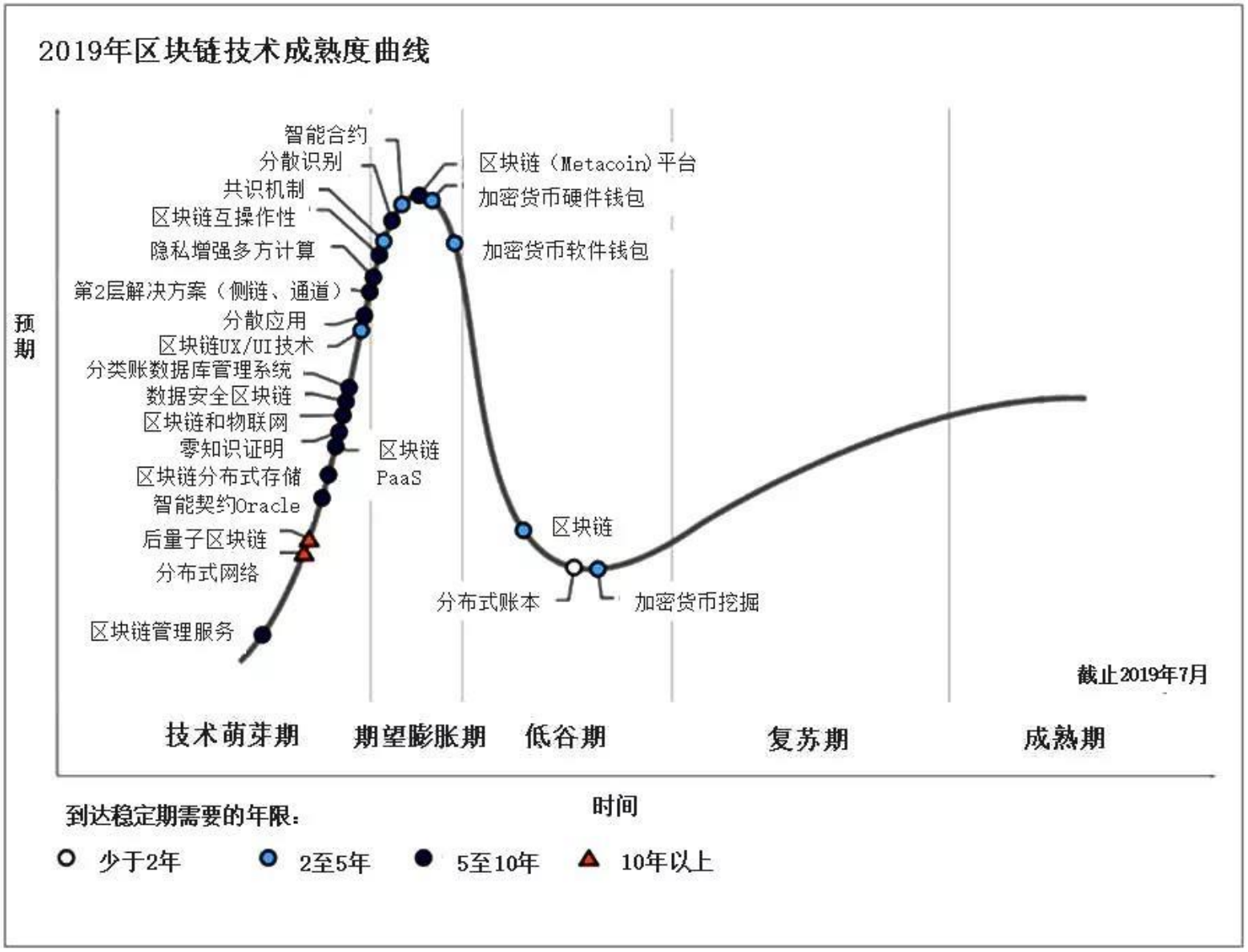
区块链与数字货币

浙江大学 杨小虎

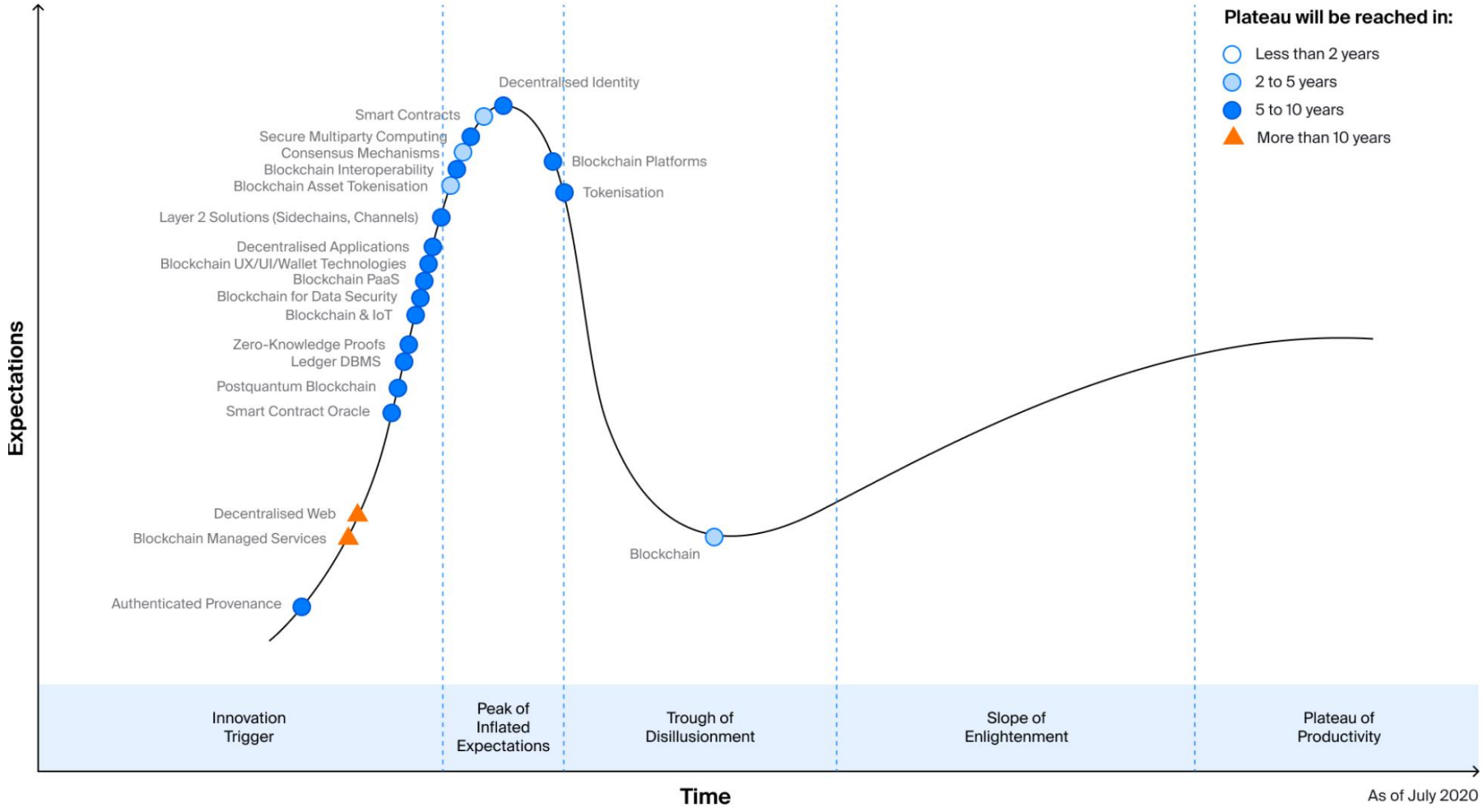
2021年1月19日

06 区块链技术发展趋势

区块链技术的发展


2019年区块链技术成熟度曲线
预期
智能合约
分散识别
共识机制
区块链互操作性
隐私增强多方计算
第2层解决方案（侧链、通道）
分散应用
区块链UX/UI技术
分类账数据库管理系统
数据安全区块链
区块链和物联网
零知识证明
区块链分布式存储
智能契约Oracle
后量子区块链
分布式网络
区块链管理服务
区块链PaaS
区块链（Metacoin）平台
加密货币硬件钱包
加密货币软件钱包
区块链
分布式账本
加密货币挖掘
截止2019年7月
技术萌芽期
期望膨胀期
低谷期
复苏期
成熟期
时间
到达稳定期需要的年限：
少于2年
2至5年
5至10年
10年以上

Hype Cycle for Blockchain Technologies, 2020



区块链技术存在的问题

- **性能问题**
  - 交易处理慢，吞吐量小
  - 链上数据存储量小，无法应对实际应用场景下的海量数据
- **安全问题**
  - 区块链底层协议可能存在缺陷
  - 智能合约引入安全漏洞，造成重大损失
- **隐私保护问题**
  - 信息隐匿性较低
- **链链互联问题**
  - 不同区块链之间数据难以互通
- **区块链软件开发生态问题**
  - 软件开发者社区的治理与发展
  - 软件代码的原创性
- **与其他信息技术集成的问题**
  - 链上链下数据协同问题
  - 物理世界与数字世界的对应问题：集成区块链和物联网用于产品溯源

区块链前沿技术

1. 共识机制
2. 新型存储
3. 智能合约与应用开发
4. 链链互联
5. 隐私保护
6. 区块链安全
7. 区块链监管
8. 区块链体系结构
9. “区块链+”

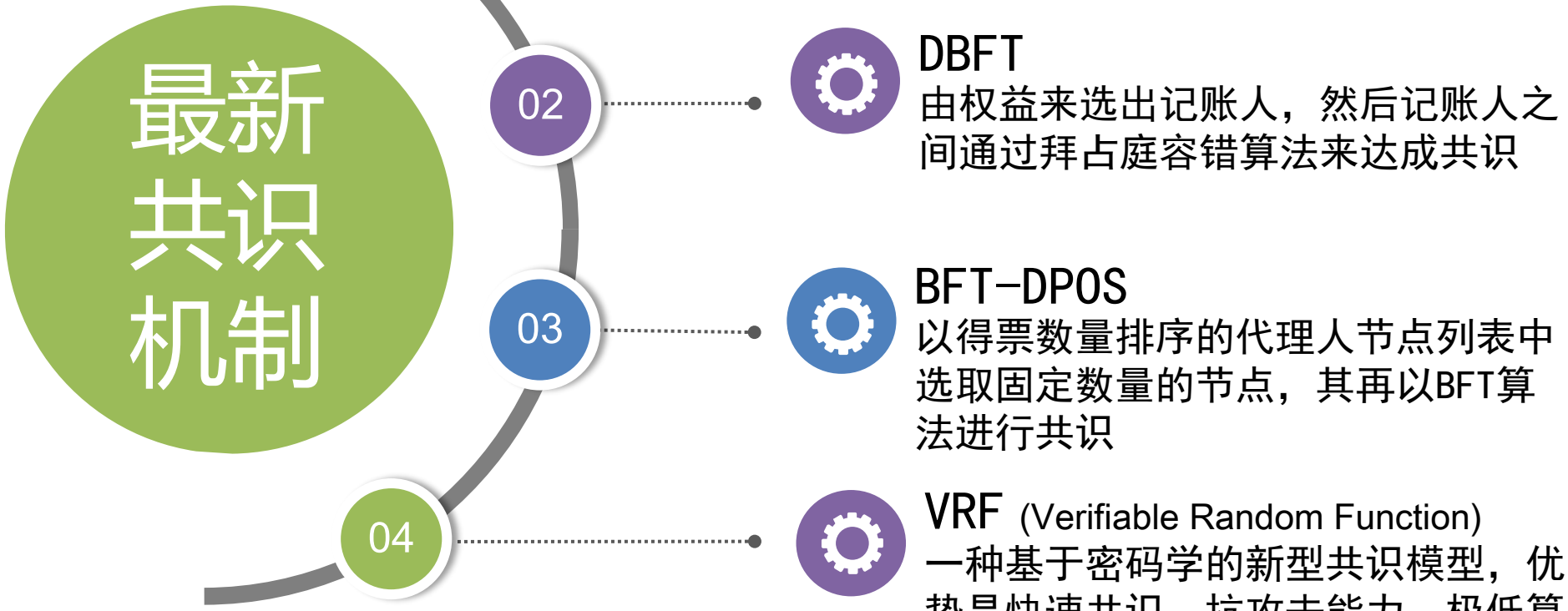
共识机制

- 共识机制解决了区块链如何在分布式场景下达成一致性的问题，是保障区块链系统长期稳定运行的关键技术。
- 常见共识算法

共识算法	工作原理	优缺点	应用
PoW	竞争性哈希计算来确定记账	优点：BFT，不可逆 缺点：消耗大量电能，记账成本高，记账速度慢	比特币，以太坊
PoS	根据资产的多寡来调整获得记账权的概率	优点：低能耗，速度快，不可逆 缺点：寡头优势，失去公平性	以太坊，Casper
DPoS	选中一小群节点作为代表进行PoS记账	优点：速度更快，更民主化 缺点：没有考虑账户重要性	Bitshare，EoS.io

共识机制

- 针对现有共识算法存在的一些弊端，近几年又提出了许多新的共识机制



共识机制

- **最新共识机制的对比**

共识机制	适用场景	性能效率	资源消耗	容错率
POS-POW混合共识	公链	低	中	50%
授权拜占庭容错（DBFT共识）	公链/联盟链	高	低	33%
BFT-DPOS混合共识	公链/联盟链	高	低	33%
VRF共识之Algorand算法	公链/联盟链	高	低	33%

隐私保护

- 区块链交易具有匿名特性，在一定程度上保护了个人的隐私
- 但由于区块链上的交易对全网是完全公开的，不法分子可获取用户所有的交易记录，通过大数据分析等方式最终确定用户的真实身份。此外，通过线下交易获得用户的钱包地址，也会导致区块链的匿名性不复存在。
- 为了加强区块链隐私保护的能力，业界普遍开始研究零知识证明、同态加密等算法

隐私保护

- **零知识证明**：证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的
  - 没有人可以假冒证明方，使这个证明成功
  - 证明过程完成后，验证方只获得了“证明方拥有这个知识”这条信息，而没有获得关于这个知识本身的任何一点信息。

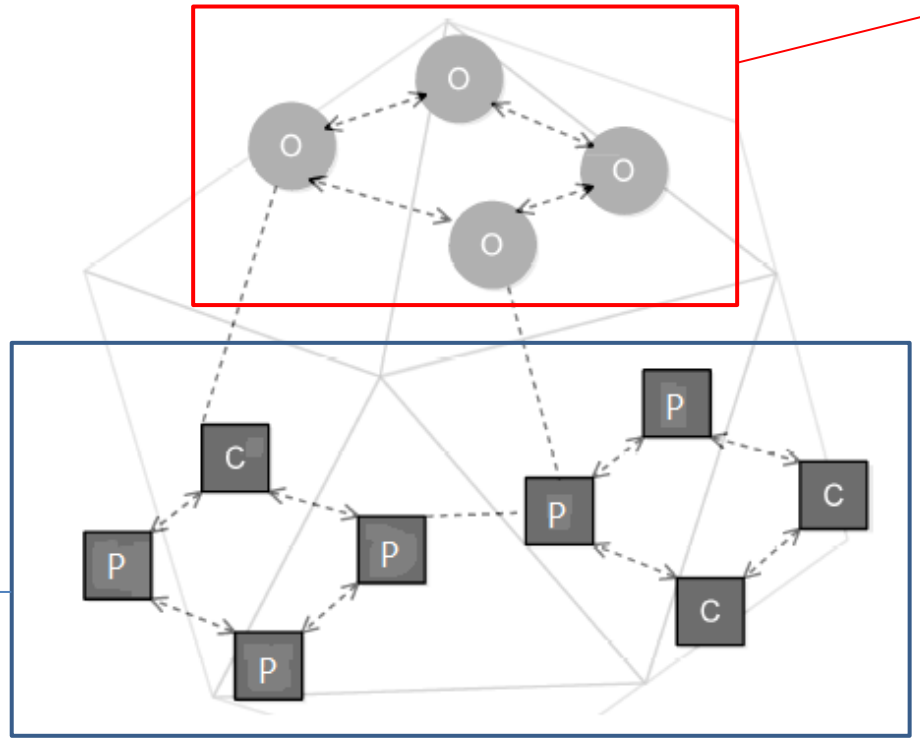
- **同态加密**：对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的
  - 对余额的操作仅在密文上进行，无法得知用户的余额以及转账的数额

侧链与跨链

- 目前，区块链之间处于完全独立的状态，如共识协议不兼容、数据账本不共享
- 为了实现区块链间的相互合作，打破区块链的信息孤岛，行业内目前采用侧链与跨链的策略
- 在具体实现策略上，联盟链与公有链有不同的方法

侧链与跨链—联盟链

- 联盟链的跨链一般为同构链跨链。联盟链相对公有链可以选择更强一致性的共识算法以提高跨链安全性，同时联盟链也拥有更高的可监管度，进一步增强了跨链安全性。其中比较典型的是Fabric的跨链技术。



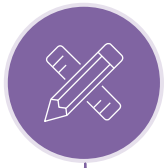
共识节点：承担与具体区块链无关的公共服务

服务节点：可以跨越多个账本，参与多个区块链事务，实现跨链

侧链与跨链—公有链

公证人模式

不关注所跨链的结构和共识特性，而是引入一个可信的第三方充当公证人，作为跨链操作的中介公证人模式代表性的平台是Ripple Interledger。



中继链模式

可以理解为中间人模式，其主要特点是中继链从平行链上采集数据，扮演着中间人的角色。中继链模式代表性的平台是Cosmos和PolkaDot

侧链模式

一种较为轻量的跨链技术，是通过智能合约在一个区块链网络中构建其他区块链的一个小型区块链，以简单支付验证（SPV）的方式来验证其他区块链上的交易，从而实现跨链资产转移。侧链技术中代表性是BTC Relay。

哈希锁定模式

在不同链之间设定相互操作的触发器，触发条件通常是一段私密数据的哈希值满足了预先设定的哈希值。哈希锁定模式代表性的技术是闪电网络

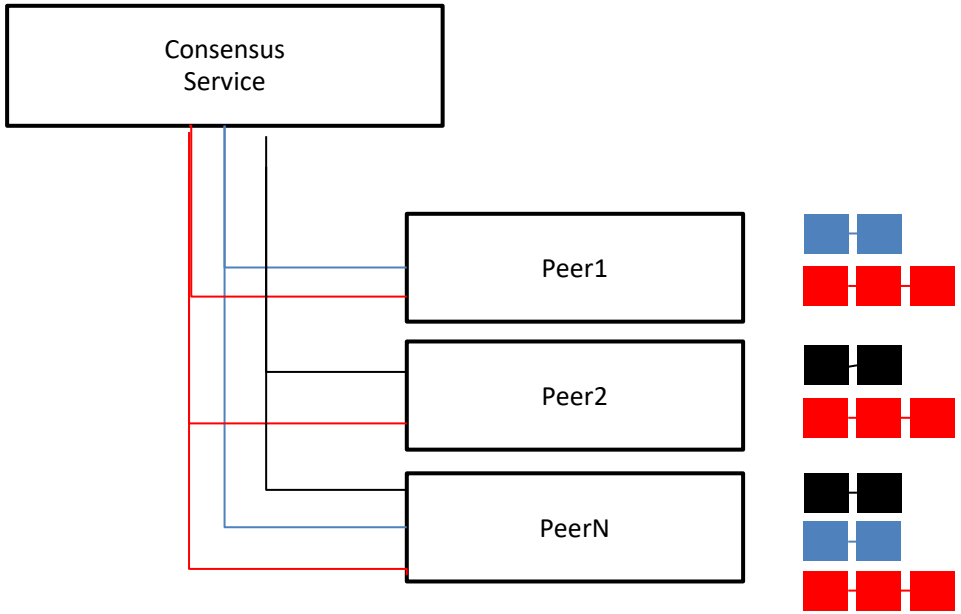
多链和多通道

- 现有区块链技术在单链架构下存在性能、容量、隐私、隔离性、扩展上的瓶颈。因此某些应用在单链上无法完整实现，需要在多链架构下的可扩展性、隔离性、高性能、互操作等特性的帮助下实现。

  Fabric定义了链、Peer、通道、共识服务的概念

  - 链——代表了账本和所对应的共识服务。
  - Peer——一个Peer可以拥有多个逻辑账本，并且可以参与多条链。
  - 通道——将Peer连接共识服务的虚拟通信方式。
  - 共识服务——可信的与链无关的公共服务。

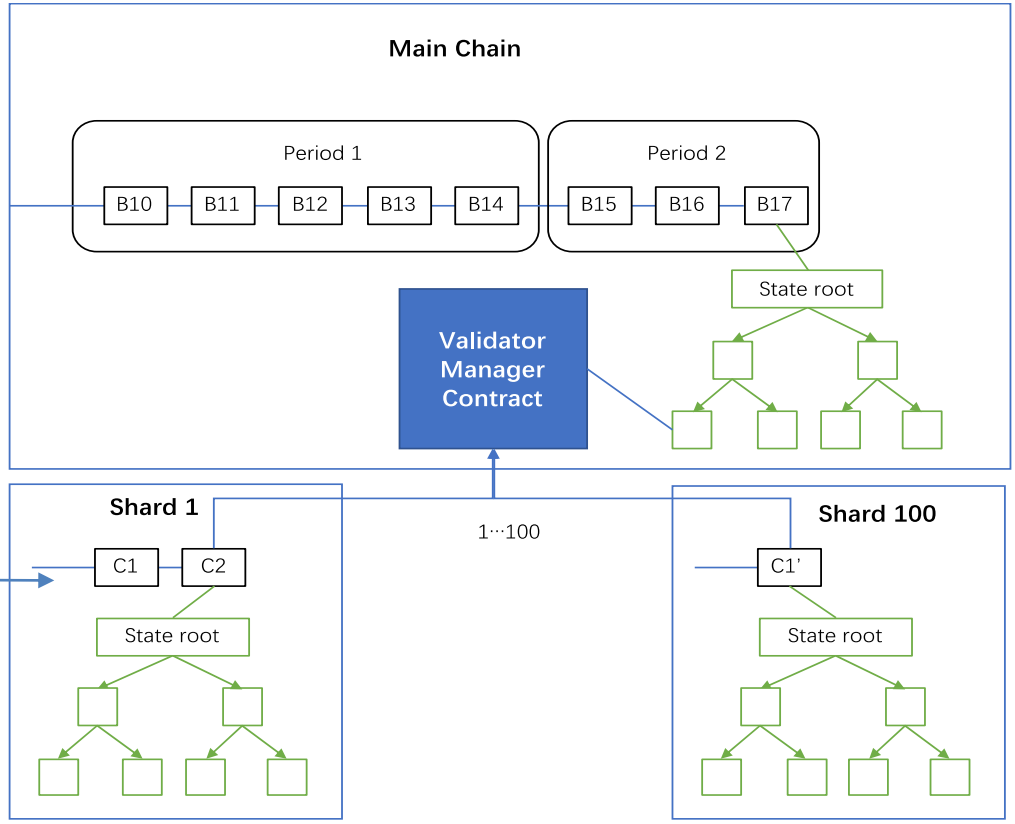
Fabric多链和多通道



- Peer1、Peer2和PeerN订阅了红色channel，并在它们之间管理对应的红色的ledger；
- Peer1和N订阅蓝色通道并管理蓝色ledger
- Peer2和N在黑色channel中并且管理黑色的ledger

分片技术

- 目的：解决扩展性问题，提高网络吞吐量
- 分片(shard)与分片处之间在业务上相互独立，在绝大多数情况下不需要相互通讯，每个分片都有自己的共识节点，使得计算得以真正并行化。



分片上的交易处于自己独立的空间中，分片验证人（共识节点）只需要验证他们所关注的分片

主链上运行VMC，按一定周期提名分片，被提名分片打包出块并向父链报备区块头信息

状态通道

- **状态通道也是以提高区块链执行效率为目的，其基本理念是通过将部分流程转移到链外执行来提高区块链的效率，且不会增加参与者的风险**

- **现在主要采用的技术是闪电网络和雷电网络**
- **闪电网络：**在无需与区块链进行互动的情况下，仍能安全地进行
  - **特点：**不存在交易对手的风险，无需信任对方以及第三方即可实现实时的、海量的交易网络

- **雷电网络：**类似于闪电网络，参与者在互相转账时，不需要通过以太坊主链交易确认，而是通过参与者之间创建状态通道在链下完成
  - **特点：**即时到账、低转账费用、可大规模扩展、隐私保护

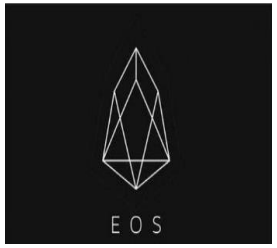
代码安全性

- The Dao事件：2016年6月17日以太坊最大众筹项目The Dao被攻击，攻击者组合了2个漏洞攻击，最终导致1200万以太币资产从The Dao资产池中分离

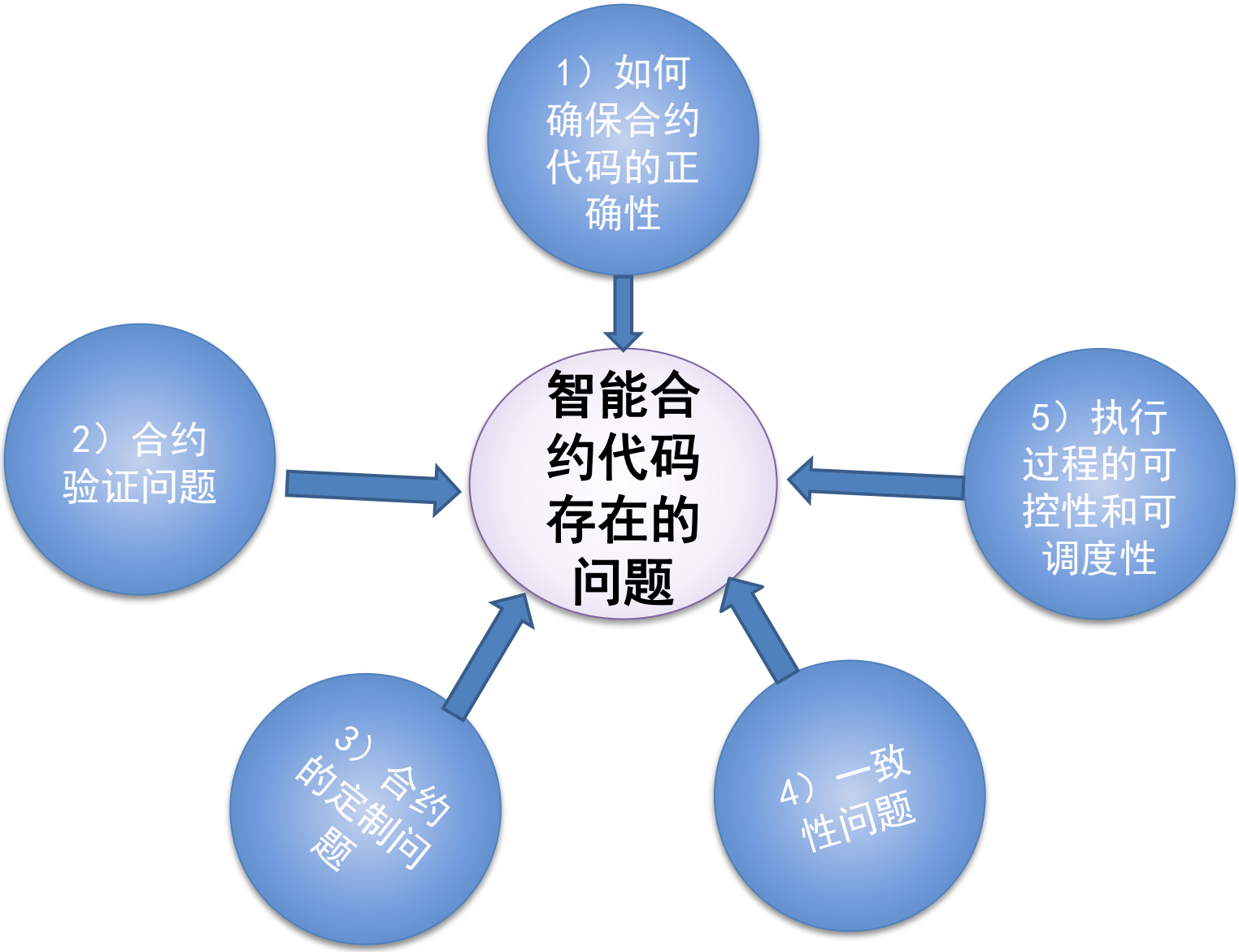
- 2018.4.22，有黑客利用以太坊 ERC-20智能合约中BatchOverFlow漏洞攻击BEC（美链的代币“美蜜”）智能合约，成功向两个地址转出了天量级别的 BEC代币，导致市场上海量BEC被抛售，此事使得当日BEC的价值几乎归零，64亿人民币瞬间蒸发。

- 2018.4.25，仅仅三天后，另一个智能合约SmartMesh(SMT)曝出漏洞，交易所表示，因SMT出现异常交易，各交易平台暂停SMT的充提和交易。

- 2018.5.29 ，360公司Vulcan（伏尔甘）团队发现了区块链平台EOS的一系列高危安全漏洞。经验证，其中部分漏洞可以在EOS节点上远程执行任意代码，即可以通过远程攻击，直接控制和接管EOS上运行的所有节点。

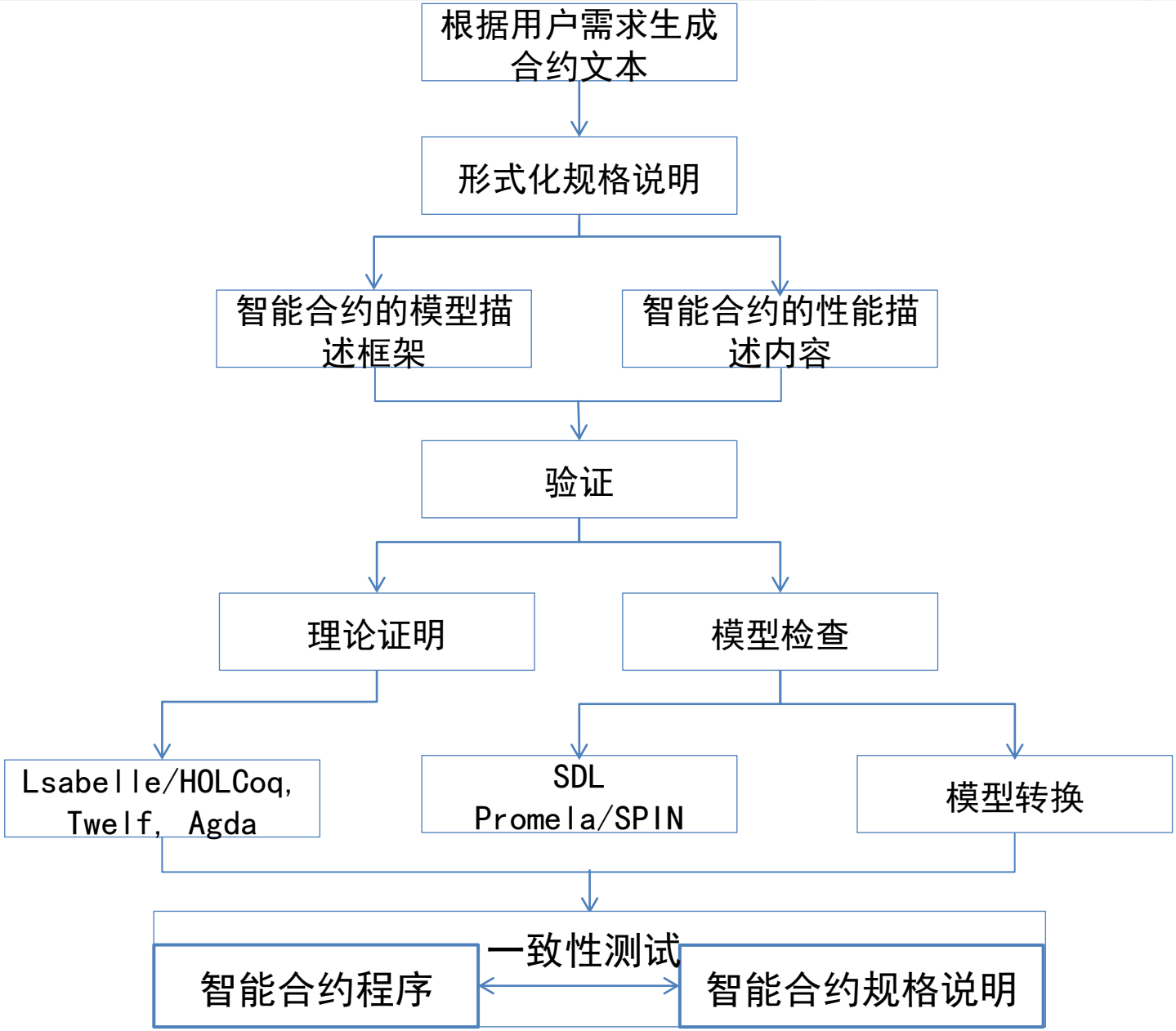


智能合约代码安全性


1）如何确保合约代码的正确性
2）合约验证问题
智能合约代码存在的问题
5）执行过程的可控性和可调度性
3）合约的定制问题
4）一致性问题

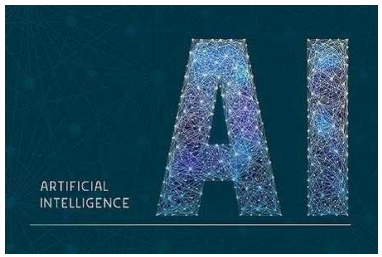
形式化验证方法

形式化方法应用框架



“区块链+”

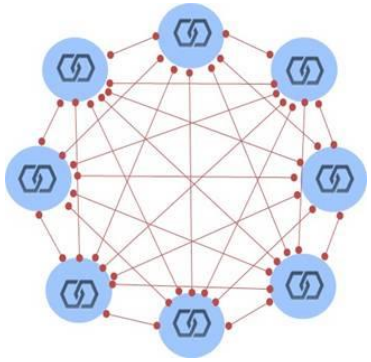
人工智能



实现智力与算力的共享与交易，形成开放的AI生态

形成数据线下采集与线上流转的可信闭环

物联网



云计算

降低区块链部署门槛，打造Baas平台

明确数据所有权，促进数据的开放共享

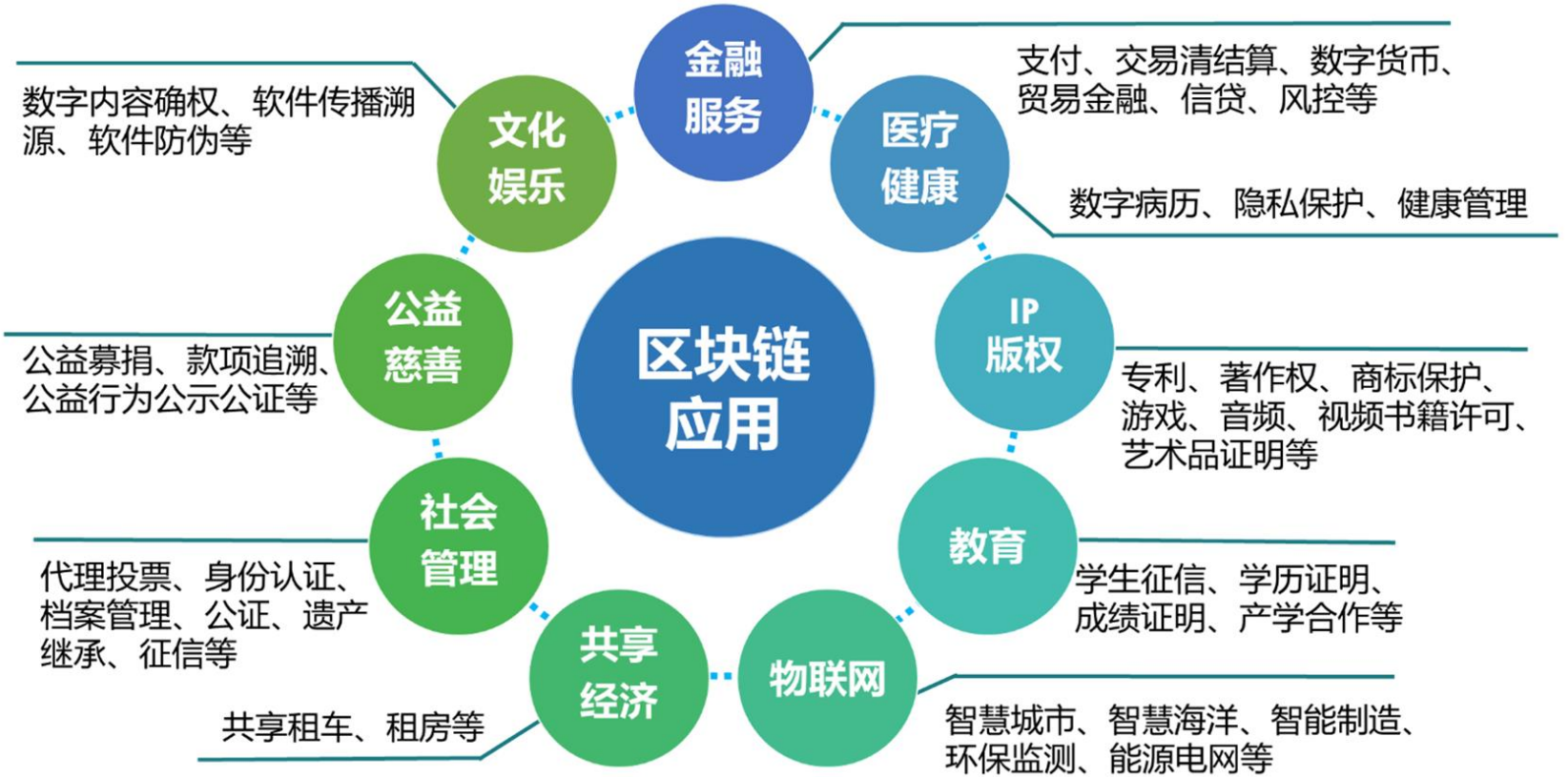
大数据

区块链软件开发生态

- 区块链代码的原创性
- 区块链软件的测试与验证
- 区块链软件开发的组织与管理
- 区块链开发者社区的治理与发展

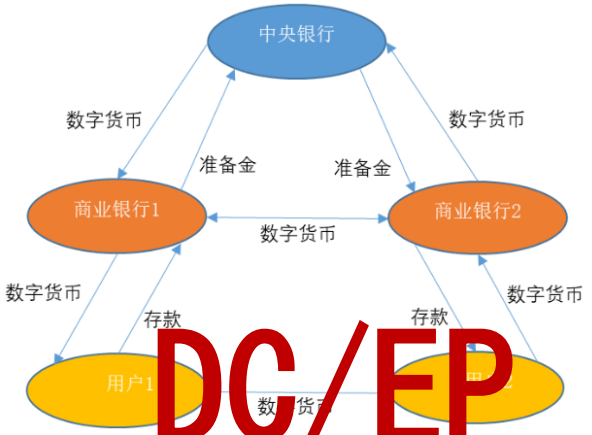
区块链应用场景

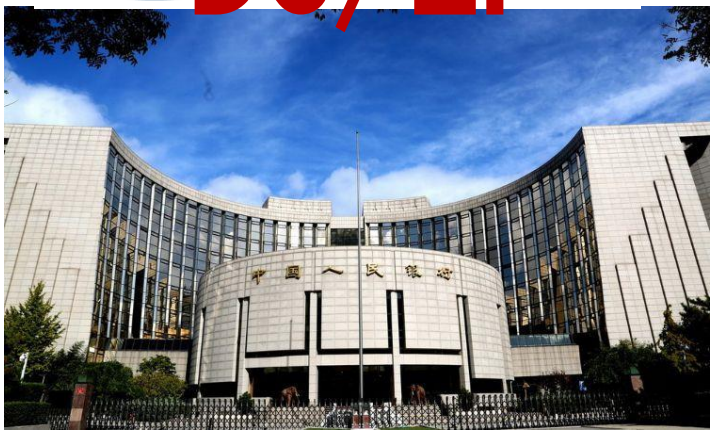
区块链的应用领域



区块链的应用：数字货币


MERCY CORPS
Women's World Banking
kiva
vodafone
BOOKING HOLDINGS
USV Union Square Ventures
ANDREESSEN HOROWITZ
Ribbit Capital
FARFETCH
THRIVE CAPITAL
iliad
VISA
mastercard
lyft
Uber
stripe
PayU
BREAKTHROUGH INITIATIVES
mercado pago
libra
ebay
coinbase
Spotify
PayPal
ANCHORAGE
CREATIVE DESTRUCTION LAB
xapo
BisonTrails
facebook
calibra


中央银行
数字货币
数字货币
准备金
准备金
商业银行1
商业银行2
数字货币
数字货币
数字货币
存款
存款
用户1
DC/EP



Libra

- Libra的使命：一种简单的全球化数字货币和为数十亿人服务的金融基础设施

Libra的要点：

- 一个稳定的跨国界的数字加密货币Libra：100%由一揽子法币和短期国债支持和锚定
- 智能合约编程语言MOVE
- 基于LibraBFT共识算法的可扩展许可型联盟链技术
- 开放式非营利自治组织Libra Association

Libra Association第一批成员（最终100家）

Libra锚定的法币

- 美元 50%
- 欧元 18%
- 日元 14%
- 英镑 11%
- 新加坡元 7%

Libra 2.0

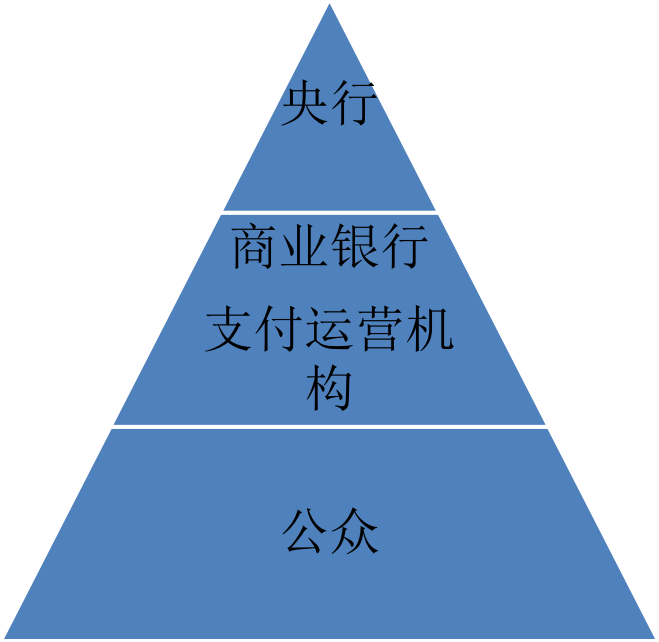
- 提出了Libra不只是锚定“一篮子货币”，也会推出锚定单一法币的产品，例如与美元锚定的LibraUSD、与欧元锚定的LibraEUR等。

- 删除了关于未来成为“非许可区块链”的描述，表明Libra彻底放弃转为公链的计划，只做联盟链。

- 新增大量拥抱监管的内容，表明无意挑战现有法币，尤其是美元的权威。

DC/EP投放及使用

DC/EP采用**双层运营**体系，即央行先将数字货币兑换给商业银行或其他运营机构，再经由它们将数字货币兑换给公众。



DC/EP不需要到商业银行开户，只需通过客户端，注册数字货币钱包即可使用。通过手机碰一碰或扫一扫，就能够**无网、跨银行、跨支付机构支付**。

- **DC/EP钱包**
  - ✓ 尚未公布
- **无网支付**
  - ✓ 像现金一样双离线支付
  - ✓ DC/EP是中心化账本模式，可以先记账再扣款
  - ✓ 基于安全考虑，双离线支付主要用于小额支付

DC/EP vs Libra

	DC/EP	Libra
用户群体	中国（目前）	全球
技术结构	是否运用区块链技术取决于商业银行的技术路线	结算采用联盟区块链技术
治理模式	双层运营体系+中心化管理模式	Libra协会作为治理机构
资产储备	以人民币作为资产储备，没有汇率风险，但有通胀风险。	以一篮子货币作为资产储备，可以兑换任何币种，会有汇率浮动。
运营机制	“双层投放”和“双层运营”机制，与现在人民币的投放方式和渠道基本一样。	借助区块链技术，联合多家机构，储备法币和政府债券。

DC/EP vs 第三方移动支付

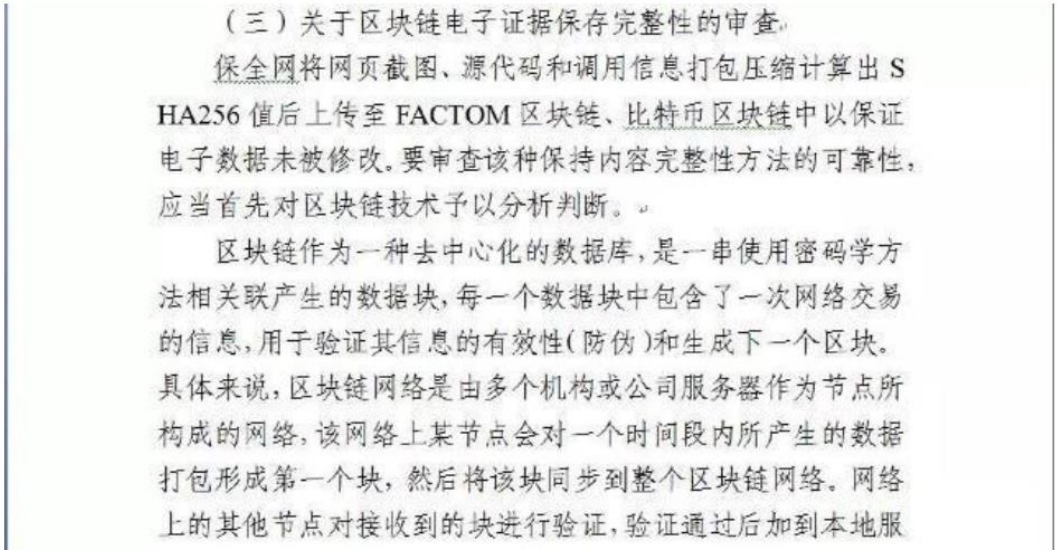
DC/EP	移动支付
法定数字货币	微信和支付宝可能成为DC/EP节点和DC/EP钱包
DC/EP可以无网且跨App使用	必须联网且存在平台支付壁垒
法律地位和安全性更高	存在被盗等安全风险

全国首例：杭州互联网法院认可区块链存证

Bianews
百家号 | 06-28 17:30

Bianews 6月28日消息，据公众号“网络法实务圈”报道，2018年6月28日上午10时，全国首例以区块链为存证的案件在杭州互联网法院一审宣判，法院支持了原告采用区块链作为存证方式，并认定了对应的侵权事实。

在判决书中，杭州互联网法院肯定了区块链作为判定侵权与否的有效存证的资格和效力，提及区块链的部分节选如下：

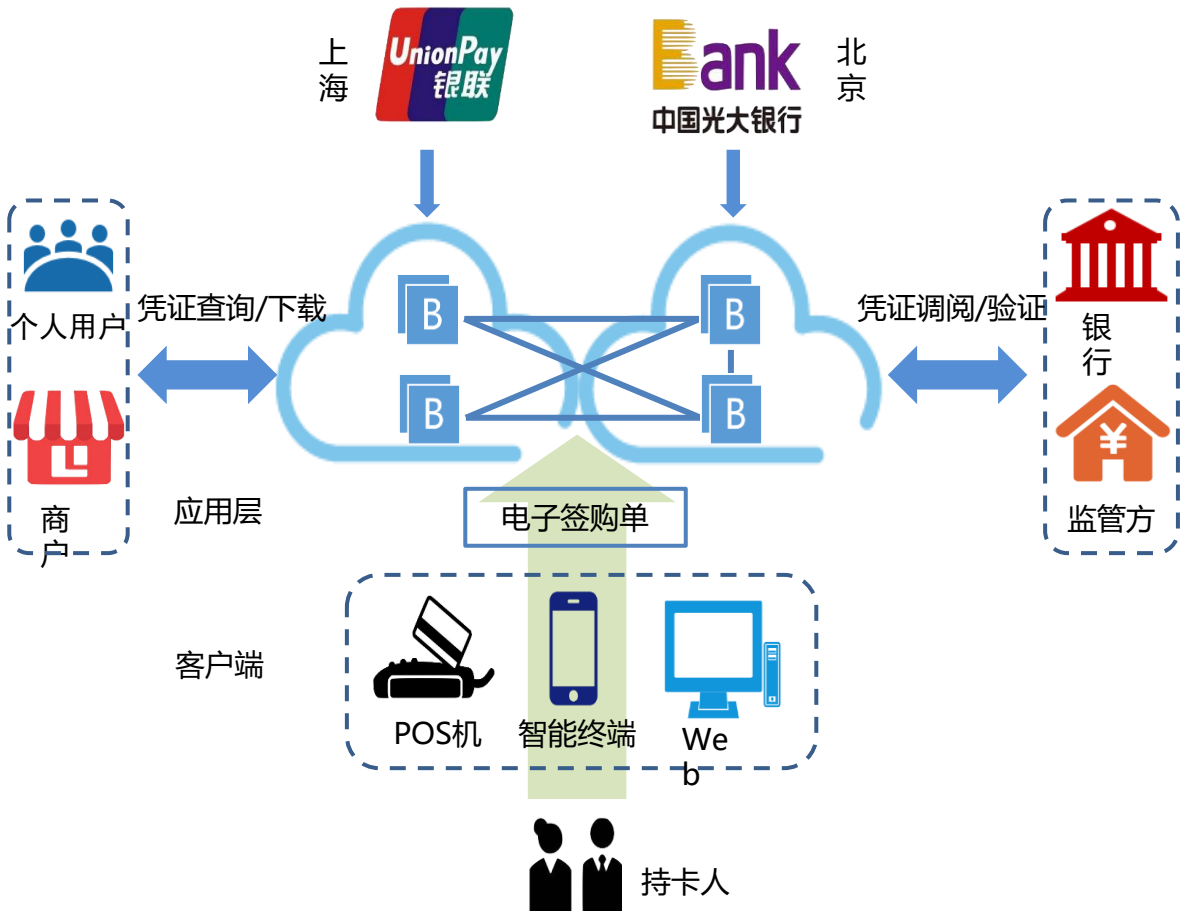


（三）关于区块链电子证据保存完整性的审查。

保全网将网页截图、源代码和调用信息打包压缩计算出SHA256值后上传至FACTOM区块链、比特币区块链中以保证电子数据未被修改。要审查该种保持内容完整性方法的可靠性，应当首先对区块链技术予以分析判断。。

区块链作为一种去中心化的数据库，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。具体来说，区块链网络是由多个机构或公司服务器作为节点所构成的网络，该网络上某节点会对一个时间段内所产生的数据打包形成第一个块，然后将该块同步到整个区块链网络。网络上的其他节点对接收到的块进行验证，验证通过后加到本地服

应用场景：数字信息存证



解决痛点

1 银行内部凭证管理提升

- 凭证不可篡改和伪造
- 易监管
- 可溯源

2 凭证信息跨机构、跨地域共享

- 业务协作
- 形成可信信息流
- 易拓展

3 银行业务外延（监管、司法机构等）

- 电子合约
- 发票抵押查询

4 与传统系统对比

- 每天减少120万元小票纸成本
- 扩展业务如发票抵押查询，缩短验证时间缩短到秒级，基本杜绝重复质押的情况

深圳国税联手腾讯推出区块链数字发票

e公司
百家号 | 05-24 13:17

e公司讯，5月24日，深圳市国家税务局与腾讯公司共同召开“智税”创新实验室成立签约仪式，在实验室的研究基础上，双方将推出国内首个基于区块链的数字发票解决方案，探索新型发票生态，希望每一张发票都可以做到可查、可验、可信、可追溯，并利用区块链技术对发票流转全过程进行管理，让发票数据全场景流通成为现实。

区块链在金融领域的应用场景

- 数字货币
- 支付/转账
- 数字票据
- 证券交易
- 保险
- 供应链金融
- 资产通证化

应用场景：跨境转账和支付

瑞波（Ripple），基于区块链技术的全球转账和支付网络。

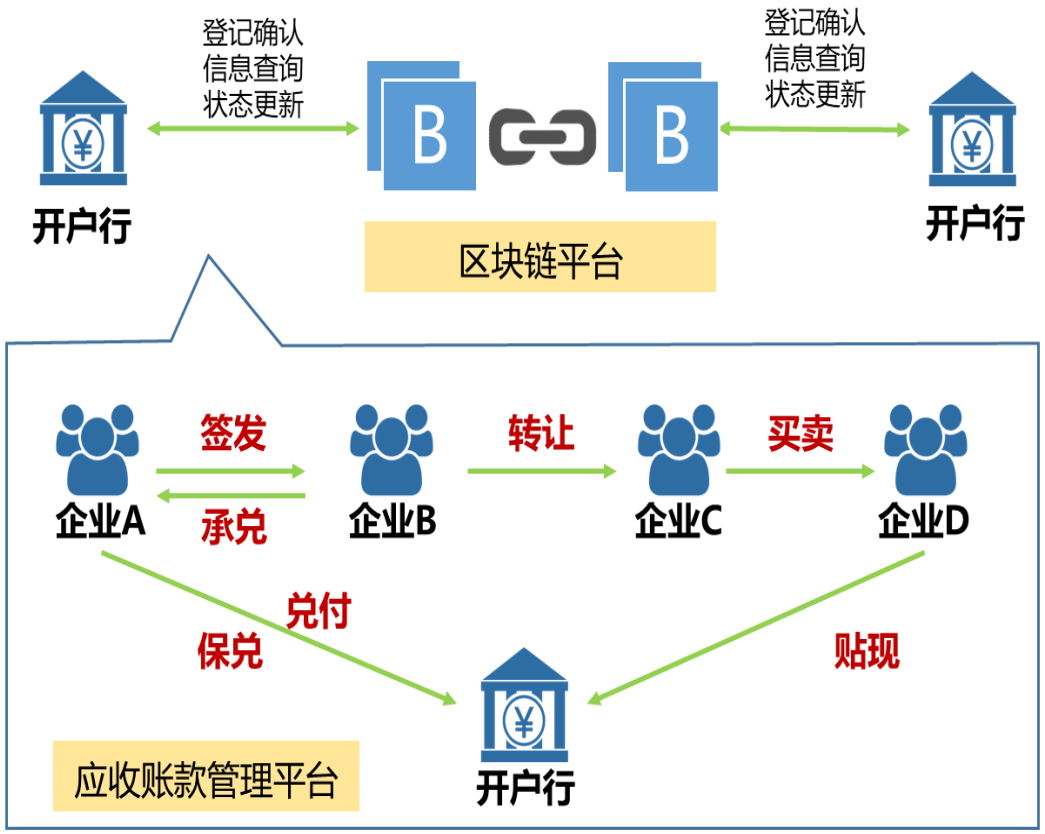
交易确认在几秒以内完成，交易费用几乎是零，没有所谓的跨行异地以及跨国支付费用。

AlipayHK开通区块链跨境支付通道

来源：玩币族　2018-06-27 15:59:51

蚂蚁金服是中国电子商务巨头阿里巴巴(Alibaba)旗下的支付子公司，它已经为消费者推出了一个基于区块链的跨境结算服务通道。

应用场景：供应链金融



解决痛点

1 应收账款可信交易和管理

- 电子签名交易
- 不可抵赖
- 智能合约权限状态控制

2 交易全程追溯

- 时间戳记录生命周期
- 资金流、信息流可查询

3 跨机构互通互利

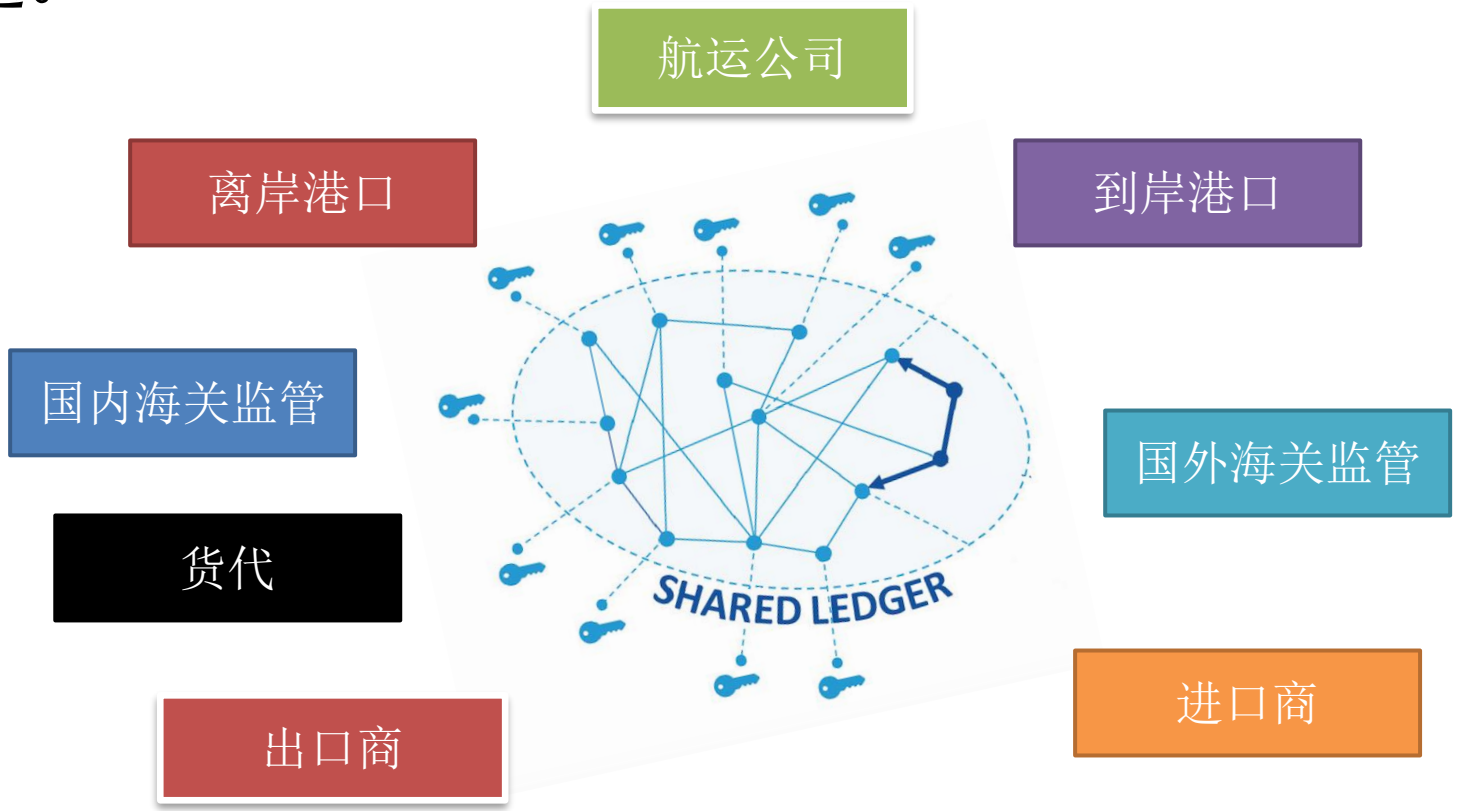
- 数字资产存储交易
- 多金融生态圈

4 与传统系统对比

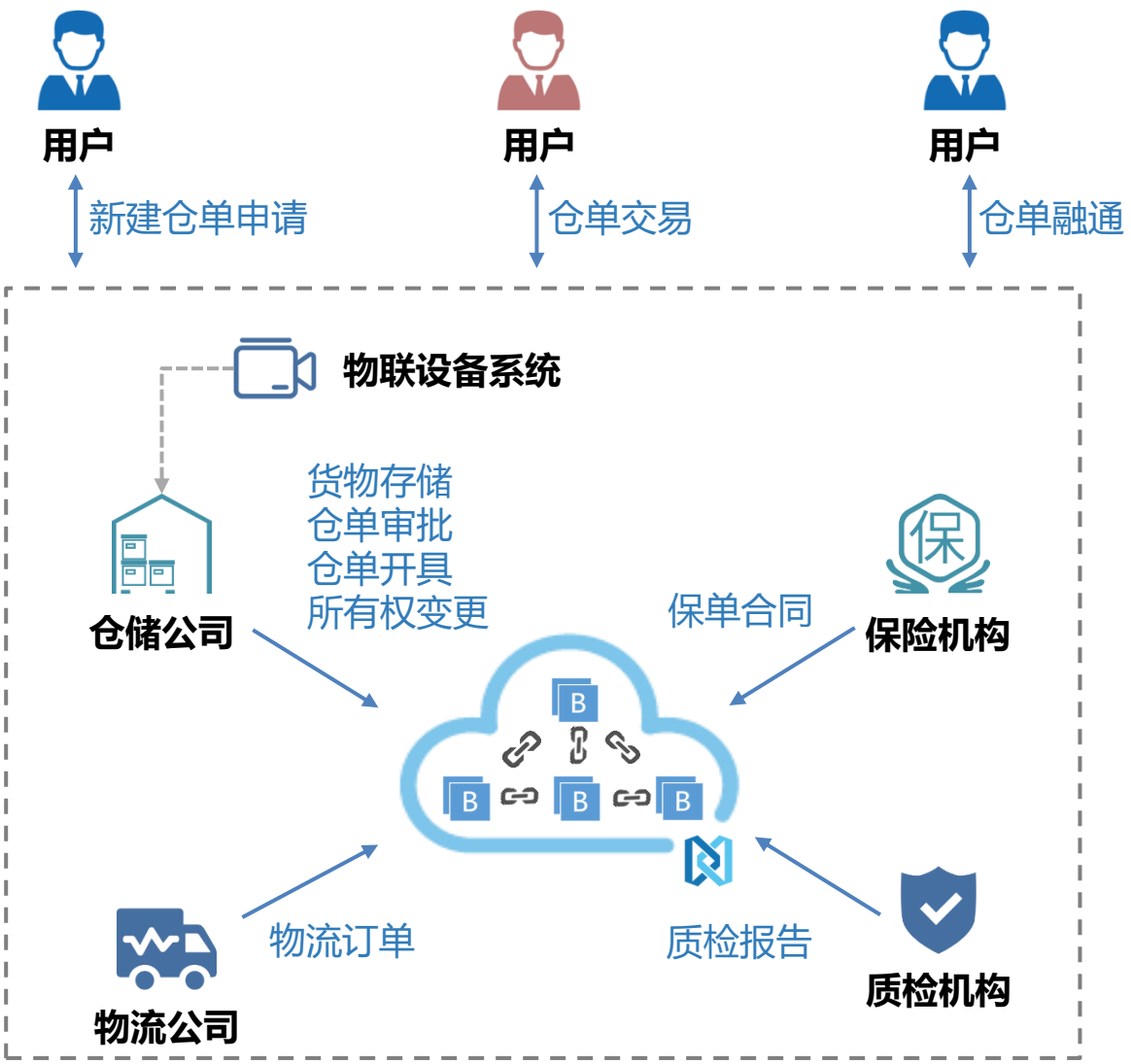
- 解决企业三角债问题
- 通过信用流通，提高企业资金使用效率
- 银行获取保兑费用与更高的业务流量及更大的企业客户群

应用场景：国际贸易

- 通过区块链网络，提货单/信用证等单据可以通过电子形式数字签名后直接发给相关方，防止凭据伪造和丢失的问题。



应用场景：电子仓单


用户
用户
用户
新建仓单申请
仓单交易
仓单融通
物联设备系统
货物存储
仓单审批
仓单开具
所有权变更
仓储公司
保单合同
保险机构
物流订单
质检报告
物流公司
质检机构

基于区块链的数字版权保护

基于区块链的公益项目

- 公开透明
- 不可篡改
- 可追溯

基于区块链的防伪溯源

- 优势：上链的数据具有可信、不可篡改、可追溯等特性
- 问题：如何解决物理世界中的实体与数字世界中的对象的唯一性对应
  - 物联网
  - Ditigal twin

Digital Twin

- Digital Twin数字孪生：是充分利用物理模型、传感器更新、运行历史等数据，集成多学科、多物理量、多尺度、多概率的仿真过程，在数字空间中完成映射，从而反映相对应物理实体的全生命周期过程。
- 最早是由美国空军研究院提出，在数字空间建立真实飞机的模型，并通过传感器实现与飞机真实状态完全同步。
- 是智能制造系统的基础。
- 为区块链应用时连接物理世界和数字世界提供桥梁。

区块链与共享经济

- 打通共享经济领域的各个行业（包括不限于共享充电宝、共享单车、共享租房、共享汽车、共享雨伞等）

区块链就像20年前的互联网和电子商务，前景是美好的，但面临很多挑战和困难

谢谢！