

区块链应用落地

郑子彬 教授

中山大学
数据科学与计算机学院
<http://www.inpluslab.com>

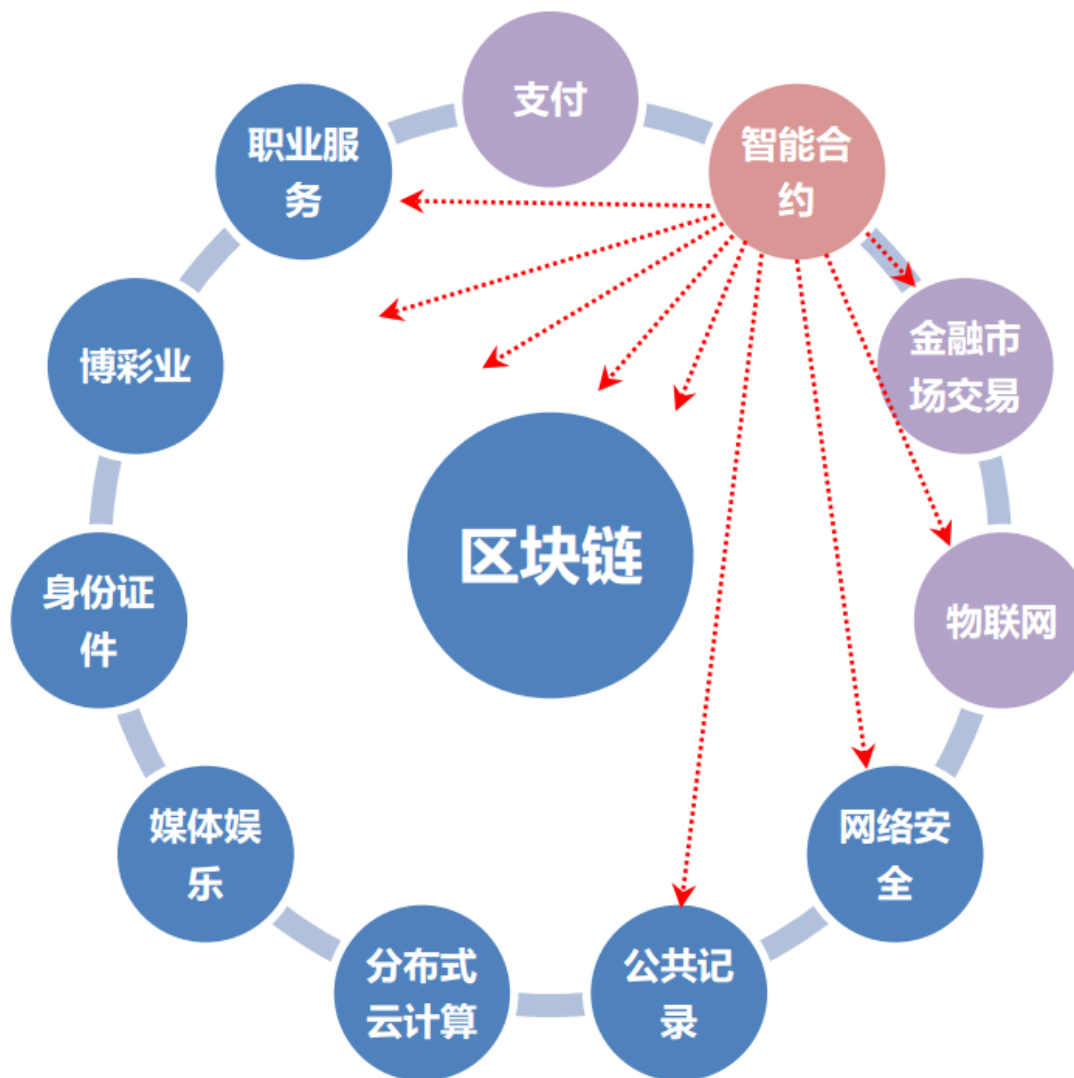


中山大學
SUN YAT-SEN UNIVERSITY



- 公有链
- 联盟链
- 私有链

区块链应用

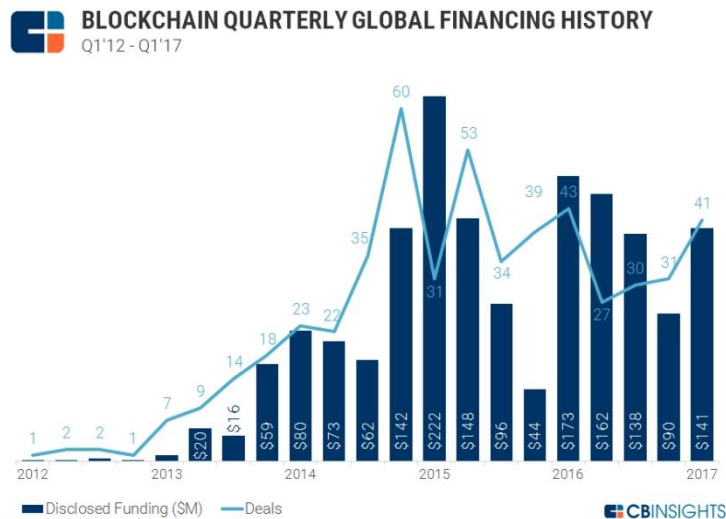


■ 区块链应用生态（鲸准数据）



■ 相关创业公司融资情况

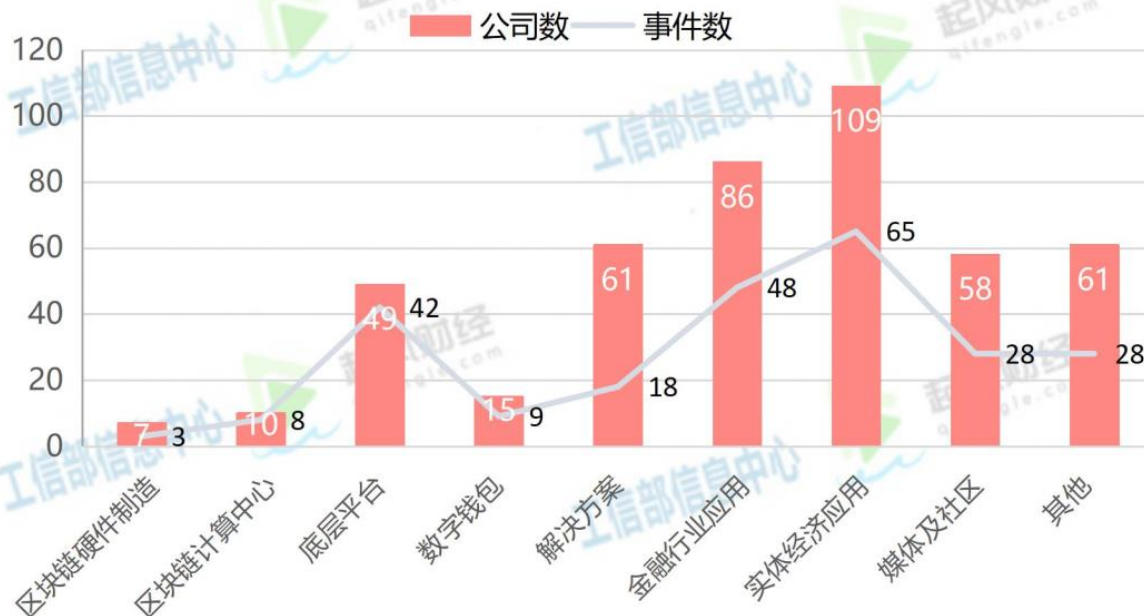
- 国外起步早，呈稳步增加的趋势
- 国内起步较晚，但近期迎来投资井喷



■ 区块链产业生态

区块链领域的行业应用类公司数量最多，其中为金融行业应用服务的公司数量达到 86 家，为实体经济应用服务公司数量达到109家。此外，区块链解决方案、底层平台、区块链媒体及社区领域的相关公司数量均在 40 家以上。

中国区块链产业细分领域公司和融资事件数分布



数据来源: itjuzi.com, IT 桔子

截止时间: 2018.3.31

案例1：区块链电子发票



■ 区块链电子发票在广州及深圳开出



深圳电子普通发票



发票代码: 144031809110
发票号码: 00000001
开票日期: 2018 年 08 月 10 日
校验码: 88500

扫描二维码
查询发票真假

购买方	名称: 深圳萨摩耶互联网金融服务有限公司	密码区	a 7 4 e 7 2 a 2 4 8 9 6 4 0 3 e 5 1 2 4 e 5 f 2 8 c 9 7 3 9 c 3 5 7 4 3 4 6 4 0 8 1 0 f b d 1 6 f a a 8 3 6 2 7 4 4 3 4 e 8 8 5 0 0					
	纳税人识别号: 91440300342626556K 地址、电话: 电子支付标识:							
	货物或应税劳务、服务名称	规格型号	单位	数量	单价	金额	税率	税额
	餐饮服务			1	186.79	186.79	6%	11.21
	合 计					¥186.79		¥11.21
价税合计(大写)		壹佰玖拾捌元整			(小写) ¥198.00			
销售方	名称: 深圳市国贸餐饮有限公司	备注						
	纳税人识别号: 91440300738842749F 地址、电话: 深圳市罗湖区人民南路国贸大厦B48-B490755-82214922 开户行及账号: 农业银行深圳市国贸支行41008900040066766							

哈希值

收款人:

复核:

开票人:

销售方:(章)

发票专用章

案例1：区块链电子发票



■ 发票报销存在的问题：

- 参与方多，手续繁杂
- 流转周期长
- 各参与方之间信息不互通

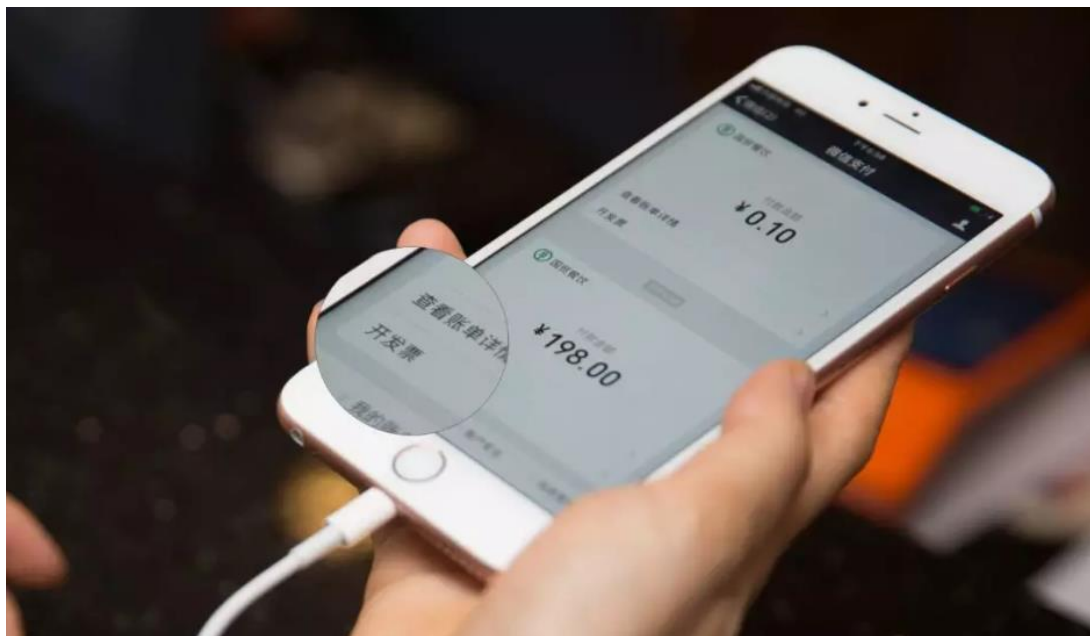
案例1：区块链电子发票



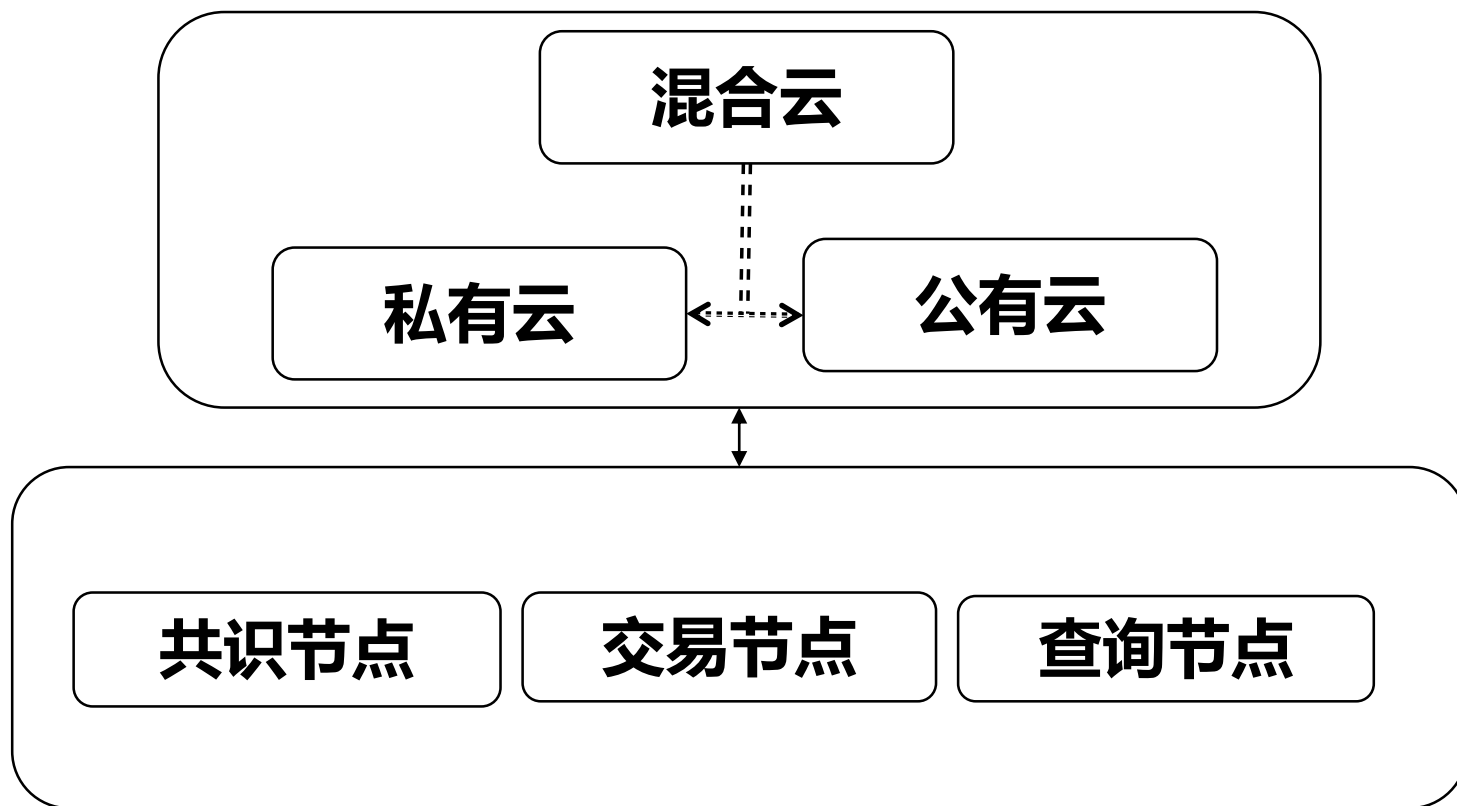
■ 由深圳市税务局、腾讯、金蝶软件三方合作

■ 流程：

- 微信支付
- 发票开具
- 报销到账



案例1：区块链电子发票



区块链电子发票的部署方案

案例1：区块链电子发票



共识节点

→ **部分可控站点部署**

全量数据

→ **只在税务内网落地**

其他参与方

→ **只有己方数据及经授权查询的数据**

案例1：区块链电子发票



■ 区块链电子发票的优势：

- 对**商户**来说：大大节省了商户时间、硬件、人员成本
- 对**企业**来说：可以安全快捷地实现发票申领、开具、查验，还可以在打通企业财务系统后，实现员工即时报销，后续可拓展至纳税申报
- 对**税局**来说：可实时监控发票开具、流转、报销全流程，实现无纸化智能税务管理，保障税款及时、足额入库

案例2：商品溯源



■ 当前商品溯源存在的痛点：

- 信息存储中心化，市场信息不对称
- 伪造成成本低，易伪造，存在信任问题
- 多点生产记录对账效率低



案例2：商品溯源



■节点部署方案：

- 在私有云上部署有运维能力的公司、机构，他们可在本地上传数据上链
- 在公有云上部署缺乏运维能力的公司

私有云

公有云

案例2：商品溯源



■ 区块链商品溯源的优势：

- 商品信息全程实时溯源
- 商品信息不可篡改
- 降低物流成本



案例3：公益项目



■ 公益领域现状：

- 公益信息散落在各块，没有被完整的收集和展示
- 难以高效地追踪公益资金流向，无法确保善款真正帮助了受助对象
- 公益需要多方对慈善进行更有效的监督，进行事后审计

案例3：公益项目



■ 将公益资金流用区块链记录



案例3：公益项目



应用实例：

[< 返回](#)[爱心捐赠](#)[分享](#)



和再障说分手

46,156.38

180,000

10982

用户捐款(元)

目标(元)

爱心(份)

25%

项目详情

爱心留言 (99+)

项目简介

捐助东方天使基金，救助再障儿童，让他们和再障分手。

项目说明

爱心传递记录

我要捐款

[< 返回](#)[爱心传递记录](#)

筹款中

查看捐款记录

2016-12-11

项目上线

[< 返回](#)[捐款记录](#)

每一笔捐赠的善款将直接到账中国红十字基金会账户

捐款人姓名	金额(元)	捐赠时间 ⌵
邱**	1.00	2016-12-19 10:28:22
邱**	1.00	2016-12-19 10:28:56
荣**	1.00	2016-12-19 10:32:12
庄**	5.00	2016-12-19 10:35:07
杨**	5.00	2016-12-19 10:35:36
张**	0.10	2016-12-19 10:35:50
周**	0.10	2016-12-19 10:36:38
陈**	0.20	2016-12-19 10:36:39
曹**	20.00	2016-12-19 10:36:47
翁**	1.00	2016-12-19 10:37:43
陈**	1.00	2016-12-19 10:37:57
杨**	0.20	2016-12-19 10:38:01

案例3：公益项目



■ 区块链应用于公益项目的优势：

- 公开透明促进各方信息趋于真实
- 分布式账本利于违法行为举证
- 时间戳获得公众信任
- 去中心化降低交易成本

案例4：保险行业



■ 保险行业痛点：

- 存在欺诈行为
- 理赔流程繁琐耗时



案例4：保险行业



■ 区块链在保险行业的应用：

- **欺诈识别和风险防范：** 通过将保险索赔置于不可更改的总帐下，区块链有助于消除保险业中常见的欺诈源。
- **财产保险和意外伤害保险：** 以智能合约形式载录的保单和共享账本可提高财产保险和意外伤害保险的效率。

案例4：保险行业



■ 区块链在保险行业的应用：

- **健康保险：**区块链技术使得医疗记录可被加密保护并在健康服务提供者间共享，从而提高医疗保险生态系统的交互操作性。
- **再保险：**通过智能合约的形式保证再保险合同在区块链平台上的信息安全，可缩减信息量，简化保险人和再保险人之间的支付流程。

案例4：保险行业



■ 区块链应用于保险行业

产品管理

营销

销售分配

保险业务

政策服务

索赔管理



通过**智能合约**实现业务规则编写和自动处理理赔，
并将索赔信息记录放在链上

案例4：保险行业



■ 区块链应用于保险行业的优势

- 能够杜绝重复保险，或利用同一保险事故进行多重索赔的情况
- 通过智能合约实现自动化理赔
- 提高理赔处理效率，使用智能合约可达到实时处理的水平

案例5：医疗数据管理



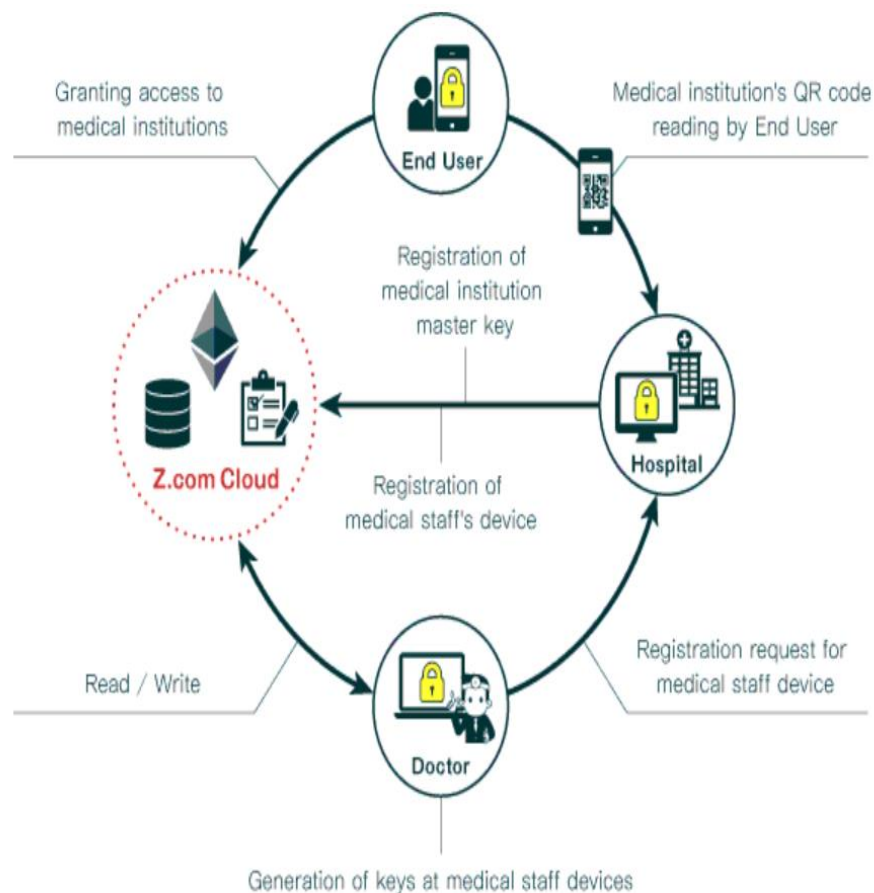
1 医学数据共享难

- 各团队都想率先突破
- 医学研究成果容易被盗取（成果确权）

1 例子：用户病历

- 用户的诊疗记录分布在各个医院，没有一份完整的记录，不利于诊断
- 用户的诊疗记录有可能出现泄露，威胁用户隐私
- 中心服务器存储的用户诊断记录可能会出错，一旦出错，很难恢复

案例5：医疗数据管理



1. 用户注册区块链地址

2. 当需要看病的时候用手机扫描医院的二维码，将自己的诊疗记录权限开放给当前的医院

3. 开放权限记录在区块链中

案例5：医疗数据管理



1 数据的安全性与隐私保密性

- 严格的监管政策，病人隐私
- 非对称加密技术
- 用户控制其他人对于自己的诊疗记录的访问权限,充分的保证自己的隐私

1 区块链通过技术手段解决缺乏中心权威机构进行协调的问题

1 数据不可篡改

案例5：医疗数据管理

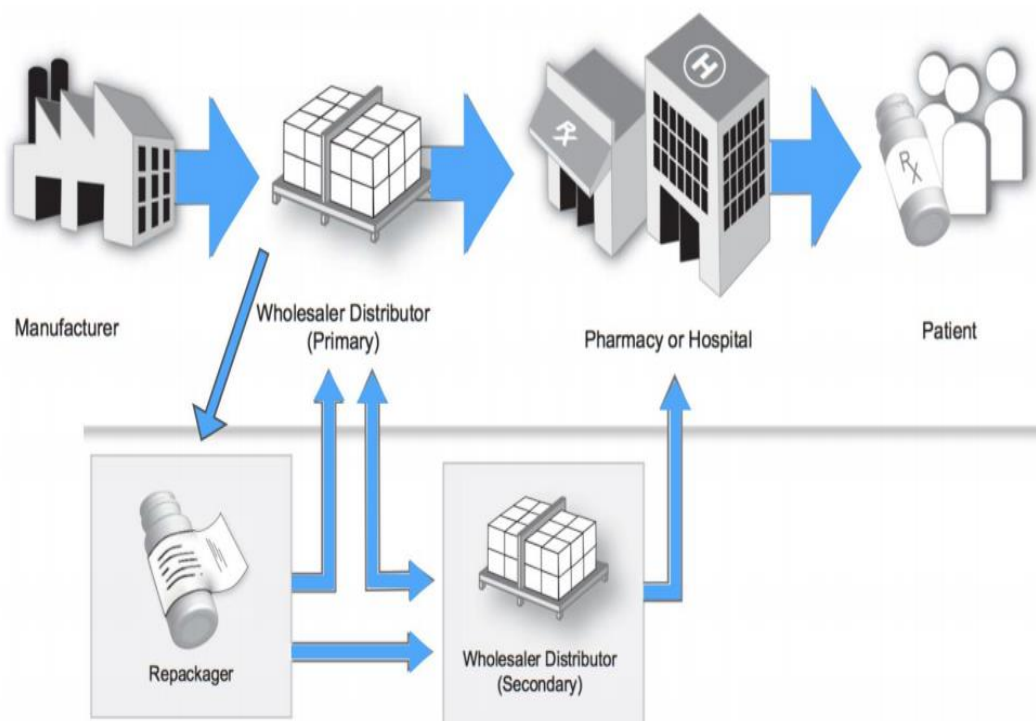


- 1 目前mit的Media lab已经有在尝试去做基于区块链的医疗记录管理项目，
<https://www.media.mit.edu/research/groups/1454/medrec>
- 1 Stanford的医学院正在利用区块链去搭建一个用户诊疗记录平台<https://medicinex.stanford.edu/blockchain/>
- 1 目前有几家公司在做区块链医疗记录分享平台，
<https://medicalchain.com/en/>
<https://guide.blockchain.z.com/en/docs/oss/medical-record>

案例6：药物供应链



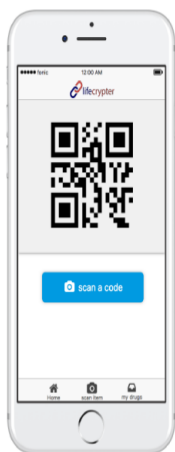
- 1 药物的供应链特别复杂，从产商到分销商再到患者手里，有着很多的环节。很有可能会出现很多的假药，对于患者来说很不放心。



案例6：药物供应链



- 1 区块链可以起到监督的作用，对于每盒药物，都会有着独特的地址，从产商最终到患者，中间的每个环节，只有那些可信的一方才可以在区块链上写下自己对于这盒药物的处理并且签名，那么每到一个环节，都可以检查该盒药物在上一环节是否出现问

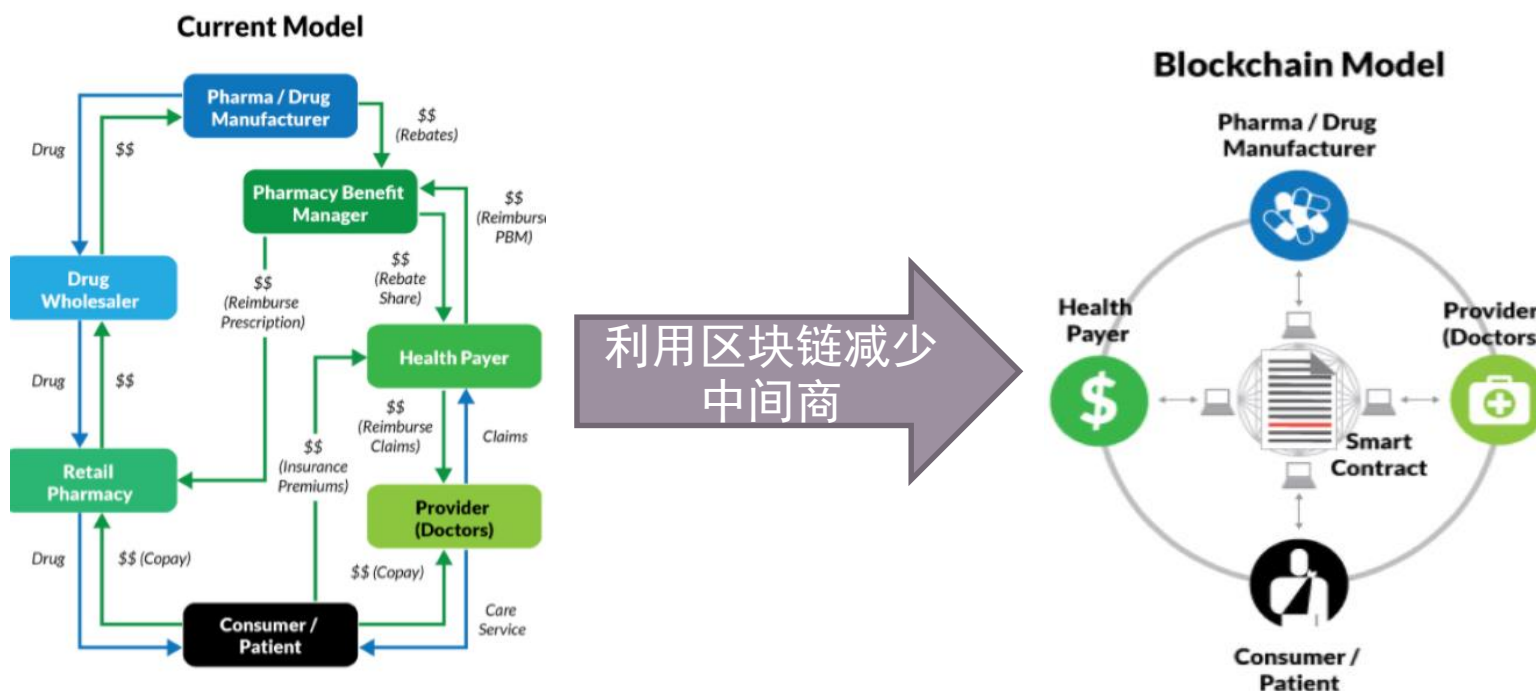


Contract unique ID
0xe41042A87817777cA01E1F8f02f0F8F580be82EF

医学应用：医疗费用



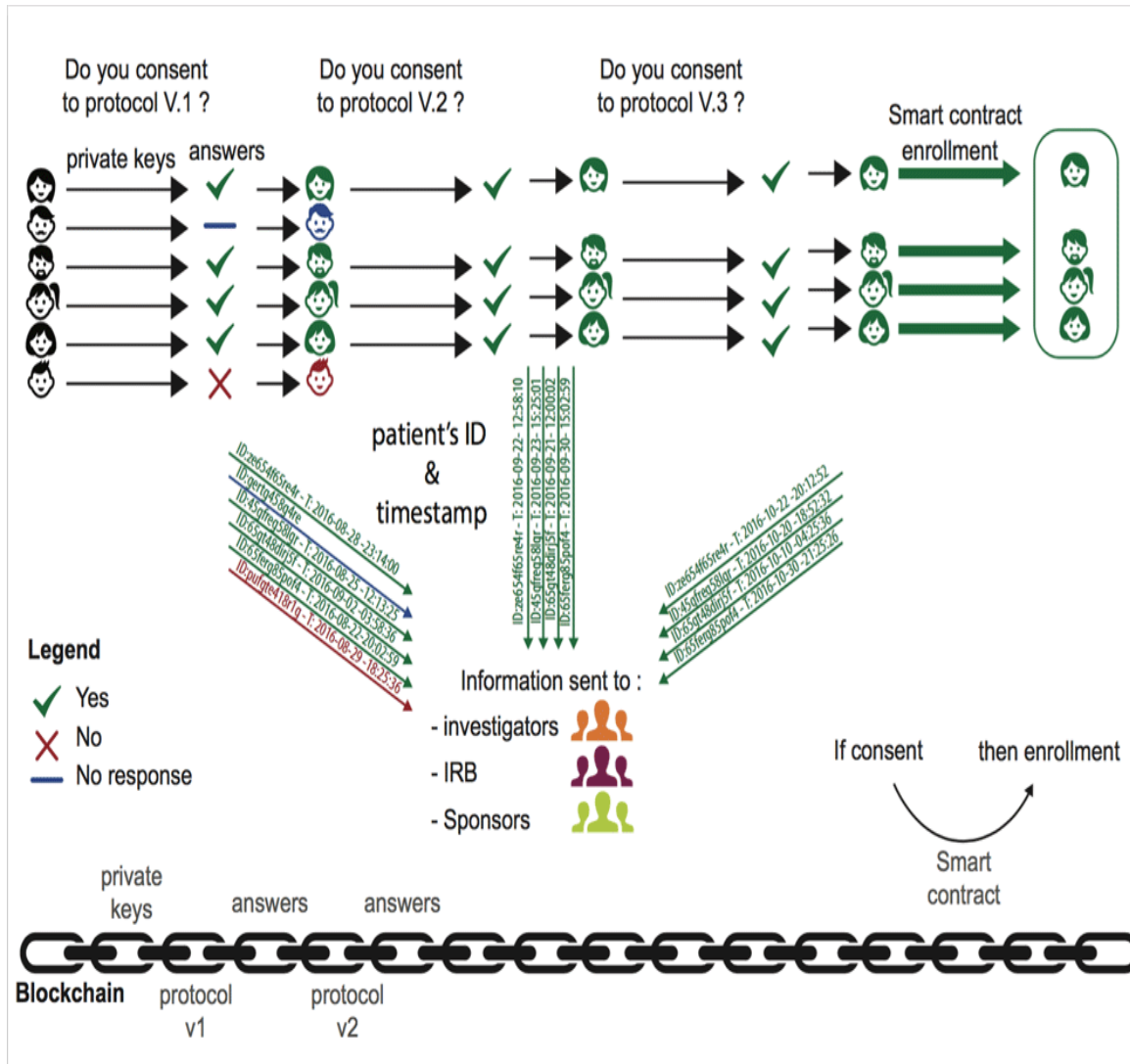
- 1 从药物制造商到医院有很多第三方，因为信任问题，虽然中间商抽取了大量费用，但药物制造商跟医院还是倾向于跟中间商合作，利用区块链可以提高交易双方的信任，避免了中间商，减少医疗的开销



- ◆ 开发出新药通常需要很久时间的测验，有可能会虚报药物的结果。比如2001年，就有一家药物公司虚报临床测试结果，称药物治疗儿童抑郁特别有用，结果后面发现不仅没用，还被发现服用后的儿童自杀的概率高了很多
- ◆ 临床医学测试clinical trial的复现工作也十分困难

使用区块链可以确保临床测试的每次协议和测试都准确的记录，并且不会被篡改

医学应用：临床医学研究

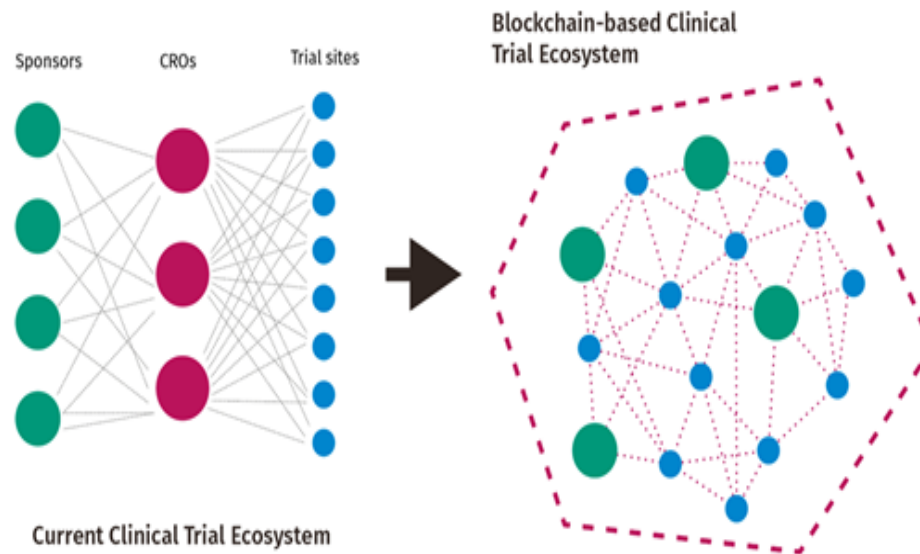


在每一次的测试前，让测试人员填写信息，确认测试用户知道自己要测试的药物之后使用智能合约登记，这些用户的反应记录会被完整的记录在区块链上，并且无法被篡改，这样一来药物公司无法去伪造临床的结果。

医学应用：临床药物测试效率



- 1 伦敦帝国理工大学开发了一个基于区块链的临床测试系统，去除第三方，从而更快的推动药物的开发
- 1 传统的药物测试需要经过Contract Research Organization(RCO)。区块链直接让药物公司跟测试用户对接，有利于加速药物的开发进程



案例7：区块链征信联盟



■ 征信行业痛点需求

- 机构之间**互不信任**
- 用户担忧**数据泄露**



案例7：区块链征信联盟



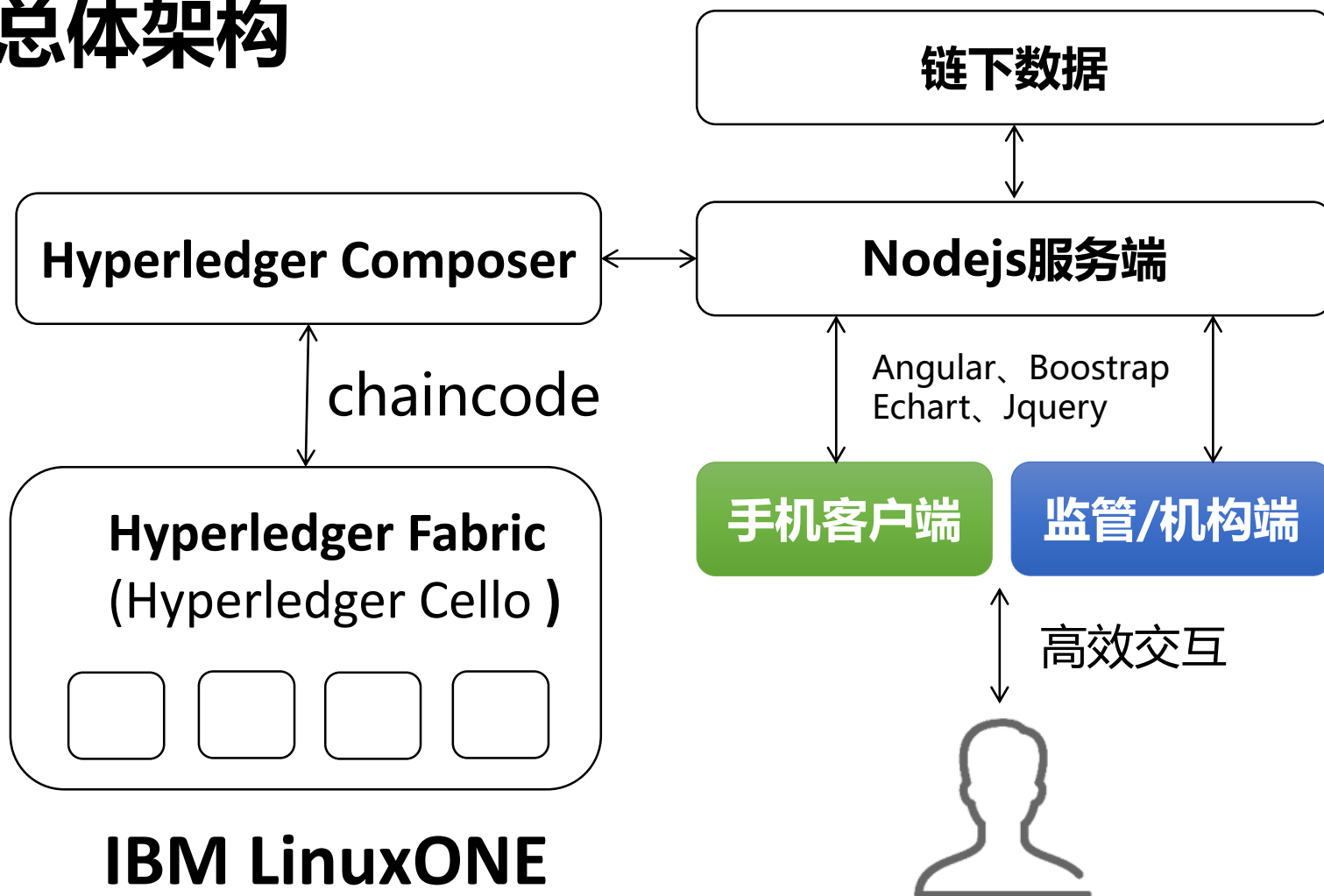
■ 功能设计



案例7：区块链征信联盟



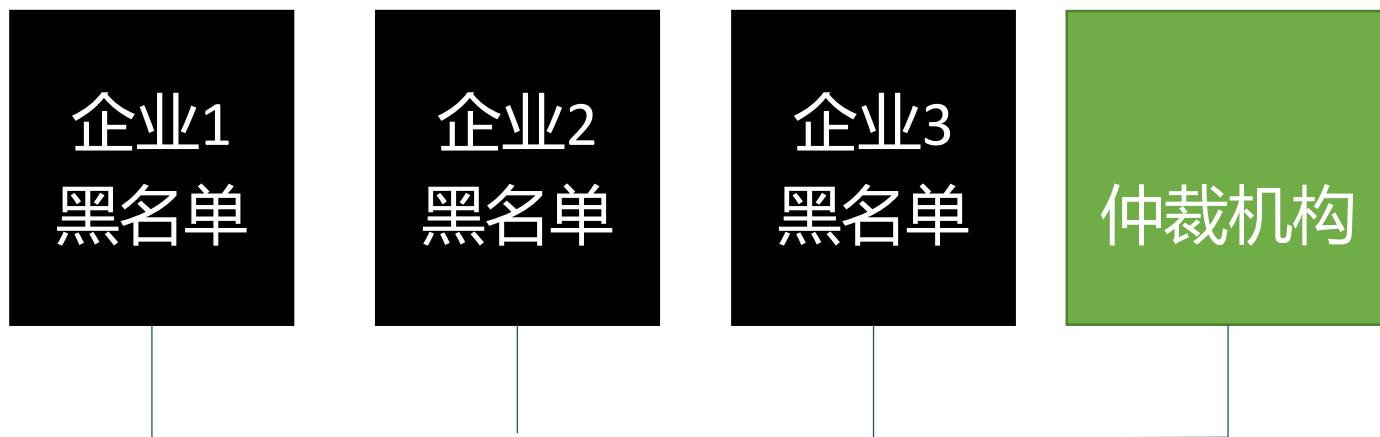
■ 总体架构



案例7：区块链征信联盟



■ 黑名单：基于区块链的共享及仲裁

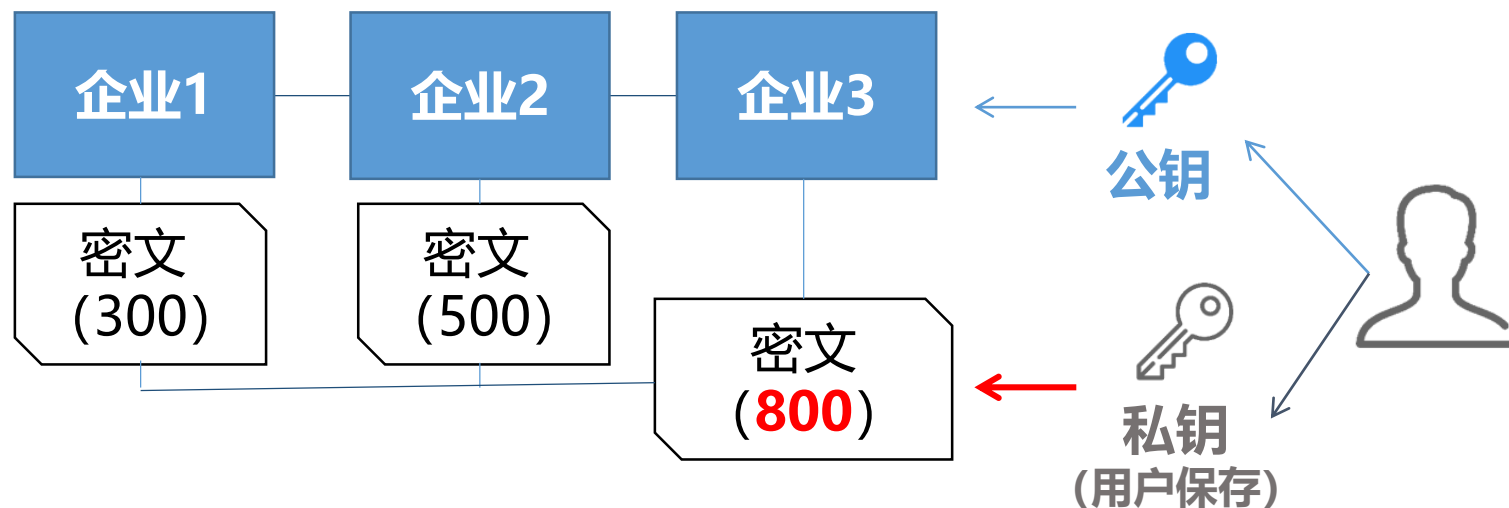


- 引入区块链智能合约的**仲裁机制**
- 比传统单点更可信、更高效共享

案例7：区块链征信联盟



■ 信用分：同态加密的智能合约计算及隐私保护



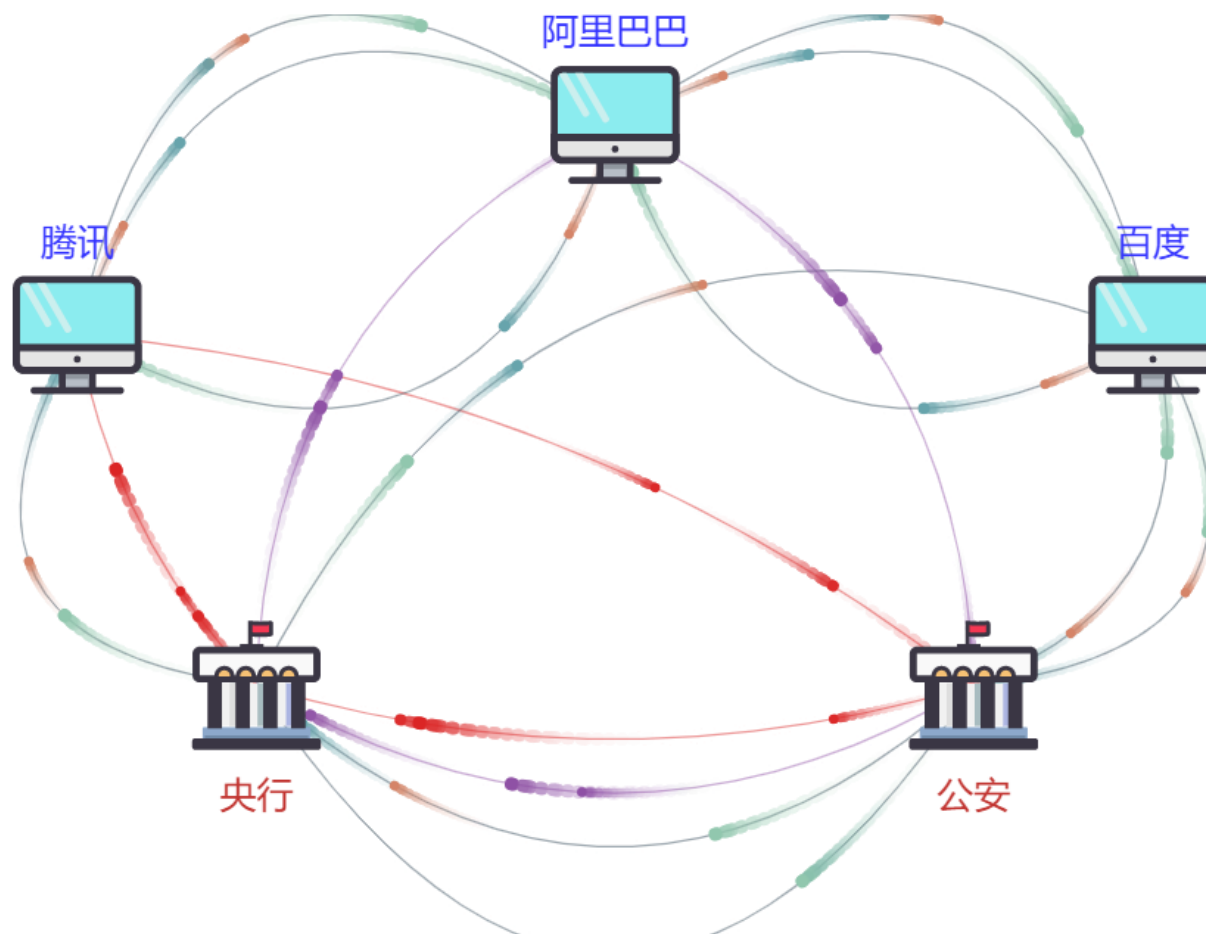
区块链数据的**计算权和所有权分离**

- 计算权：智能合约、各机构都能计算
- 所有权：用户私钥才能解密、用完可更改

案例7：区块链征信联盟



■ 交易数据：监管追溯、隐私保护



案例8：供应链金融



- 供应链金融领域备受瞩目，商业化落地的进展较快
 - 具有万亿级别的市场规模
 - 金融服务实体经济
 - 需要多方合作
 - 没有一个传统中心化的机构在治理
 - 不需要高并发
 - 存在信任问题

案例8：供应链金融



- 金融机构将供应链金融分为在**应收账款类、预付类**和**存货类融资**，其中**应收账款类**的规模尤为巨大
 - 2016年末，我国规模以上工业企业应收账款12.6万亿元，同比增长10%
 - 产生了企业巨大的融资需求
 - 2015年我国年商业保理量仅在2000亿元左右，大量供应链需求没有被满足
 - 供应链金融行业发展空间巨大

案例8：供应链金融



- **痛点1: 供应链上的中小企业融资难，成本高**
 - 资产证券化
- **痛点2: 如何自证清白，资金端风控成本居高不下**
 - 整个供应链行业对外的低透明度
 - 买方缺少可靠方法验证产品和服务的真正价值
 - 数据上链，透明可信
- **痛点3: 高居不下的交易成本**
 - 传统模式涉及多方处理，花费时间长，成本高
 - 需要信任机构完成相应认证

案例8：供应链金融



供应链金融(SupplyChainFinance): 是指将供应链上的核心企业以及与其相关的上下游企业看作一个整体，以**核心企业**为依托，以真实贸易为前提，运用自偿性贸易融资的方式，对供应链上下游企业提供的综合性金融产品和服务

案例8：供应链金融



供应链痛点

- 信息不透明
- 数据失真
- 运营效率低
- 融资成本高



数据真实可靠



交易数据透明

区块链特征

- 分布式记账
- 智能合约
- 数据防篡改
- 数据可追溯

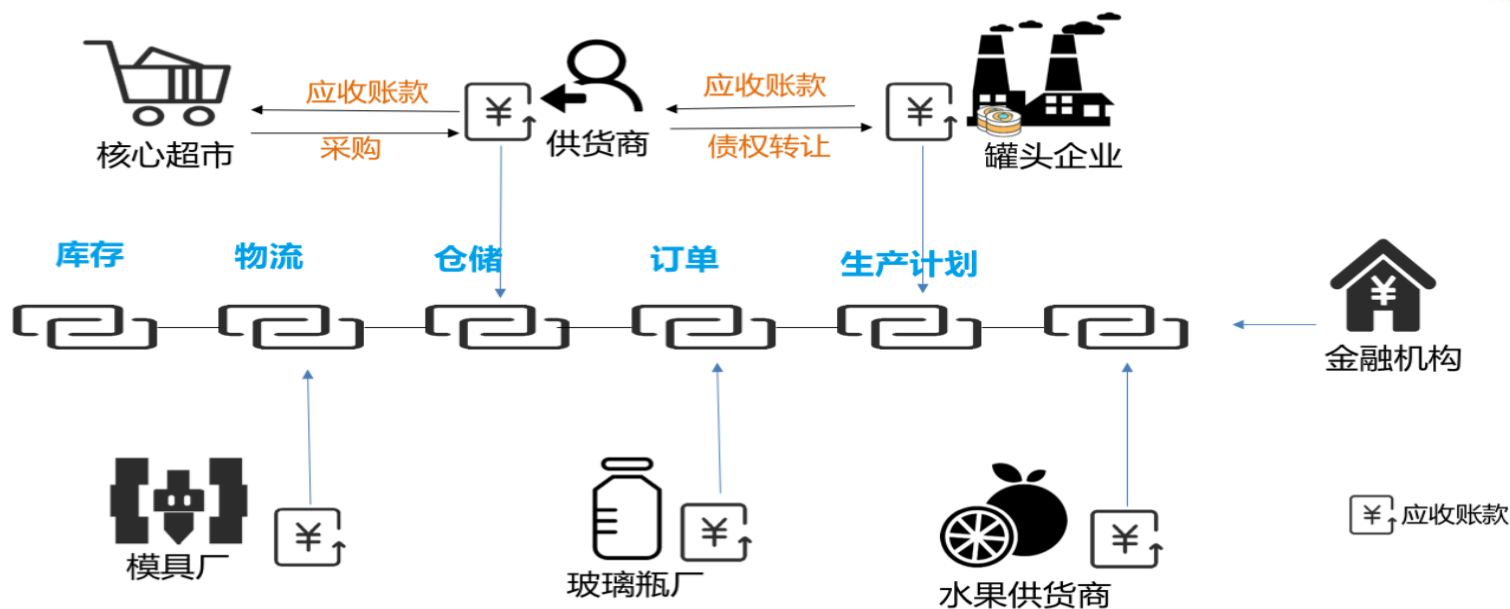


交易结算高效



降低融资成本
提高融资效率

案例8：供应链金融



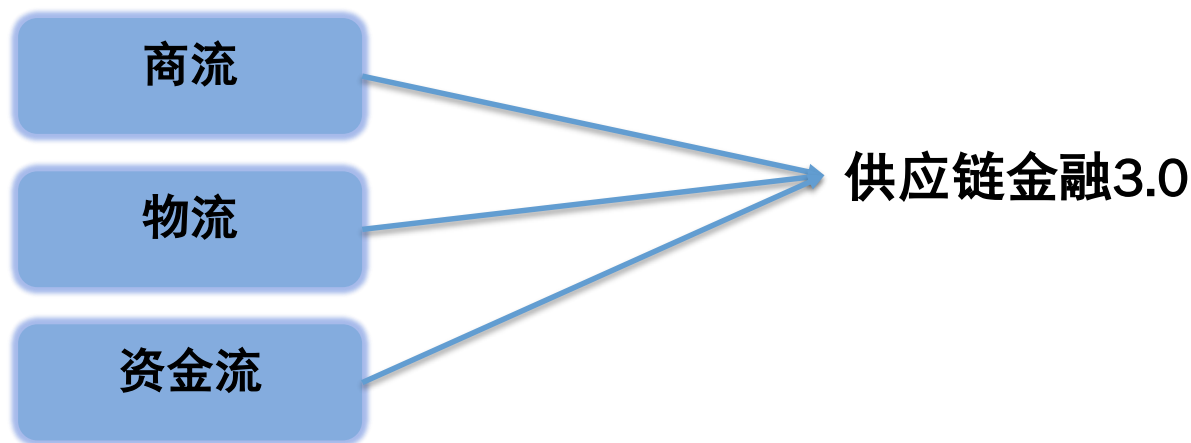
图源：宜信易启云

- ◆ 区块链将分类账上的货物转移登记为交易，以确定与生产链管理相关的各参与方以及产品产地、日期、价格、质量和其他相关信息（数据上链）。
- ◆ 区块链为供应链提供了交易状态实时、可靠的视图

案例8：供应链金融



- 供应链金融3.0以**三流合一平台**为核心
- 银行握有供应链条上所有成员企业的交易信息，以“互联网+”的思维模式，瞄准着80%的中小客层
- 有先进的互联网技术支持，大幅降低银行操作成本与风险管控成本



案例8：供应链金融



- 打造区块链+供应链金融的联盟
 - 供应链金融平台核心企业
 - 专业金融中介机构资金方
 - 保理机构
- 数据上链，提供数据确权，溯源等服务
- 资产数字化：仓单、合同等变成数字资产（唯一，不可篡改）
- 数字资产的交易：将非标的企业贷款需求转变成标准化的金融产品，进行代币化

其他应用：数字学历证书



旧金山软件工程师培训Holberton学校（霍博顿学校）宣布从2017年开始在区块链上共享学历证书信息。所以，公司可以很容易地验证雇员学历证书的真实性。

HOLBERTON
school()

About Education Students Team Admissions FAQ

Sign in [Apply now](#)

Become a Full-Stack Software Engineer

Holberton School is a project-based alternative to college for the next generation of software engineers

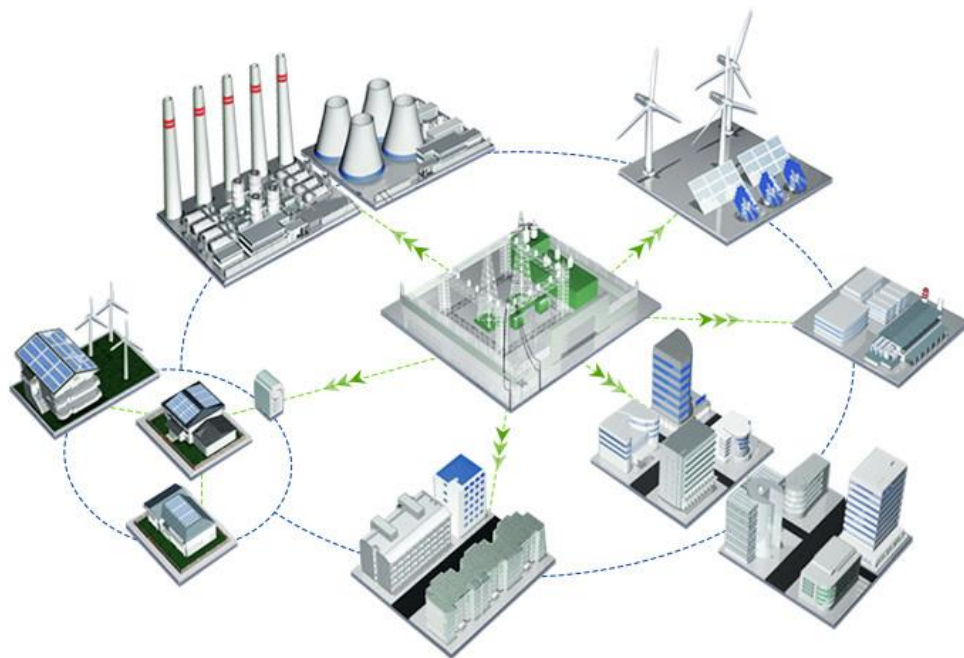
"Holberton School offers a truly innovative approach to education: focus on building reliable applications and scalable systems, take on real-world challenges, collaborate with your peers. A school every software engineer would have dreamt of!"

- Kate Volkova, Sr. Software Engineer at Microsoft

其他应用：能源交易



- 能源孤岛，缺乏中介（交易所）
- 能源交易：信任问题
- 精准计费



总结



- 分不同类型：公链、联盟链、私有链
- 通过技术手段解决信任问题，适用于互不信任的多方进行协作的场景
- 安全，可追溯，不可篡改
- 去中心化及成本效率的权衡
- 安全性及经济模型内嵌
- 基于Token的激励机制设计是关键



实验室公众号