全球区块链生态技术大会

Global Blockchain Eco-Technology Conference

区块链商用化之路

— 侧链扩展

朗豫

Bytom CTO

主办方 Geekbang. 极客邦科技 InfoQ

区块链前哨
BLOCKCHAIN OUTPOST

正本清源，打造链圈
第一技术公众号

掌握前沿区块链资讯
深度分析区块链技术
致力于区块链技术普及

扫码关注区块链前哨

TABLE OF

CONTENTS 大纲

- 区块链大规模商用瓶颈
- 侧链(Sidechain)技术的价值
- 业界对侧链的探索
- 比原链(Bytom) 上实现侧链
- 未来发展方向

区块链商用瓶颈

- 区块链交易体验差，成本高

  1. 在无边界的共识条件下，工作量证明机制需要一定的时间收敛
  2. DPOS, PBFT共识等都存在代理人风险， 扩展性差等问题
  3. 零确认存双花攻击风险，交易通道狭窄

- 区块链数据风险

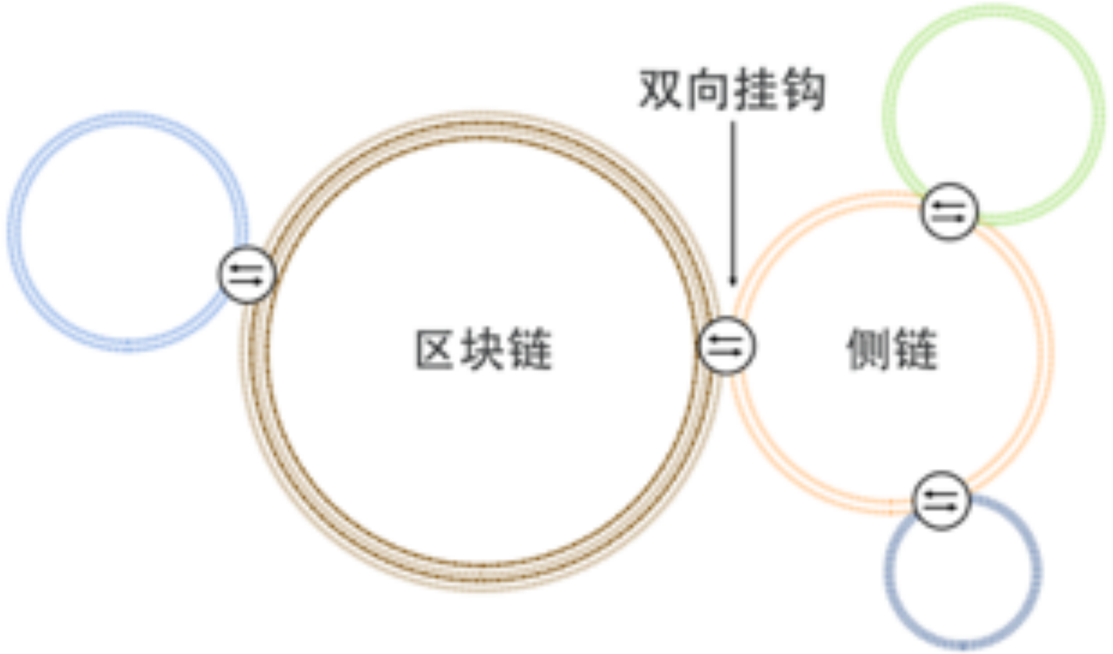
  1. 数据膨胀导致存储成本按用户数同比提升，不可持续
  2. 数据隐私暴露风险， 私密数据链上存储无法取得安全
  3. 需要业务分层机制，核心数据加密上链，无法篡改

侧链(Sidechain)

- 通过双向peg (楔入)将不同的区块链进行“连接”，使得多方价值可以在不同协议上进行交易和流转的技术

- 误区解读：“连接”指链上的交互， 不代表任何系统级的通信

- 带来问题：更多复杂性，欺诈性交易，软分叉风险



侧链特征

1. 主链token在侧链流通时还是主链，通常时1: 1的比例或者其他预定汇率。

2. 侧链自己不能产出主币，只能接受主链的输入，并在自己链上生成对应的主币。

3. 侧链可以有自己的token也可以没有。

4. 侧链需要足够的算力和共识保证侧链的安全。

5. 侧链独立于主链存在，侧链上发生的任何事情都不会影响主链，从而可以保证主链安全性。

为什么能解决问题

- 在主链安全性保障的前提下， 侧链可以在小范围共识，优化确认时间
- 多种侧链“并行”运行时，主链安全性和业务负载并不显著增加
- 侧链数据可以加密，在小范围传输，记录交易路径，且不泄露隐私

侧链技术方向

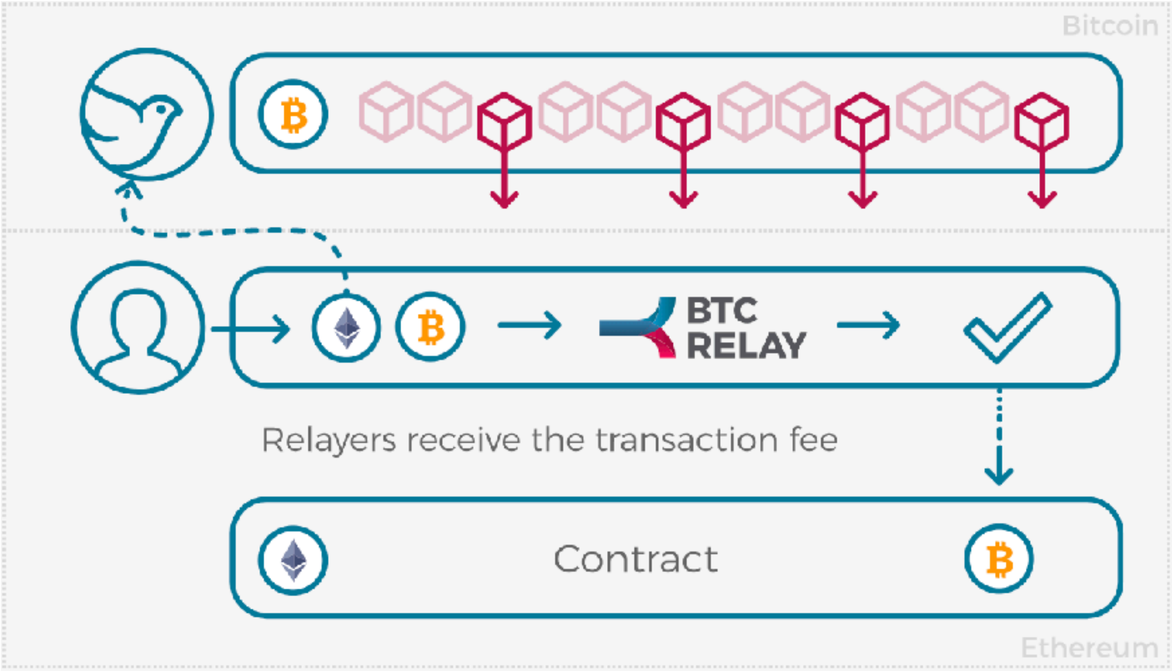
侧链的核心是解决跨链问题， 现阶段普遍使用：

1. 公证人机制（Notary schemes）
2. 中继（Relays）
3. 哈希锁定（Hash-locking）

公证人机制：中心化模式， 类似交易所

- BTC–Relay

基于Ethereum的合约实现，本质实现比特币的SPV客户端， 缺点在于需要外界的Feed，即比特币spv–proof–block 数据，和同时难以处理比特币分叉的特殊情况



- Rootstock（RSK）

建立在比特币区块链上的智能合约分布式平台。实现了以太坊虚拟机的一个改进版本，它将作为比特币的一个侧链，使用了一种可转换为比特币的代币作为智能合约的“燃料”。在RSK中，把比特币的相关信息写入sidechain，不断产生的区块信息写入SPV同时写入侧链，在比特币中任何区块产生变化都有相应的反应。在将代币解锁为比特币时使用了哈希锁定技术

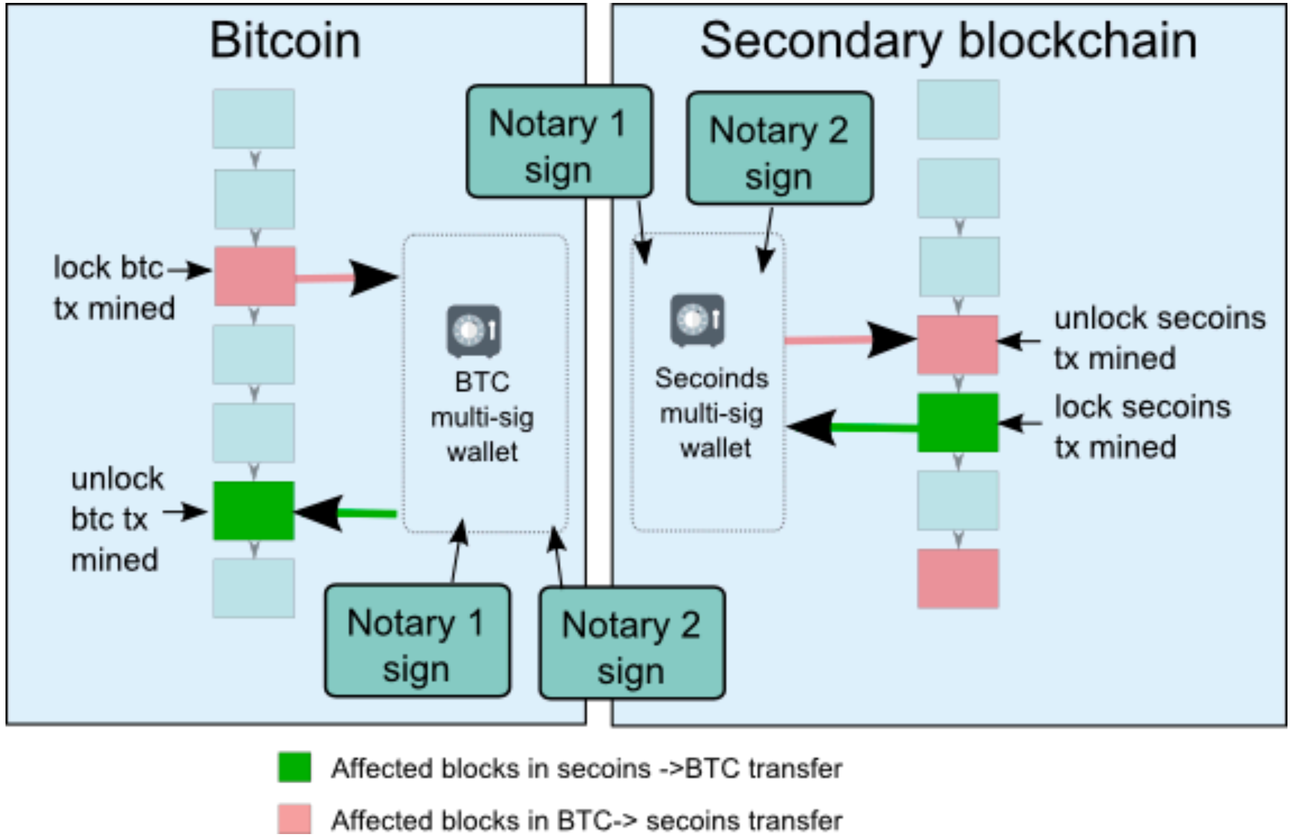
在Bytom上实现侧链

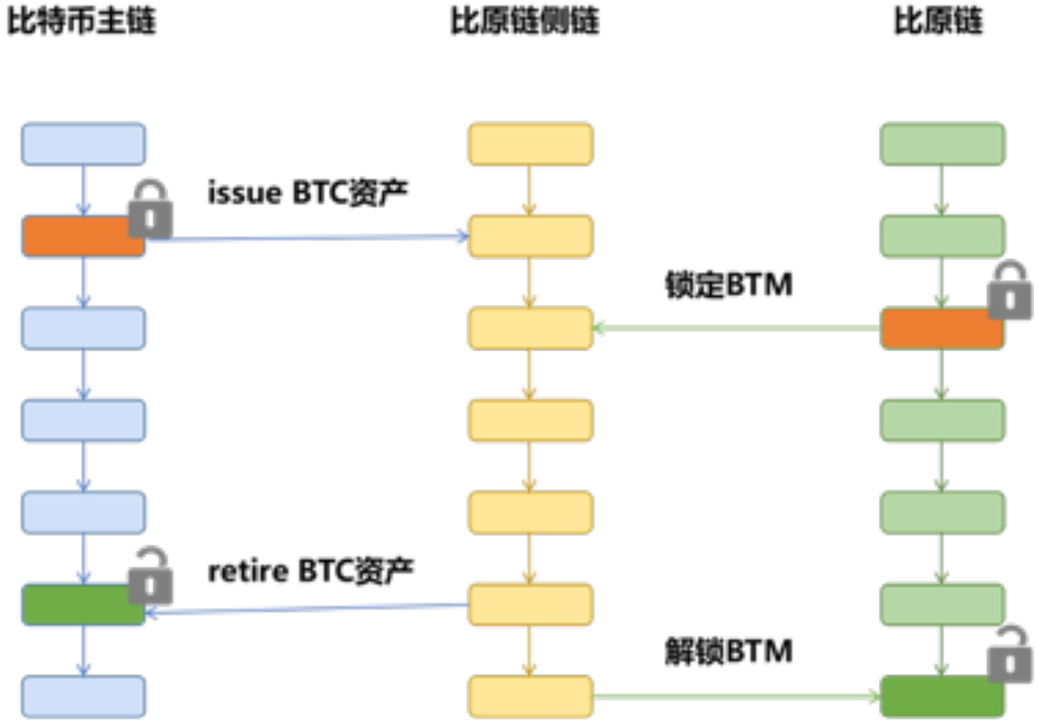
- Bytom是一种多元比特资产的交互协议，运行在Bytom有不同形态的、异构的比特资产（原生的数字货币、Token）和原子资产（股权，债券，收益权等物理世界对应的金融和非金融资产）

- 基于POW共识的区块链需要对传统世界资产进行包容性，合规性，效率性支持

- Bytom基于双向锚定（two-peg）进行修改，实现联合锚定（fed-peg）的侧链模型， 引入多方中间人机制对于资产的质量和合规性进行把控

实现场景


Bitcoin
Secondary blockchain
Notary 1 sign
Notary 2 sign
lock btc tx mined
BTC multi-sig wallet
Secoinds multi-sig wallet
unlock secoins tx mined
lock secoins tx mined
unlock btc tx mined
Notary 1 sign
Notary 2 sign
Affected blocks in secoins ->BTC transfer
Affected blocks in BTC-> secoins transfer


比特币主链
比原链侧链
比原链
issue BTC资产
锁定BTM
retire BTC资产
解锁BTM

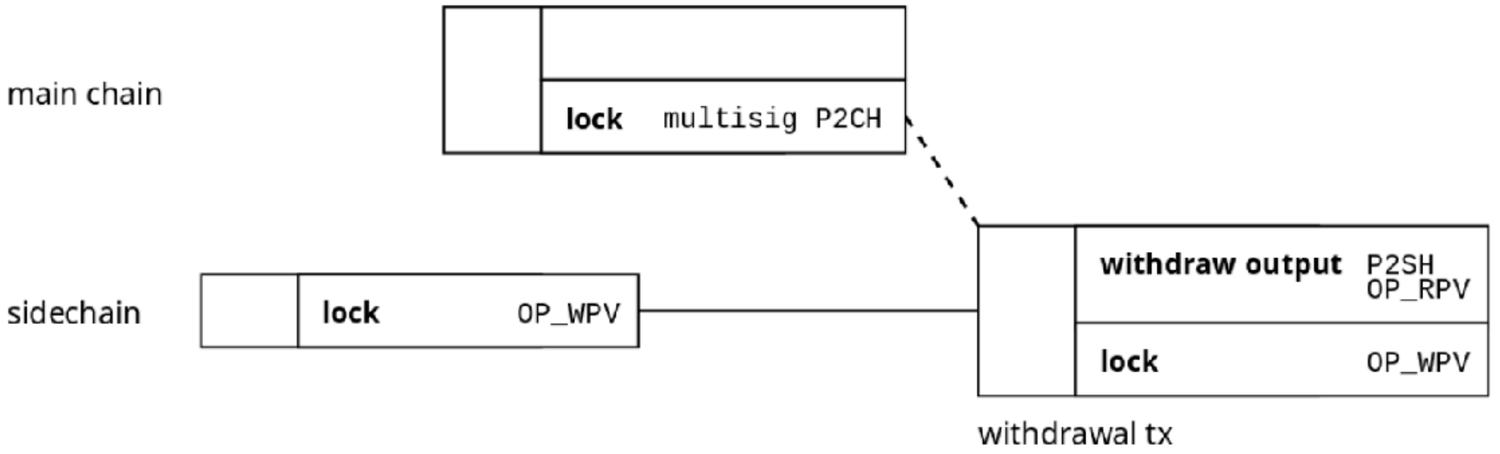
步骤关键点

- “锚定”主链资产，传递至侧链
- 等待侧链资产“成熟”， 资产在侧链流转交易
- 侧链资产“赎回”， 主链释放锁定资产， 结算手续费

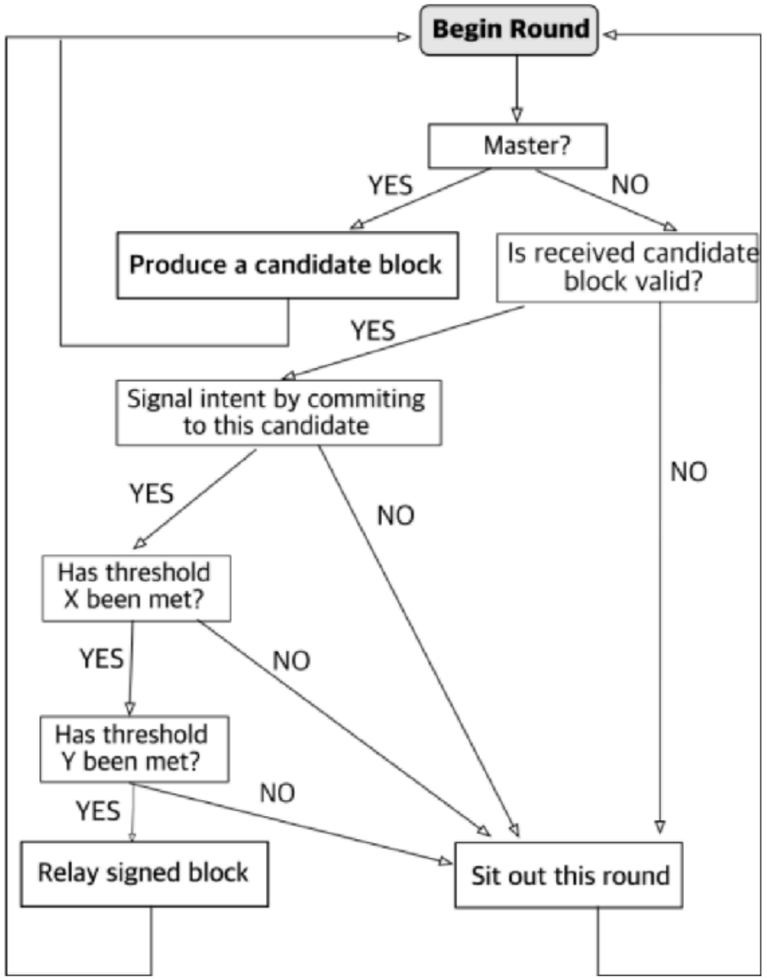
锚定

```
OP_IF
    <nLockHeight>
    <lockTxHash>
    <nLocktxOut>
    <fraudBounty>
    <HASH160(secondScriptPubKey)>
    <genesisHash>
    OP_REORGPROOFVERIFY
OP_ELSE
    144
    OP_CHECKSEQUENCEVERIFY
    OP_DROP
    OP_HASH160
    <HASH160(destinationScript)>
    OP_EQUAL
OP_ENDIF
```

- OP_WPV：运行合约堆栈中的脚本解锁侧链资产
- OP_RPV： 检测主链的SPV-BLOCK数据重新组织区块结构



侧链“成熟”运转



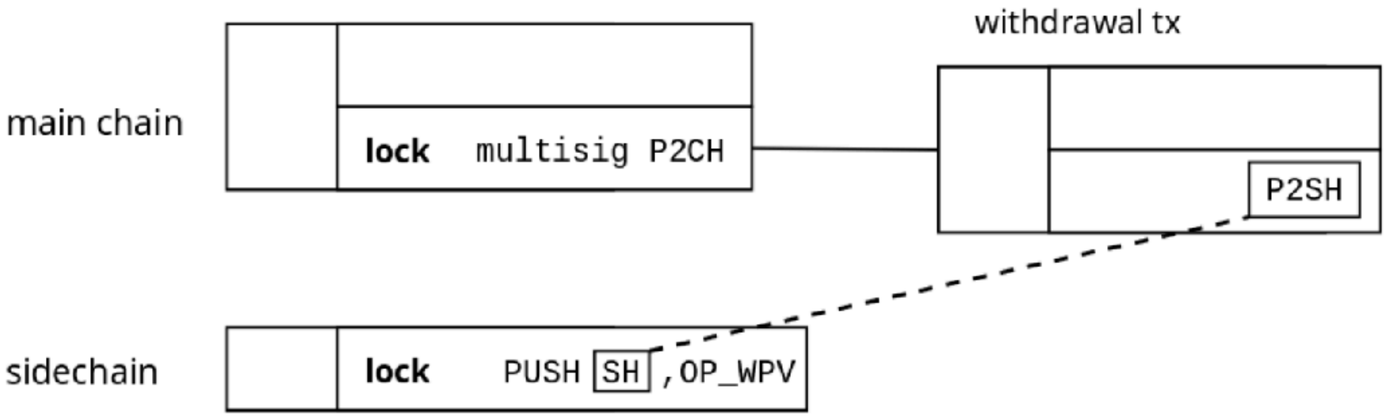
- 无Token发行共识过程

每一轮选择一个Block Producer， 查看是否有X，Y门限满足，则签发新Block

X，Y可以是各种条件，包括是否有交易，是否到截止时间

主链“赎回”

- 侧链PUSH ScriptHash，即锁定侧链资产
- 主链通过多签交易“赎回”被锁资金
- 主链资产可以正常交易



未来发展方向

- 结合二层扩展闪电网络，可以将侧链资产和主链资产同时嫁接
- 侧链在TPS和不可篡改性上进行优化， 达到普通业务场景需求
- 完善侧链和主链切换的工具，现今操作复杂且不用户友好
- 预计在2019年后侧链技术会真正用于生产环境

主办方 Geekbang. 极客邦科技 InfoQ

THANKS