区块链应用分析

朱其苗 2018.03

什么是区块链？

区块链在国内外的发展

典型案例

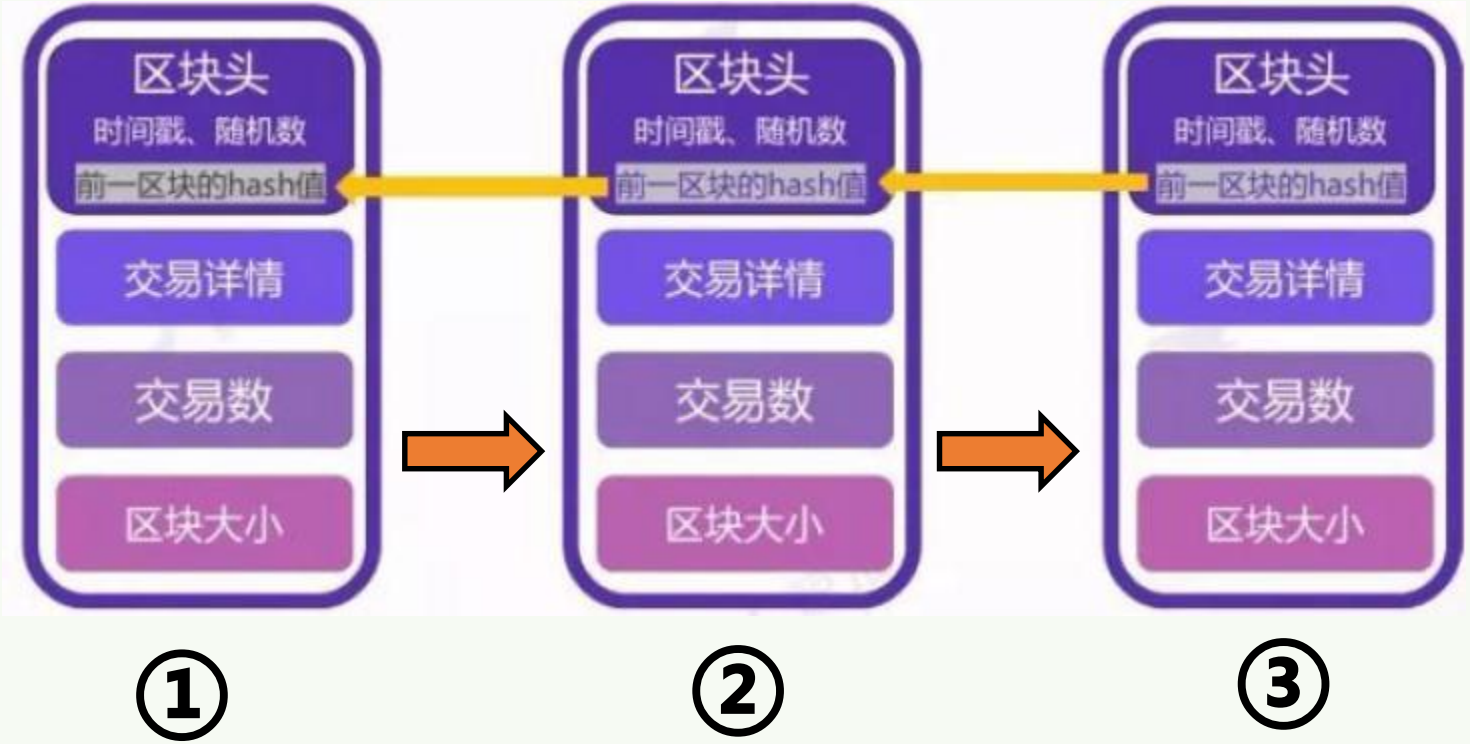
趋势、机遇与挑战

区块链应用分析

朱其苗 2018.03

01 什么是区块链？

比特币的底层实现技术
本质是一个去中心化的数据库账本



把数据分成不同的区块，每个区块通过特定的信息链接到上一区块的后面，前后顺连，呈现一套完整的数据。

每一个区块都会包含时间、地点、场合等信息，来保证区块里面交易信息的独一无二性。

多方独立拷贝存储，区块链系统的每个节点都存储同样信息。容忍少于1/3节点恶意作弊或被黑客攻击，系统仍然能够正常工作。

比特币交易

比特币交易平台

现金流

比特币 每10分钟产生一个区块，每个区块50个比特币

挖矿 计算（猜）最后一个区块的HASH值，猜中者得

矿机 用来挖矿的机器（CPU/GPU/FPGA/ASIC）

矿场 自己买来一批机器，自己租个场房

矿池 租个场房，大家把机器放进来，共享收益

什么是区块链？

传统数据库：
读写权限掌握在一个公司或者一个集权手上（中心）

区块链：
任何有能力架设服务器的人都可以读写其中内容

什么是区块链？

技术起源

- P2P、加密、数据库技术、电子支付

1.0

- 分布式账本、块链式数据、梅克尔树、工作量证明

2.0

- 智能合约、虚拟机、去中心化应用

什么是区块链？

区块链系统根据应用场景和设计体系的不同，一般分为**公有链**、**联盟链**和**专有链**。

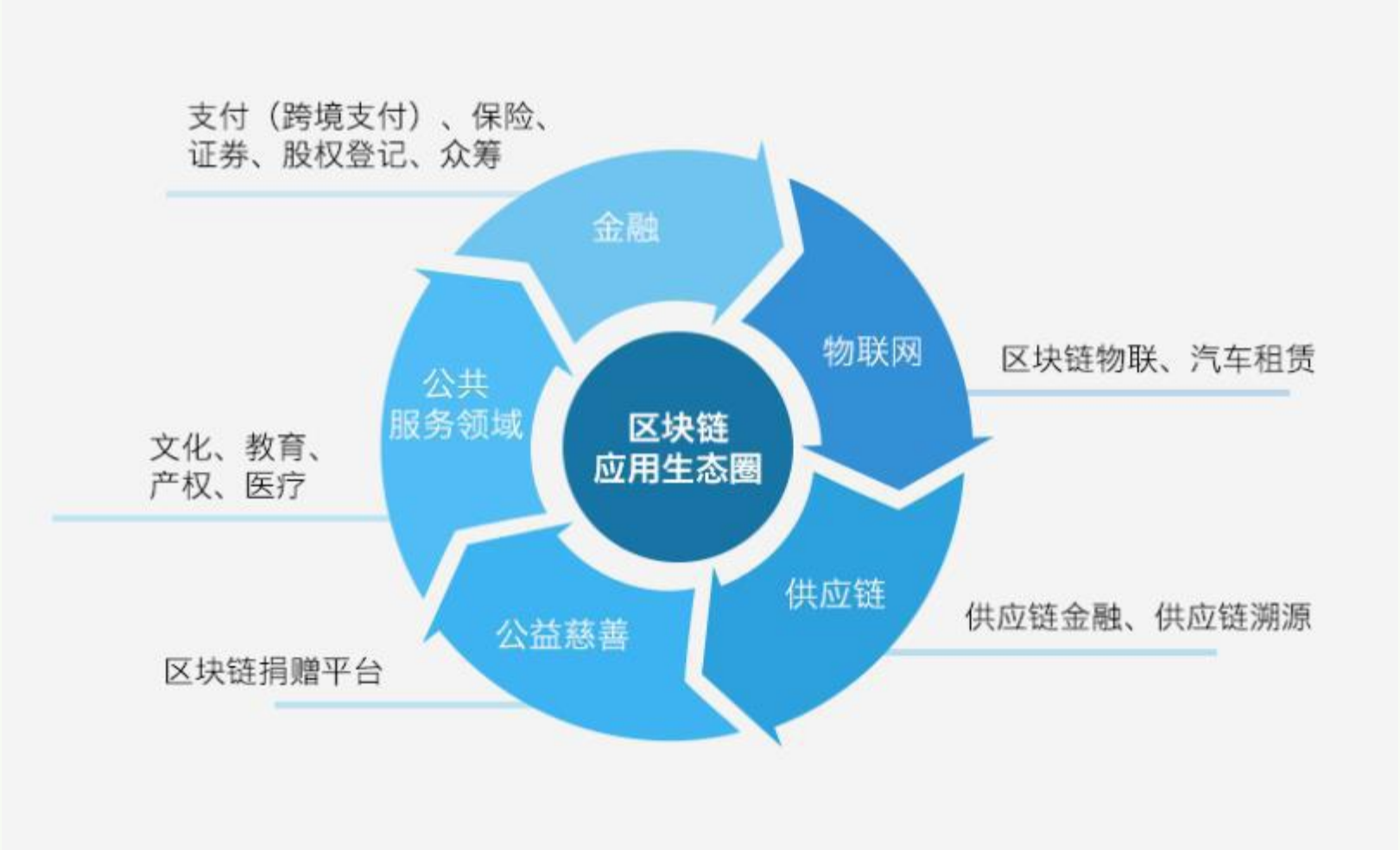
公有链。任何人都可加入网络及写入和访问数据,任何人在任何地理位置都能参与共识,每秒3 - 20次数据写入。

联盟链。授权公司和组织才能加入网络参与共识、写入及查询数据都可通过授权控制，可实名参与过程，可满足监管AML/KYC，每秒1000次上数据写入。

私有链。使用范围控制于一个公司范围内改善可审计性，不完全解决信任问题，每秒1000次以上数据写入

什么是区块链？

- 目前，区块链的应用已从单一的数字货币应用，例如比特币，延伸到经济社会的各个领域。比如金融服务、供应链管理、文化娱乐、智能制造、社会公益、教育就业等
- 但是除金融服务行业的应用相对成熟外，**其他行业的应用还处于探索起步阶段。**

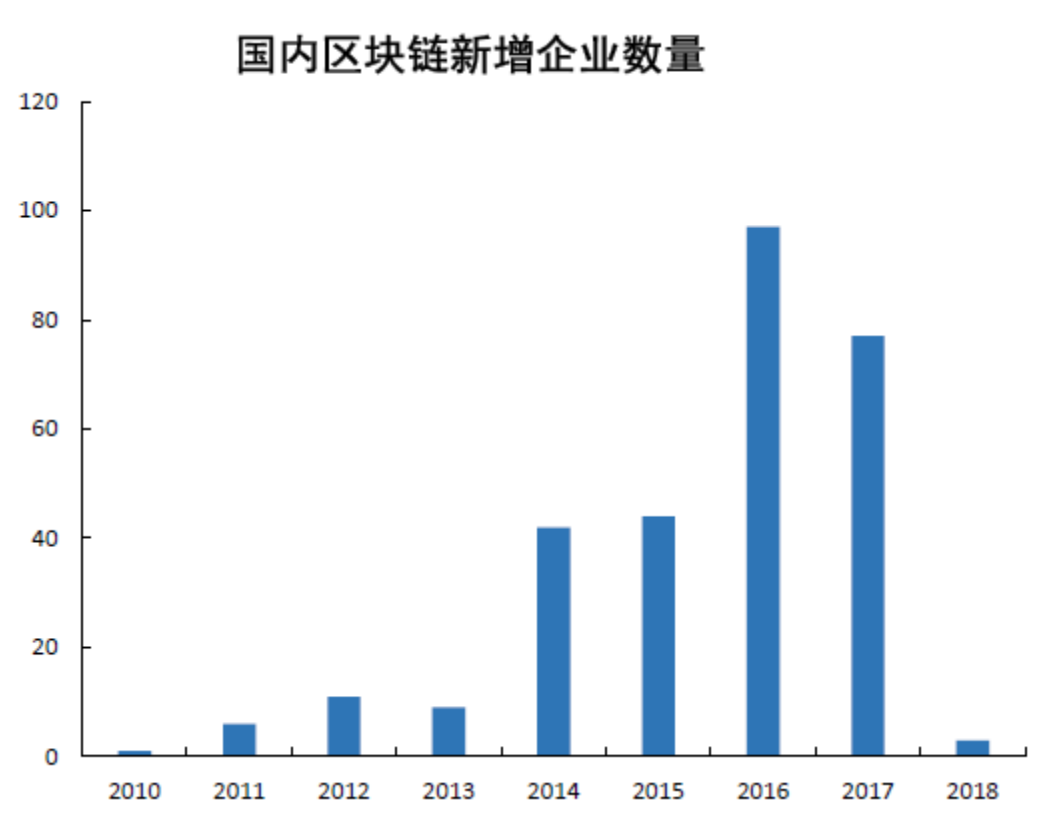


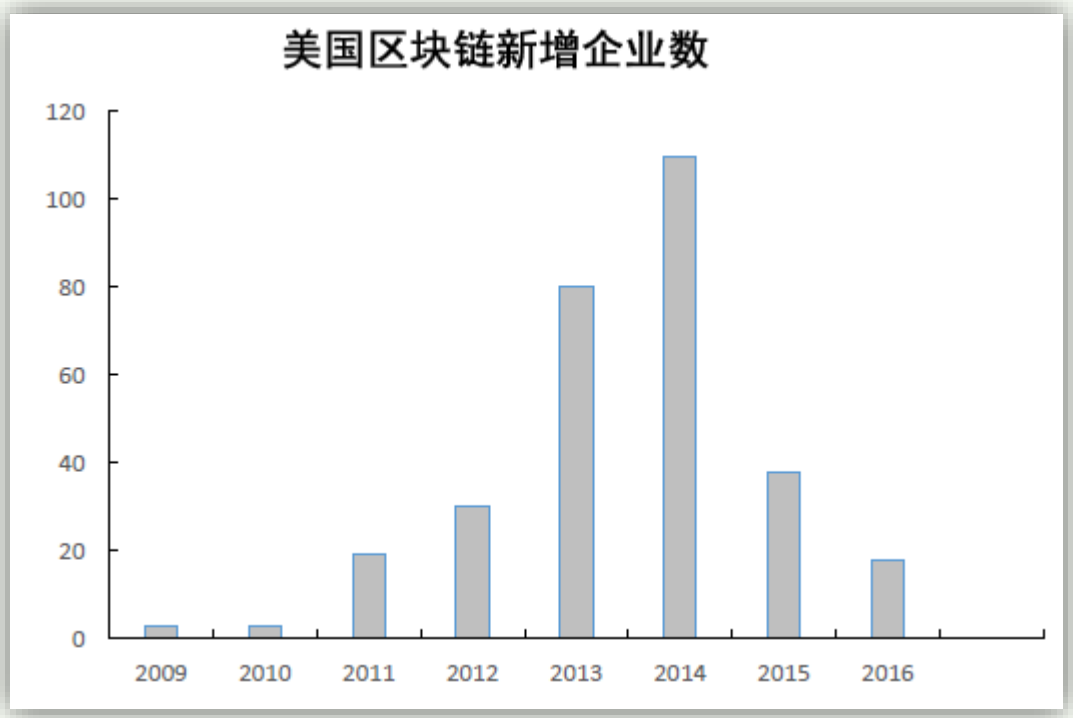
区块链

- P2P加密
- 去中心化
- 智能合约
- 分布式
- 数据库账本

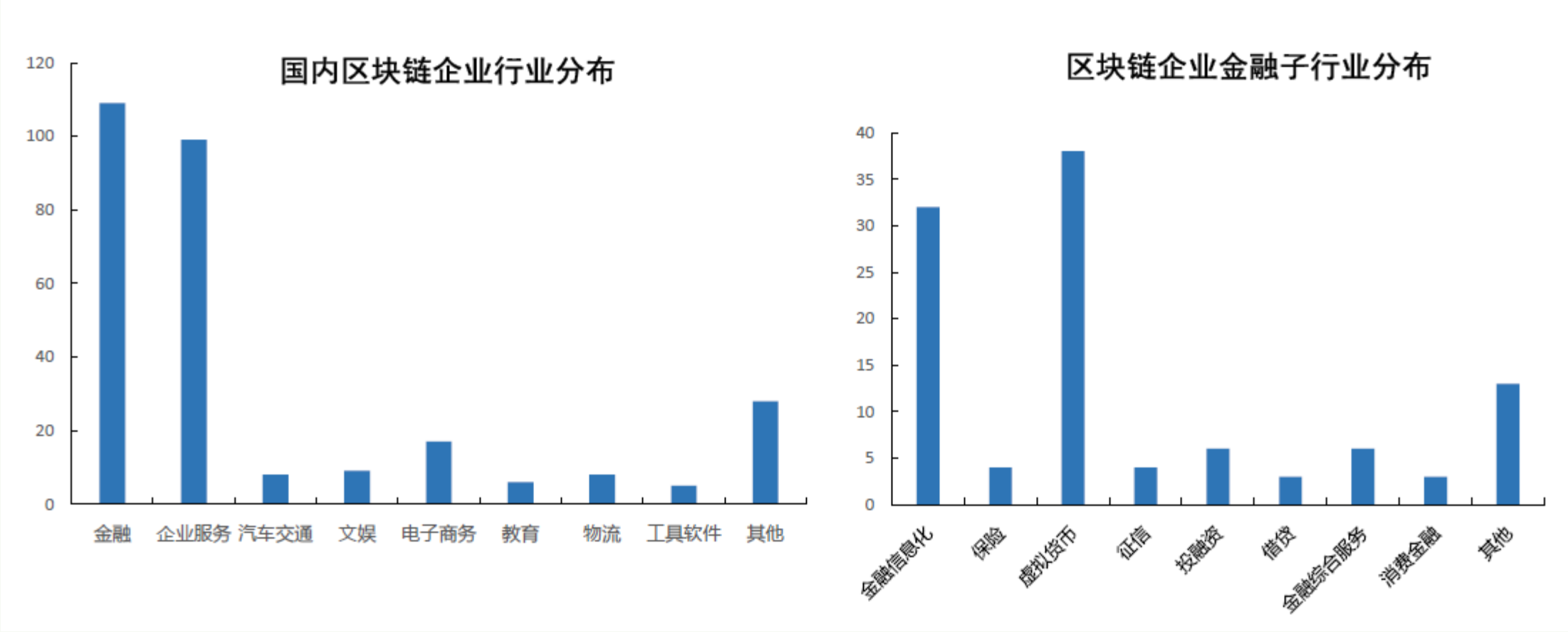
02 区块链在国内外的发展

区块链在国内外的发展


国内区块链新增企业数量
120
100
80
60
40
20
0
2010
2011
2012
2013
2014
2015
2016
2017
2018


美国区块链新增企业数
120
100
80
60
40
20
0
2009
2010
2011
2012
2013
2014
2015
2016

区块链在国内外的发展


国内区块链企业行业分布
120
100
80
60
40
20
0
金融
企业服务
汽车交通
文娱
电子商务
教育
物流
工具软件
其他
区块链企业金融子行业分布
40
35
30
25
20
15
10
5
0
金融信息化
保险
虚拟货币
征信
投融资
借贷
金融综合服务
消费金融
其他

融资及变现方式：

制造售卖矿机

搭建矿池平台

第三方交易平台_交易抽佣

风险投资（VC）

售卖头部代币

国家政策：


加拿大
美国
墨西哥
巴西
英国
俄罗斯
中国
日本
韩国
印度
新加坡
澳大利亚
蒙古国
支持
态度不明
限制
禁止
美国：
各州自有规则
美国50个联邦州执行各自规则，金融监管部门态度相左。
英国：
监管观望
英国金融市场行为监管局未禁止ICO。ICO者自行承担法律风险。
俄罗斯：
反对加密货币
加密货币为金融工具非货币，正在构建ICO的监管框架。
中国：
全面禁止ICO
央行等联合发布《关于防范代币发行融资风险公告》ICO为非法行为。
日本：
允许ICO
日本交易所集团（JPX）牵头成立区块链联盟

BAT都做了啥？

蚂蚁区块链

公益

公益资金流向全程记录，公开透明，不可篡改，
实现高公信力的阳光账本。

供应链管理

覆盖溯源全链条，多方比对验证确保数据完整可
信，向监管透明，让用户放心。

BAT都做了啥？


腾讯区块链
TrustSQL
具体区块链应用
银行
保险
证券
供应链
商业积分
其他
行业解决方案
数字票据
数字黄金
机构清结算
网络互助
知识产权保护
应用服务层
Trust Application
平台产品服务层
Trust Platform
数字资产
鉴证服务
共享账本
分享经济
底层平台
Trust SQL
用户管理
账户管理
权限管理
密匙管理
风控审计
基础服务
接口适配
共识管理
网络通信
记录存储
智能合约
合约注册
合约执行
合约触发
升级注销
运营监控
配置
可视化
告警
监控
发布
云适配

BAT都做了啥？

BaaS
BlockChain as a Service

灵活可定制、易落地

依据企业实际业务场景，可对区块链各项目属性、模块和机制进行定制及灵活配置

安全

采用包括非对称加密、签名、证书认证、审核、权限控制、隔离、共识机制等在内的技术方案，全面保证数据、通讯的安全可靠

高性能

支持高并发、低延迟的实时区块写入和查询；同时支持多副本复制、多实例部署，并通过一致性算法保证数据一致性

开放共建

平台与底层集群设施，对外开放、共建

去中心化

去中心化与弱中心化灵活切换

有限信任

企业级信任模型

03 典型案例


底层技术及基础设施层
基础协议
匿名技术
区块链硬件
通用应用及技术扩展层
智能合约
快速计算
挖矿服务
信息安全
数据服务
BaaS
解决方案
防伪溯源
垂直行业应用层
金融
房地产金融
企业金融
证券服务
支付
票据金融
名人金融
保险
资产管理
……
数字货币
钱包
投资
交易
娱乐
直播
游戏
虚拟偶像
音乐
供应链
物流
解决方案
医疗
药品溯源
健康管理
法律
版权保护
证据保全
智能合同
能源
数字化管理
电网
能源交易
公益
善款追溯
公益寻人
社交
聊天工具
社区
其他
物联网
农业

基础协议层

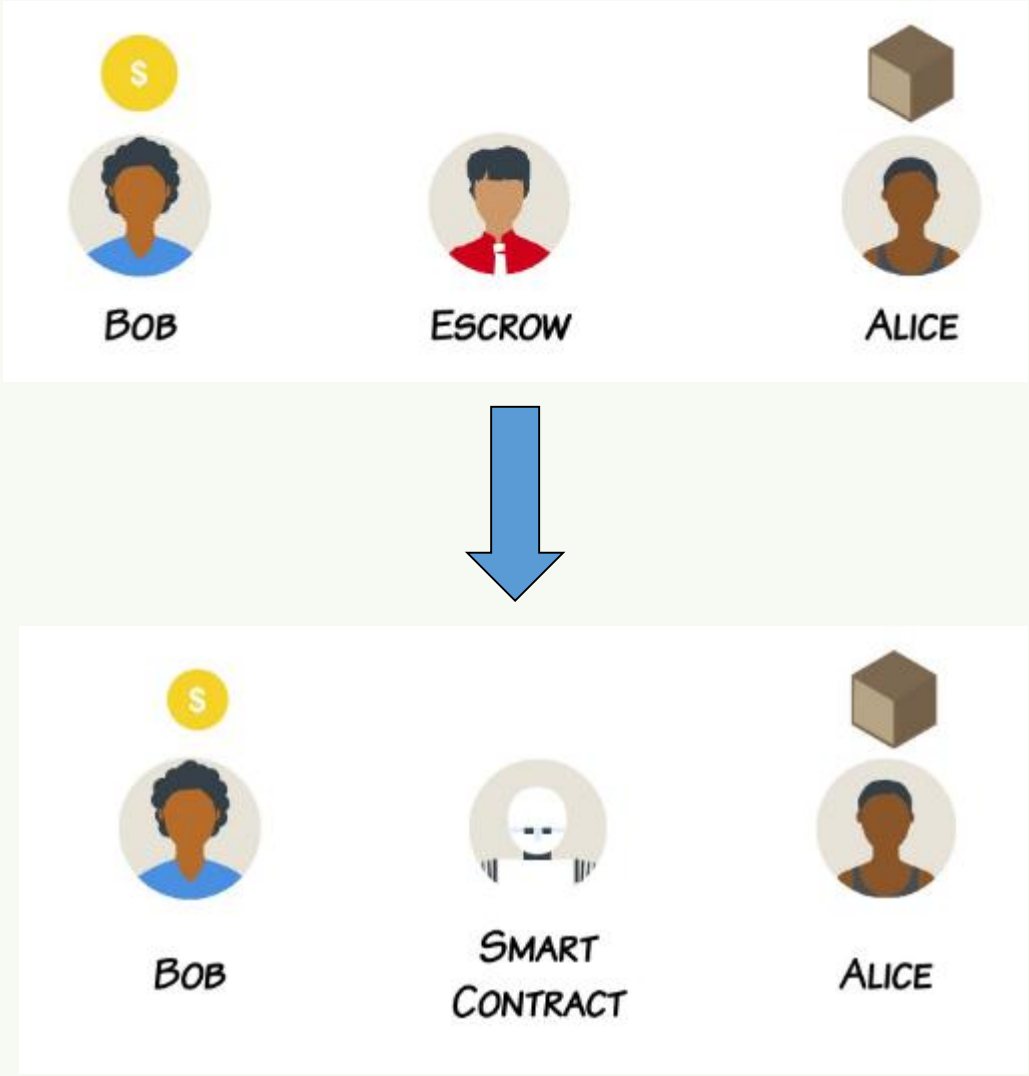

基础协议
NEO
小蚁
量子链
以太坊
莱特币
比特币
ValueCyber
Hyperledger
EOS
IOTA
Tether
Nebulas
BYTOM
比原链
万象区块链
Nebulas
星云链


匿名技术
Zcash
Monero
Dash
Zerocoin
Spectrecoin


硬件
极路由
比特大陆
嘉楠耘智
ROCKMINER
RockMiner

数字资产 + 智能合约

以太坊



NEO
smart economy

数字资产 + 数字身份 + 智能合约

NEO底层支持多种数字资产，用户可在NEO上自行注册分发资产，自由交易和流转。

支持数字证书，解决公有链信任问题，利用数字证书可以合法合规地在区块链上发行资产并且享受法律保护。

超导交易机制，可以实现去信任的数字资产交易所，在无需充值的情况下对各类数字资产进行撮合。

图灵完备的智能合约，在NeoVM中执行并且拥有确定性、可终止性、资源控制、并发、分片与无限扩展等众多优点。

NEO智能支持用C#、Java、Phthon等编程语言来开发，开发者无需学习新语言即可快速开发基于NEO区块链的智能合约。

NeoVM：NEO轻量级基于堆栈的虚拟机，拥有快速的启动时间和较高的执行效率，配合“确定性调用树”技术，可以实现理论上无限的扩展性。

独创的dBFT共识机制，共识节点之间通过拜占庭容错算法来达成共识保障交易最终性，并且可以保障小于三分之一的节点出现拜占庭故障时系统仍然拥有最终性和可用性。

跨链互操作协议，包含跨链资产交换协议和跨链分布式事务协议，可以实现多个区块链之间的原子级资产交换，还可以在多个区块链上共同执行智能合约并保证事务一致性。

引入基于Lattice（格密码学）的签名与加密技术，将加解密问题规约到量子计算机尚无法解决的SVP（最短向量）问题，从而预防“量子危机”。

区块链匿名：

比特币，以太币：你知道每笔交易发生的时间，交易双方是谁、金额、IP地址等；

有了它，你可能知道发生了一笔交易，但是不知道这笔交易在哪里发生、涉及多少钱及资金流向哪里。

极路由

路由器，升级，区块链路由器（存储和计算节点）

BITMAIN

Canaan

ROCKMINER

RockMiner

基础协议层的项目关键：

- 区块链2.0向3.0升级，现有底层的协议大部分要被淘汰

  2.0 ：智能合约、虚拟机、去中心化应用
  3.0： 全领域生态应用及**垂直**行业**商业应用**，更高的**性能**要求

- 人才匮乏、开发周期长、技术实现难度高

应用服务层

快速计算

在底层区块莲的基础上进行优化，借以解决底层区块链固有的一些问题，如提高区块链的计算速度。

智能合约

智能合约可编程化
让智能合约编程更容易，提升合约执行能力

信息安全

安全+智能合约

数据服务

数据共享、数据保护为主要切入点

应用服务层

区块链云服务平台

为特定商业场景提升完整解决方案

数据货币

产品信息区块链

供应链-应收款融资

满足借款人因应收款占用造成短期流动资金不足的融资需求，优化客户财务报表。

了解更多>>

供应链-票据融资

让票据持有人能够快速地利用票据进行融资，提高了票据流转的高效性和安全性。

了解更多>>

供应链-授信融资

真实记录企业信用信息，借款方便灵活；降低企业筹资成本，提高财务工作效率。

了解更多>>

区块链合同存证

在线签订合同，使用电子签名技术保证合同具有法律效力，合同记录真实可靠。

了解更多>>

预付卡系统

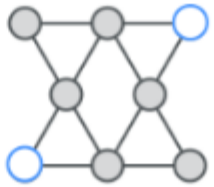
整合多家商户资源，让用户方便地使用一个APP在不同地店家间兑换服务。

了解更多>>

资产数字化

将实体资产通过智能数字化的方式更加便利的进行资源共享。

了解更多>>



积分联盟系统

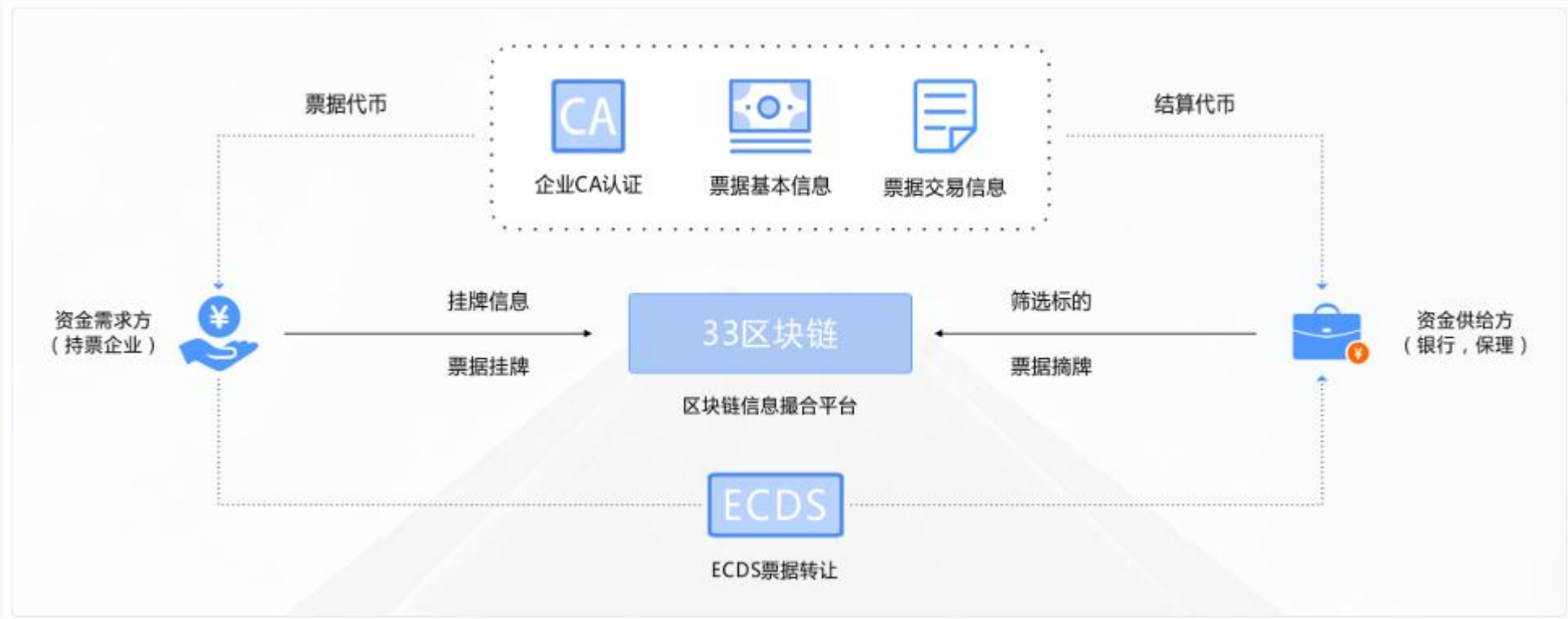
使用区块链技术记录积分的信息，让积分有效地流通，提升积分利用率。

了解更多>>

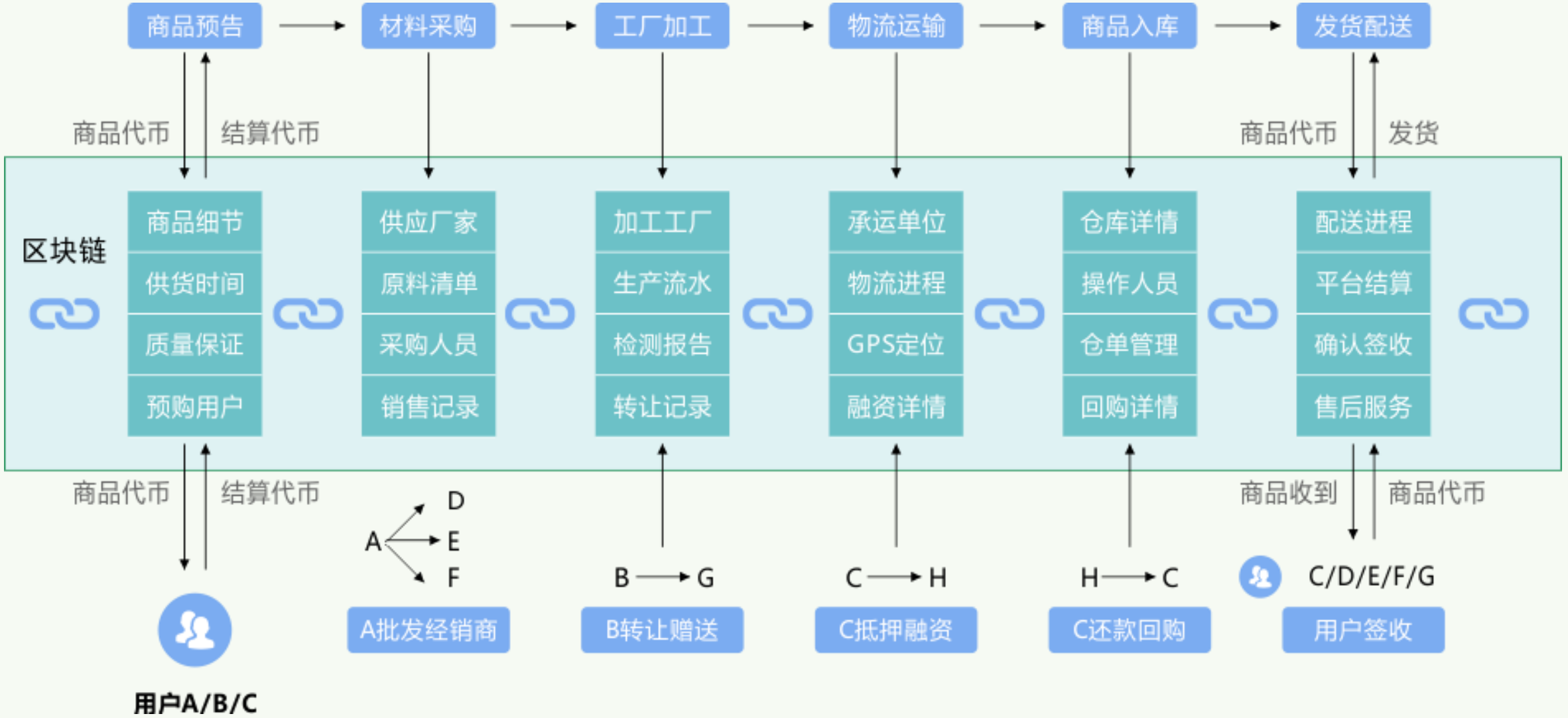
商品生命周期跟踪

从商品的预告、生产到配送都写入区块链内，最大程度地保证商品质量可控。

了解更多>>



票据融资


商品预告
材料采购
工厂加工
物流运输
商品入库
发货配送
商品代币
结算代币
商品代币
发货
区块链
商品细节
供货时间
质量保证
预购用户
供应厂家
原料清单
采购人员
销售记录
加工工厂
生产流水
检测报告
转让记录
承运单位
物流进程
GPS定位
融资详情
仓库详情
操作人员
仓单管理
回购详情
配送进程
平台结算
确认签收
售后服务
商品代币
结算代币
商品收到
商品代币
A
D
E
F
B → G
C → H
H → C
C/D/E/F/G
用户A/B/C
A批发经销商
B转让赠送
C抵押融资
C还款回购
用户签收

最大的分布式账本联盟

银行业区块链组织

基于比特币

可编程智能合约
即时支付
倾向种类、系统可扩展性

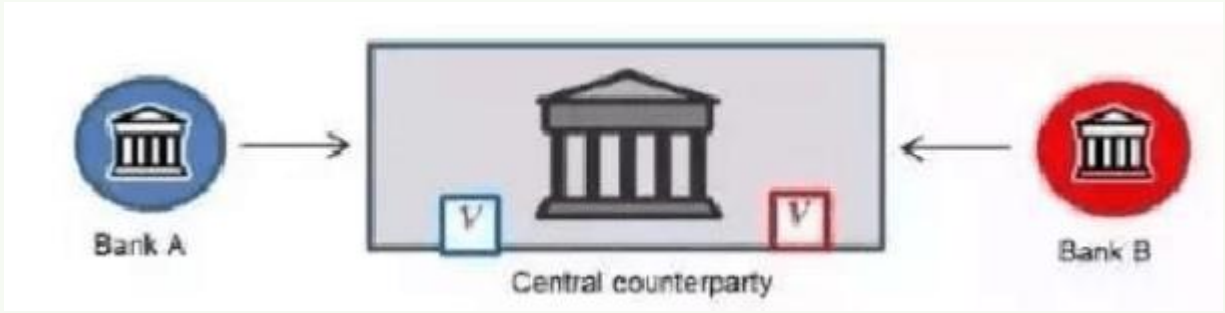
物联网区块链
连接并控制智能硬件

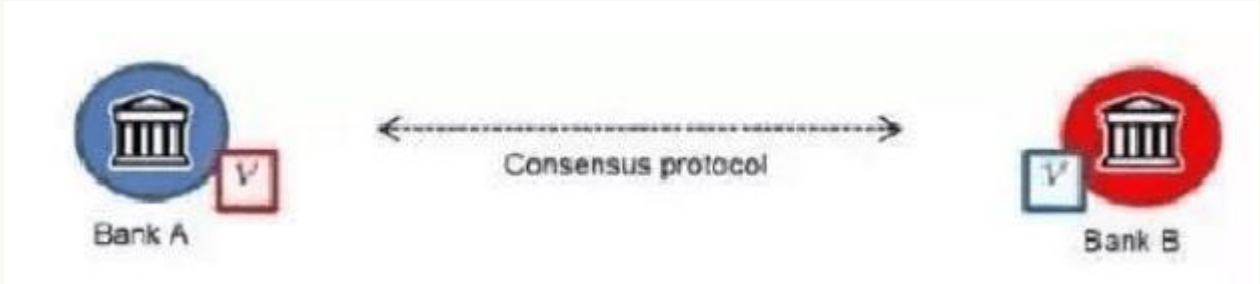
行业应用层：


底层技术及基础设施层
基础协议
匿名技术
区块链硬件
通用应用及技术扩展层
智能合约
快速计算
挖矿服务
信息安全
数据服务
BaaS
解决方案
防伪溯源
垂直行业应用层
金融
房地产金融
企业金融
证券服务
支付
票据金融
名人金融
保险
资产管理
……
数字货币
钱包
投资
交易
娱乐
直播
游戏
虚拟偶像
音乐
供应链
物流
解决方案
医疗
药品溯源
健康管理
法律
版权保护
证据保全
智能合同
能源
数字化管理
电网
能源交易
公益
善款追溯
公益寻人
社交
聊天工具
社区
其他
物联网
农业

区块链 - 支付

雷达支付 REMITSY 质数金服 DECENT区块链

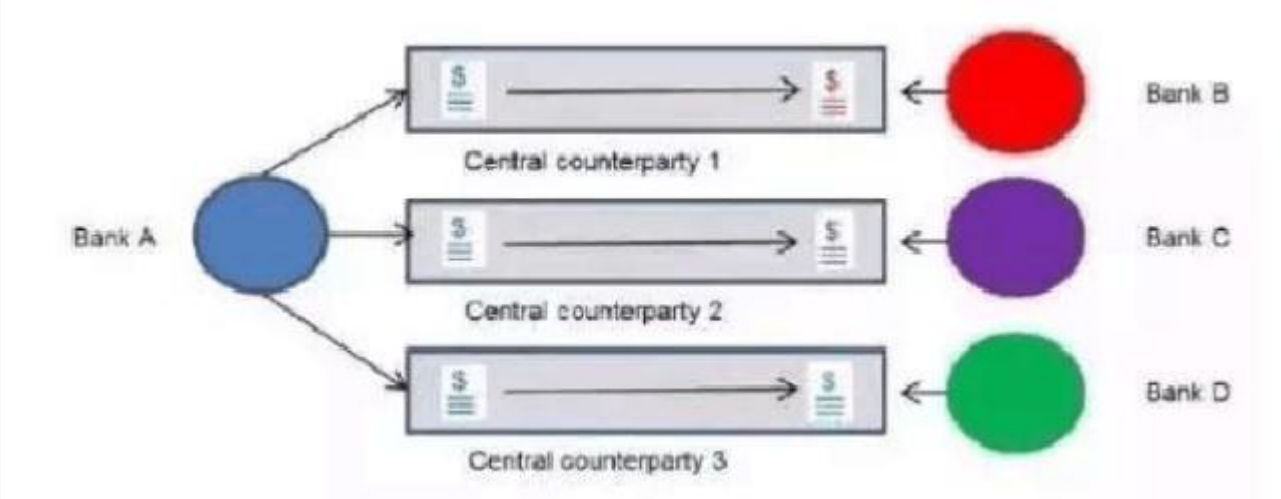


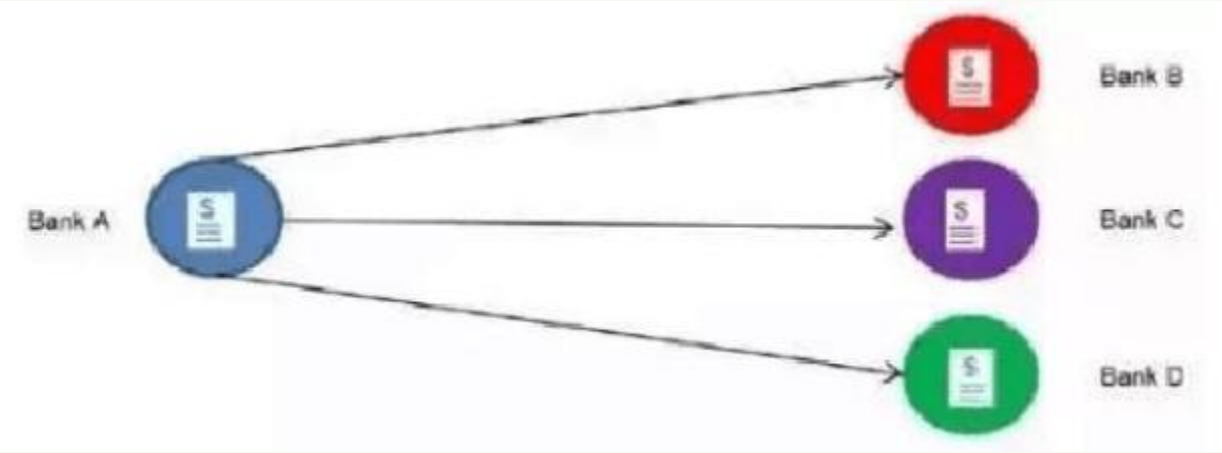


支付清算模式：由智能合约系统完成交易清算，未来的挑战在于风控

交易撮合：银行撮合变成智能合约自动撮合

区块链 - 支付





银行间交易模式变革：由多关联方交易变为直接交易

区块链 - 支付

雷达支付 REMITSY 质数金服 DECENT区块链

RADR Laboratory

- 人民币
- 欧元
- 英磅
- 美元
- 马来西亚币

ICO：

- VRP — 交易手续费
- VBC — 推广佣金奖励

挑战：

1、道德犯罪
2、外汇管理，货币政策
3、数字货币总量
4、中心化与中心化对抗
5、分布式存储与算力的资源消耗

区块链 - 数字货币

币发行：

币交易：

矿机商城：

区块链 - 供应链管理

Crowdz 唯链 物链

vechain

全球最早期的区块链技术公司，顶级的区块链团队

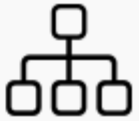
奢侈品，酒类，农业，汽车等多行业的区块链项目落地实施经验

在法国，新加坡，香港等多个国家和地区设立了分支机构，拥有海外项目实施能力和经验

通过商品管理平台将商品上链

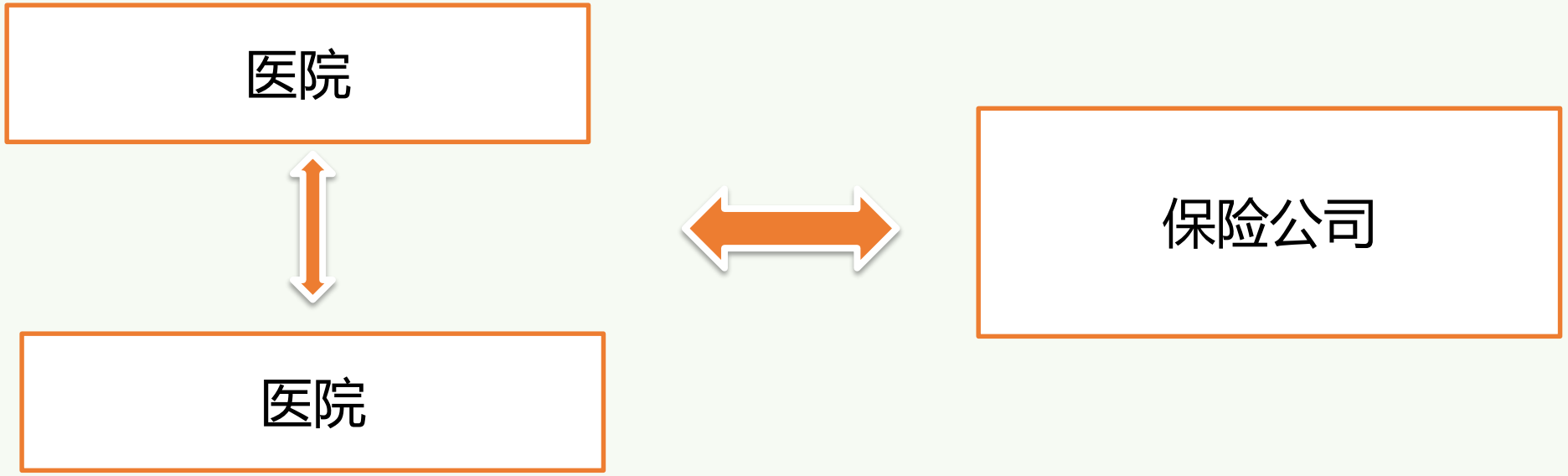
物流服务方扫码操作进行物流信息上链

通过销售管理平台对售出商品转移所有权



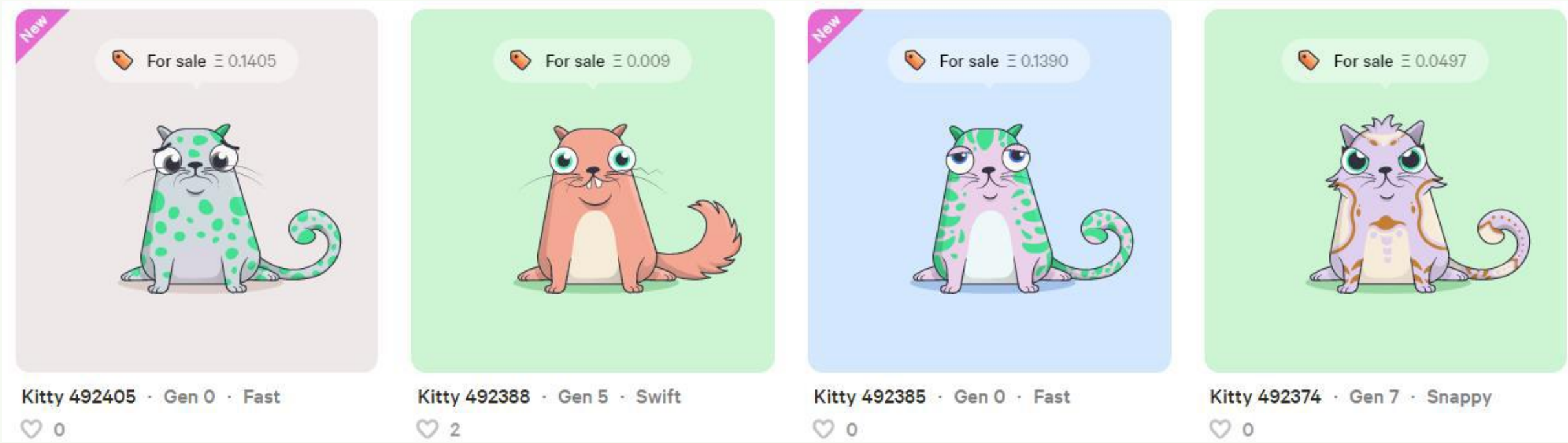
消费者验证真伪并宣告所有权

区块链 - 医疗



区块链 - 游戏

CryptoKitties。世界上最早的区块链游戏之一。是基于以太坊平台的一个养殖类游戏，发明者设定了100只创始猫，它们都带有各自的不同基因（每只猫有256种），然后出售给用户，用户可以自相繁殖，或者跟其他人的猫繁殖。因此可以产生下一代，而每一只猫所带有的基因都不会完全一样（按照算法可产生40亿种不同组合），从而呈现出不同的外貌，每一只猫都是唯一的，因此其价格也不一样。这个游戏的交易以以太币交易，在交易所里可以与现金兑换，以太币的价格本身也会影响猫的价值，可变现又让它成为像股票一样的资产。

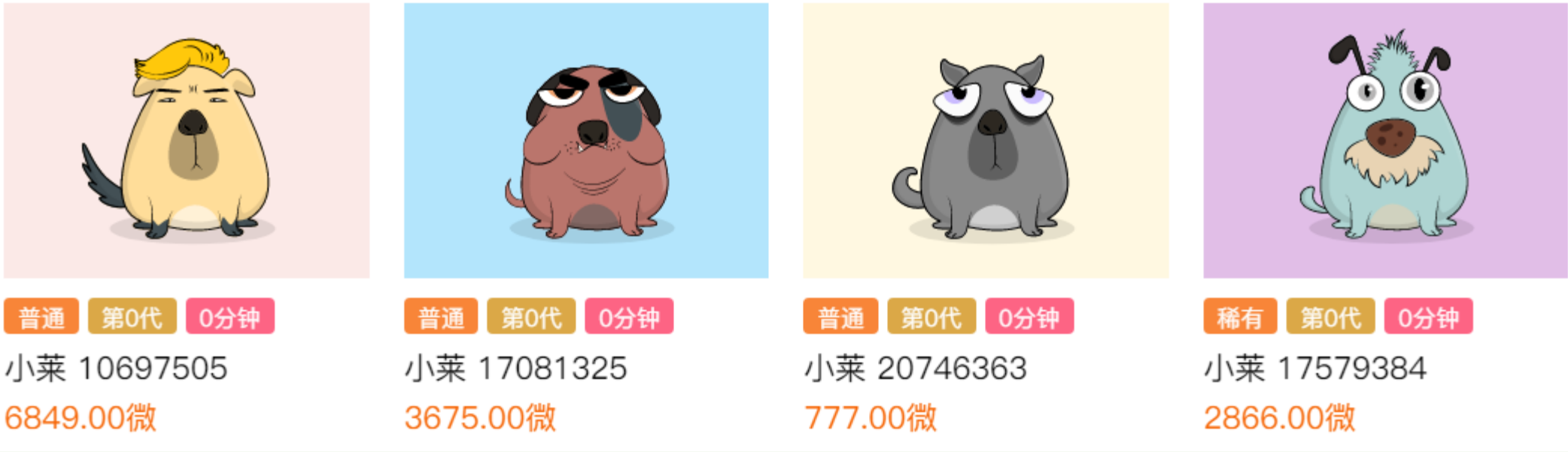


“零代”猫咪大约每15分钟产生一只！照顾不周的猫咪要生病。配种繁育，领养，购买都要花虚拟币。

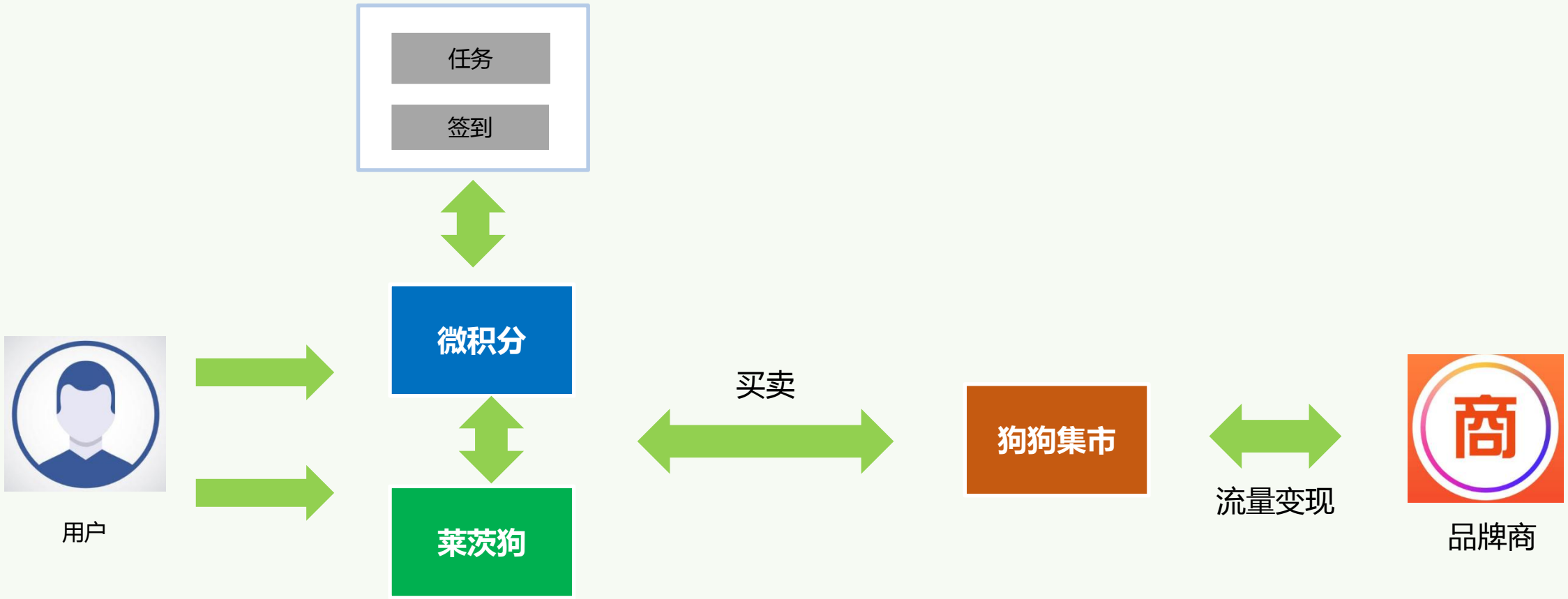
区块链 - 游戏

莱茨狗，百度推出区块链游戏项目，提供形态各异的虚拟宠物狗供领养，每只都有独一无二的基因。每只莱茨狗被系统冠以体型、花纹、眼睛、眼睛色、嘴巴、肚皮色、身体色、花纹色这8个外貌特征，每个特征有两种不同的属性：稀有属性和普通属性。这些属性组合起来，将会决定宠物狗最终的稀有等级，包括普通、稀有、卓越、史诗、神话、传说。

百度金融区块链实验室数字狗仅在内部测试阶段，是区块链技术应用领域的一次尝试。



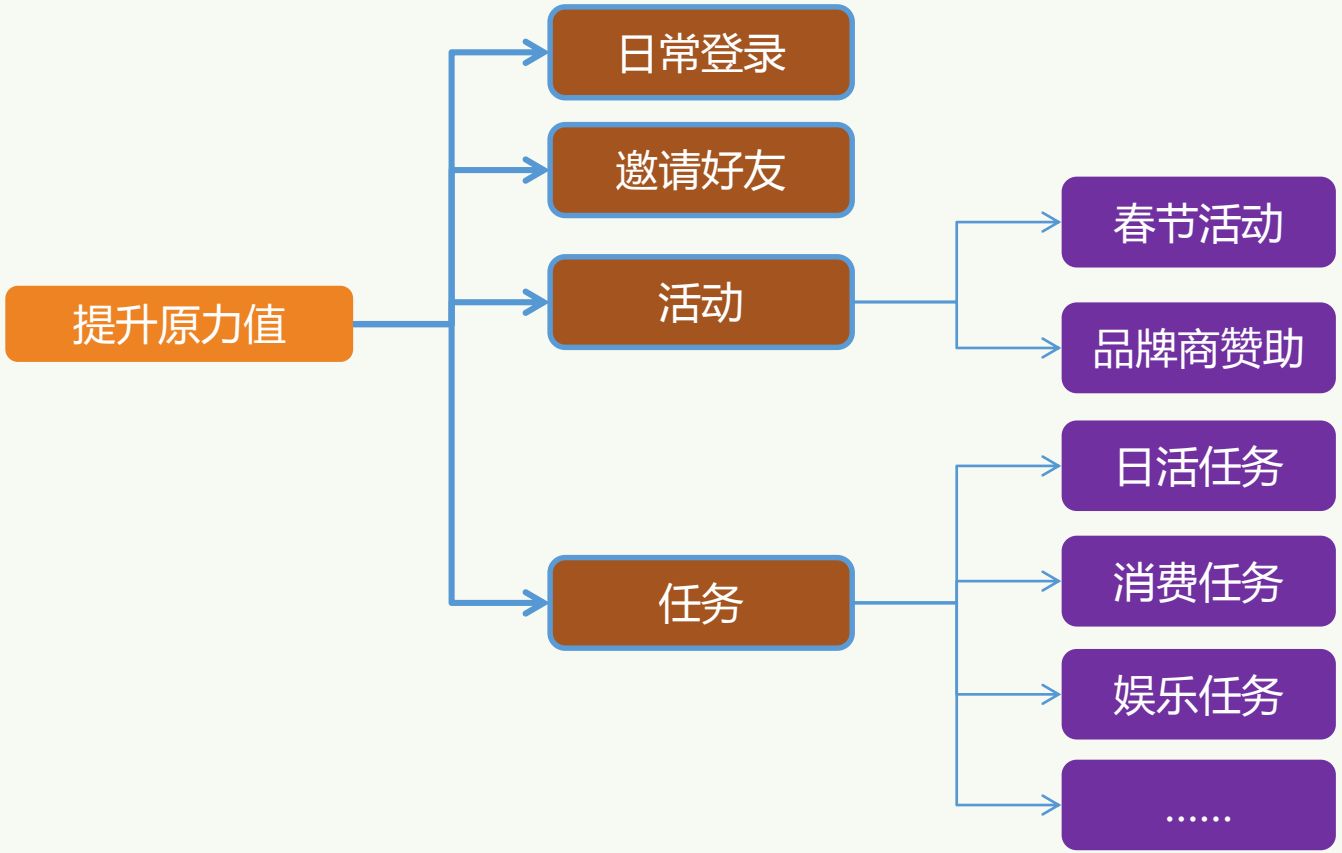
区块链 - 游戏



区块链 - 游戏


网易星球APP

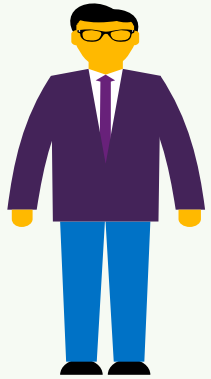

提升原力值
获取黑钻
黑钻商城


提升原力值
日常登录
邀请好友
活动
任务
春节活动
品牌商赞助
日活任务
消费任务
娱乐任务
……

区块链 - 互联网工具

brave

用户



授权、兴趣、打赏

激励、广告、隐私安全

Brave浏览器

区块链的代币体系

Adblocker

区块链溯源技术

区块链加密技术

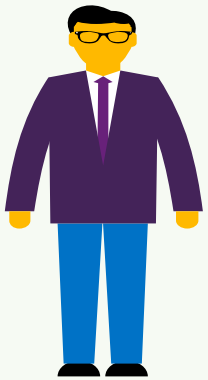
?

广告主

广告精准投放、费用打赏

受赏、广告追踪

广告主



用虚拟币去广告，看广告得虚拟币

付出

- 授权广告主给自己投放广告
- 发布自己的广告偏好
- 打赏广告主

获得

- 看广告拿激励
- 无被动广告，加快页面加载并减少流量使用
- 隐私信息加密，不会造成个人信息暴露

只要花钱的地方都可以有区块链

用虚拟币投放广告

付出

- 广告投放
- 广告观看激励金

获得

- 广告投放后观看记录追踪
- 接受用户的打赏，从而制作个性化广告
- 避免传统广告投放的刷单行为

区块链 - 行业应用

meitu 美图区块链

美图智能通行证

连接数字世界与现实世界的钥匙

美图智能档案

去中心化的保护用户隐私

人脸AI开放平台

基于人脸AI技术创造各类产品

行业层	互联网	物联网	金融	安防	…
产品层	美颜美妆	影像处理	皮肤管理	三维形象	…
技术层	人脸技术	三维重建	增强现实	深度学习	…
数据层	原始数据	专业数据	结构化数据	画像数据	…

区块链 - 行业应用

迅雷链克是玩客云共享计算生态下的基于区块链技术的原生数字资产。用户通过玩客云智能硬件分享网络带宽、存储空间等资源来获得该数字货币。在玩客云共享计算生态系统中，它将成为用户交换可共享计算资源的媒介，保证用户的权益和提供的计算资源对等。而且在这个生态中，通过区块链技术的智能合约，保证用户共享计算资源和内容的付出和收益对等，不可抵赖；通过去中心化的记录，保证所有记录真实

玩客云

奖励

链克

共享智能硬件，分享闲置的网络带宽、存储空间

04 趋势、机遇与挑战

趋势、机遇与挑战

区块链面临的问题？

技术：

- 行业高性能应用
- 稳定的运行环境
- 足够去中心化
- 简单的部署环境
- 低成本低能耗
- 简单高效的合约执行环境

产品与运营：

- 行业应用落地
- 行为信息化基础

政策：

- 政策监控

趋势、机遇与挑战

区块链未来的热点：

1、区块链 + 人工智能

2、区块链 + 物联网

3、区块链（智能合约 账本） 金融行业应用

Part4：趋势、机遇与挑战

比特币
以太坊

矿机
币交易平台

钱包
交易平台
金融资产管理
（2019年）

供应链溯源

物联网

生态应用
（2021年）

Thanks.