



区块链技术原理与FISCO BCOS平台介绍

李昊轩asherli
2018年10月

目录

1. 区块链相关知识介绍
2. FISCO BCOS 案例分析
3. FISCO BCOS 底层平台开发知识介绍

01

区块链相关知识介绍

目录

1. 区块链相关知识介绍
 - 1.1 区块链行业发展现状
 - 1.2 区块链技术架构总览
2. FISCO BCOS 案例分析
3. FISCO BCOS 底层平台开发知识介绍

011

区块链行业发展现状

◆ 区块链技术的发展历程概要



◆ 背景介绍：Bitcoin 开源社区

比特币是一个创新的支付网络，一种新的货币。



即时对等
交易



全球
支付



零或极低的
手续费

Search: bitcoin

We've found 7,775 repository results

Sort: Best match ▾

Repositories	Code	Issues	Users
7,775	3,307,156	26,360	572

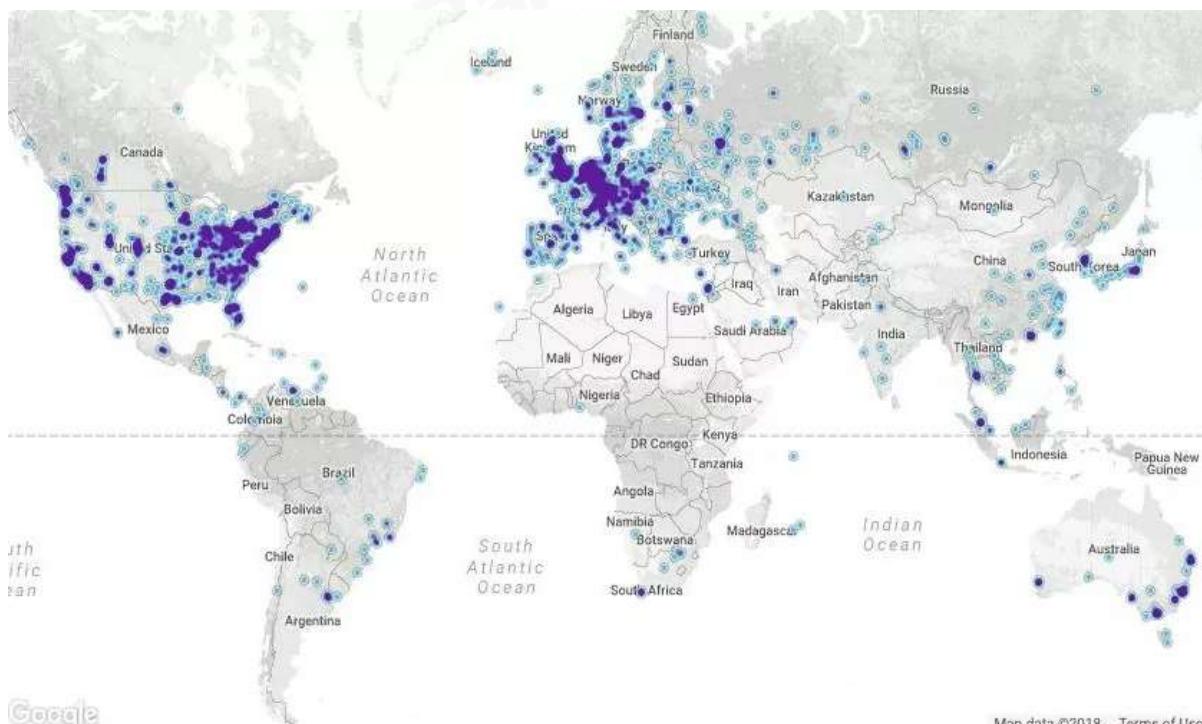
bitcoin/bitcoin
Bitcoin Core integration/staging tree
Updated 2 hours ago

bitcoinbook/bitcoinbook
Mastering Bitcoin - Unlocking digital currencies
Updated 6 days ago

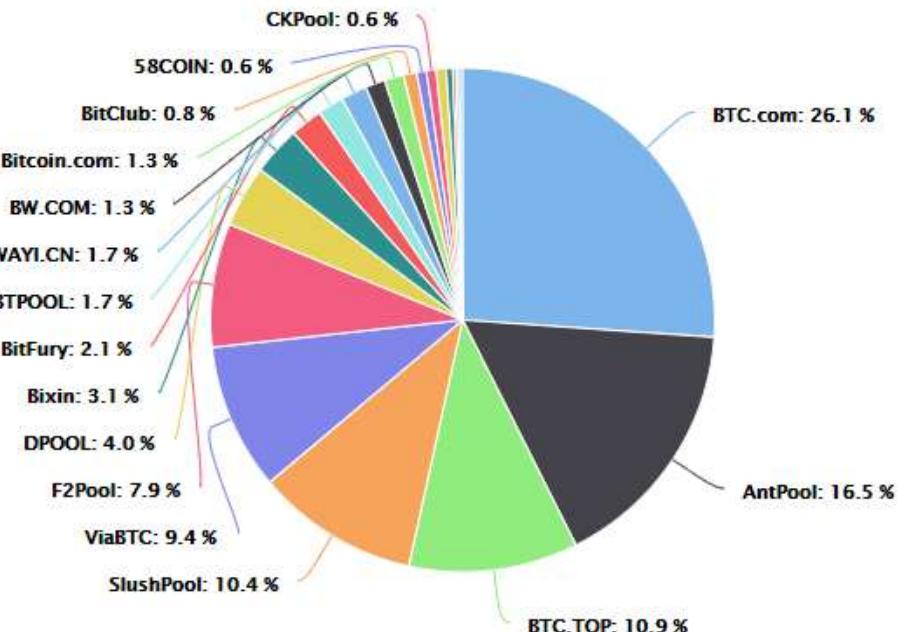
bitcoinj/bitcoinj
A library for working with Bitcoin
Updated 2 days ago

比特币全球网络和算力一览

全节点最多的几个国家包括了美国、德国、中国、法国、荷兰、加拿大、英国以及俄罗斯。这些节点同时还在那些网络服务以及经济发展很差的国家运行着，这些国家包括了委内瑞拉、阿尔及利亚、墨西哥、那非、纳米比亚、巴基斯坦以及尼日利亚。



Map data ©2018 Terms of Use



◆ 比特币的支付?



BUSINESS INSIDER UK

TECH

May 22, 2010, a developer bought two pizzas using 10,000 units of a then-little-known digital currency called bitcoin.

Today, 10,000 bitcoins are worth more than \$20 million (£15.4 million).

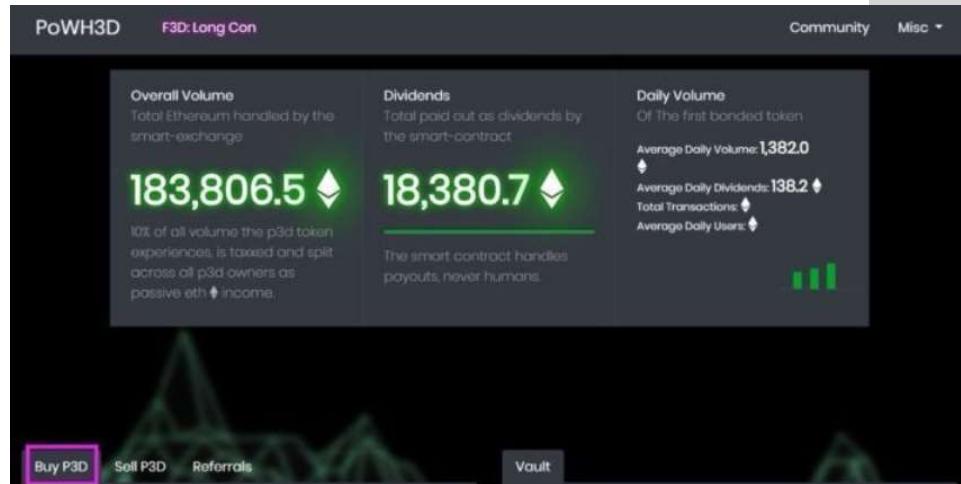
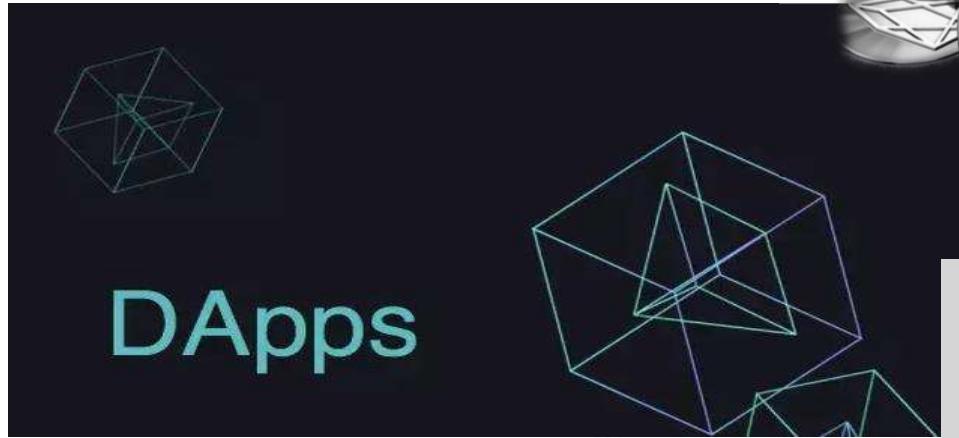
Bitcoin is going nuclear. Its price is tearing upward, with each bitcoin worth \$2,128 (£1,638) — a little shy of its all-time-high of \$2,185 (£1,682) reached earlier Monday morning.



Laszlo Hanyecz bought these pizzas for 10,000 bitcoins on May 22,

◆ 背景介绍:以太坊





Smart Contracts



Self-enforceable
Trust-less
Faster
Cheaper

◆ 百花齐放的区块链平台方案



大规模高速共识机制:DPOS/Algorand/VRF和BFT混合 ...

DAG, 多链, 跨链, 闪电网络, 分布式存储...

高速计算(通用虚拟机), 链外计算, 可信验证...

◆ 联盟链现状



◆ 金融区块链合作联盟（深圳） - 简称：金链盟

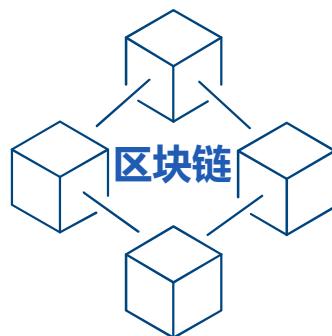
- 2016年5月31日正式成立；
- 深圳市金融科技协会、微众银行、深证通等二十余家金融机构和科技企业共同发起；
- 非营利组织，下设成员大会、主席团、秘书处、技术委员会、标准技术工作委员会、顾问委员会；
- 成员覆盖24个城市，涵盖银行、基金、证券、保险、地方股权交易所、科技公司等六大类行业的92家机构；



银行业金融机构
微众银行、广发银行、华夏银行、南京银行、江苏银行、包商银行、长沙银行、洛阳银行、徽商银行、华瑞银行、恒丰银行、上饶银行、山东城商行联盟、百信银行、天津金城银行、营口银行等；
保险业金融机构
太平洋财产保险、泰康人寿、太平共享金融等；
证券与基金业金融机构
光大证券、安信证券、国信证券、招商证券、国泰君安证券、广发证券、博时基金、南方基金、招商基金等；
其他知名机构
深圳市金融科技协会、前海通、深证通、腾讯、华为、京东金融、万达网络、招银网络、恒生电子、中证信用、中证信用云等；

◆ 联盟链的路径选择

- 区块链作为一种整体技术解决方案，融汇吸收了分布式架构、分布式存储、点对点网络协议、加密算法、共识算法、智能合约等多类技术；
- 联盟链作为支持分布式商业的基础组件，更能满足分布式商业中的多方对等合作与合规有序发展要求



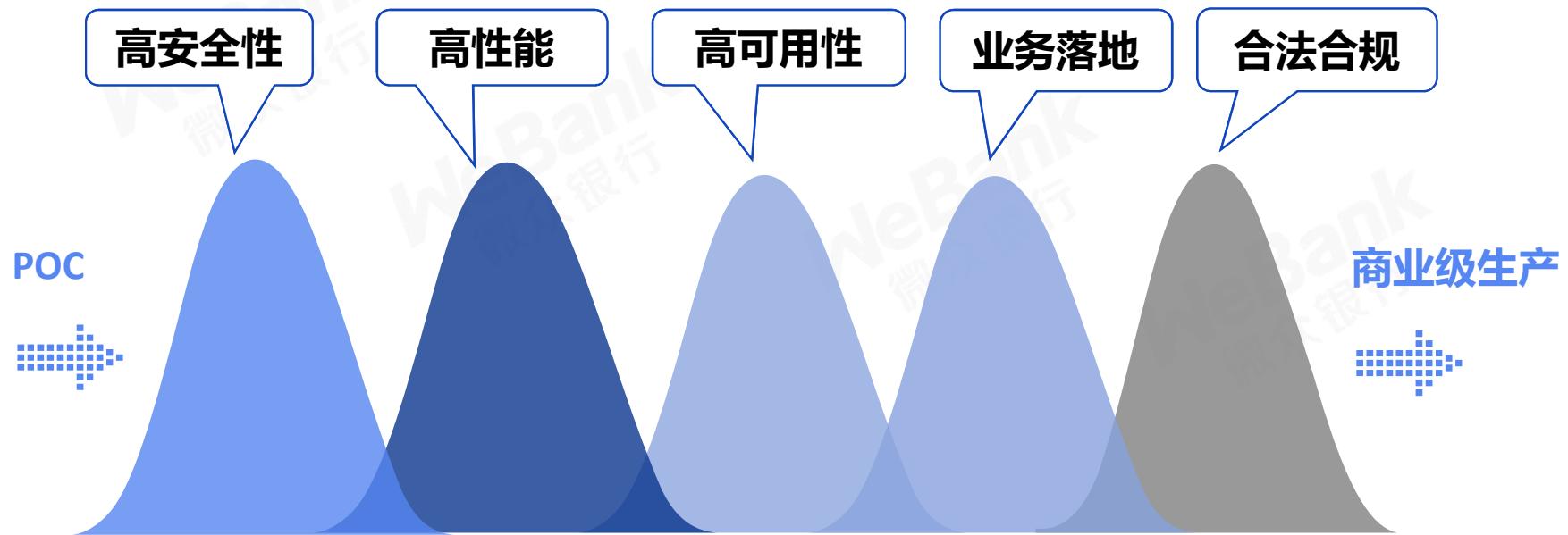
- 可信数据与分布式账本
- 共识机制与技术信任
- 加解密与隐私保护算法
- 分布式对等网络
- 智能合约



- 准入机制
 - 监管节点
 - 身份认证
 - 去代币
- 虚拟代币
 - 挖矿激励
 - 匿名交易

我们的选择：联盟链，兼顾金融创新与金融稳定

◆ 联盟链的挑战：五座大山



FISCO-BCOS概要

由金链盟开源工作组进行规划和开发，历时多年打造，全面开源

联盟链



聚焦金融，商业，工业，文化...

自主可控



自主知识产权
包含大量前沿技术
合法合规

生产级



安全，高性能，高可用，
功能完备，运维友好

全面开源



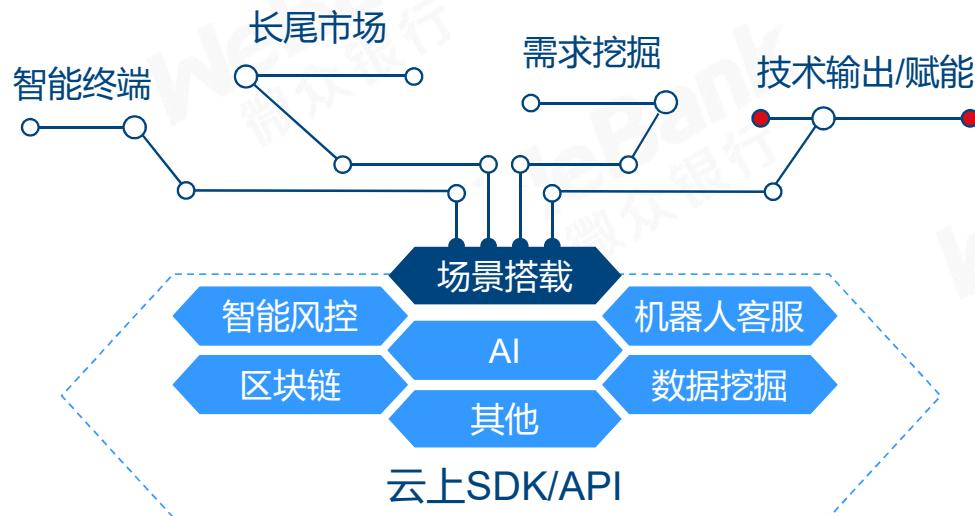
代码开源，社区活跃，
立体化支持



WeBank

Copyright 微众银行©版权所有，不得侵犯

金融科技创新战略总览



价值体现: 三升两降 ($\frac{\text{效率} \times \text{体验} \times \text{规模}}{\text{成本} \times \text{风险}}$)

012

区块链技术架构总览

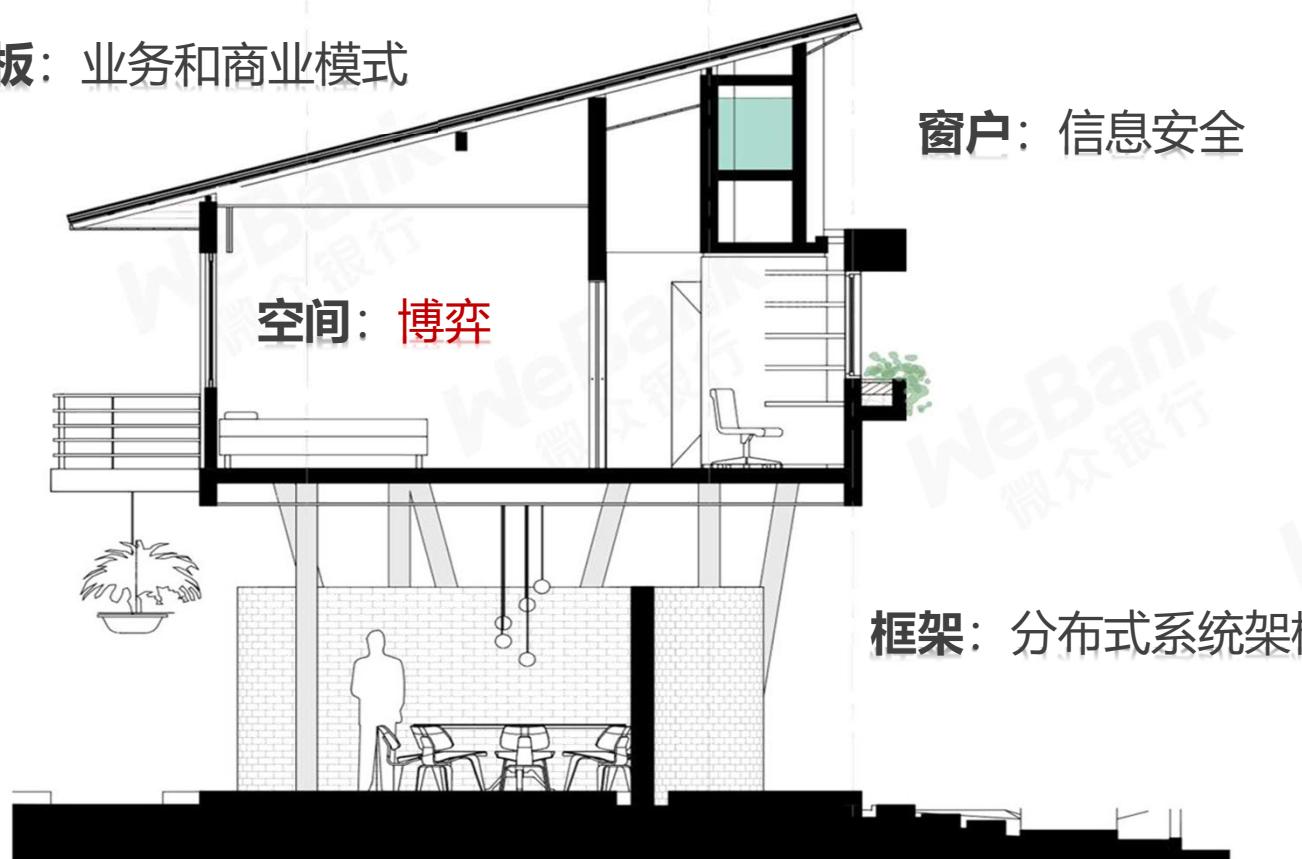
一个比喻

天花板：业务和商业模式

窗户：信息安全

空间：博弈

框架：分布式系统架构



地基：数学，密码学，操作系统，编译原理

区块链这个黑科技
其实并没有发明什么新的技术
都是成熟技术的组合



◆ 区块链的核心特性

密码学



区块数据



分布网络



分布式数据库

共识协作



可信的多方合作

- 计算，通信，存储，隐私均进行加密保护，数字签名的运用导致行为无法抵赖
- 独特的链式数据，容易验证和追查，难以篡改，数据具有高一致性，多方冗余存储不怕丢失
- 对等网络通信，多中心，无中介，高效率高可用
- 结合共识机制和智能合约，进行协同计算和群体验证，具有高确定性和高可信性，共同构建高效商业模式

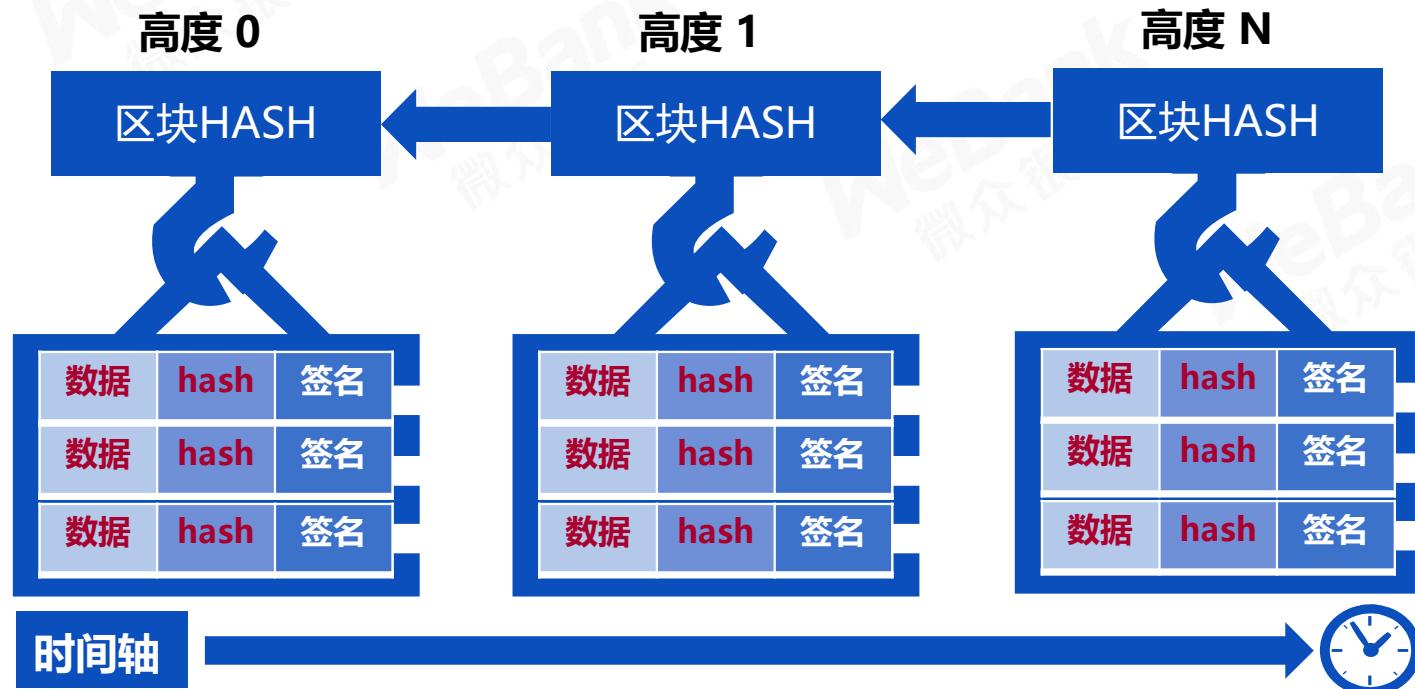
◆ 密码学:实现数据的验证和确权

- **哈希(HASH)**:表示大量数据的唯一摘要值。原数据的少量更改会在哈希值中产生不可预知的大量更改,可以作为数据的验证凭据
- **数字签名**:信息的发送者(掌握私钥)能产生的别人无法伪造的一段数字串,且可以通过其公布出去的公钥验证是由他发送。



◆ 区块数据: 数据合入区块，区块构成数据链

- 每个区块包含一段时间（如10秒）内产生的交易数据
- 把相关的数据汇总计算摘要，进行汇总的完整性正确性证明
- 每个区块计算摘要时，把前一个区块的摘要做为一个数据计算在内，构成了数据链
- 最新区块包含了所有数据链的完整性证明，整个链条上的任何数据改动都会破坏数据链的相关性



◆ 分布网络：点对点网络里的反复接力传播



- 消息无差别的对自己相邻的节点进行发送，所以称为广播，存在一定的冗余
- 所谓“一传十，十传百，百传千”
- 所有消息通过反复的广播传递，具有极大的概率达到全网

◆ 共识机制：分布式一致性

区块链的使命是要解决去信任的问题，达成这个使命需要采用去中心或者多中心的手段，而多个参与者的系统就会存在一致性的问题，要解决一致性的问题就必须引入共识机制



02

FISCO BCOS 案例分析

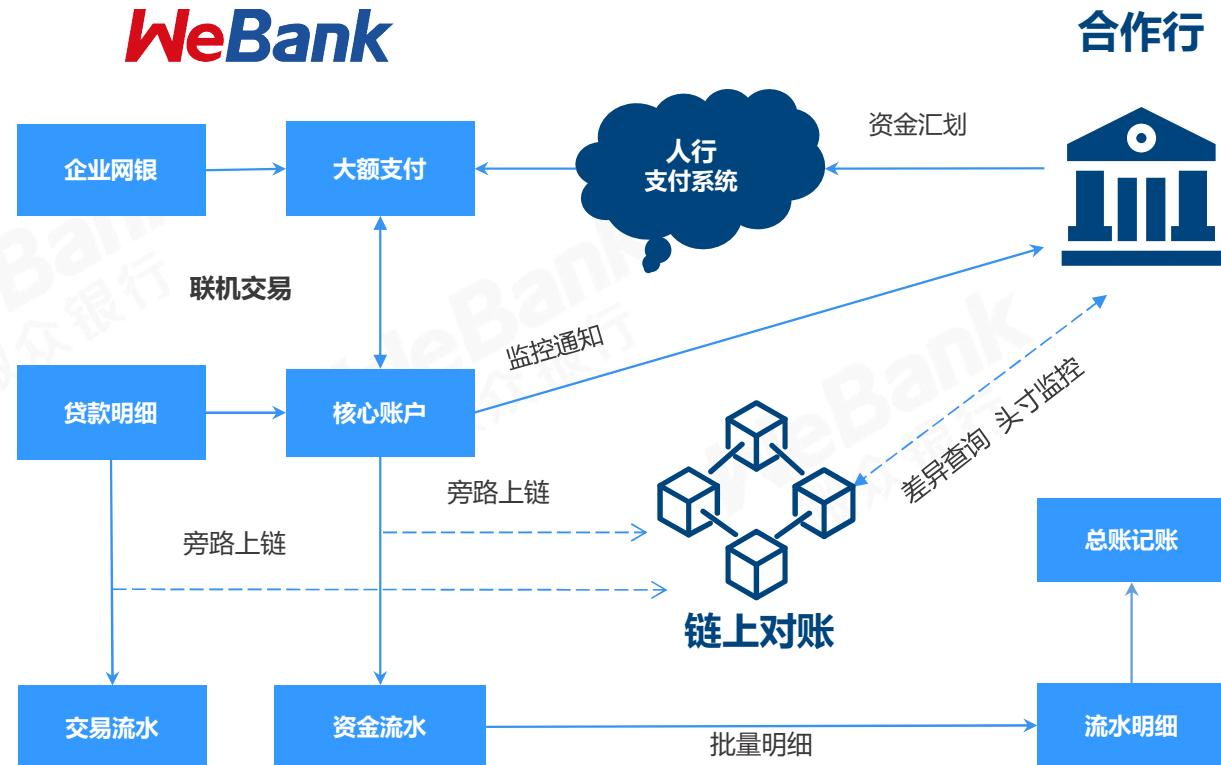
目录

1. 区块链相关知识介绍
2. FISCO BCOS 案例分析
 - 2.1 机构间对账
 - 2.2 仲裁链
3. FISCO BCOS 底层平台开发知识介绍

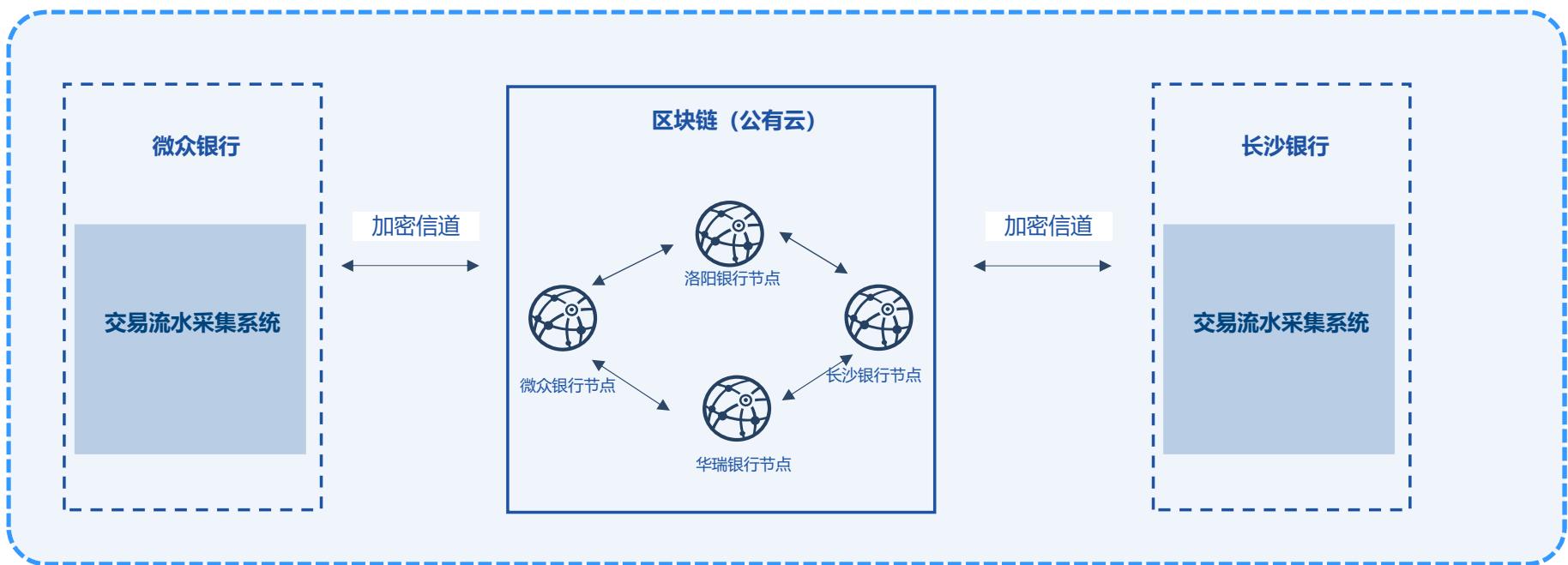
WeBank

业务概述

- 国内首个在生产环境投产运行的多金融机构间的区块链应用；
- 目前已接入3家合作行，在生产环境中运行的交易记录笔数已达1500万笔；
- 上线两年多时间，保持零故障运行。



系统架构

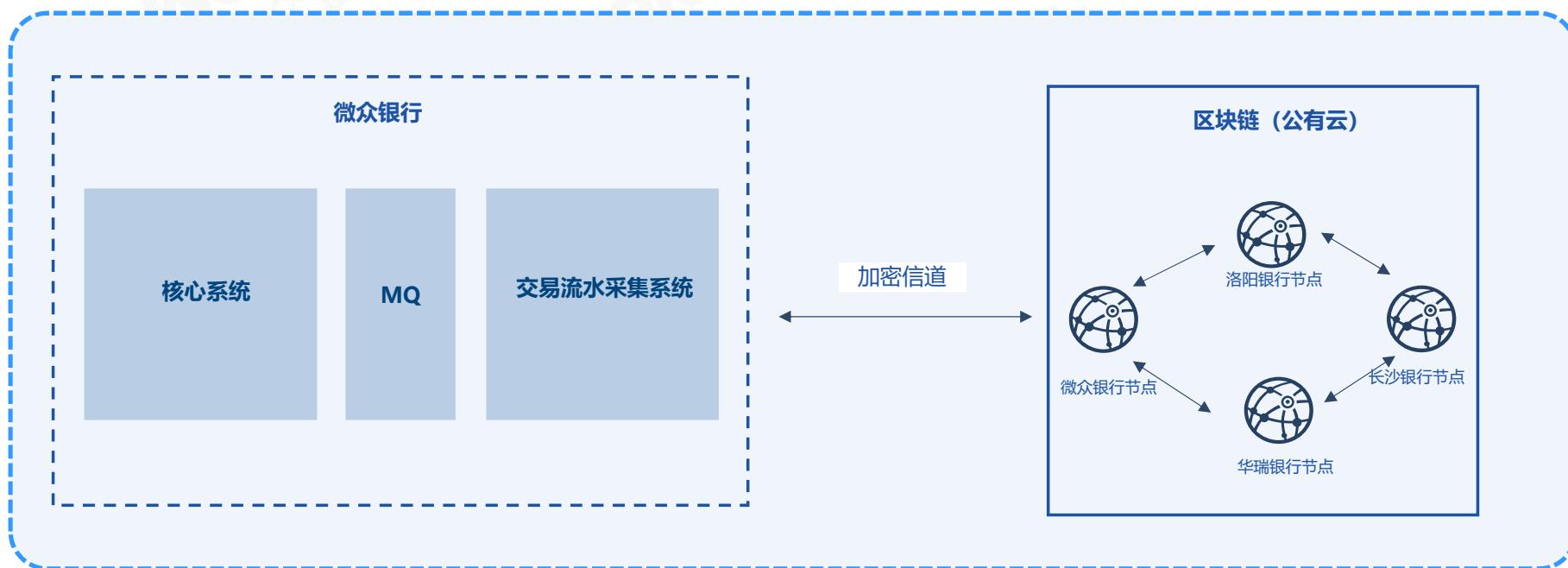


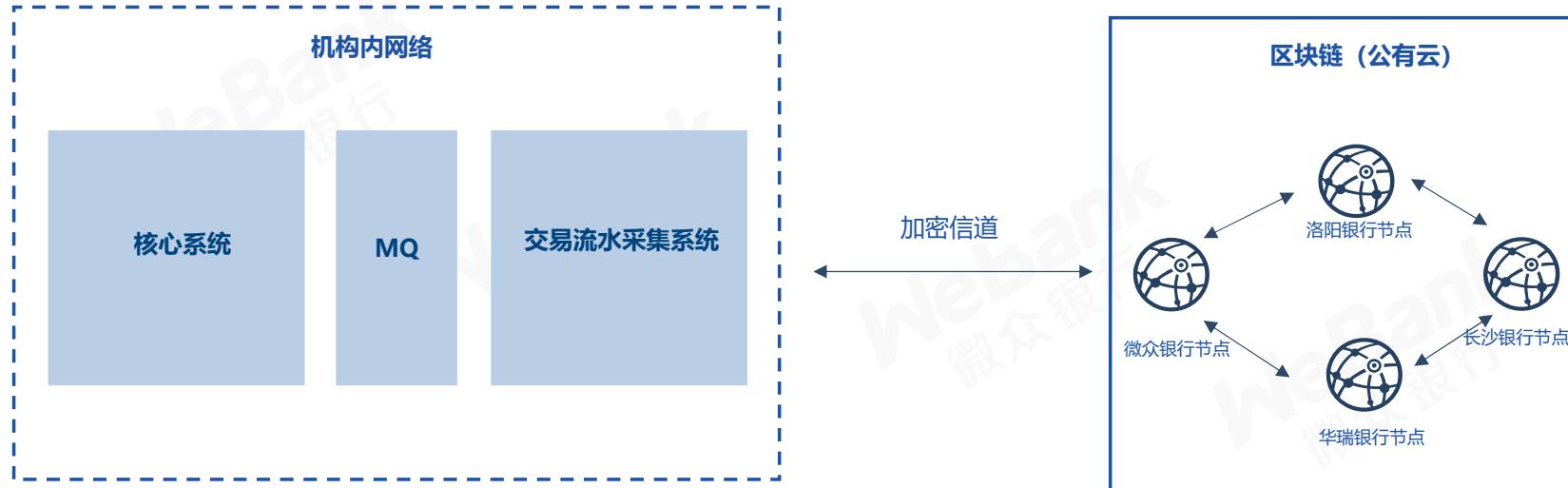
区块链对账的优势

传统对账	区块链对账
需要协商银行流水格式	提供统一区块链对账标准协议
需要搭建专线，考虑异地、灾备和切换的问题	网络架构灵活，即支持走公网网络、也支持走专线网络，或混合部署
对账数据集中传输，对带宽和可用性要求高	对账数据实时传输，对带宽要求低
日终对账，发现问题存在滞后	对账实时性高，能在秒级确认账目不平
只支持两方对账	支持两方、多方对账

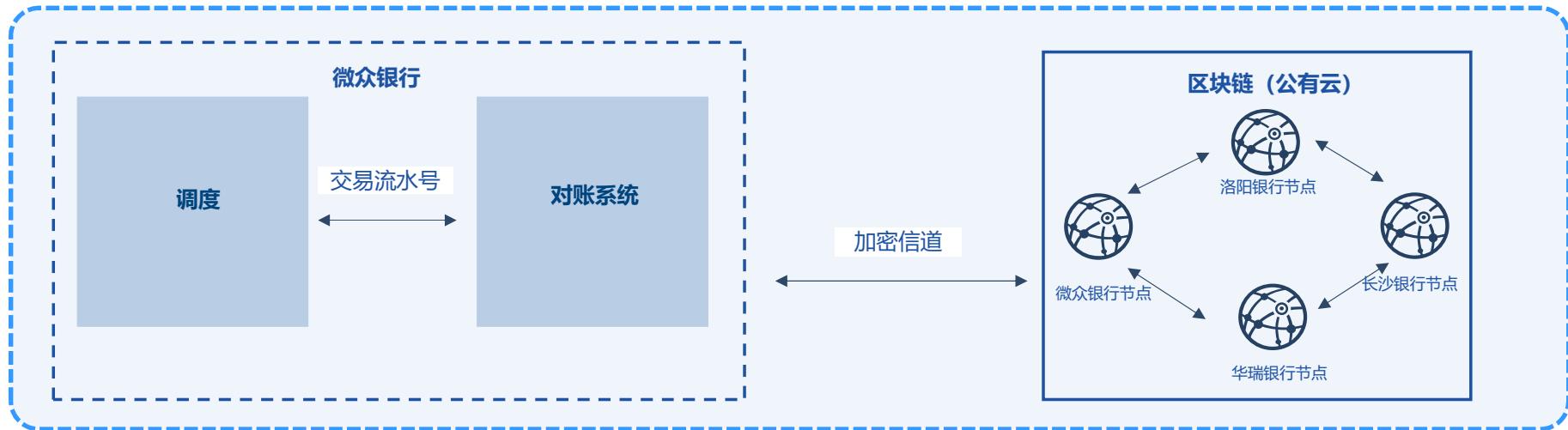
交易流水实时上链

- 机构在行内部署交易流水采集系统，接入到行内的 MQ，实时采集每一条流水，并发送到区块链
- 流水被发送上链后，通过 P2P 网络和 PBFT 共识机制，同步到全网
- 每天日终，交易流水采集系统的流水与与核心系统的流水，进行内部对账，补发上链





准实时对账



交易流水号	微众银行流水	长沙银行流水
201810210005	10月21日，张三转账5000元给李四（借）	10月21日，李四查收张三的5000元（贷）

有借必有贷，借贷必相等

统一对账标准

- 制定统一对账标准，任何金融机构都可以加入和参与区块链对账
 - 标准流水格式
 - 标准对账逻辑
 - 标准系统架构

022

仲裁链

WeBank

Copyright 微众银行©版权所有，不得侵犯

业务概述

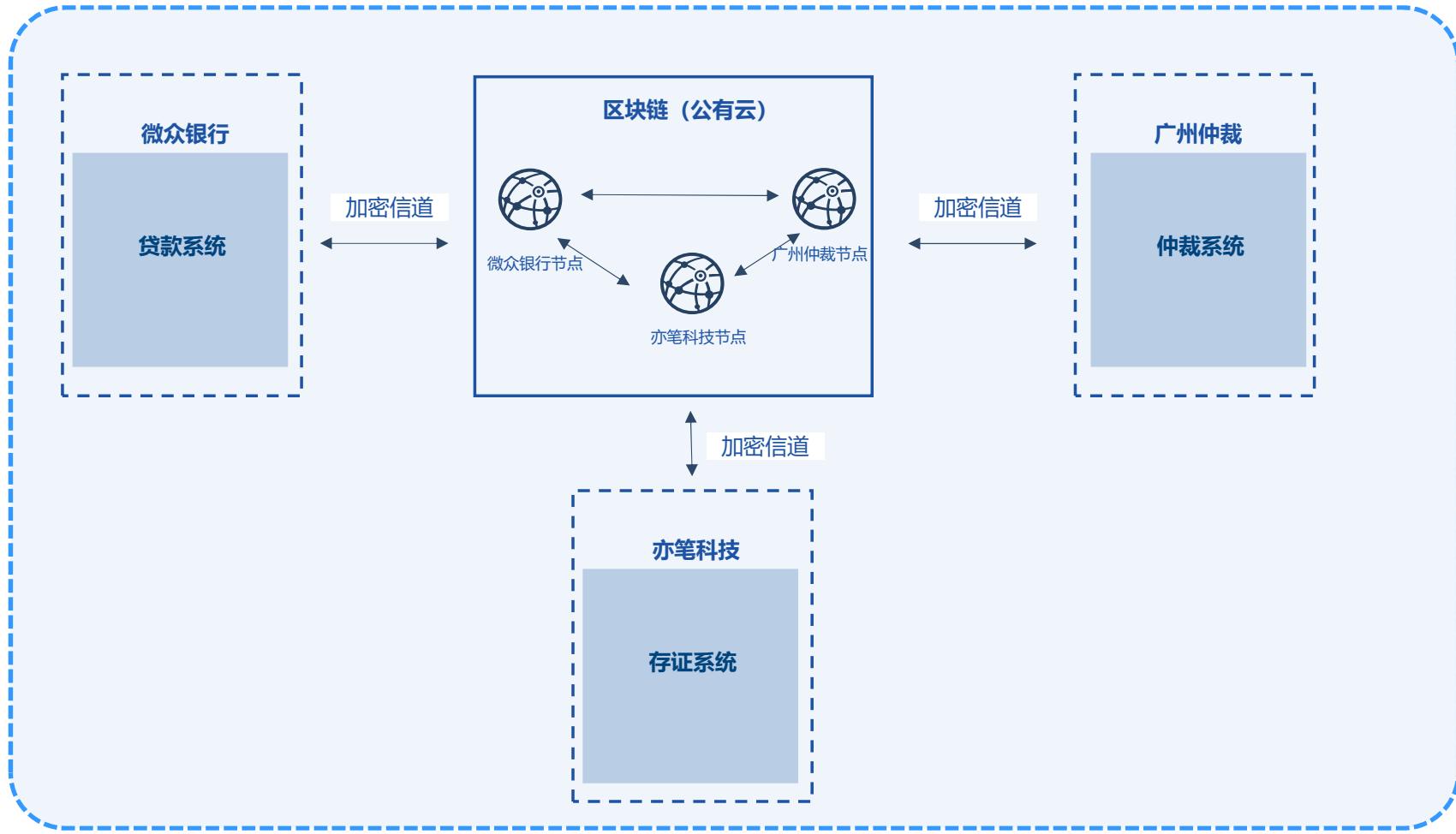
- 完善的防篡改机制：**使用区块链技术保全证据，进一步加强了证据的不可篡改性。
- 证据效力得到机构认可：**司法机构为作链上节点，对上链数据参与认可和签名，事后可从链上确认数据的真实有效性。
- 服务持续有效：**数据被多方共识上链后，即使有部分共识方退出也不会造成数据的丢失或失效。
- 诞生首份裁决书：**2018年2月，广州仲裁委基于“仲裁链”出具了业内首个裁决书，标志着区块链应用在司法领域的真正落地并完成价值验证。



仲裁链的优势

- 传统仲裁业务
 - 证据数据保存在存证公司，存在丢失、篡改的风险
 - 存证公司作恶
 - 存证公司运营状况
- 仲裁链
 - 证据数据即可保存在银行、也可保存在存证公司
 - 证据数据，无法被任何一方篡改
 - 任一区块链参与方退出，不影响已共识的证据

系统架构



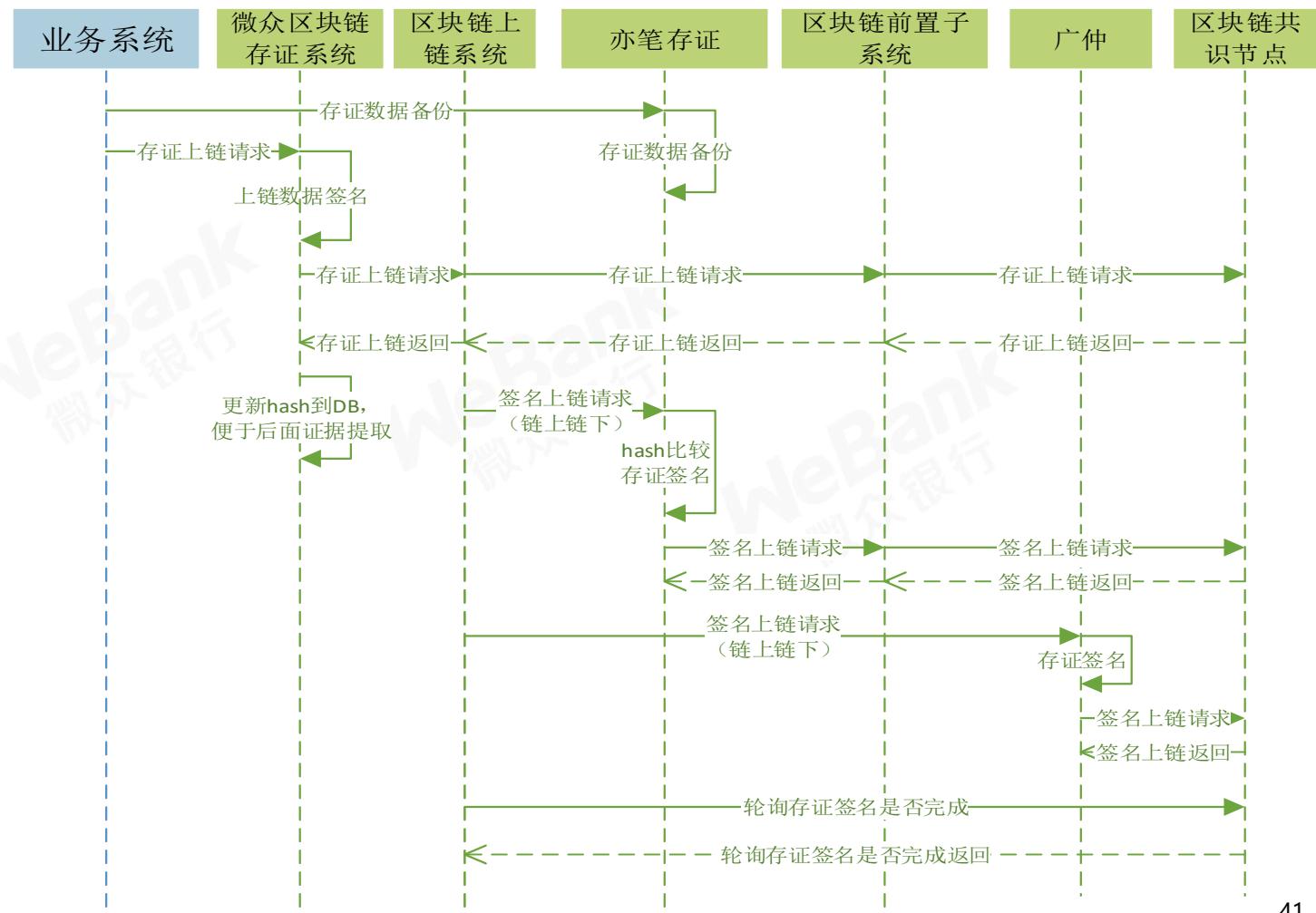
证据智能合约

- 每个证据，保存为一个证据智能合约
- 证据智能合约包括几个部分
 - 证据 Hash：证据数据以压缩包或 PDF 格式保存在微众银行和亦笔科技，证据数据不上链，证据数据的 Hash 值上链
 - 微众银行签名：微众银行对证据 Hash 的签名
 - 广州仲裁签名：广州仲裁对证据 Hash 的签名
 - 亦笔科技签名：亦笔科技对证据 Hash 的签名



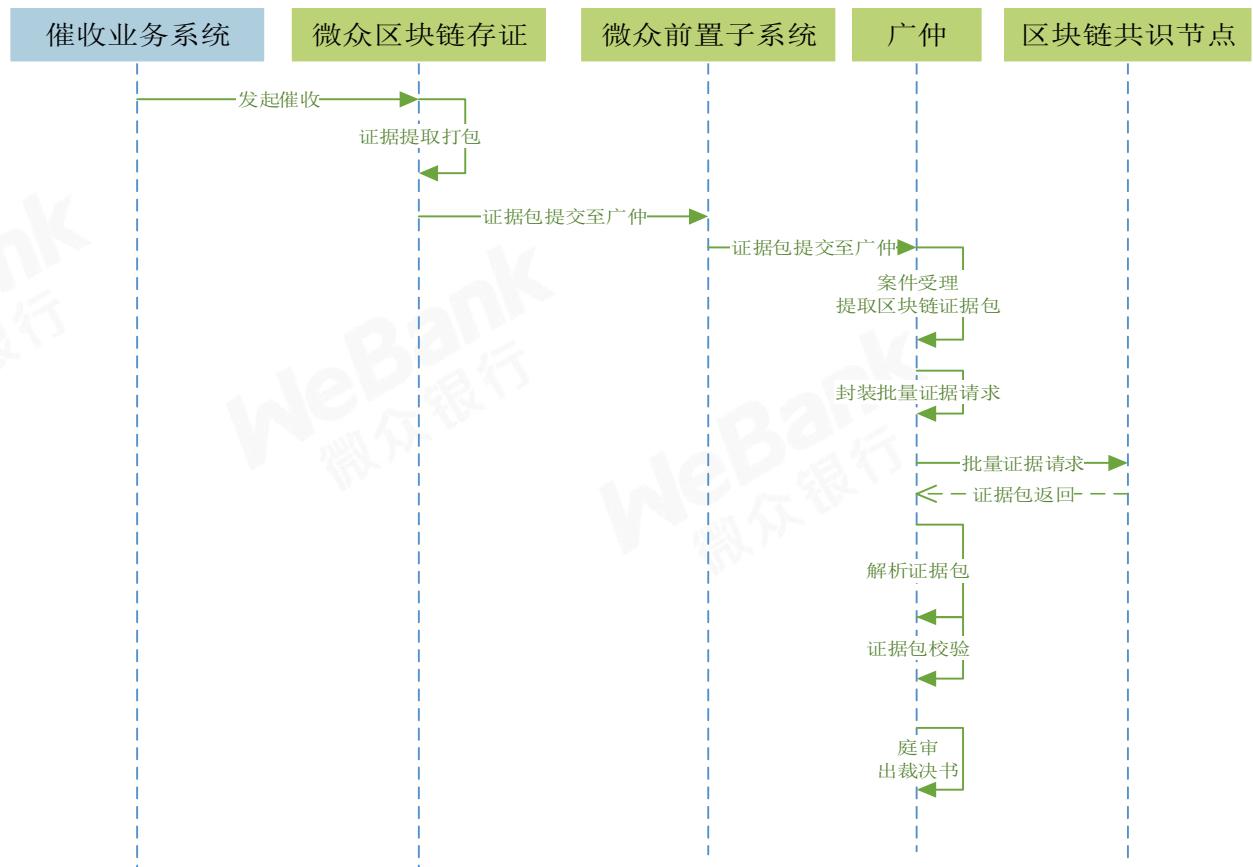
证据上链

1. 微众银行，将证据智能合约部署到区块链
2. 微众银行，通知广州仲裁和亦笔科技，有新证据上链
3. 广州仲裁和亦笔科技，获取证据智能合约，对证据 Hash 签名，通过交易发送上链



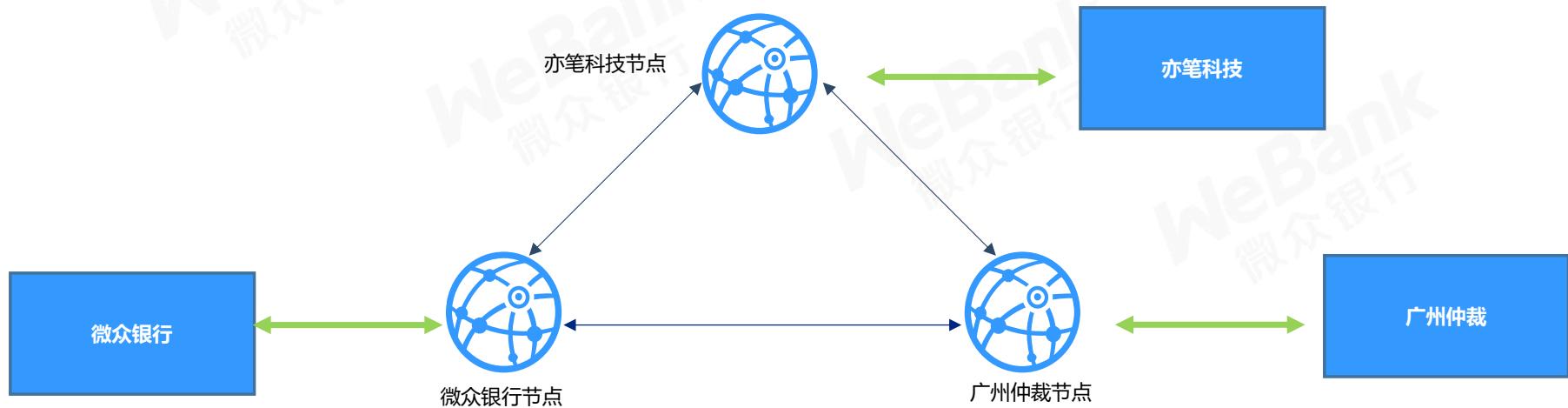
证据取证

- 微众银行，催收业务系统筛选出违约用户，将证据包和证据智能合约地址发送给广州仲裁
- 广州仲裁，从区块链节点获取证据智能合约，校验证据包的 Hash
- 广州仲裁，校验证据智能合约是否有足够的签名



通知机制

- 使用 AMOP 功能，进行可靠的消息通知



更多案例

- FISCO BCOS目前已有多数应用落地，百级参与机构，千级社区成员，并且仍在与日俱增中。
- 其影响力遍及以支付、对账、交易清结算、资产数字化、供应链金融、数据存证、征信、场外市场等为代表的金融领域，以及司法存证、文化版权、娱乐游戏、社会管理、政务服务等领域。
- 我们甄选其中较为典型的应用场景制作了一个《FISCO BCOS案例精编》，从场景解决方案的维度，介绍区块链优势、区块链解决方案，及目前落地的实践案例。



扫码下载《FISCO BCOS案例精编》

03

FISCO BCOS底层平台开发知识介绍

目录

1. 区块链相关知识介绍
2. FISCO BCOS 案例分析
3. FISCO BCOS 底层平台开发知识介绍
 - 3.1 基础介绍
 - 3.2 体验指南

031

FISCO BCOS底层平台基础介绍

FISCO-BCOS 集实践大成的开源底层平台

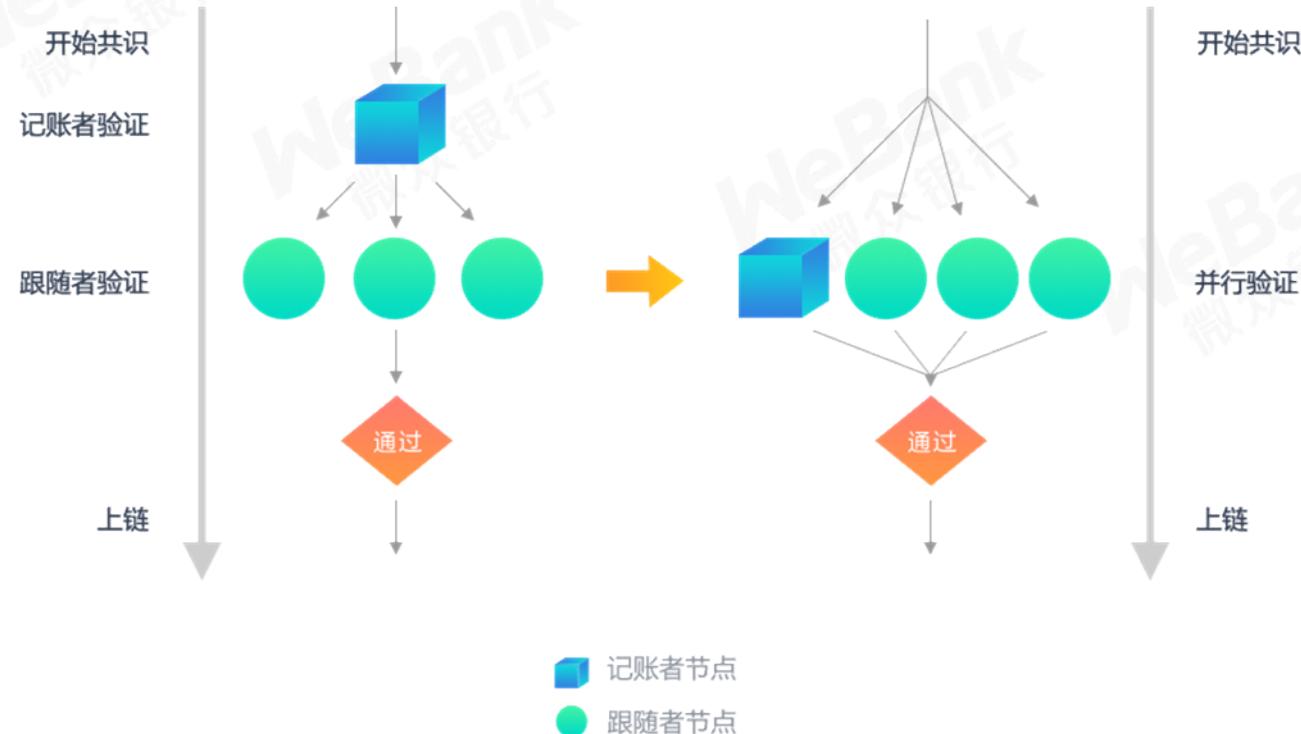
- 基于BCOS，进行模块升级与功能重塑；
- 打造自主可控的区块链底层平台；
- 完全对外开源；
- 针对金融行业的监管合规与特定业务需求；
- 由金链盟开源工作组开发和完善；
- 定期将新属性提交主干版本。



金融分支版本FISCO BCOS

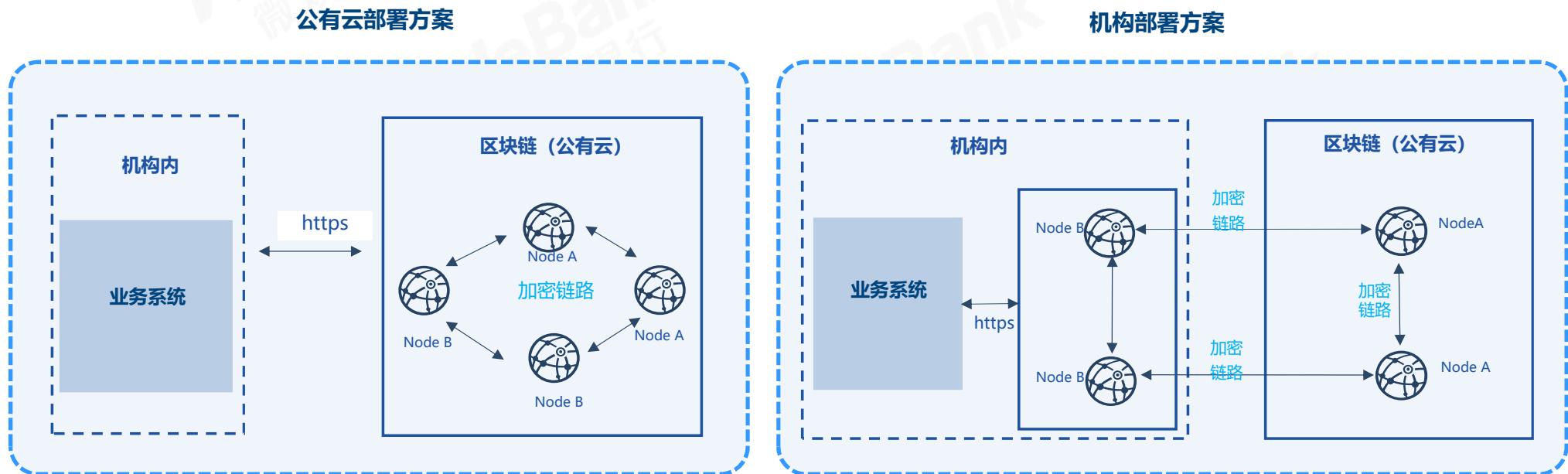
共识机制

- PBFT 共识机制，保证区块链上的数据一致不被篡改
- 区块链机制，保证区块数据篡改成本极高



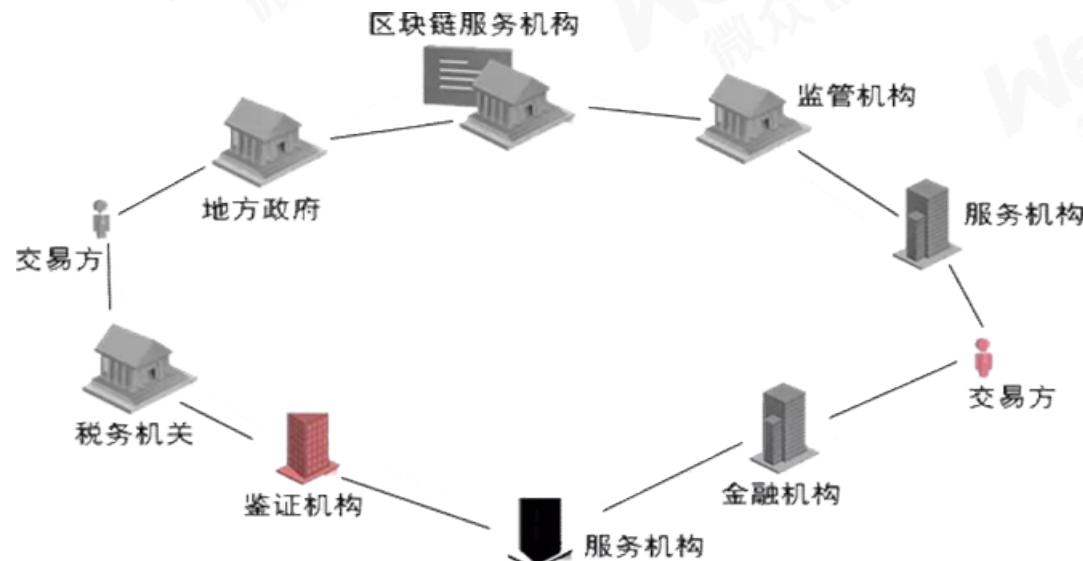
P2P 网络机制

- P2P 网络机制自动维护区块链网络节点间的长连接，在程序故障、网络异常时，自动尝试重连和恢复故障
- P2P 网络机制采用密钥协商和信道加密技术，使 FISCO-BCOS 区块链节点可以安全地部署在公网环境上
- P2P 网络机制基于 TCP 长连接技术，兼容市面上大多数网络设备和防火墙



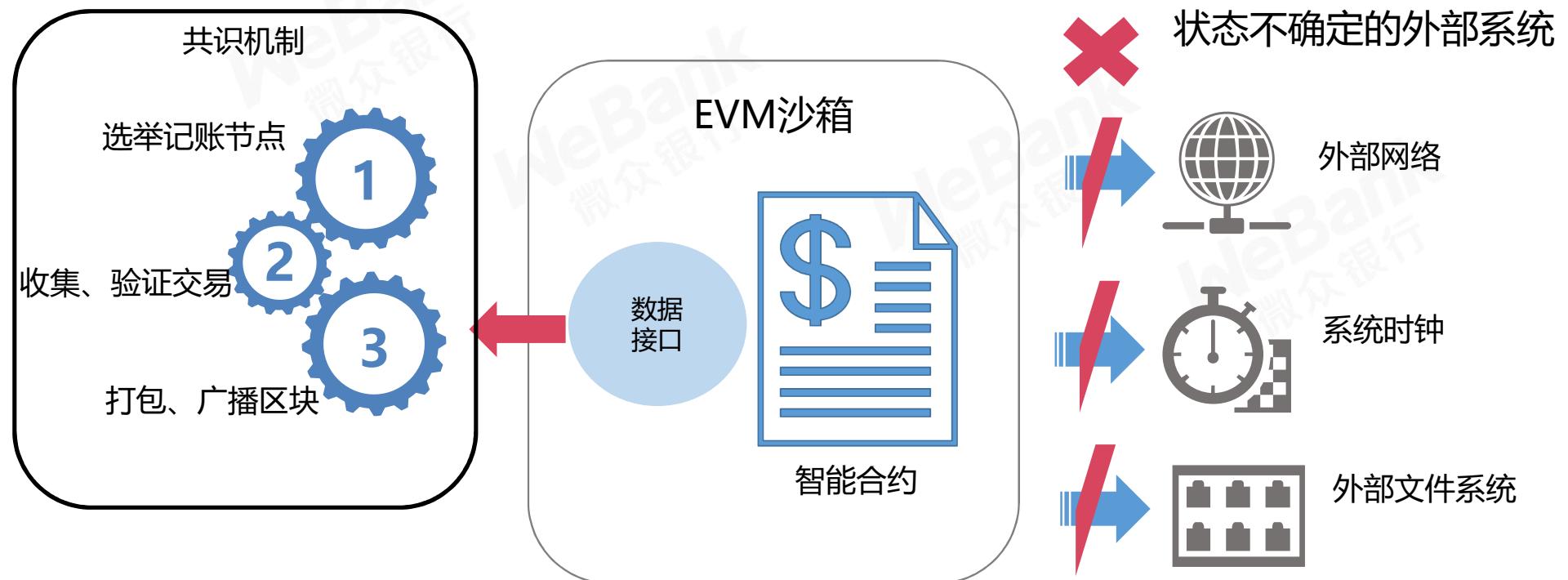
密码学技术

- SHA256 技术，保证区块链上的数据不被篡改
- CA 认证技术，确保区块链网络中所有节点都有合法的许可和授权
- 密钥协商和对称密钥加密技术，确保区块链网络的通信无法被窃听
- 非对称加密和签名技术
 - 确保每个区块链节点拥有唯一的标识，在共识机制中无法被仿冒
 - 确保每个交易发起者拥有唯一的标识，在发送交易时无法被仿冒



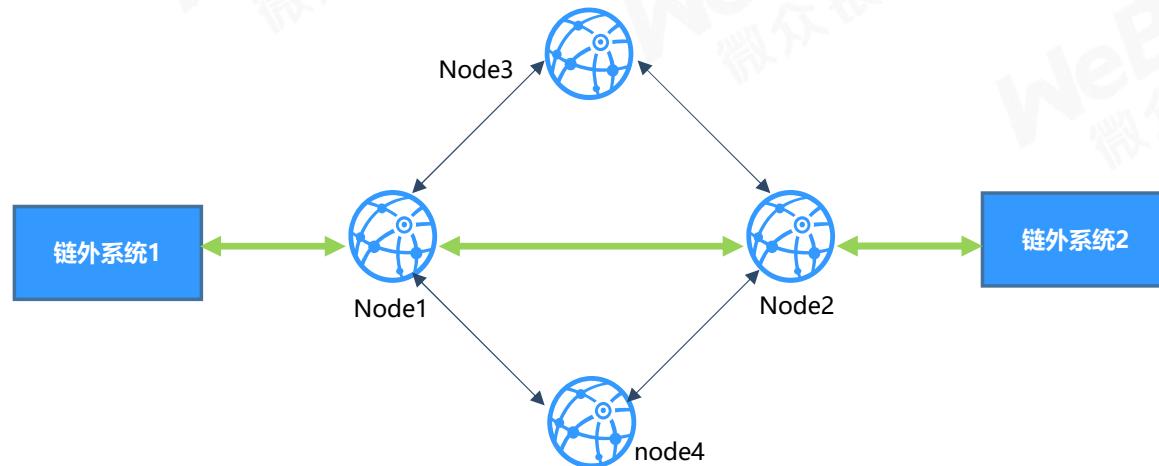
智能合约

- 智能合约是图灵完备的编程语言
- 支持复杂的业务逻辑



AMOP

- 高效、可靠，基于区块链网络的消息通信协议——AMOP (Advanced Messaging On-chain Protocol)
- 支持跨机构之间，点对点的实时消息通信
- 为链外系统和区块链之间的交互提供标准化接口
- 基于 P2P 网络机制的密钥协商和信道加密技术，保证 AMOP 通信无法被窃听
- 消息收发均有异常重传、超时检测和路径规划机制，确保消息传输的可靠性



032

FISCO BCOS体验指南

FISCO BCOS 开源文档

The screenshot shows the FISCO BCOS documentation website. The top navigation bar includes the FISCO BCOS logo, a search bar, and a 'latest' version indicator. The sidebar on the left lists several sections: Quick Guide, Manual Deployment, Usage Guide, Advanced Contract调用 (web3sdk), Enterprise Deployment Tools (Material Package), Chinese Version FISCO BCOS, Feature Details, Application Practice, Wiki, and Community. At the bottom of the sidebar is an advertisement for 'RACHEL' (the easiest way to bring content to offline areas). The main content area is titled '快速指引' (Quick Guide) and features a green header with an exclamation mark icon and the text '重要' (Important). It contains sections for '快速部署工具' (Quick Deployment Tools) with links to FISCO BCOS material packages and Docker, '手工部署' (Manual Deployment) with a link to the manual deployment section, '国密版FISCO-BCOS' (Chinese Version FISCO-BCOS) with links to the Chinese version and web3sdk, and 'web3sdk' with links to the SDK usage guide and application development guide.

FISCO BCOS 物料包

物料包sample体验

极简方式快速搭建一条区块链，让你拥有一条属于自己的联盟链

```
INFO|2018-10-25 11:12:53:513|PBFTClient.cpp:343|+++++ Generating seal onb6b27cc318f3a804  
e67a8089d7324ebbd9fcb53b0c80d971e76f4af4451b5ef#1tx:0,maxtx:1000,tq.num=0time:1540437173513  
^[[B^[[AINFO|2018-10-25 11:12:56:555|PBFTClient.cpp:343|+++++ Generating seal on26a0e15e  
b86241377fcf85fa3f98a48c52490a8a4d796e9da0981b84fd839ef9#1tx:0,maxtx:1000,tq.num=0time:1540437176555  
INFO|2018-10-25 11:12:59:594|PBFTClient.cpp:343|+++++ Generating seal on869e5b4caae9014b  
d8227108fcccb192adc93178a0f50fa7127e63a0d4f61685#1tx:0,maxtx:1000,tq.num=0time:1540437179594  
INFO|2018-10-25 11:13:02:628|PBFTClient.cpp:343|+++++ Generating seal on2455a6e6d2f35611  
846a41d644ec51c234989f40c29a50e0a51ec433f97cf56#1tx:0,maxtx:1000,tq.num=0time:1540437182628  
INFO|2018-10-25 11:13:05:677|PBFTClient.cpp:343|+++++ Generating seal on32fc3caed29d7405  
1eee134f626fe4fdf16ee2eb614d14d219aaff89e319646b#1tx:0,maxtx:1000,tq.num=0time:1540437185677
```

FISCO BCOS 浏览器

通过部署浏览器直观看到区块上的相关数据

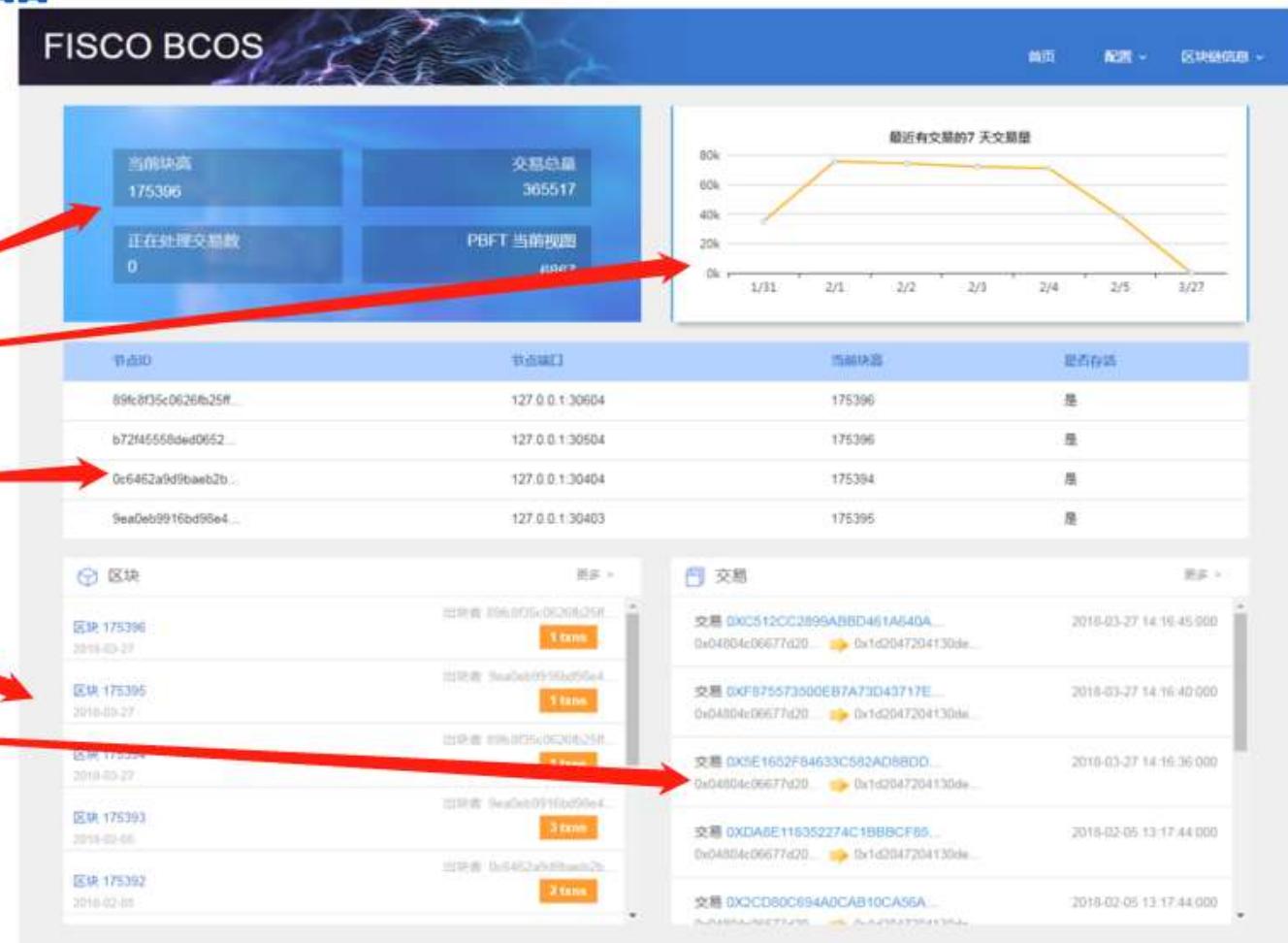
交易数目

消息概览

记账节点

区块数据

交易数据



FISCO BCOS 进阶体验

手工搭链 => 国密版搭链

从无到有一步步搭建区块链，了解区块链相关原理

存证业务体验

在区块链上跑起属于自己的业务

FISCO BCOS 1.5版本

体验分布式存储，了解FISCO BCOS如何解决以太坊性能瓶颈

FISCO BCOS Wiki

了解FISCO BCOS的相关技术

FISCO BCOS 群环签名，零知识服务操作手册

体验密码学在区块链中隐私保护的作用

0x

开源之路

FISCO BCOS——集实践大成的开源底层平台

- 由金链盟开源工作组进行规划和开发，针对金融行业的监管合规与特定业务需求；
- 打造安全可控的区块链底层平台，完全对行业开源；



社区群管理员



金融区块链平台FISCO BCOS



开源社区GITHUB网址

WeBank

Copyright 微众银行©版权所有，不得侵犯

◆ 开源生态—应用大赛



金链盟中国区块链应用大赛

盟九州·链未来



扫码报名



大赛专业度

专家评审
技术支持



大赛关注度

媒体传播
年度盛事



项目孵化

加速器对接
产业资源



奖项设置

特等奖 奖金100万
一等奖 奖金50万
二等奖 奖金30万
三等奖 奖金5万



谢谢

Thanks



社区群管理员

