

区块链专题研究之

回归商业本质

区块链的概念、典型案例与市场趋势

***本资料仅限内部浏览，禁止对外发布！**

我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

——习近平



/01

区块链的概念与发展历程



区块链诞生的历史文化背景



社会学背景-生物进化论

信息社会的进化论不同于工业社会，是基于数字关系，是从控制到失控，从边缘到中心，从他治到自治。



政治学背景-无政府主义

无政府主义在数字世界重新兴起，区块链最初是一些具有无政府主义价值观的人创造出来的。

经济学背景-自由主义经济学

哈耶克的自由主义经济学提到，要把货币的发行权还给任何一个人、机构，即货币非国家化。



技术背景-分布式网络技术

分布式网络技术成熟是区块链得以诞生的基础，没有分布式网络技术，就不可能产生区块链。





区块链发展历程

从区块链技术角度出发，区块链行业发展可分为三个阶段：以数字代币为典型特征的区块链 1.0 和以智能合约为典型特征的区块链 2.0，目前正在向**多行业应用探索的 3.0 阶段**发展。

区块链的发展阶段表

区块链发展阶段	典型事件	作用
2009-2014（区块链 1.0）	比特币 系统公布	区块链技术起源
2014-2017（区块链 2.0）	以太坊 ，超级账本等区块链开源项目发布	区块链协议层和框架层优化，智能合约支持，公有链和联盟链、私有链等方向出现
2017-现在	商业应用 项目爆发出现，但仍未大规模落地	区块链在不同行业的应用探索，可能向 3.0 进化

资料来源：华为区块链白皮书



你印象中的区块链有什么重要特点？

关于“区块链是什么”“区块链价值”的关键字描述

人民日报

去中心化、不可篡改、
全程留痕、可以追溯、
集体维护、公开透明

多方合作
共享平台
防篡改
提高效率 节约成本
安全信任
赋能未知领域的创新
去中心化
安全程度提升
复杂
难懂
难以量化
ICO

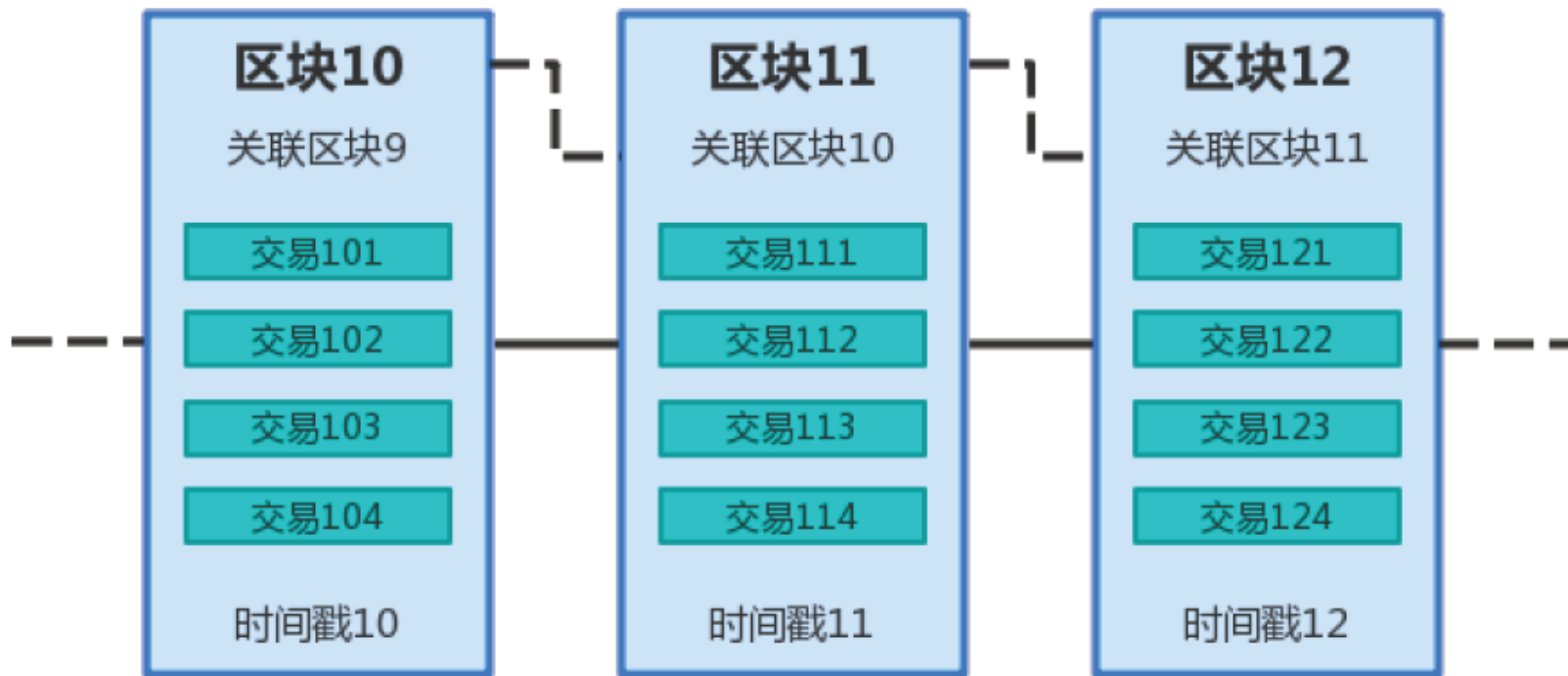
来源：普华永道调研报告



区块链的定义

区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的链式数据结构，以密码学的方式保证数据不可篡改、不可伪造，具有去中心化的特征。

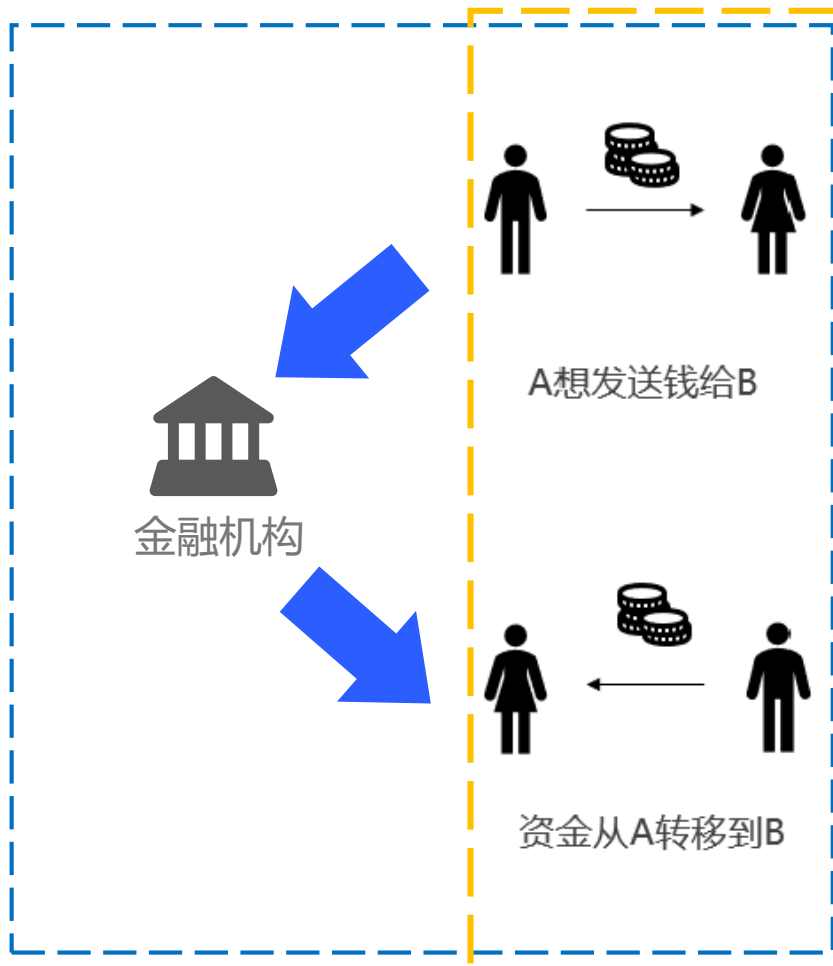
IDC 将区块链定义为记录信息和数据的**分布式数字账本**，该账本存储于对等网络的多个参与者之间，参与者可以使用加密签名将新的交易添加到现有交易链中，形成安全、连续、不变的链式数据结构；从数据的角度来看，区块链是一种不可能被更改的分布式数据。



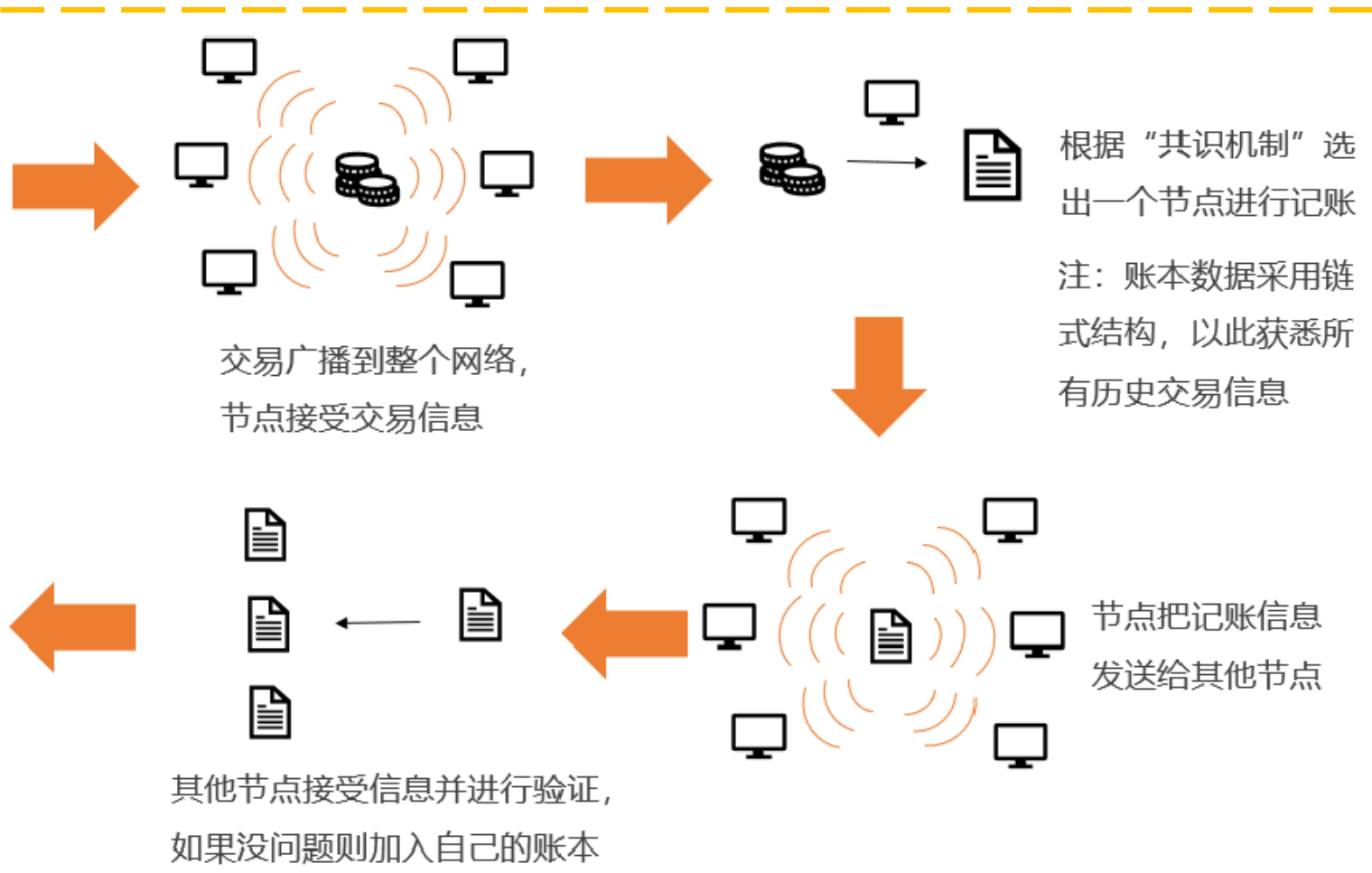


区块链技术工作原理

传统交易：中心化账本



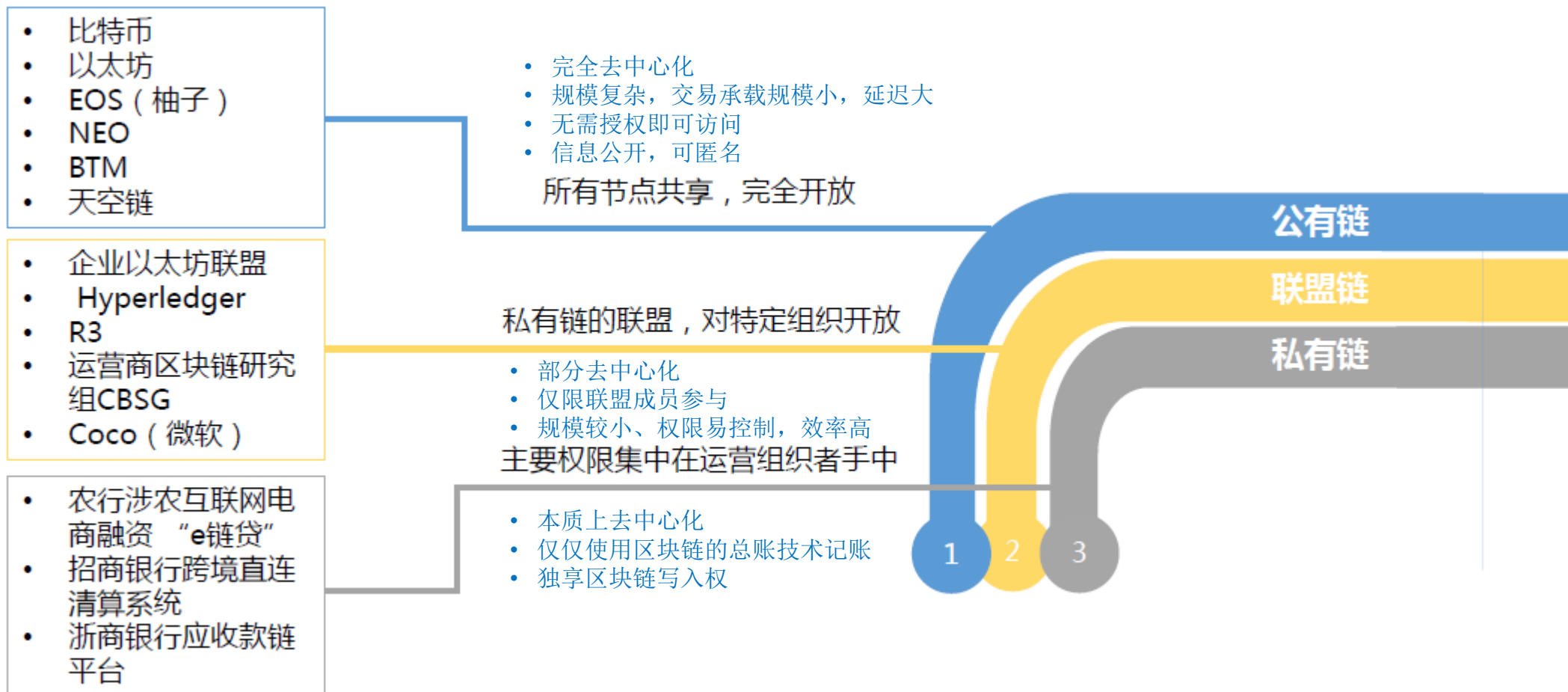
区块链交易：去中心化分布式账本





区块链的分类

- 区块链可分为公有链、联盟链、私有链三类，相比公有链的完全开放和公开，联盟链和私有链允许有多个或单个中心控制者控制参与主体范围和信息公开范围
- 金融行业需严格控制交易和信息等的保密，且有参与者的适合性要求，联盟链和私有链对于金融行业更加适用





区块链技术架构

■ 区块链基础架构分为 6 层：

包括数据层、网络层、共识层、激励层、合约层、应用层。

■ 共识层、网络层、数据层：

属于协议层，是构成区块链技术的必要层级，是实现区块链技术的基本保障。





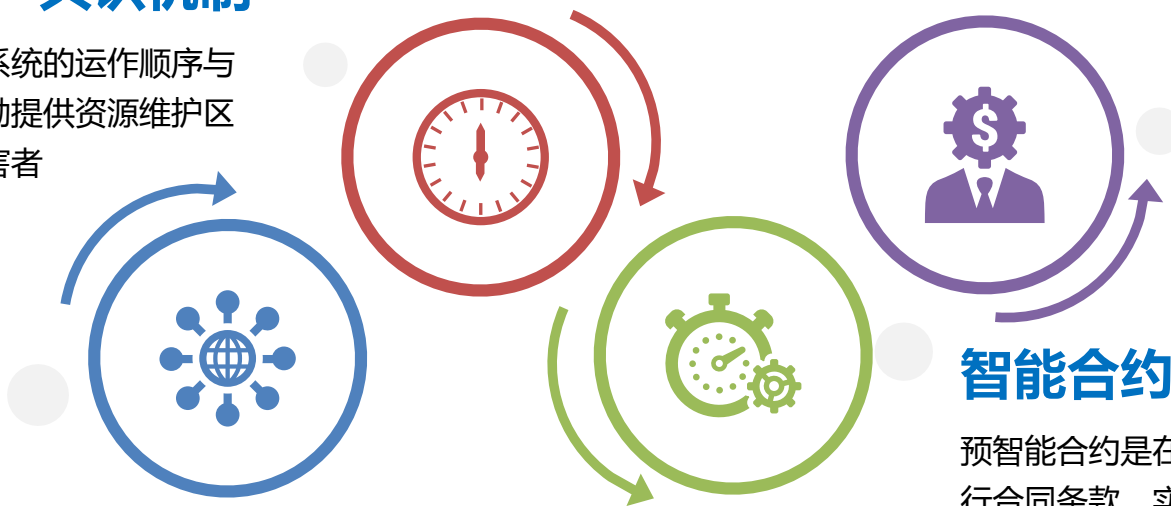
区块链的核心技术

共识机制

区块链中必须设计一套制度来维护系统的运作顺序与公平性，统一区块链的版本，并奖励提供资源维护区块链的使用者，以及惩罚恶意的危害者

分布式账本

多个网络节点、多个物理地址或者多个组织构成的网络中进行数据分享、同步和复制的去中心化数据存储技术



密码学

哈希算法、对称加密、非对称加密、数字签名、密码学

智能合约

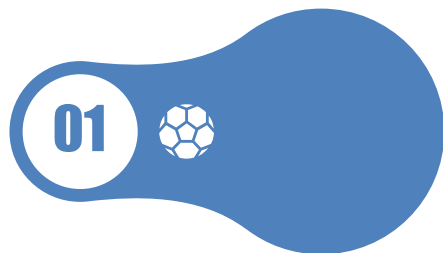
预智能合约是在一定条件满足时，能够自动强制的执行合同条款，实现“代码即法律”的目标



区块链有什么特性?

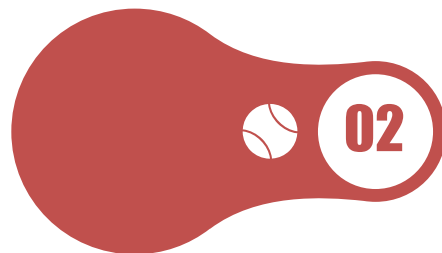
分布式 (去中心化)

没有中心化的硬件设备和管理机构，系统由多个节点共同维护。



不可篡改

区块链上的区块只能新增、不能被替换，交易可以通过新增区块的方式予以修改，但是区块记录将永久保留。



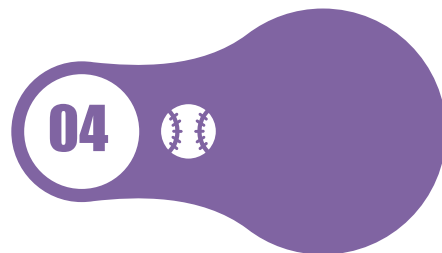
多节点共识 (去信任机制)

淘汰了中心化管理员来审批结算交易的角色，各个节点之间无需相互信任，通过共识机制对入链数据进行验证



隐私性和公开性

加密技术 (Hash碰撞) 使得全部人的账单并不会显示用户名字，而只是一串唯一识别码，保证了隐私性的同时也保证了公开性。





区块链依旧面临诸多挑战



数据真实性

难以解决上链之前源头数据的可信度问题



数据存储能力

区块链数据只增不减，难以满足商业应用存储需求



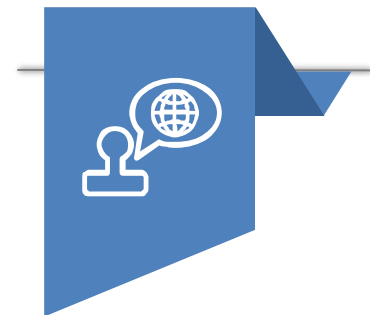
通用标准

目前的区块链系统大多缺少可插拔能力，很难灵活适应不同场景要求



隐私问题

如果要多方真正愿意将真实数据在链上共享，打破数据孤岛，必须要在隐私计算技术上得到提升



学习成本高

区块链由多种技术构成，学习成本高、实施难度大、复合人才稀缺



/02 区块链典型案例



区块链行业应用全景图

2017-2019年是区块链在应用落地方面**大规模尝试的时期**。但在现阶段区块链基础设施并不完善的情况下，大多数行业应用仍处于早期探索阶段，从概念验证到商业检验还需要更多的时间。





京东区块链案例：从猪脸识别到区块链养猪

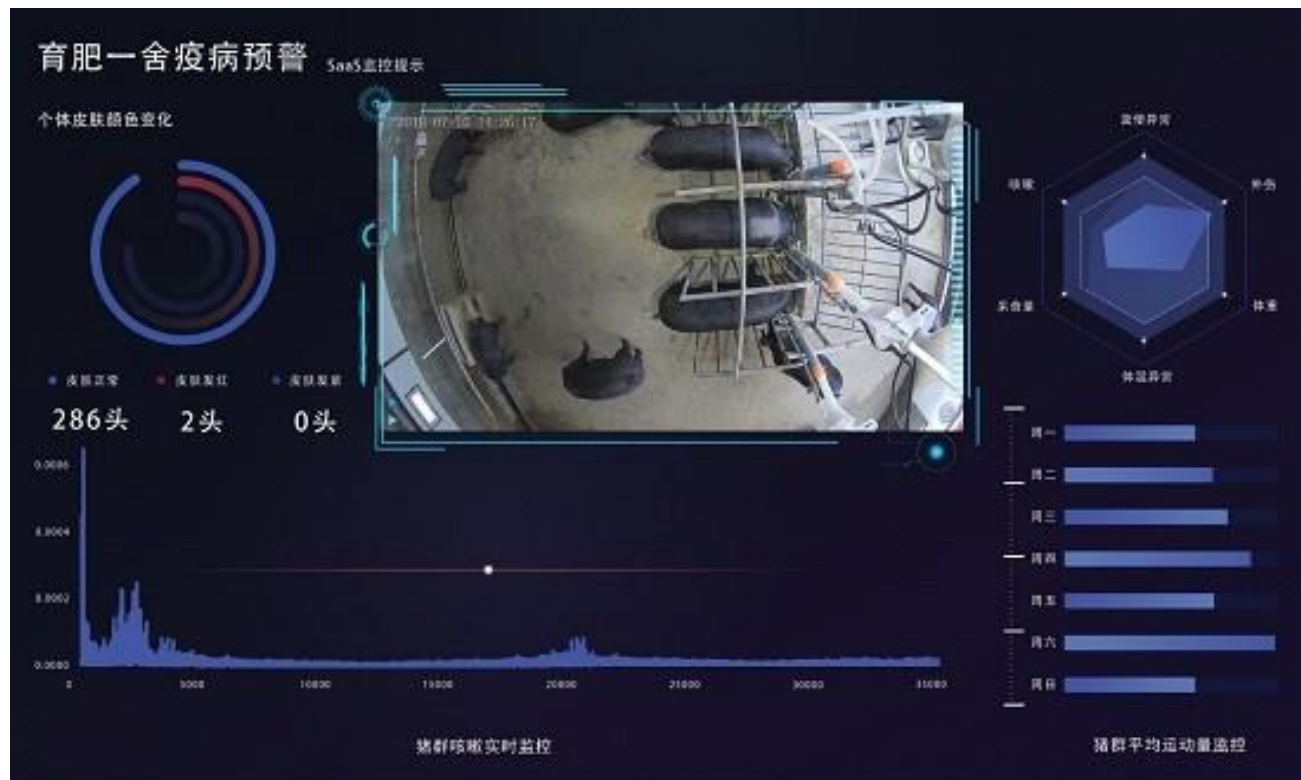
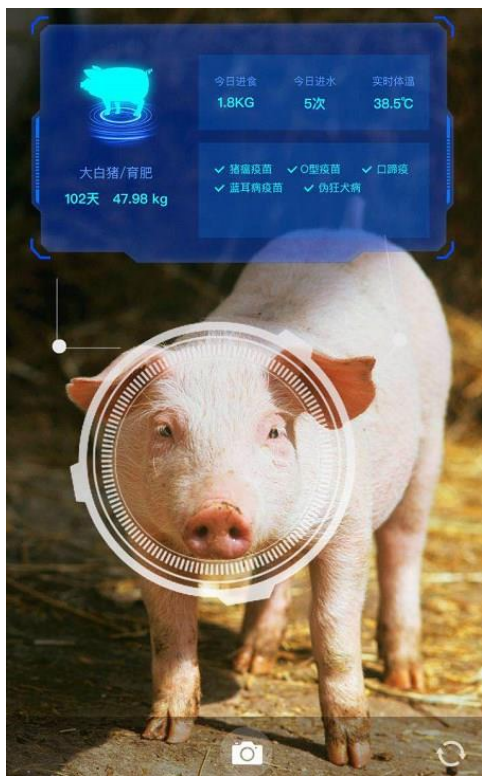
养殖

全流程追溯

猪脸识别

声纹识别

区块链养猪





腾讯区块链案例：电子发票

区块链电子发票是从开具、报销到申报的全流程管理解决方案，“假票真开、真票假开”一直是传统发票的痛点，区块链技术可以实现税款计算和汇缴流程的自动化，从而降低税收征管正本且提高交易数据的安全性。

腾讯区块链电子发票流程



腾讯区块链电子发票整体架构



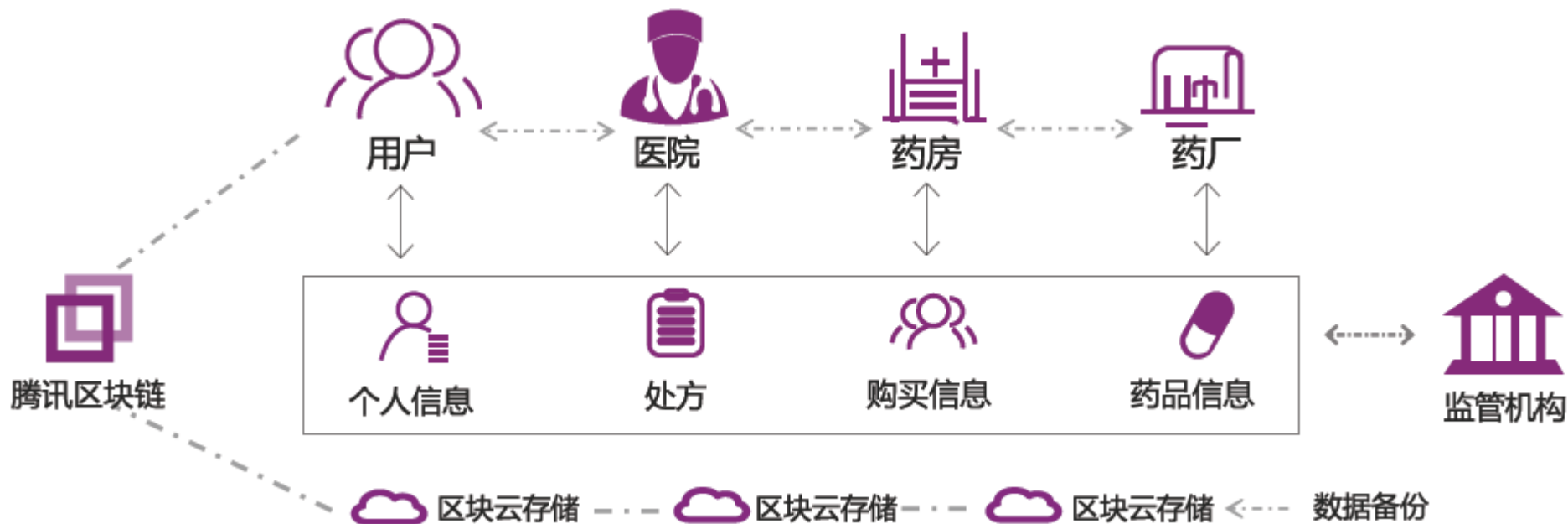
来源：腾讯区块链白皮书



腾讯区块链案例：微信智慧医院3.0计划

微信智慧医院3.0，把所有的知情方全部纳入区块链，过商企实现实时可查可监督，链上的各个节点共享利用，多方存证，实现信息可追溯，保证了链接上的安全。另外，基于腾讯的安全风控管理体系，可以做到安全识别。

腾讯区块链微信智慧医院业务逻辑图



来源：腾讯区块链白皮书

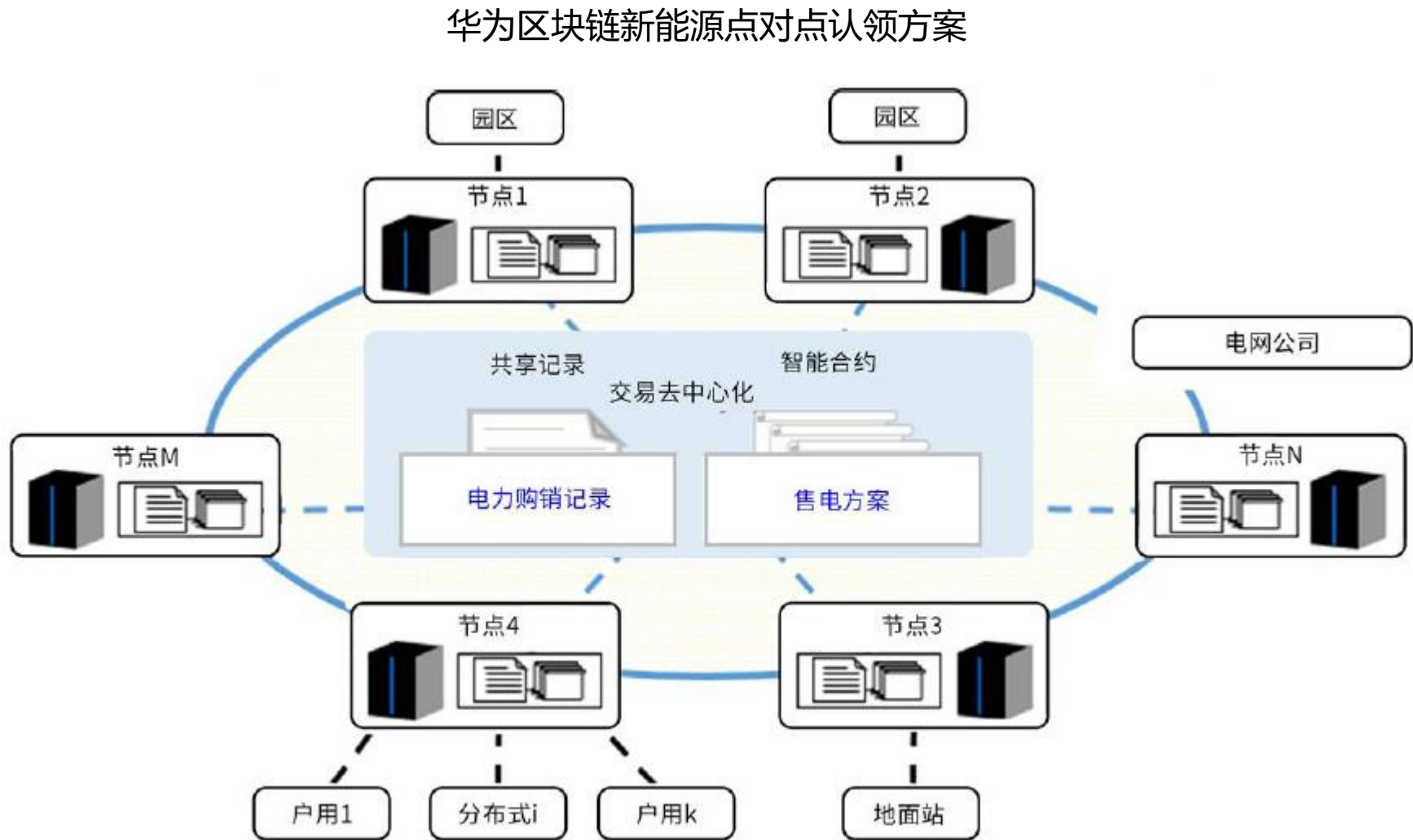


华为区块链案例：新能源点对点认领方案

- 区块链技术能让用户清晰查阅使用的电量来自哪家公司哪个光伏板，自主选择供电来源。
- 智能合约直接配对电站和用户间的认领。

通过认领清洁电力，用户获得权威子证书明其对节能减排做的相关贡献。

发电企业根据用户所提交的用电申请，动态计算各站的供需状态，及时调整发电策略和价格。



来源：华为区块链白皮书



百度区块链案例：莱茨狗

区块链在度小满莱茨狗产品方案中的优势：

- 可追溯
- 通证
- 智能合约

度小满莱茨狗系统



来源：度小满区块链白皮书



Airbnb区块链案例：P2P住宿流程的优化

用区块链解决共享经济中存在的问题

降低双方取信时间成本

在共享民宿经济中，租户和户主为了安全和避免损失，会花费很多时间询问对方信息，取信的时间成本高。区块链技术不可篡改的特性，使双方可对过往交易记录进行查询，大大降低取信时间成本

杜绝虚假交易评价

在中心化平台中，虚假交易和评价盛行，区块链技术不可篡改的特点可以杜绝虚假交易和评价

降低信用担保成本

押金是一种信用制约机制，但押金机制本身更有利于平台商家，提高了消费者消费的信用成本，使得共同的信用风险制约具有不平等性。如果使用区块链技术证明用户的信用，避免押金，则可以降低信用担保成本

智能合约提高交易速度

现有中心化平台中，为避免商家违约风险，商家收款时间和用户付款时间有较长的时间间隔，使用基于区块链的智能合约可以优化现有支付流程



2016年4月，Airbnb收购了一家区块链技术公司ChangeCoin.

在2016年3月与伦敦金融城早报的访谈中，Airbnb的CTO Nathan Blecharczyk表示Airbnb正在考虑使用区块链技术来管理声誉信息，他说：“就Airbnb而言，你的声誉就是一切，而且我认为这只会越来越重要。”



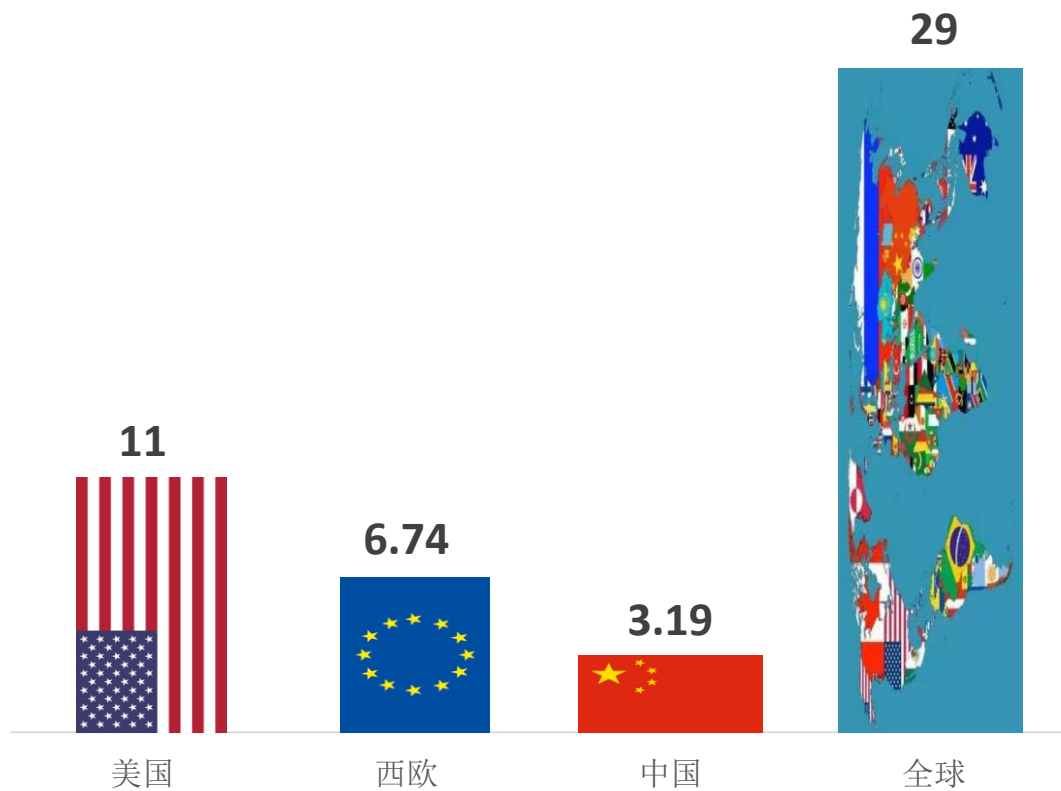
/03

区块链市场发展趋势

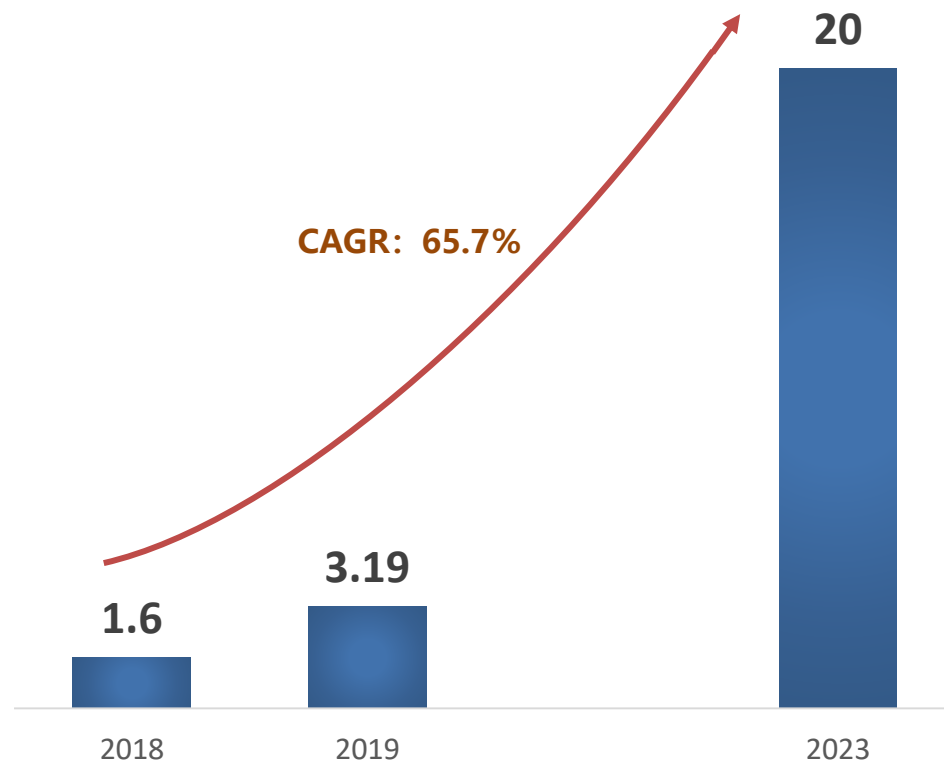


区块链支出将以强劲的速度增长

2019年全球区块链的支出（亿美元）



中国区块链的支出（亿美元）



数据来源：IDC



区块链技术发展阶段：即将走出泡沫破裂期

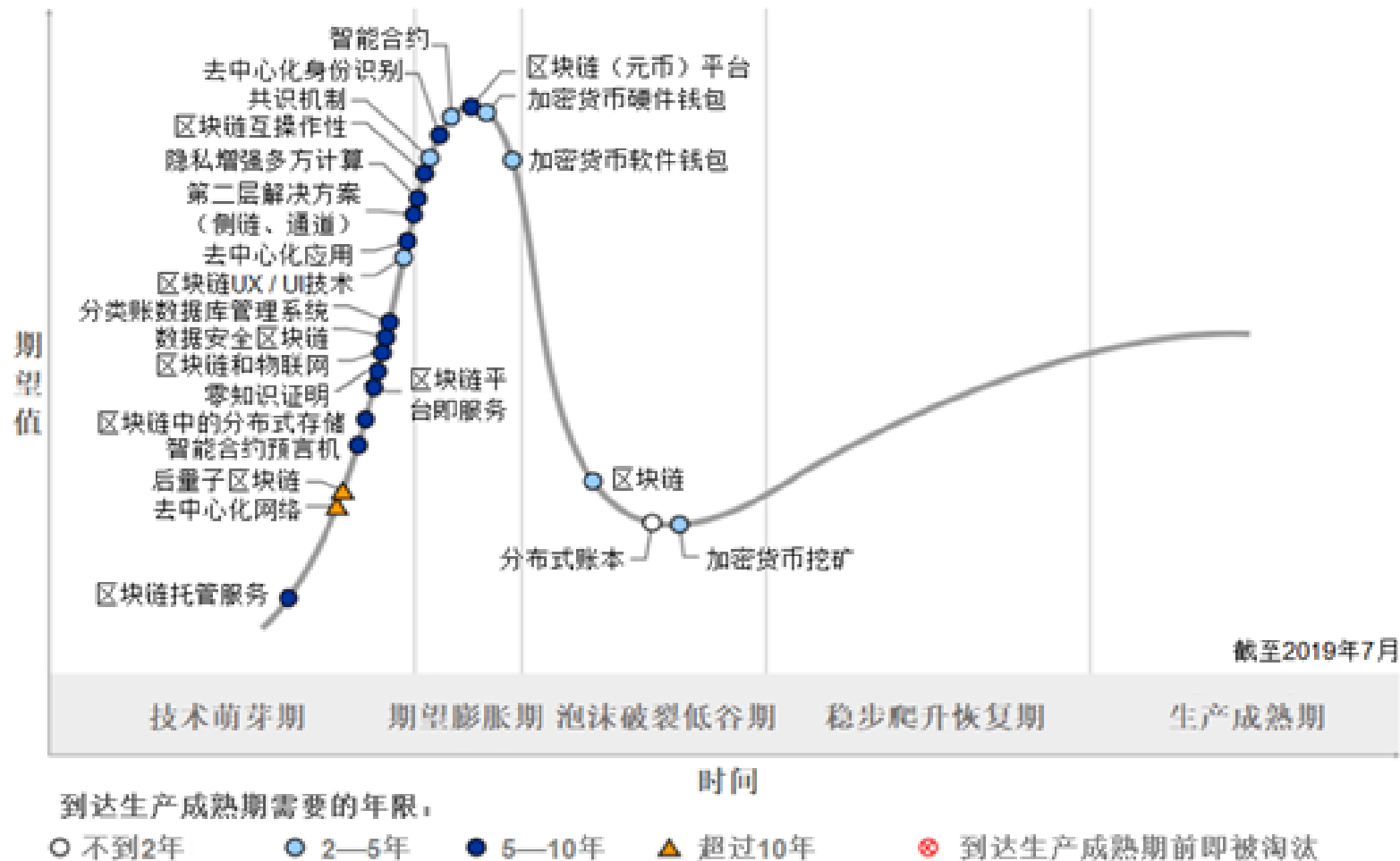
Gartner 2019年区块链科技技术成熟度曲线

2019年区块链科技技术成熟度曲线

Gartner

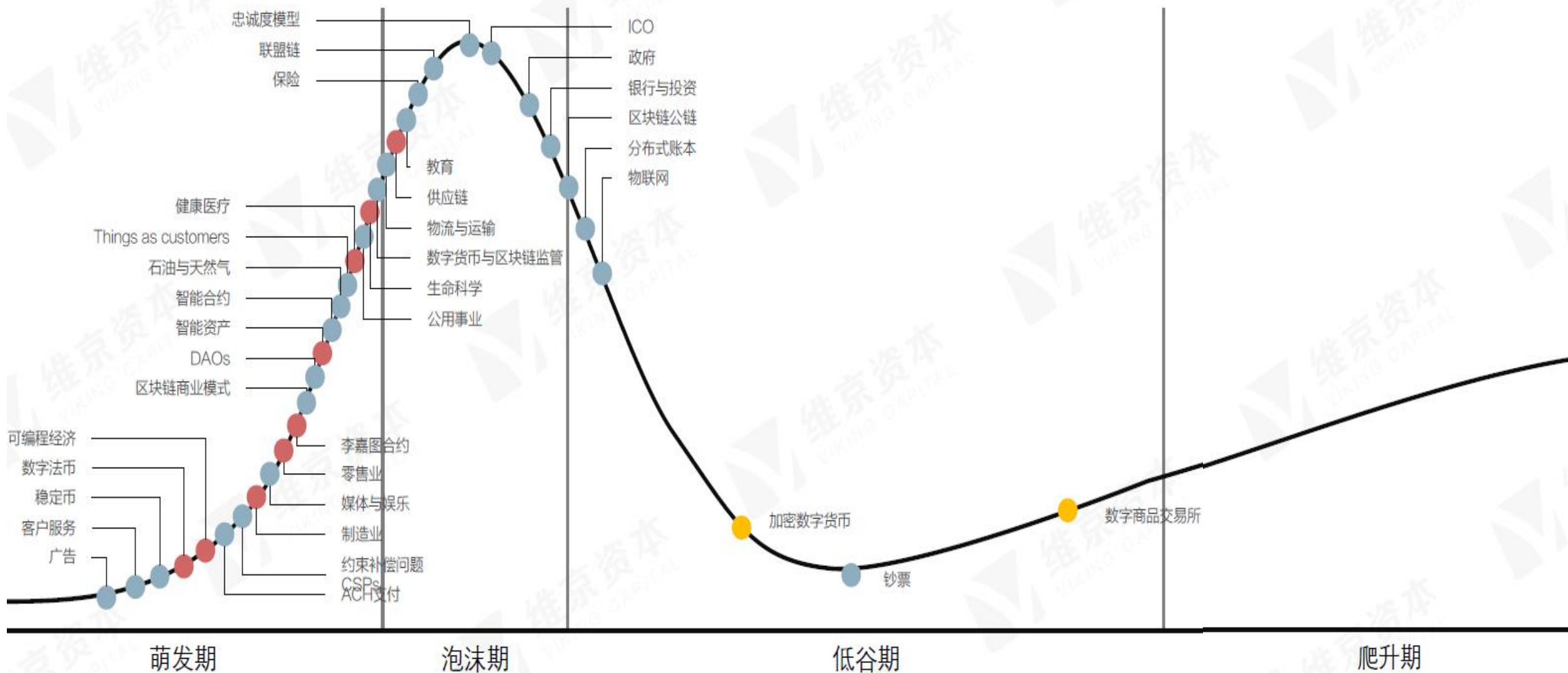
Gartner公布的报告显示，区块链已进入泡沫破裂低谷期。

- 随着科技的进步以及区块链独有实际应用的继续普及，该市场将在2021年脱离泡沫破裂期。
- 到2028年，区块链技术和运营将实现全面扩展。
- 到2030年，区块链技术将产生1.76万亿美元至3.1万亿美元的商业价值。





区块链应用趋势：商业应用处于早期，关键要形成生态



数据来源：Gartner



区块链的行业发展趋势：金融业已经具备落地的条件

■ 底层技术

尽管 2018 中国区块链专利位列世界第一，但整体价值不高，大部分企业围绕加密数字货币、钱包、存证溯源等应用层开展研发工作，较少涉及区块链关键技术。中国区块链底层技术（如共识算法、密码学、跨链）亟待突破。

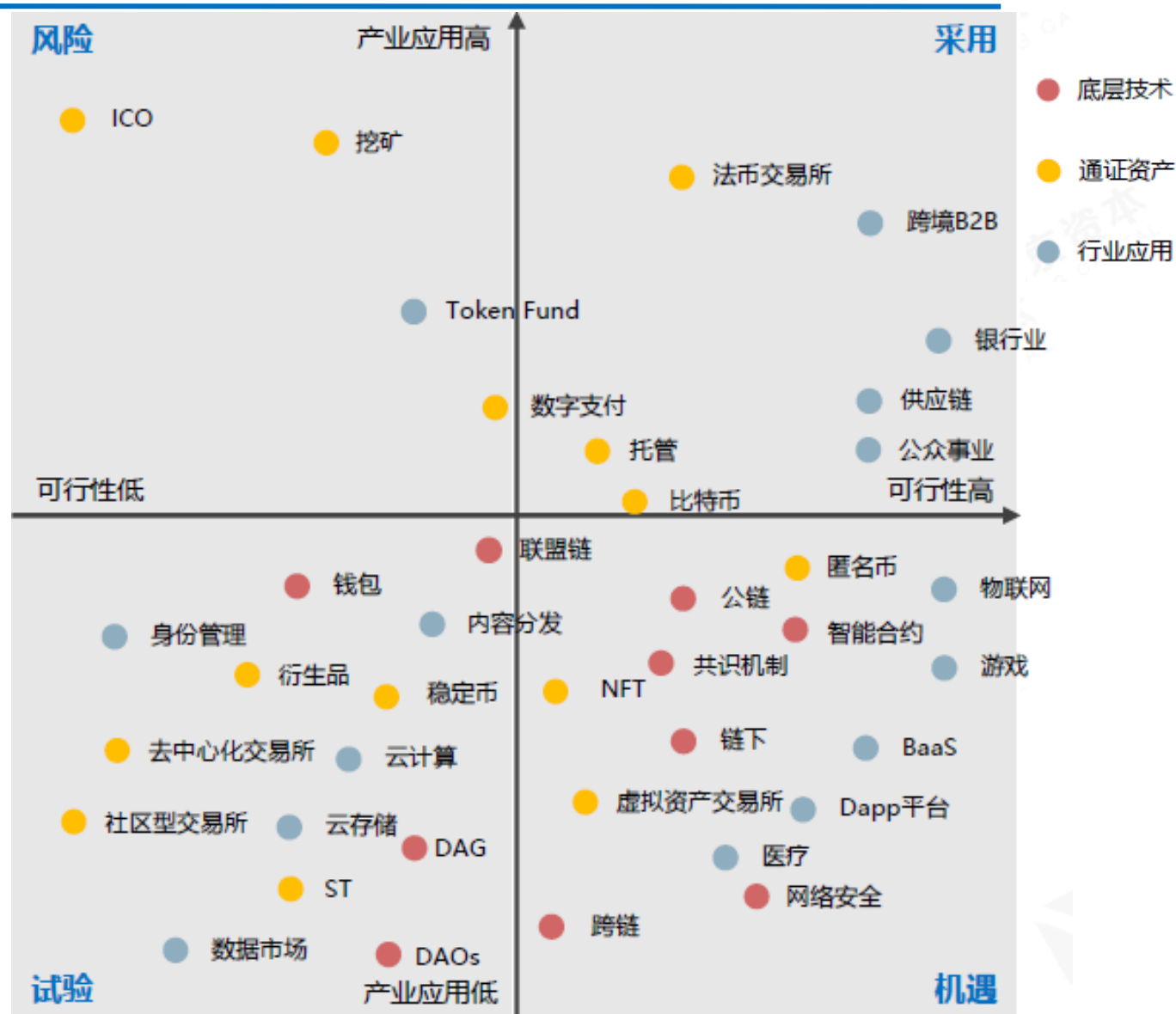
■ 通证资产

资产托管、数字支付、区块链金融已临近大规模应用，而在 NFT、ST、衍生品、匿名币、稳定币方面，尽管具备发展条件，但仍需挖掘广泛的应用场景。

■ 行业应用

银行业、金融业、供应链、物联网以及公众事业已有多年探索并具备较为充分的落地条件，而在游戏、数据、DApp平台等原生数字领域，与区块链技术的结合性高、进展迅速。

数据来源：CBInsights





中国的业界大咖怎样看待区块链发展

□ 周小川（中国人民银行原行长、中国金融学会会长）：

人民银行选择了两个系统做区块链试点，一个是票据交易，一个是贸易融资。前者是因为交易对手方相互了解，相互负责，监管方面没有太多的任务和责任。后者也是因为换手频率相对低。如果不充分重视，并考验新技术的稳定性和可靠性会伤及投资者或消费者。

□ 陈 纯（浙江大学教授、中国工程院院士）：

中国主要的研究热点集中于联盟区块链的关键技术，联盟区块链的关键技术有四：首先是联盟区块链高性能技术，包括高性能的共识算法、高效智能合约引擎，也包括新型的共识机制；第二是区块链安全隐私关键技术；第三是高可用性的关键技术；第四是高可扩展的关键技术。

□ 盛松成（中国人民银行参事、中国人民银行调查统计司原司长）：

区块链来说，最重要的是实际应用的落地，为实体经济服务。区块链最不适合应用的领域就是货币领域，区块链的应用最好不要集中在金融领域。如果区块链必须与虚拟货币联系在一起，那么区块链这种技术我认为，是没有前途的。

□ 任泽平（恒大经济研究院院长）：

在高速发展同时，区块链（尤其是大型公链），还需要面对交易性能偏低、安全性隐患、标准尚未统一、监管政策不完备等诸多技术、商业与监管方面的挑战。这正说明技术本身仍然处在从0~1的初始阶段。



Thanks