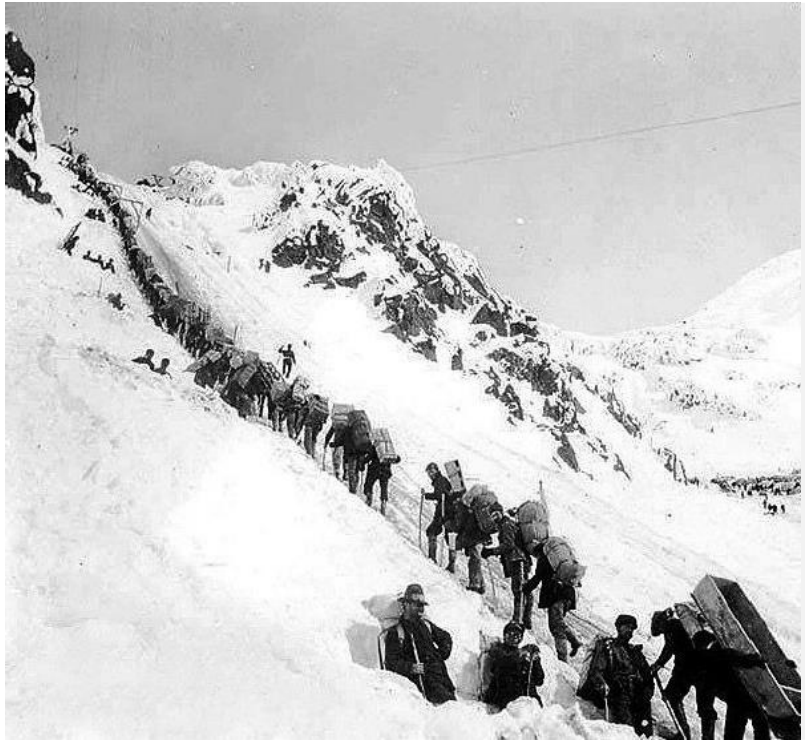
区块链思想、技术及应用场景

范磊

上海交通大学

区块链的诞生



一般等价物

原始人使用以物易物的方式交换物品，并使用贝壳等作为一般等价物

黄金货币

黄金等贵金属因为开采困难，不容易形成通货膨胀因而适合作为货币

纸质货币

由国家金融机构发行并由国家信用担保的货币

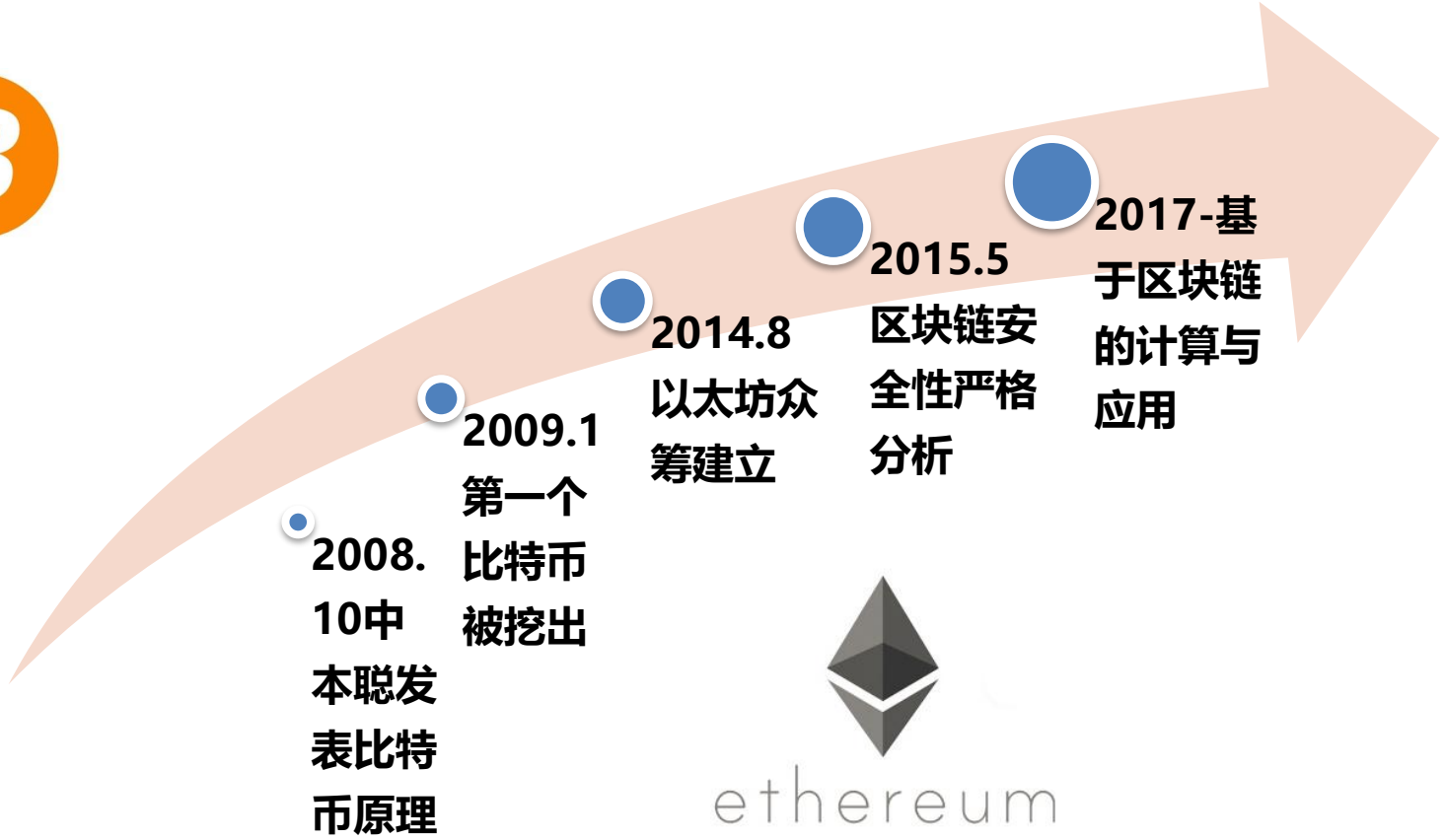
电子货币

由计算机系统管理、并完成交易流程的货币

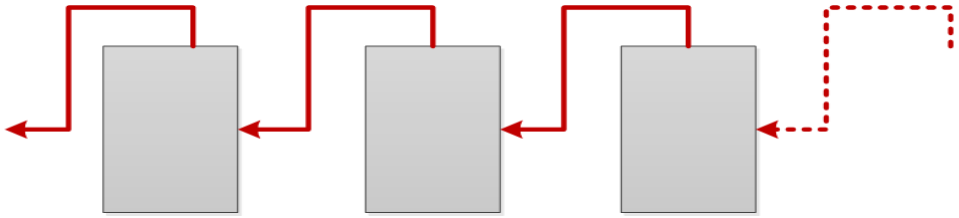
区块链是作为去中心化数字货币的技术基础诞生的

区块链的直观解释

区块链技术的发展历史


2008.10中本聪发表比特币原理
2009.1第一个比特币被挖出
2014.8以太坊众筹建立
2015.5区块链安全性严格分析
2017-基于区块链的计算与应用
ethereum

什么是区块链



- 从名字定义理解区块链：一种链式数据打包存储的数据结构
- 从数字货币角度理解区块链：比特币等数字货币的基础设施
- 从数据存储的角度理解区块链：高冗余的数据存储系统
- 从分布式计算角度理解区块链：去中心化的分布式计算平台

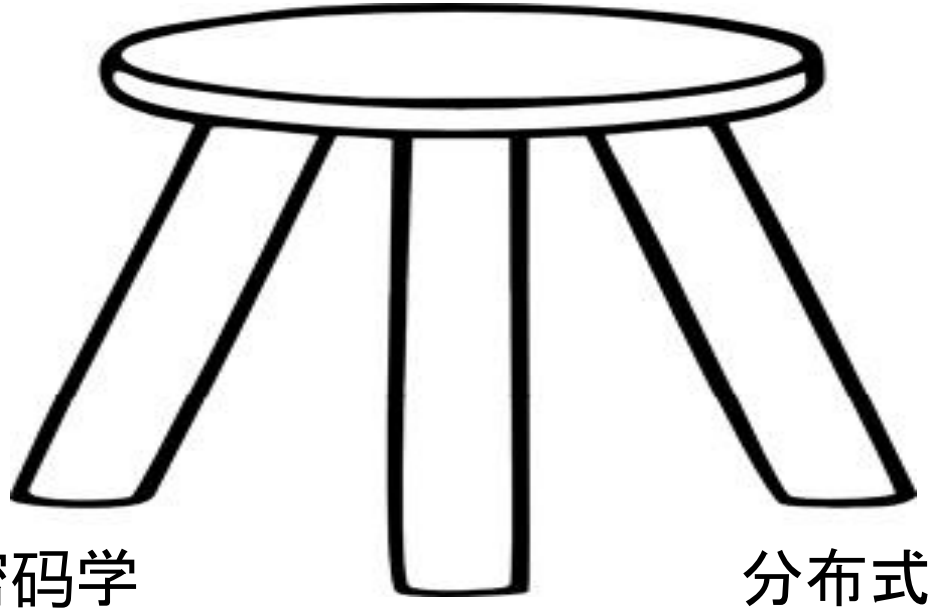
什么情况下需要使用区块链

区块链的基本应用原则:

- 需要多方参与的应用场景
- 在多方的参与者中难以选择一个可信方

如果存在可信方，无需使用区块链，区块链相对集中式系统通常具有更低的效率

区块链的理论基础

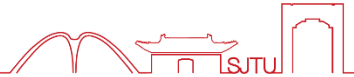


密码学

分布式计算

经济学

区块链研究什么内容



Layer 3: **user facing tools** (cloud servers)

Layer 2: **applications** (DAPPs, smart contracts)

Layer 1.5: **compute layer** (blockchain computer)

Layer 1: **consensus layer**

Layer 0: **network layer**

Layer 0 网络层

去中心化的P2P通信网络:

- **模拟广播信道**: 通过P2P网络实现数据的广播（ Propagation ）
- **数据打包**: 将交易数据封装为标准数据区块
- **数据分片:** 将数据切分为固定大小
- **数据存储**: 实现数据的冗余存储

Layer 0: network layer

Layer 1 共识层

公开可验证的单调增加的数据结构:

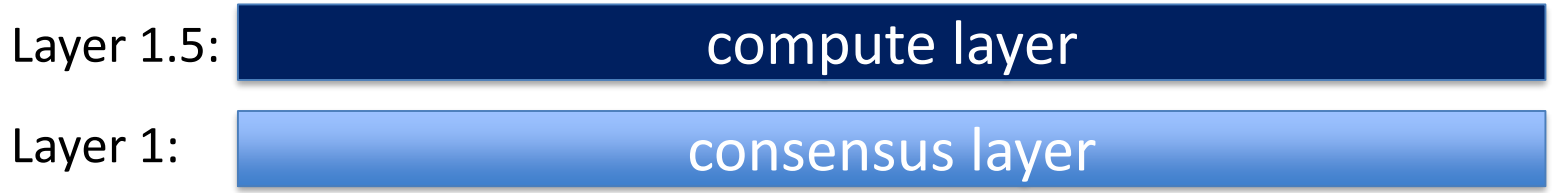
- **持久性**: 一旦数据被确认，永远不能删除或修改
- **一致性**: 所有的诚实参与者可以得到完全相同的数据
- **活　　性**: 系统始终可增加新的数据
- **安全性**: 诚实用户始终可以为系统增加新数据

Layer 1: consensus layer

Layer 1.5：计算层

区块链共识节点支持去中心化应用的计算逻辑

- 支持通用计算：支持图灵完备的高级程序语言
- 逻辑公开：所有的执行代码是公开可审计的
- 全局可验证：所有执行结果可被其他节点验证
- 安全特性：提供隐私保护、结果认证等安全特性



Layer 2: 去中心化应用(DAPPS)

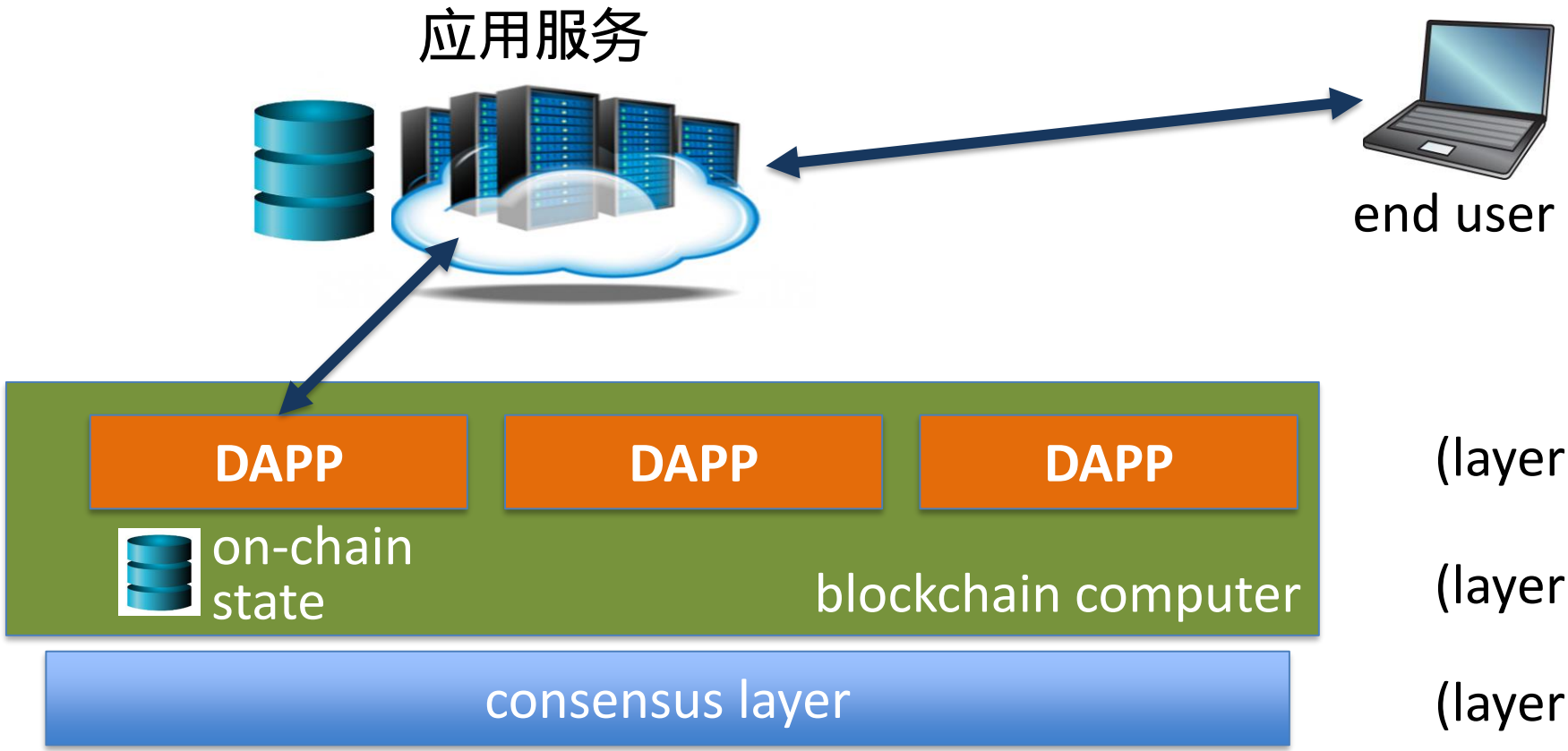
Run on blockchain computer

Layer 2: **applications** (DAPPs, smart contracts)

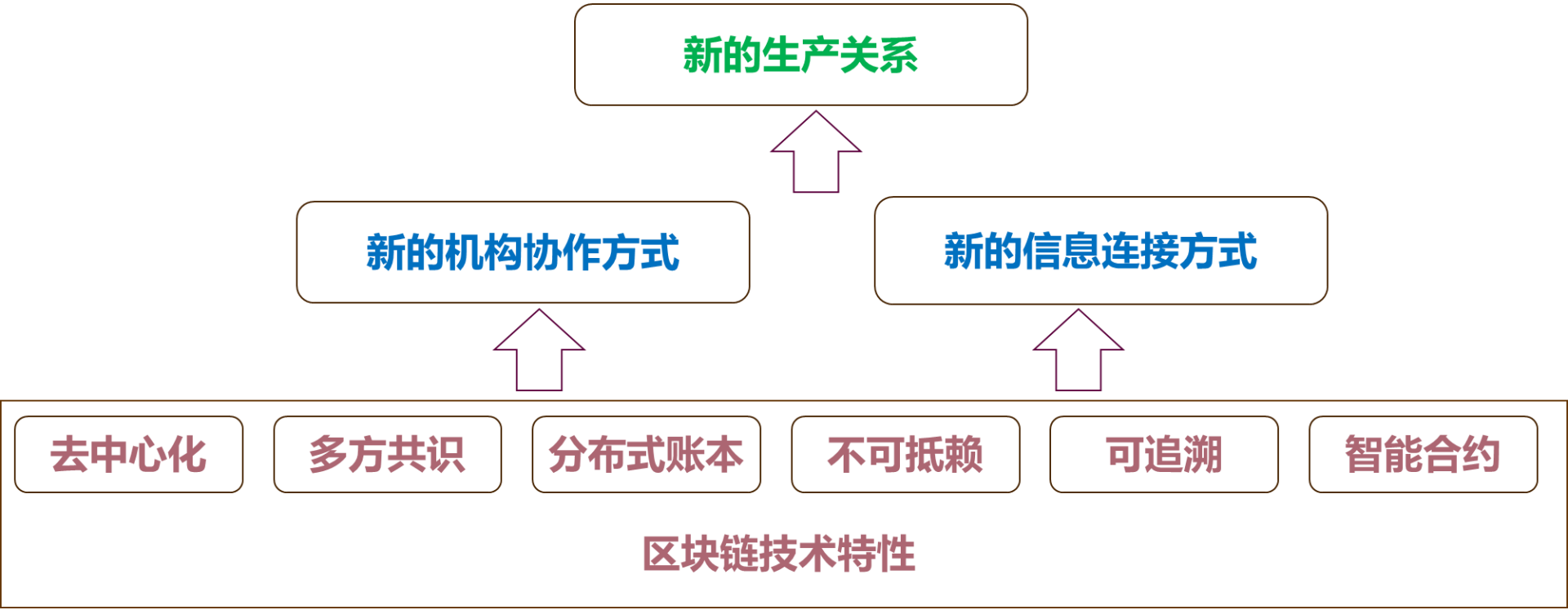
Layer 1.5: blockchain computer

Layer 1: consensus layer

Layer 3：用户访问层



区块链的核心价值


新的生产关系
新的机构协作方式
新的信息连接方式
去中心化
多方共识
分布式账本
不可抵赖
可追溯
智能合约
区块链技术特性

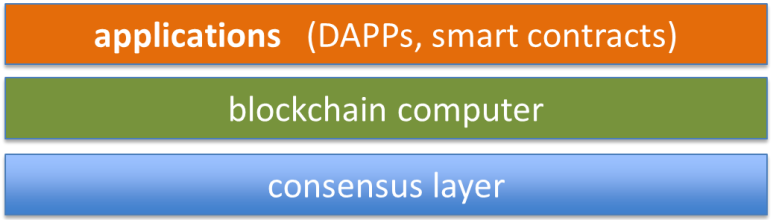
区块链有哪些应用场景

- 基本应用：数字货币系统

  价值存储流转、新型金融工具
- 扩展应用：数据存储与存证

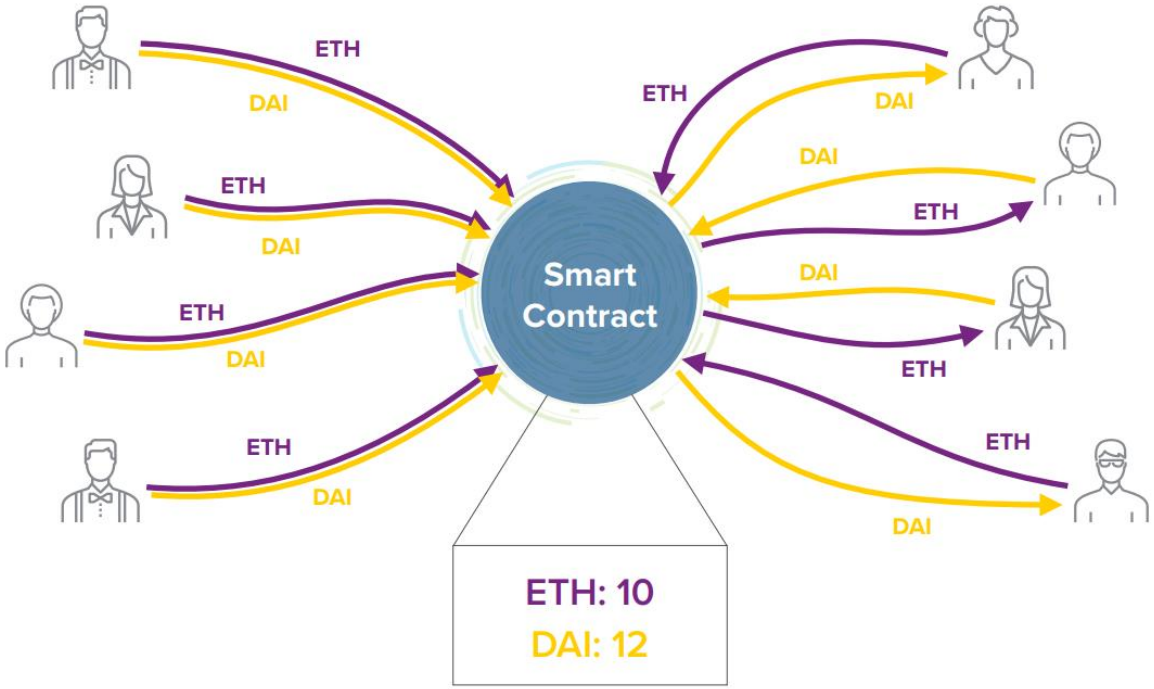
  证据保存、分布式存储
- 通用应用：分布式计算系统

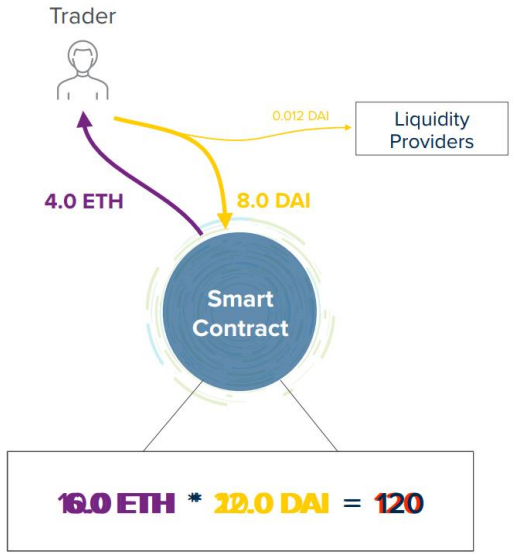
  安全多方计算、隐私保护数据共享



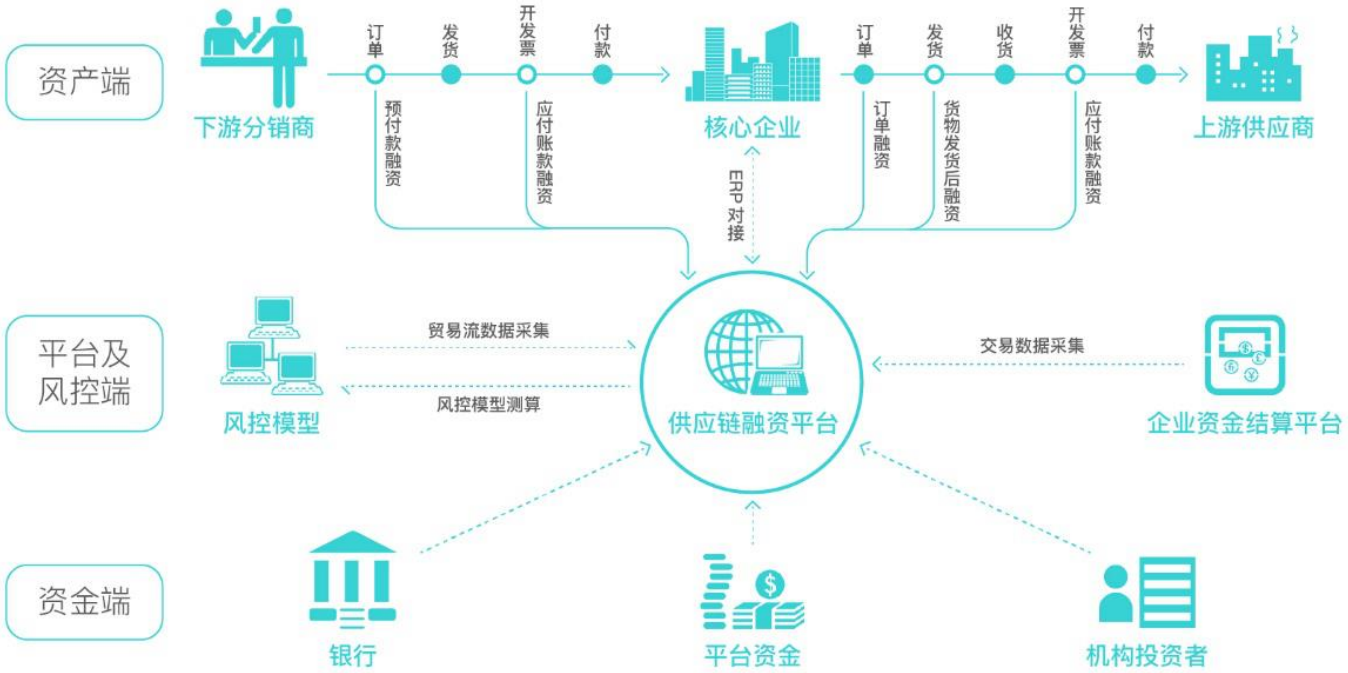
[区块链改变了传统网络应用中的生产关系]

应用场景1：去中心化金融

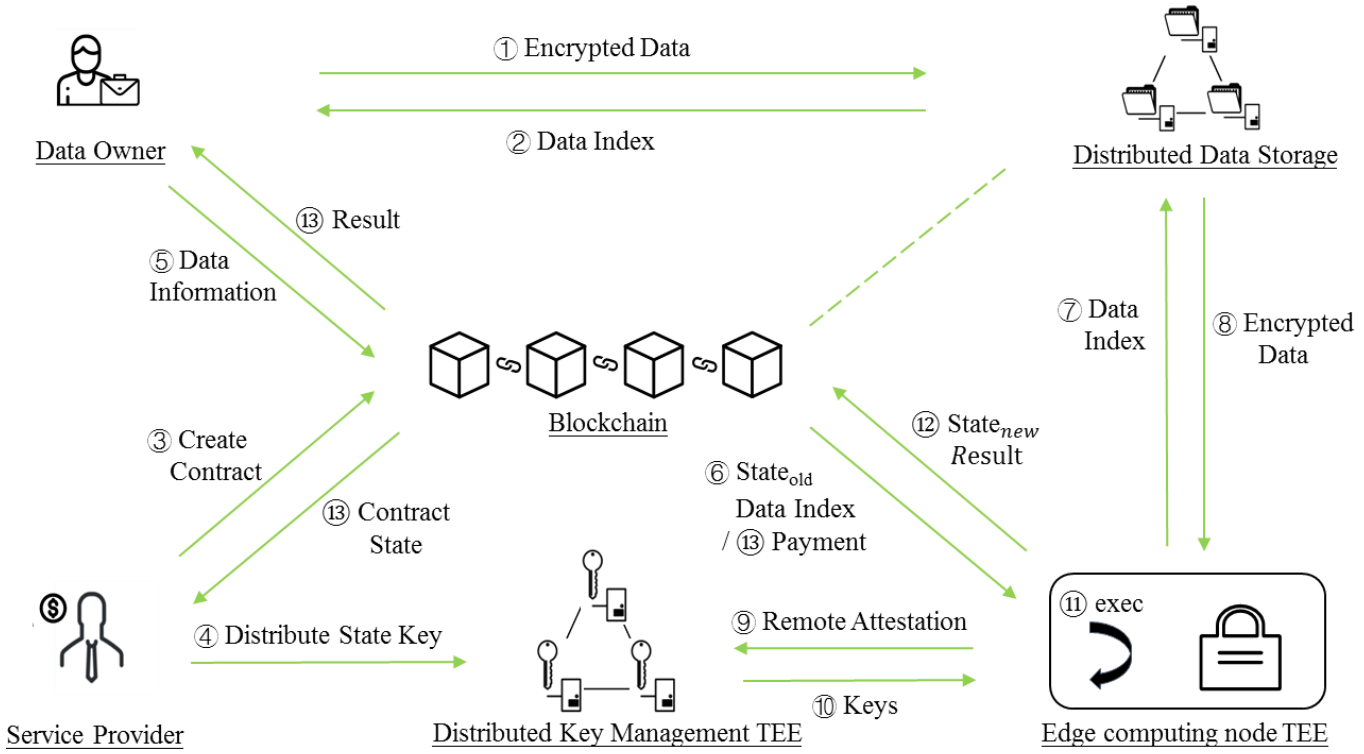




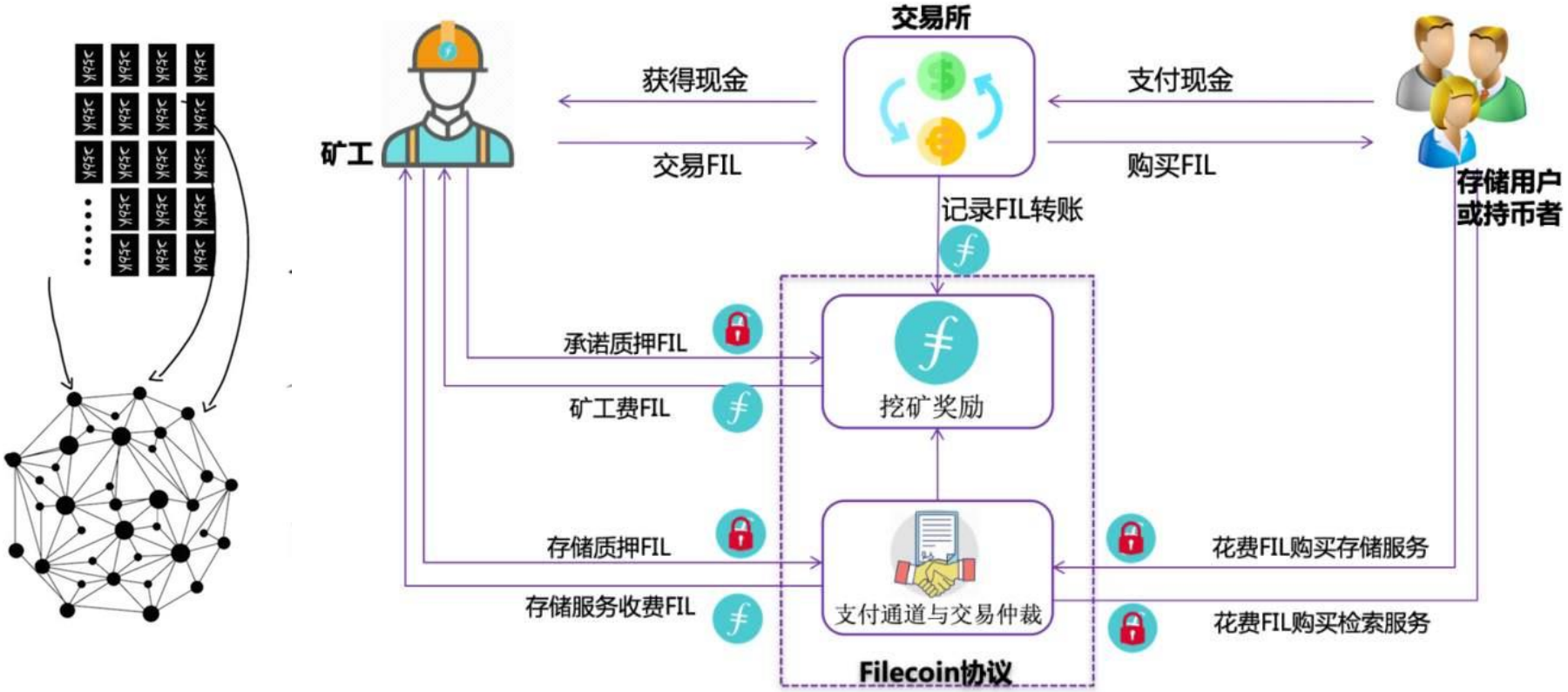
应用场景2：供应链管理


资产端
平台及风控端
资金端
下游分销商
订单
发货
开发票
付款
预付款融资
应付账款融资
核心企业
ERP对接
订单
发货
收货
开发票
付款
订单融资
货物发货后融资
应付账款融资
上游供应商
风控模型
贸易流数据采集
风控模型测算
供应链融资平台
交易数据采集
企业资金结算平台
银行
平台资金
机构投资者

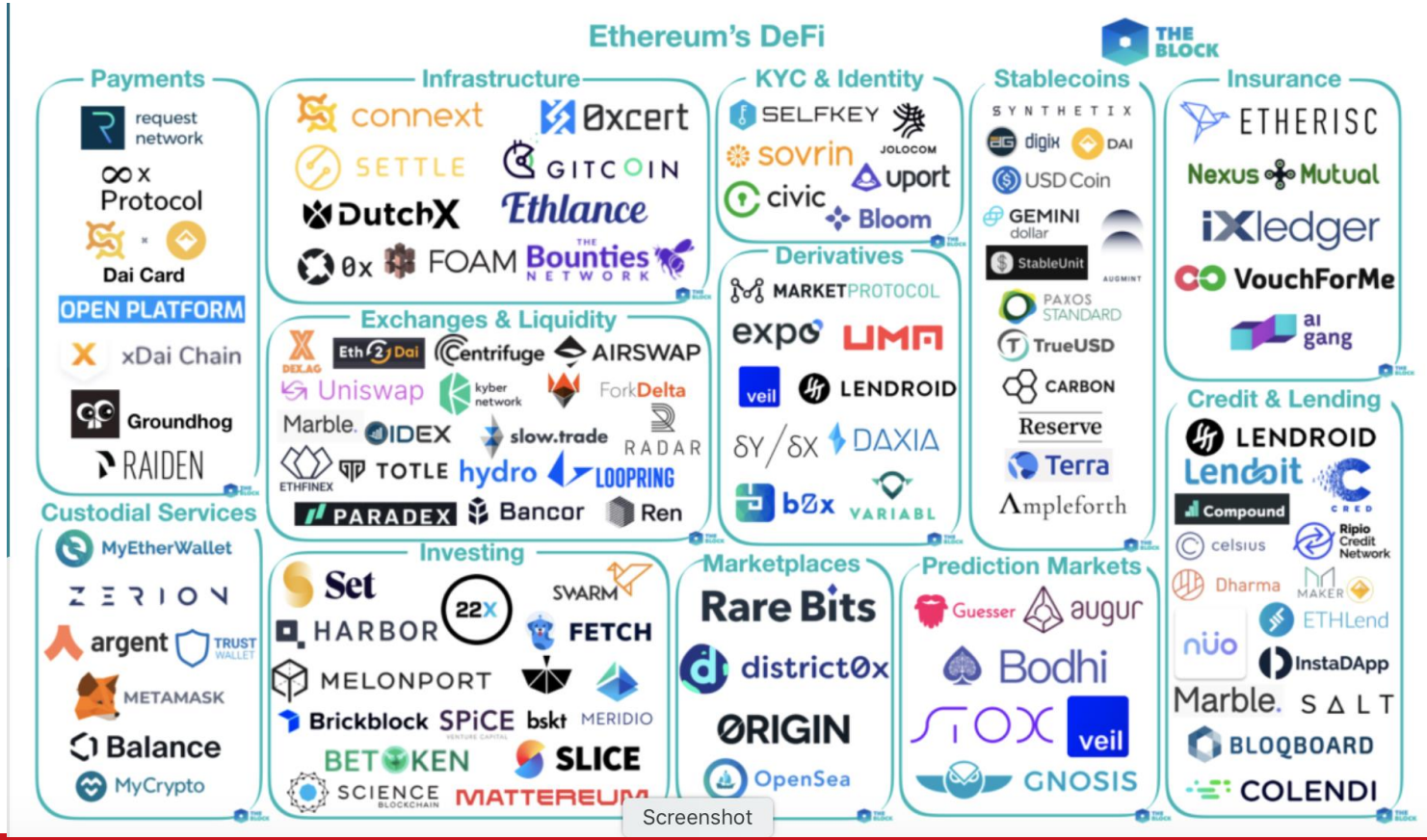
应用场景3：数据安全计算



应用场景4：去中心化存储



区块链（以太坊）生态系统



Screenshot

谢谢