



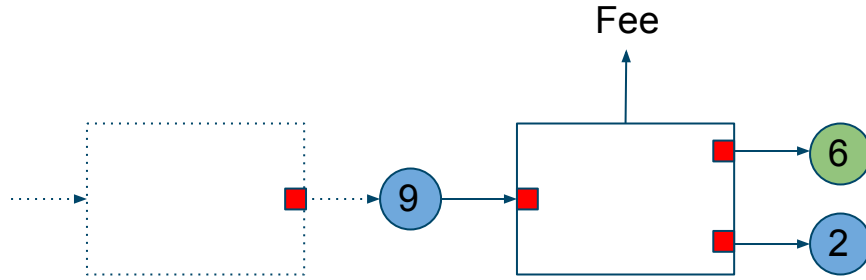
Blockstream

History of the Lightning Network

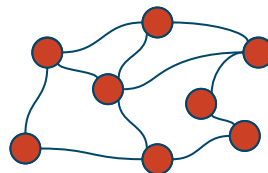
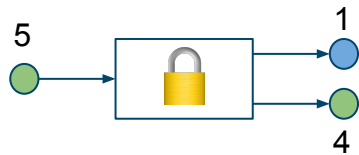
Dr. Christian Decker

Core Tech Engineer

Bitcoin Transactions



Let's Buy a Coffee



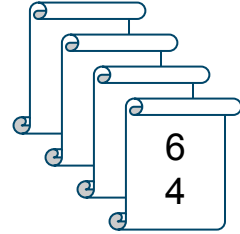
1

What are off-chain protocols?

Off-Chain Protocols



User	Balance
Alice	5 6
Bob	4 5
Carol	5



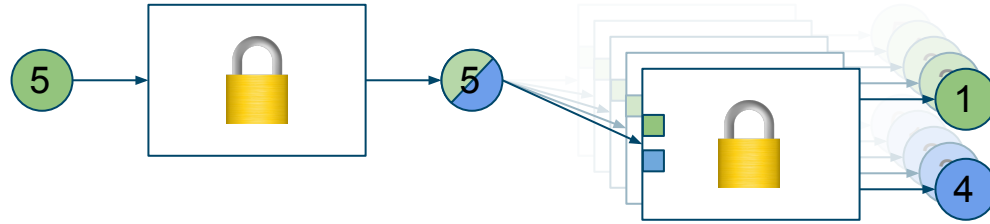
2

Update Mechanisms

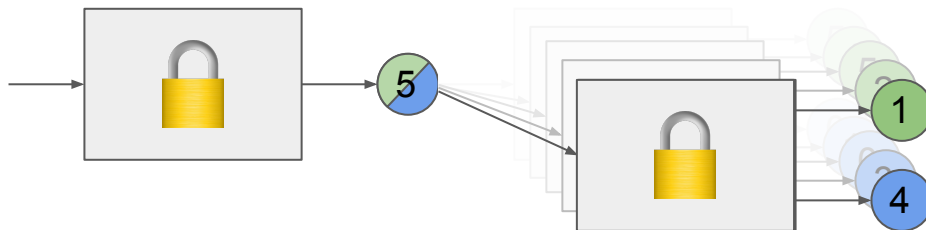
nSequence Transaction Update (Satoshi 2009)

```
bool fNewer = false;
unsigned int nLowest = UINT_MAX;
for (int i = 0; i < vin.size(); i++)
{
    if (vin[i].nSequence != old.vin[i].nSequence)
    {
        if (vin[i].nSequence <= nLowest)
        {
            fNewer = false;
            nLowest = vin[i].nSequence;
        }
        if (old.vin[i].nSequence < nLowest)
        {
            fNewer = true;
            nLowest = old.vin[i].nSequence;
        }
    }
}
```

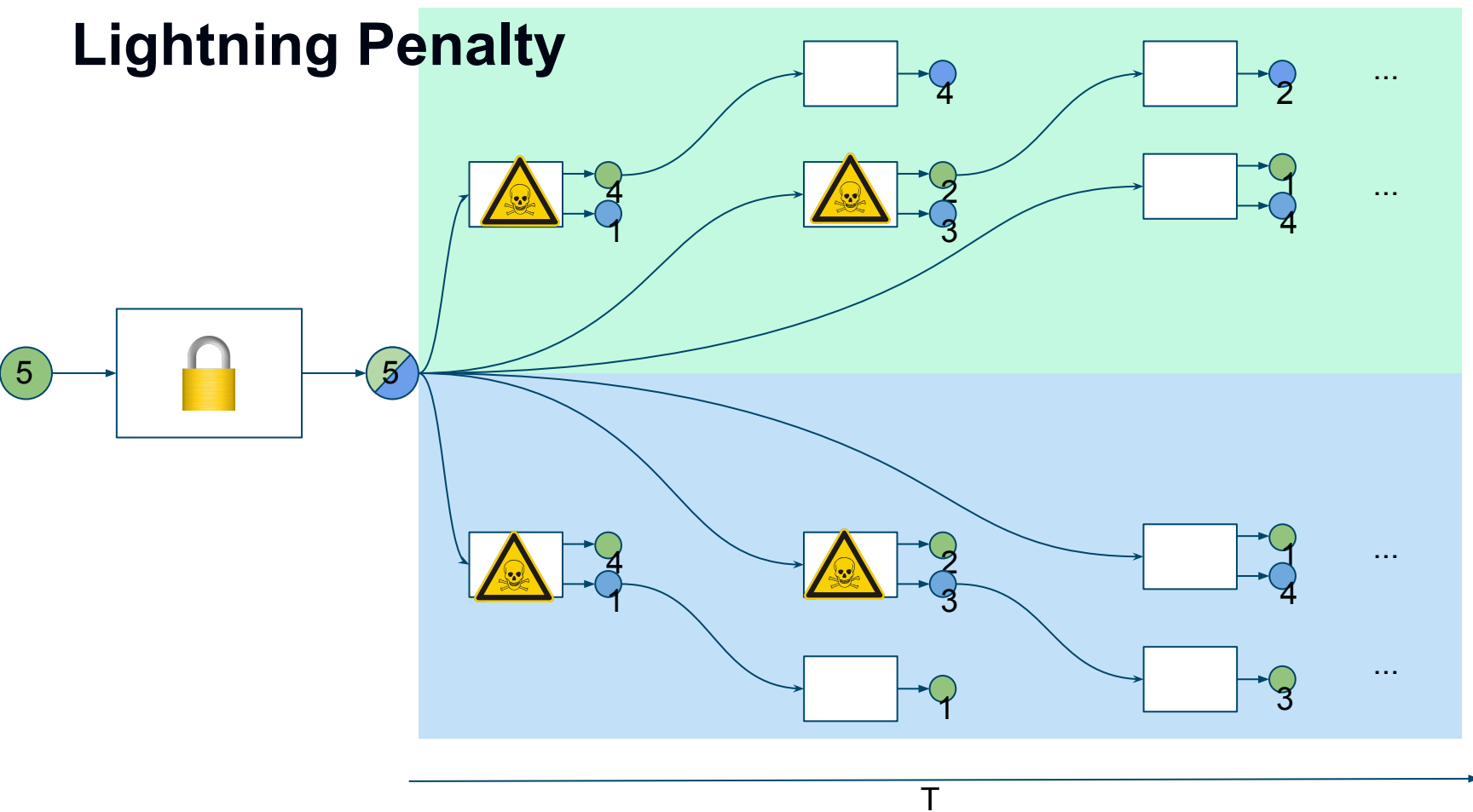
Simple Micropayment Channel (Spilman 2013)



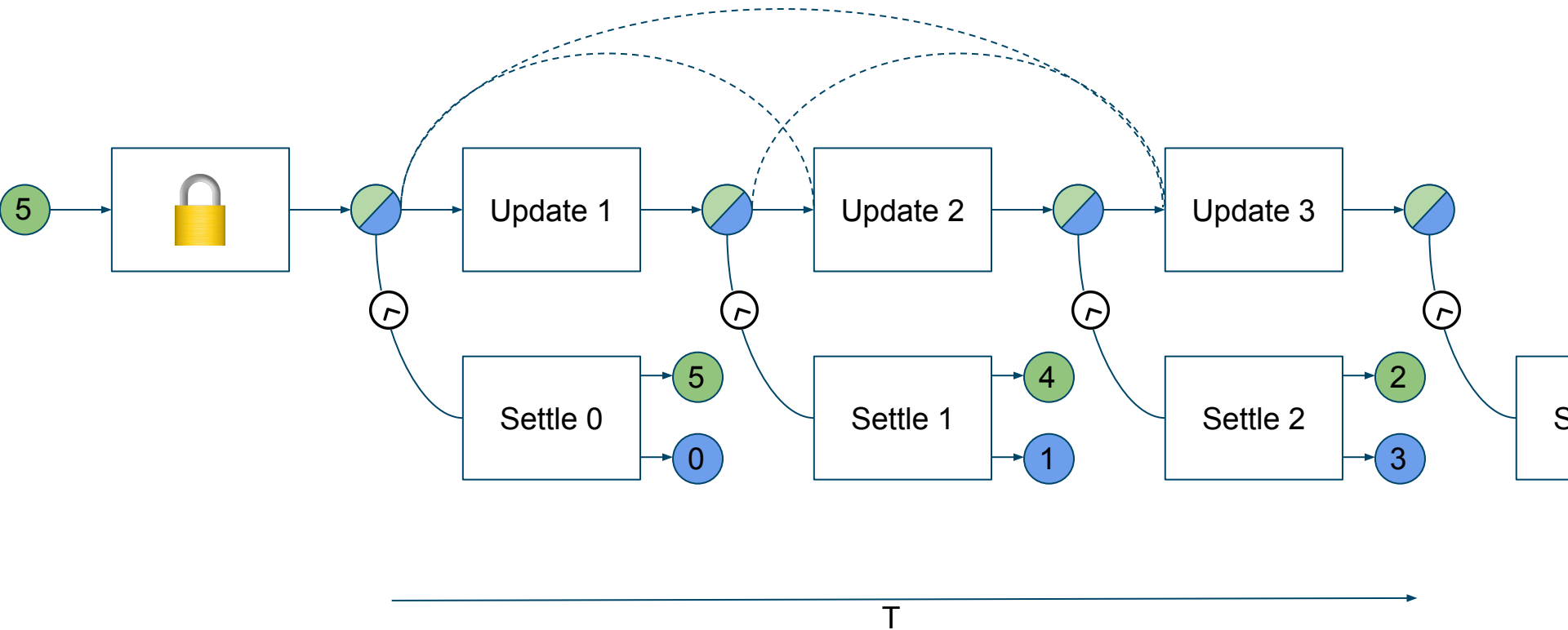
Duplex Micropayment Channels



Lightning Penalty



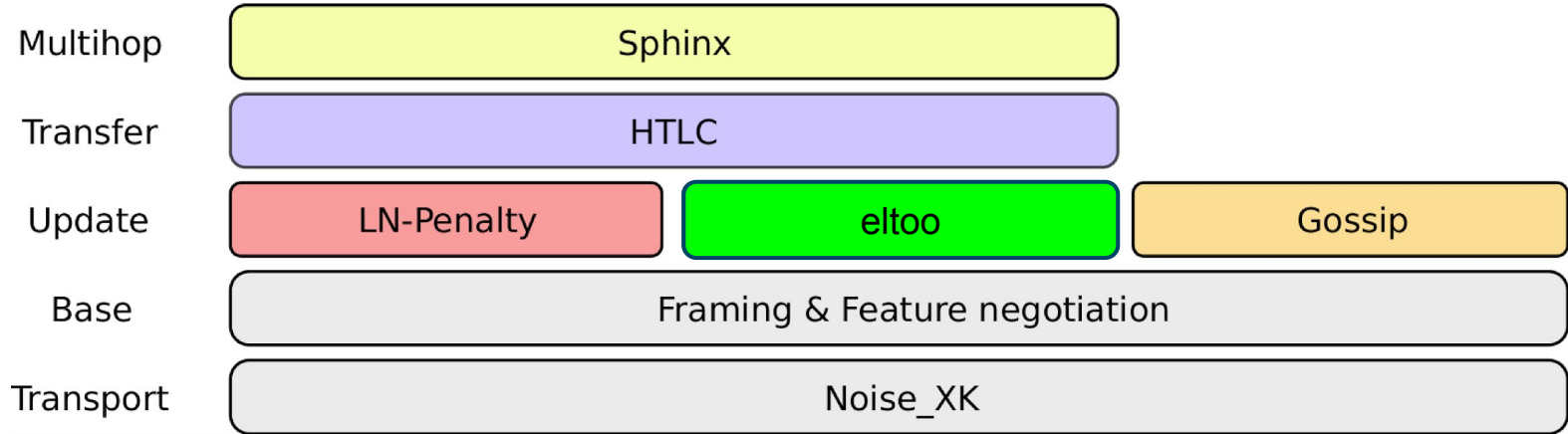
eltoo Update Mechanism



3

Layers all the way down...

The Lightning Stack



Secure Multihop Payments

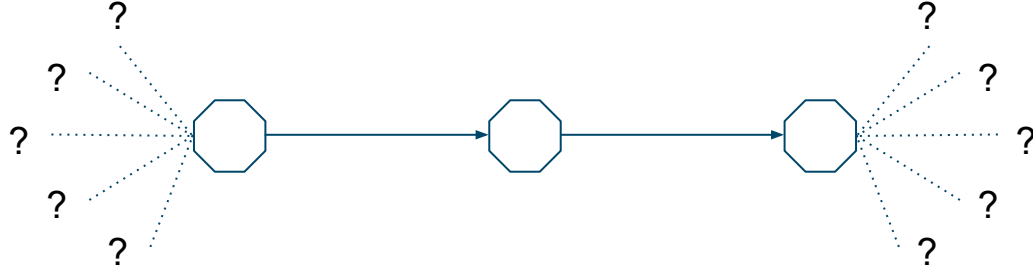


Hashed Timelock Contract (HTLC)

5

```
OP_IF
  OP_HASH160 <secrethash> OP_EQUALVERIFY
  <green-pubkey>
OP_ELSE
  36 OP_CSV
  <blue-pubkey>
OP_ENDIF
OP_CHECKSIG
```

Onion Routing





Blockstream

Thanks!
Questions?