



区块链发展新阶段：应用驱动技术

申屠青春 银链科技CEO



目录

01

银链科技



02

区块链技术发展



03

区块链应用



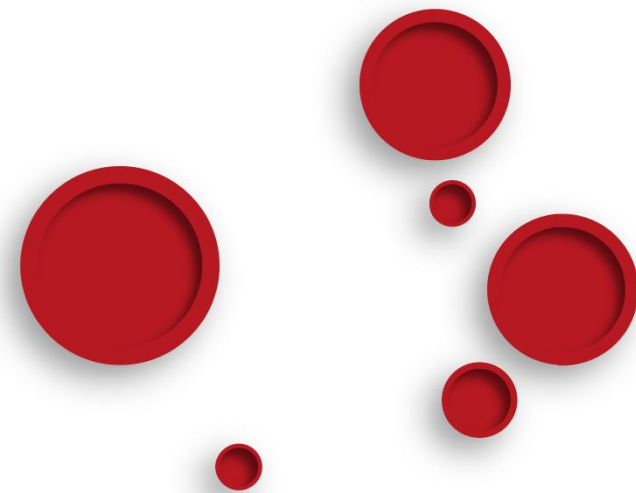
04

应用驱动技术





一、银链科技





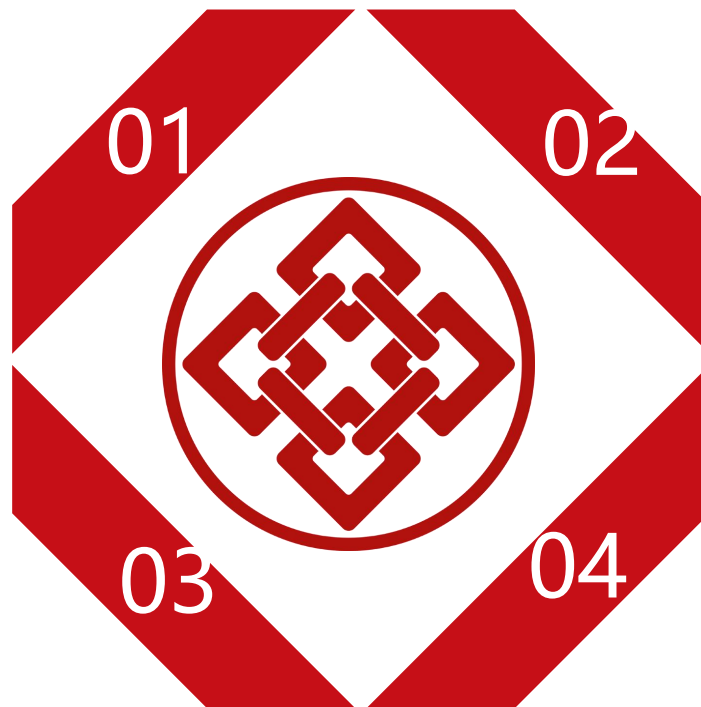
银链科技

金链盟主席团成员

金链盟现已有67家金融机构及金融科技企业。大部分为上市公司。获取客户成本较低。

黑客马拉松二等奖

2017年3月参加黑客马拉松比赛，其项目合同链获得该比赛的二等奖；并与IBM达成合作意向。



南京政府资助单位

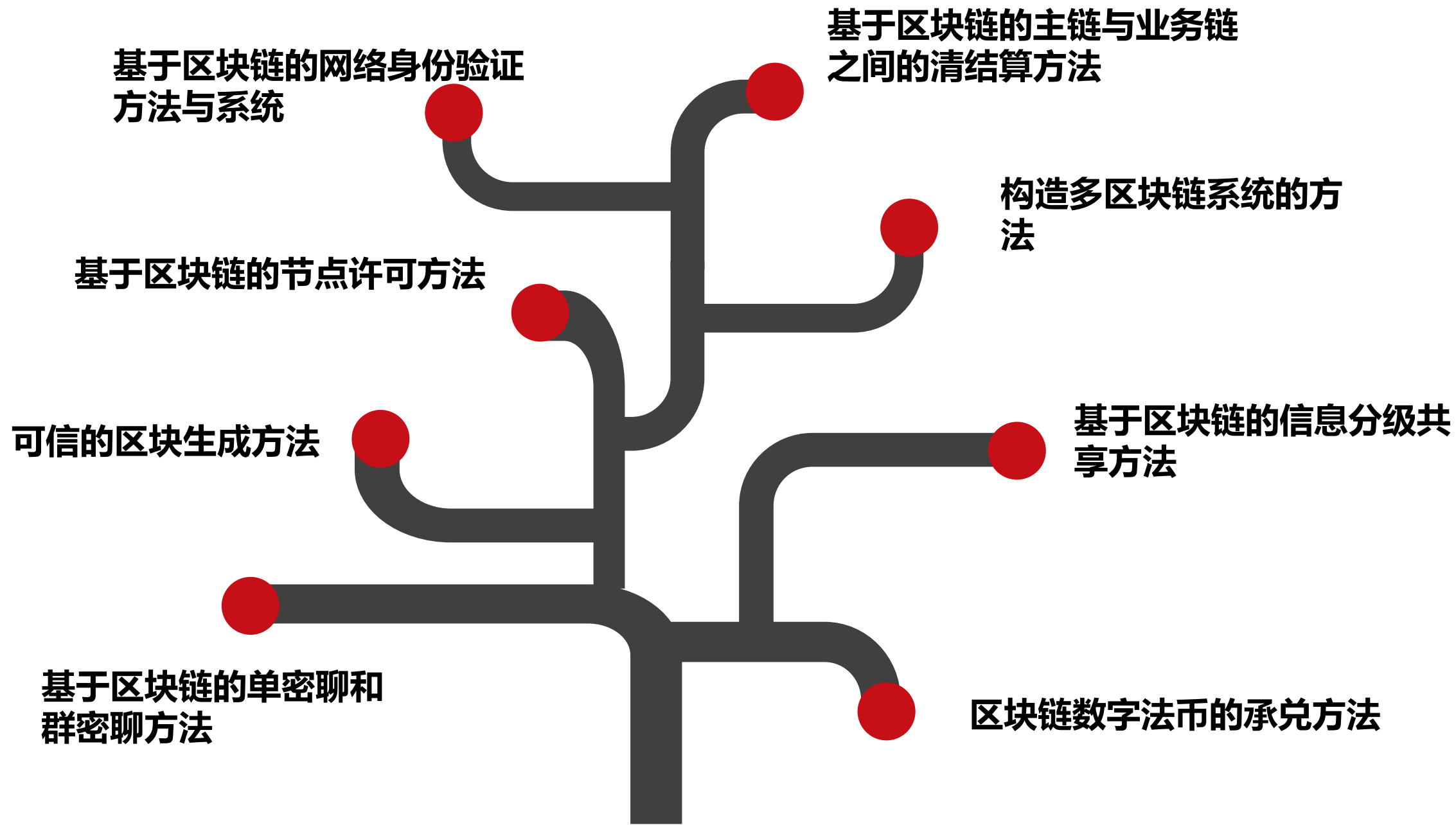
2016年12月份，银链科技获得南京市政府150万项目资助；

天使融资

2016年5月，银链科技获得上市公司300W人民币投资。



八大专利





银链产品线

链圈

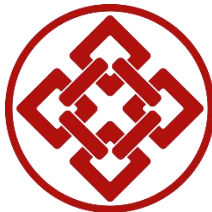
银链中间件
BMWare

供应链金融
SupplyChain

币圈

选举链
ElectionChain

暗网空间
DarknetSpace



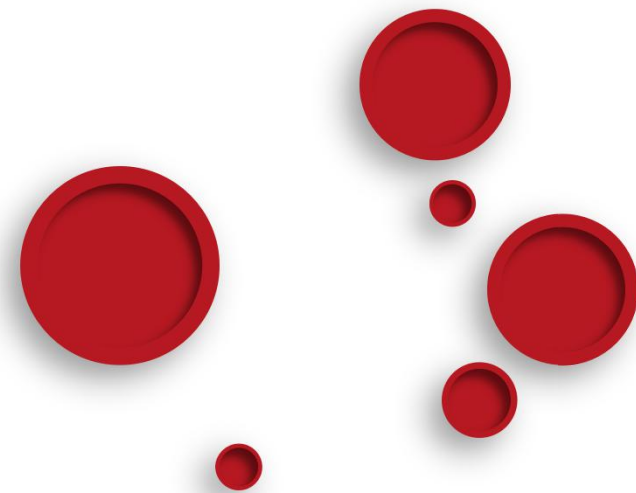
商业模式

目标客户：
想实施“区块链+”的金融机构和
企事业单位；





二、区块链技术发展





区块链核心价值

去中心化：

维护简单，自动更新
同步的数据网络，



公开数据库

公开透明、不可更改、
永不丢失，可纪录证
明、公开纪录.



**信任机器
多方协作
提高效率
降低成本**

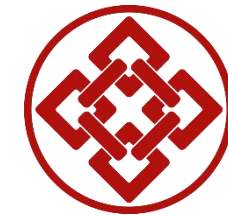
共识机制

无信任环境 可信地
处理数据，交易，消
除第三方





比特币 (Bitcoin)



01

比特币的特点：

- 去中心化、专属所有权、
- 交易的便捷性、全世界流通性、
- 低交易费率、跨平台

02

比特币优点

- 完全的去中心化发行
- 健壮性
- 匿名、免税、免监管
- 无国界、跨境

03

比特币缺点：

- 价格波动极大
- 交易确认时间较长
- 交易平台的脆弱性



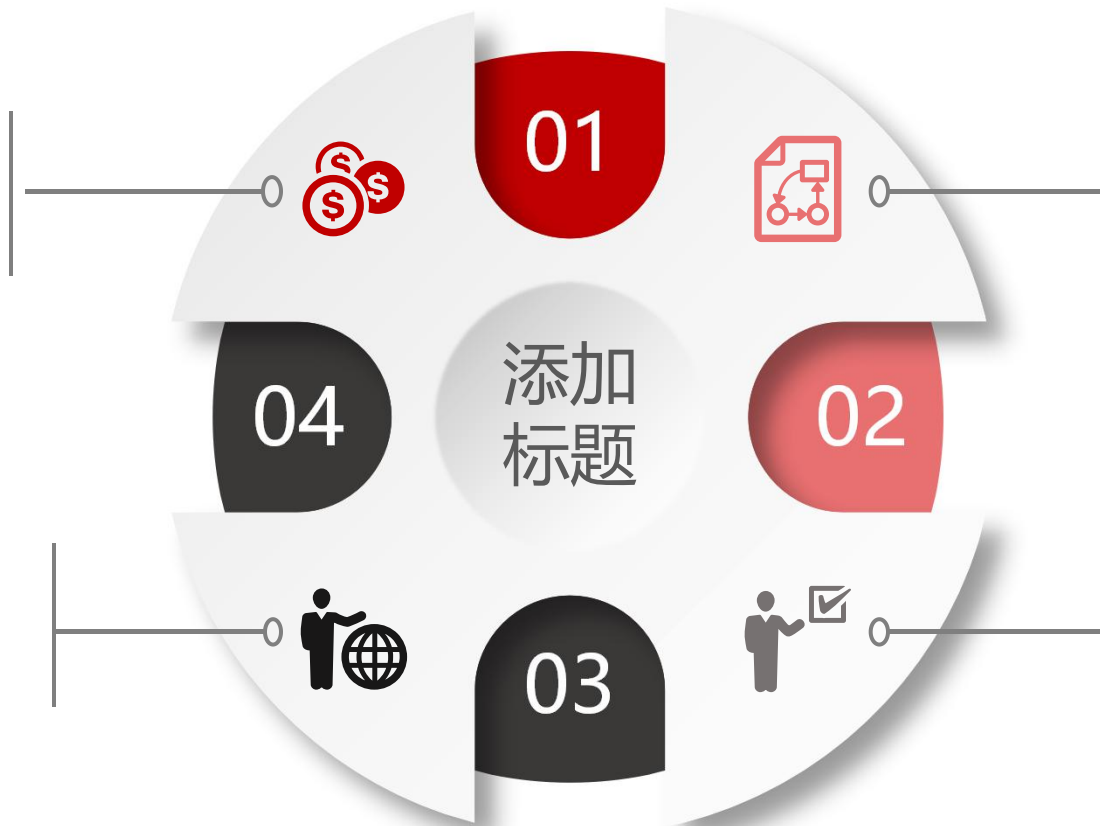
以太坊（ETH）

可编程的区块链

以太坊是一个全新开放的区块链平台，它允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用。

去中心化应用平台的协议

核心是以太坊虚拟机（“EVM”），可以执行任意复杂算法的编码。在计算机科学术语中，以太坊是“图灵完备的”。开发者能够使用类似于现有JavaScript和Python等语言为模型的其他友好的编程语言，创建出在以太坊模拟机上运行的应用。



以太坊的区块时间更短

与比特币区块的10分钟相比，以太坊区块间时间大约在14秒左右。

以太坊虚拟机上可以运行智能合约

智能合约代码在一种被称为以太坊虚拟机的东西上运行，以太坊虚拟机分布在网络中所有参与者的计算机上运行着。现在可以简单的把智能合约类比为传统服务器端的代码。



Fabric

Fabric是一种开源区块链实现，部署环境可以是私有服务器，也可以直接部署在公有云上，部署方式可传统可docker化，共识算法插件化，支持用Go和JavaScript开发智能合约，**尤以企业级的安全机制和CA机制为特色**。Fabric之于区块链，很可能正如Hadoop之于大数据。

核心逻辑



Membership

Membership Services这项服务用来管理节点身份、隐私、保密性、可审计性。



Blockchain

Blockchain services使用建立在HTTP/2上的P2P协议来管理分布式账本，提供最有效的哈希算法来维护区块链世界状态的副本。采取可插拔的方式来根据具体需求来设置共识协议，IBM首选PBFT算法。



Chaincode

Chaincode services 会提供一种安全且轻量级的沙盒运行模式，来在VP节点上执行chaincode逻辑，类似以太坊的EVM虚拟机及其他上面运行的智能合约。

Fabric 1.0账本设计



设计目标

①提升性能 ②提升可拓展性 ③提供更丰富的查询功能 ④更多模块的可插拔



账本组成

最大的不同是增加了对基于文件系统的区块链账本的支持，可以更好地支持不可篡改的特性。



完整交易步骤

鉴于Consenter部分还没完全完工，从目前的交易执行过程来看，对节点角色的功能拆分，解决Fabric0.6的拓展性问题。



交易流程

①提交提案 ②执行chaincode并在集群节点中模拟提案 ③返回提案结果 ④提交交易 ⑤Order服务创建交易的批处理 ⑥从Order服务接收生成的区块 ⑦验证每个交易并写进账本



传递的消息结构

①Endorsing Peer (仿真)
②Committing Peer (验证/提交)



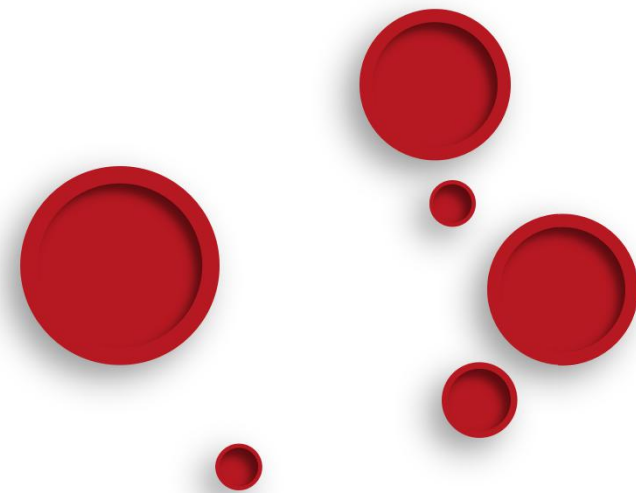
智能合约数据

依托可插拔特性引入的CouchDB数据库，提供了基于JSON数据格式的多种数据查询能力，丰富了合约代码可以实现的功能。





三、区块链应用





区块链应用挑战

应用落地周期长

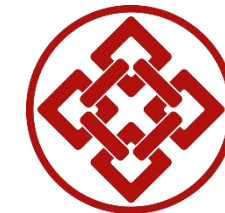
- 先掌握区块链技术和理念
- 再选取应用场景
- 在选用一家区块链平台研究
- 最后进行区块链应用开发

从业人才成本高

- 从业人才层次、技术积累和理念改变提出了较高的要求
- 金融和区块链的交叉人才较少，培养成本较高

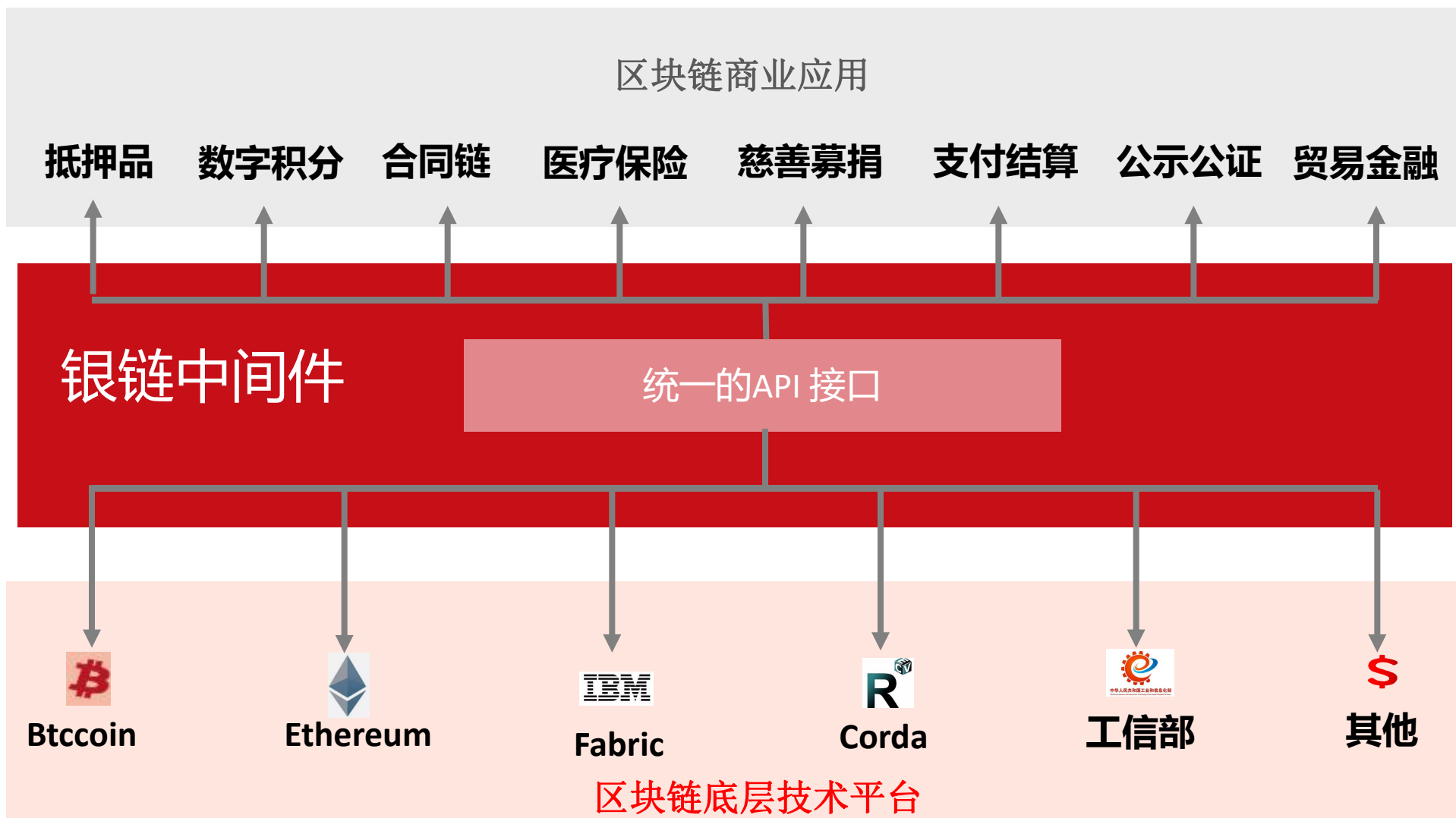
区块链选用难

- 发展前景不确定
- 是否合规
- 版权、运维等



银链科技-中间件

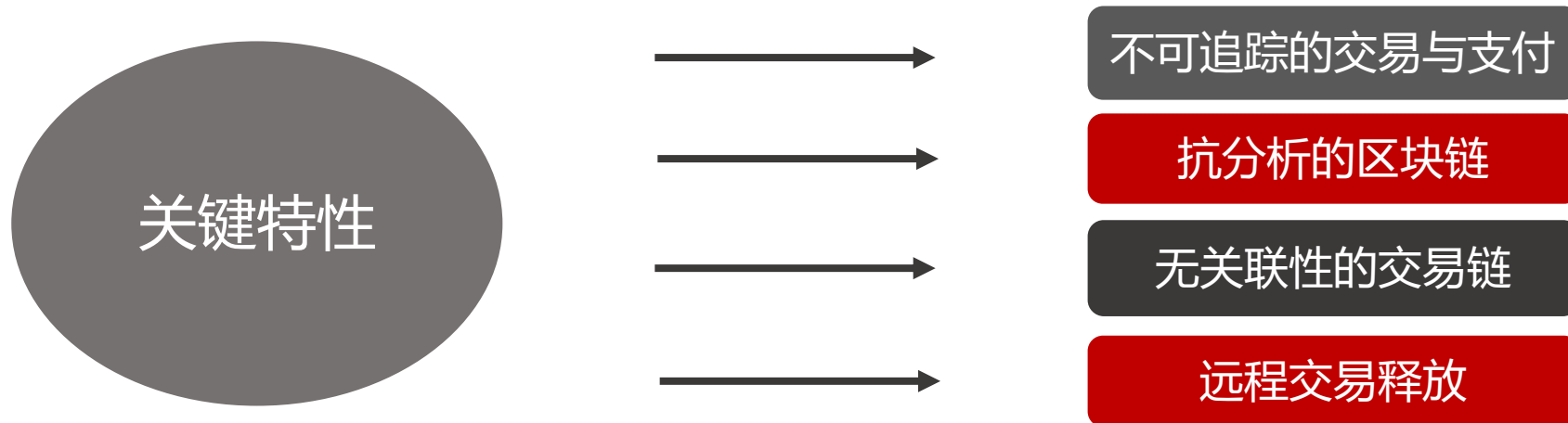
网络架构





暗网空间与暗网币

暗网空间是一个以强匿名为主题的二代币应用系统，**暗网币(DarkNetCoin)**是其中的基准货币。



DNC二代版本特点：

1、存币 理财

2、私密通信，包括个人以及群组

3、地址簿

4、钱包直接挖矿

5、钱包嵌入区块浏览器

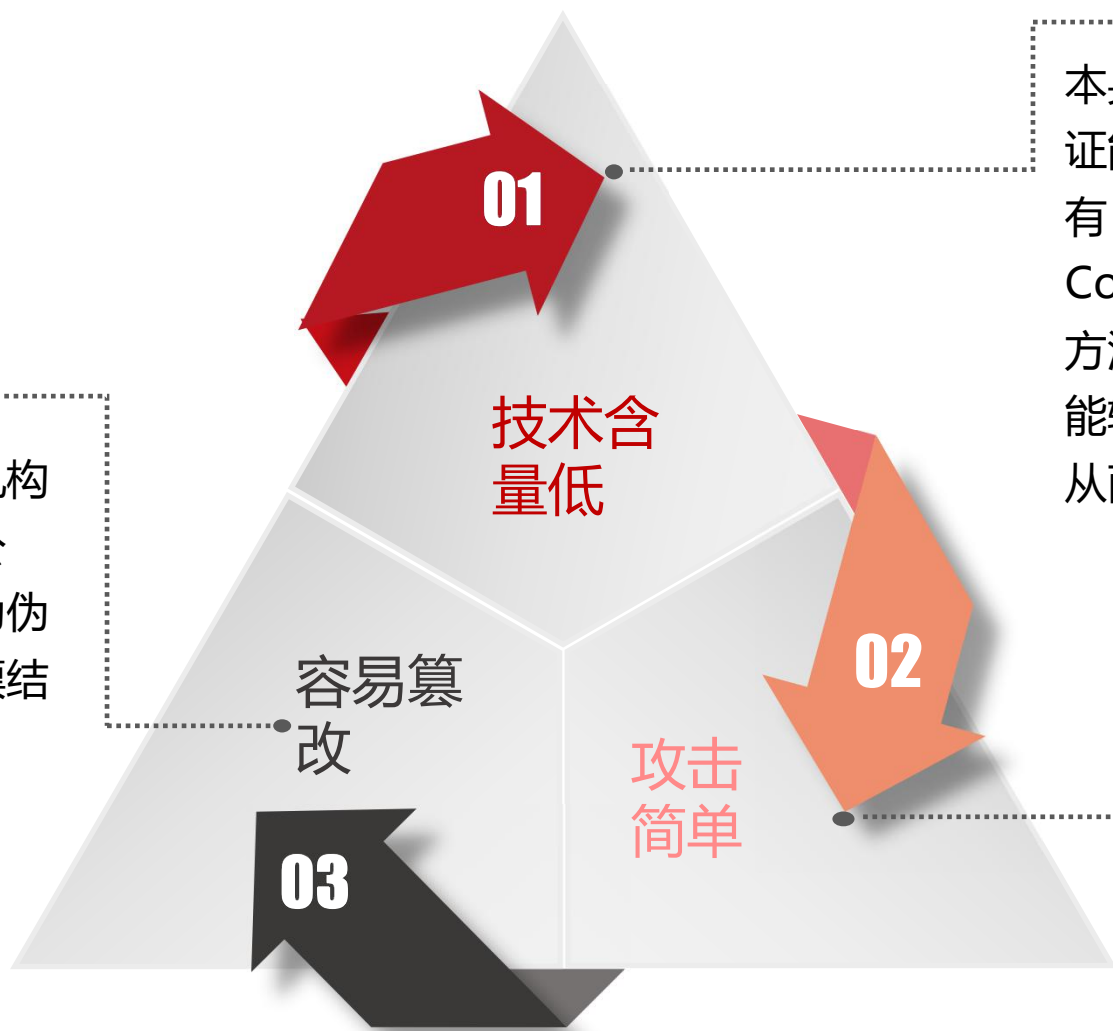
6、查看区块还未打包的交易

7、查看连接节点



网络投票问题

投票系统本身由一家中心化的机构管理、运营，其数据很难做到公开、透明化，甚至可能存在人为伪造的数据，这样将无法保证投票结果可信度；



本身的技术含量并不高，对于连续投票的验证能力薄弱，比如现在普通使用验证技术有：注册用户验证、Session 验证、Cookies验证、IP地址验证。对于这些验证方法，只要懂点计算机软件知识的人士，就能轻而易举的破解，就可以做到连续刷票，从而影响到投票结果；

数据一般存放在数据库中，只要黑客攻破数据库服务器，篡改投票结果，就能达到某些人的目的，因此失去了公平、公正性；

选举链应用场景

娱乐化竞猜

一般值得竞猜的主题应该是大众化的、重要的投票结果，如总统选举、脱欧等，人们可以进行竞猜哪个候选人或决策会最终胜出。

对接现有彩票系统

选举链不会自行发行彩票，其中的彩票场景将与国内和国外的彩票机构合作进行。

选举，决策，民意调查

全球所有投票和选举都可以在选举链上进行，以及就某个主题向公民征求意见，一般以区块链问卷调查的方式进行，如总统支持率调查、对某项事情的看法等等。

捐款

人们可以在选举链上对候选人进行捐款，区块链可记录下选民或非选民对候选人的捐款，使得款项更透明。

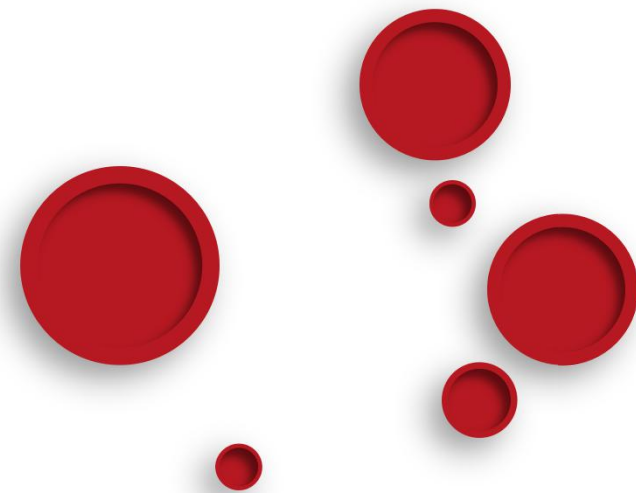
娱乐化投票

引入竞选演说、直播和打赏、竞选游戏和其他娱乐性应用，使得选举链更有趣味性，而非政治化的项目。





四、应用驱动技术



应用需求下的技术创新

实名投票

01



- 1 : 身份认证技术
- 2 : 引入多个权威身份认证机构
- 3 : 投票结果可验证

参与方激励

02



- 1 : 在DPOS加入挖矿激励，成为EDOPS
- 2 : 身份认证方激励，来核实真实身份，得到奖励
- 3 : 投票组织方奖励

性能要求

03



- 1 : 交易吞吐量均值6KTPS，峰值10WTPS
- 2 : 使用bitshares石墨烯开发引擎
- 3 : 闪投协议，参照闪电网络的思想，进行快速投票
- 4 : 多链体系由投票子链、身份子链和支付子链构成，建立各国或各机构的选举侧链；

应用需求下的技术创新

隐私保护

04



- 1 : 真实身份匿名投票
- 2 : 虚拟身份虚拟投票

智能合约

05



- 1 : 去中心化租借市场
- 2 : 一定数量 (可自动调节) ELC绑定1个选票 , 锁定和消耗更多ELC , 流动ELC更有价值 ;

智能合约

06



- 1 : 在一些复杂低吞吐量要求的电子投票场景中
- 2 : 常规的标准化的投票使用Bitshares的操作模式



感谢大家的支持