比特币热点问题
Bitcoin Technology

北京交通大学
计算机与信息技术学院
信息安全系

李超 (li.chao@bjtu.edu.cn)
段莉 (duanli@bjtu.edu.cn)

目录

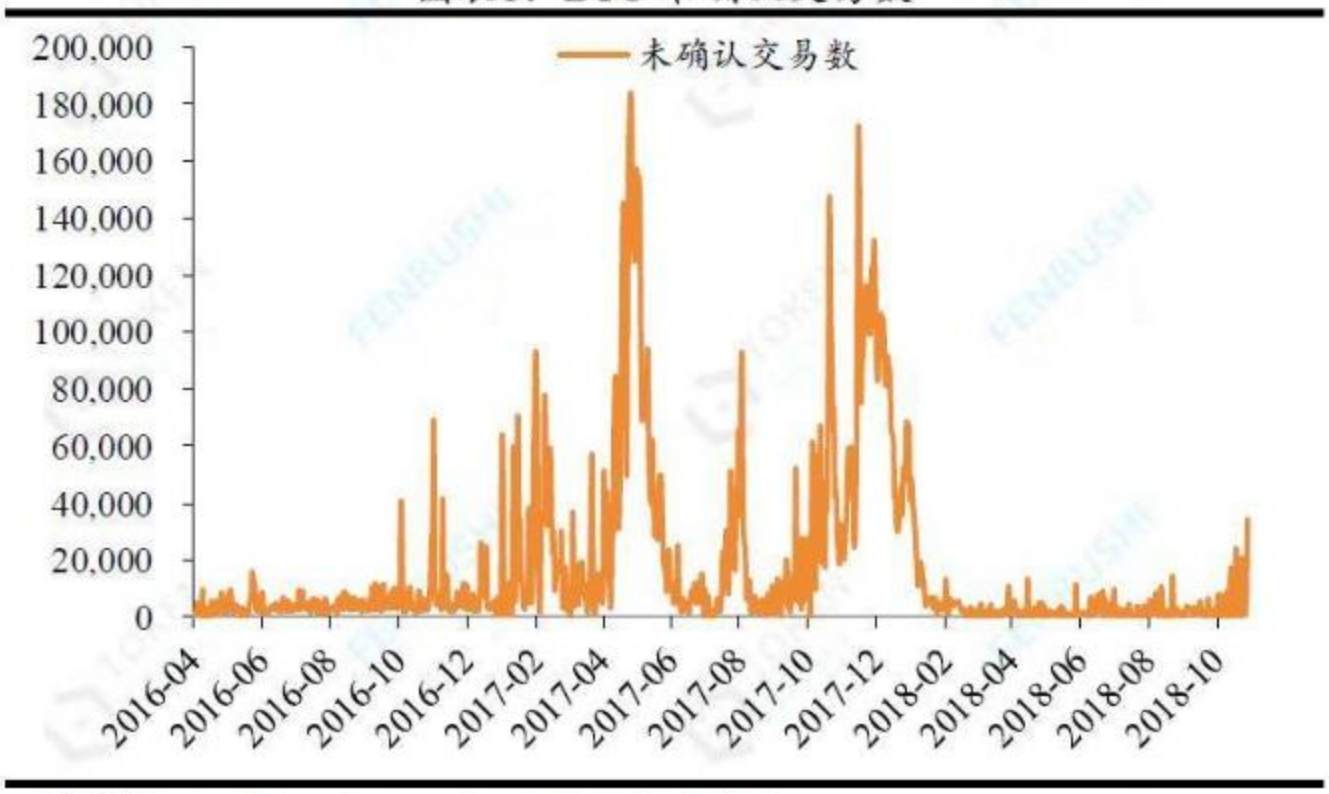
Contents

比特币交易问题

- 交易网络可扩展性过低
  - 交易速度慢（需要很长时间处理）
  - 交易量小
  - 交易费用偏高（不支持小额支付）

拥堵的区块链

图表1：BTC 未确认交易数



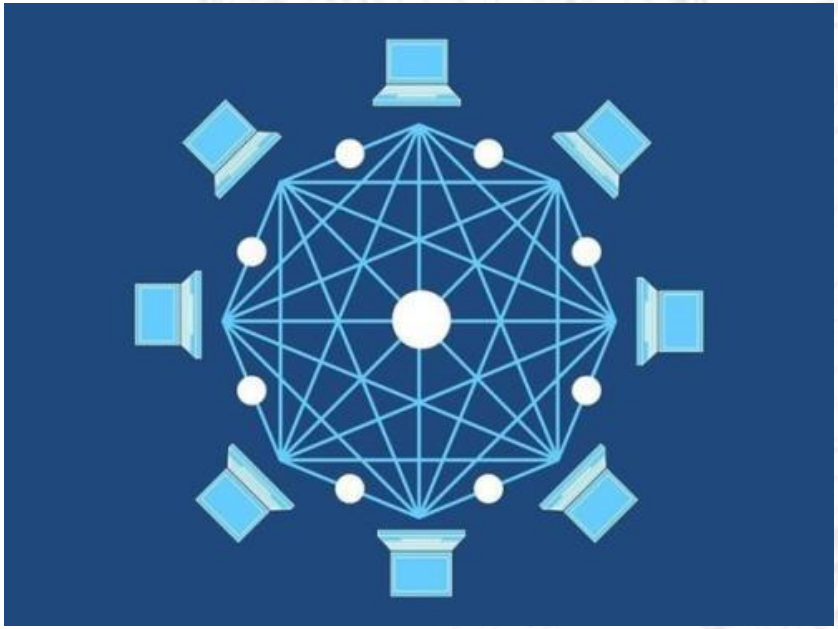
资料来源：Blockchain.info，通证通研究院

- 区块链领域的扩容：围绕如何在“更短的时间实现更多的交易”，增强区块链的可扩展性（scalability）。

可扩展性问题

- 可扩展性是一种对软件系统计算处理能力的设计指标
- 延迟和吞吐量是衡量可扩展性的一对指标，我们希望获得低延迟和高吞吐量的系统架构
- 可扩展性目标：用可接受的延迟获得最大吞吐量

◆低延迟：用户能感受到的系统响应时间短



◆吞吐量：同时多少用户能够享受到这种低延迟

设计中的权衡

比特币在安全与效率上的折衷是拥堵的原因

- 区块容量：更大的区块容量可以带来更高的交易吞吐率，但会增加挖矿成本，带来中心化的风险，同时增大存储的代价。兼顾多方面的考虑，当前的区块容量上限设定为1MB。
- 出块间隔时间：更短的出块间隔可以缩短交易确认的时间，但也可能导致分叉增多，降低网络可用性。
- 脚本支持程度：更强大的脚本指令集可以带来更多的灵活性，但也会引入更多的安全风险。

如何解决可扩展性问题

- 链上扩容
  - 增加区块容量
  - 隔离见证
- 链下扩容
  - 闪电网络
  - 侧链

链上扩容

- 通过优化、改进比特币基本协议提升扩展性

- **扩块**
  增加区块大小
- **隔离见证SegWit**
  改进区块结构
- **分片Sharding**
  改进网络验证方式

扩块

类似于汽车多了一层，变成双层巴士

TPS = transactions / block_time

- transactions 由区块大小和平均每笔交易大小决定。
- 直接增大区块容量可以提高TPS。

优点

- 方案简单，技术风险小
- 实施周期短

缺点

- 扩容效果不明显
- 未来系统容量上升空间较低
- 无限制的区块扩容会损害比特币的去中心性

扩块

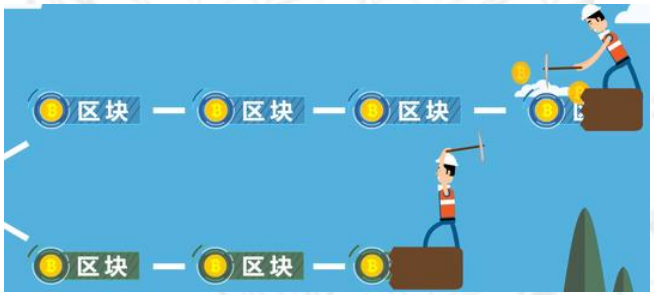
- 比特现金BCH（也称BCC）

- BTC在2017/08/01 硬分叉成两个独立的比特币（BTC）和比特币现金（BCH）。
- 比特币现金（BCH） 的区块大小为8MB，去掉了对隔离见证的支持。
- 比特现金的系统容量相对比特币提升了8倍。

分叉

- 分叉：对区块链的共识规则做一些改变
  - 硬分叉：共识规则改变无法向前兼容，旧节点无法认可新节点产生的区块

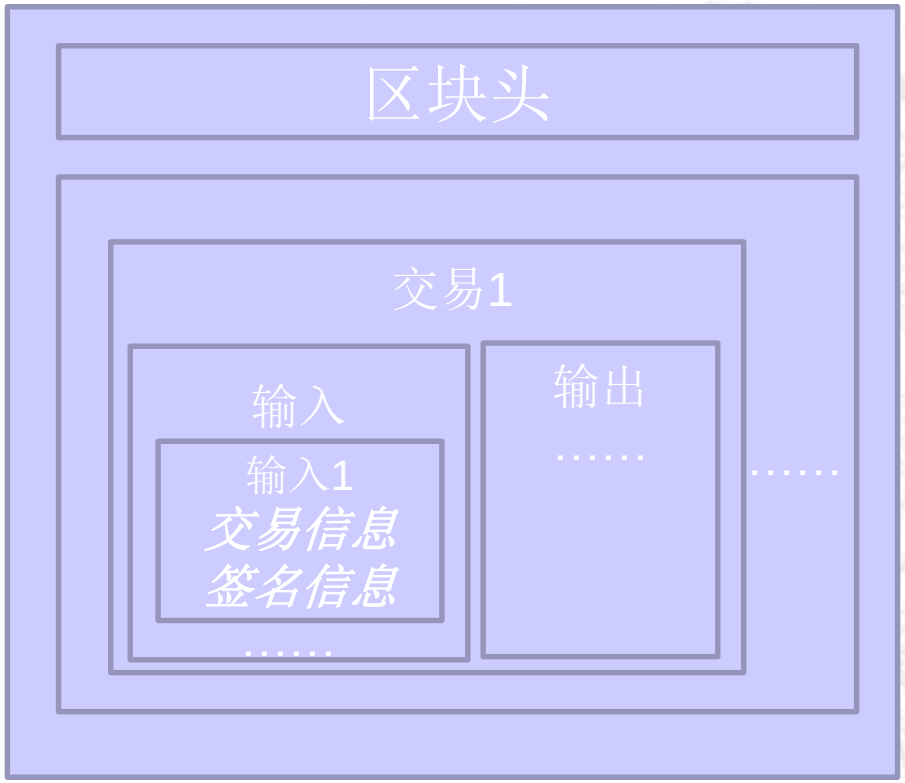
旧的规则一概不认



  - 软分叉：共识规则改变是向前兼容的，旧节点可以兼容新节点产生的区块

例如：WIN10能兼容XP系统的软件

隔离见证



比特币区块结构

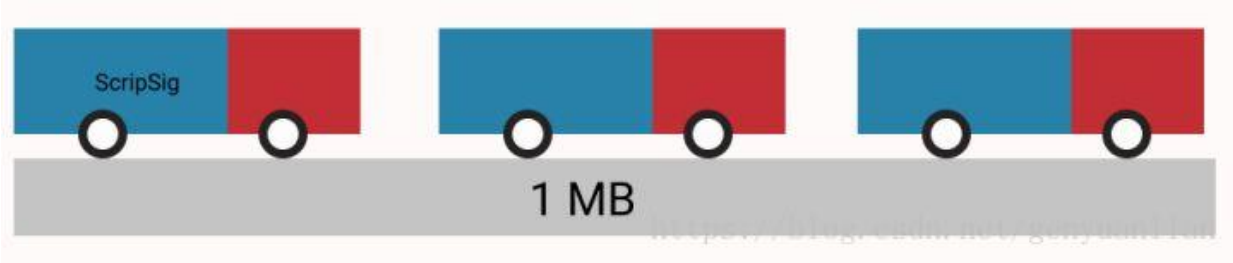
每笔交易平均 250 字节，签名信息的数据约为 150 字节，其余部分 100 字节。

数字签名占了60%，太高了。

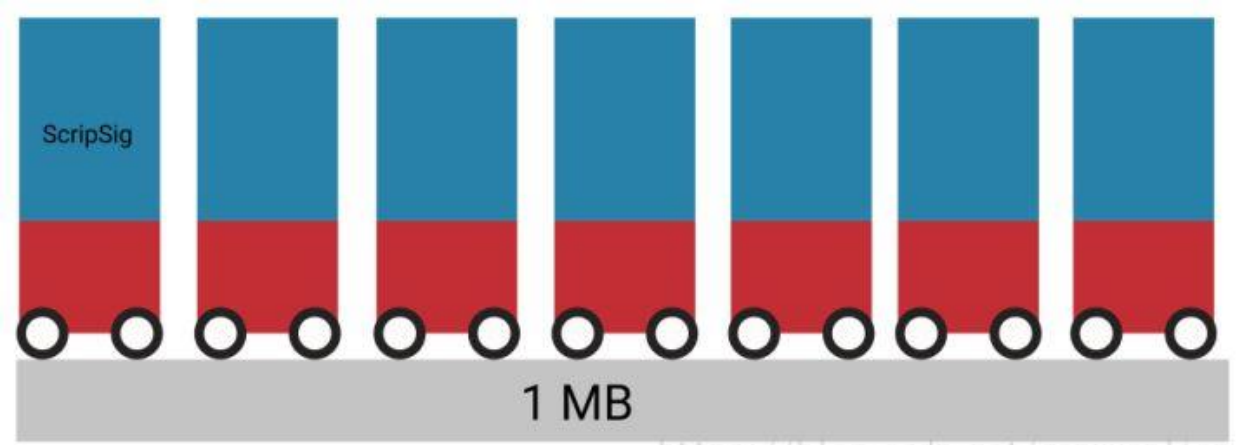
【注】签名的信息只有在验证的时候才需要。

隔离见证

- 隔离见证 Segwit(Segregation Witness)：隔离（segregate）数字签名（witness）与其他交易数据。



隔离见证前



隔离见证后

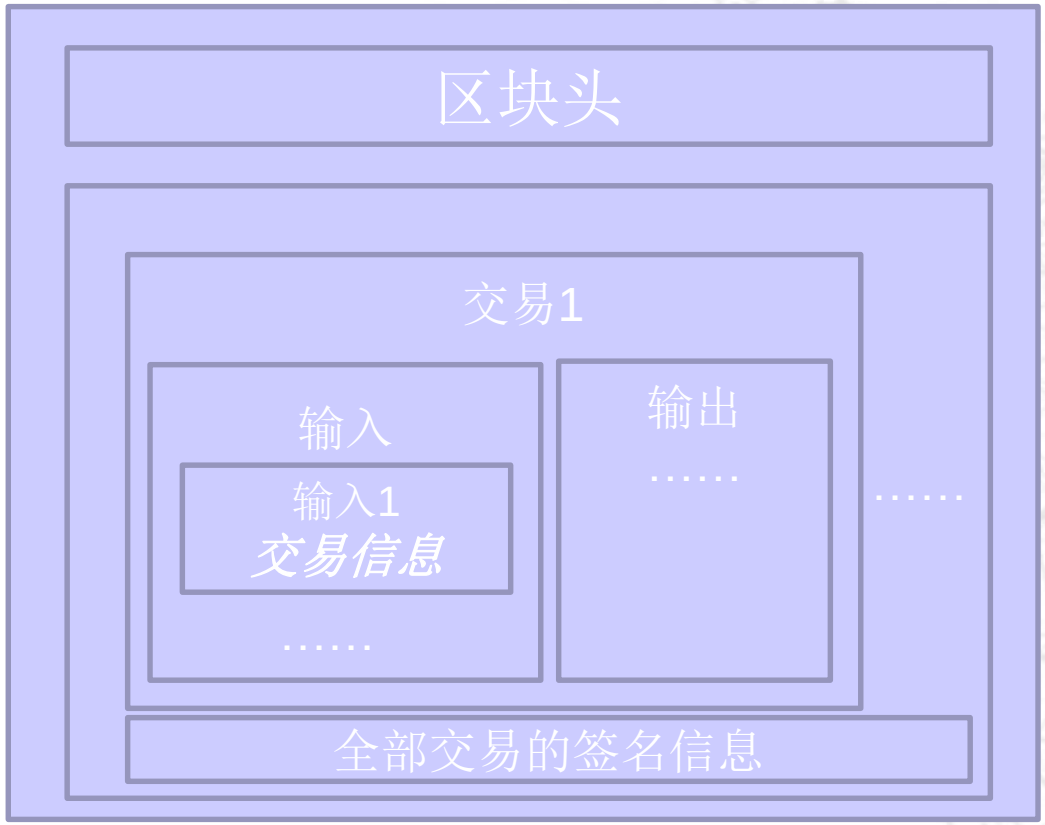
思考：

签名和交易还是在一起的。 类比：人的行李在车顶上放着，人在车里坐着，只是把行李和人分开了，但人和行李还是在车上。

问题1： 脚本签名是不是和每笔交易在一起？

问题2：见证是不是在区块链上？

隔离见证



隔离见证后
比特币区块结构

- 验证交易时签名信息同样会被验证。
- 签名信息依然在区块中。

隔离见证

- 隔离见证发布：2015年12月，BitcoinCore发布Segwit方案
  - 安全隐患，黑客通过改变交易签名信息改变交易ID
  - 将签名部分从交易中移除，从而间接扩容
- 香港共识：2016年2月相关会议，Core团队的代表同意在实施隔离见证后扩容到2M
- 纽约共识 Segwit2x：2017年5月纽约会议，85％以上算力的矿池在纽约达成 Segwit2x扩容
  - 实现BIP141(SegWit) + BIP91(缓和折中方案) + BIP102（升级到2M）

隔离见证优点

- 解决了延展性攻击（Malleability Attack）

延展性攻击

- 每个交易都有一个交易ID(txid),通过对整个交易哈希得到。
- 比特币本身使用的签名方式使得任何人在拿到一个交易记录后，可以在不需要知道私钥的情况下，通过**改变签名信息**，拼凑出另外一个有效的签名信息。
- 在交易上传到网络但尚未被打包时，攻击者通过修改交易中的签名生成同样有效的签名，交易ID会发生变化。
- 如果拼凑出来的交易记录先被写入区块链，原始交易记录会被认为是无效的交易。
- 这种方式不会造成双花，但是可能对原始交易记录的发起者会造成困扰。

隔离见证将签名信息与交易信息隔离，交易ID(txid)不受签名信息影响，避免了延展性攻击。

延展性攻击事件

- “门头沟”交易所倒闭事件：2014年2月25日，日本时间上午11点，MT.GOX交易所停盘。

1. 黑客将自己账号的比特币转移到在交易所新开的账号中。
2. 黑客申请提现（withdraw）,交易所发起1笔提款Transaction。
3. 在提款交易被广播到网络上，还未打包进区块链时，黑客收到这笔Transaction，生成新的交易广播出去，此时Transaction Id已经改变。
4. 新交易早于旧交易被区块链接收。黑客向交易所投诉，说没收到钱。交易所根据自己生成的Transaction Id查询该笔交易，在网络上查询不到， 会再次转账给黑客。

隔离见证优点

- 降低交易成本

  交易费=单笔交易容量*单位容量交易费定价

- 增加容量

  - 隔离出签名信息后，区块能够打包的交易数量提高。

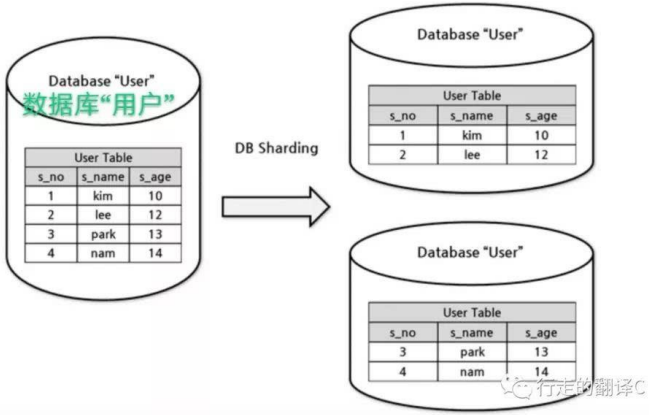
- 提高交易速度

  - 区块中可以容纳更多的事务，因此TPS会更高。

⑤ 众多技术的基础，如闪电网络、侧链

分片技术

- 分片：一种传统数据库技术，它将大型数据库分成更小、更快、更容易管理的数据分片（sharding）。



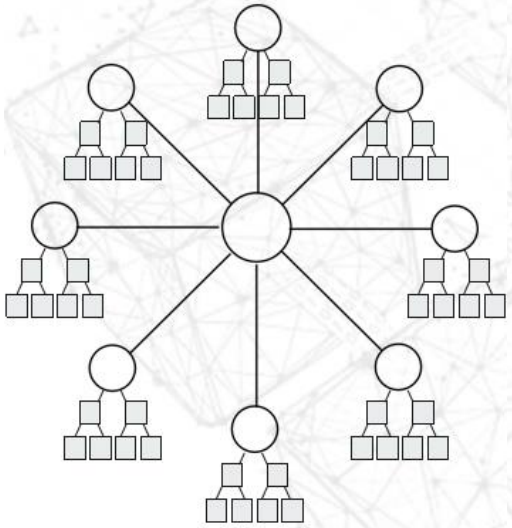
- 优点：数据分片分别存放在不同的服务器中，以减小每个服务器的数据访问压力，从而提高整个数据库系统的性能。

分片技术

- 分片技术来自以太坊。以太坊依据账户地址将全网划分为**多个相对独立的分片**，每个分片内维护一条**独立子链(分片链)**。

分片前的链

所有节点下载和验证所有交易。
严重的扩展性限制：比特币 7 交易/秒，以太坊 10-15 交易/秒。



分片后的链

每个节点只下载和验证一小部分（比如1/1024）的交易。节点工作并行进行，性能大幅提升。

- 优点：每个节点只需对自己分片内的交易进行验证
  各个分片并行工作，吞吐量大幅提高。

闪电网络

- 比特币的侧链项目：在比特币之上建立了一个结算层，也就是侧链。由此使得比特币主网压力减轻，资源浪费变少。
- 主要思路：将大量交易放到比特币区块链之外进行，只把关键环节放到链上进行确认

该设计最早于 2015 年 2 月在论文《*The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*》中提出。

闪电网络

使用Unix时间戳表示

- nLockTime：绝对时间
- sequence number：相对时间

闪电网络

locktime


```
"txid": "0627052b6f28912f2703066a912ea5[illegible]2ce4da4caa5a5fbd8a57286c345c2f2",
"hash": "0627052b6f28912f2703066a91[illegible]a577f2ce4da4caa5a5fbd8a57286c345c2f2",
"version": 1,
"size": 258,
"vsize": 258,
"weight": 1032,
"locktime": 0,
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig": {
      "asm": "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df
9cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813[ALL] 0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ad
8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
      "hex": "483045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08
f09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ad
8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf"
    },
    "sequence": 4294967295
  }
],
"vout": [
  {
    "value": 0.01500000,
    "n": 0,
    "scriptPubKey": {
      "asm": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG",
      "hex": "76a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788ac",
      "reqSigs": 1,
      "type": "pubkeyhash",
      "addresses": [
        "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA"
```


比特币某个交易的详细信息

闪电网络

时间锁——绝对时间
nlockTime

- Locktime字段即nlockTime
- 通常nLockTime = 0，代表这笔交易不会积压，节点收到这笔交易之后，立即会进入Memory Pool，之后开始打包，挖矿的过程；
- 当nLockTime > 0 时，这笔交易会被节点Hold在那，不会打包，不会进入区块链网络，直到到达某个区块高度或者未来的某个时间戳后。
- 为了验证nLockTime属性，script language有一个对应的操作符，叫做OP_CHECKLOCKTIMEVERIFY（CLTV）。
- nLockTime是Transaction级别的，每个Transaction有1个nLockTime字段。

闪电网络

时间锁——相对时间
Sequence Number

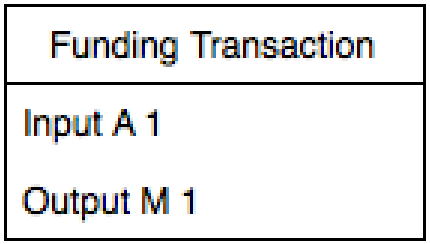
- Sequence Number是Input级别的，1个Transaction里面多个Input，每个都对应1个Sequence Number
- Sequence Number约束该交易必须等到Input所引用的交易（也就是上1个交易的UTXO）所在的Block，后面跟随了sequence number个Block之后，该交易才能被打包，被广播进区块链网络。

闪电网络

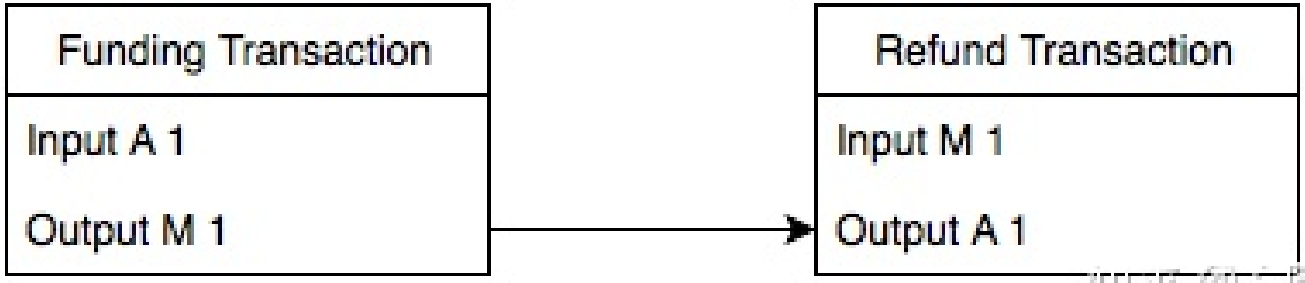
- 微支付通道

场景：A是用户，B是一个数据提供商，B需要把1个100G的大数据文件发给A，价值是100元。为了降低风险，A不想1次性把100元给B，而是每接收到1G的数据，给B支付1元。

Step1:A生成1个保证金交易(Funding Transaction）



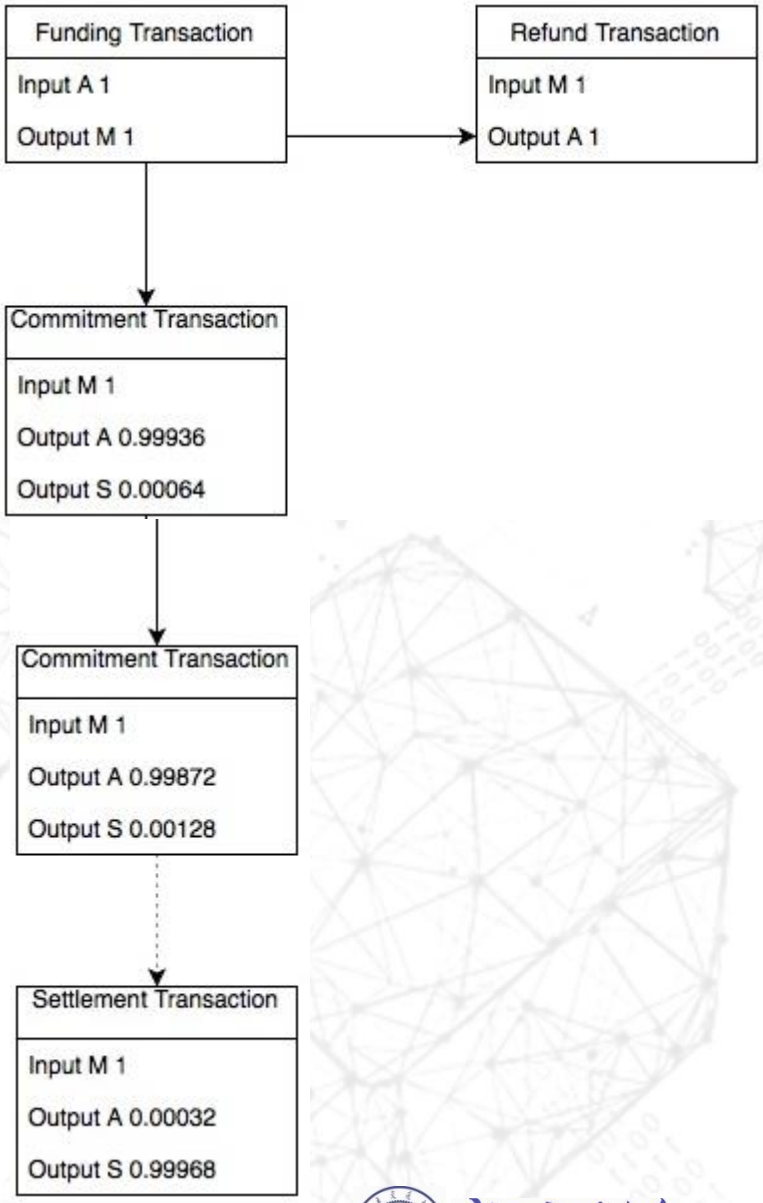
Step2:A为这笔钱生成退款交易（Refund Transaction），然后广播到比特币区块链上



闪电网络

- 微支付通道

Step3:拷贝Refund Transaction



Step4:A 发起结算交易Settlement Transaction，nLockTime = 0，B收到这个交易，广播到网络上

闪电网络

- 微支付通道

整个过程只有保证金交易和结算交易被广播到网络中。

Q1：为什么到第二步才把Funding Transaction广播？

Q2：如何避免A跑路，B的利益受到损失？A用户跑路了，但B星巴克也会把transaction广播到全网

Q3：A是否有双花的风险？不会

闪电网络

- 微支付通道

微支付通道成立的关键是A和B都握有对方的“把柄”，双方都无法违约。其缺点是：

① 通道是单向的，只能用来A给B转账。如果反过来，需要另外再建立B到A的通道。
② nLockTime的限制。如果一方跑路，另一方只有在nLockTime后才能拿回钱。

闪电网络优化了微支付通道，解决了上面的问题。

闪电网络

- 基本思想：通过智能合约完善链下交易通道
- 整合两种类型的交易合约
  - RSMC：保障两个人之间的直接交易可以在链下完成；
  - HTLC： 保障了任意两个人之间的转账都可以通过一条“支付”通道来完成。
- 实现任意两个人间的交易都在链下完成。
- **其出现的主要理由就是为了应对链上的高额手续费和小额支付交易。**

- RSMC(Revocable Sequence Maturity Contract):序列到期可撤销合约
- HTLC（Hashed Timelock Contract）: 哈希时间锁定合约

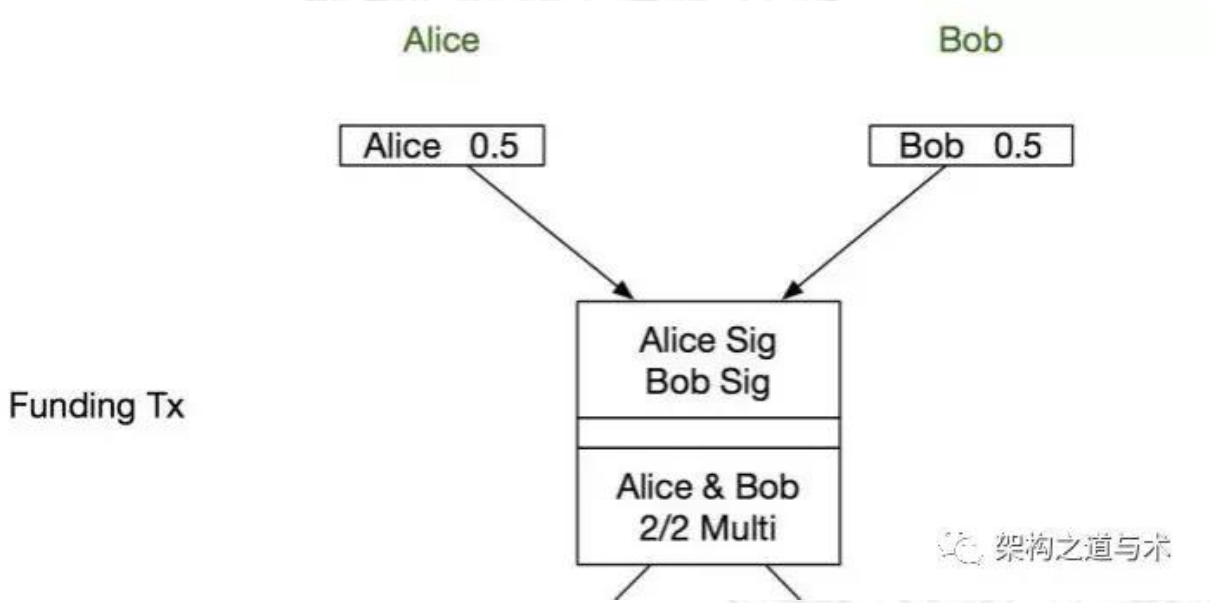
闪电网络-RSMC

- RSMC（Revocable Sequence Maturity Contract）可撤销的、基于Sequence成熟度的合约。RSMC可以做到：

  - 双向通道。
  - 一方退出，另一方立即收到钱，而且对退出方进行惩罚。

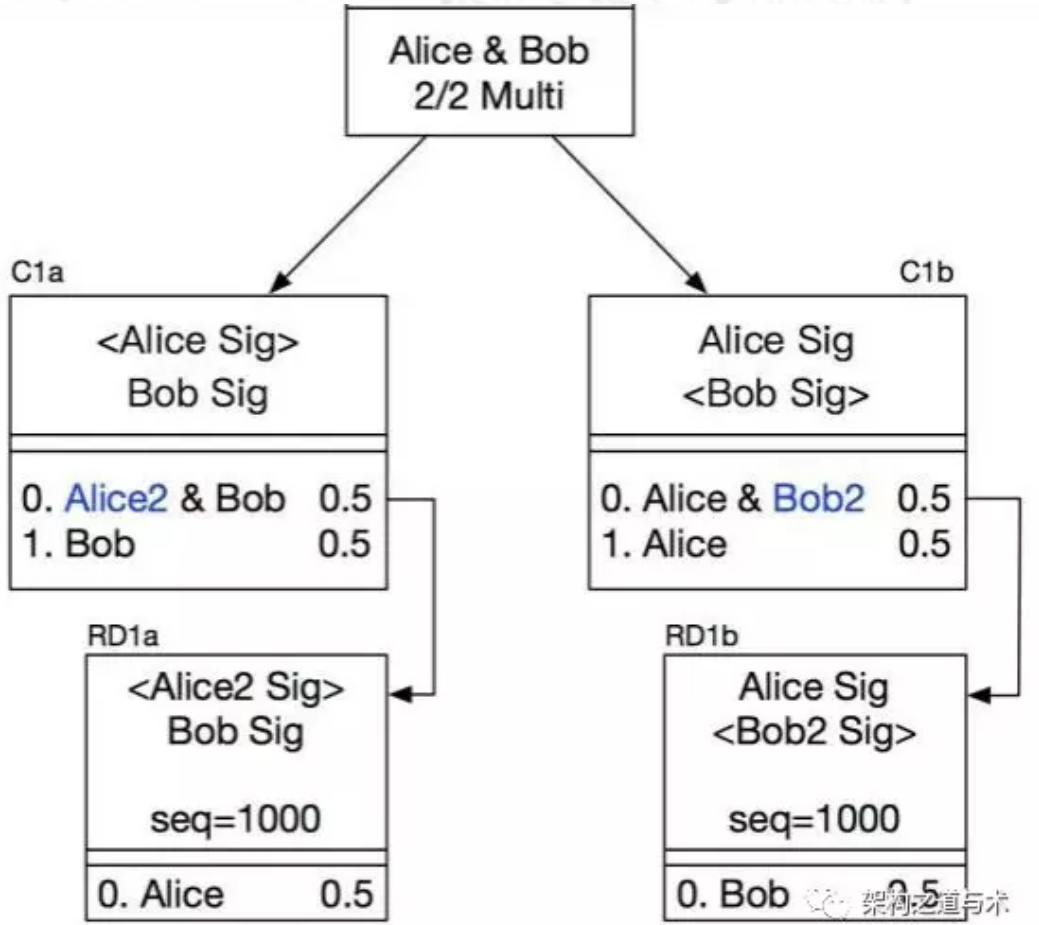
闪电网络-RSMC

Step1:
同微支付通道一样，生成1个保证金交易(Funding Transaction）。不同点在于这里是双向支付。所以双方各拿1笔钱出来，打入这个公共账户。



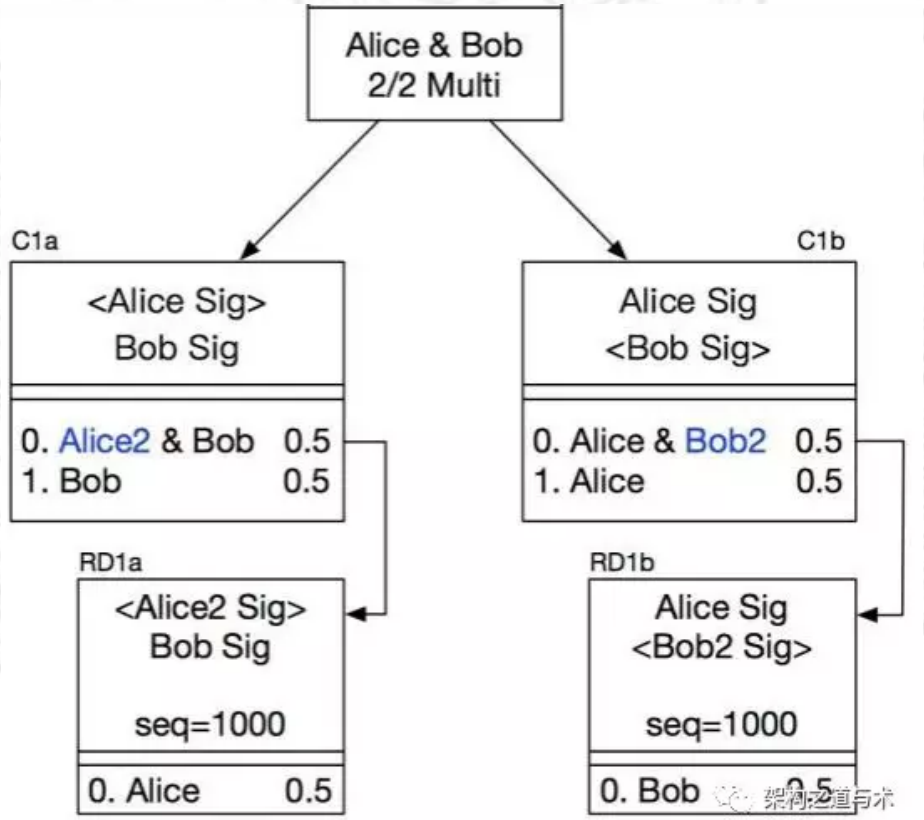
闪电网络-RSMC

Step2:
为这笔钱生成退款交易（Refund Transaction）。双方可以各自拿回自己的0.5比特币。
Alice生成的退款交易是C1a + RD1a，Bob生成的退款交易是C1b+RD1b，二者是对称的。



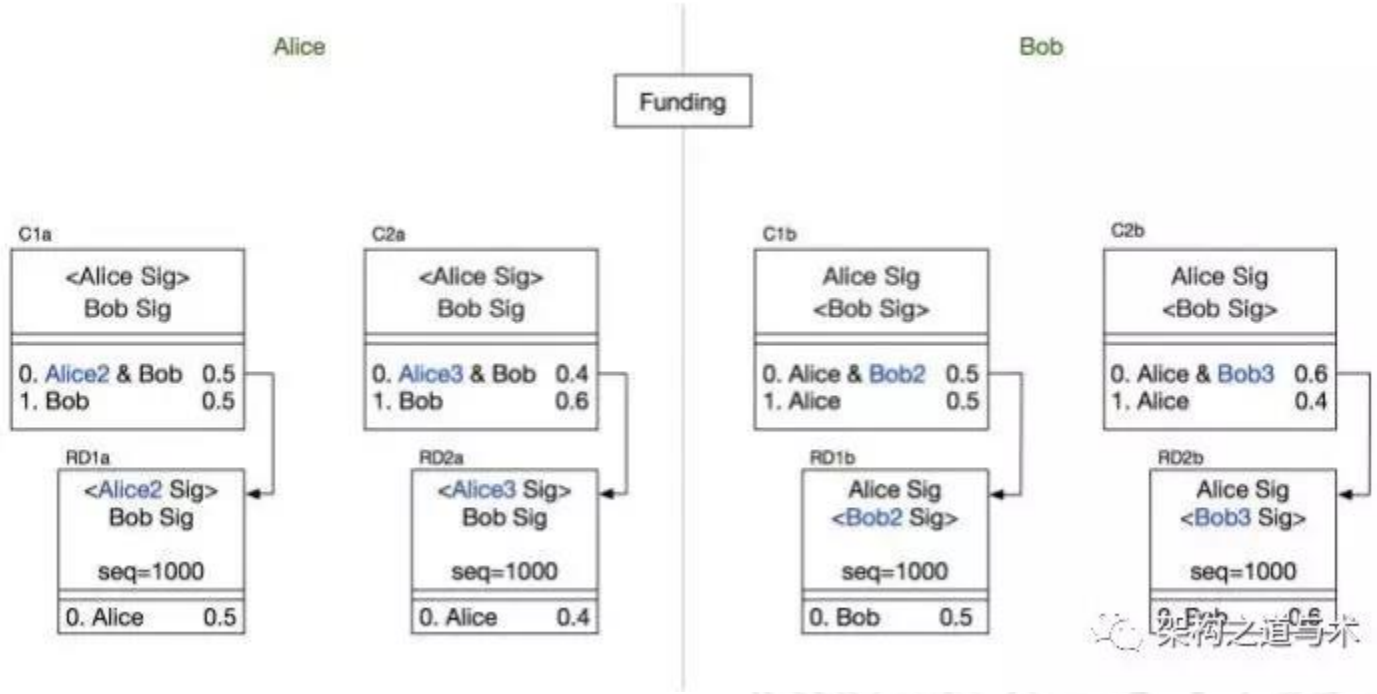
闪电网络-RSMC

假设Alice想主动中断交易，也就是它把C1a + RD1a 广播到了区块链网络上。
C1a里面，会把Bob的0.5比特币立即返还给Bob，Bob立即收到钱。而Alice的0.5比特币被打到了1个新的公共账号： Alice2 & Bob里。



Alice想要拿回自己的钱需要RD1a兑现，而其seq=1000,说明要等到C1a所在的块，后面被追加了1000个块之后，RD1a这个交易才会被进入区块链里面，Alice才能拿到自己的钱。

闪电网络-RSMC



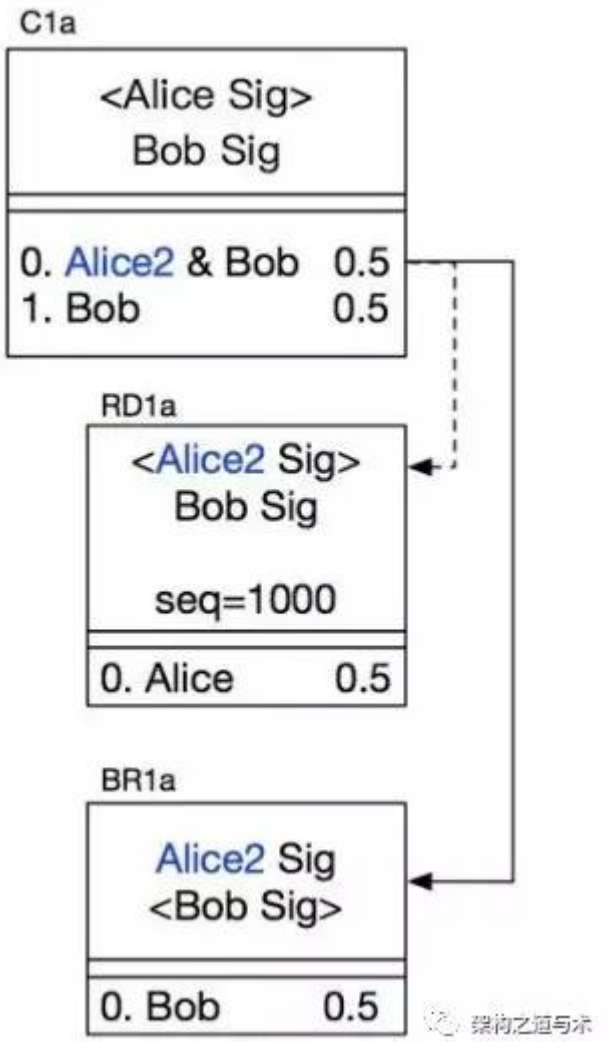
Step3:

假设Alice要付给Bob 0.1 比特币，那么公共账号里面的资金分配，就从0.5/0.5，变成了0.4/0.6。Alice生成了C2a与RD2a，C1a与RD1a废除。同样，Bob生成了C2b与RD2b，C1b和RD1b废除。

闪电网络-RSMC

- 在双方达成了C2a/RD2a, C2b/RD2b之后，如何废除C1a, RD1a, C1b, RD1b ？

- 这里引入**惩罚机制**，在Alice生成C2a/RD2a之前，他要把自己在C1a里面的私钥 Alice2发给Bob；同样，Bob把自己的C1b里面的私钥Bob2发给Alice。Alice把秘钥Alice2给了Bob，Bob会为C1a生成1个惩罚交易BR1a，以防Alice反悔。
- 假设Alice反悔，将C1a + RD1a广播出去，Bob就把BR1a广播出去。BR1a由于没有Sequence，会先于RD1a执行，所以结果是RD1a不会被执行，BR1a执行。Alice的0.5转移给了Bob。



闪电网络-RSMC

Step4:
同微支付通道一样，双方最终完成了交易。把Step3里面最后1次更新，广播到网络上，各自得到自己的钱。最后1次sequence = 0，双方都立即拿到自己的钱。

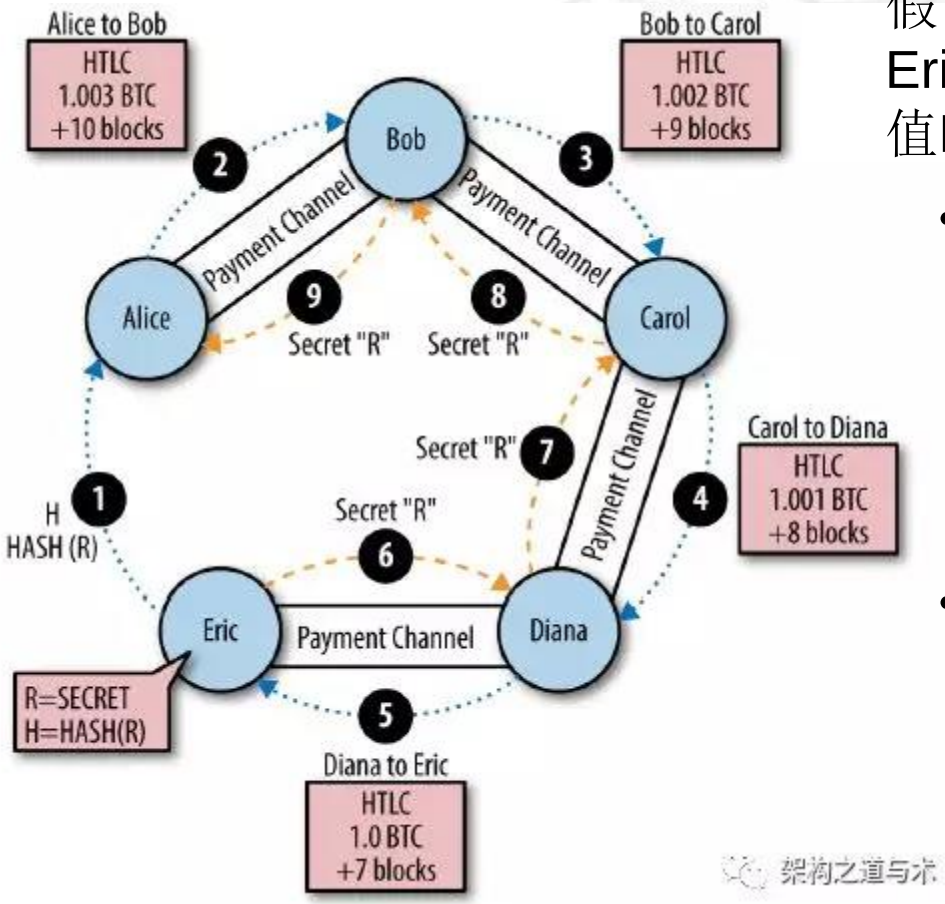
- 通过RSMC，已经实现了双向通道和立即支付。但是任何时候2个人之间要交易，就得建立支付通道，这同样很麻烦。
- 闪电网络中采用重用之前的通道，比如A和C要建立交易，已经有A和B，B和C的通道，AC的交易可以通过AB和BC的通道进行。实现技术是**HTLC**。

闪电网络

- HTLC - Hashed timelock contract - 限时转账的概念
  - 交易双方没有设立资金池，实现任意2人之间转账可以通过“中间人支付通道”完成
  - 中间人之间通过在规定的时间内互相传递secret来解锁Token
  - 小红要给小蓝转1BTC，二人没有共同资金池，小红发现小黄和小绿分别和自己与小蓝有资金池，发起支付通道搭建

闪电网络-HTLC

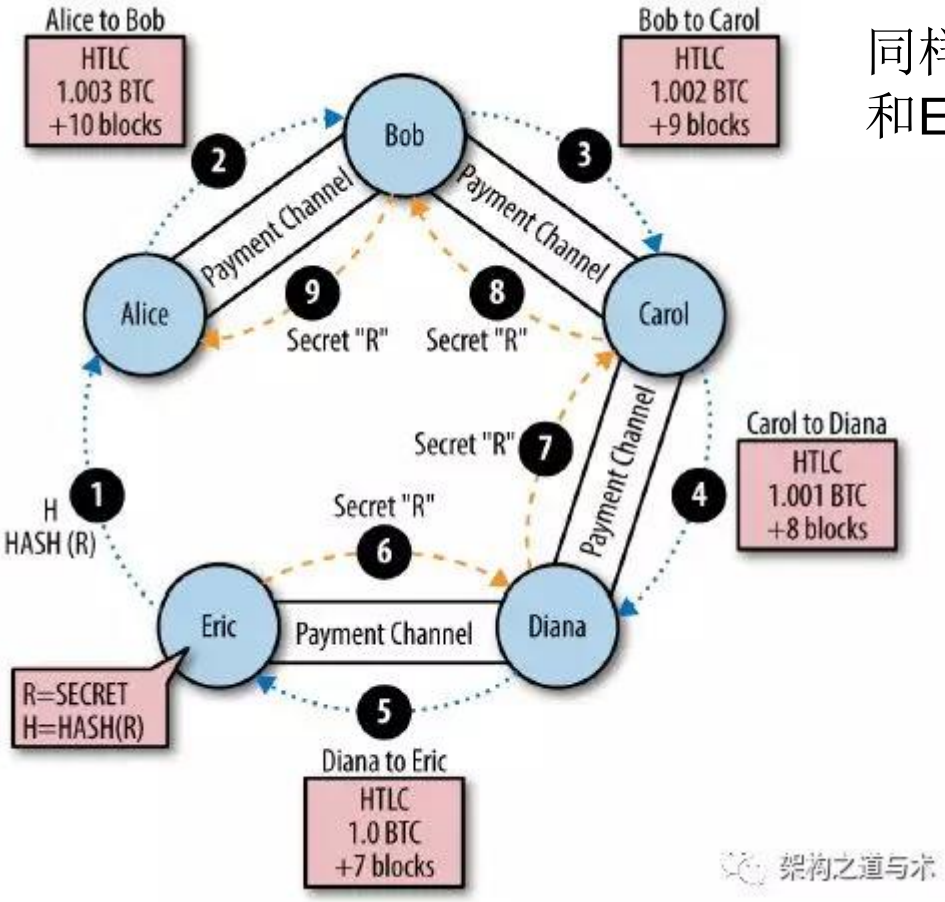
- HTLC（Hashed Time Lock Contract）



假设Alice需要付给Eric 1个比特币。Eric构建了1个秘钥R和对应的Hash值H，然后把H给了Alice。

- Alice和Bob之间达成了一个合约：如果Bob在4天内，可以给Alice H对应的密钥R，Alice就支付Bob 1.003比特币，如果超过4天，Alice将取回钱。
- Bob和Carol之间达成了一个合约：如果Carol在3天内，可以给Bob H对应的密钥R，Bob就支付Carol 1.002比特币，如果超过3天，Bob将取回钱。

闪电网络-HTLC



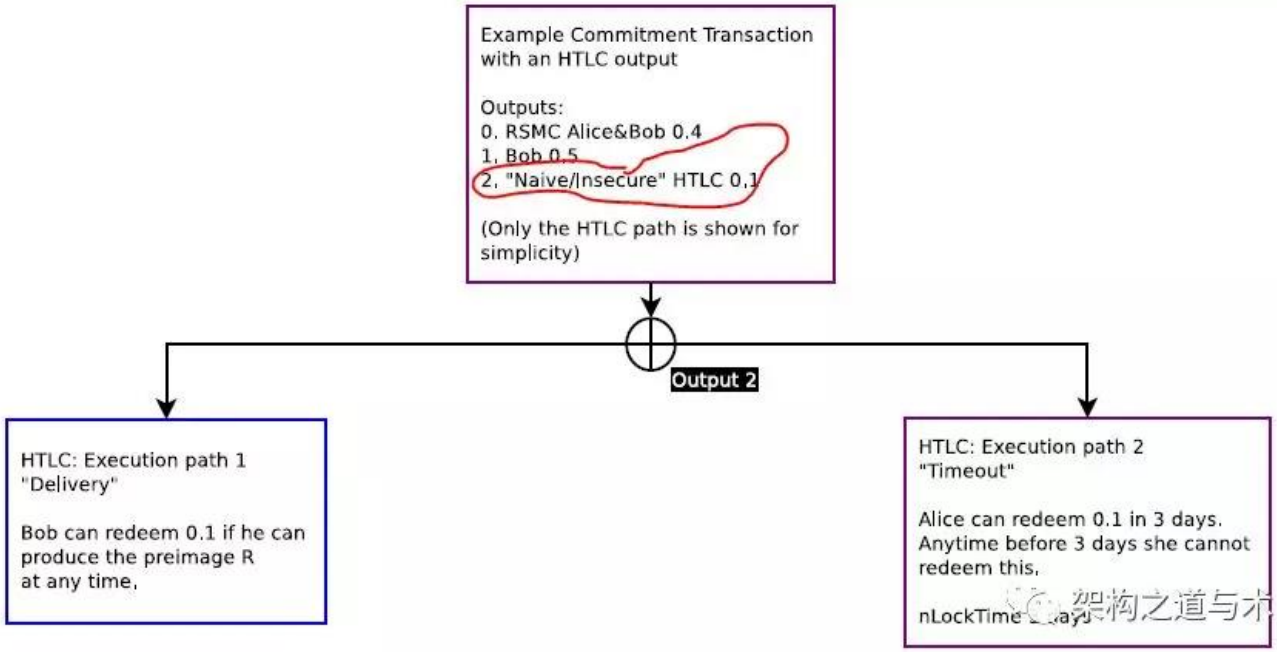
同样Carol和Diana达成和约，Diana和Eric达成合约。

- 整个的交易顺序是：Eric把R给了Diana，拿到1.0比特币；Diana把密钥给Carol，拿到1.001比特币……Bob把R给了Alice，获得1.003比特币。
- 最终，Alice付出了1.003个比特币，Eric收到1.0个比特币，每个中间方，收到0.001个比特币的手续费。

闪电网络-HTLC

- HTLC实际是通过Script Language中的OP_IF和OP_ELSE执行。
- HTLC会借用通常的RSMC交易通道，在其中塞进1个HTLC的合约。
- HTLC本身的想法并不复杂，但它需要和RSMC紧密结合，才能形成一个完善的、具有多个中间节点的支付通道。

闪电网络-HTLC



Alice和Bob各有0.5比特币在这个通道里面，现在Alice和Bob建了一个HTLC（Alice向Bob支付0.1元，只要Bob能提供密钥R）。在Transaction里面，新加了1个output（红线部分）。

Bob想兑现这0.1比特币，就以output2为输入，构建左边分支的Delivery Transaction（包含密钥R）。Alice想拿回这0.1比特币，同样以output2为输入，构建右边分支的Timeout Transaction（时间到了之后，钱就回到Alice账号）。

闪电网络

- 基于这两项技术协议的闪电网络速度更快，可以达到百万级TPS。其不仅具有安全、匿名的优点，还做到了跨链原子交换，也就是允许加密货币在不同区块链上点对点的转移。
- 支付通道
- 基本流程

--打开通道

--交易

--关闭通道

闪电网络的缺陷

- 每个节点都需要维护所有的节点和通道列表，占用带宽越来越大。
- 路径查找时的路由优化和防御路由攻击。
- 节点可以发送的最大金额取决于经过路线中资金量最小的那个通道的金额。
- 离线风险。闪电网络中通道维持需要双方节点不断签名，这需要双方节点都在线，当一方离线时，通道关闭。

闪电网络的缺陷

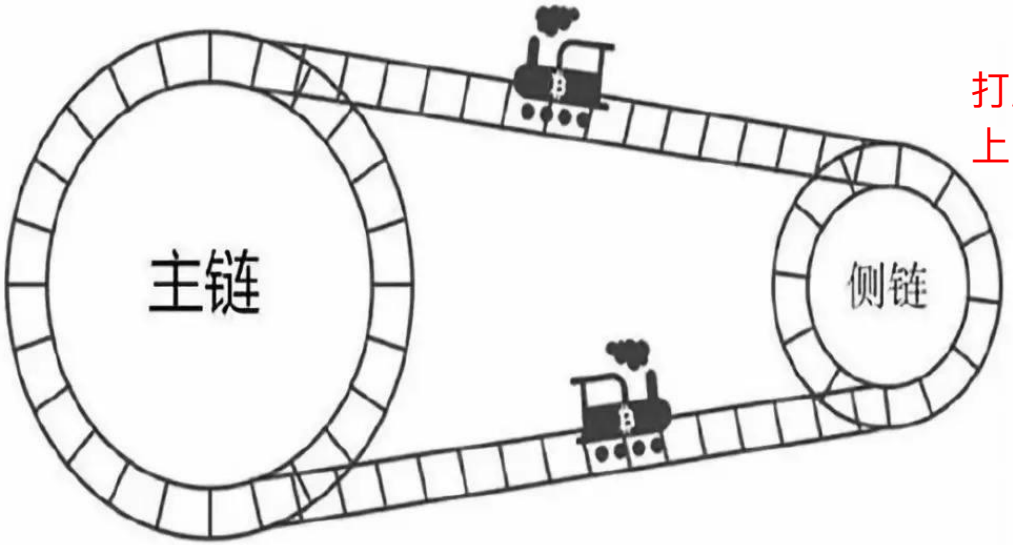
- 容易遭受DDoS攻击

2018/3/22新闻：闪电网络节点遭受DDoS攻击，20%节点被下线 其实要攻击闪电网络很简单，只要骨干节点被攻击，部分就要瘫痪。

侧链

- 以比特币区块链作为主链（parent chain），其他区块链作为侧链，二者通过双向挂钩（two-way peg），实现比特币从主链转移到侧链进行流通。

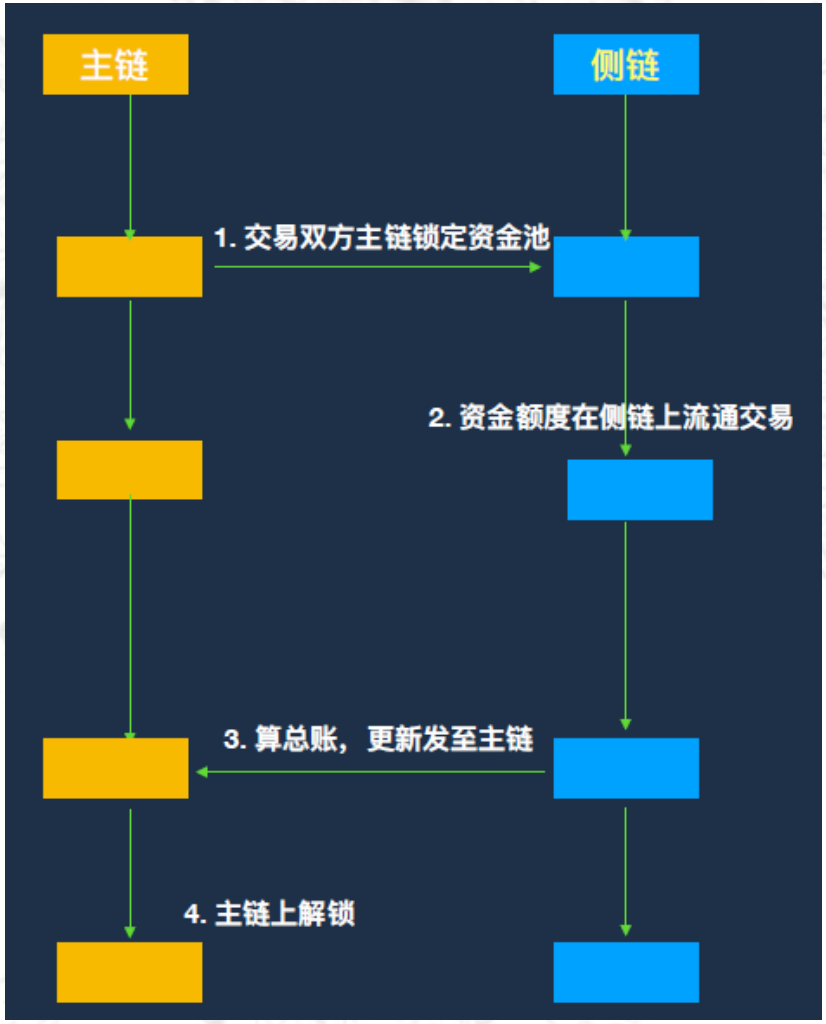
最后打完麻将，结算时在主链上进行。



打麻将每局的输赢记在侧链上，不立即结算

侧链

- 侧链-Side Chain，相对于主链的附属链，用于同主链的资产转移
- 对高频交易另外建立一套账本（侧链），用于临时记账，等最后双方结算时再上主链
- 有效降低比特币区块链的交易拥塞



侧链

❖ 闪电网络和侧链都需要用到的密码学技术

多重签名（n-of-m 多重签名）：

指有m个参与方，且只需任意n方签名，交易便有效。

交易的解锁脚本与普通交易不同:

它会将A、B、C三个地址的公钥写进去

同时将参与方“3”和需签名数“2”也写进去。

解锁脚本里的数字签名是这么来的：

1、构造交易；

2、A（或B）用自己的私钥先对整个交易签名，然后将签名填入交易；

3、B（或A）用自己的私钥再对第2步生成的交易进行签名。

侧链

- 侧链的必要性
  - 性能，所有交易都在主链处理，主链速度慢
  - 功能，非币智能合约
  - 成本， 所有交易都记录于区块，存储成本高

侧链

- 侧链实现的技术基础是**双向锚定**（Two-way Peg），通过双向锚定技术，可以实现暂时的将数字资产在主链中锁定，同时将等价的数字资产在侧链中释放，同样当等价的数字资产在侧链中被锁定的时候，主链的数字资产也可以被释放。以比特币为例，具体实现包括：

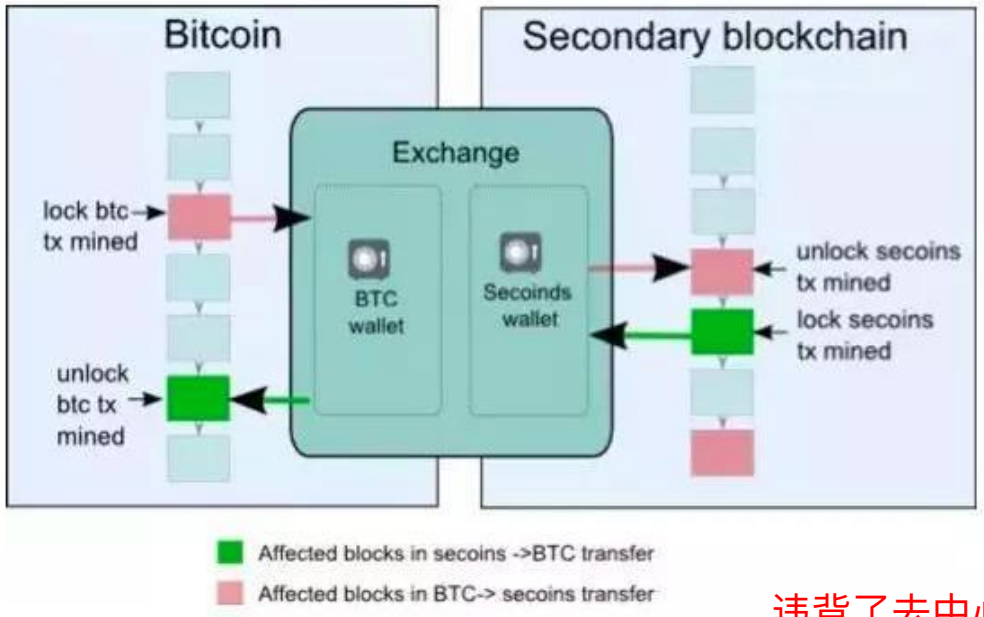
  - 单一托管模式
  - 联盟模式
  - SPV模式
  - 驱动链模式
  - 混合模式

不需要对现有比特币协议进行修改。

侧链

➢ 单一托管模式

将数字资产发送到一个主链单一托管方（类似于交易所），当单一托管方收到相关信息后，就在侧链上激活相应数字资产。



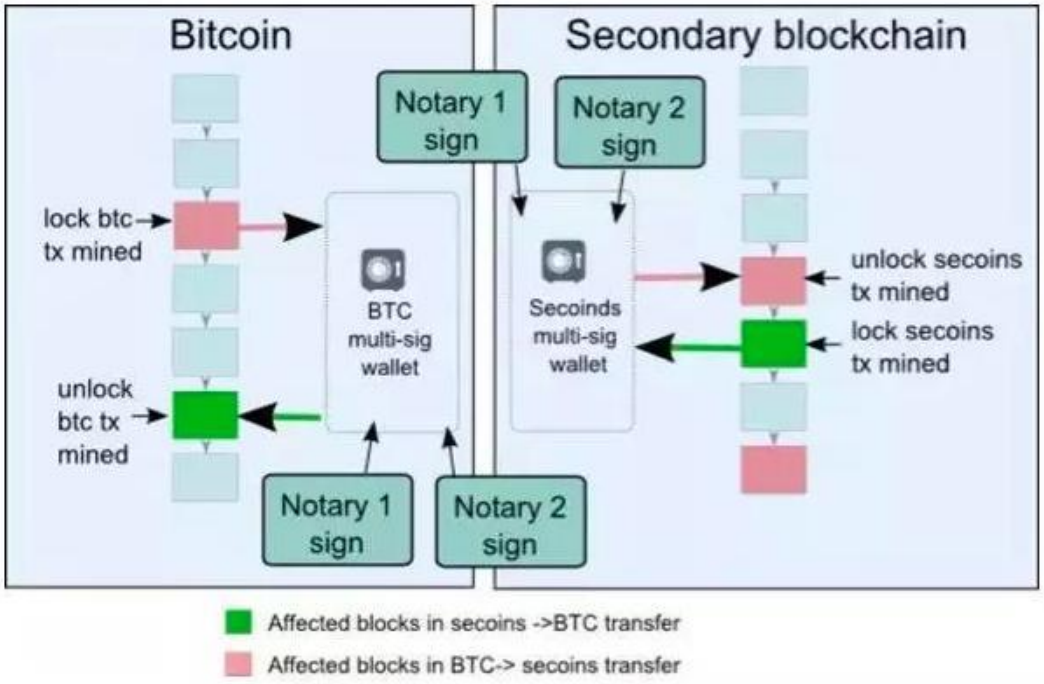
违背了去中心化的原则

单一托管模式的问题在于过于中心化。

侧链

➢ 联盟模式

使用公证人联盟来取代单一的保管方，利用公证人联盟的多重签名对侧链的数字资产流动进行确认。



侧链安全仍然取决于公证人联盟的诚实度。

侧链

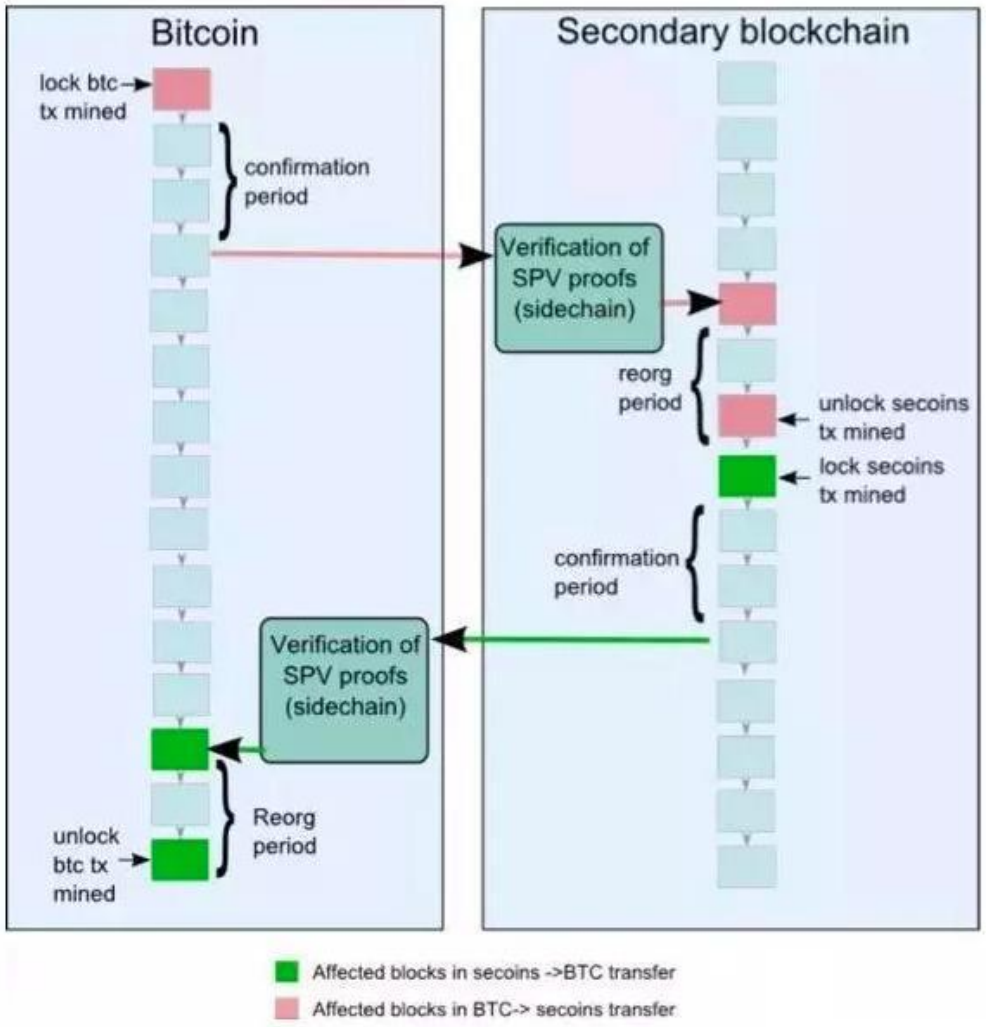
➢ SPV模式

- SPV (Simplified Payment Verification)。证明一个交易确实已经在区块链中发生过，称为 SPV 证明。

- SPV证明包含两部分：
  - ➢ 一组区块头列表，表示工作量证明
  - ➢ 一个特定输出确实存在于某个区块中的密码学证明

侧链

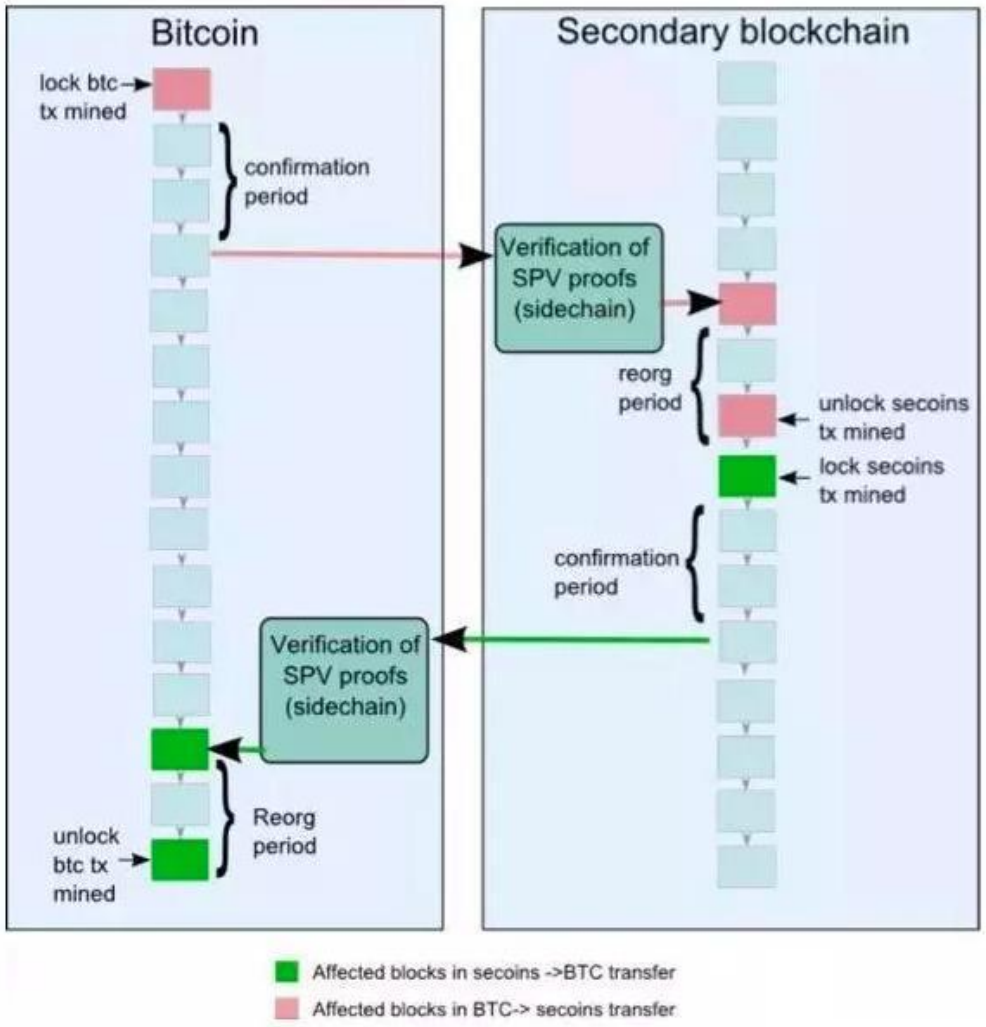
- SPV模式



用户在主链上将数字资产发送到一个特殊的地址，起到锁定主链的数字资产，该输出仍然会被锁定在可能的竞争期间内，以确认相应的交易已经完成。随后会创建一个SPV证明并发送到侧链上。此刻，一个对应的带有SPV证明的交易会出现在侧链上，同时验证主链上的数字资产已经被锁住，然后就可以在侧链上打开具有相同价值的另一种数字资产。

侧链

- SPV模式



当这种数字资产返回到主链上时，该过程会进行重复。它们被发送到侧链上锁定的输出中，在一定的等待时间后，就可以创建一个SPV证明，来将其发送回主区块链上，以解锁主链上的数字资产。

SPV模式的问题是需要对主链进行**软分叉**。

侧链

了解即可

➢ 驱动链模式

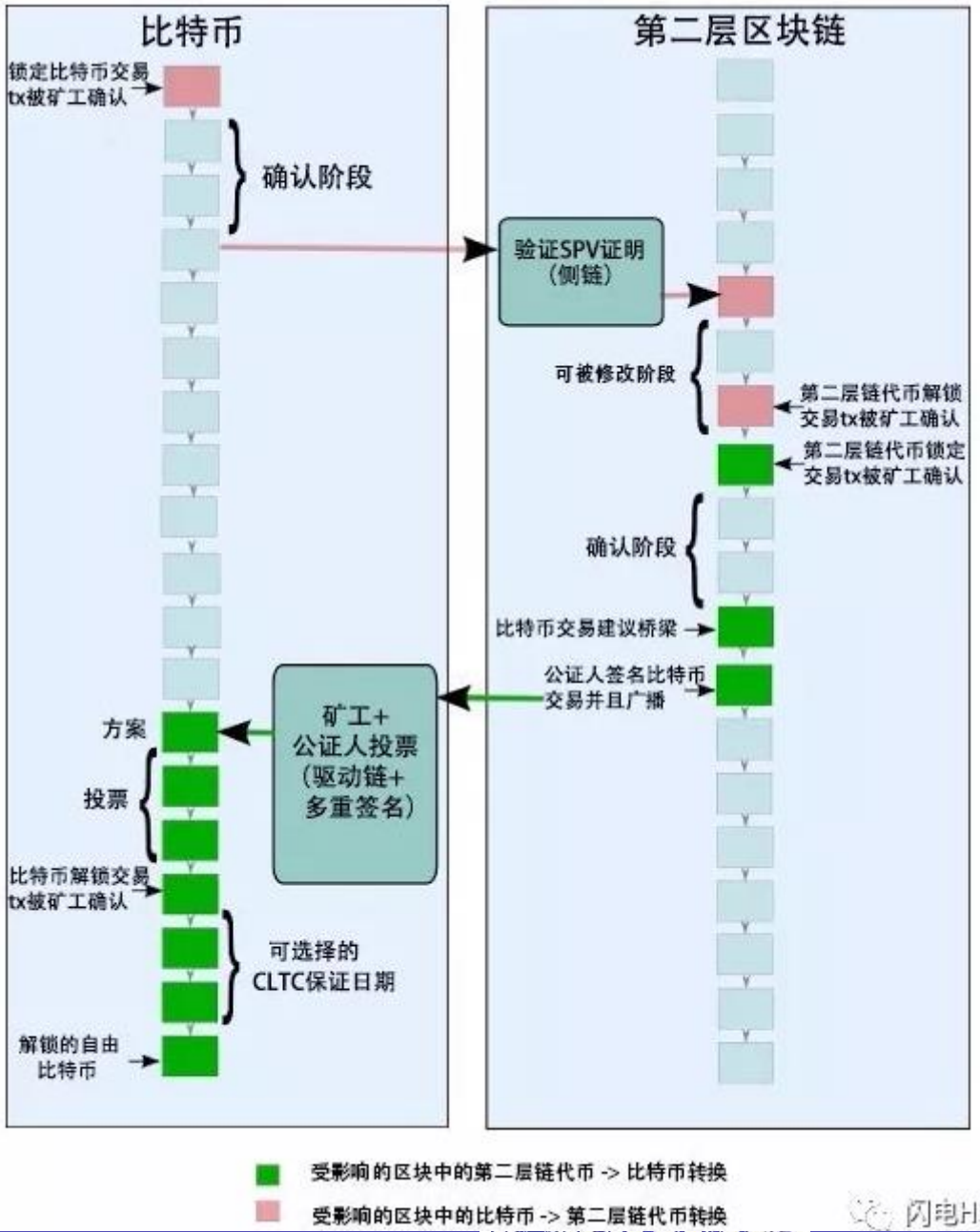
- 驱动链概念是由Bitcoin Hivemind创始人Paul Sztorc提出。在驱动链中，矿工作为“算法代理监护人”，对侧链当前的状态进行检测。矿工本质上就是资金托管方。

- 诚实矿工在驱动链中的参与程度越高，整体系统安全性也就越大。如同SPV侧链一样，驱动链也需要对主链进行软分叉。

侧链

➢ 驱动链模式

驱动链将被锁定数字资产的监管权发放到数字资产矿工手上，并且允许矿工们投票何时解锁数字资产和将解锁的数字资产发送到何处。矿工观察侧链的状态，当他们收到来自侧链的要求时，他们会执行协调协议以确保他们对要求的真实性达成一致。



侧链

➢ 混合模式

- 由于主链与侧链在实现机制存在本质的不同,所以对称的双向锚定模型可能是不够完善的。
- 混合模式则是将上述获得双向锚定的方法进行有效的结合的模式。混合模式是在主链和侧链使用不同的解锁方法，例如在侧链上使用SPV模式，而在主链网络上则使用驱动链模式。
- 同样，混合模式也需要对主链进行软分叉。

比特币安全性

- 51%算力攻击

掌握51%以上算力的节点统一行为，可以随意生成最长链，伪造区块

- 重放攻击

这里的“攻击”不是黑客发起的某种侵略或偷盗行为。而是因为区块链分叉后的两个分支链，都有相同的地址、私钥和交易格式。在分叉点前出现的UTXO，在分叉后引出的交易，如果分叉时未加入防御重放攻击的代码，自动会被分叉后的两条链都确认，从而构成双花。

比特币安全性

- 延展性(Transaction Malleability)攻击

延展性攻击者侦听比特币P2P网络中的交易，利用交易签名算法的特征修改原交易中的input 签名，

生成拥有一样input和output的新交易，然后广播到网络中形成双花，这样原来的交易将有一定的

概率不能被确认，造成不可预料的后果

- 量子计算威胁

比特币的POW和授权/验证交易所用的签名是量子计算利用强大算力进行攻击的两大弱点。

比特币交易追踪

- 比特币是完全匿名的吗？

不是，有一定的匿名性

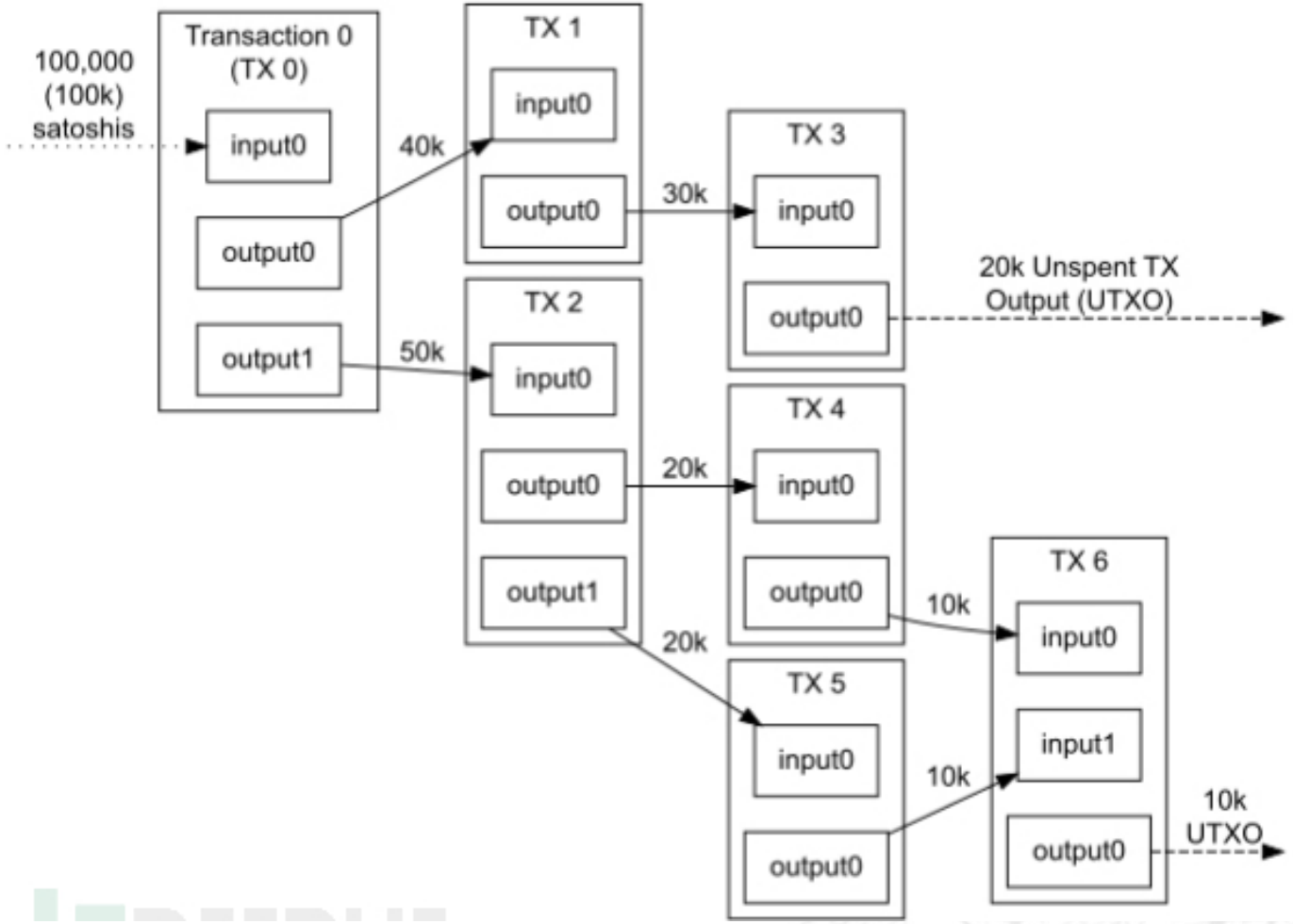
- 如何进行比特币交易追踪？

通过钱包地址查询钱包现金的流入和流出，并可向上追溯至这些比特币的终极起源

比特币交易追踪原理

- 比特币整个支付网络中所发生的每一笔交易都会被记录在“区块链”（blockchain）中——这是比特币货币体系用以追踪谁何时拥有哪些比特币，以及防止欺诈和伪造的分散化交易记录机制。

63


100,000
(100k)
satoshis
Transaction 0
(TX 0)
input0
output0
output1
40k
50k
TX 1
input0
output0
TX 2
input0
output0
output1
30k
20k
20k
TX 3
input0
output0
TX 4
input0
output0
TX 5
input0
output0
20k Unspent TX
Output (UTXO)
10k
10k
TX 6
input0
input1
output0
10k
UTXO

区块中输入输出信息

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
51d37bdd87...	0	0.135	Generation: 50 + 0.01 total fees	15nNvBTUdMaiZ6d3GWCeXFu2MagXL3XM1q: 50.01
60c25dda8d...	0	0.259	1HuppjXz7dPrt2a67LqacDW5T4VanFrpqC: 29.5	1B8vkT58i8KUPVJvvyQfrbc8Wjwu3vEarQ: 0.5 1BQbxzgRSLEsmv1JNc8MG76wdUgMwbsaww: 29
01f314cdd8...	0.01	0.617	1NdzSE6sHubscXJrv7jJn2gd4fL9L3ai6E: 0.03 1Jjv9m5VrRUE7VoktCsj18KUSqkqchhbum: 0.02 1HsYJJPqTn34DEjMnTb3VfKckX7ZcWPibm: 4.82	175FNxcLc1YrTwwG6TcsywcsHYdVqyhbwC: 0.01 1MueNMRJmcqVQeqE7v4dqogpNbhyxqq8R6: 4.85
b519286a10...	0	0.404	12DCoCVvDCkQShZ5RTh9bysgCkmkRMNQbT: 0.14 13CJwnnXJPwkzY4Xnaoqf8dnyNBwrHG9fe: 0.01	1Mos7p8fqJKBcYNRG1TdT5hBRxdMP6YHPy: 0.15

65

比特币交易追踪技术

- 网页爬虫技术
- 聚类技术
- 社会工程学技术
- 深度学习
- 数据挖掘、大数据分析

网页爬虫技术

- 通过网页爬虫技术获取比特币交易网站的交易商品信息（商品类别、数量、时间、图片等）和用户信息。
- 现有爬虫对抓取目标的描述可分为：基于目标网页特征、基于目标数据模式和基于领域概念。
- 网页分析算法：基于网络拓扑结构 、基于网页内容、基于用户访问行为。
- 通过网页爬虫技术可以抓取和提取违法交易。

聚类技术

- 聚类技术主要是对“区块链”中的公钥地址信息分类，获取用户信息或异常点信息。

- 主要的聚类算法可以划分为如下几类：划分方法、层次方法、基于密度的方法、基于网格的方法

社会工程学技术

- 通过对网络的监控交易用户的TCP/IP信息，获取用户的IP地址。
- 通过对比特币交易网站、比特币论坛等社区的监控，例如电子邮件地址、发货地址、信用卡和银行账户细节,IP地址、公钥地址等信息。
- 把IP地址信息、用户账号信息和公钥地址关联。

政府该如何监管比特币

- 比特币虽说有一定的匿名性，但其所有交易都是公开的，加上中国政府几乎能监控到所有的现实社会。所以，中国政府要对比特币进行监管，其实不难，甚至比传统的交易方式更加容易监管。
- 1、 比特币交易网站实名化
- 2、 大数据
- 3、 监管数据节点
- 4、 全民监管

70