闪电网络的伟大意义

The Significance of the Lightning Network

潘志彪

zhibiao.pan@blockin.com

2018-03

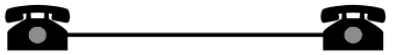
币印

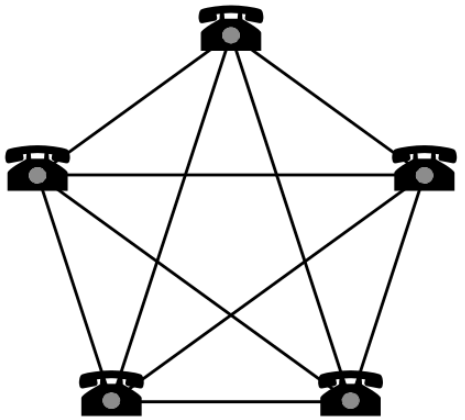
比特币第一优先级 Bitcoin’s first priority

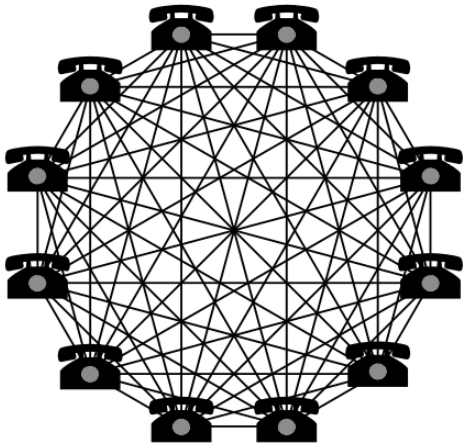
生存 Survive

币印

比特币扩容的挑战 Challenges of scaling







- 梅特卡夫定律 Metcalfe's law
  - 一个网络的价值等于该网络内的节点数的平方，而且该网络的价值与联网的用户数的平方成正比
  - Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2).

币印

比特币扩容的挑战 Challenges of scaling

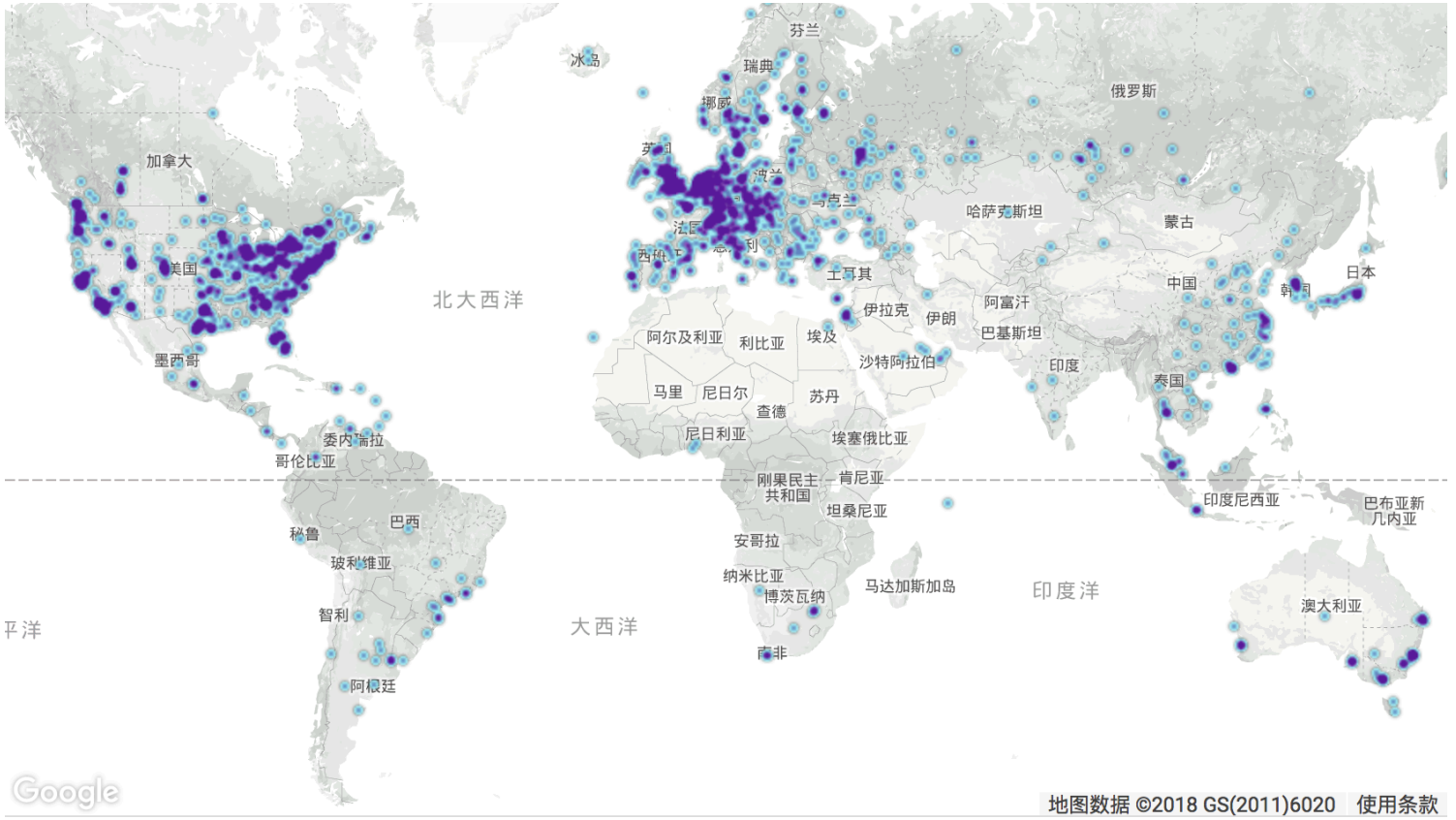
$$V_{Facebook} = 5.70 \times 10^{-9} \times n^2$$

$$V_{Tencent} = 7.39 \times 10^{-9} \times n^2$$

- 梅特卡夫定律延伸
  - 比特币交易数量是超过线性增长的
  - 提升区块大小是带来的空间增长是线性的
  - 线性增长的方案是无法真正解决指数增长的问题的

比特币扩容的挑战 Challenges of scaling

- 节点的意义
  - 制约中心节点
  - Constraining the central node
  - 数据备份：保护系统
  - Backup data



比特币扩容的挑战 Challenges of scaling

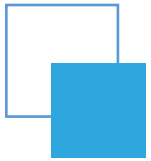
- 区块链的节点并非真正的分布式系统中的协同节点
  - 因需要形成共识：故每个节点必须见证所有数据
  - 节点之间是镜像关系，而非协同关系
  - 单个节点的瓶颈往往是扩容考虑的一个重要因素

比特币扩容的挑战 Challenges of scaling

- 节点的瓶颈
  - 节点 != 服务器，可能是一个可能是多个
    - 分片等扩容方案是针对单个节点而言的
  - 提高10倍区块体积在目前来说可能都是比较困难的
    - 当前交易总量（num of transactions）： 194,450 条
    - 当前区块链大小（Blockchain Size）： 161 GBytes (仅块数据 / only blocks)

分层扩容之路 Road to Multi-layer

- 交易的一些特征
  - 局部性
    - 国家、地区、人群
  - 可重复性
    - 短时期内人际关系是相对固定的
    - 多次交易对象占据一定比例



分层扩容之路 Road to Multi-layer

- 局部化的技术应用
  - CDN，多节点分发，流量地区化
- 交易的局部化场景
  - 同银行转账 -> 跨银行转账 -> 国际汇款

币印

分层扩容之路 Road to Multi-layer

- 分层/多层 Multi Layer
  - 主链作为顶层 Mainchain as the top layer
  - 挑战 Challenges
    - 去信任化 No Trust
    - 去中心化 Decentralized

分层扩容之路 Road to Multi-layer

- 老式通道 Old School Channel
  - 中本聪式 Nakamoto high-frequency transactions
    - Unconfirmed, nLockTime, nSequence
    - 问题 problems： 易被矿工攻击 potential miner attack
  - Spillman-style payment channels / Bitcoinj
    - Multisig / nLockTime
    - 问题 problems：单向的 unidirectional: payer -> payee;

分层扩容之路 Road to Multi-layer

- 闪电通道 LN Channel
  - 双向 bidirectional：双向的才有可能构建出网络 Only bidirectional channels could build network
  - 去信任化 No Trust

分层扩容之路 Road to Multi-layer

- SegWit
  - 带来了扩容效果 increase block limit
  - 解决了延展性问题 fixed malleability issue
    - 无需考虑交易哈希可变问题，简化通道合约技术细节

币印

闪电网络 Lightning Network

- 闪电通道 LN Channel
  - RSMC 序列到期可撤销合约, Revocable Sequence Maturity Contract
  - HTLC 哈希时间锁定合约, Hashed Timelock Contract

币印

闪电网络 Lightning Network

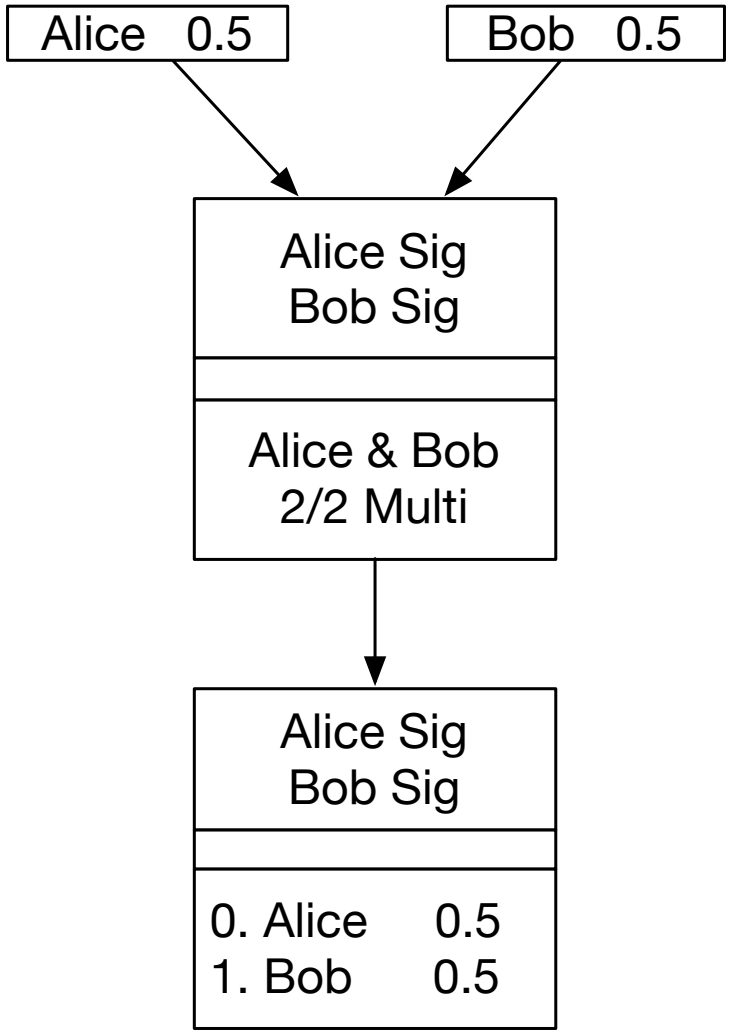
- RSMC 序列到期可撤销合约
  - 解决了通道中币单向流动问题 unidirectional -> bidirectional
  - OP_CSV, OP_ CHECKSEQUENCEVERIFY (Check Sequence Verify)
- HTLC 哈希时间锁定合约
  - 解决了币跨节点传递的问题 payments could cross channels
  - OP_CLTV, OP_CHECKLOCKTIMEVERIFY (Check Lock Time Verify)

闪电网络 Lightning Network

简易通道模型
Simple Channel Model

Funding Tx

broadcast, onchain



Commitment Tx

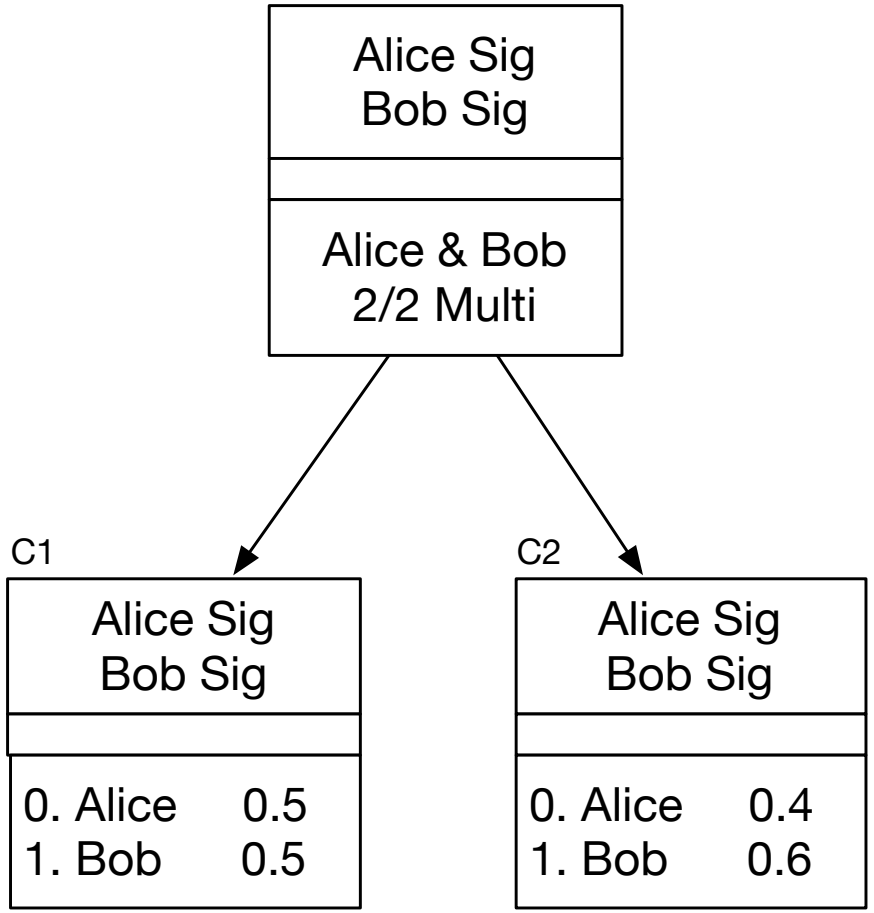
not broadcast, offchain

闪电网络 Lightning Network

简易通道模型
Simple Channel Model

Funding Tx

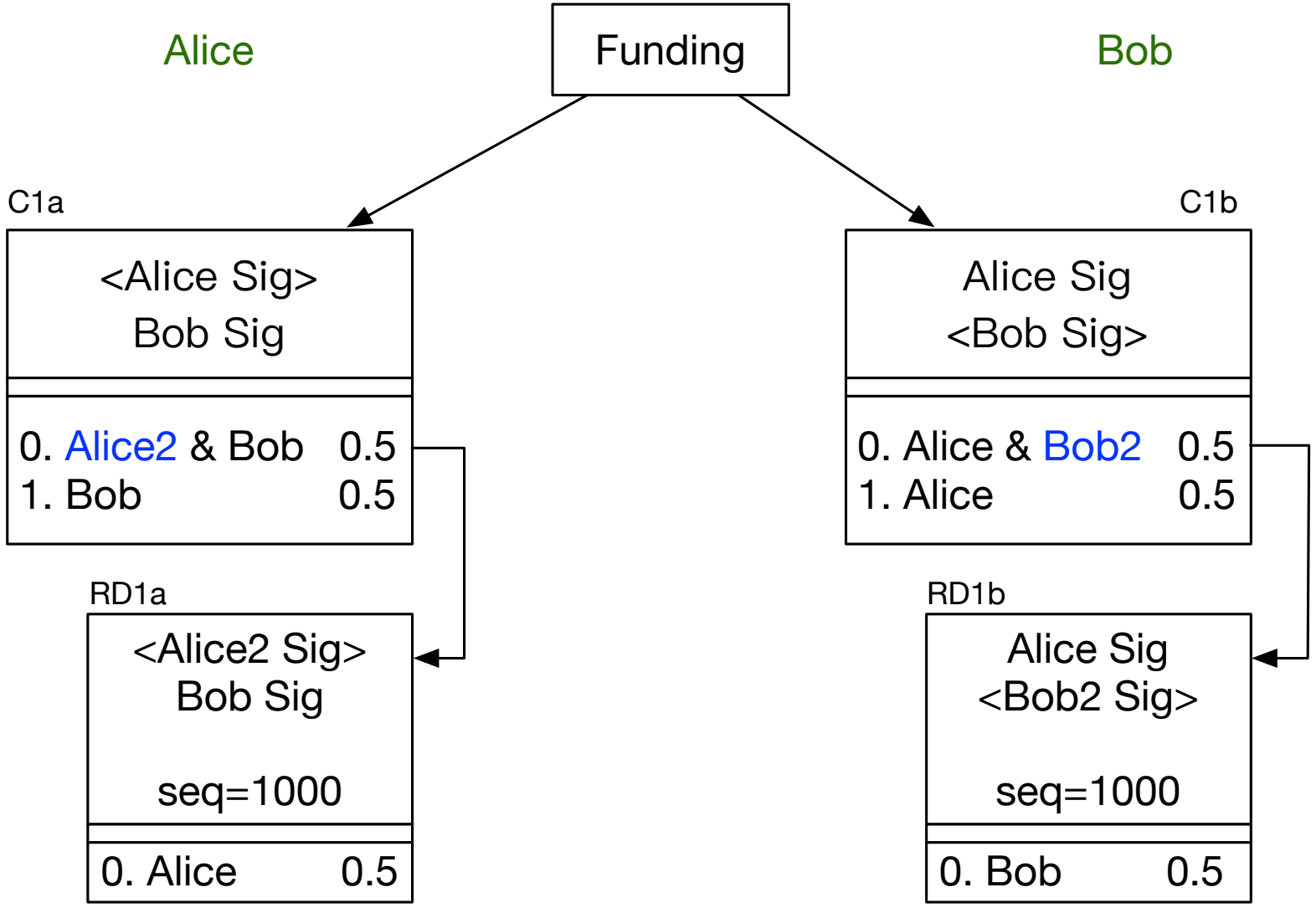
broadcast, onchain



Commitment Tx

not broadcast, offchain

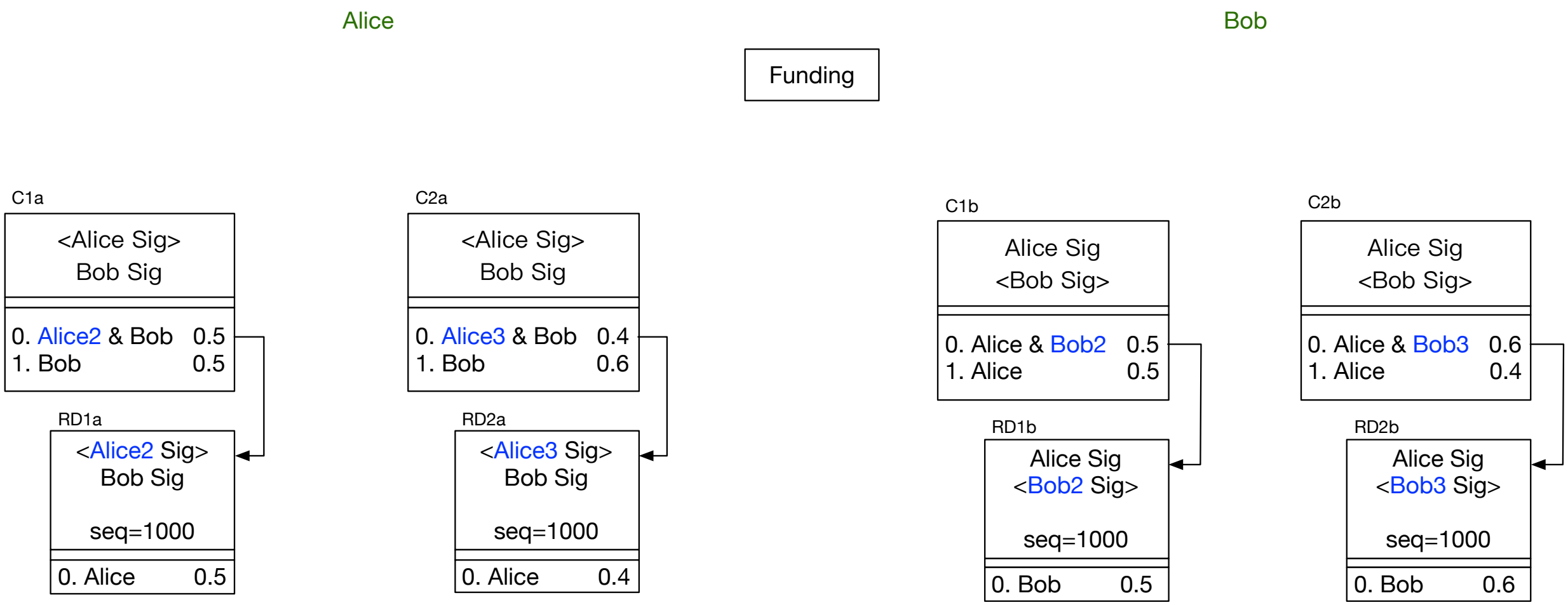
LN - RSMC


Alice
Funding
Bob
C1a
<Alice Sig>
Bob Sig
0. Alice2 & Bob 0.5
1. Bob 0.5
C1b
Alice Sig
<Bob Sig>
0. Alice & Bob2 0.5
1. Alice 0.5
RD1a
<Alice2 Sig>
Bob Sig
seq=1000
0. Alice 0.5
RD1b
Alice Sig
<Bob2 Sig>
seq=1000
0. Bob 0.5

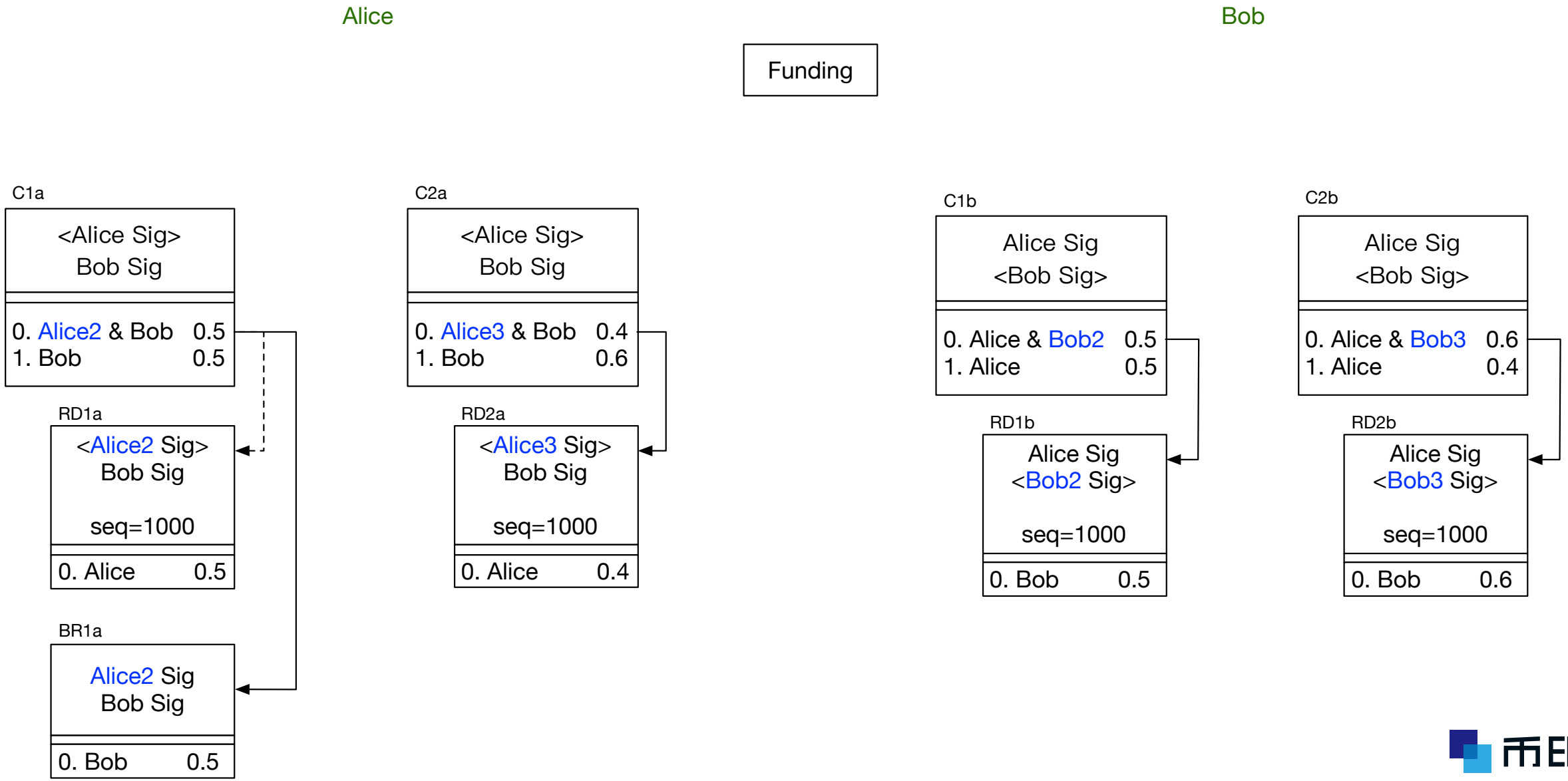
LN - RSMC

- RSMC
  - nSequence 阻止交易确认，形成惩罚窗口期 stop tx confirm, could have time punish the evil guy
  - 交出私钥(或签名放弃），进而废弃上一个状态

LN - RSMC


Alice
Bob
Funding
C1a
<Alice Sig>
Bob Sig
0. Alice2 & Bob 0.5
1. Bob 0.5
RD1a
<Alice2 Sig>
Bob Sig
seq=1000
0. Alice 0.5
C2a
<Alice Sig>
Bob Sig
0. Alice3 & Bob 0.4
1. Bob 0.6
RD2a
<Alice3 Sig>
Bob Sig
seq=1000
0. Alice 0.4
C1b
Alice Sig
<Bob Sig>
0. Alice & Bob2 0.5
1. Alice 0.5
RD1b
Alice Sig
<Bob2 Sig>
seq=1000
0. Bob 0.5
C2b
Alice Sig
<Bob Sig>
0. Alice & Bob3 0.6
1. Alice 0.4
RD2b
Alice Sig
<Bob3 Sig>
seq=1000
0. Bob 0.6

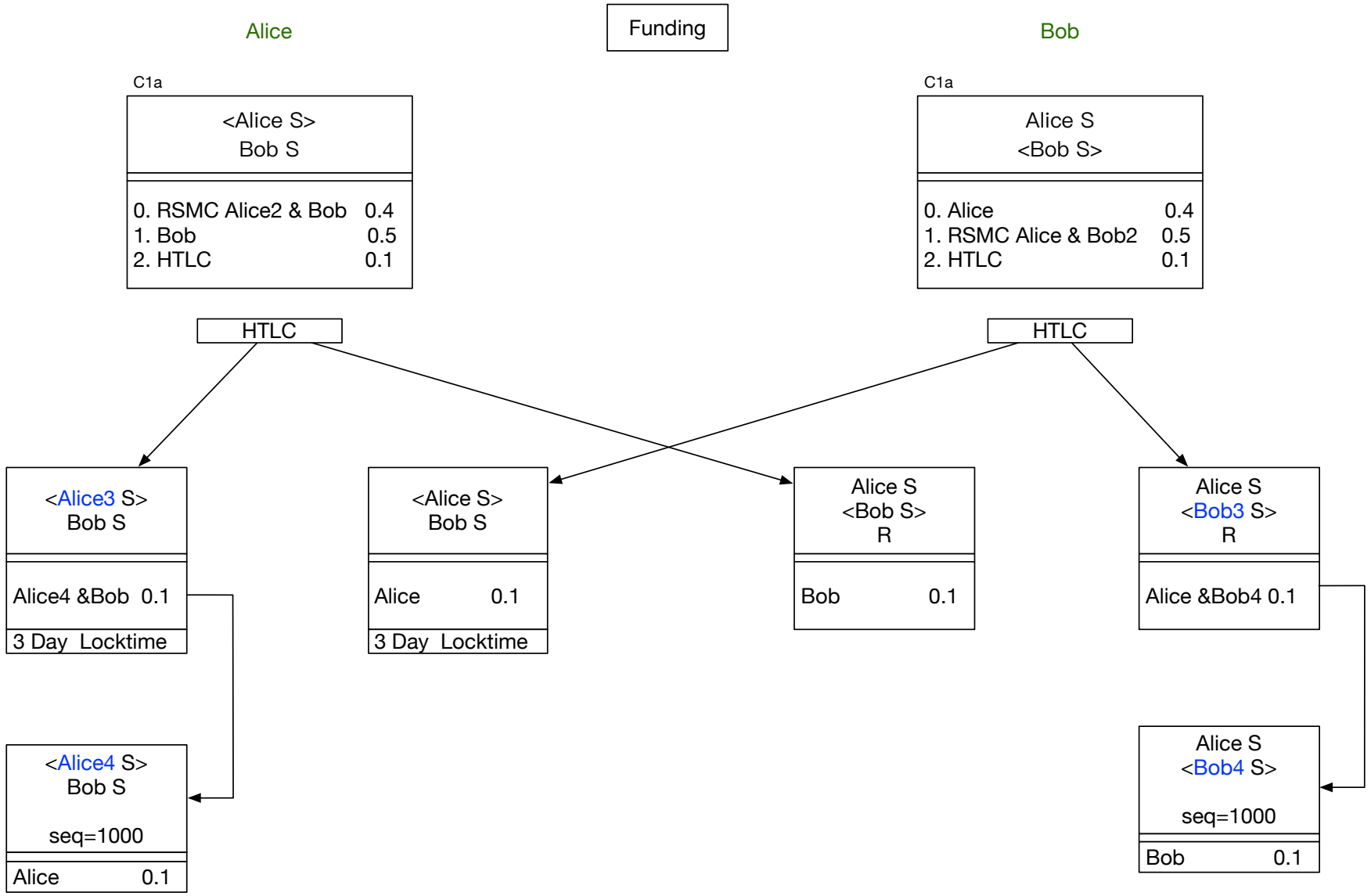
LN - RSMC


Alice
Bob
Funding
C1a
<Alice Sig>
Bob Sig
0. Alice2 & Bob 0.5
1. Bob 0.5
RD1a
<Alice2 Sig>
Bob Sig
seq=1000
0. Alice 0.5
BR1a
Alice2 Sig
Bob Sig
0. Bob 0.5
C2a
<Alice Sig>
Bob Sig
0. Alice3 & Bob 0.4
1. Bob 0.6
RD2a
<Alice3 Sig>
Bob Sig
seq=1000
0. Alice 0.4
C1b
Alice Sig
<Bob Sig>
0. Alice & Bob2 0.5
1. Alice 0.5
RD1b
Alice Sig
<Bob2 Sig>
seq=1000
0. Bob 0.5
C2b
Alice Sig
<Bob Sig>
0. Alice & Bob3 0.6
1. Alice 0.4
RD2b
Alice Sig
<Bob3 Sig>
seq=1000
0. Bob 0.6

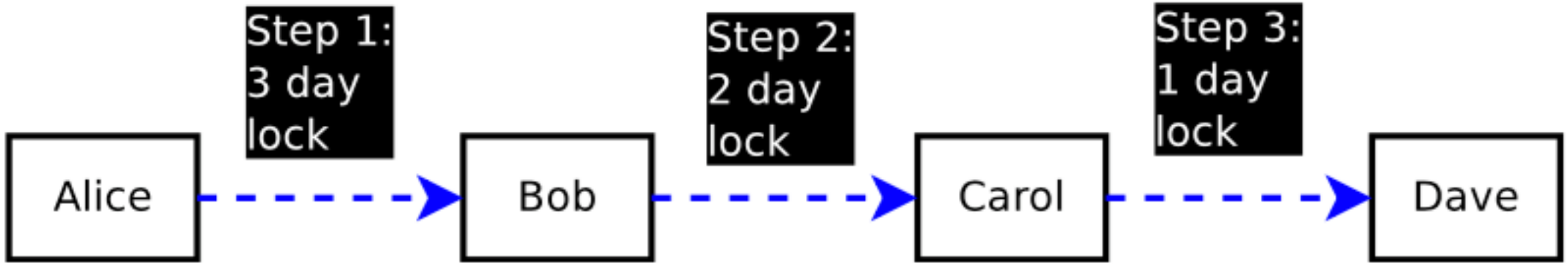
LN - HTLC

```
OP_IF
    OP_HASH160 <Hash160(R)> OP_EQUALVERIFY
    2 <Alice1> <Bob1> OP_CHECKMULTISIG
OP_ELSE
    2 <Alice2> <Bob2> OP_CHECKMULTISIG
OP_ENDIF
```

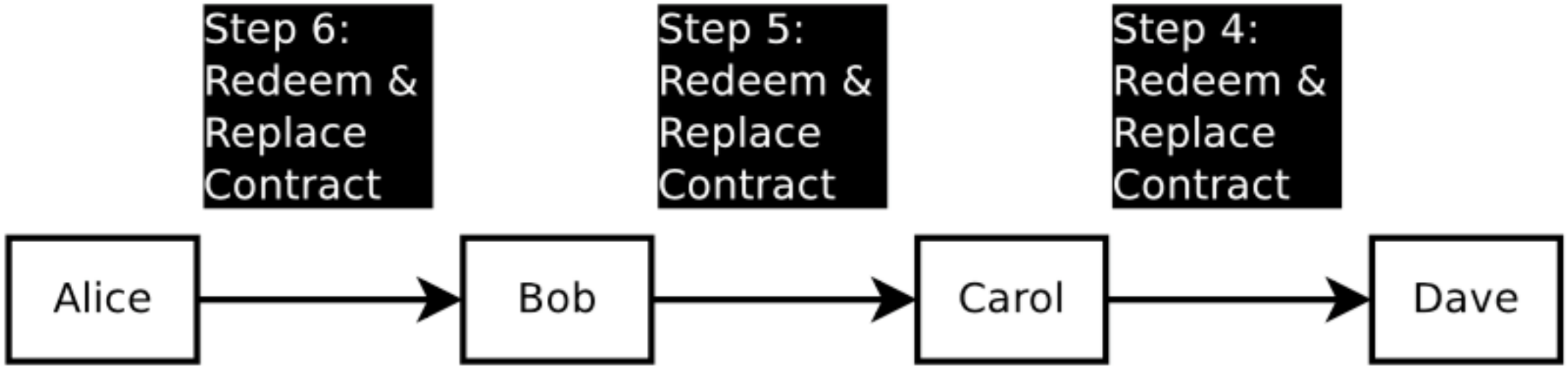
LN - HTLC


Alice
Funding
Bob
C1a
<Alice S>
Bob S
0. RSMC Alice2 & Bob 0.4
1. Bob 0.5
2. HTLC 0.1
C1a
Alice S
<Bob S>
0. Alice 0.4
1. RSMC Alice & Bob2 0.5
2. HTLC 0.1
HTLC
HTLC
<Alice3 S>
Bob S
Alice4 &Bob 0.1
3 Day Locktime
<Alice S>
Bob S
Alice 0.1
3 Day Locktime
Alice S
<Bob S>
R
Bob 0.1
Alice S
<Bob3 S>
R
Alice &Bob4 0.1
<Alice4 S>
Bob S
seq=1000
Alice 0.1
Alice S
<Bob4 S>
seq=1000
Bob 0.1

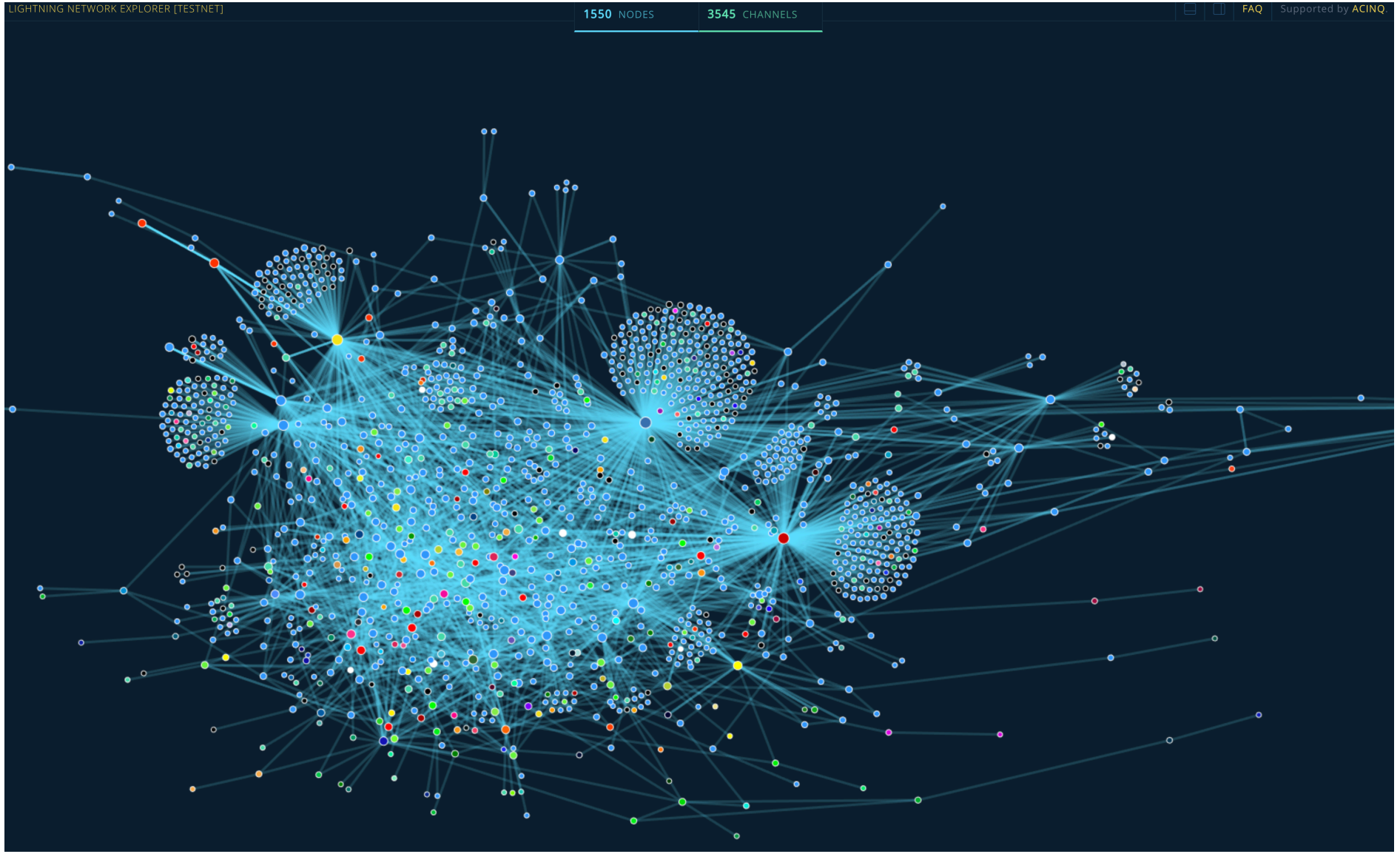
LN - HTLC


Step 1:
3 day
lock
Step 2:
2 day
lock
Step 3:
1 day
lock
Alice
Bob
Carol
Dave

LN - HTLC


Step 6:
Redeem &
Replace
Contract
Step 5:
Redeem &
Replace
Contract
Step 4:
Redeem &
Replace
Contract
Alice
Bob
Carol
Dave

闪电网络 Lightning Network



闪电网络 Lightning Network

- 闪电网络特征
  - 去信任，去第三方 no trust, no third party
  - 几乎可以无限扩容 almost scale unlimited (funding/commitment txs still limited by mainchain)
    - 高性能 High performance
  - 完全兼容，LN网络中的交易与主链交易完全一致 ln's tx = mainchain tx
  - 低成本 low cost, low fee
    - 实时/小额支付 Instant/micro payments

闪电网络 Lightning Network

- 闪电网络是否中心化?
  - 代码开源、社区管理，无垄断技术/专利
  - 进入门槛相对较低，自由竞争市场

谢谢
THANKS

币印

招贤纳士 Join us

币印