优权天成
YQTC TECH

比特币进阶之路

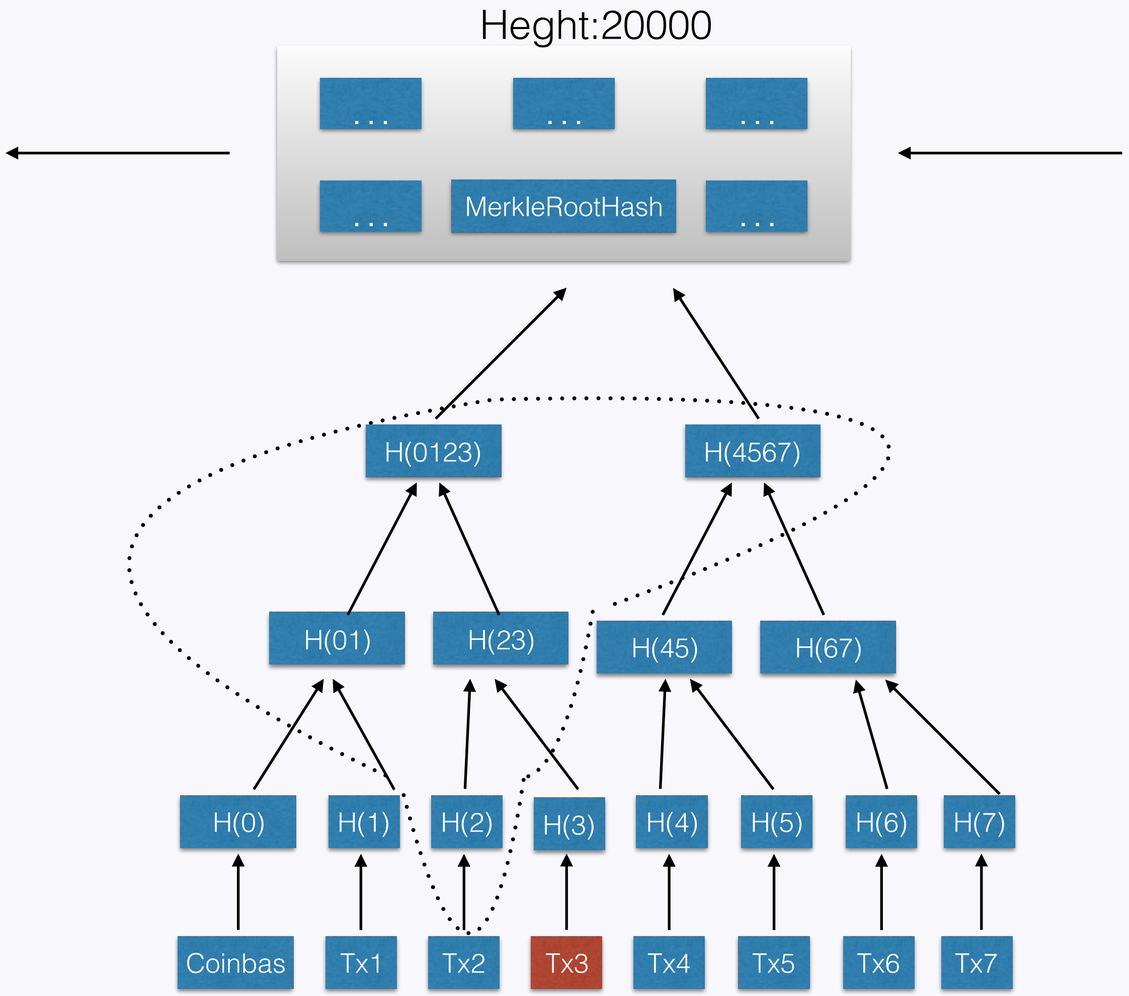
主讲： 韦忠汕

目录

优权天成 YQTC TECH

优权天成 YQTC TECH

1.1 merkle树与SPV验证



SPV简单支付验证：

1. B向A提供交易数据（金额、汇款地址、签名等）
2. A根据数据构造交易，计算Txid
3. 从交易记录中找到Txid所在的区块
4. 获取所需的节点hash：H(2)、H(01)、H(4567)
5. 计算merkleRootHash，并对比

1.2 支付类型

1.2.1 P2PK

scriptPubkey: <PubK> OP_CHECKSIG

scriptSig: <Sig>

verify: <Sig> <PubK> OP_CHECKSIG

1.2.1 P2PKH

scriptPubkey: OP_DUP OP_HASH160 <pubkeyHash> OP_EQUALVERIFY OP_CHECKSIG

scriptSig: <Sig> <PubK>

verify: <Sig> <PubK> OP_DUP OP_HASH160 <pubkeyHash> OP_EQUALVERIFY OP_CHECKSIG

1.2 支付类型

1.2.3 MS

scriptPubkey: 2 <PubK1> <PubK2> <PubK3> 3 OP_CHECKMULTISIG

scriptSig: OP_0 <Sig1> <Sig2>

verify: OP_0 <Sig1> <Sig2> 2 <PubK1> <PubK2> <PubK3> 3 OP_CHECKMULTISIG

1.2.1 P2SH

script: 2 <PubK1> <PubK2> <PubK3> 3 OP_CHECKMULTISIG

redeemScript: 2 <PubK1> <PubK2> <PubK3> 3 OP_CHECKMULTISIG

scriptPubkey: OP_HASH160 RIPEMD160(SHA256(script)) OP_EQUAL

scriptSig: <Sig1> <Sig2> <redeemScript>

verify: <Sig1> <Sig2> <redeemScript> OP_HASH160 RIPEMD160(SHA256(script)) OP_EQUAL

2.1 背景

1. 比特币网络拥堵、扩容迫在眉睫

2. 比特币交易延展性问题长期困扰一直得不到解决

2.2 解决方案

比特币核心开发员Pieter Wuille 在香港提出隔离见证 (Segregated Witness，简称SW) 软分叉方案，以期彻底解决这些问题。SW用户在交易时，会把比特币传送到有别于传统的地址。当要使用这些比特币的时候，其签署 (即见证)并不会记录为交易ID的一部份，而是另外处理。

2.3 SW交易类型

1. P2WPKH、P2WSH

交易类型	P2PKH	P2WPKH	P2SH	P2WSH
ScriptPubkey	OP_DUP OP_HASH160 <pubkeyHash> OP_EQUALVERIFY OP_CHECKSIG	OP_0 <20-byte-pubkey-hash>	OP_HASH160 RIPEMD160(SHA256(script)) OP_EQUAL	OP_0 <32-byte-witnessScript-hash>
ScriptSig	<Sig> <PubK> OP_CHECKSIG	(empty)	<..> <..> <redeemScript>	(empty)

P2WPKH witness: <Sig> <PubK>

P2WSH witness: <Sig1> <PubK1> <Sig2> <PubK2> <witnessScript>

P2WSH witnessScript: 0 <Sig1> <Sig2> 2 <PubK1> <PubK2> <PubK3> 3 OP_CHECKMULTISIG

2.3 SW交易类型

2. P2SH-P2WPKH、P2SH-P2WSH

P2PKH的地址类型以1打头 P2SH的地址类型以3打头。为了与旧版本兼容，隔离见证以P2SH的方式来实现P2WPKH、P2WSH。对于一笔隔离见证的交易，旧节点把其当成普通P2SH交易处理，而新节点则当成新型隔离见证交易类型处理。

交易类型	P2SH-P2WPKH	P2SH-P2WSH
ScriptPubkey	OP_HASH160 <redeemScriptHash> OP_EQUAL	OP_HASH160 <redeemScriptHash> OP_EQUAL
ScriptSig	<redeemScript>	<redeemScript>

P2SH-P2WPKH redeemScript: OP_0 <20-byte-pubkey-hash> verify: <redeemScript> OP_HASH160 <redeemScriptHash> OP_EQUAL —> CheckSig(P2PKH)

P2SH-P2WSH redeemScript: OP_0 <32-byte-witnessScript-hash> verify: <redeemScript> OP_HASH160 <redeemScriptHash> OP_EQUAL —> CheckSig(MS)

2.3 SW交易类型

3. P2PKH、P2SH-P2WPKH、P2SH-P2WSH交易过程

Image url : http://cdn.8btc.com/wp-content/uploads/2016/12/10.jpg

2.4 SW的效果

扩容： non-witness data + witness data * 0.25 < 1MB

协议	~Tx 尺寸（字节）	基础尺寸（字节）	见证尺寸（字节）	见证折扣（字节）	基础区块尺寸（字节）	总区块尺寸（字节）	容量（txs/块）	比率（tx/s）
标准	500	500	0	0	1,000,000	1,000,000	2,000	3.33
隔离见证	500	250	250	62.5	1,000,000	1,600,000	3,200	5.33
等价标准	500	500	0	0	1,600,000	1,600,000	3,200	5.33

消除交易延展性：

签名转移至见证字段，使得交易不再具有延展性，避免交易延展性攻击。

为闪电网络架设铺平道路：

消除延展性，能够实现未对父交易签名的情况下签名子交易，使得闪电网络得以顺利实施。

3.1 背景

1. 比特币系统日益堵塞，交易手续费高昂

2. 隔离见证扩容只能解决燃眉之急，并非长远之计

3. 小额高频交易在比特币网络中几乎无法实现

怎么解决?

POW动不了?

死守1M?

链上没法玩。

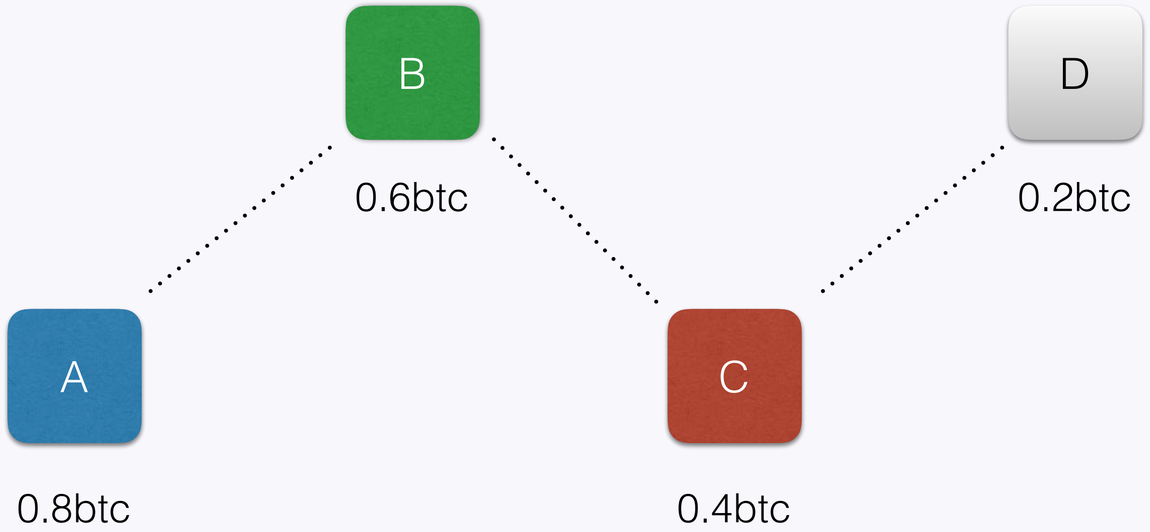
反向思考问题：　链上无法扩容转链下

发不了那么多交易干脆不发

闪电网络!

优权天成 YQTC TECH

3.2 LN基本原理



A -> C : 0.5btc

1. C想出一个随机数R，将H(R)的值告诉A

2. A向自己的好友B宣称：如果你能够在2天内给我一个值R’，使得H(R’)=H(R)，那么我将给你一张0.5btc的欠条

3. B向自己的好友C宣称：如果你能够在1天内给我一个值R”，使得H(R”)=H(R)，那么我将给你一张0.5btc的欠条

4. C知道该值并给B自己当初设定的值R。B验算通过后给C一张0.5btc欠条。B将该值给A，A经过验算确认无误后给B打一张0.5btc欠条。

B -> D : 0.1btc

.
.
.

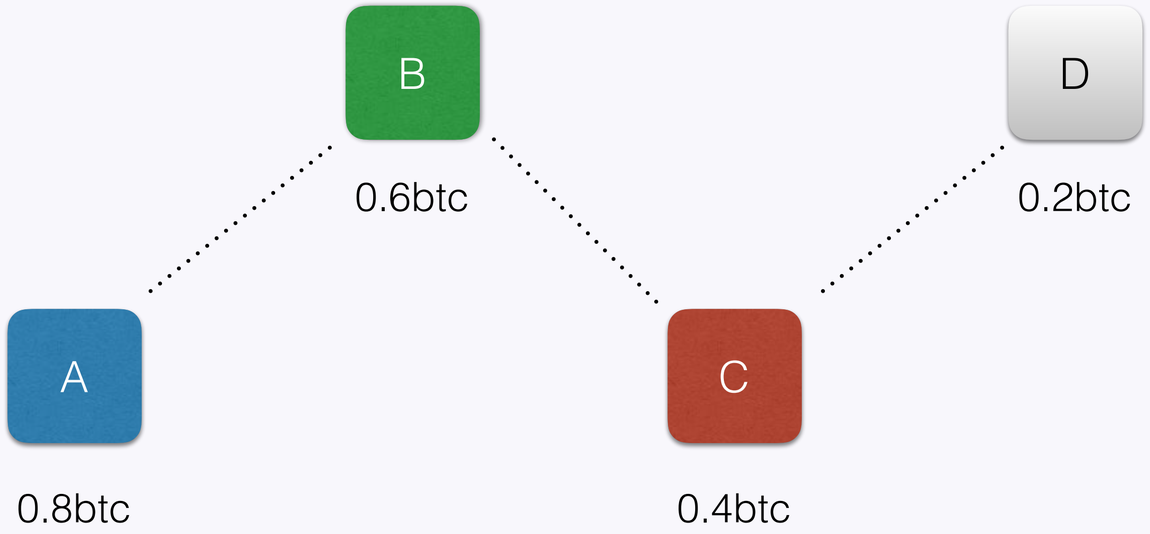
A: 0.8btc → A: 0.3btc

B: 0.6btc A: 0.5btc → B: 0.5btc

C: 0.4btc B: 0.6btc → C: 0.9btc

D: 0.6btc C: 0.1btc → D: 0.3btc

3.2 LN基本原理



通道： 好友双方就资金往来最大欠条额的定义。

在上述案例中通道可定义成如下：

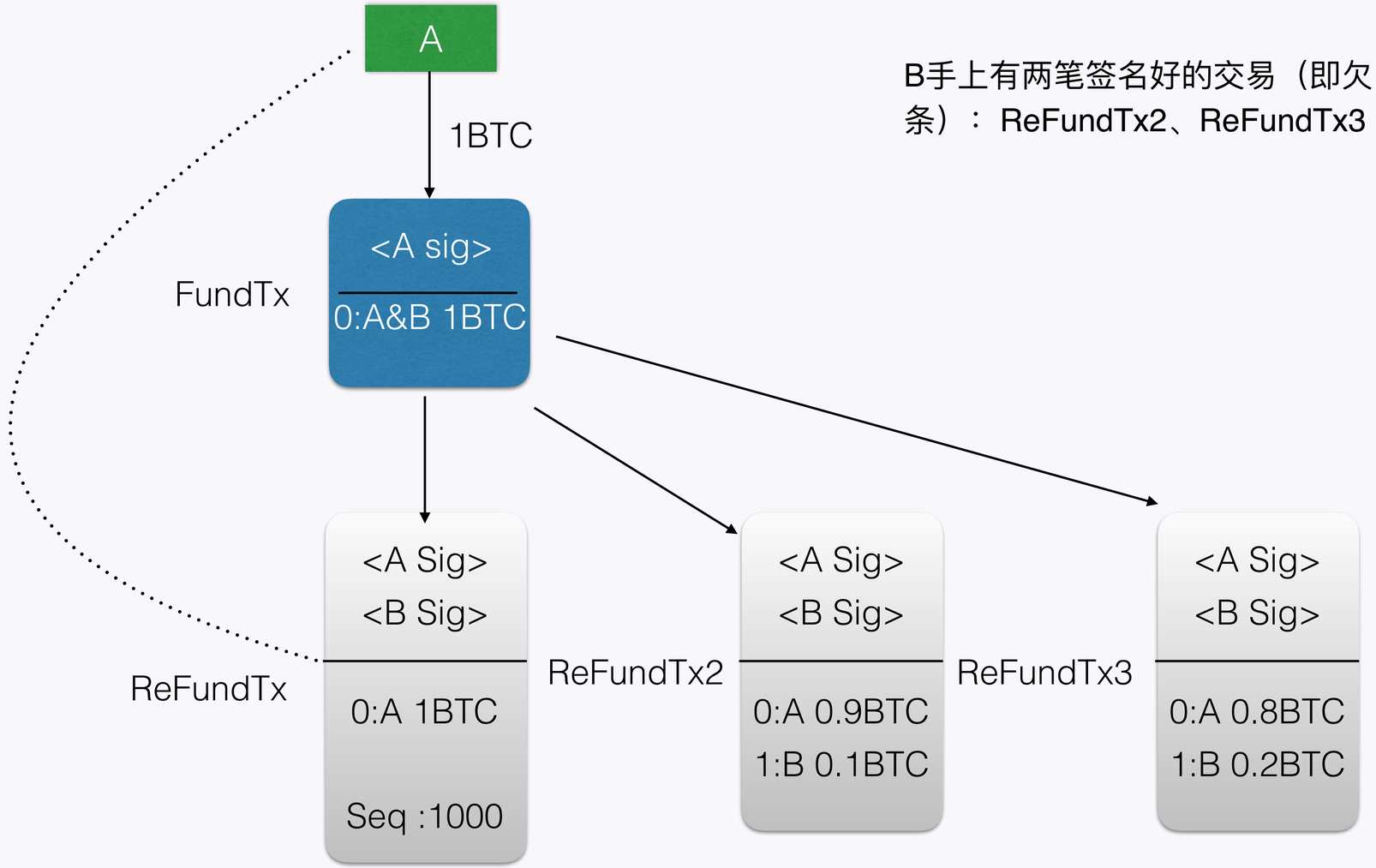
AB(0.5):BA(0) BC(0.6):CB(0) CD(0.1):DC(0)

哈希锁定： 在限定时间内提供一个原始值，其哈希值H(R)满足给定的值则可以获得一张欠条，并能够随时兑换。

由于区块链的去信任性，任何节点间都可以随意相互建立通道，从而组成一个庞大的网络。该网络内的成员间转账以欠条的形式给出，达到瞬间转账的效果，故称之为闪电网络!

3.3 微支付通道

微支付通道能够实现比特币的小额、高频交易处理，是一个单向传输通道。

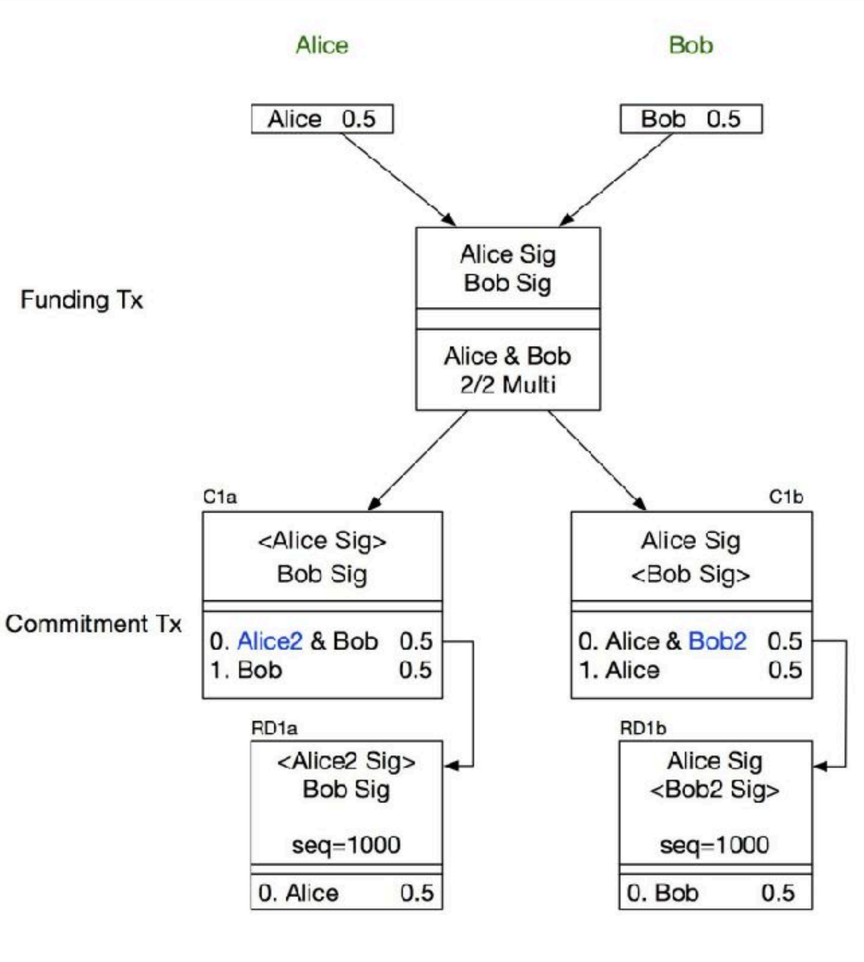


B手上有两笔签名好的交易（即欠条）：ReFundTx2、ReFundTx3

优权天成 YQTC TECH

3.4 RSMC

RSMC(Recoverable Sequence Maturity Contract) 即序列到期可撤销合约，由微支付通道发展而来，解决了通道中币单向流动问题。



委托交易: C1a、C1b

可撤销交易: RD1a、RD1b

步骤:

1. Alice、Bob准备好FundingTx，暂时不签名。
2. Alice准备好自己的子交易C1a、孙交易RD1a，让Bob先进行签名；Bob进行相同操作。
3. 当各自的子、孙交易准备好之后，开始对父交易进行互换签名。
4. 广播父交易FundingTx，Alice和Bob之间的通道建立完成。

Alice手上有两笔待广播的交易C1a、RD1a
Bob手上有两笔待广播的交易C1b、RD1b

疑问:

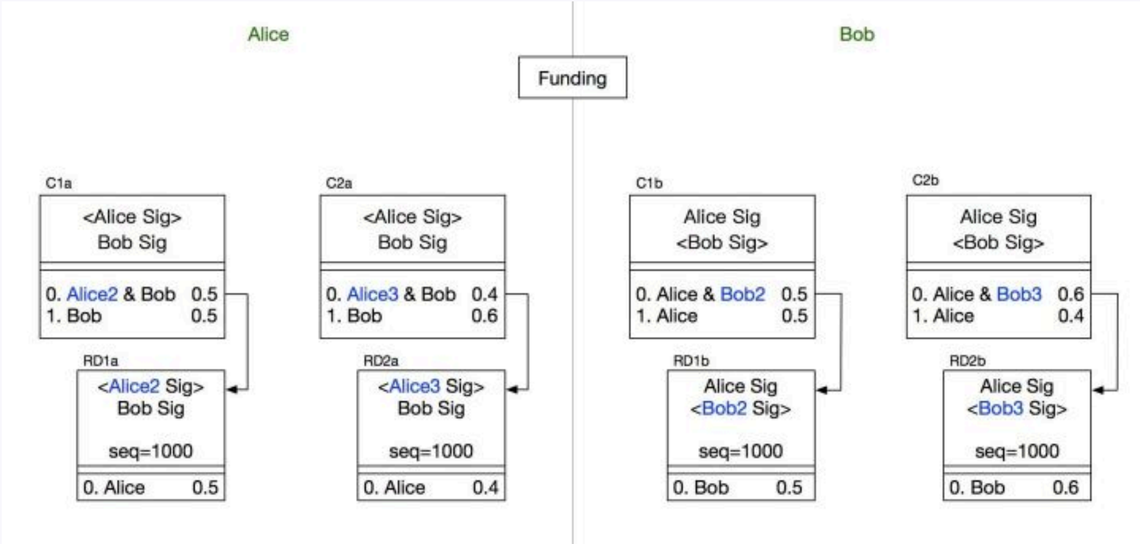
为什么先对子孙交易签名再对父交易签名?

同一个人为什么需要多个账户的公私钥?

为什么子交易和孙交易不能合并，而需要分开?

3.4 RSMC

Alice给Bob转账0.1BTC:



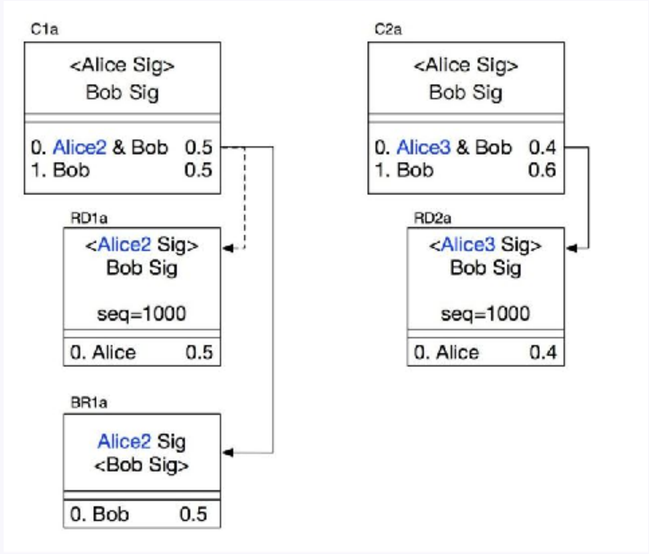
步骤：

1. Alice重新准备一套子孙交易C2a、RD2a。
2. Bob重新准备一套子孙交易C2b、RD2b。
3. Alice和Bob对各种的子孙交易互换签名。

Alice手上有四笔待广播的交易C1a、RD1a、C2a、RD2a。

Bob手上有四笔待广播的交易C1b、RD1b、C2b、RD2b。

如何防止Alice背叛?

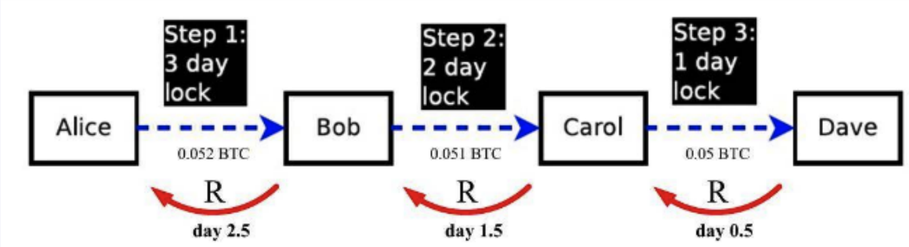


Alice在给Bob签名C2a、RD2a时必须附带惩罚交易BR1a，表示放弃C1a、RD1a。

3.5 HTLC

HTLC(Hashed Timelock Contract) 即哈希时间锁定合约，
解决了币跨节点传递的问题。

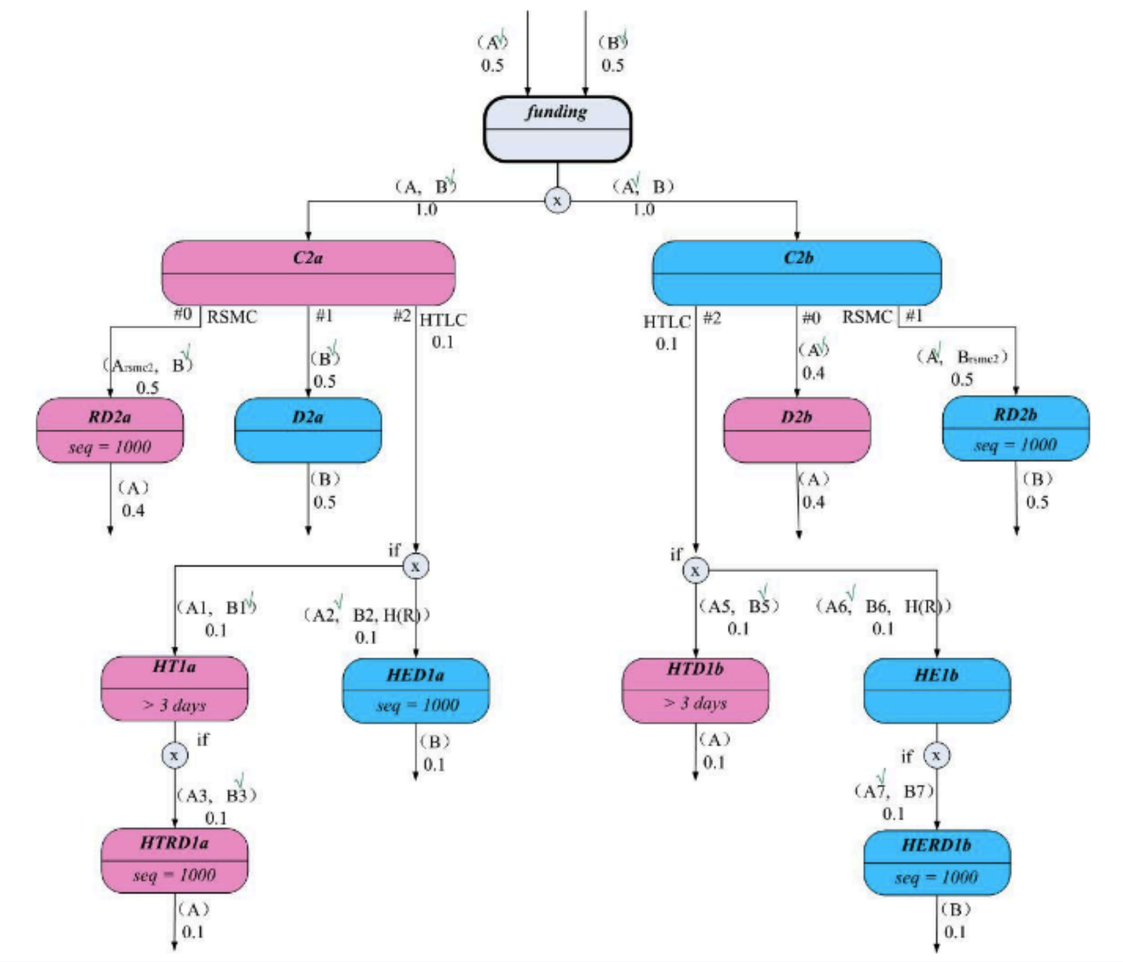
Alice使用HTLC给Dava转账0.5BTC:



优权天成 YQTC TECH

3.5 HTLC

RSMC + HTLC 完整交易



Alice使用HTLC给Dava转账0.1BTC:

HTLC解锁脚本

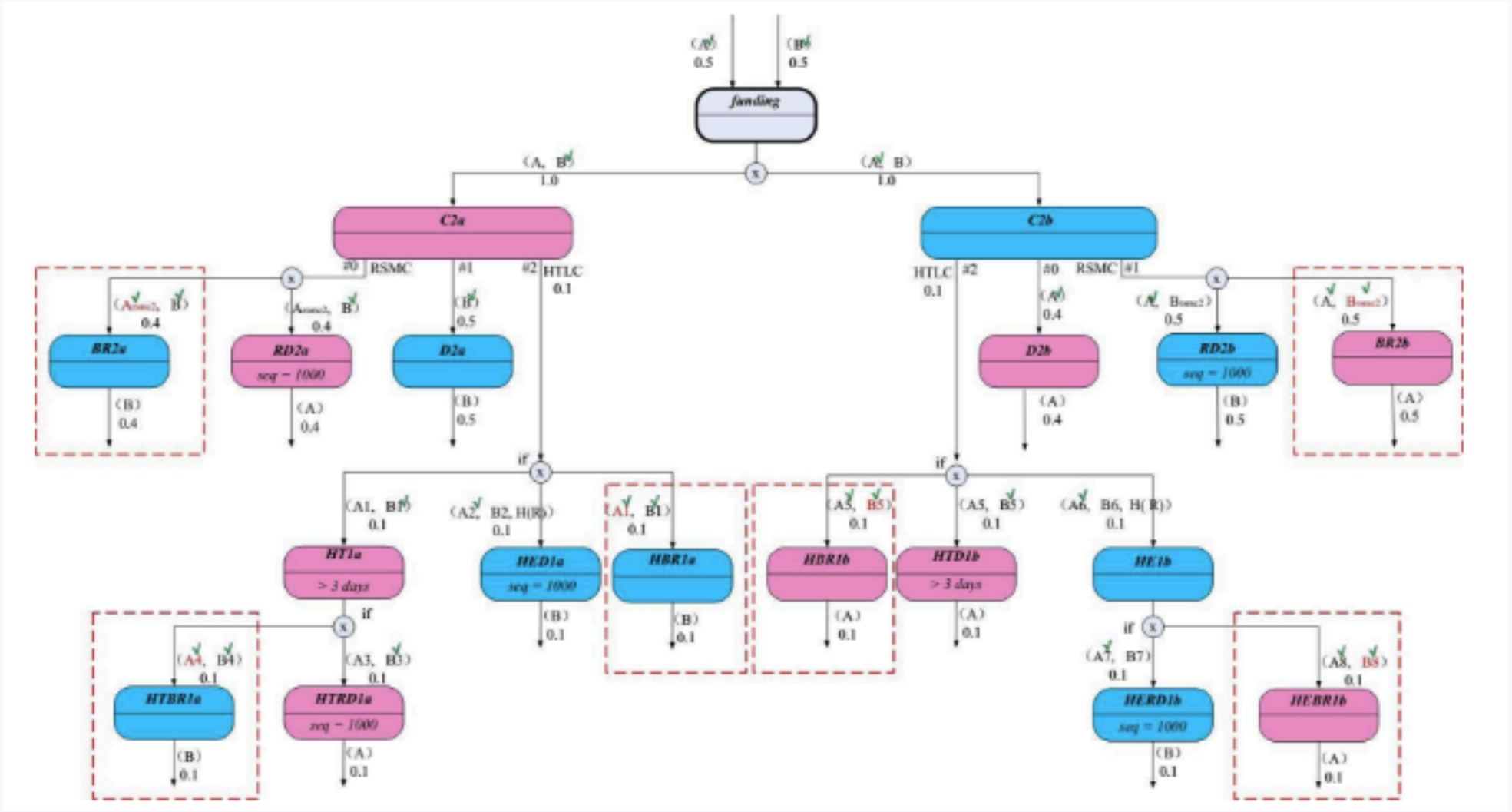
```
OP_IF
        OP_HASH160 <Hash160(R)> OP_EQUALVERIFY
        2 <Alice2> <Bob2> OP_CHECKMULTISIG
OP_ELSE
        2 <Alice1> <Bob1> OP_CHECKMULTISIG
OP_ENDIF
```

1. Alice准备好HT1a、HTRD1a交易，让Bob进行签名并取回
2. Alice准备好HED1a，自己签名后给Bob发送
3. 如果在超过规定时间仍不能得到符合条件的R，则Alice可以通过HT1a、HTRD1a、C2a、RD2a拿回自己的资金
4. 如果在规定时间Bob能够提供满足条件的R，则可以通过HED1a取走0.1个btc

3.5 HTLC

闪电网络终极版交易

闪电网络将比特币网络从一个支付系统改造成为了一个结算系统。比特币的交易脱离主链进行，只有当需要结算时才通过主链进行。大大减轻了比特币主链的负担，大幅提升交易速度。



4.1 介绍

跨链是什么?

跨链能够解决什么问题?

资产转移

原子交易

跨链数据oracle

跨链执行合约

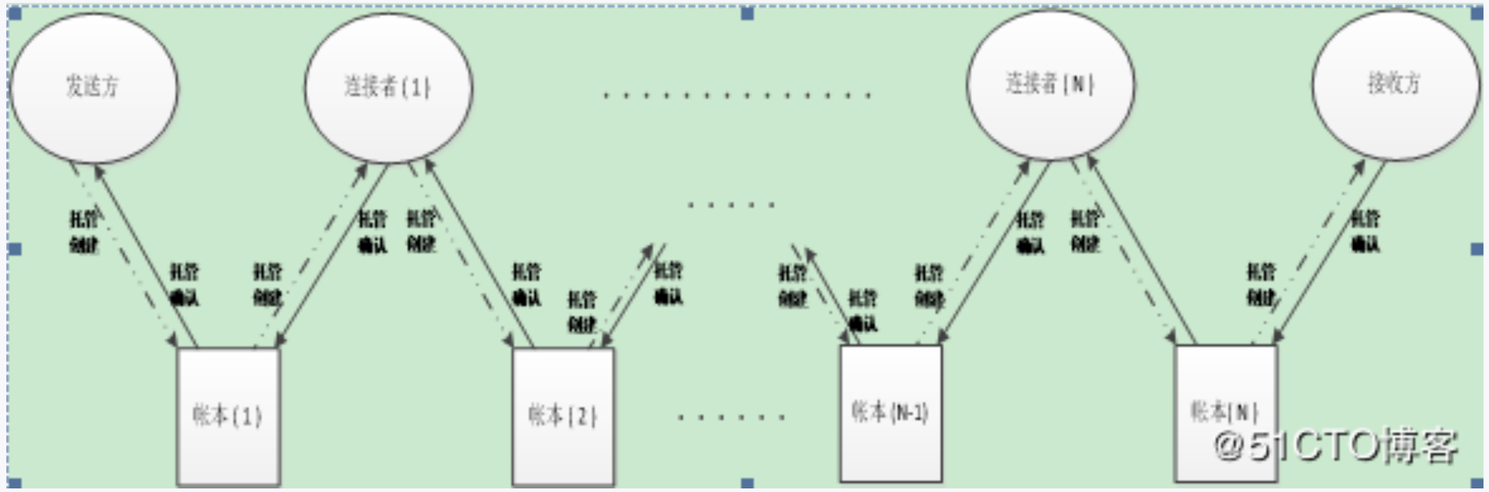
扩容、缓解主链压力

4.2 见证人模式

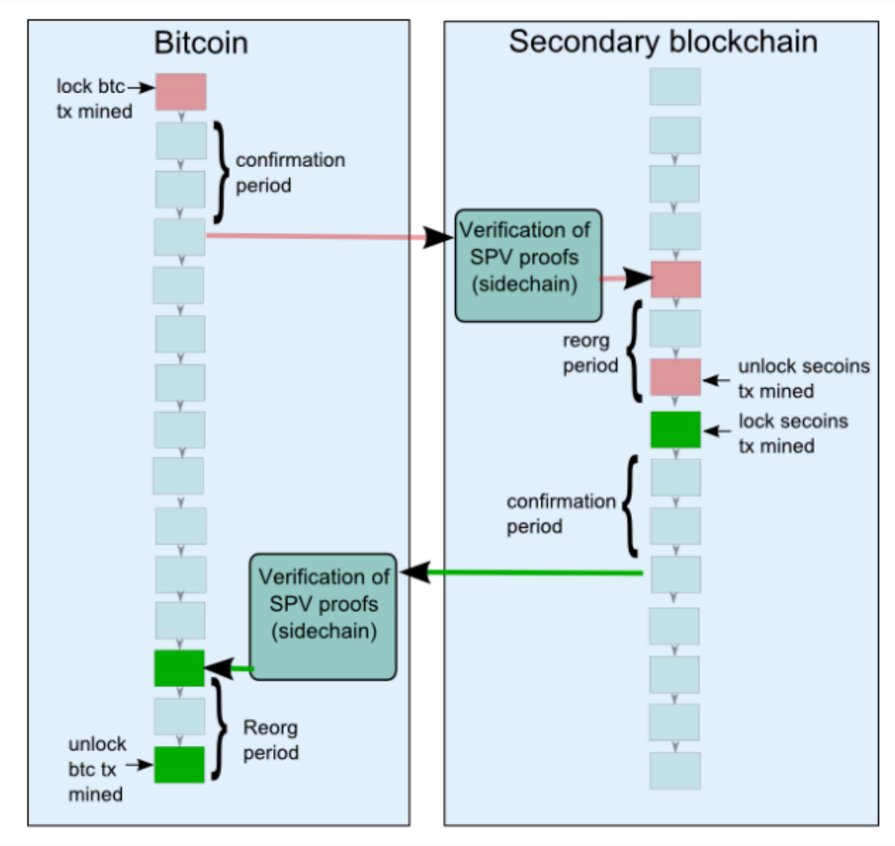
1. 可信任的中间人

2. 可信多方多重签名

Ripple:



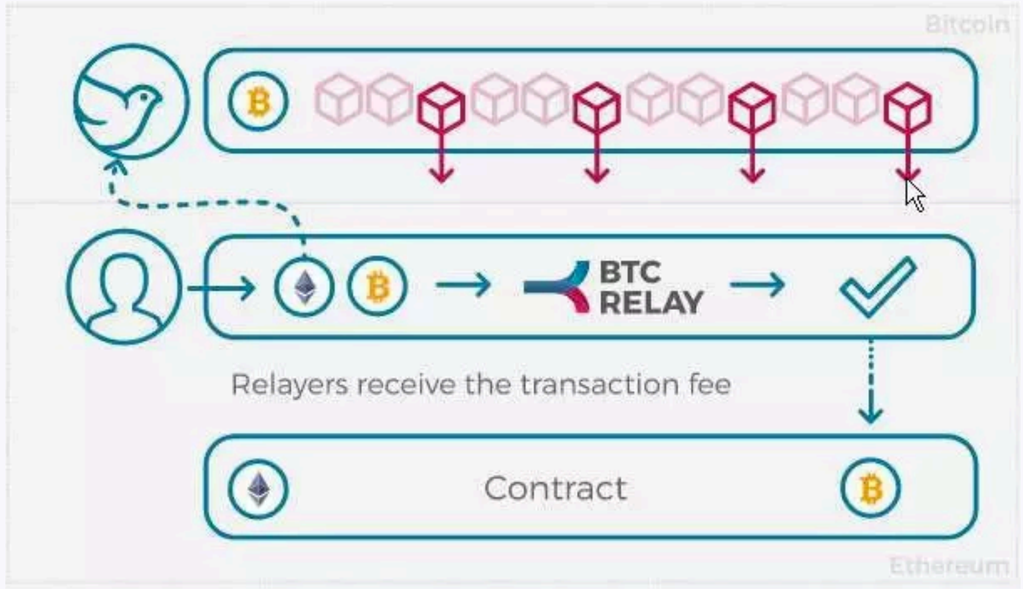
RootStock:



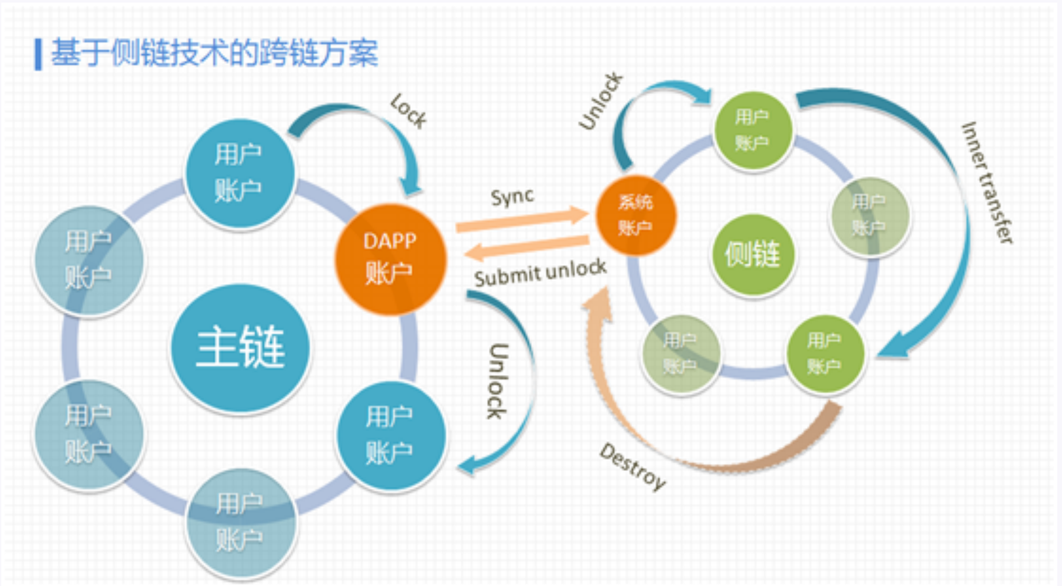
4.3 侧链/中继

B能够直接读取或者通过某种途径来获取A链的信息，则称B为A的侧链

BtcRelay:

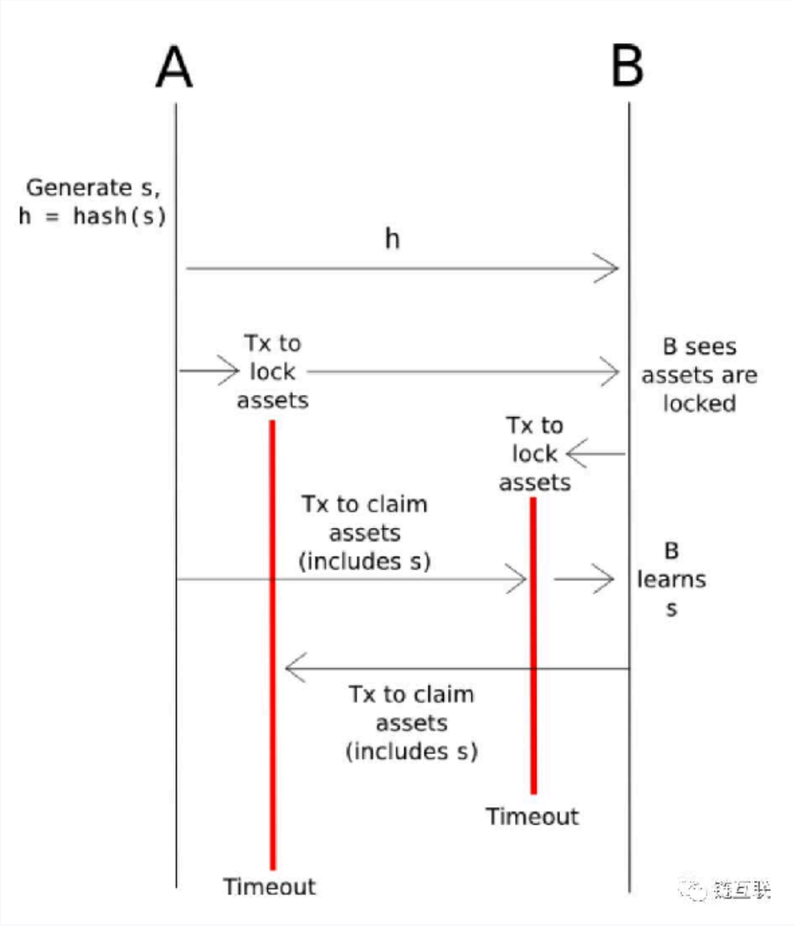


Asch:



4.4 哈希锁定

哈希锁定灵感来源于闪电网络，能够进行跨链资产交换



1. A生成一个随机数s，计算h=hash(s)，将h提供给B

2. A发送一笔交易，只要能够提供原始值s，，其H(s)满足条件就能够花费该笔输出，并设置超时时间2T

3. B看到A锁定比特币后创建智能合约，只要提供原始值s，其H(s)满足条件就能够获得一定数额以太币，并设置超时时间T

4.A通过s调用智能合约，取走B的以太币

5.B能够感知取走以太币的原始值s，并通过s取走A的比特币

参考文献

http://www.360doc.com/content/17/0831/16/46341144_683606363.shtml

http://www.8btc.com/tan90d144

http://8btc.com/article-3472-1.html

http://www.360doc.com/content/17/0709/07/31679168_669966473.shtml


THANK YOU
优权天成
YQTC TECH