BraftChain: 搭建区块链与智能合约平台

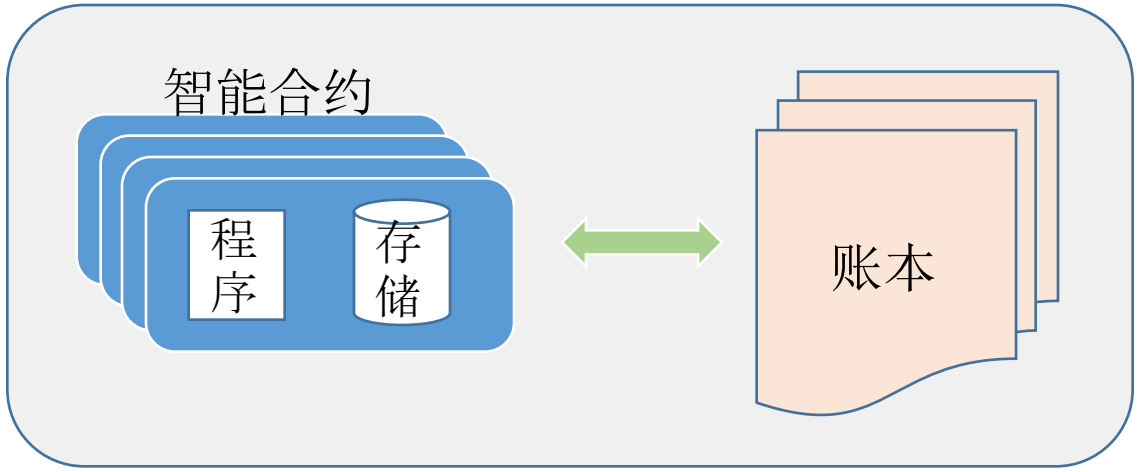
比特大陆 庄重
zhong.zhuang@bitmaintech.com
2016-03-20

比特币与智能合约

- 智能合约是一段无法修改执行行为和结果的程序，控制着数字货币或者其他数字资产
- 比特币与智能合约
  - 中本聪引入了内建的脚本语言支持各种交易类型，带来可能性
  - 比特币对智能合约的支持是有限的
    - 没有循环
    - 程序能使用的资源（内存，CPU 时间）有限
    - 无法保存状态
    - 许多设计上的指令被禁用或者还未加入
  - 常见的应用
    - 多重签名钱包

区块链+智能合约

- 解决这些问题的思路有
  - 合约不在区块链上执行(offchain)，依赖于可信的硬件或者第三方
  - 在链下执行并提供零知识证明，在区块链上做验证
  - 以太坊
    - 合约在区块链上执行
    - 每个节点都能得到确定而唯一的状态
    - 代价是可扩展性和私密性



BraftChain

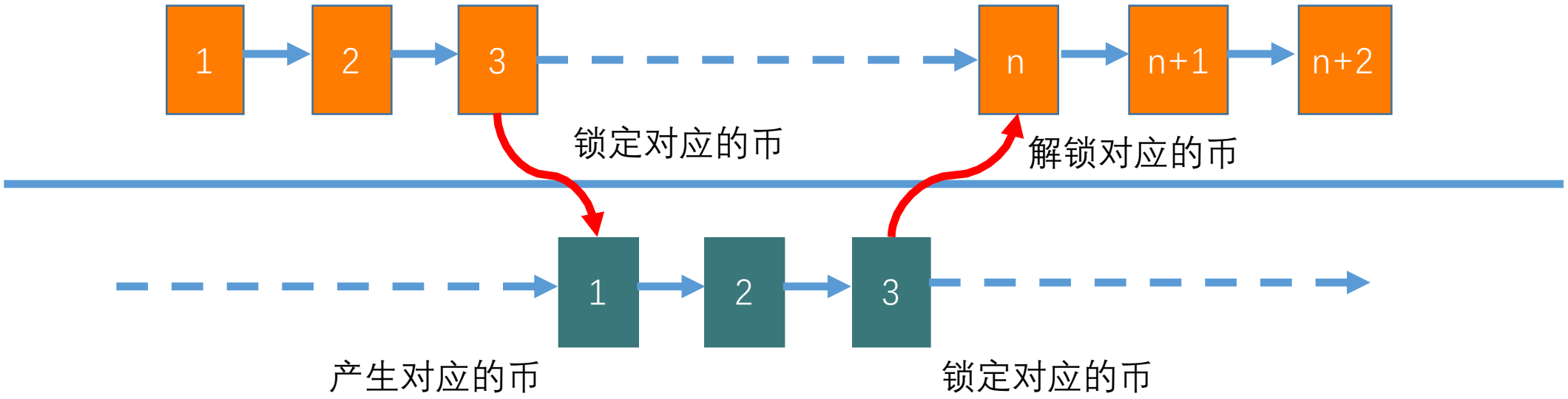
- 可作为私有链或者联盟链运行
- 比特币或者其他数字货币的侧链，双向锚定
- 基于Braft算法的共识协议
- 兼容以太坊的智能合约
- 完善的升级和管理机制

侧链

侧链的概念

- 把比特币或者其他数字货币转移到另一条区块链上，产生对应的侧链币

- 双向锚定意味着侧链上的币也能再转移回主链



侧链的实现方式

- 联盟+多签名地址
  - 目前已经实用
- BlockStream 公司的 Sidechain 项目
  - 依赖于 Bitcoin Core 对于所需要的新脚本指令的支持
  - 会跟进相应的实现方式
- Drivechain

BraftChain的侧链实现

- 主链上有联盟地址，转入的币被锁定在这个地址上
- 联盟地址是 n-m 的多签名地址
- 每个BraftChain节点 运行一个与主链同步的网关，控制解锁联盟地址上的币，通知节点处理转入的币
- 转入过程需要等待较长的时间(>10小时)避免主链分叉的情况
- 通过和参与方合作，可以采取收手续费等参与方承担一定风险的方式加快转入的速度

BraftChain

BITMAIN

技术特点

- BraftChain共识协议基于 Raft算法，支持Byzantine Fault Tolerance，在不超过1/3的节点异常（出现故障或恶意攻击）的情况下可以正常运行

- 协议保证在正常运行时区块链不会出现暂时或永久的分叉——**一次确认即为可靠确认**

- 交易确认速度可达到**秒级**

- 节点运营方均为实名，并且有严格的增删节点机制，以保证网络质量以及异常情况可追责

协议升级机制

- BraftChain支持一种特殊类型的区块“Reconfig Block”，用于更改配置和更新协议，如调整区块容量，升级智能合约虚拟机等等。标准流程为：
- 各节点运营方讨论通过更新方案
- 上线新的程序文件，但仍以原配置运行（此时区块链的运作没有发生变化）
- 写有新配置的Reconfig Block通过（原配置下的）共识协议加入区块链
  - 意味着有2/3以上的节点开始以新配置运行
- 之后的区块将按照新配置确认和执行

智能合约

智能合约的实现

- 扩展了以太坊虚拟机 EVM 的指令
- 可直接运行以太坊上编译的智能合约
- 兼容以太坊的 Web3.js，可以无缝切换到 BraftChain
- 开发中的即时编译优化

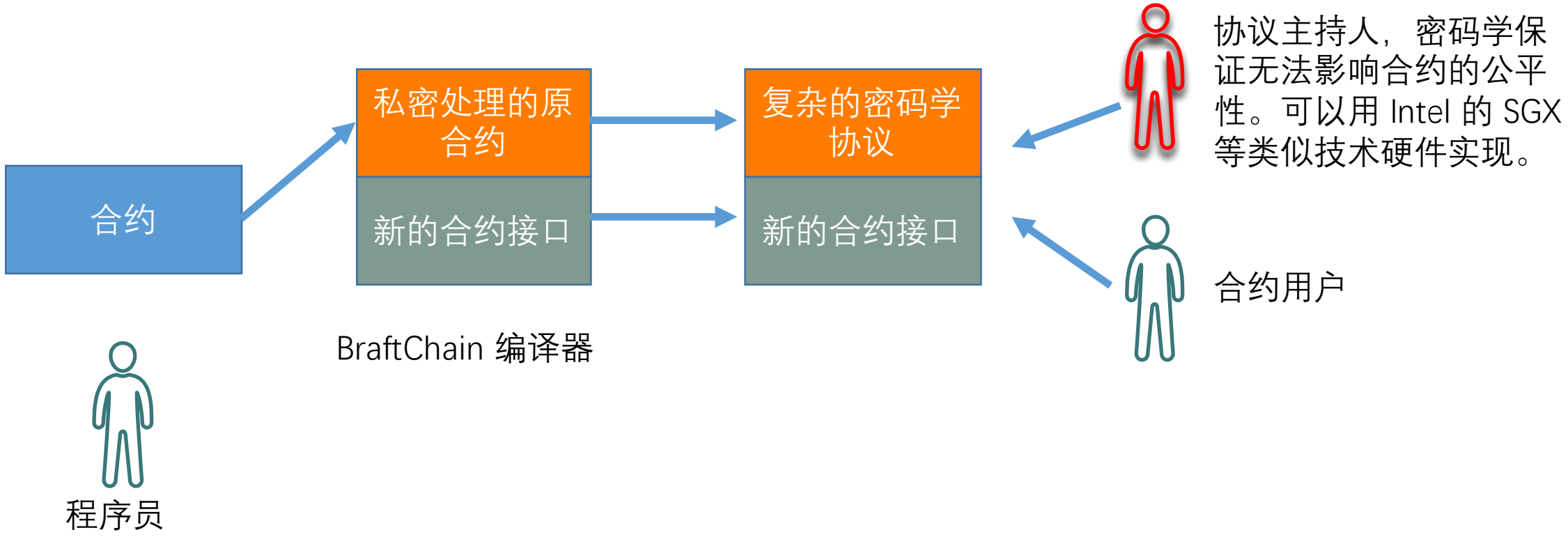
合约的安全与私密性

- 合约的参与方可能随时退出，参与方发送给合约的钱需要能找回
- 对智能合约的调用是公开的，合约的参与方可以通过他人的行动谋利
- 合约的执行可能意外中止，如嵌套层数太深，代码中的 Bug
- 矿工是否能有选择性得加入交易以及不广播对自己不利的区块
  - 联盟链下不存在这个问题

合约的安全与私密性

- 用合约的形式实现 ZeroCash，隐藏交易的发送/接收方和数额

- BraftChain将提供开发工具帮助用户开发智能合约
  - 用户的智能合约将被工具加上BraftChain 提供的加密协议
  - 仍在初步开发过程中


合约
私密处理的原合约
新的合约接口
复杂的密码学协议
新的合约接口
协议主持人，密码学保证无法影响合约的公平性。可以用 Intel 的 SGX 等类似技术硬件实现。
合约用户
BraftChain 编译器
程序员

总结

Blockchain as a Service

- BraftChain的共识算法和具体的区块格式无关，可以根据业务需求设计区块链上的数据存储方式
- BraftChain可快速搭建和删除，适应灵活的业务
- 根据业务需求定制智能合约的虚拟机
- 协助用户设计领域专用语言开发所需的智能合约，提供完善的开发流程

感谢，欢迎提问！