Blockstream

History of the Lightning Network

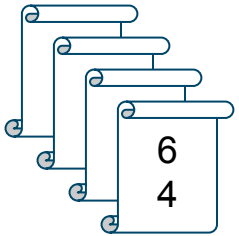
Dr. Christian Decker

Core Tech Engineer

1 What are off-chain protocols?

Off-Chain Protocols

User	Balance
Alice	~~5~~ 6
Bob	~~5~~ 4
Carol	5

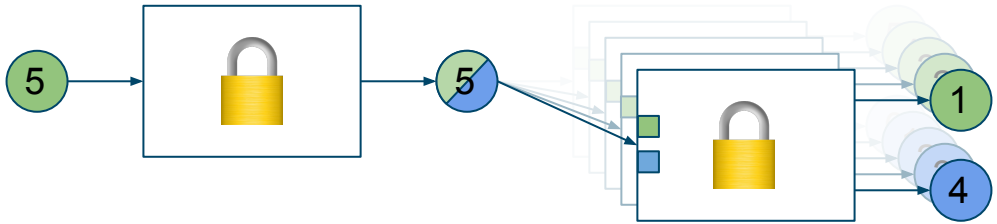


2 Update Mechanisms

nSequence Transaction Update (Satoshi 2009)

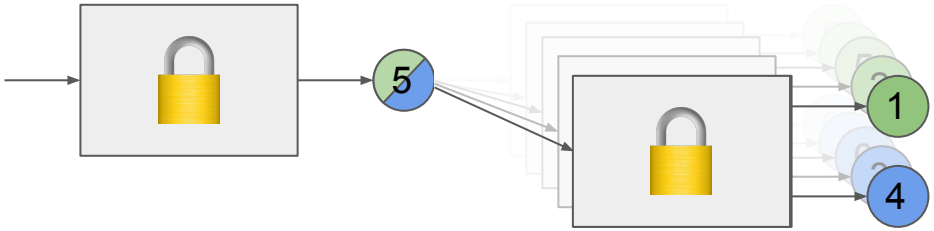
```
bool fNewer = false;
unsigned int nLowest = UINT_MAX;
for (int i = 0; i < vin.size(); i++)
{
    if (vin[i].nSequence != old.vin[i].nSequence)
    {
        if (vin[i].nSequence <= nLowest)
        {
            fNewer = false;
            nLowest = vin[i].nSequence;
        }
        if (old.vin[i].nSequence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

Simple Micropayment Channel (Spilman 2013)



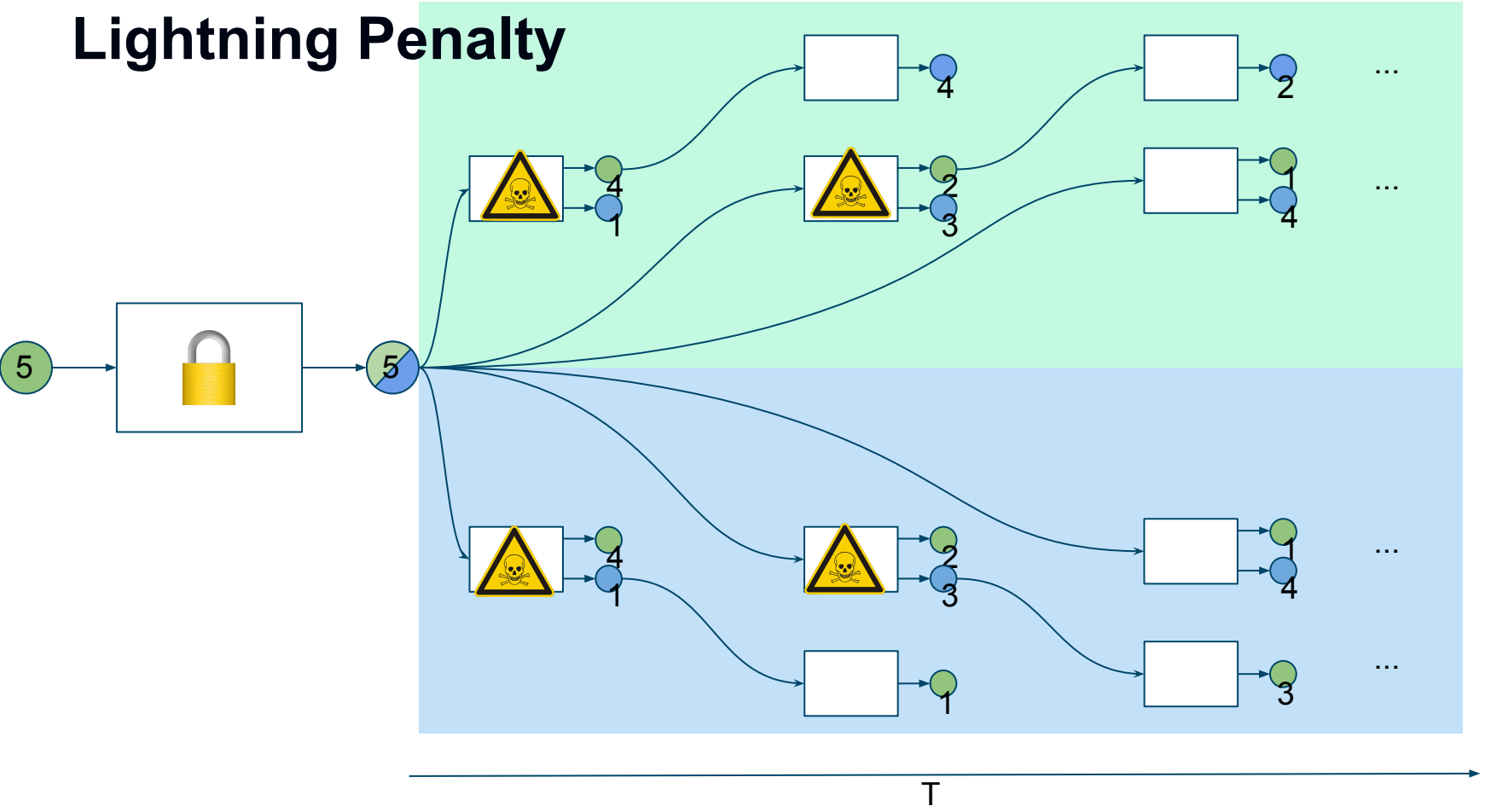
Decker and Wattenhofer, 2015

Duplex Micropayment Channels



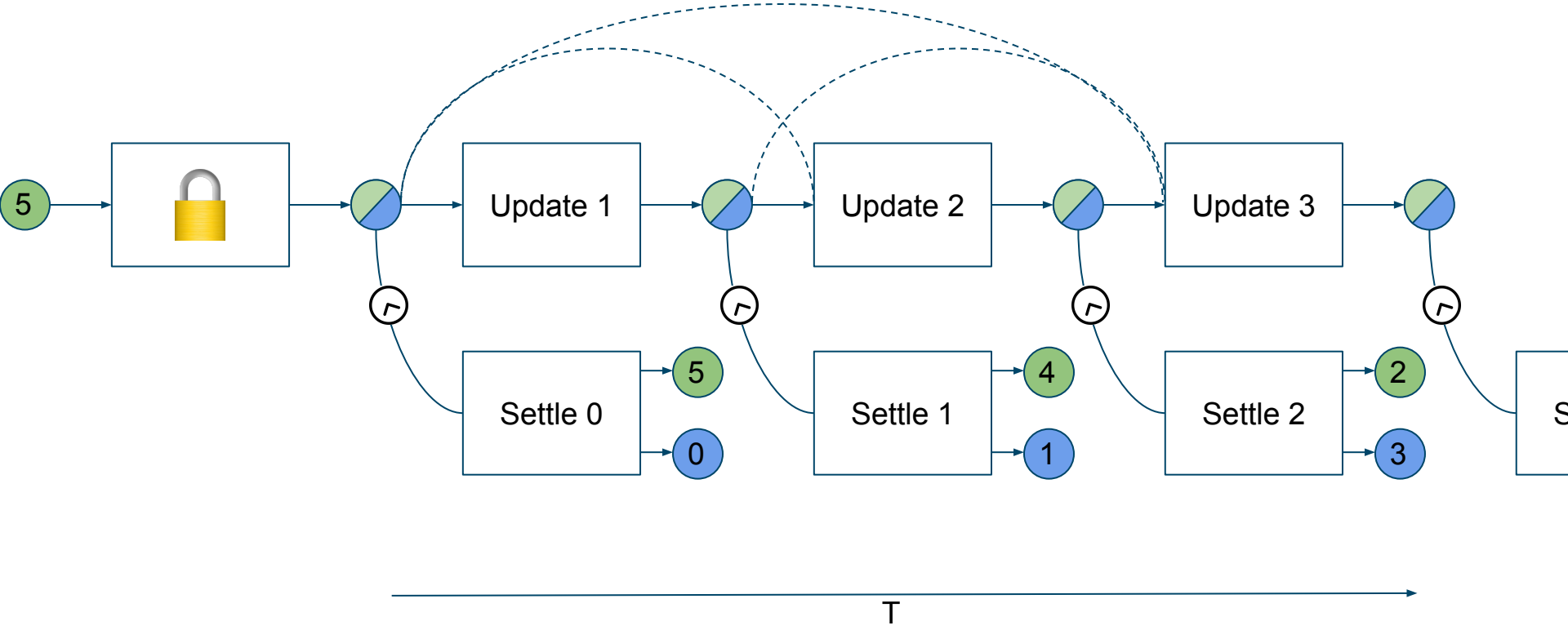
Poon and Dryja, 2015

Lightning Penalty



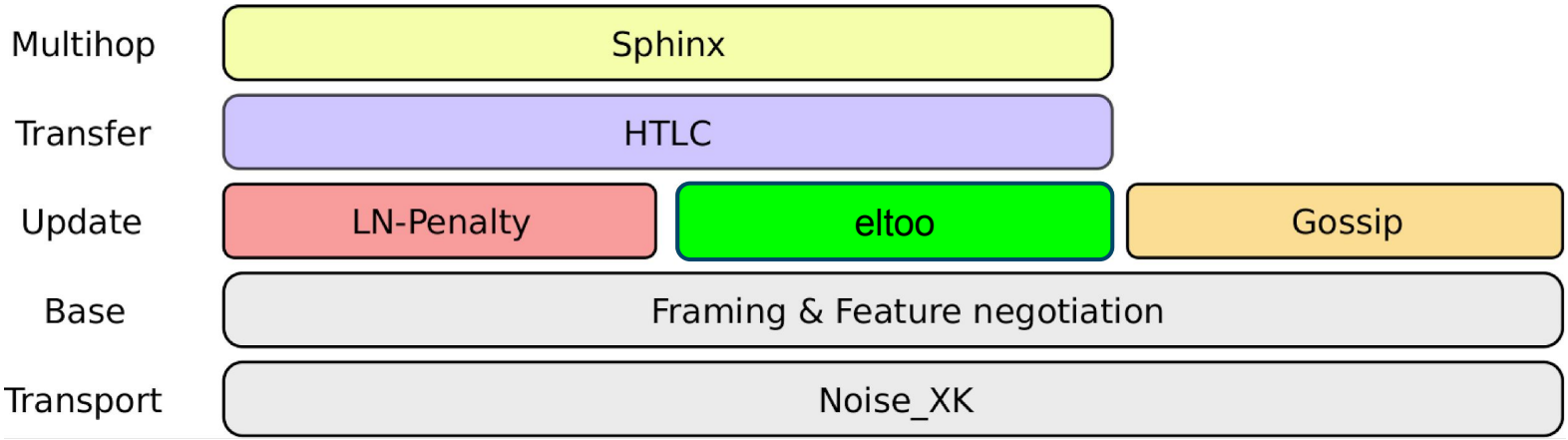
Decker et al., 2018

eltoo Update Mechanism



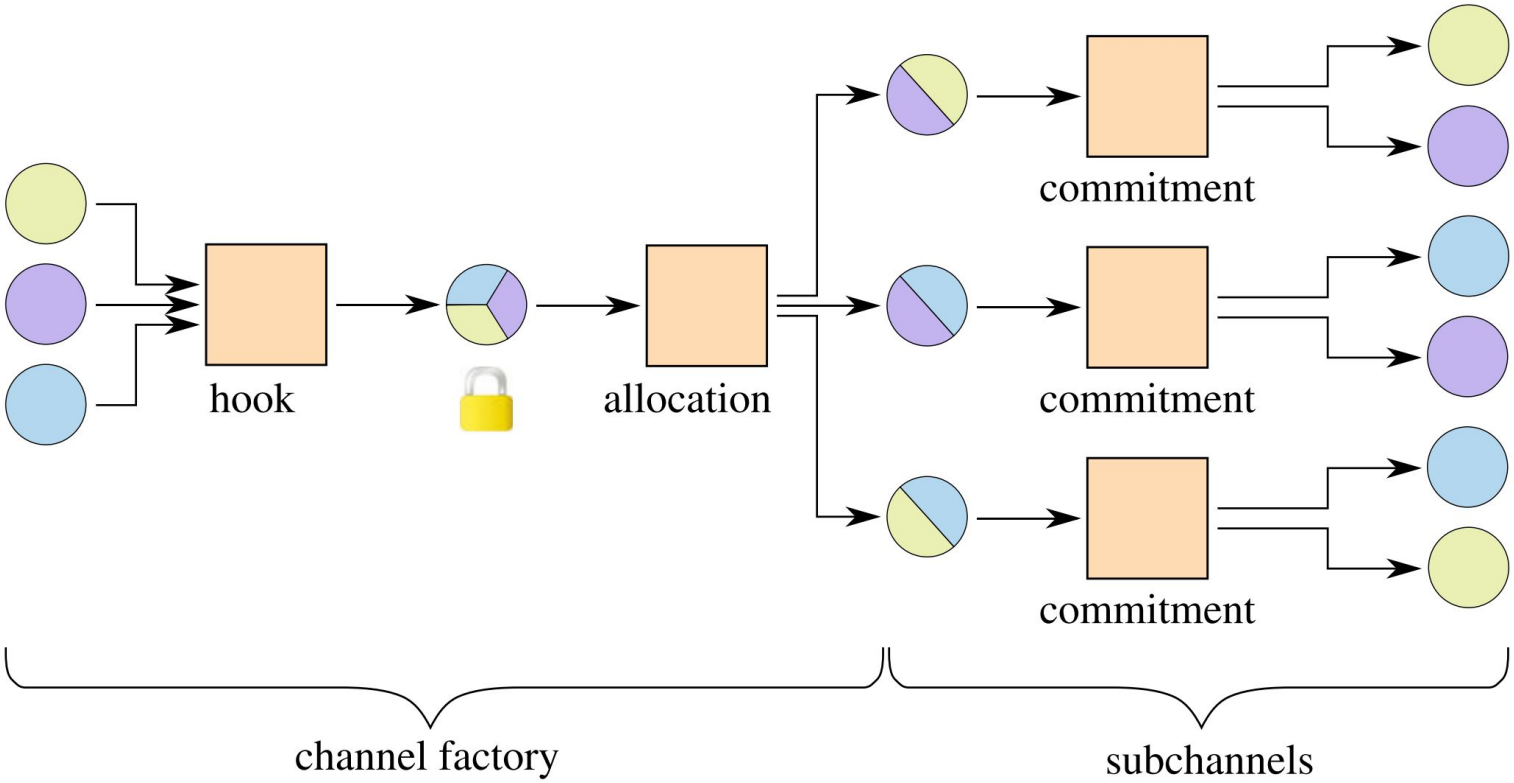
3 Layers all the way down...

The Lightning Stack



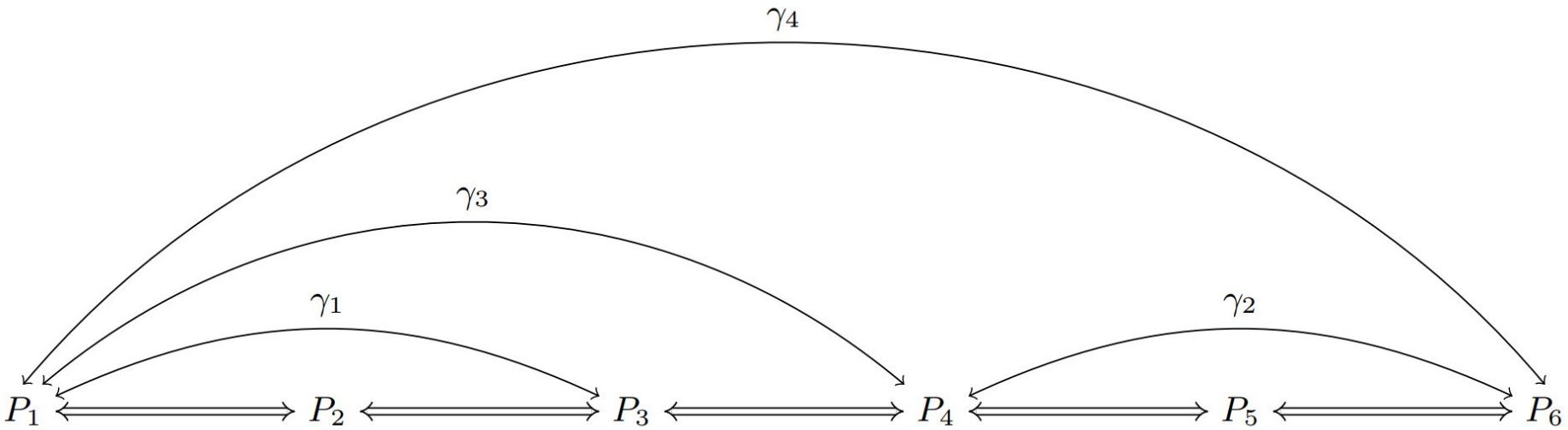
Burchert et al., 2015

Channel Factories



Dziembowski et al., 2018

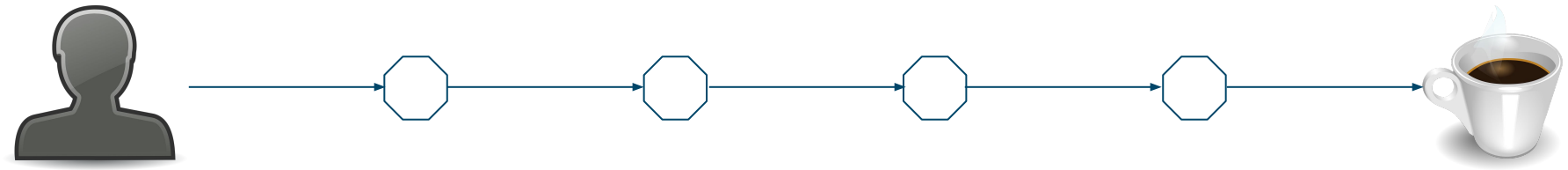
Perun



Blockstream

Thanks!
Questions?

Secure Multihop Transfers



Hashed Timelock Contracts (HTLC)

5

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

Onion Routing