区块链催生互联网金融下一代技术

--区块链技术在金融领域的应用

01 异军突起的区块链技术

关于区块链架构师须知的那些事

02 区块链成为FinTech2.0的代表

区块链在金融应用实战中面临的挑战

03 区块链在其他领域的突破

仰望星空、脚踏实地

金融行业区块链热潮-跨境支付、征信、交易转让、存管结算

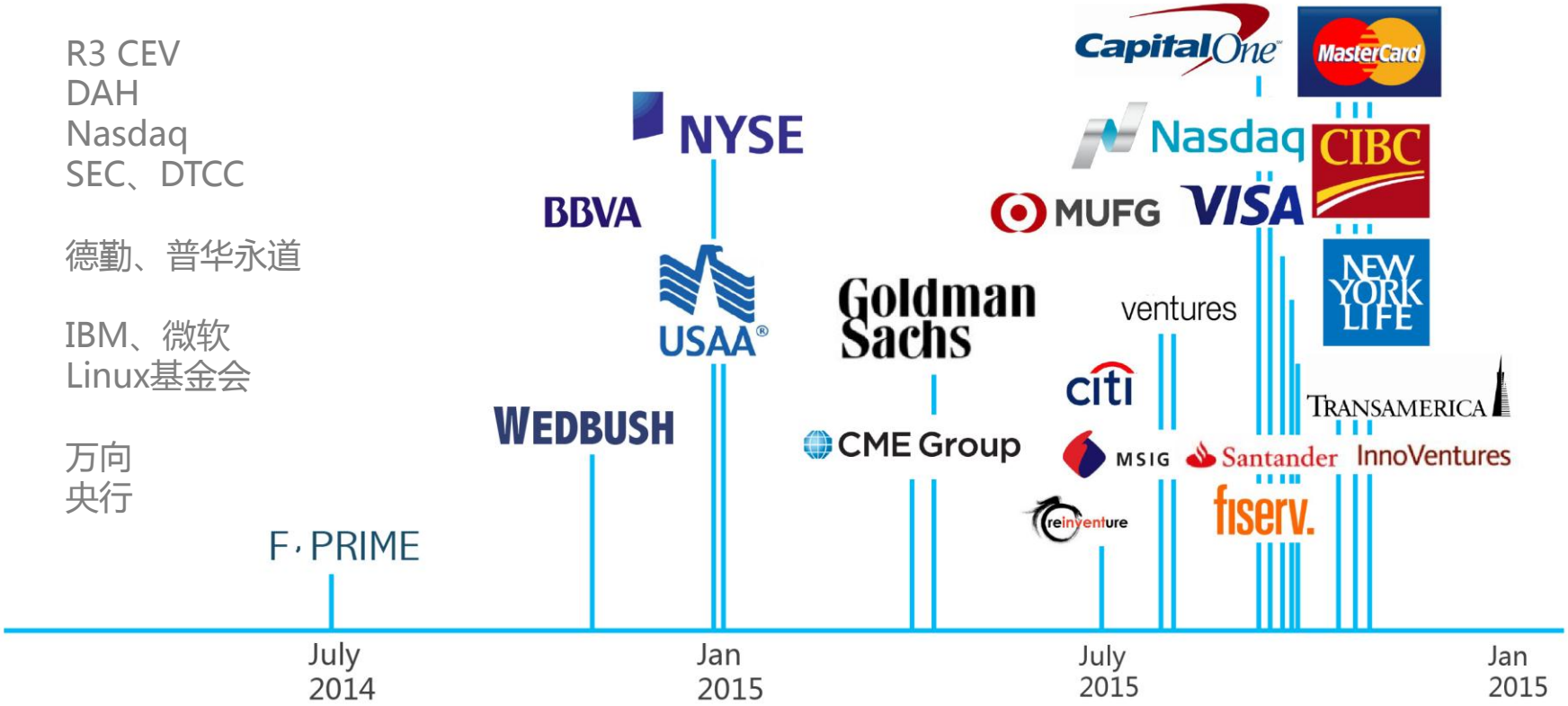
一年间重量级玩家尽数亮相

R3 CEV
DAH
Nasdaq
SEC、DTCC

德勤、普华永道

IBM、微软
Linux基金会

万向
央行



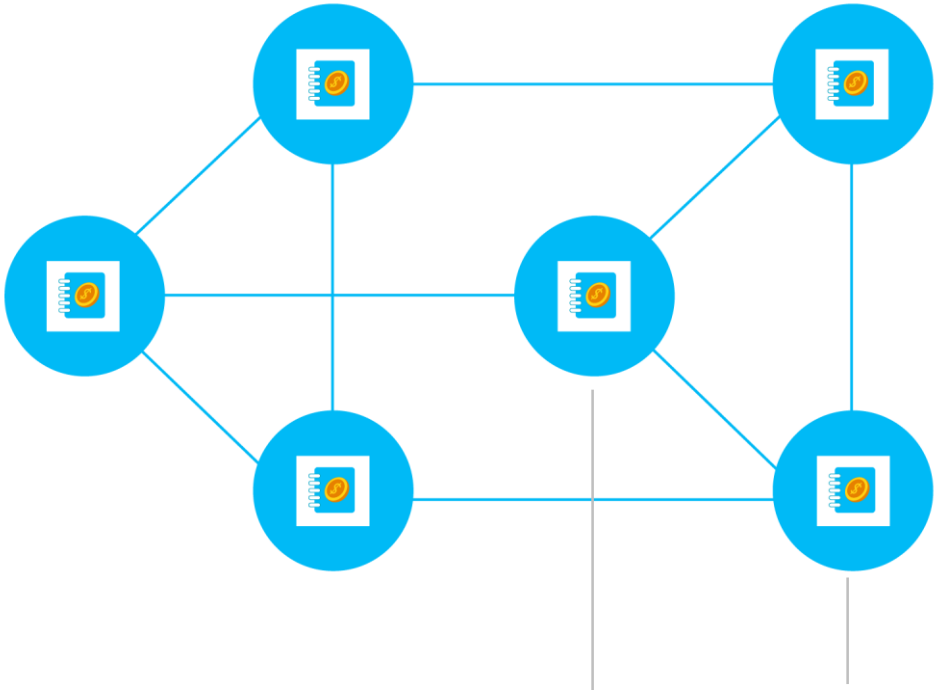
区块链技术源起8年前的“比特币”

大神用极简方式实现一套点对点现金系统

1. 一份所有参与人共同维护的公开账本 - 70G数据

2. 一套加密货币发行机制 - 500亿市值

去中心、去信任的记账模式



1. 产生新交易
2. 争抢记账权
3. 扩散验证后的交易

每个用户节点，都可以自由加入网络。（完全分布式的p2p网络）

每个用户节点，都维护有账本。某个节点的恶意篡改，不能得到其余节点的认同。

区块链的特性与关键技术基础

去中心、去信任、不可篡改、可追溯性、可匿名性、开放性

记账与经济激励机制

1.令人迷惑的“分布式”

烧脑 一张表是如何支撑起一套支付系统的？

2.传说中的“矿工”就是记账员

烧脑 400年依赖可信任记账员的记账规则就这么颠覆了？

3.用经济激励让矿工争抢记账权

烧脑 怎么防止唯利是图的矿工乱记账？

4.一个简单精巧的争抢游戏-“掷色子”

烧脑 算法是怎么保证账本的不可篡改性？

区块链选用的数学算法-简单、成熟

HASH算法：SHA256安全散列算法

特点

1. A的内容有细小变动， 经SHA256运算后的结果B（长度固定为256位）几乎每位都有差异；
2. 验证B是否为A的SHA256运算结果很简单，但用B反推出A几乎不可能，只能靠暴力穷举。

用途

矿工“掷色子”大赛、数字指纹等

公私匙非对称加解密算法：secp256k1椭圆曲线算法

特点

1. 私匙加密，只能用公匙解开—可用作数字签名，可以确认是持有私匙的发信人所发；
2. 公匙加密，只能用私匙解开—可用作数字信封，确保只有持有私匙的收信人才能打开。

用途

数字签名，证明身份，不用账户照样可以管好资产、执行交易

无法篡改区块链账本-通过P2P网络全球复制同步

出现不一致了，如何裁决？-很简单就是比分叉的长短

交易要等多久之后可以防篡改？真是“6度空间理论”

真的无法篡改吗？控制51%算力的人能干的坏事

公开的P2P网络，坏人还会怎么攻击？粉尘攻击、女巫攻击

最成功的比特币区块链存在的困境

1.挖矿带来无法承受的成本

全网挖矿成本接近每币3000元，每天1千万，价格回落挖矿收入减少是否会导致计算资源的撤出？

2.交易平台的脆弱性，性能、监管、黑客

交易确认速度变慢、区块同步速度慢、日处理交易峰值数有限；总节点规模较小，尚未经历大规模的广播风暴。

3.矿工与持有者社区的割裂

矿工只关注投入产出，欠缺对集中式矿池的自我制约动力，给生态带来风险。

4.失效的进化机制，系统迭代更新进展缓慢

系统开发者的收益无法保障，基金会靠捐款。

困境催生出的创新尝试带来 一个繁荣的生态

元币类：依附于比特币-增加上层协议

1. 彩色币，万事达币以及合约币Counterparty

山寨币类：克隆比特币-修改某些参数和行为

1. 货币策略不同（发行量，发行速度）：莱特币、狗狗币和Freicoin
2. 一致性机制创新：BitShares（比特股）,peercoin，Myriad，Blackcoin，vericoin 和 NXT
3. 多目的挖矿创新（解决电能浪费问题）：Primecoin, Curecoin, Gridcoin
4. 致力于匿名性的竞争币：CryptoNote, Bytecoin, Zerocash/Zerocoin, Darkcoin
5. 私有链、联盟链：R3、Hyper ledger

非货币型竞争块链类：仅利用区块链技术

1. 域名币：去中心的域名服务
2. Bitmessage：去中心化安全消息服务
3. Ethereum(以太坊)：解决比特币扩展性不足的问题，比特币网络是一套分布式的数据库，而以太坊则可以看作是一台分布式的计算机：区块链是计算机的ROM，合约是程序，而以太坊的矿工们则负责计算，担任CPU的角色

架构师关心什么？

1.性能

烧脑 定时记账，每秒多少笔？存储有多大？

2.可靠性

烧脑 P2P网络不稳定脑裂了怎么共识？集群怎么做？

3.安全性

烧脑 开放的网络、开源的代码、技术成熟度？

4.易用性

烧脑 随时要在线同步账本、交易的不确定性

5.可维护性

烧脑 去中心无主的系统，有Bug了怎么办？

6.兼容性

烧脑 还是那些熟悉的技术吗

01 异军突起的区块链技术

关于区块链架构师须知的那些事

02 区块链成为FinTech2.0的代表

区块链在金融应用实战中面临的挑战

03 区块链在其他领域的突破

仰望星空、脚踏实地

区块链成为FinTech2.0的代表

成本效益、防欺诈控制、全球可达

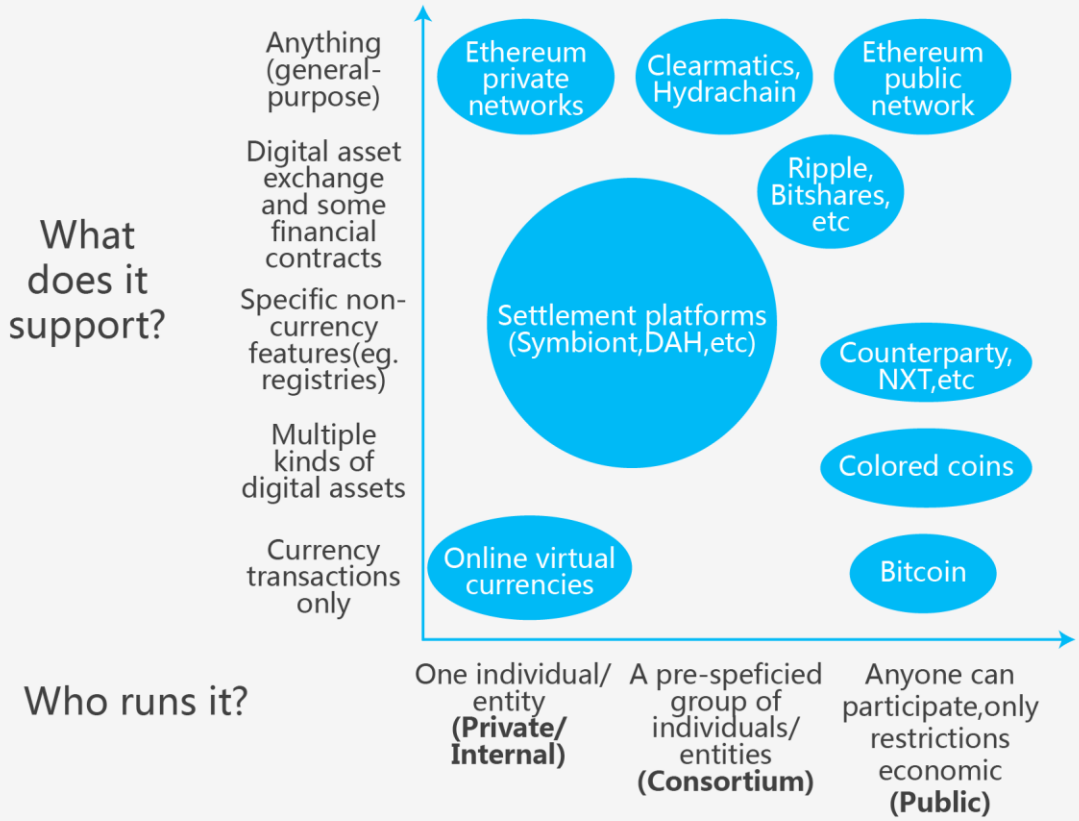
高盛最近预测

区块链技术每年能
为金融资本市场节

约60亿美金

区块链成为FinTech2.0的代表 – 重构金融基础设施

区块链的类型



私有链 | 联盟链 | 公有链

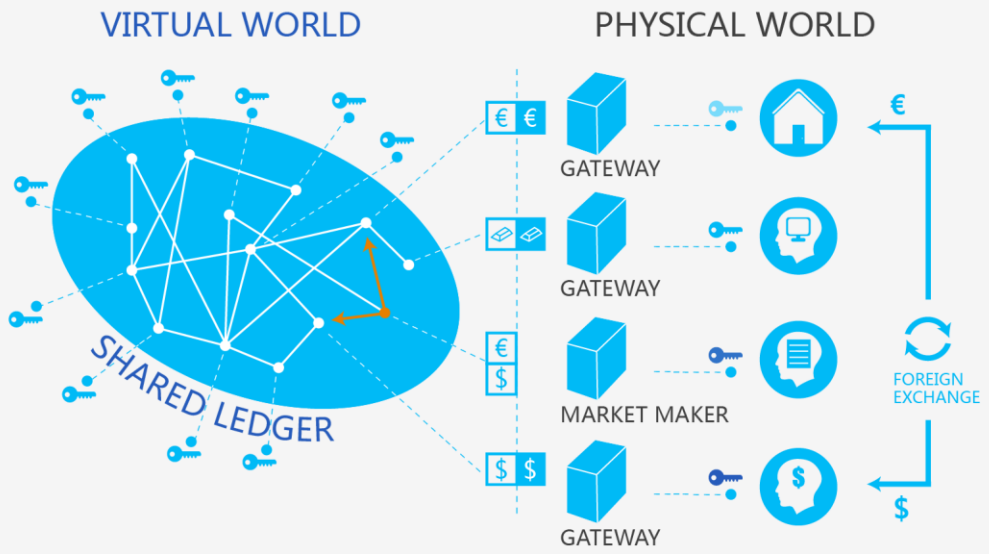
信息网络→价值网络

通用计算 去中心组织	区块链3.0
金融合约 资产交易	区块链2.0
数字公证	
数字资产	区块链1.0
加密货币	

区块链在金融领域的部署模式选择：联盟链

公有链的应用给人无限想象，联盟链也许是脚踏实地的选择：

分布式总账与网关应用的模式（Asset-Centric Application）



联盟链上的金融合约平台

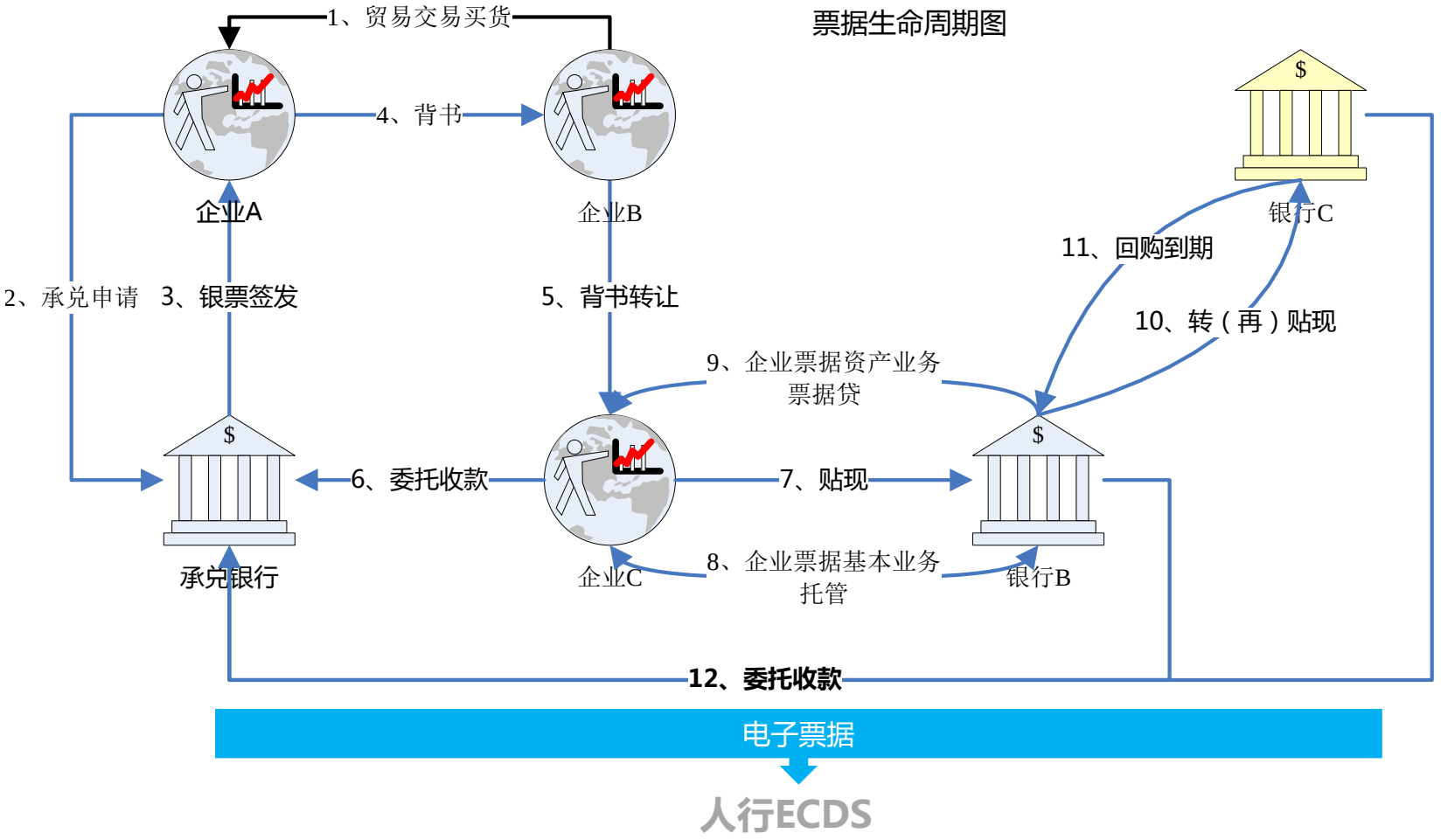
- 规避性能问题
- 优化共识机制
- 确保迭代进化
- 满足监管要求

成功的联盟链：业务跨界、规模足够

从“票据业务”剖析区块链应用面临的机会与挑战

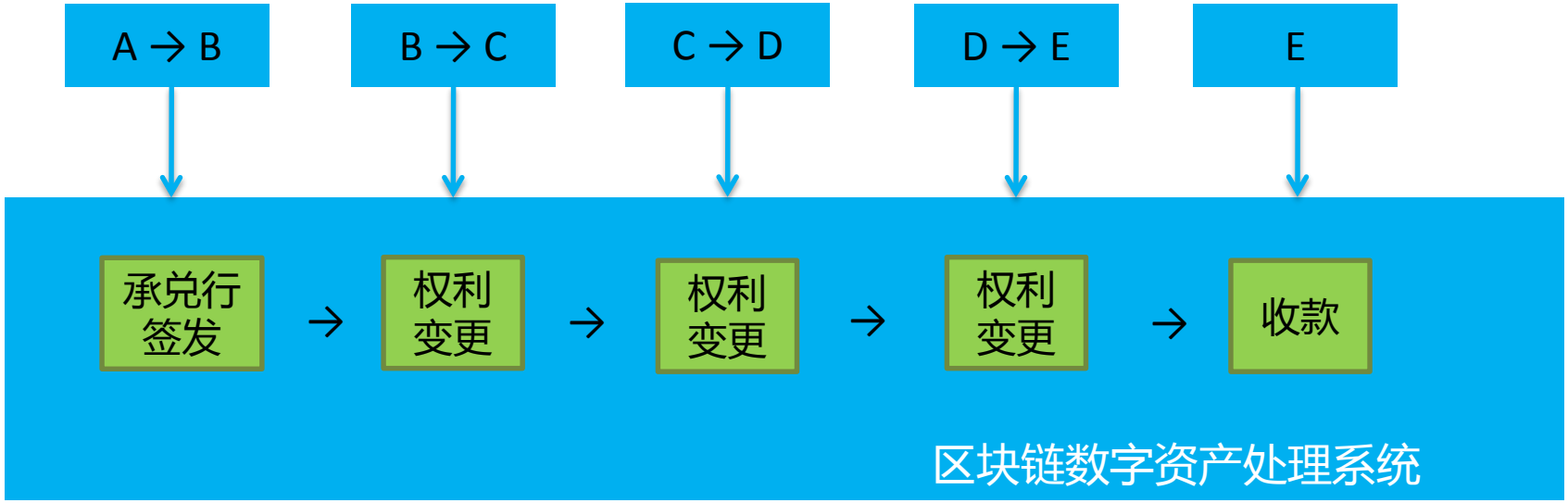
痛，然而电子化、集中化的过程会有多长？

从“票据业务”剖析区块链应用面临的机会与挑战



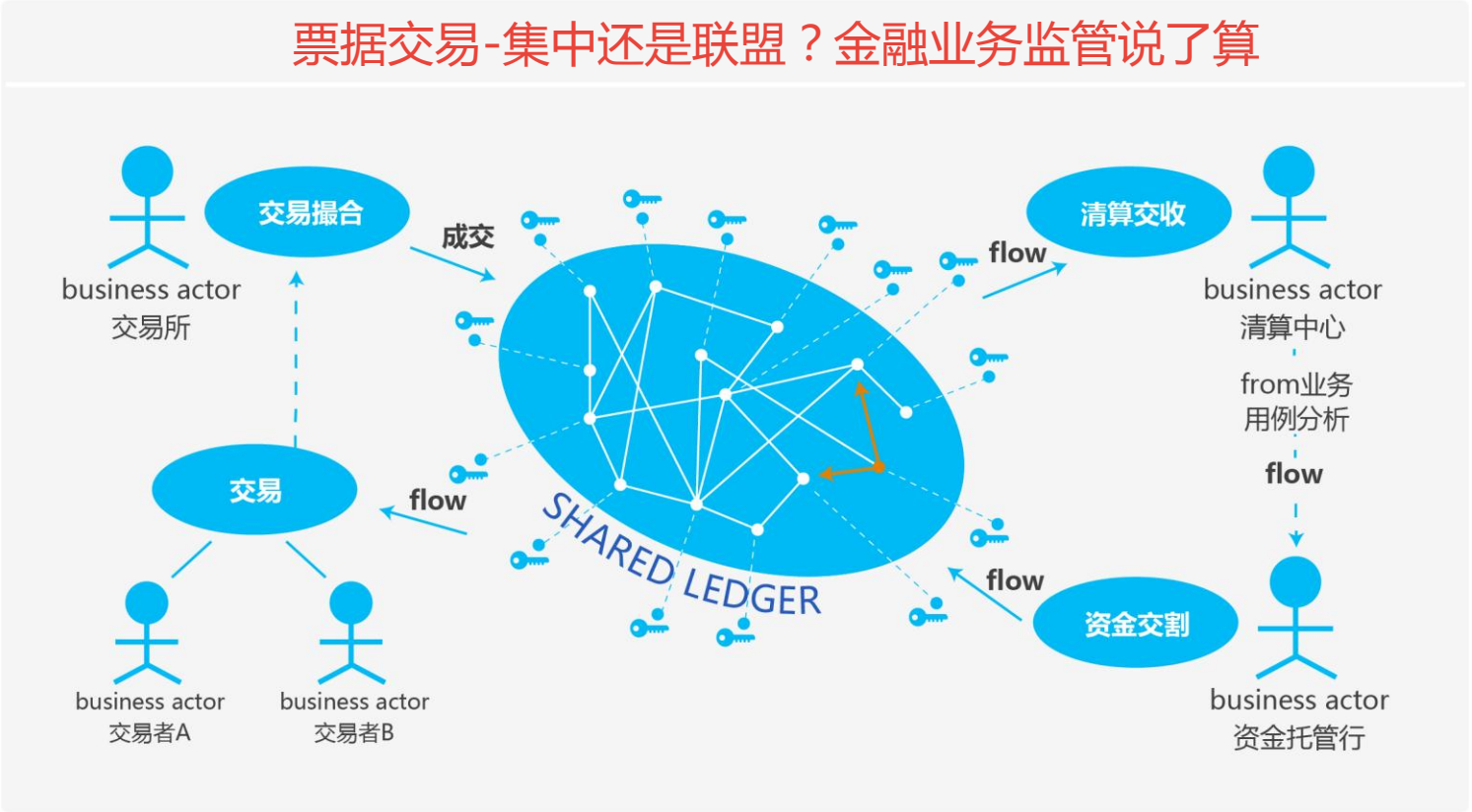
业务价值链中寻找合适应用场景

从“票据业务”剖析区块链应用面临的机会与挑战-背书转让场景



从简单“背书转让公证”理解“去中心、去信任”
防止链上链下一起作假，信任源追溯到对“承兑行签名”的信任

从“票据业务”剖析区块链应用面临的机会与挑战-票据交易场景



1. 从票据到各类同业业务、场外业务
2. 从交易后清结算环节到从C2C交易

区块链在金融领域的需要化解的技术问题（1）

部署模式	1.公有，全球可达，安全与监管问题 2.联盟，性能安全各种改造 3.私有，最受传统集中式技术方案挑战
成本性能	1.选择适当共识机制替代高成本的“挖矿” 2.解决现有区块链“单线程”处理瓶颈
开放安全	1.引入用户认证、权限机制 2.集成国密算法满足监管要求

区块链在金融领域的需要化解的技术问题（2）

万能的智能合约？

1. 合约技术标准
2. 商业冲突和业务流程的差异
3. 合约数据隐私、交易响应速度及吞吐量

最重要的：还是程序员在开发智能合约！

“不可篡改的区块链产生上不可篡改的BUG”

区块链在金融领域的需要化解的业务问题（1）

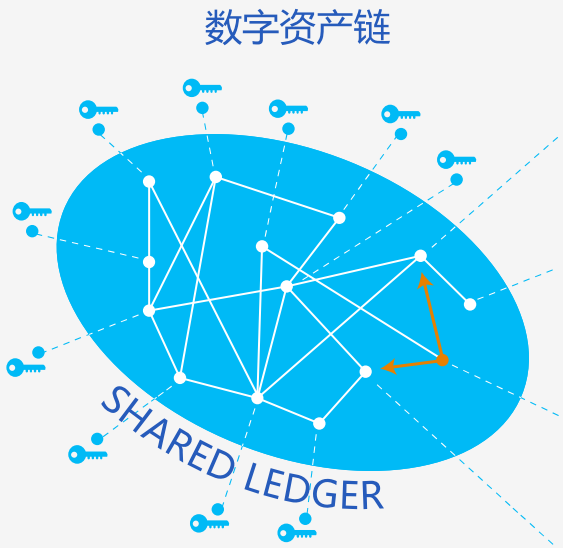
1.如何解决链上数字资产与实际金融资产的锚定对接？

2.代表区块链2.0的智能合约能自动处理金融资产吗？

是金融机构被去中心、去信任吗？

区块链在金融领域的需要化解的业务问题（2）

金融资产转让涉及资金清算



清算交割

代币承兑

清算结算机构

承兑机构

1. 可以发“结算代金券”吗？
2. 如果央行用区块链发行数字货币，世界将会怎样？

区块链不是银弹-寻找金融领域中的适用场景

着眼点

1. 分立系统的互联
2. 集中系统的痛点
3. 高风险的线下手工作业场景

限制点

1. 速度与容量限制（串行记账）
2. 最终一致性 (CAP定理)
3. 用户使用习惯（隐私、交易确定性）

01 异军突起的区块链技术

关于区块链架构师须知的那些事

02 区块链成为FinTech2.0的代表

区块链在金融应用实战中面临的挑战

03 区块链在其他领域的突破

仰望星空、脚踏实地

物联网与区块链

ADEPT物联网

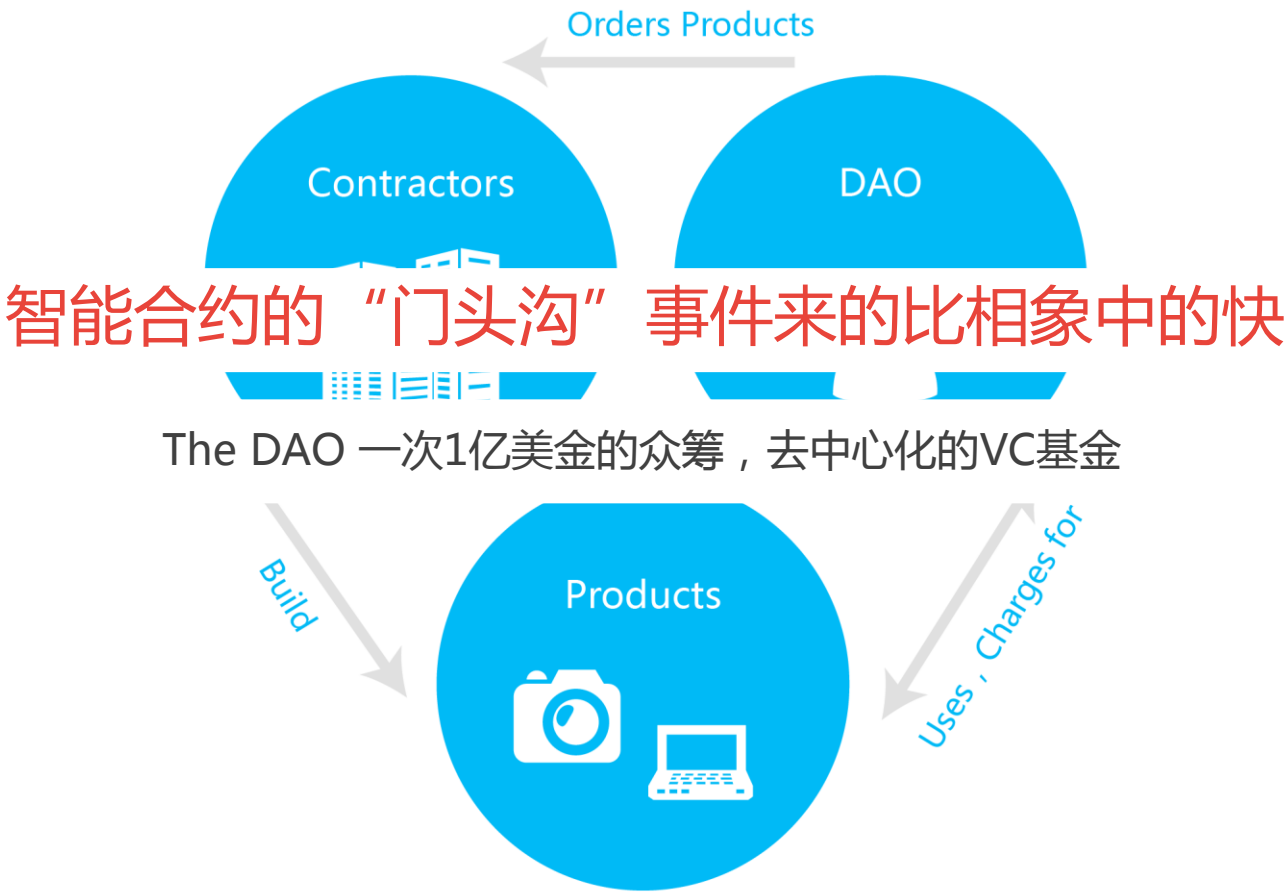
由IBM与三星联合打造，利用区块链技术来打造去中心化的物联网。ADEPT 的全称是“Autonomous Decentralized Peer-to-Peer Telemetry（去中心化的 p2p 自动遥测系统）”，它旨在为交易提供最优的安全保障。该系统基于三种协议：Blockchain（区块链）、BitTorrent（文件分享）、和 TeleHash（p2p 信息发送系统）

Slock区块锁，去中心化的共享经济

物理世界的各种“锁”与区块链上的“锁合约”绑定互动，安全高效的出租你的公寓，房子，自行车，汽车，洗衣机，剪草机等等，而合约的履行和支付都会被自动处理。

https://github.com/slockit/smart-contract/blob/master/BasicSlock.sol

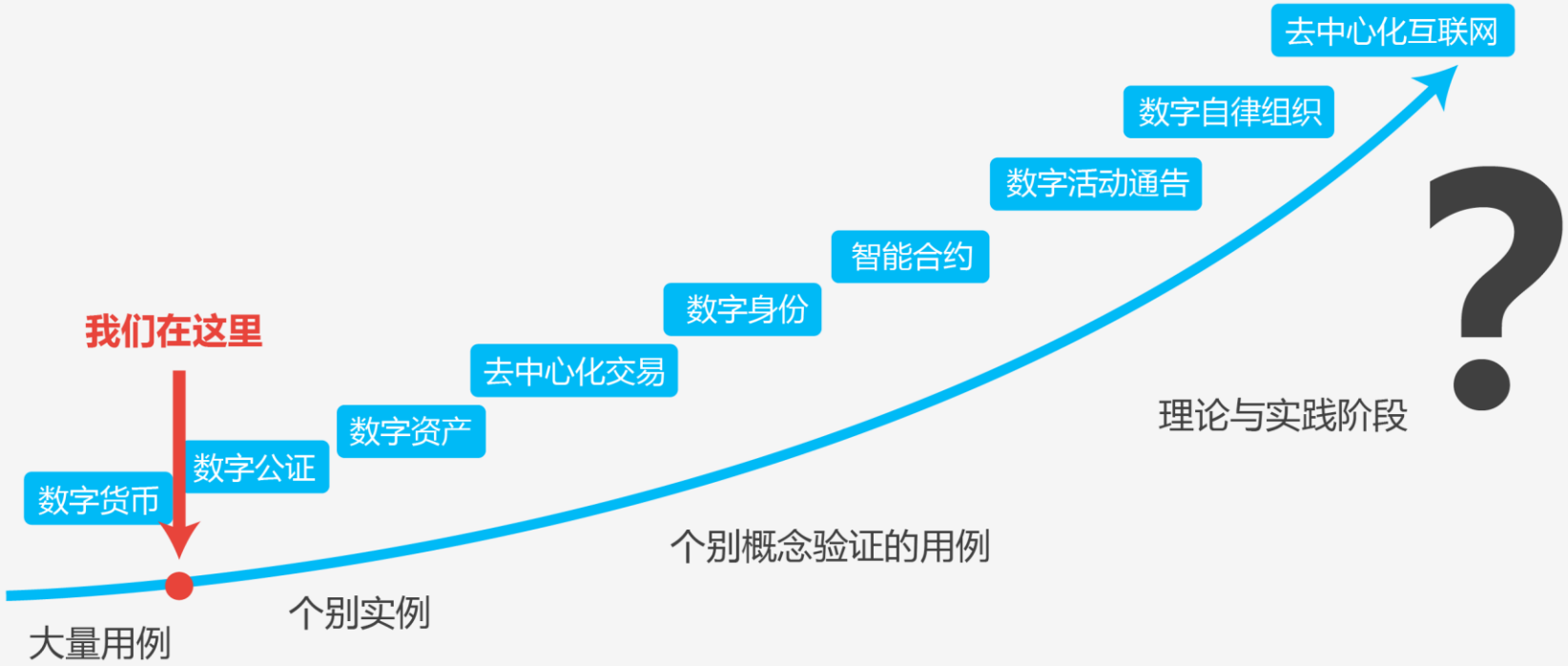
DAO（去中心自治组织）与区块链



没有人可以预测它的未来

区块链历程

区块链技术在快速演变，新的性能在不断结合创造更强有效的解决方案。



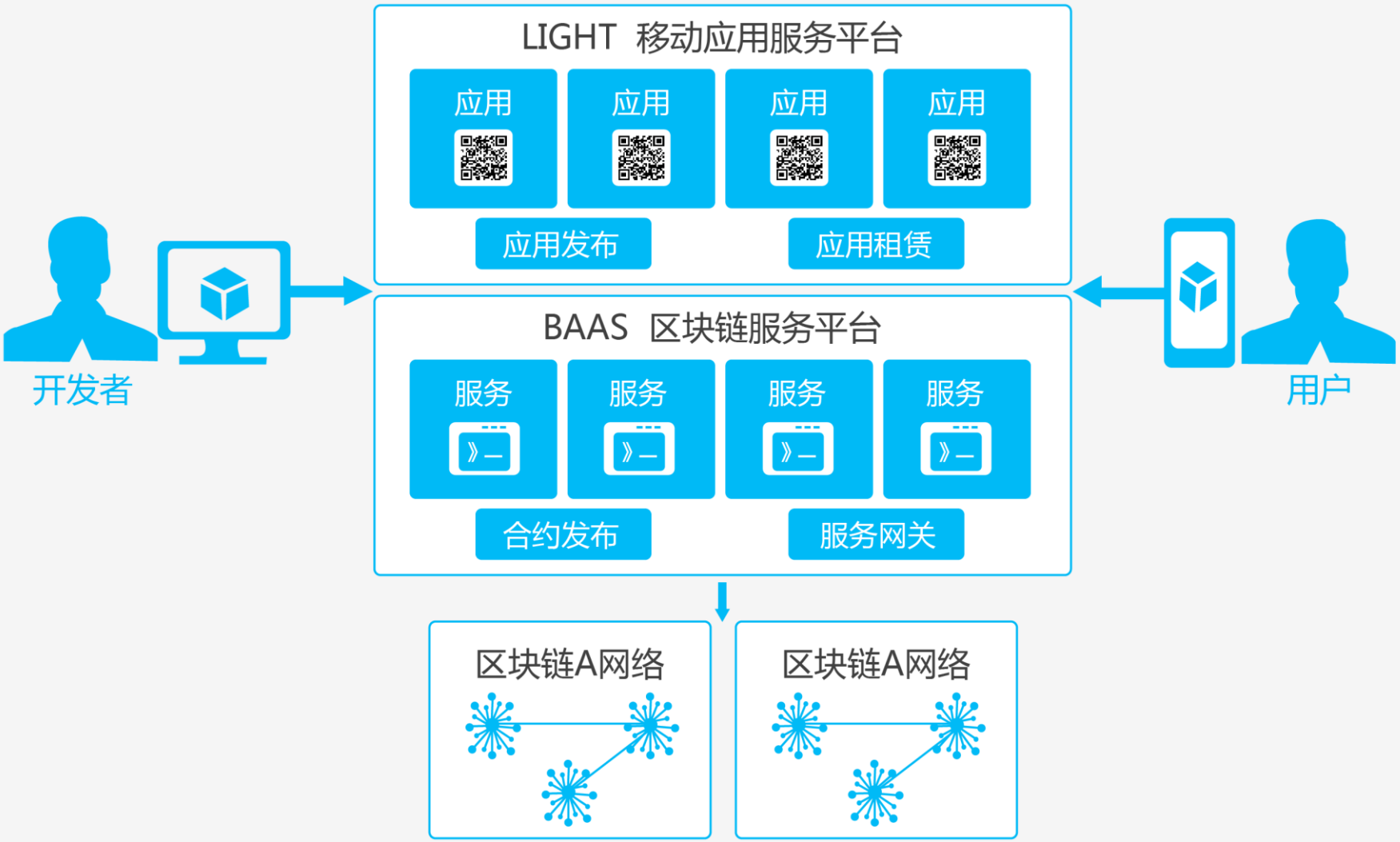
我们相信

我们相信

工程师定义未来：

Code Is Law!

与未来站在一起：恒生致力打造区块链应用中间件平台与开发者社区



THANKS!

了解更多恒生技术分享