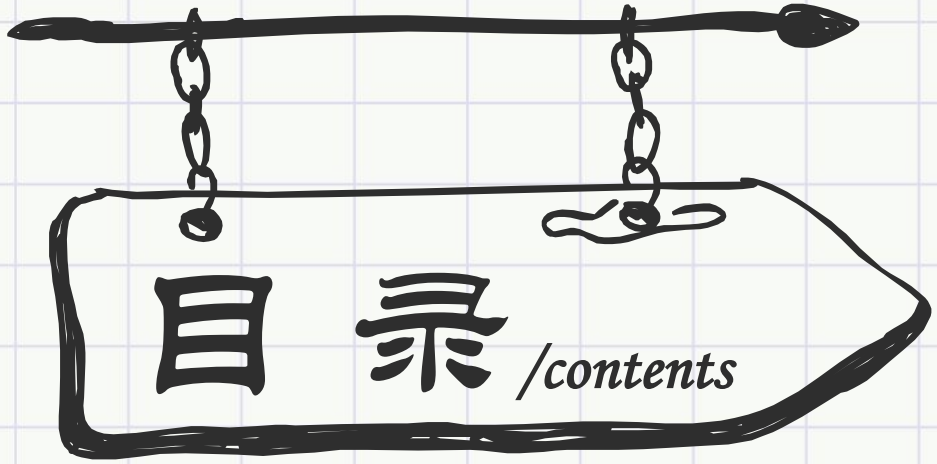
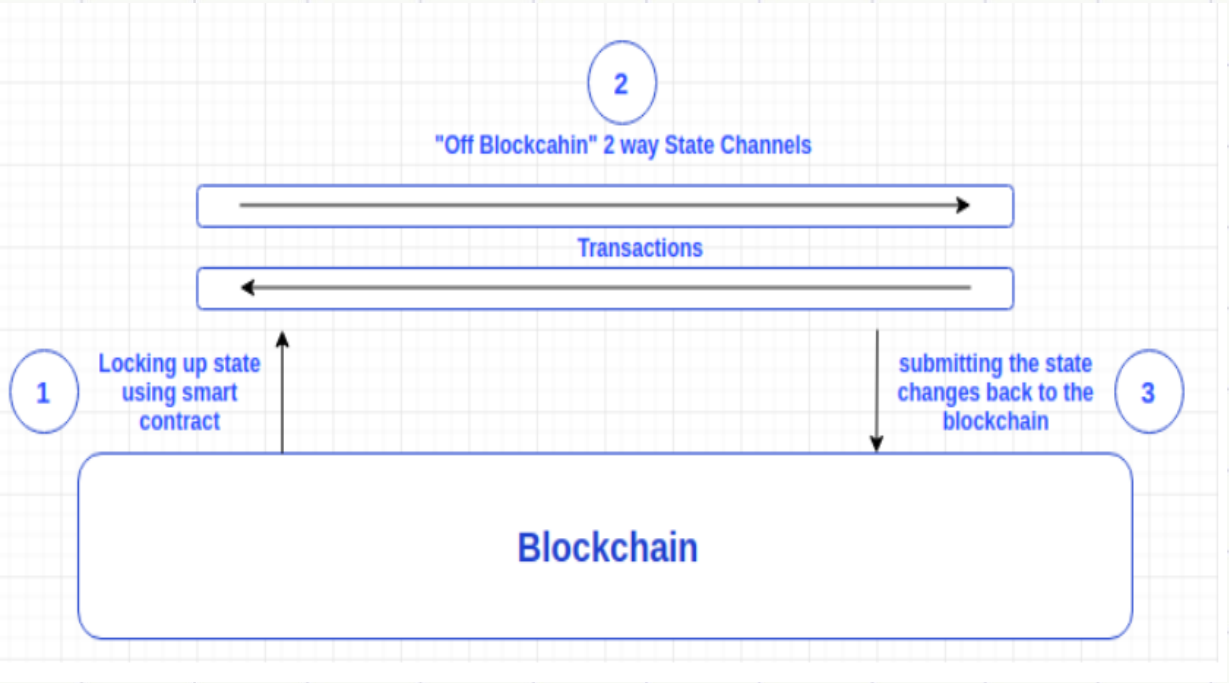
状态通道与闪电网络

俱乐部技术分享

Lightning Network



什么是状态通道



1

区块链的部分状态通过多个签名和部分智能合约锁定

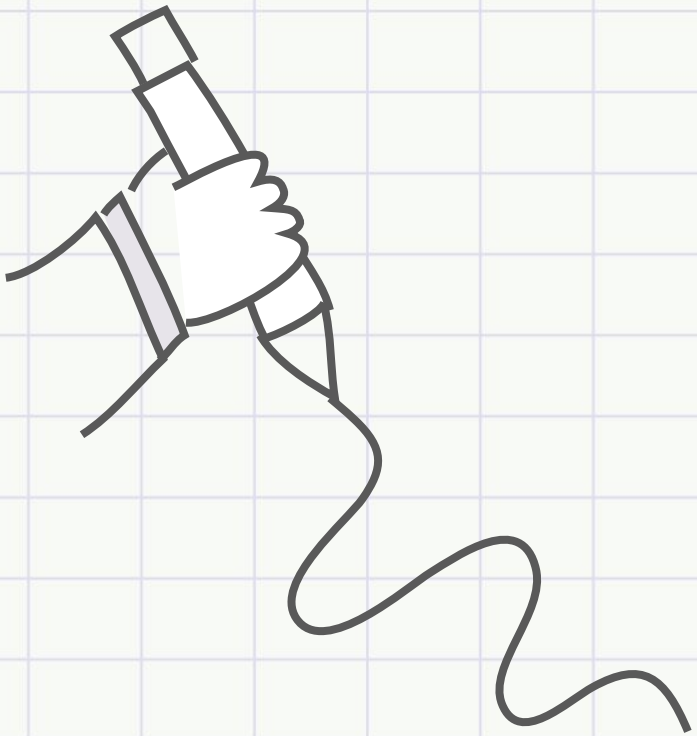
2

参与者通过产生以及签名来时时更新状态

3

参与者将状态传回到区块链上，然后关闭状态通道，并且再次锁定状态

状态通道的概念



状态通道的核心就是上述那种架构设计

状态通道一般被视为layer 2层（可拓展层），链上为layer 1层（安全层）

状态通道的组成：

- 多签钱包或者智能合约
- 互相构建和签署交易，相互更新状态
- 提交区块链，关闭通道

状态通道的类型

特殊状态通道

- 支付通道
- App定制型

通用状态通道

- 反事实实例化

1 支付通道

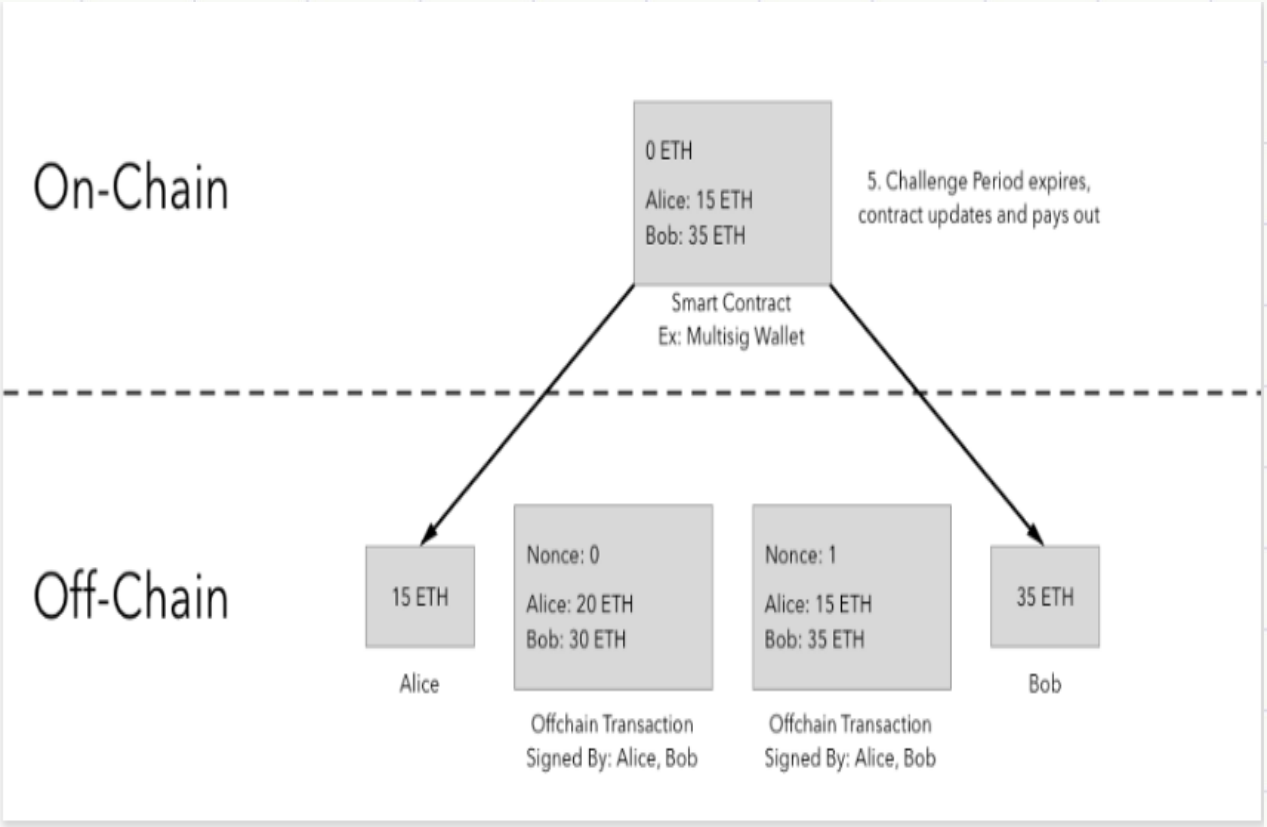
支付通道的由来

BTC

链上交易的缺陷：

- 交易费用高
- 速度慢
- 效率低

什么是支付通道



01

打开通道：

链上锁定状态，建立合约

02

链下交易：

频繁双向支付交易

03

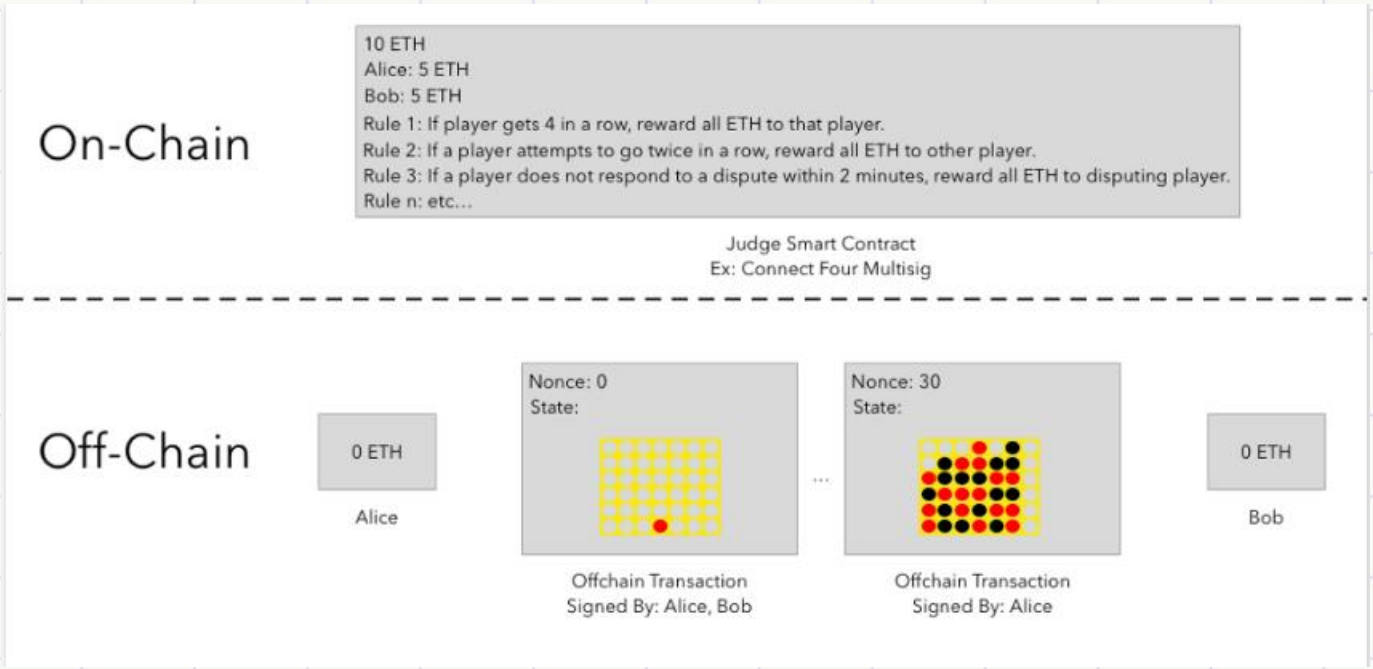
关闭通道：

向链上提交状态，并进行争议性解决

样例： https://ethfans.org/posts/counterfactual-for-dummies-part-1

2 APP定制通道

定制型状态通道



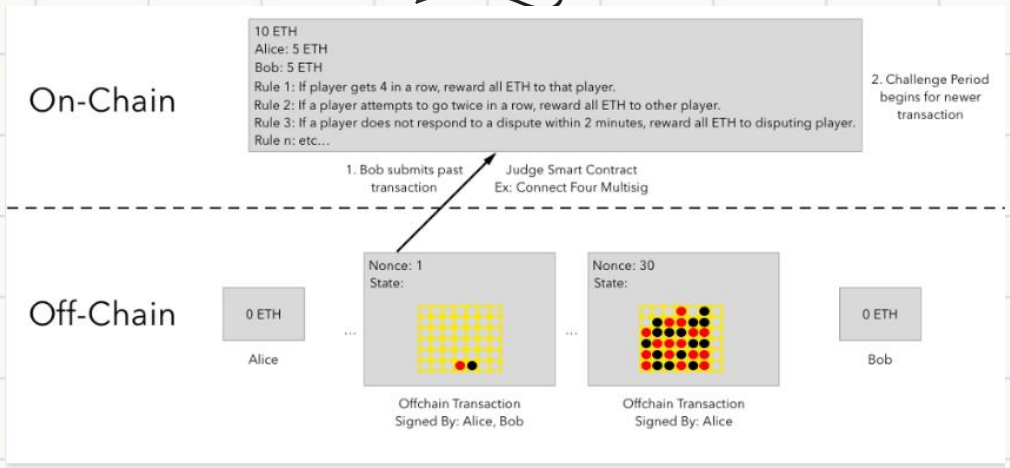
法官职责：

- 在比赛期间持有游戏资金
- 作为游戏规则的真相来源，解决玩家纠纷（例如：欺骗，拖延）
- 在某一方赢或双方平局的情况下适当分配资金

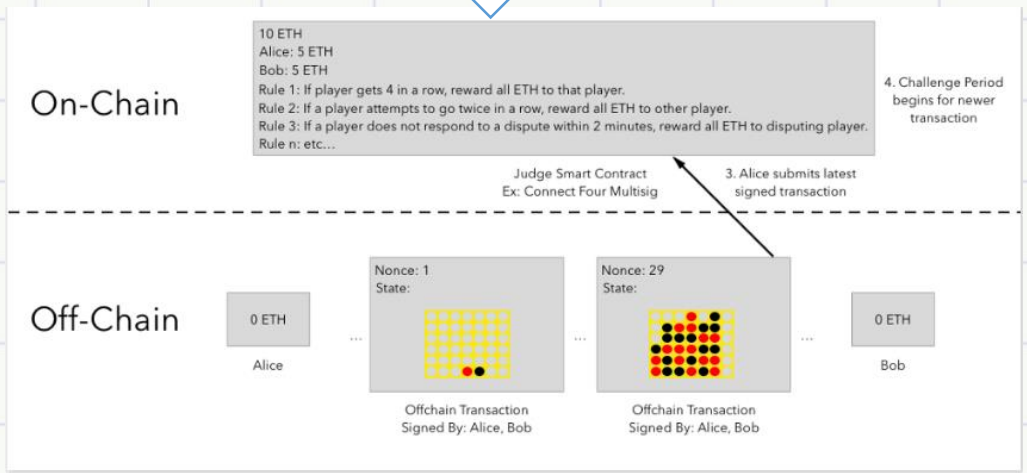
游戏规则：

- Rule 1: …
- Rule 2: …
- Rule 3: …
- Rule 4: …

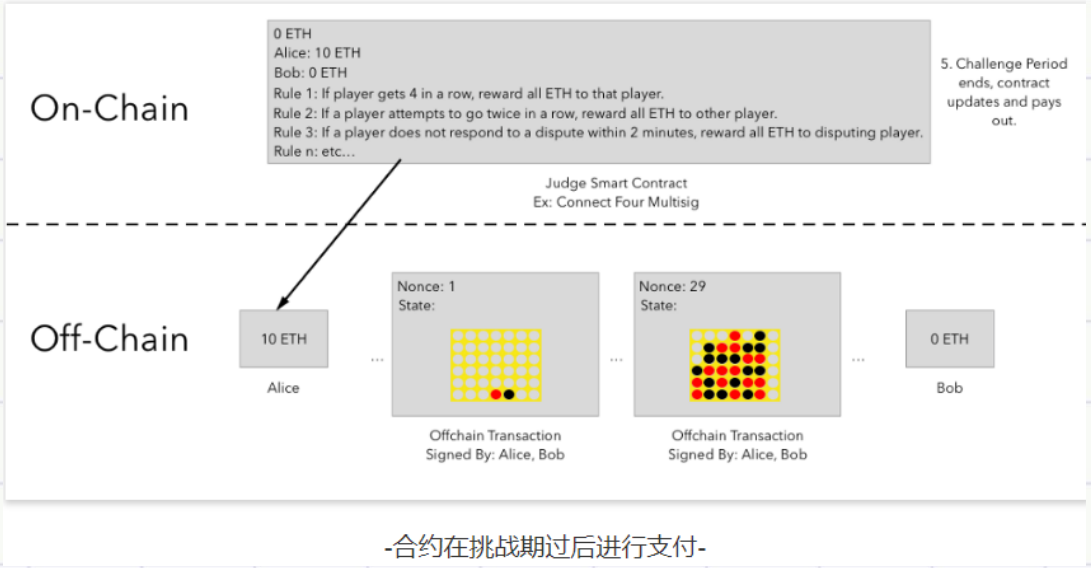
防作弊手段



- Bob 试图提交一个旧交易-



- Alice 提交一个双方都签署的新的交易-



-合约在挑战期过后进行支付-

参考：https://ethfans.org/posts/state-channel-for-dummies-part-2

3 闪电网络

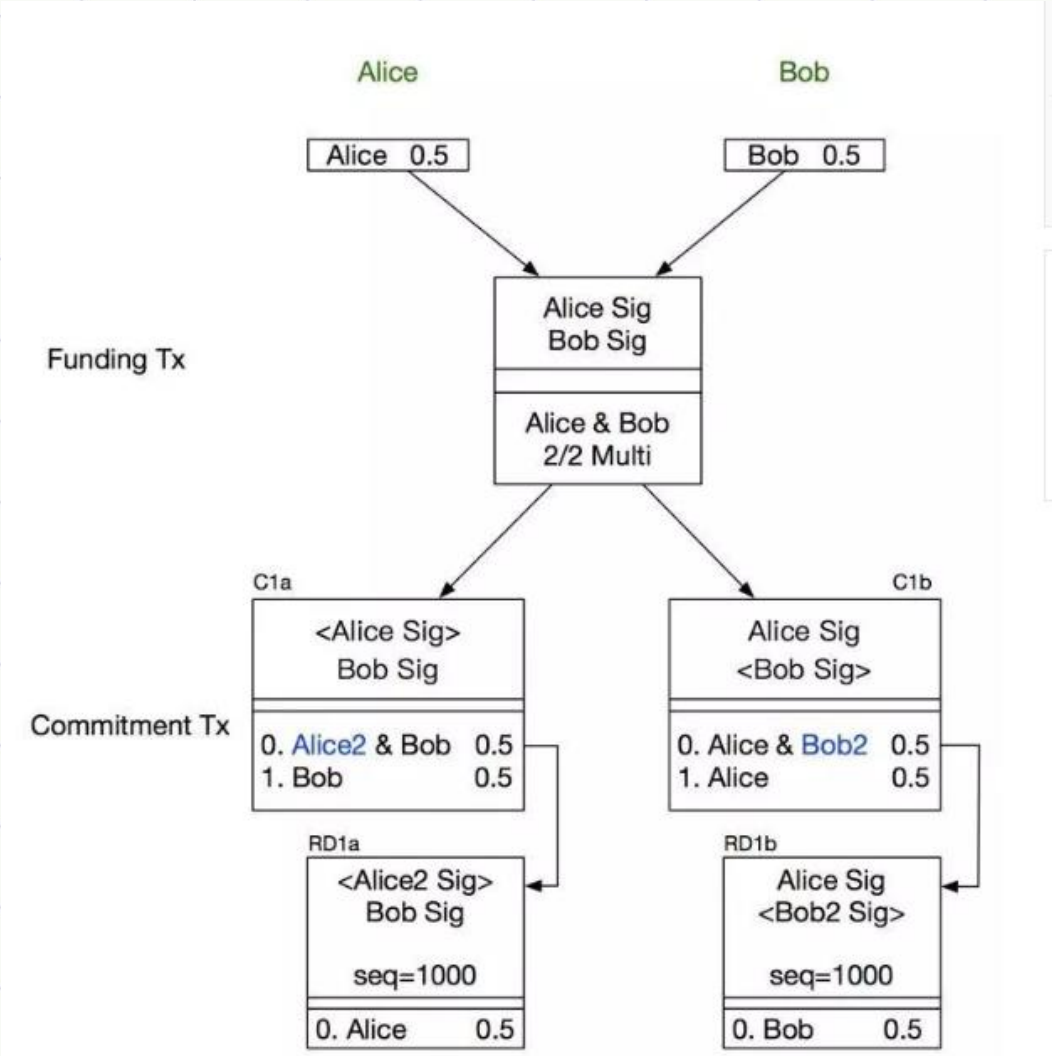
什么是闪电网络

BTC

闪电网络就是支付状态通道的应用，核心交易类型有两种：

- RSMC （序列到期可撤销合约）
- HTLC （哈希时间锁定合约）

RSMC



交易结构图：

1、双方各拿出0.5BTC，构建Funding Tx，输出为爱丽丝和鲍伯的2/2多重签名。此时， Funding Tx未签名，更不广播。

2、爱丽丝构造Commitment Tx：C1a和RD1a，并交给鲍伯签名。C1a的第一个输出为多重签名地址，爱丽丝的另一把私钥爱丽丝2和鲍伯的2/2多重签名，第二个输出为鲍伯 0.5BTC。

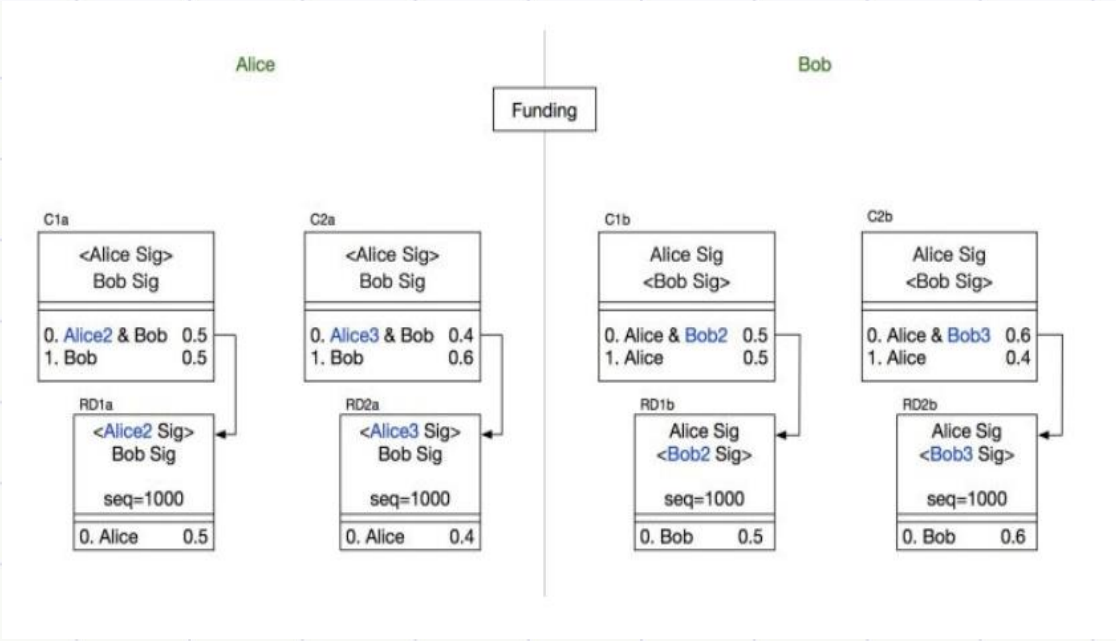
3、 RD1a为C1a第一个输出的花费交易，输出给爱丽丝0.5BTC，但此类型交易带有sequence，作用是阻止当前交易进块，只有前向交易有sequence个确认时才能进块。

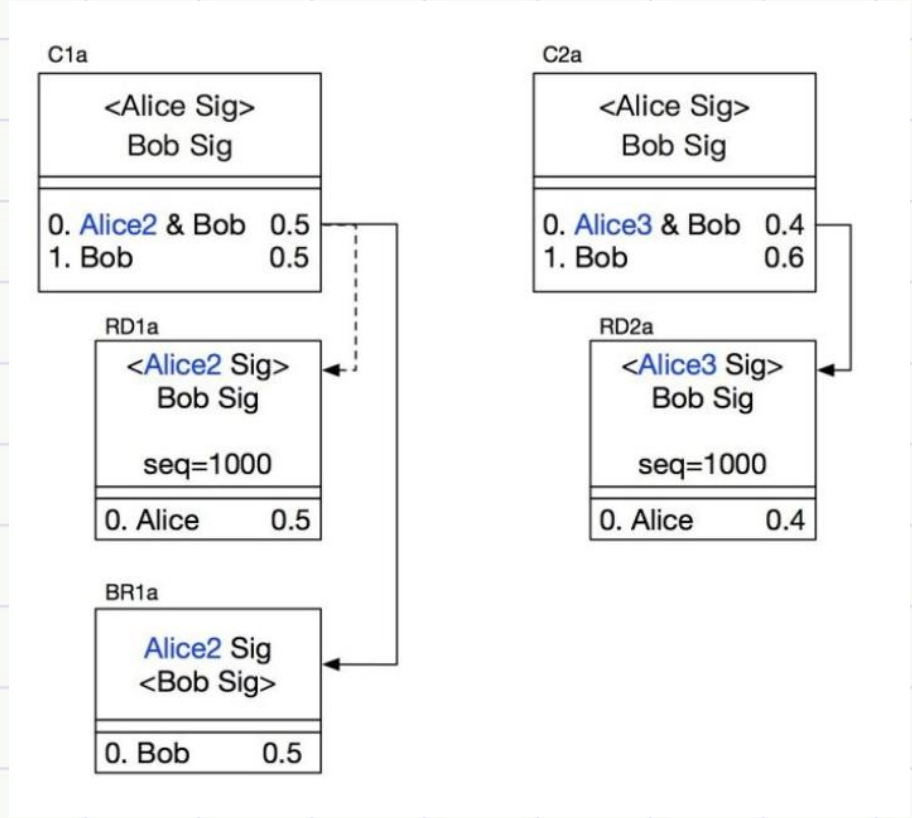
4、鲍伯构造Commitment Tx：C1b和RD1b，并交给爱丽丝签名。结构与C1a、RD1a是对称关系。

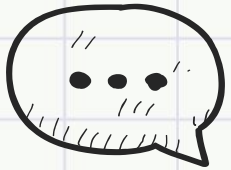
5、鲍伯对C1a和RD1a进行签名，并将签名给爱丽丝；同理，爱丽丝对C1b和RD1b签名，完成后给鲍伯。此时，由于并未对Funding Tx进行签名，任何一方均无法作恶，任何一方也不会有任何损失。

6、双方均完成对commitment Tx的签名并交换后，各自再对Funding Tx进行签名，并交换。此时，Funding Tx是完整的交易，广播之

RSMC







交易更新：

1. 如何才能彻底废弃掉C1a和C1b?
2. 爱丽丝交出爱丽丝2的私钥给鲍伯，即意味放弃C1a，而仅能认可C2a
3. 爱丽丝破坏合约存在C2a的情况下依然广播出C1a,那么鲍伯就可以修改RD1a的输出给他自己，形成新的交易BR1a。 BR1a由于没有Sequence，肯定会先于RD1a执行那么爱丽丝的惩罚就是失去她全部的币

其他参考：
https://www.jianshu.com/p/e326802294e1
https://blog.csdn.net/chunlongyu/article/details/80354563

防作弊机制

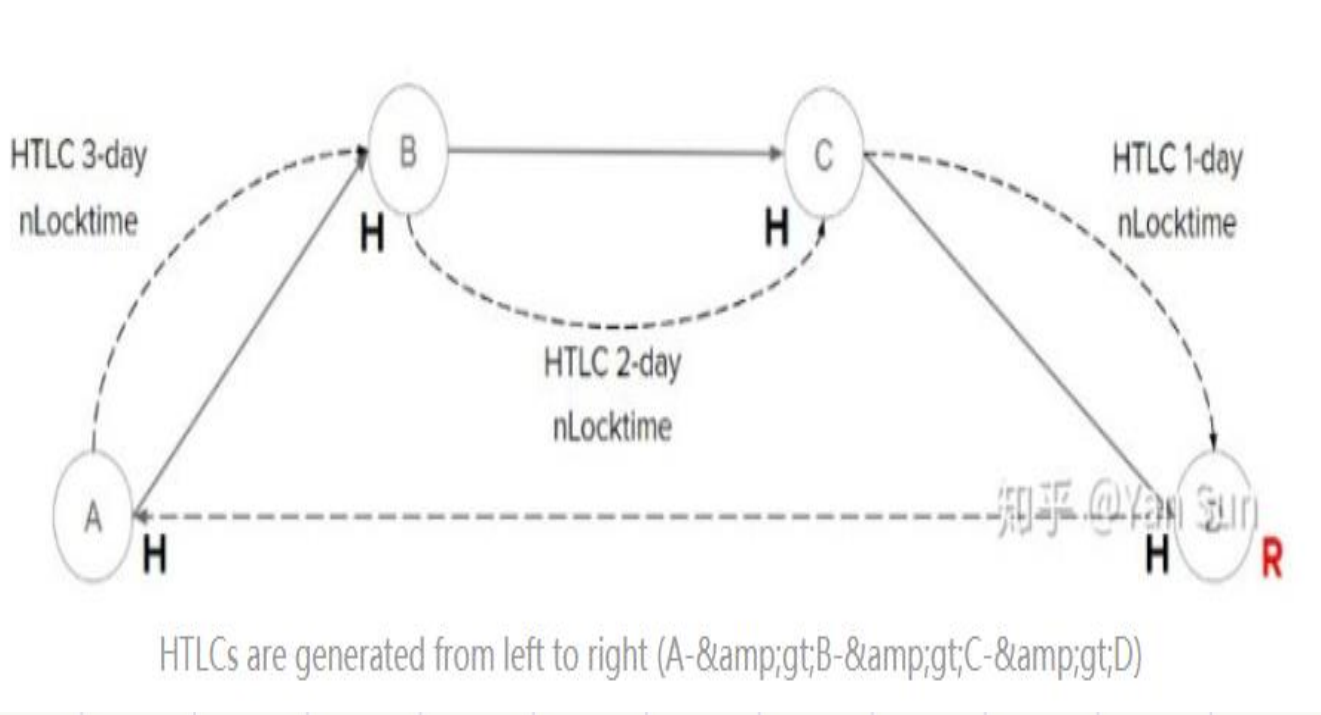
引入第三方来解决“始终在线”的假设

闪电网络“监视器”/“瞭望塔”

Pisa“保管人（Custodians）”

Celer“状态防卫网络”

HTLC



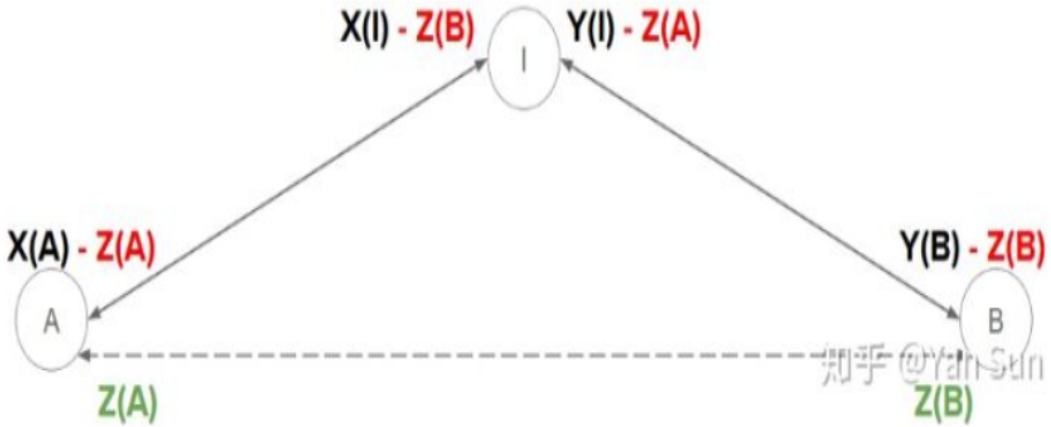
交易结构图：

- 如果Alice和Bob之间建立一个通道，Bob和Charlie之间建立一个通道，同时Charlie和Dave之间也建立了一个通道，那么Alice可以通过Charlie和Bob把她的付款转给Dave。为了在不引入额信任假设，Alice需要确保Bob或Charlie不会带着她的钱跑路。这个攻击向量可以通过HTLCs来解决，交易最终遵循一个多步骤的过程来完成。

- 在这个模型中，Dave生成了一个随机数R作为原像，并将该原像的哈希值H共享给Alice。然后Alice就和Bob就达成了一个HTLC——“如果你告诉我H对应的原像R，我将支付你1比特币，但如果你三天内不给我看原像，我将收回我的1比特币”。然后Bob与Charlie达成一个类似的HTLC，不同之处在于它将在两天后退还这1个比特币。类似地，Charlie与Dave达成一个HTLC，同样其退款周期更短。

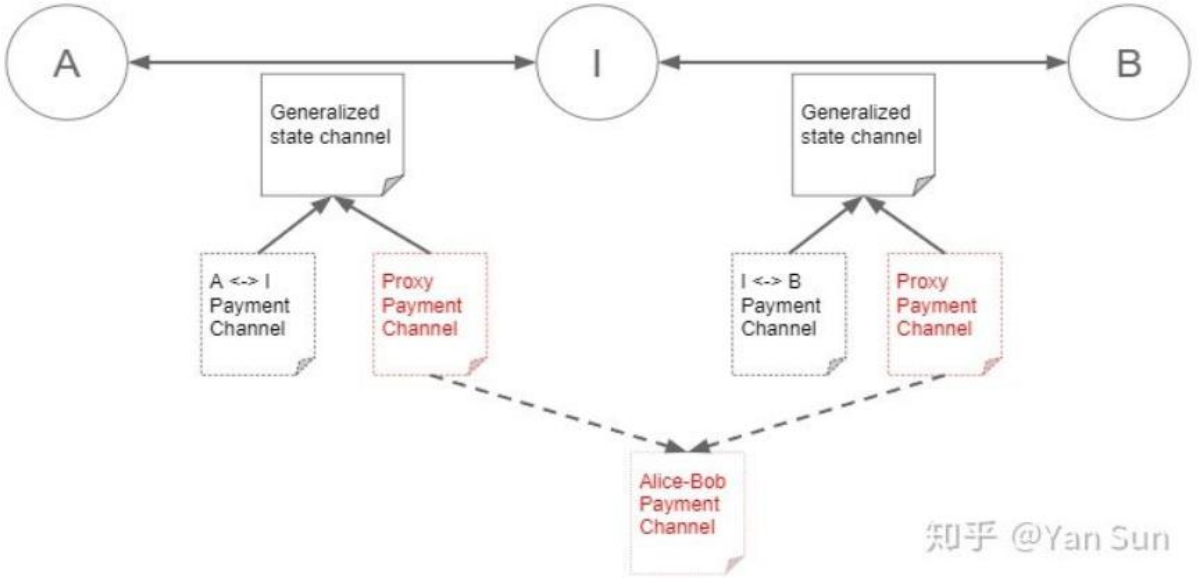
拓展

通过“虚拟通道”路由



Z(A) and Z(B) become the balances in Alice’ s and Bob’ s virtual channel (dotted line), respectively.

通过“元通道（Meta Channels）”路由



参考：https://zhuanlan.zhihu.com/p/53953613

比较

闪电网络

- **安全性：**
绝对安全，不存在资金冻结等风险
- **支付速度：**
除上链确认操作外，其交易速度几乎与支付宝等价
- **隐私程度：**
线下足够隐私
- **风险：**
无法复原

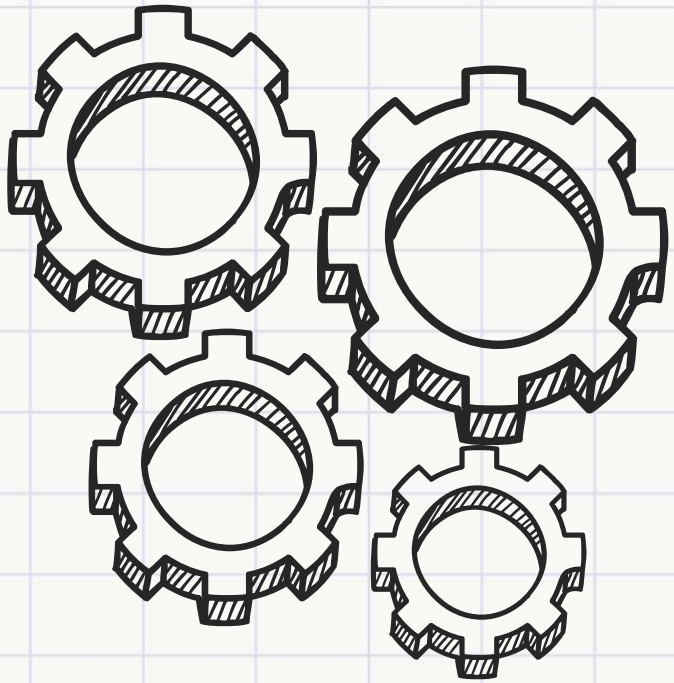
支付宝

- **安全性：**
依赖于其商业信用和规模，资金受法律监管
- **支付速度：**
秒速
- **隐私程度：**
依赖第三方
- **风险：**
较小，可中心化恢复

闪电网络的优缺点

优点：

- 快速支付
- 无需可信第三方
- 为区块链减负
- 支付通道可以无限期地保持开放
- 双方约定可快速关闭通道
- 洋葱式路由
- 具有多重签名功能
- 跨链



缺陷：

- 收款时要求必须在线，没有离线付款
- 监控通道的需求
- 匹配失败
- 对于大额付款并不理想
- 集中化

4 实操

环境部署介绍

BTC

bitcoin节点：
- bitcoind
- btcd
- neutrino

Lightning Network

三个版本：
- c-lightning
- lnd
- Éclair钱包

测试链支付操作

1. **环境：**
   Bitcoin 测试链全节点
   c-lightning 版本闪电网络
2. **操作指令：**
   i) 启动比特币节点和闪电网络
   bicoind –daemon –testnet
   lightning –-network=testnet –log-level=debug
   ii) 创建通道

   iii) 转账与状态更新

   iiii) 关闭通道

参考：

- https://www.8btc.com/article/156211

感谢在座各位聆听

Thanks for your listening!