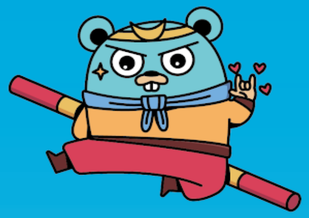


闪电网络—BTC小额支付解决方案

方圆

Agenda

- BTC简介
- 闪电网络介绍
  - 基本原理
  - LND介绍
  - 支付流程
- 问题及改进
- 结论

Go语言&区块链

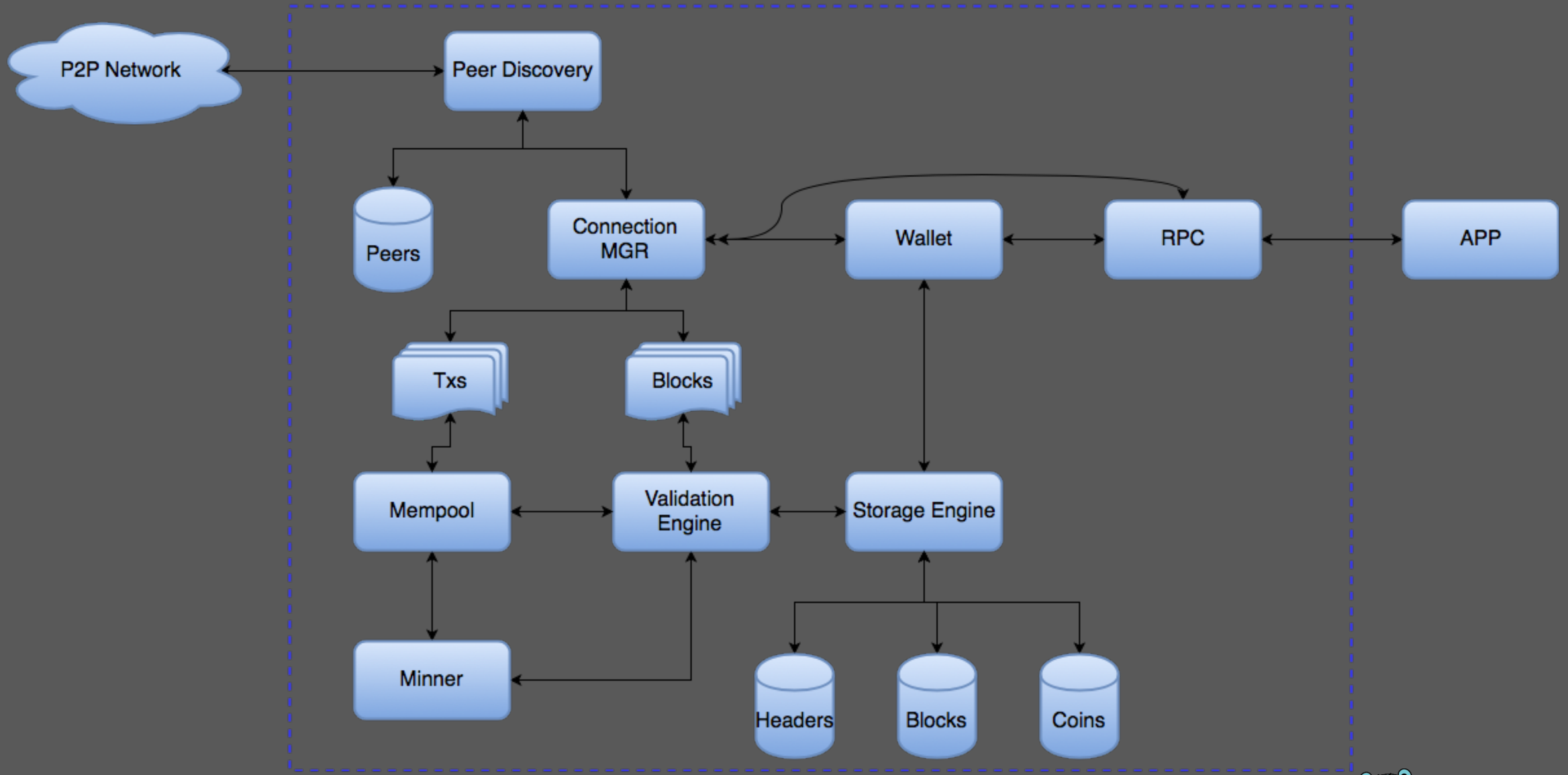
- 以太坊
- 闪电网络

BTC历史

- 2008年 中本聪(Satoshi Nakamoto)发表比特币论文
  - Bitcoin: A Peer-to-Peer Electronic Cash System
- 2009年启动
- 2011年中本聪退出公共视野
- BTC->BCH/LTC

BTC

- 核心特性
- P2P网络
- 交易
- 区块链
- 问题


P2P Network
Peer Discovery
Peers
Connection MGR
Wallet
RPC
APP
Txs
Blocks
Mempool
Validation Engine
Storage Engine
Minner
Headers
Blocks
Coins

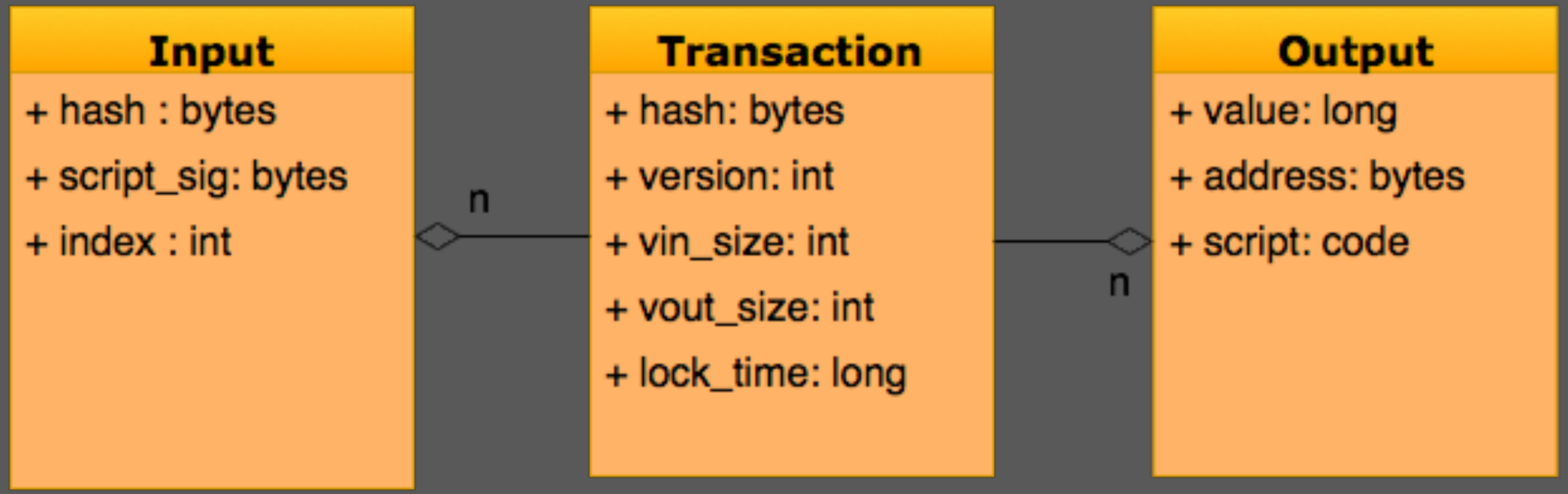
P2P网络

- P2P网络是比特币的基础
- 比特币的P2P是完全去中心化的
- 交易与区块通过P2P网络广播至所有比特币客户端

比特币地址

- 公钥与私钥是一对
- 公钥就是所谓的比特币地址
- 你有多少币=你的拥有的所有地址上币的总和
- 要花币需要用地址对应的私钥签名
- 所以，私钥丢了=钱没了、你知道了别人的私钥=发财
- 你可以随便生成公钥、私钥对，空间无限大

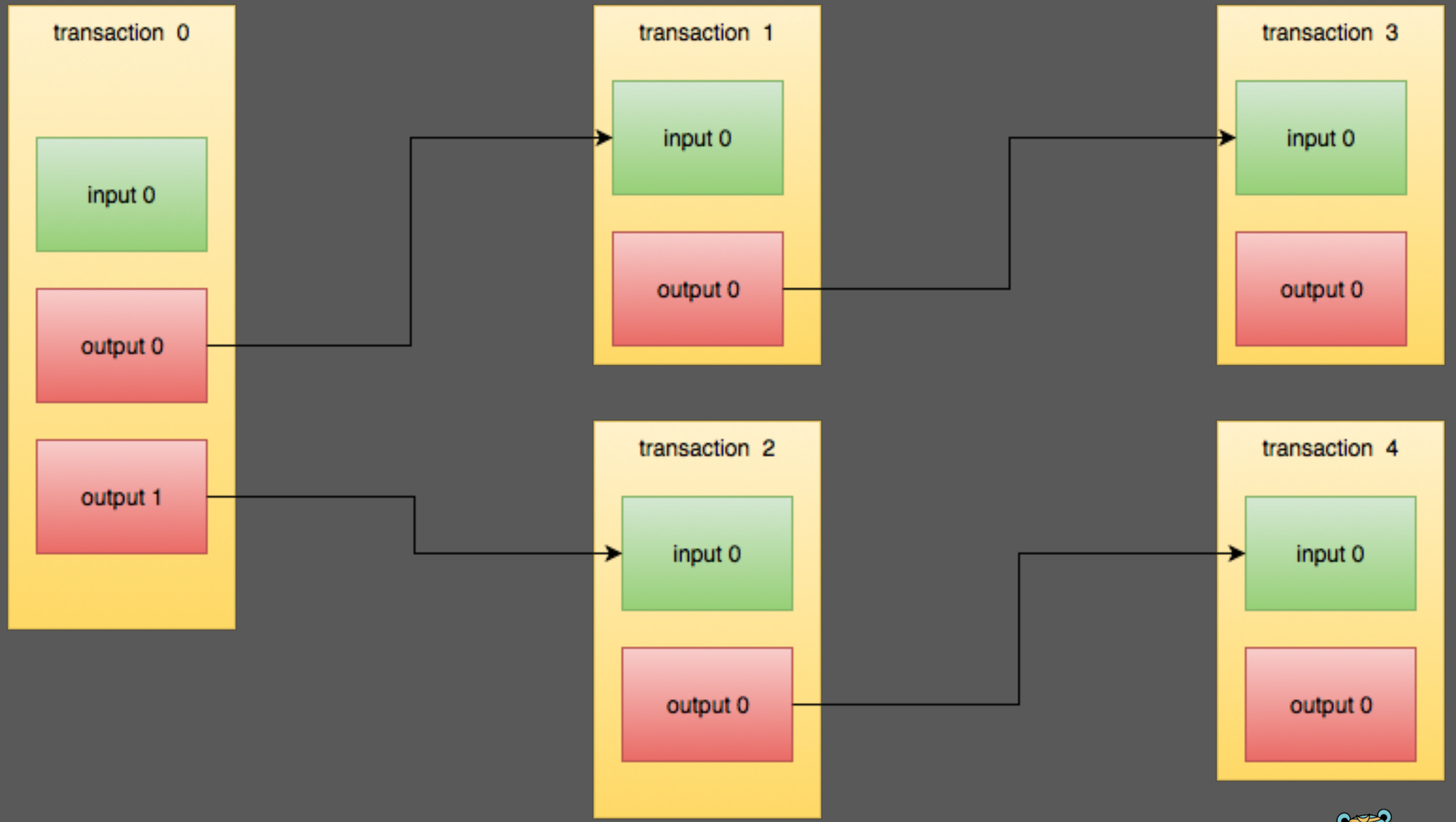
交易


Input
+ hash : bytes
+ script_sig: bytes
+ index : int
n
Transaction
+ hash: bytes
+ version: int
+ vin_size: int
+ vout_size: int
+ lock_time: long
n
Output
+ value: long
+ address: bytes
+ script: code

```
type MsgTx struct {
        Version  int32
        TxIn     []*TxIn
        TxOut    []*TxOut
        LockTime uint32
}
```

```
type TxIn struct {
        PreviousOutPoint OutPoint
        SignatureScript  []byte
        Sequence         uint32
}
```

```
type TxOut struct {
        Value  int64
        Pk     []byte
        Script []byte
}
```



transaction 0
input 0
output 0
output 1
transaction 1
input 0
output 0
transaction 2
input 0
output 0
transaction 3
input 0
output 0
transaction 4
input 0
output 0

交易

Details

3 Inputs Consumed

0.19751433 BTC from
3D8faXEDBcHuaCKk5F2eQbpWYERvHQDC4y (output)

0.19640209 BTC from
35AuE653A4yAvpuDVEpPPtfU4S7yfgqwNf (output)

0.196002 BTC from
3LyhX5muDpkETGfsGAmdtSruVYEHPLyYeL (output)

2 Outputs Created

0.426007 BTC to
1GBWfHDR9PuFkEUtRugKym1EjLj4ng6uFv (unspent)

0.16372447 BTC to
3CgPiiPgP7ZoVHW6ak1PrP2NANrs44jsGC (unspent)

交易

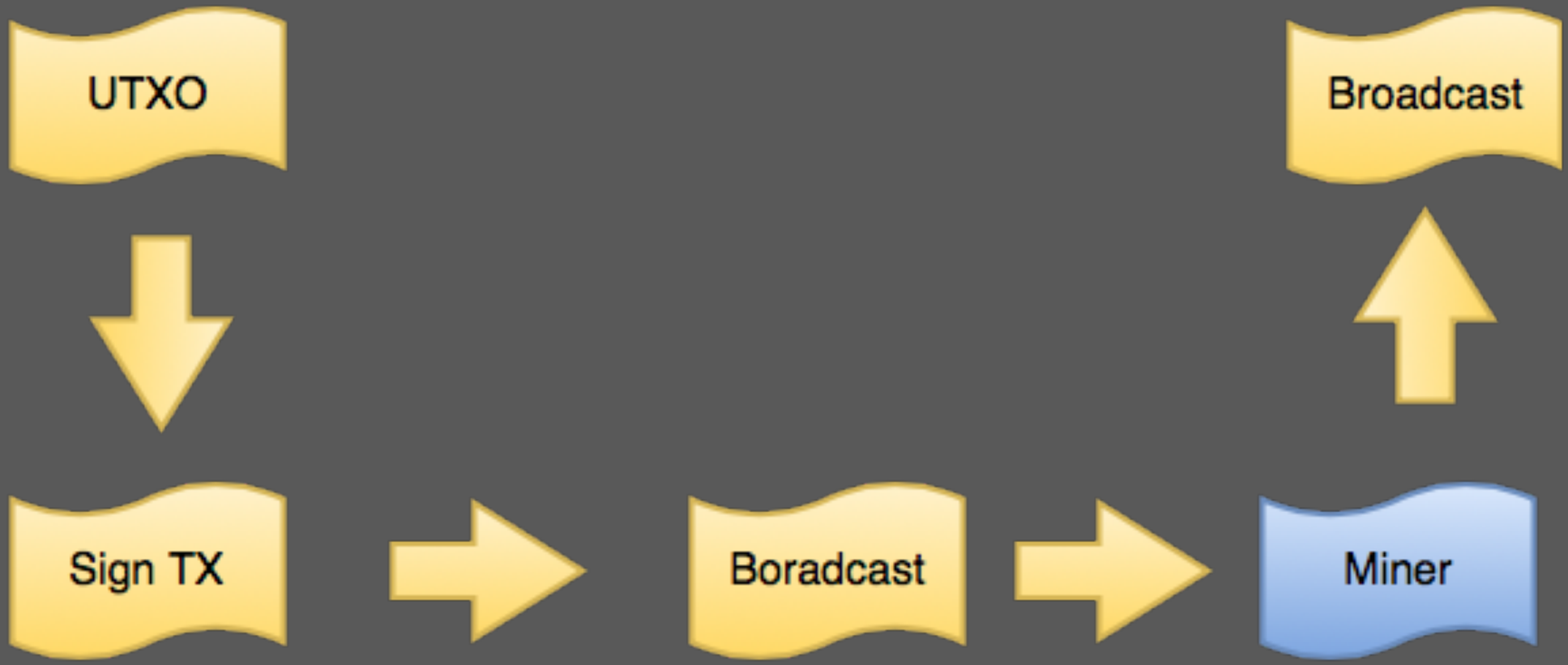
Unlocking Script

Locking Script

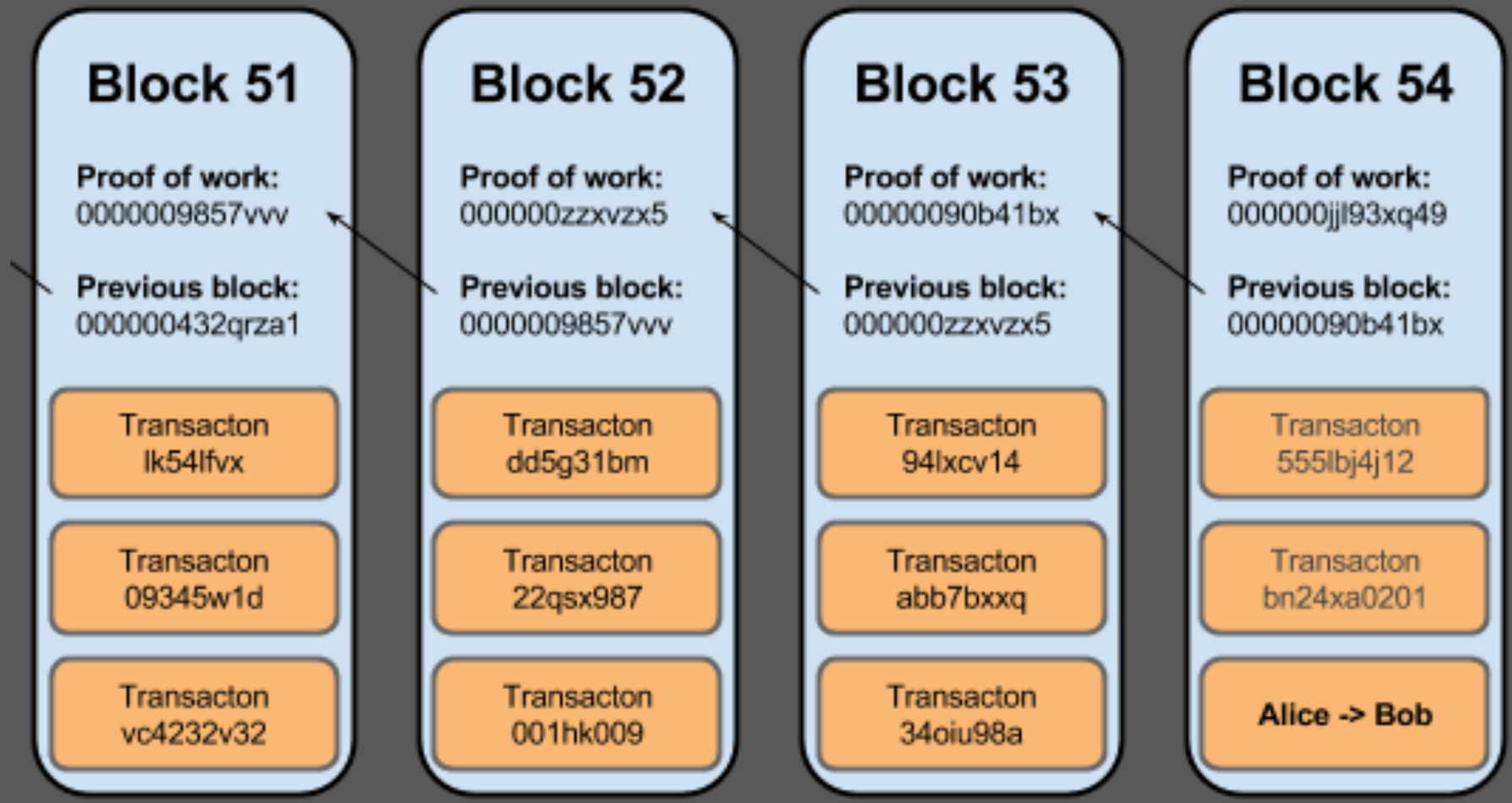
sig

verify(pk,sig) ==true

交易



区块链


Block 51
Proof of work:
0000009857vvv
Previous block:
000000432qrza1
Transacton
lk54lfvx
Transacton
09345w1d
Transacton
vc4232v32
Block 52
Proof of work:
000000zzxvzx5
Previous block:
0000009857vvv
Transacton
dd5g31bm
Transacton
22qsx987
Transacton
001hk009
Block 53
Proof of work:
00000090b41bx
Previous block:
000000zzxvzx5
Transacton
94lxcv14
Transacton
abb7bxxq
Transacton
34oiu98a
Block 54
Proof of work:
000000jjl93xq49
Previous block:
00000090b41bx
Transacton
555lbj4j12
Transacton
bn24xa0201
Alice -> Bob

交易

- 花币就是生成一笔交易
- 然后用私钥签名交易
- 广播交易至P2P网络
- 交易被矿工打包进区块就意味着交易完成吗

BTC

- 完全去中心化的P2P网络
- 去中心化的交易，验证系统
- 去中心化的交易账本
- 去中心化的数字货币发行

问题

- 冗余存储过于严重
- 每秒交易数<7，如何去扩容
- 交易延迟（60分钟）

如何解决问题

- 交易吞吐量问题
- 交易延迟

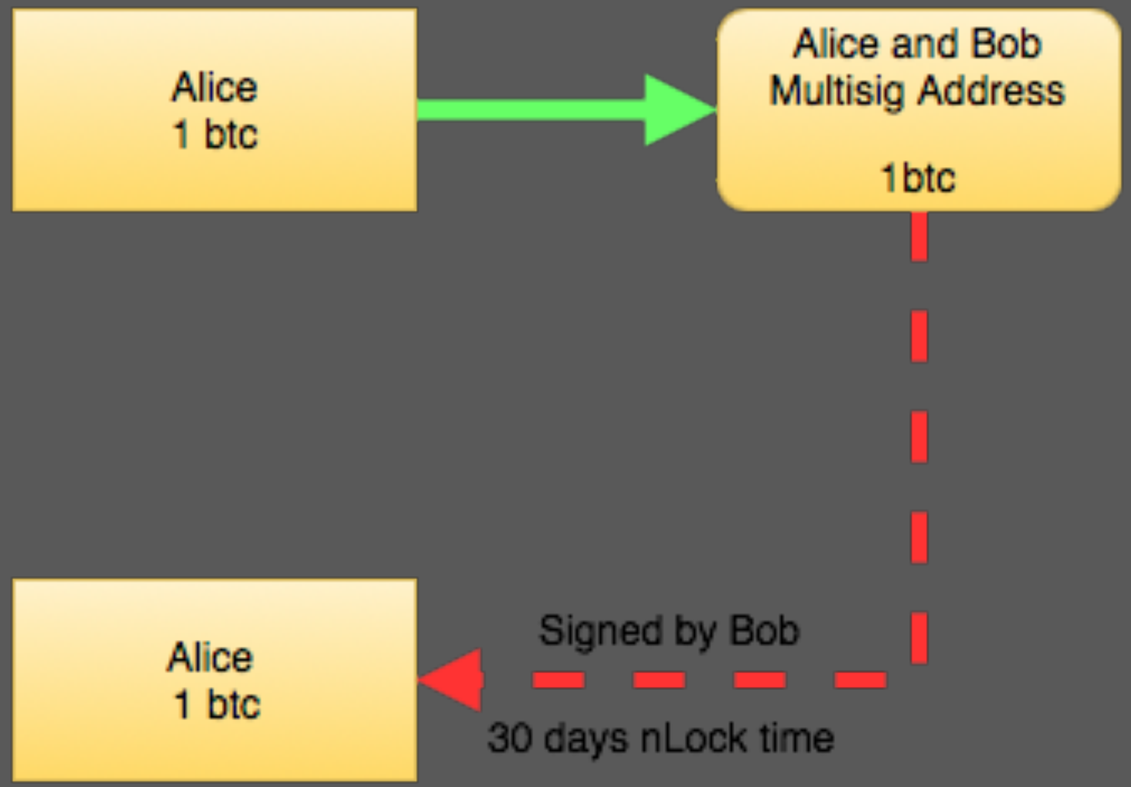
区块链二层

- layered blockchain
- payment channel

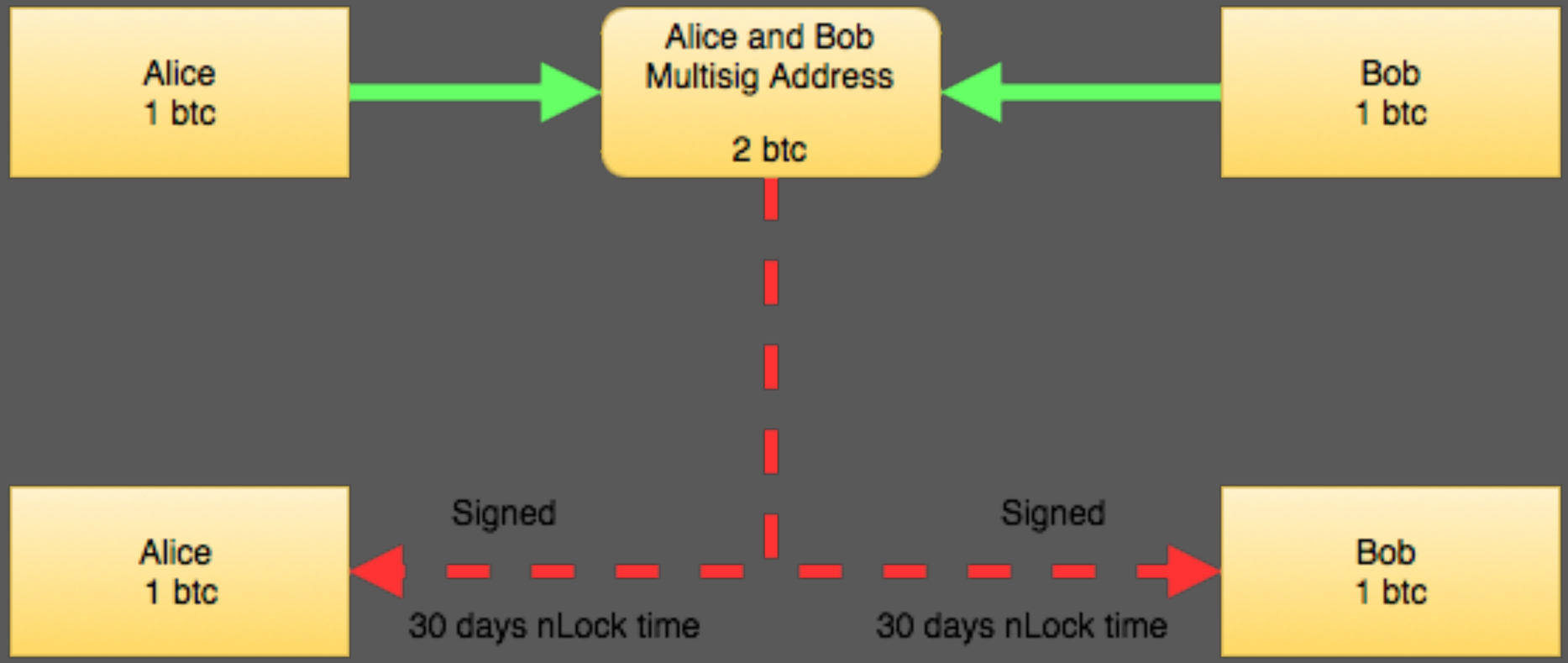
闪电网络

- 支付通道
- 基本流程
  - 打开通道
  - 交易
  - 关闭通道

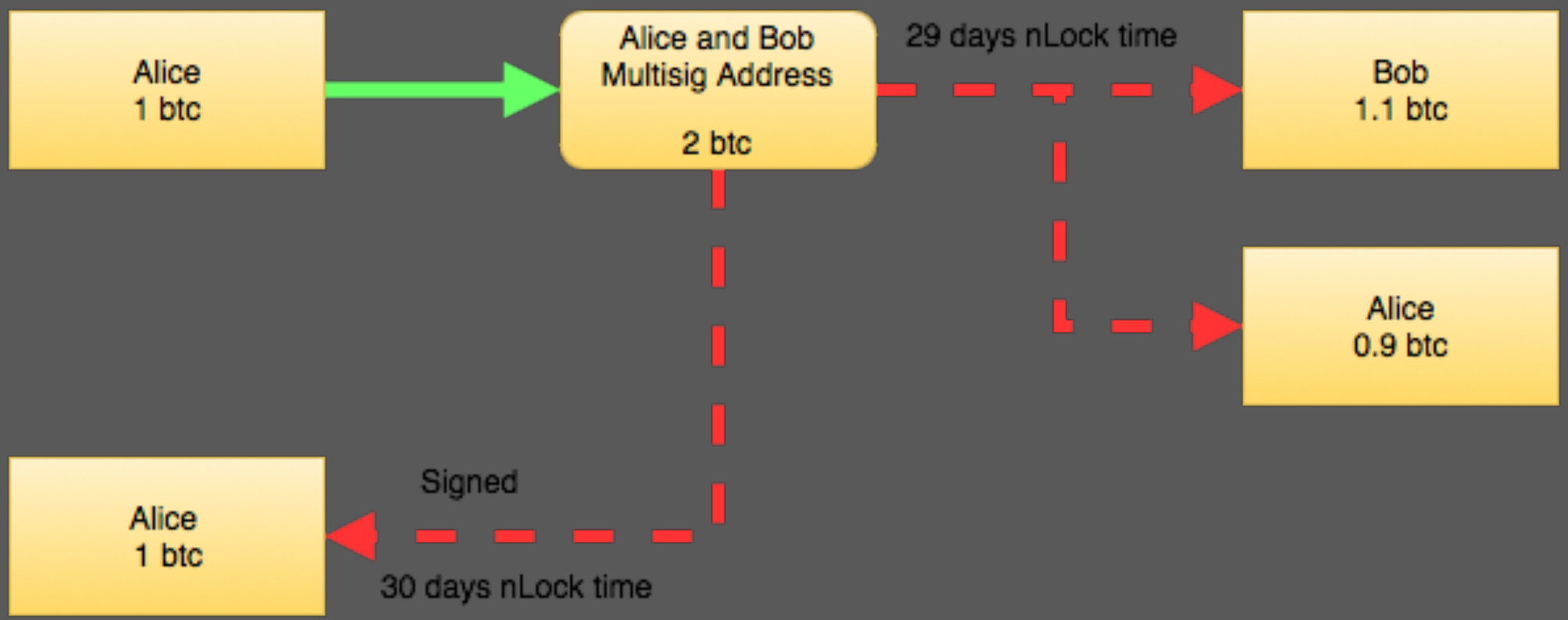
Open Channel



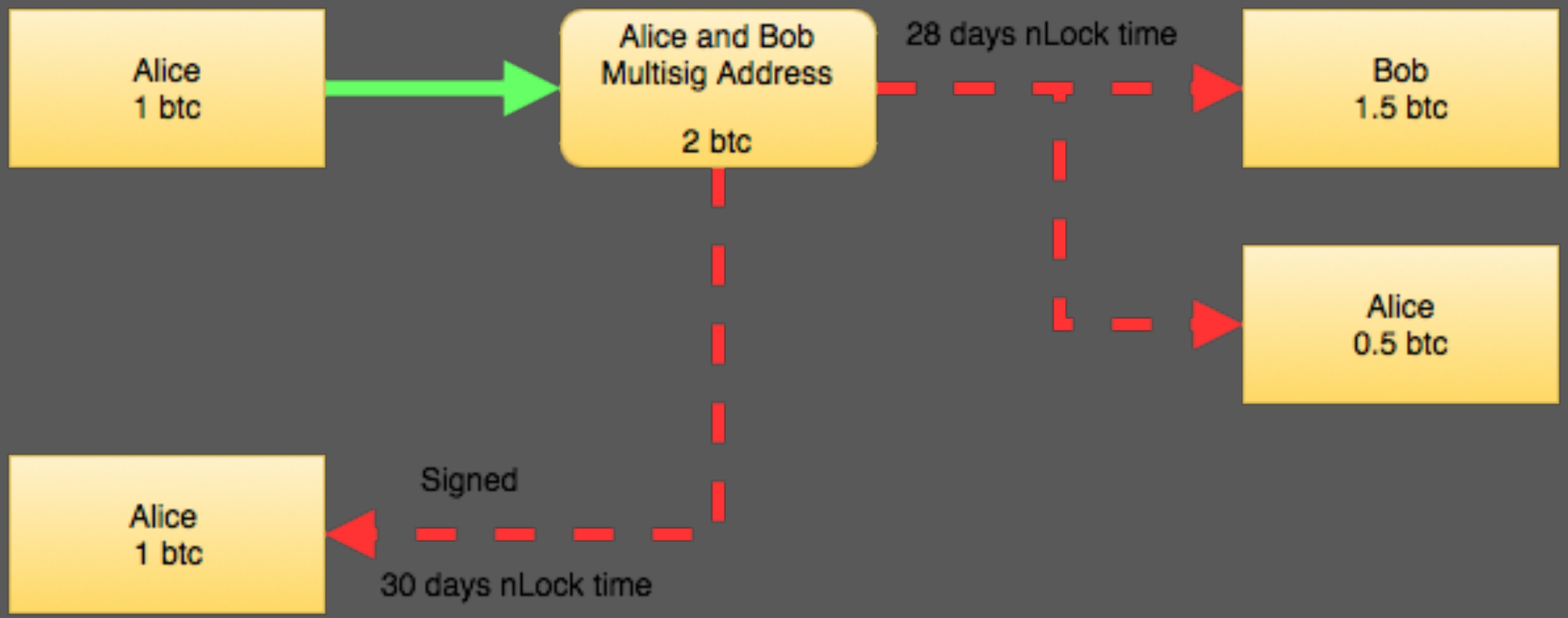
Open Channel



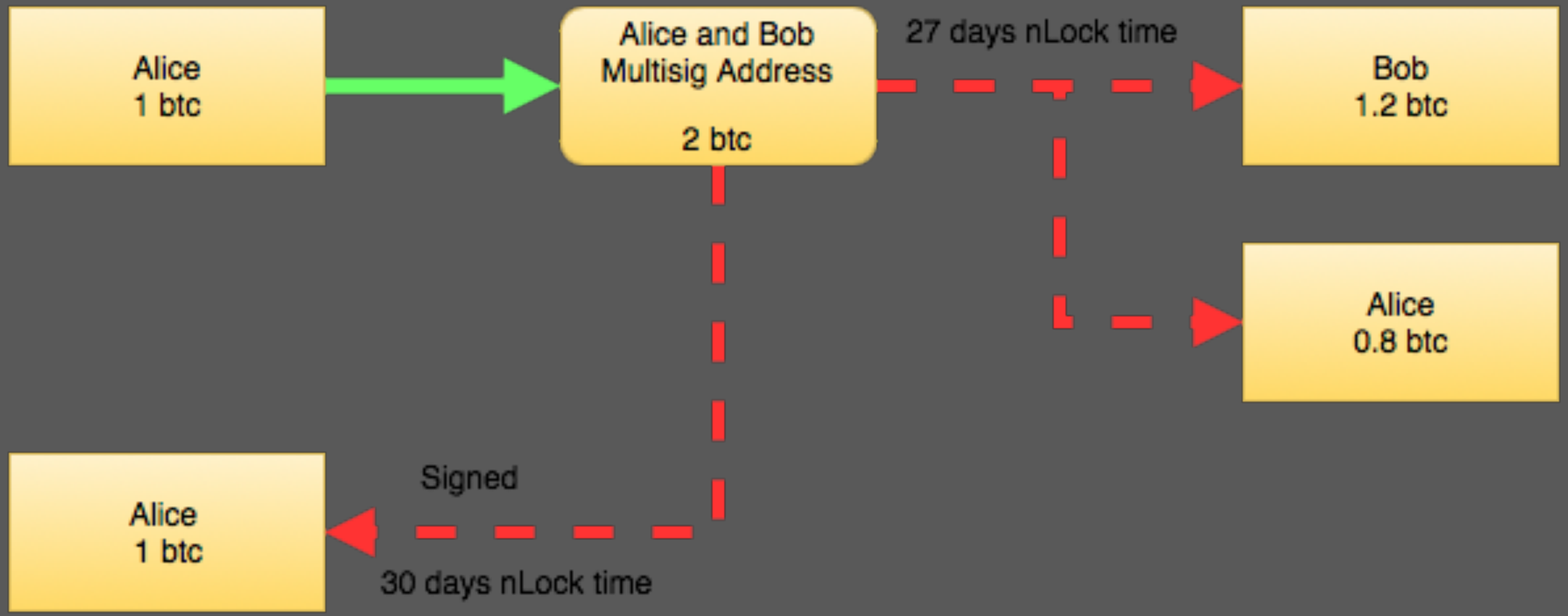
Pay


Alice
1 btc
Alice and Bob
Multisig Address
2 btc
29 days nLock time
Bob
1.1 btc
Alice
0.9 btc
Signed
Alice
1 btc
30 days nLock time

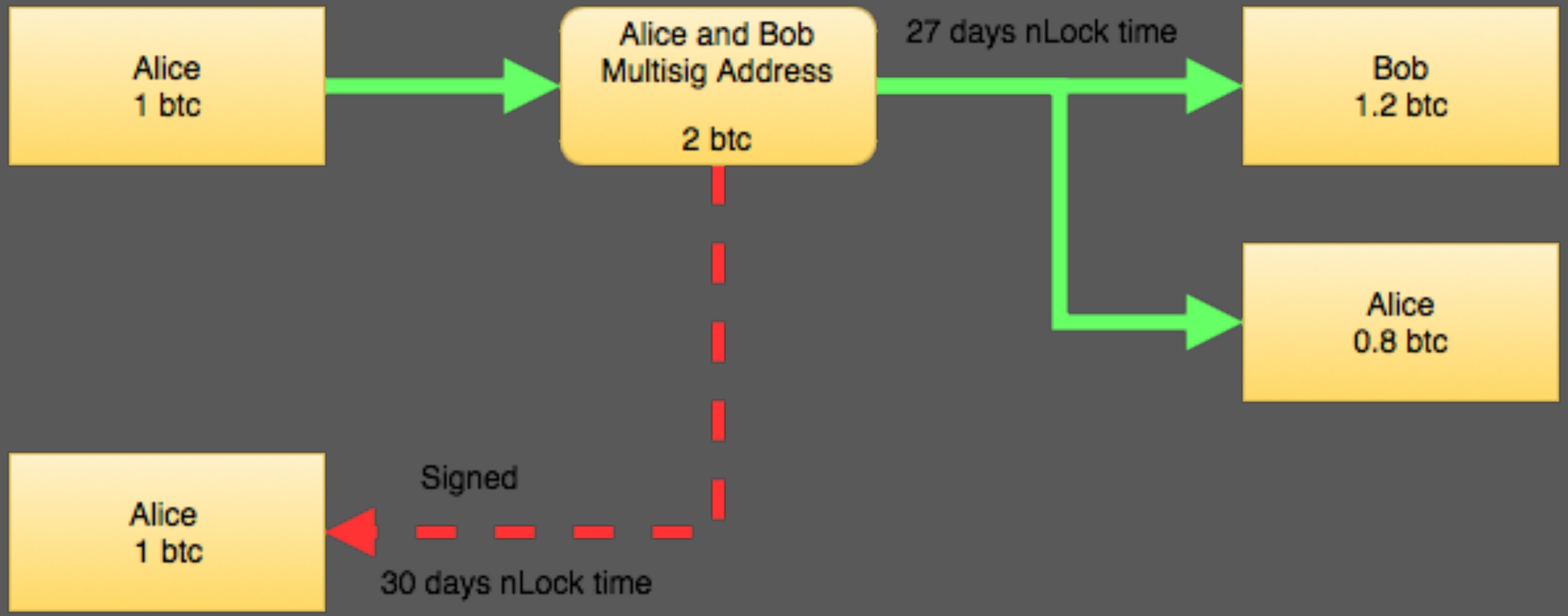
Pay

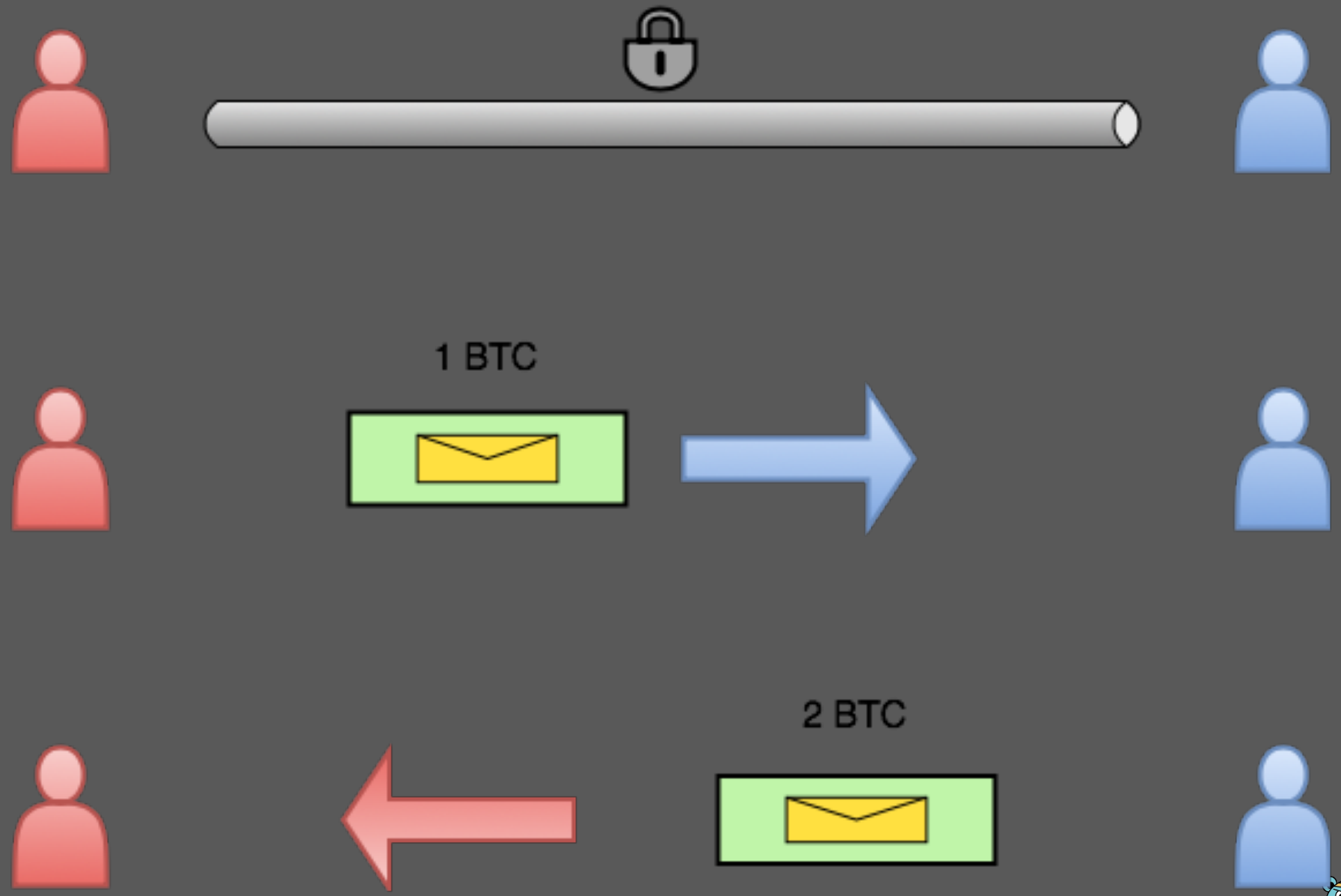

Alice
1 btc
Alice and Bob
Multisig Address
2 btc
28 days nLock time
Bob
1.5 btc
Alice
0.5 btc
Signed
Alice
1 btc
30 days nLock time

Reversing Direction Pay

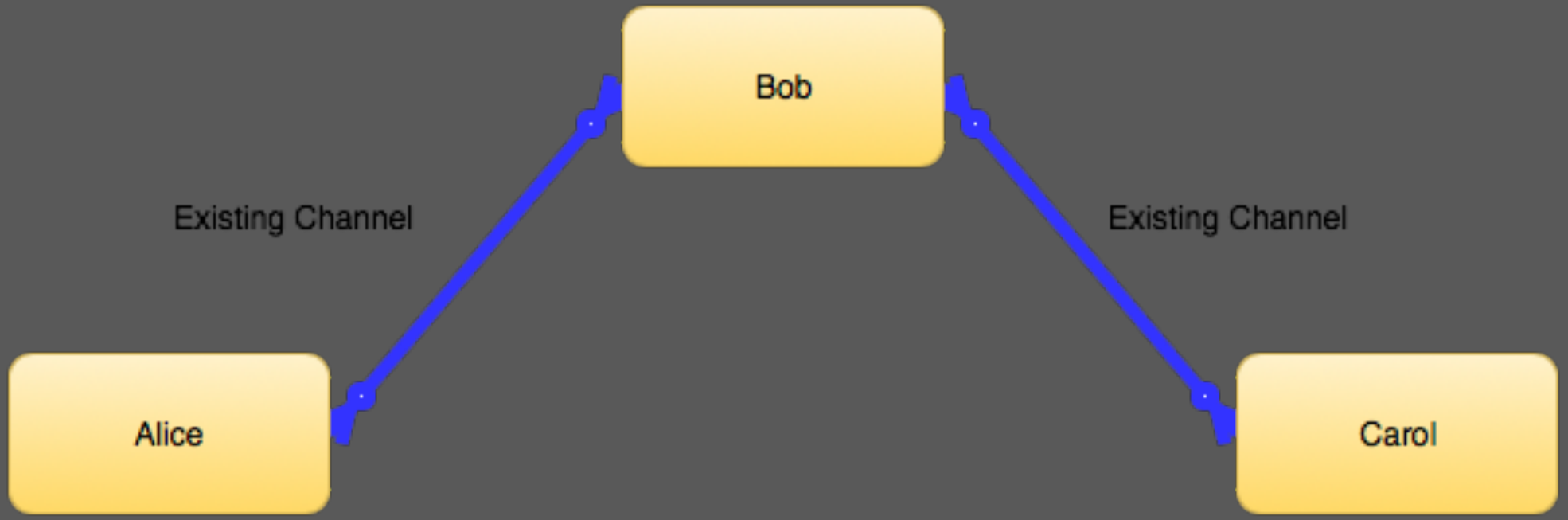


Close Channel

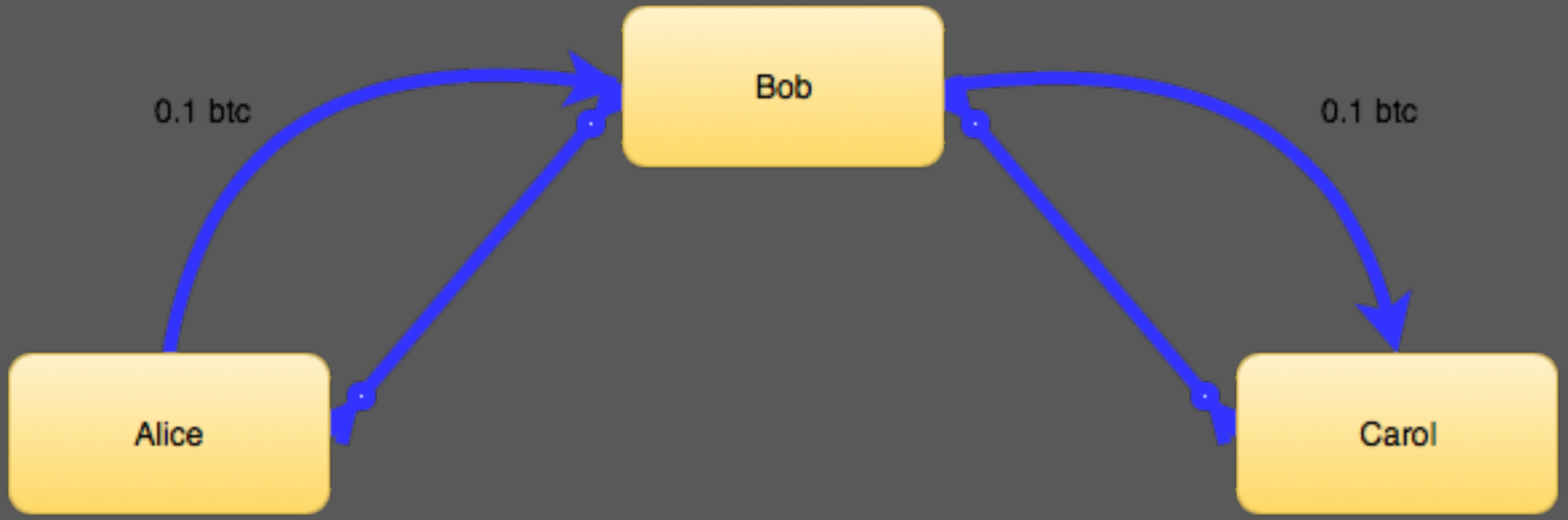



1 BTC
2 BTC

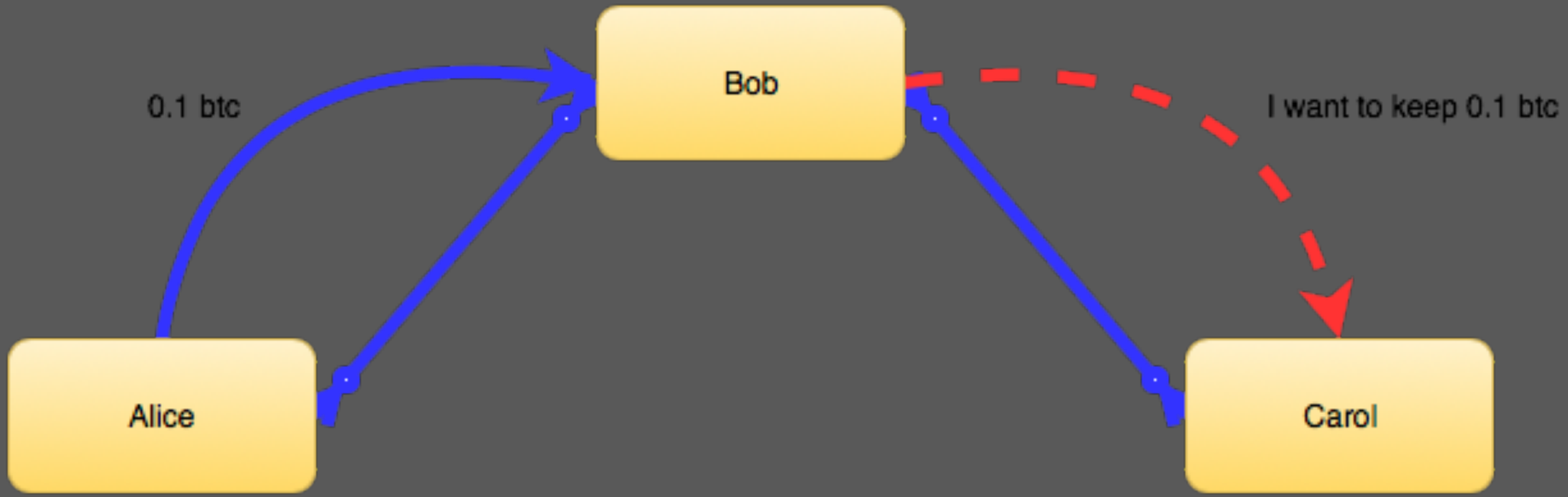
3 Party Payment



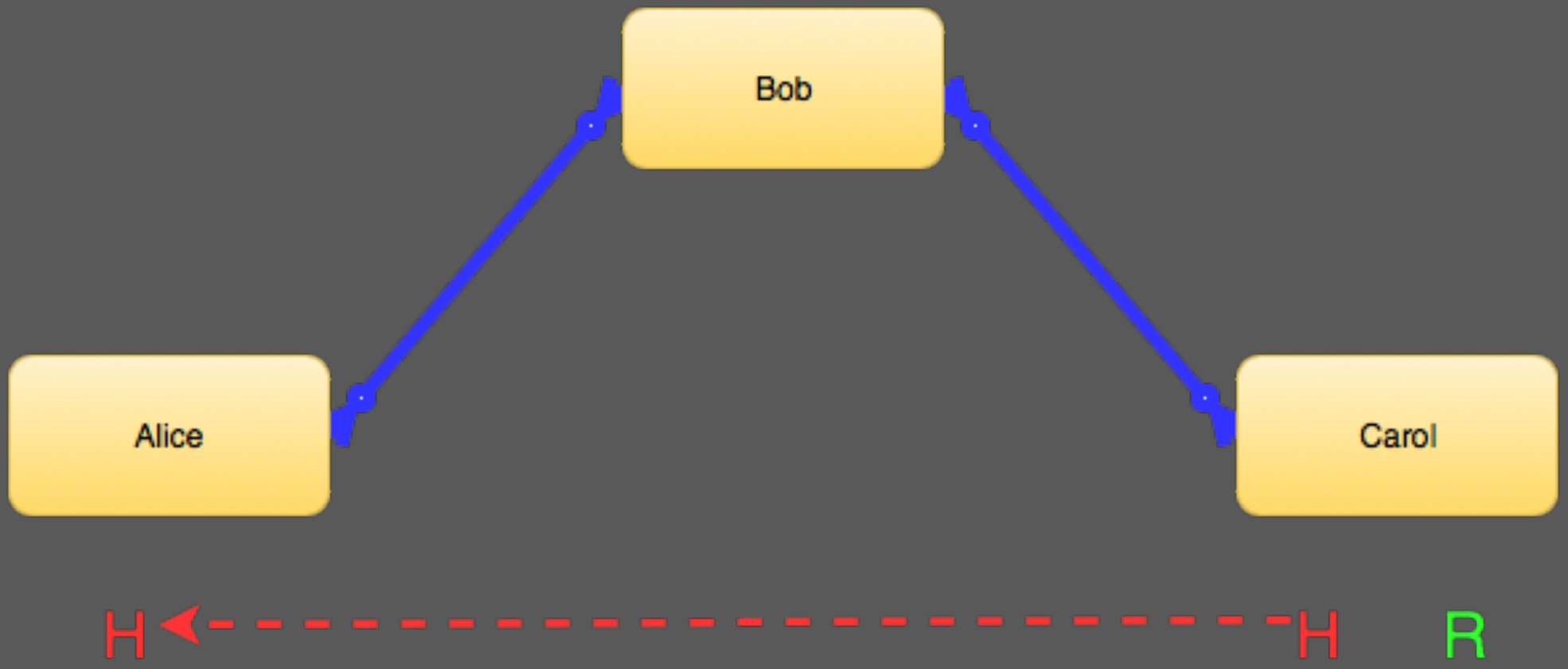
3 Party Payment



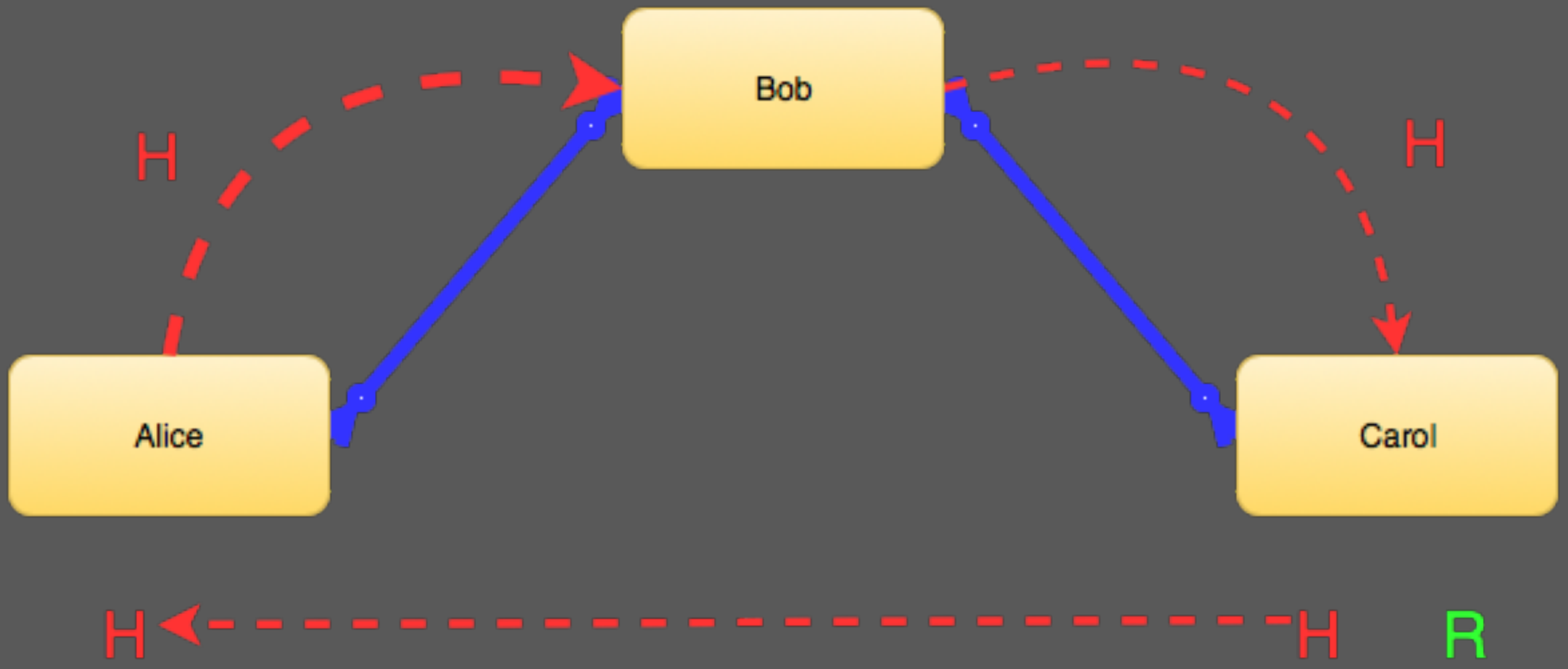
3 Party Payments - Trust Issues



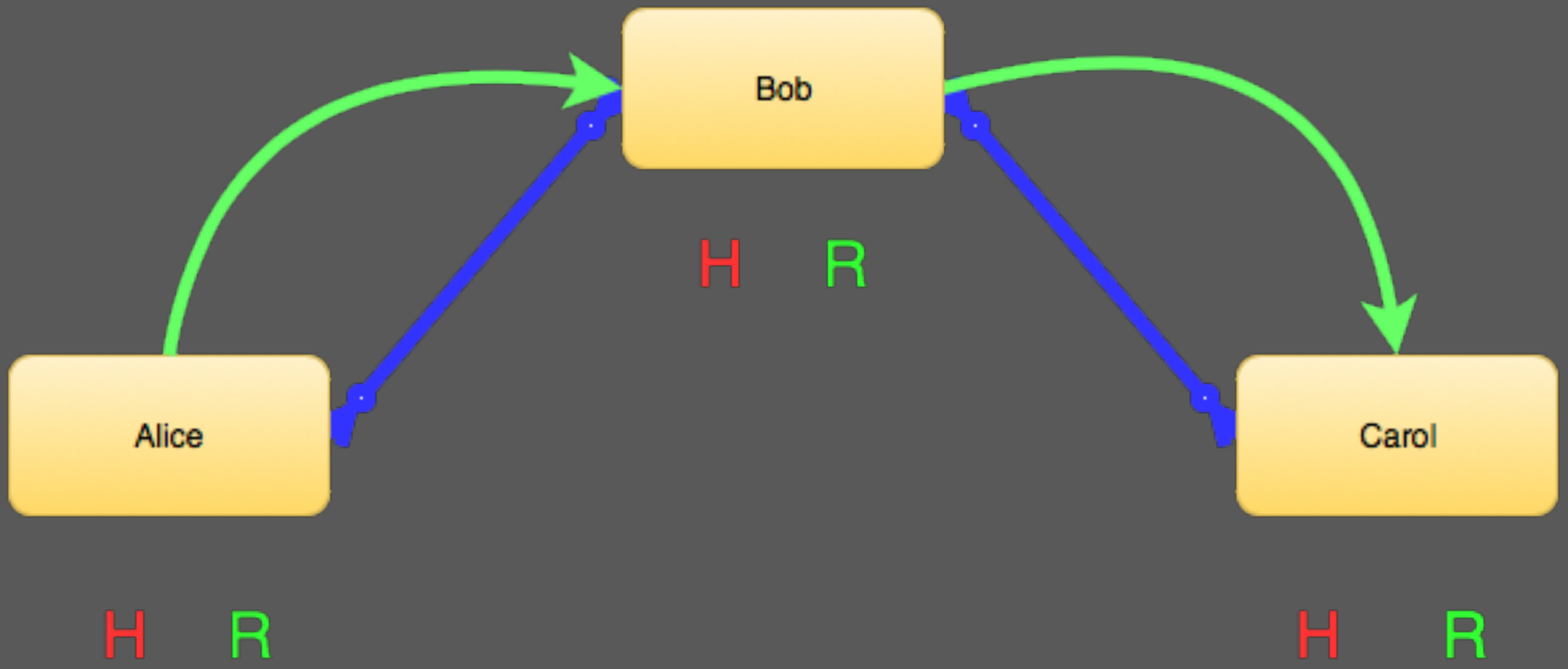
Hash Lock Contract

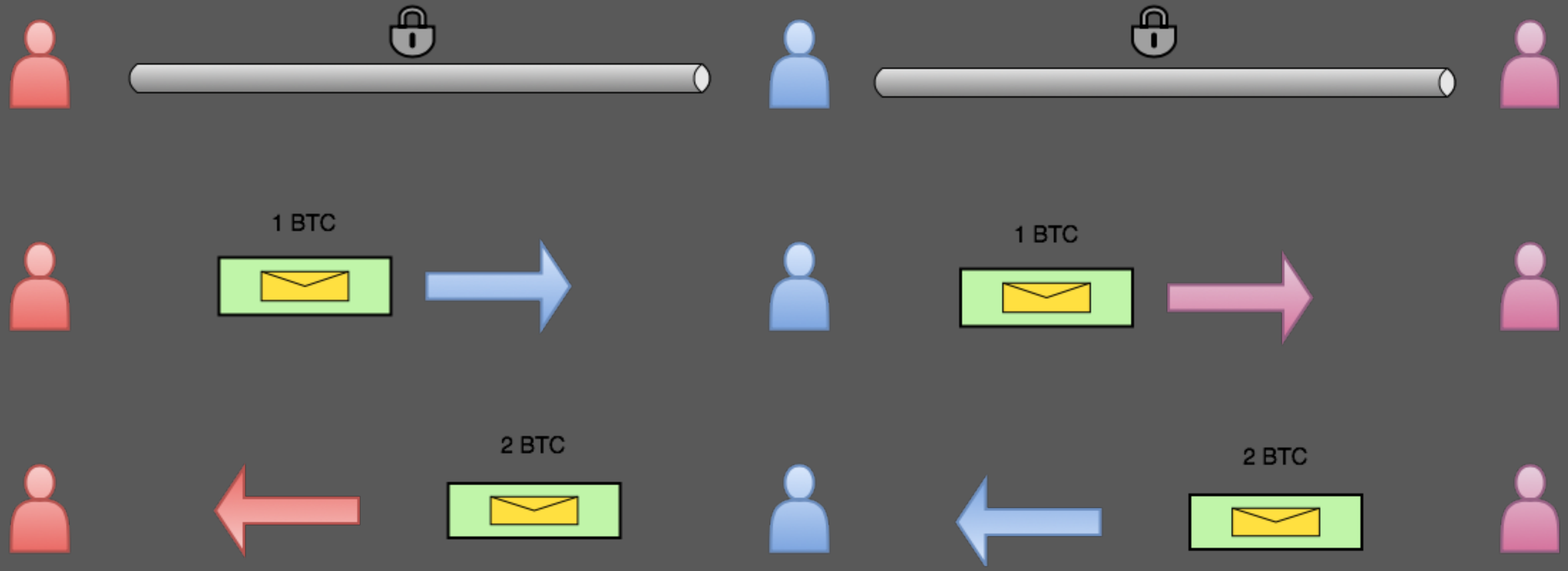


Hash Lock Contract



Hash Lock Contract

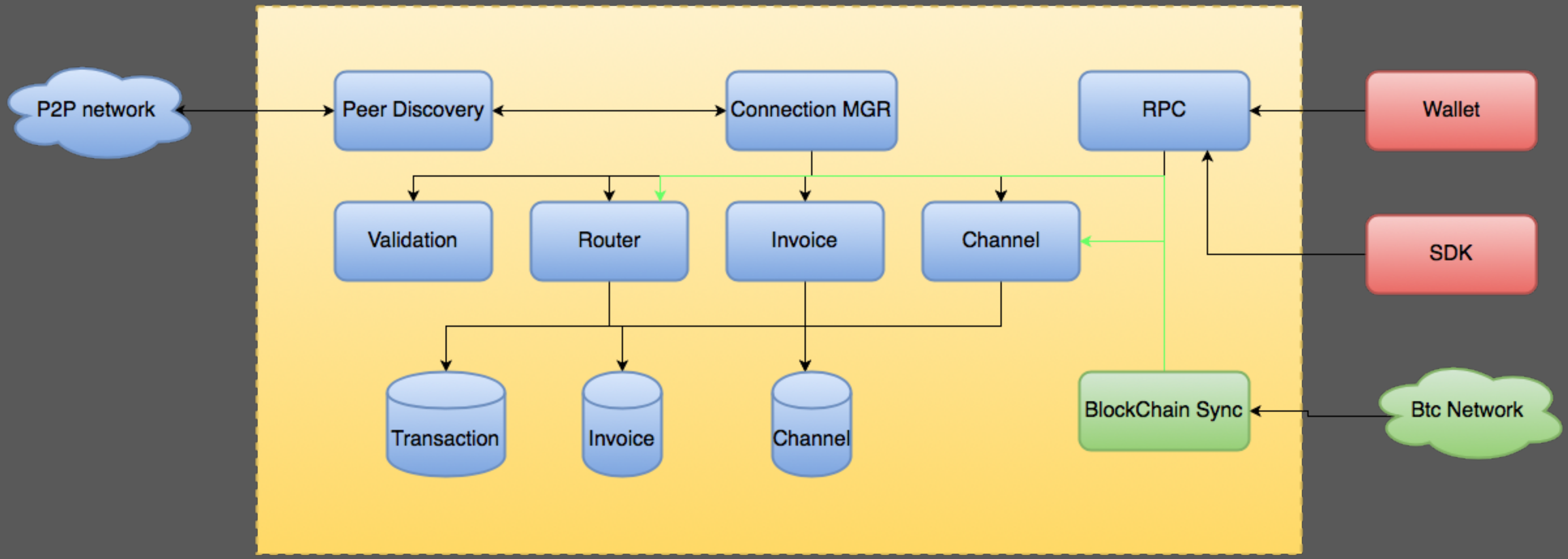



1 BTC
1 BTC
2 BTC
2 BTC

Implements

- LND
- c-lightning
- eclair

LND


P2P network
Peer Discovery
Connection MGR
RPC
Wallet
Validation
Router
Invoice
Channel
SDK
Transaction
Invoice
Channel
BlockChain Sync
Btc Network

LND

- Setup Node
  - btc/ltc
  - lnd
- Connect
- Open Channel
- Add invoice
- Pay
- Close Channel

LND

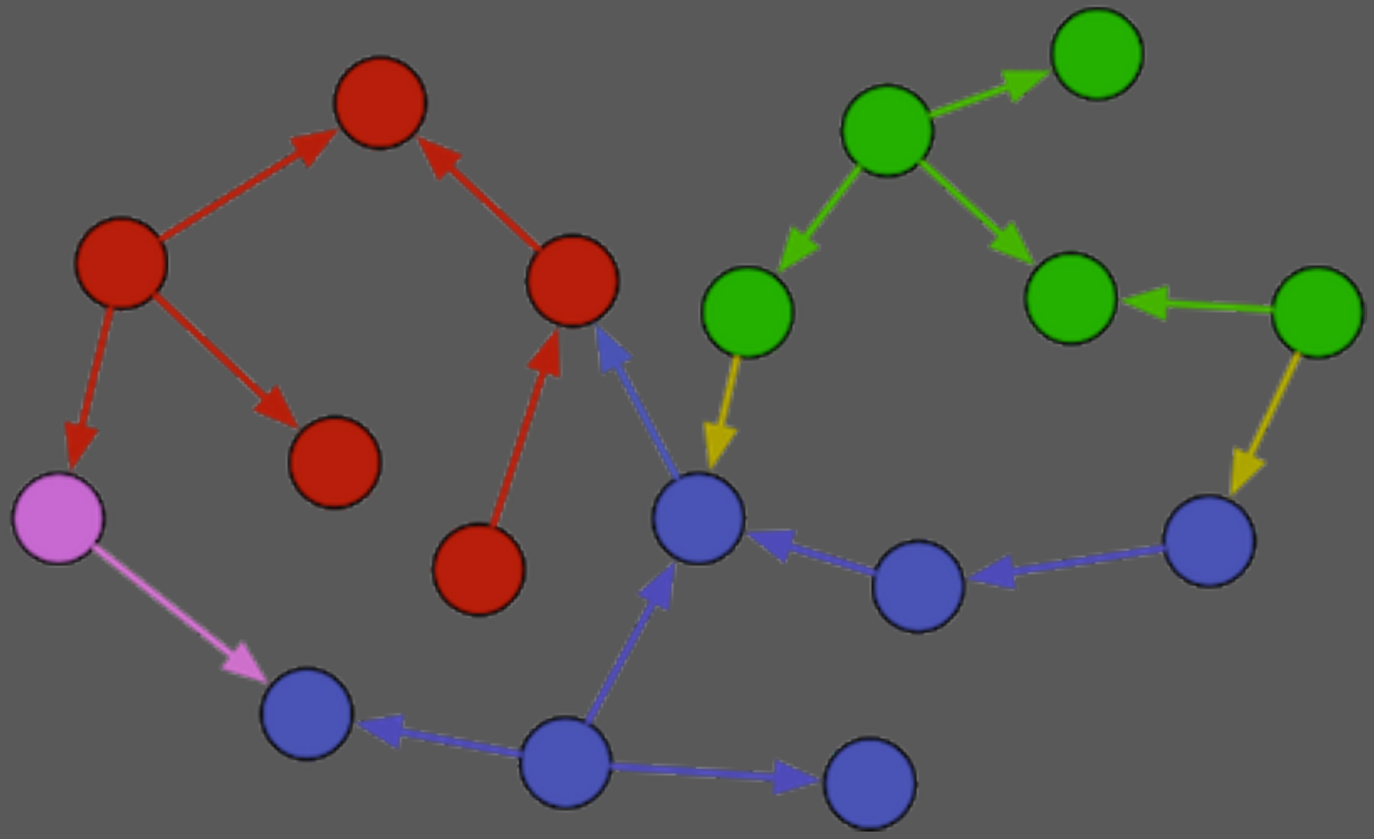
```
# Add invoice on "Bob" side:
bob$ lncli --network=simnet addinvoice --amt=10000
{
        "r_hash": "<your_random_rhash_here>",
        "pay_req": "<encoded_invoice>",
}

# Send payment from "Alice" to "Bob":
alice$ lncli --network=simnet sendpayment --
pay_req=<encoded_invoice>
```

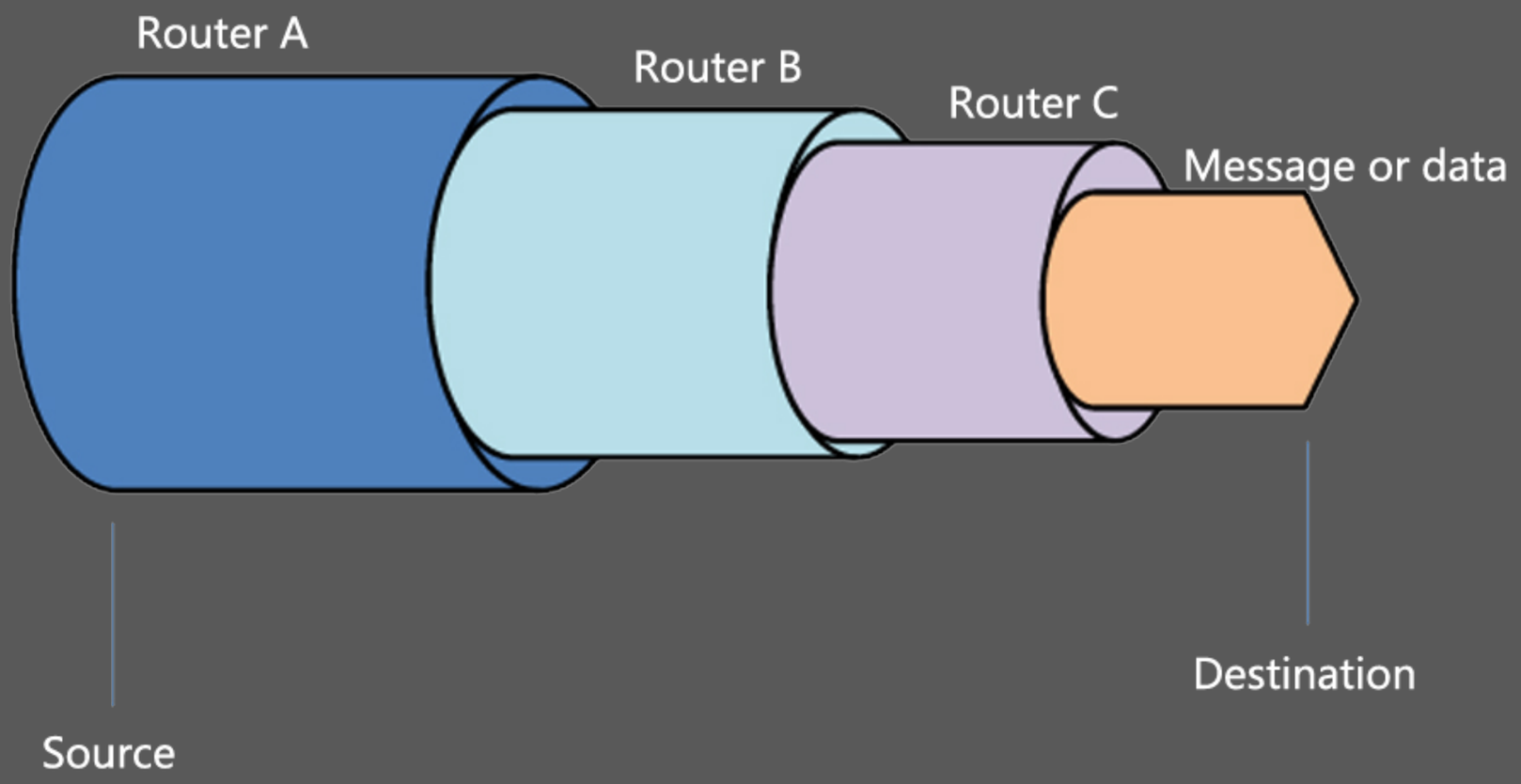

LND router

- Sender Routing
- Onion Routing
- Routing Fee

LND Routing Graph DB



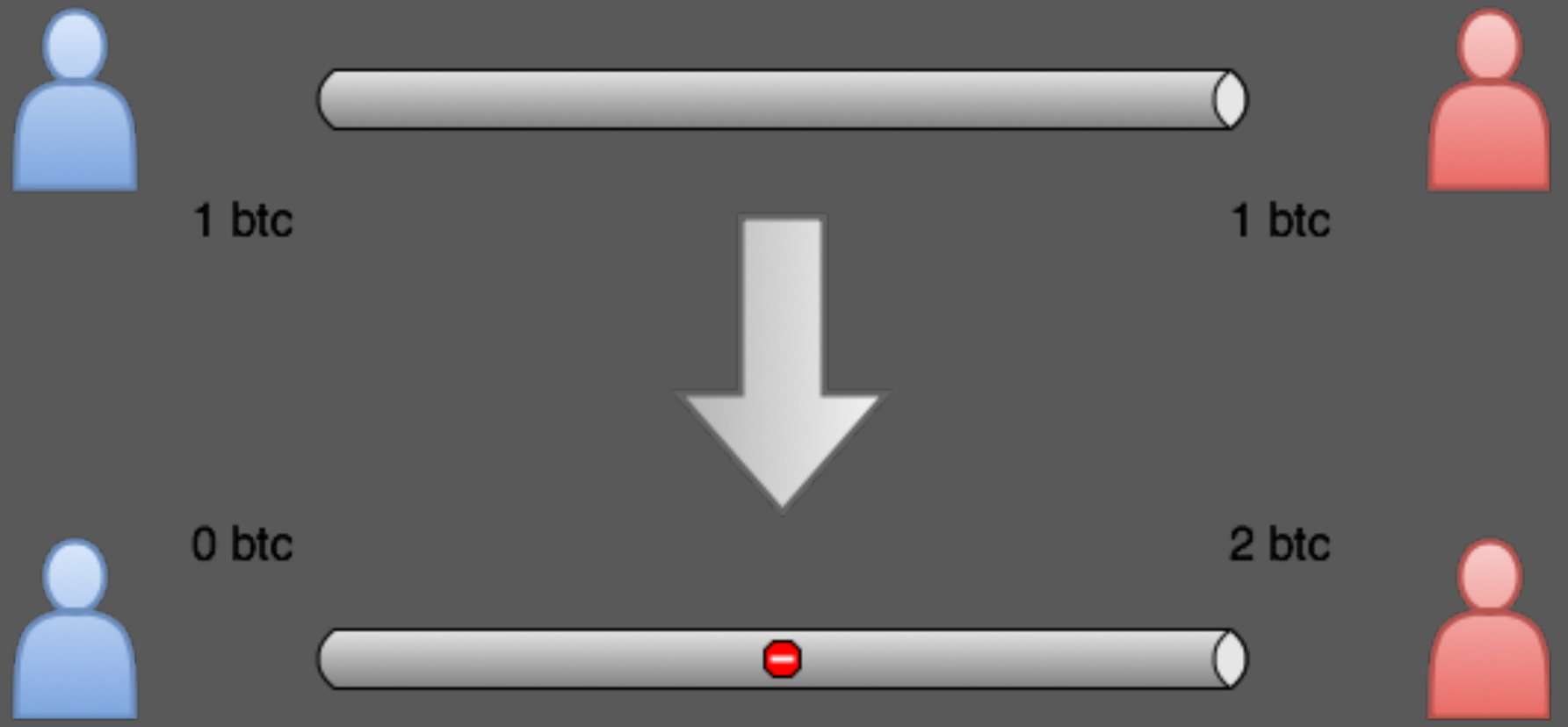
LND Onion Routing



闪电网络

- 方案问题
- 实现问题

Balance Problem



闪电网络

- 链上交易->链下交易
- 减少链上交易数量
- 加速交易进行

闪电网络

- over 1k btc network capacity
- over 8k nodes
- over 38k payment channels

- Q&A