 6., both Alice and Bob have ability to publish commitment Tx, but they do not yet publish it.

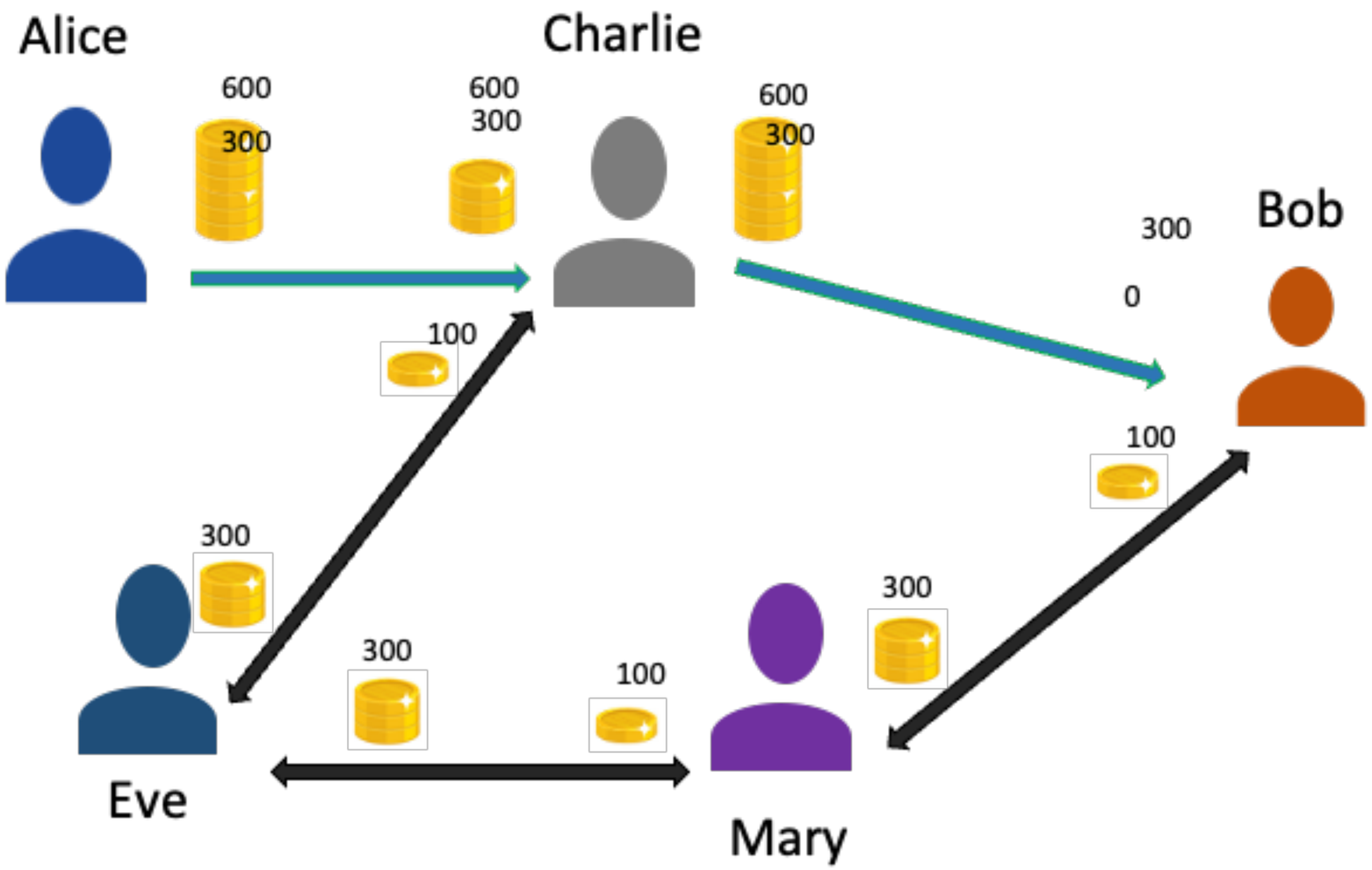
ROUTING IN THE LIGHTNING NETWORK



ROUTING IN THE LIGHTNING NETWORK

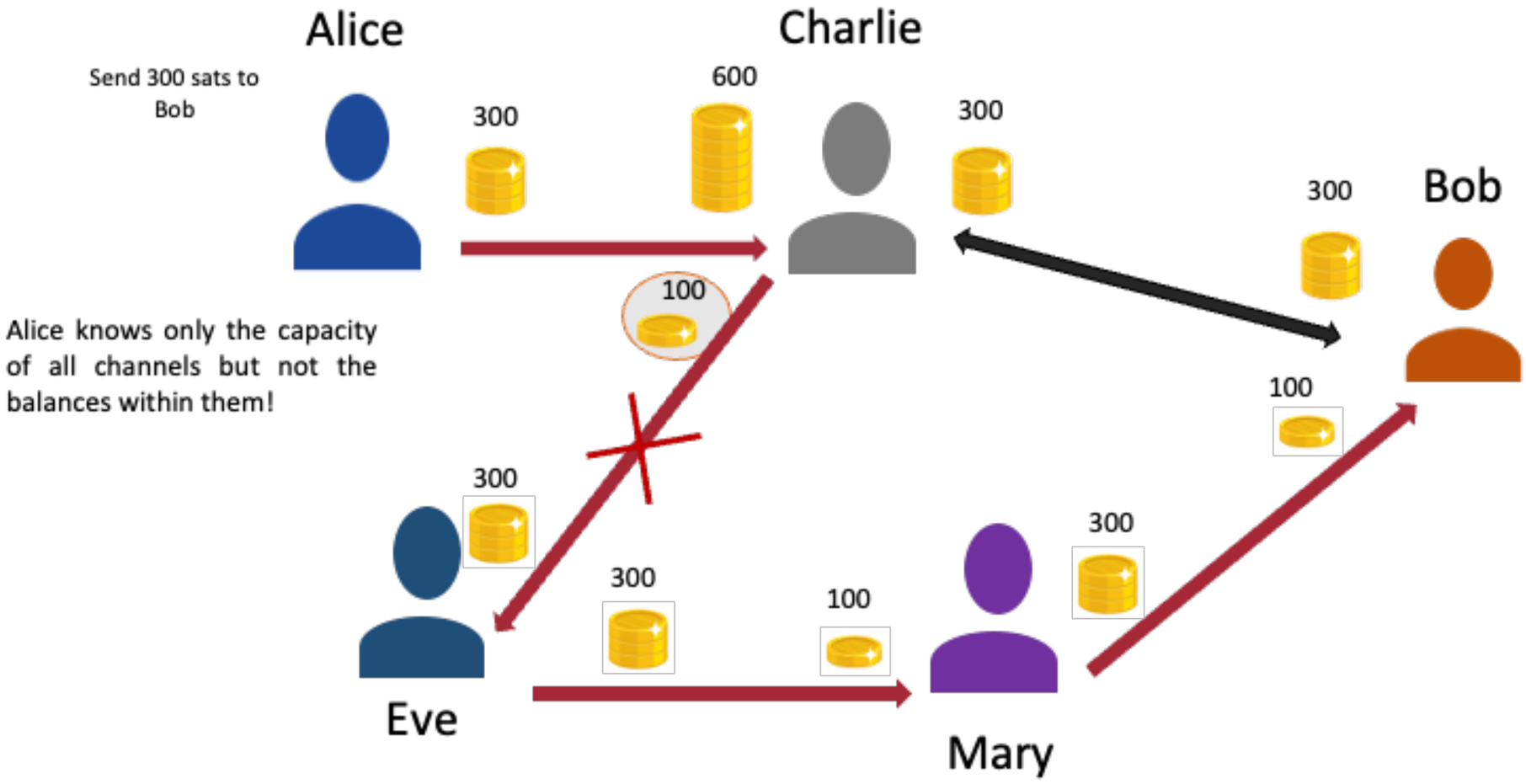


ROUTING IN THE LIGHTNING NETWORK



▷ In reality of the LN, Charlie receives small "reward" for routing Alice's payment to Bob "routing fee". ⟶ Economic incentive

ROUTING IN THE LIGHTNING NETWORK



THREE DIFFERENT WAYS TO CLOSE A CHANNEL

Scenario: Alice's balance is 100,000 sats and Bob's balance is 40,000 sats.

- **Mutual Close:**
  Both Alice and Bob are online and agree to close the channel
  -> Create and both sign transaction (similar to most current commitment transaction) with appropriate on-chain fees, both receive their respective balances.
- **Force Close:**
  E.g.: Alice is not reachable. Therefore, Bob publishes most recent commitment transaction, both receive their balances.
- **Protocol Breach & Punishment Transaction:**
  E.g.: Bob publishes outdated commitment Tx which pays him 80,000 sats and Alice only 60,000 sats. Bob has a timelock of 2016 blocks (two weeks) on his 80,000 sats. If Alice sees this transaction in a block, she can "sweep" the 80,000 sats back from Bob to her in a separate transaction.

Required Readings about the Lightning Network:

- Andreas M. Antonopoulos, Olaoluwa Osuntokun, and René Pickhardt, "Mastering the Lightning Network", Textbook, O'Reilly Media, Inc., 2021, available at https://github.com/lnbook/lnbook,
  - Part I, Understanding the Lightning Network, Chapter 1, "Introduction", pp. 1-14.
  - Part I, Understanding the Lightning Network, Chapter 3, "How the Lightning Network Works", pp. 39-72.