



隐私与跨链

演讲人：宁志伟



目录 contents

01

隐私技术概览

02

跨链技术概览

03

方案对比分析

04

CITA 侧链方案

隐私技术概览







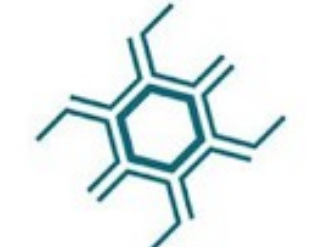





◆密码学方案

- 零知识证明
- 环签名
- 多方计算
- 同态加密

◆可信硬件

◆常规手段

- 混币
- 侧链 /offchain

<u>Privacy Coins</u>	<u>Smart Contract Privacy</u>
 CASH  MONERO  BEAM  Grin  MobileCoin	Zether  KEEP   enigma OASIS LABS
<u>Privacy Infrastructure</u>	<u>Privacy Research</u>
CoinJoin  KOVRI BOLT  ORCHID NUCYPHER  STARKWARE	Zero-Knowledge Multiparty Computation Fully Homomorphic Encryption 

优缺点分析

◆密码学方案

- 性能差
- 前向安全风险
- 不支持智能合约
- 系统安全性高

◆可信硬件

- 侧信道攻击
- 受制于厂商
- 性能较差
- 支持智能合约

◆常规手段

- 性能好
- 数据隔离
- 系统安全性低

相关工作

- ◆ 零知识证明

- ◆ https://github.com/cryptape/cita/blob/develop/cita-executor/core/src/contracts/native/zk_privacy.md
- ◆ <https://zhuanlan.zhihu.com/p/51469616>
- ◆ <https://zhuanlan.zhihu.com/p/51472383>

- ◆ 环签名

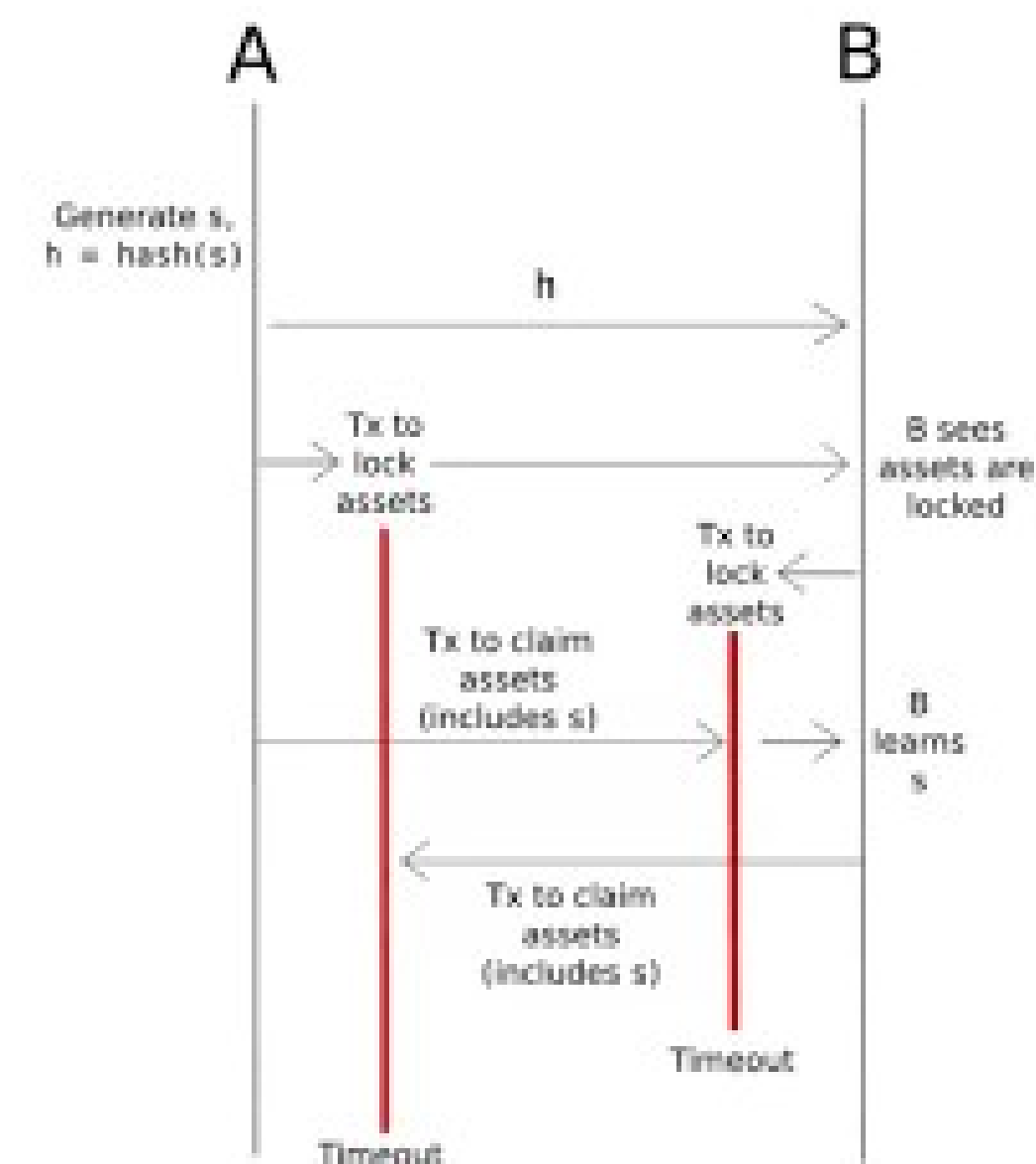
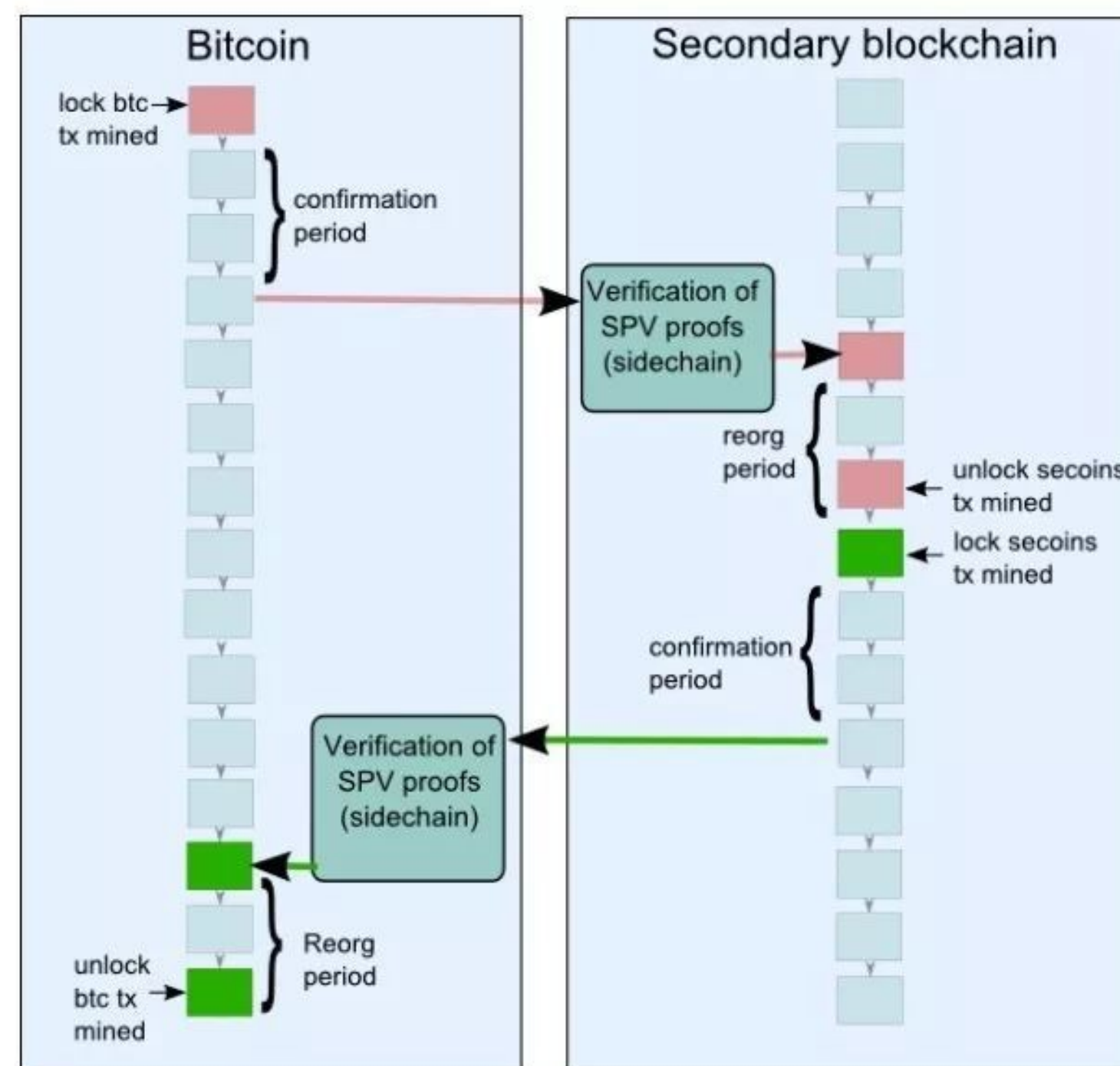
- ◆ <https://zhuanlan.zhihu.com/p/34359611>

- ◆ 可信硬件——SGX

- ◆ https://www.initc3.org/files/retreat/sgx_contracts.pdf

跨链技术概览

- ◆ 见证人
 - 交易所
 - 多重签名
- ◆ 侧链 / 中继
 - 链能相互验证对方信息
 - 锁定资产 - 验证证明 - 解锁资产
- ◆ 哈希锁定
 - 哈希承诺锁定资产
 - 链下交换信息



方案对比

功能	见证人	侧链 / 中继	哈希锁定
跨链类型	全部	全部	部分
信任模型	多数诚实	链正常工作	链正常工作
支持跨链资产转移	是	是	否
支持跨链资产交换	是	是	是
支持跨链先知	是	是	不直接
支持跨链产权质押	是	是	较难
实现难度	中等	难	容易

CITA 侧链方案

◆ 为什么是侧链方案

- 功能最强大
- 同构链

◆ 系统安全性设定

- 侧链验证者是主链验证者的子集，侧链无条件相信主链的状态
- 侧链验证者在主链上抵押保证金，解决主链不相信侧链的问题
- 传递的是信息是密码学证据（默克尔树证明），对 Relayer 无要求

◆ 侧链管理

- 假定主链已经存在，并且永久运行，上面有侧链管理合约
- 侧链可以动态的开启和关闭
- 可以有多个侧链，但是只有一条主链
- 侧链提供验证者公钥列表进行注册，获取管理合约分配的 id

CITA 侧链方案

◆侧链启动

- 注册并得到侧链 id
- 将侧链 id 和主链的验证者公钥列表写入创世块
- 运行，在主链上的侧链管理合约中 enable 对应的侧链

◆CITA 提供的功能

- `cita_getTransactionProof` 传入交易 hash，返回证明该交易已经上链的证据
- 提供系统合约验证前述证据

◆跨链

- 主链和侧链双向皆可
- 侧链之间不能直接跨链，需要通过主链中转

跨链合约

```
address portal_account;

event cross_chain(uint256 from_chain_id, address origin_contract, uint256 to_chain_id, address
dest_contract);

// chain id must be first argument, relayer can extract chain_id
function send_to_side_chain(uint256 to_chain_id, address dest_contract, uint256 _value) {
    require(balanceOf[msg.sender] >= _value);
    balanceOf[msg.sender] -= _value;
    balanceOf[portal_account] += _value;
    cross_chain(chainmanager.chain_id, msg.to , to_chain_id , dest_contract, RECV_FUNC_HASHER);
}

function recv_from_side_chain(raw_tx, block_header, receipt_merkle_tree_proof) {
    require(raw_tx.dest_contract == msg.to); // Check dest contract address
    require(raw_tx.to_chain_id == chainmanager.chain_id); // Check chain_id
    // Check tx proof after valid check because verify_tx_proof will record tx hash to prevent
    duplication use the proof
    require(verify_tx_proof(raw_tx, block_header, receipt_merkle_tree_proof));
    balanceOf[raw_tx.sender] += raw_tx._value;
    balanceOf[portal_account] -= raw_tx._value;
}
```

CITA 侧链方案

◆侧链关闭

- 在侧链系统管理合约中 disable 该侧链
- 等待一段举证时间，没有问题才能拿回保证金
- 如果发现作恶情况，扣除保证金

◆退出机制设定

- Relayer 同步侧链的每个区块头到主链的侧链管理合约
- 验证之后记录该条侧链每个高度的 state root
- 用户通过 getStateProof 证明自己的剩余资产
- 验证者对用户的举证有异议，提交最新高度的 state proof 进行反驳
- 针对用户一直不上线的情况，在跨链的同时，relayer 负责获取 state proof
- 侧链关闭时还没有执行的跨链交易，可以获取 nonce 的 state proof，直接回退到主链

参考资料

- ◆ <https://ethfans.org/posts/an-overview-of-privacy-in-cryptocurrencie>
- ◆ <https://zhuanlan.zhihu.com/p/52208681>
- ◆ <https://ethfans.org/posts/chain-interoperability-report>
- ◆ https://docs.nervos.org/cita/#/crosschain/crosschain_contract_example

THANK YOU



CRYPTAPE
秘境科技

