BCCon 全球区块链生态技术大会
Global Blockchain Eco-Technology Conference

百度自研超级链的安全经验

荆博

百度区块链业务部资深研发工程师

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

- 密钥生成与保护
- 签名算法
- 网络层
- 通信层
- 共识层/智能合约
- 应用层
- 隐私层

区块链安全风险综述

技术

密钥生成与保护
签名算法和散列算法的安全防护
网络稳定性和通信安全性
共识机制和智能合约的升级修复

社会

面向B端商户的服务稳定性
面向C端的高性能场景下的安全防护

行业

缺乏标准协议
开发者很难从其他人的错误中受益

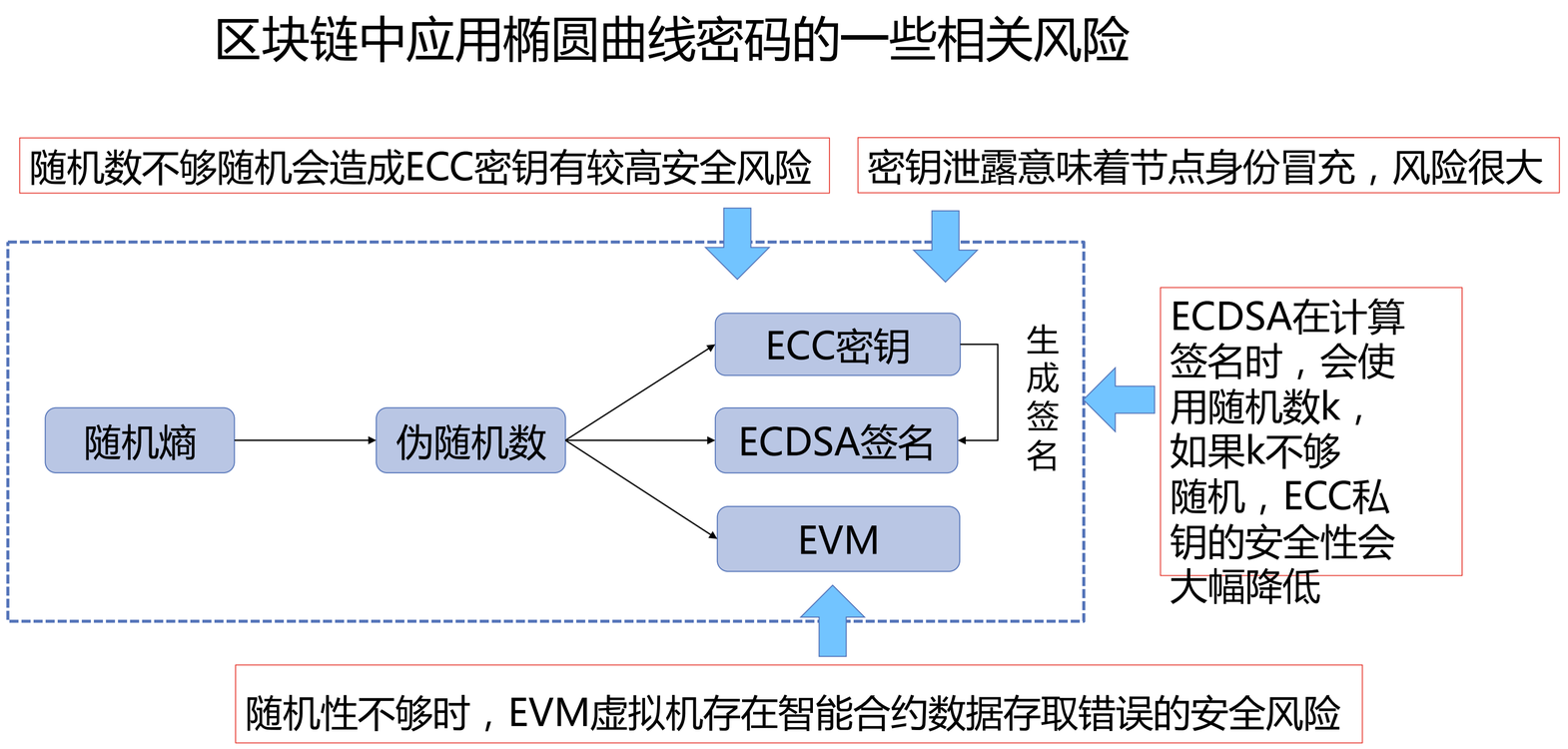
政府

防范公众隐私泄露
防止有害信息上链

密钥生成与保护 – 风险

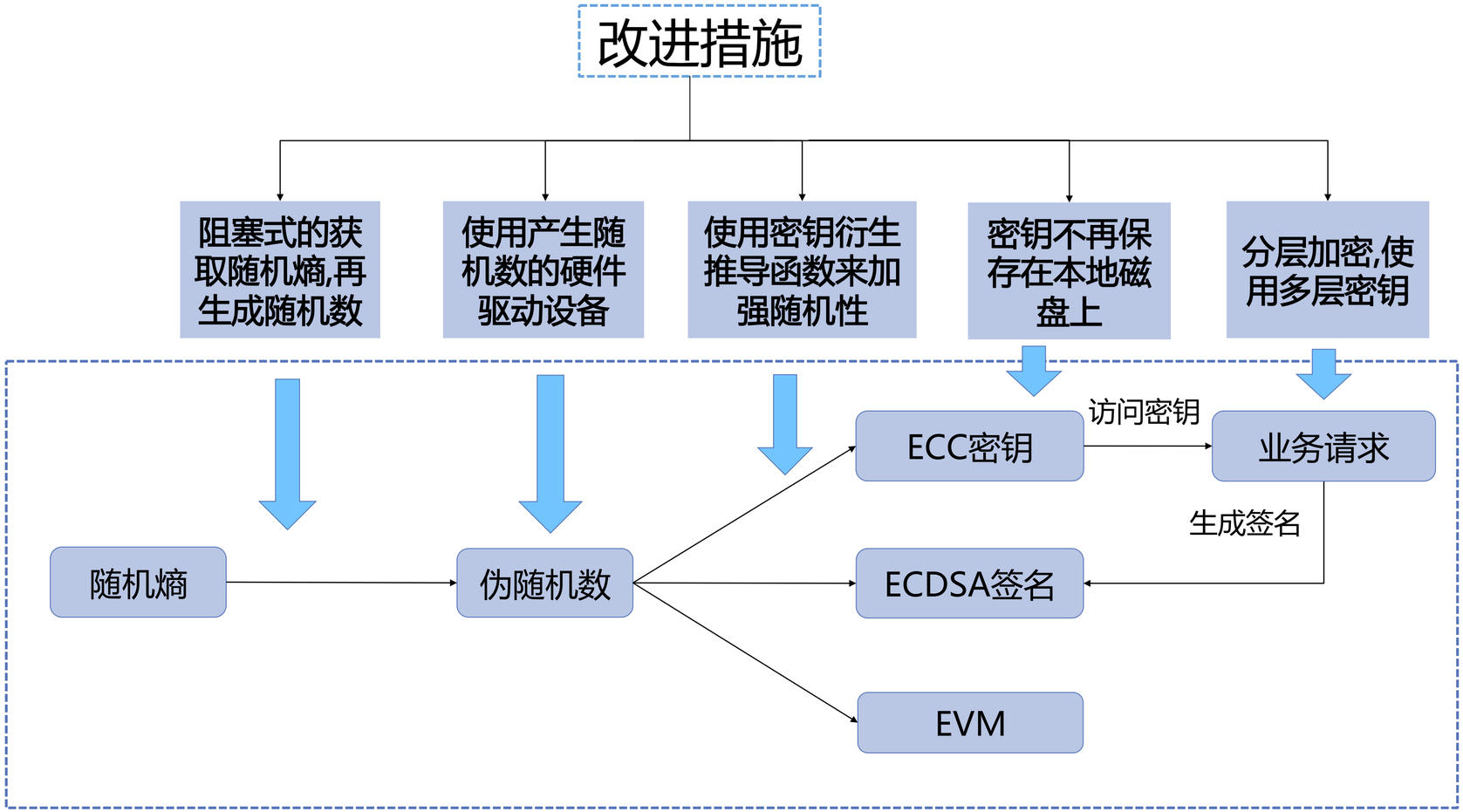
➢linux系统中伪随机数来源于系统维护的随机熵，而随机熵来源于系统收集的环境噪声。弱随机数对ECDSA等方案的安全性有极大的影响。

➢保存的密钥被其它人读取



密钥生成与保护 – 方案

- 加锁，同步等待生成随机数，参考EVM
- 使用专门的设备来进行生成签名和验签。无法直接读取出密钥。
- 使用密钥衍生推导函数来加强随机性，如：更长的随机块、更复杂的散列函数，加大散列轮次



签名算法的安全保护

可变类型密钥生成和签名算法

标志符	FIPS ECC P384
公钥值	P384 公钥内容

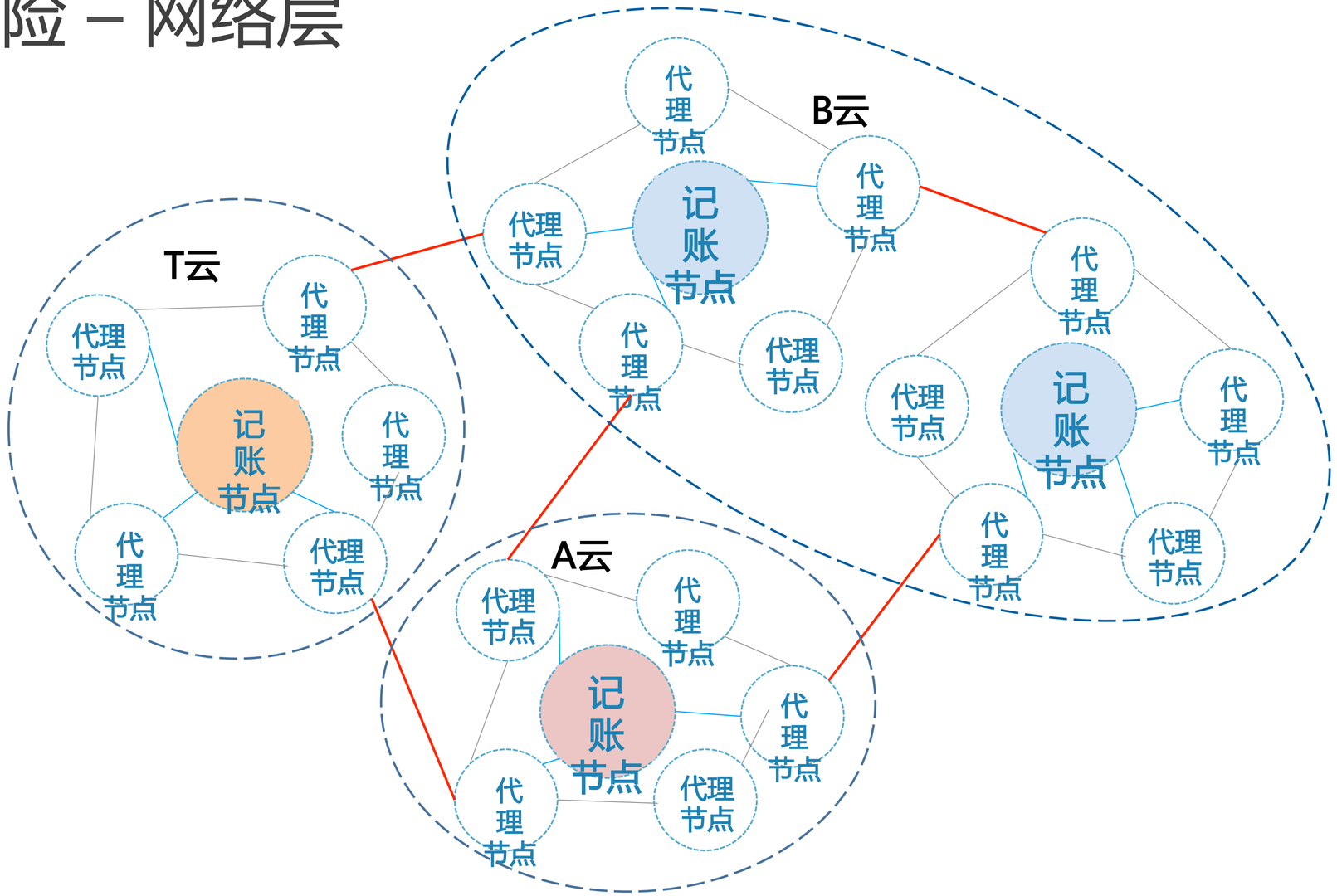
标志符	BTC ECC secp256k1
公钥值	Secp256k1 公钥内容

标志符	FIPS ECC P521
公钥值	P521 公钥内容

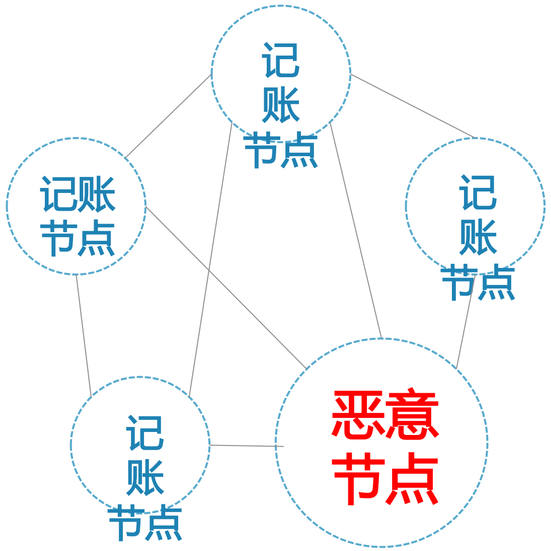
资产安全	当出现某种签名算法的安全漏洞时，用户可以申请使用新密钥生成算法获得新的地址，把资产转移到新的地址去，避免丢失资产。资产转移完毕后，再使用新的签名算法来使用资产。
易于升级	密码学领域如果有新的进展，可以很快的升级到新的算法。此外，万一某一种签名算法或是某一条椭圆曲线出现漏洞，可以迅速迁移到新的签名算法或者新的一条椭圆曲线来降低损失。
高兼容性	可以使用多种主流区块链网络的签名算法，来提高开源软件的兼容度。进一步降低资产跨链方案的技术复杂度。
无需分叉	签名算法的升级不再需要硬分叉。

区块链安全风险 – 网络层

- 在众多代理节点之后隐藏真正的记账节点。大幅提高无边界网络攻击的成本。
- 多云架构，单个云服务商的服务宕机后，只会瘫痪一小部分的节点，区块链网络服务仍然可用。



区块链安全风险 - 通信层

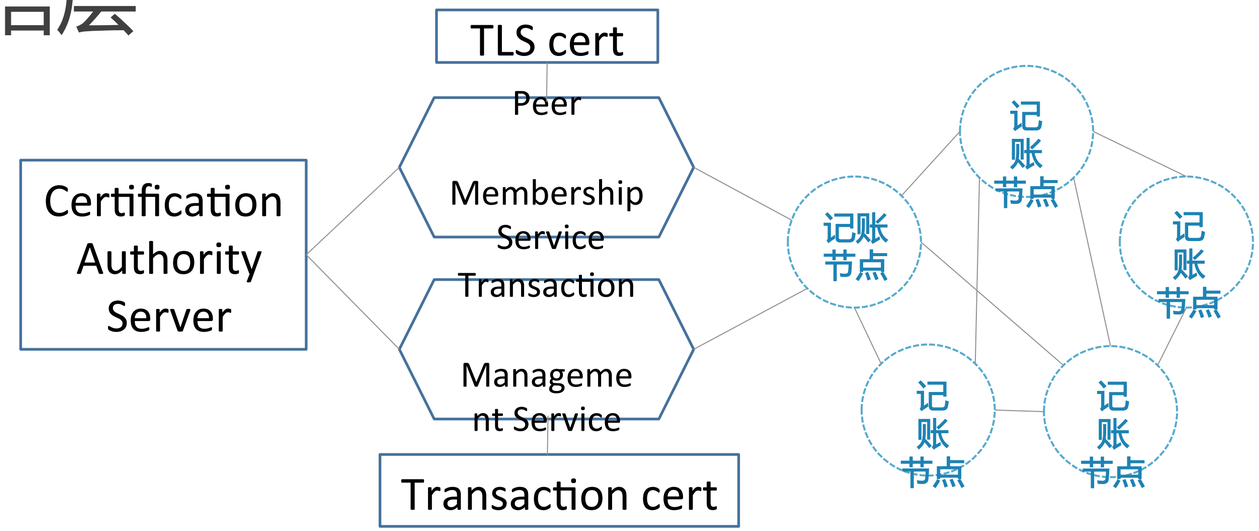


数据泄露和节点身份泄露

I. 对于联盟链，流量不加密会导致恶意节点可以侦听到全网交易信息及发起源。

II. 对于公链，可以侦听到发起交易的节点信息。容易暴露身份。

联盟链



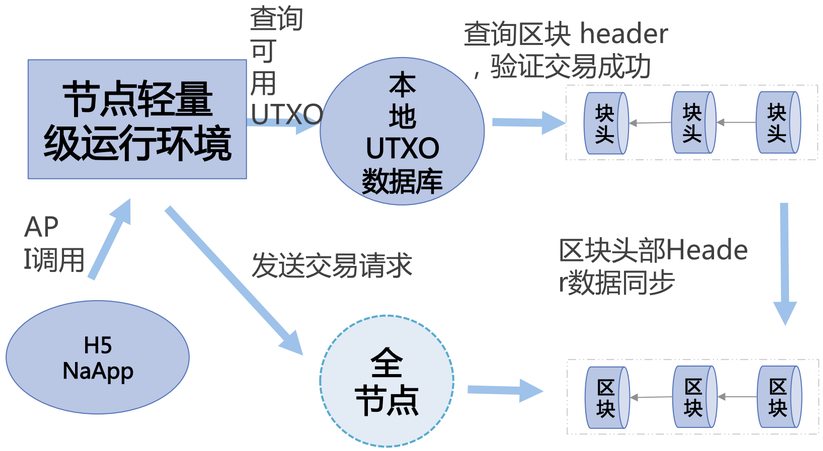
公链

P2P链路通信加密技术

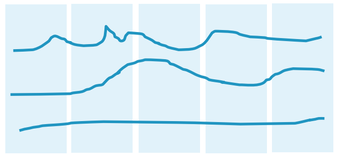
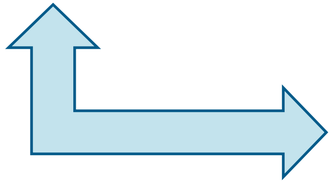
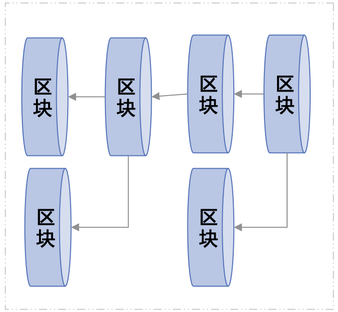
类似于以太坊的RLPx的链路通信加密机制

- Node Discovery
- Encrypted Transport
- Framing
- Flow Control

节点轻量级技术



区块链安全风险 - 共识层

背景	风险	解决方案
挖矿算法asic化	 PoW算力大幅波动，导致出块不稳定、服务不稳定	1. 使用抗asic的散列算法 2. 不定期的升级散列算法
共识机制/哈希算法/加密算法存在风险或发现漏洞	 数字资产的安全问题无法迅速解决，修复问题需要硬分叉，代价巨大	通过提案机制来升级区块链网络使用的共识机制和核心配置
DPOS的密钥泄漏导致的恶意分叉	 区块数据经常性的分叉，基链数据频繁回滚，严重降低网络性能	1. 对于联盟链，升级P2P节点维护算法。使用CA服务或投票来移除恶意节点。 2. 对于公链，引入检查点机制，非完全最长链可逆

通过对智能合约/共识的升级来修复安全漏洞

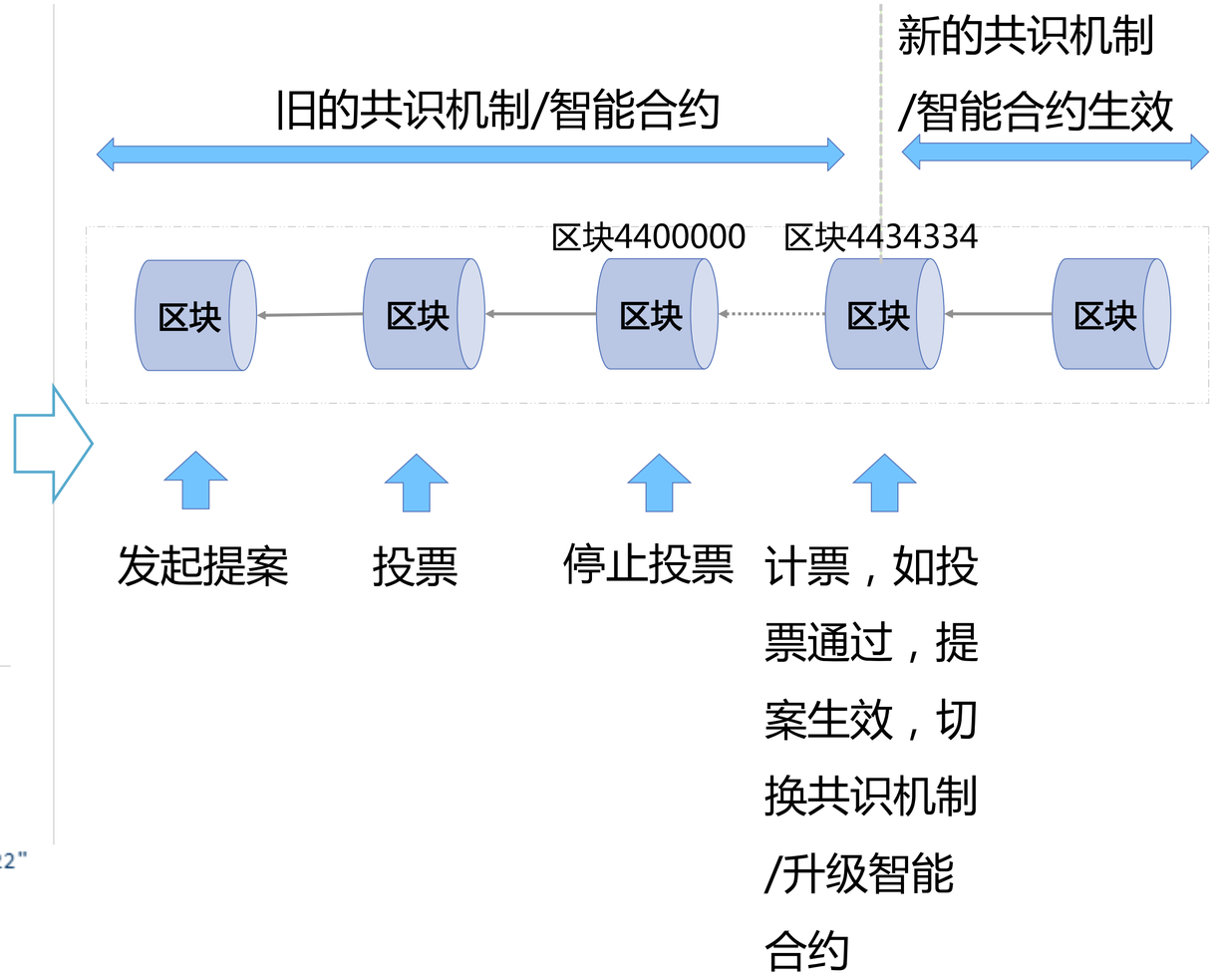
百度自己开发的公链架构支持可升级的共识机制和智能合约。

发起提案来升级

```
{
  "module": "kernel",
  "method": "propose",
  "args" : {
    "min_vote_percent": 68,  //获得通过的最少票百分比（分母是整个链当前的总资产）
    "stop_vote_height": 4400000, // 投票截止高度
  },
  "trigger": { //通用定时器机制，用于设置延时触发执行的合约
       "height": 4434334, //触发执行的高度，需要大于stop_vote_height
       "module": "consensus",
       "method": "update_consensus",  // 举例：比如触发共识机制的更新
       "args" : {
          "name": "dpos"
       }
   }
}
```

进行投票来支持升级

```
{
    "moduel":"kernel",
    "method": "vote",
    "args" : {          //提案的txid
        "txid":"8bec1a342f5bafb389193610b5ea7e4a58b02d09429902823ac696d4b6e5c822"
    }
}
```



区块链安全风险 - 应用层

风险	解决方案
有害信息上链	1.上链前执行黄反、上链后浏览器屏蔽 2.对于联盟链，通过交易内容的访问权限控制，屏蔽有害信息的访问
输入错误的钱包账户地址	加入校验位，支持地址校验算法
用户私钥丢失遗忘	1. 引入助记词，可以恢复钱包账户 2. 密钥分存，门限签名技术

区块链安全风险 - 隐私层

风险

虚拟身份对应到现实生活中：

1.侦听网络节点的发起交易时的信息

2.追踪交易历史

方案

1.分层确定性钱包

2.SPV轻量级支付技术

3.动态更换收款地址

4.零知识证明

主办方 Geekbang 极客邦科技 InfoQ

THANKS