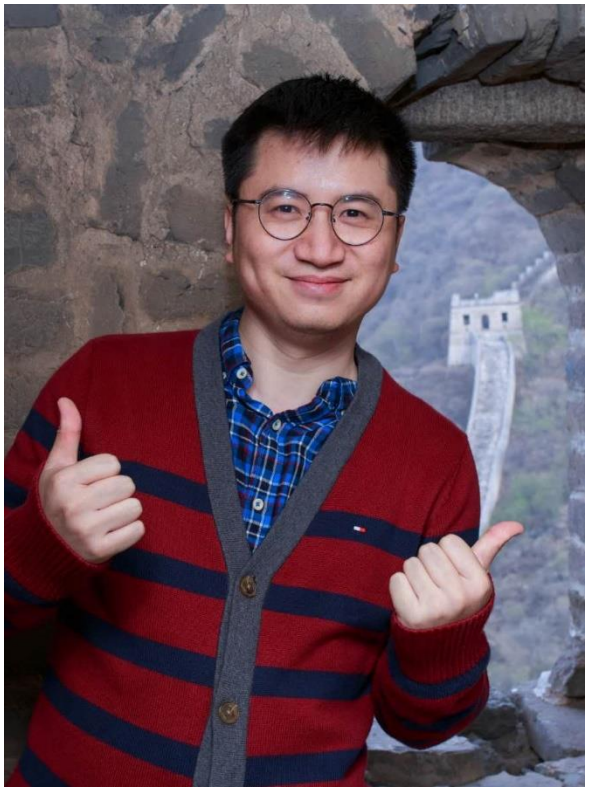
区块链在物联网中的应用

卿苏德

中国信息通信研究院

2017年7月13日

个人简介

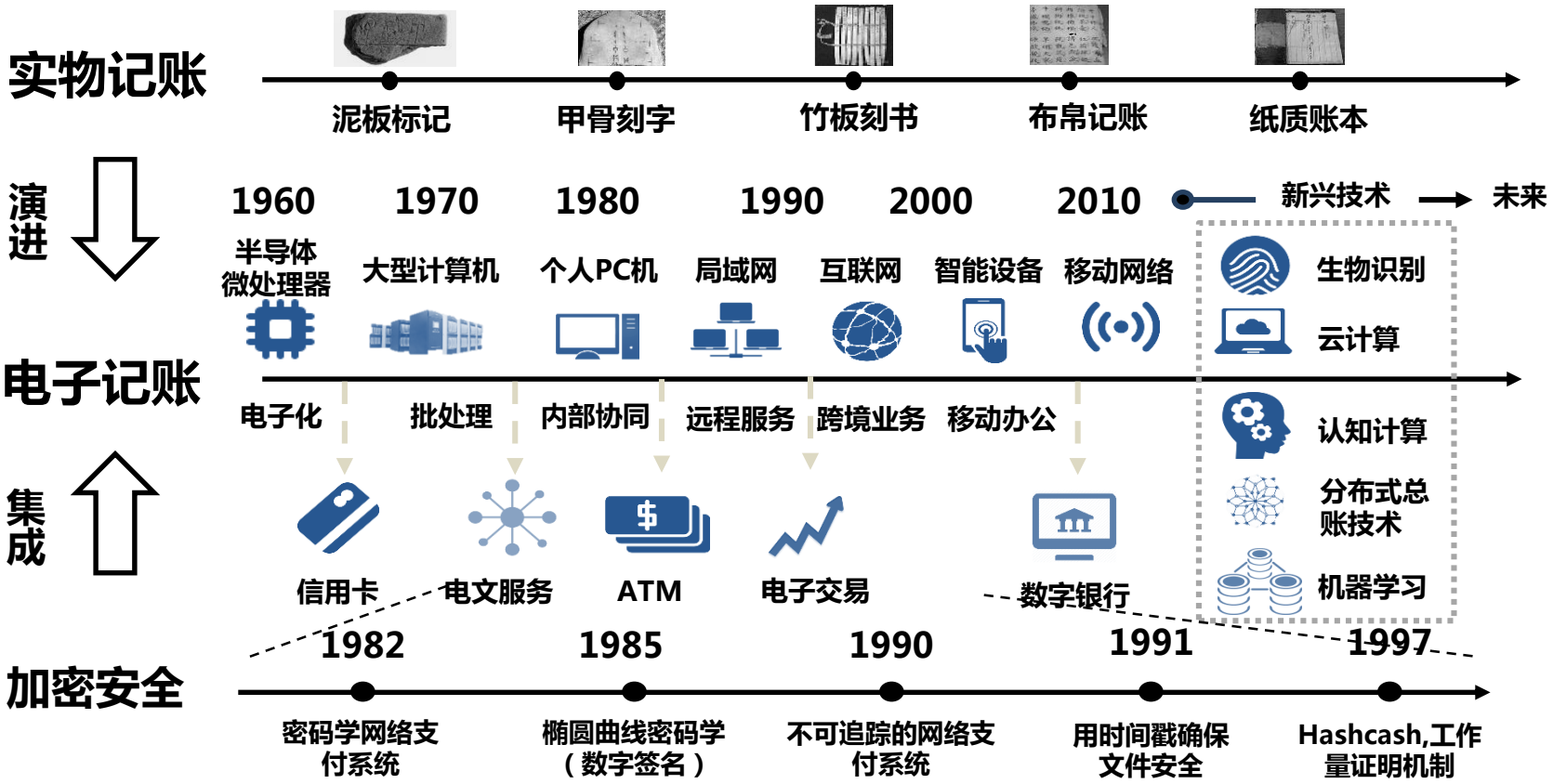


卿苏德，博士，高级工程师，毕业于北京邮电大学网络与交换国家重点实验室，国家教育部颁发的国家奖学金获得者，目前就职于中国信息通信研究院（CAICT），技术与标准研究所，可信区块链的评测负责人。

- ✓ 《“十三五”国家信息化规划》的核心编制团队的团队秘书，解读文章刊于光明网，被人民网转载
- ✓ 马化腾《数字经济》、周宏仁《中国信息化形势分析与预测》区块链章节的撰写人
- ✓ 贵阳2017年数博会“区块链论坛”邀请演讲嘉宾
- ✓ 中国信通院《全球区块链应用十大趋势》的核心编制人员
- ✓ 同济苏州金融科技研究院特聘导师，CSDN区块链特邀编辑，渡鸦区块链专栏作者。在CSDN上有区块链的公开课，学习人数超过2100+。

目录

分布式账本的演进历史


实物记账
泥板标记
甲骨刻字
竹板刻书
布帛记账
纸质账本
演进
1960
1970
1980
1990
2000
2010
新兴技术
未来
半导体
微处理器
大型计算机
个人PC机
局域网
互联网
智能设备
移动网络
生物识别
云计算
电子记账
电子化
批处理
内部协同
远程服务
跨境业务
移动办公
认知计算
分布式总
账技术
集成
信用卡
电文服务
ATM
电子交易
数字银行
机器学习
加密安全
1982
1985
1990
1991
1997
密码学网络支
付系统
椭圆曲线密码学
（数字签名）
不可追踪的网络支
付系统
用时间戳确保
文件安全
Hashcash,工作
量证明机制

什么是区块链

区块(Block) + **链**(Chain) = **区块链**(Blockchain)

区块链（Blockchain）是一种分布式数据库技术，也称为分布式总账技术。在典型的区块链系统中，数据以区块（block）为单位产生和存储，并按照时间顺序连成链式（chain）数据结构。所有节点共同参与区块链系统的数据验证、存储和维护。新区块的创建需得到全网超过半数节点的确认，并向各节点广播实现全网同步，之后就不能更改或删除。

麻将

卿苏德

记账

吕旭军

朱志文

张 蕾

记 账

方勇
/
何宝宏

UEC GROUP LTD

IT大咖说 知识分享平台

记账

吕旭军
朱志文
卿苏德
张　蕾

吕旭军

荣之联 UEC GROUP LTD

IT大咖说 知识分享平台

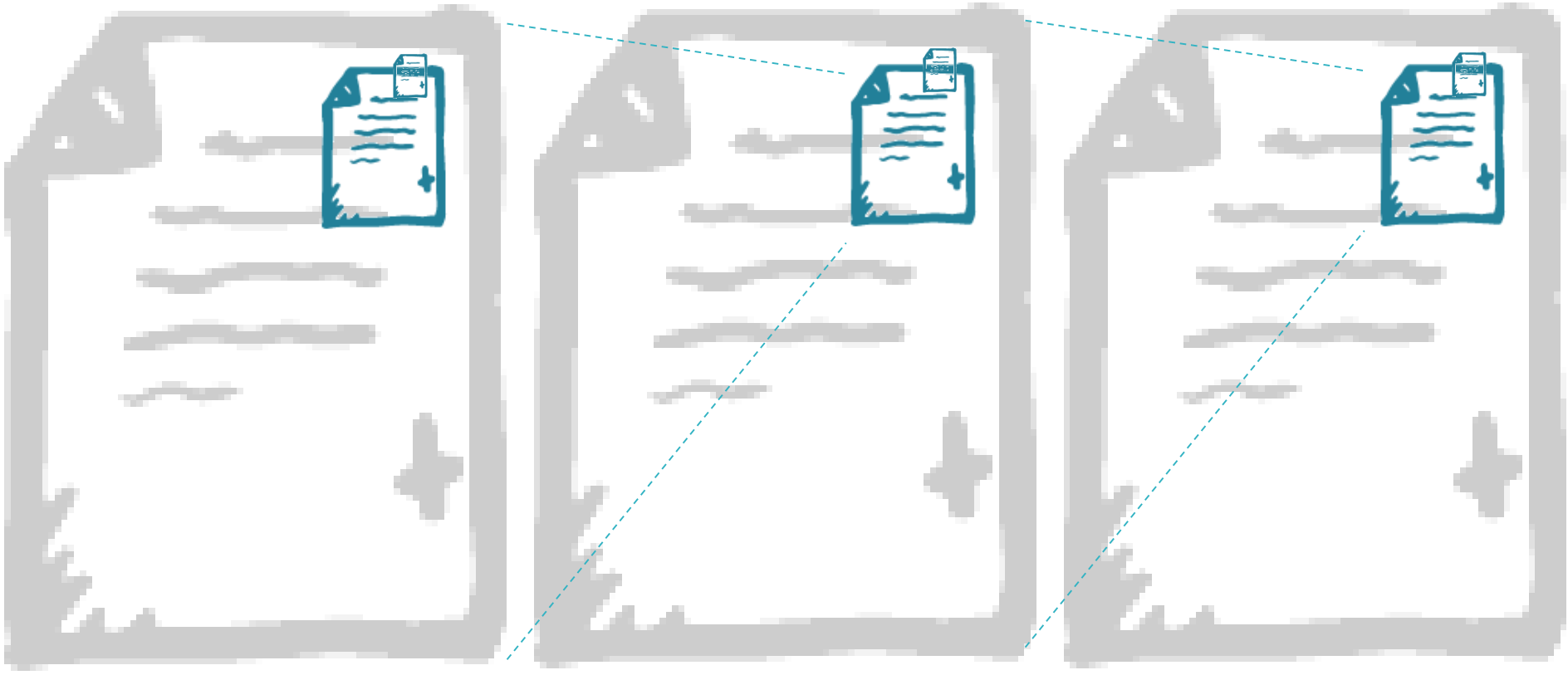
记 账

张　蕾

朱志文

区块链的链

区块链的链



吕旭军

荣之联 UEC GROUP LTD

IT大咖说 知识分享平台

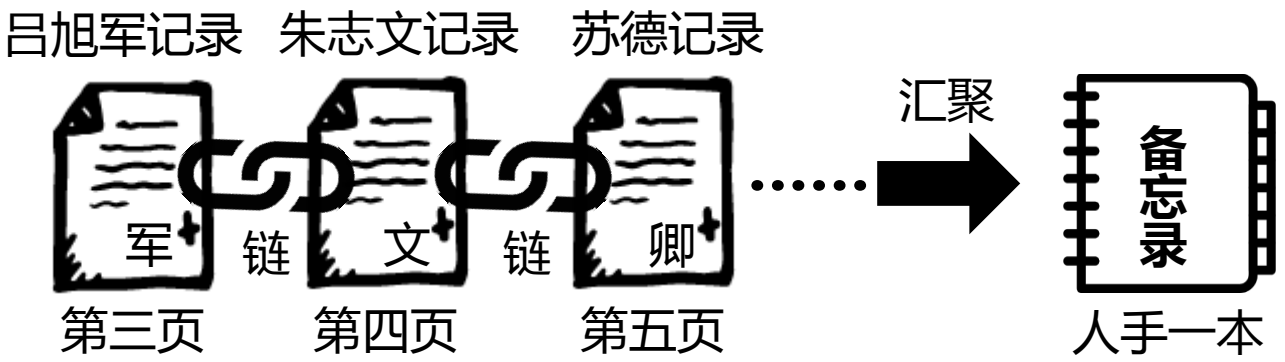
记账

张　蕾

朱志文

区块链

区块链可以简单地理解为一张张的记录（区块），装订（链接）在一起形成的大家都能看到的、不可更改的备忘录（区块链）。



流程约定

定时记录，换人来记账

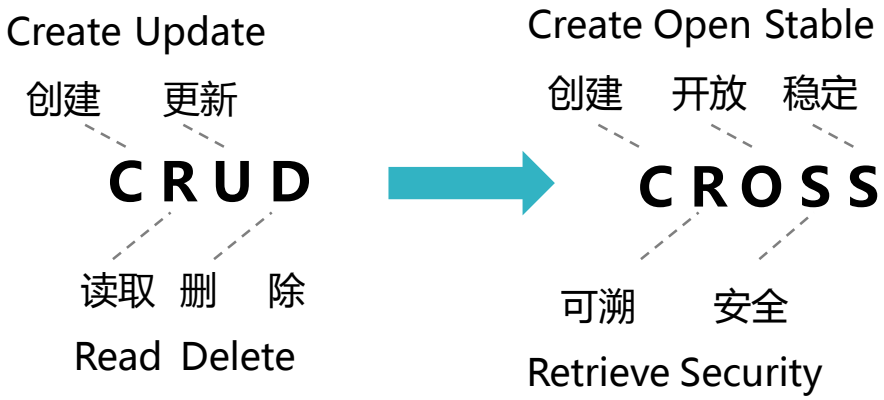
整页账本不能涂改，下方记录人签名

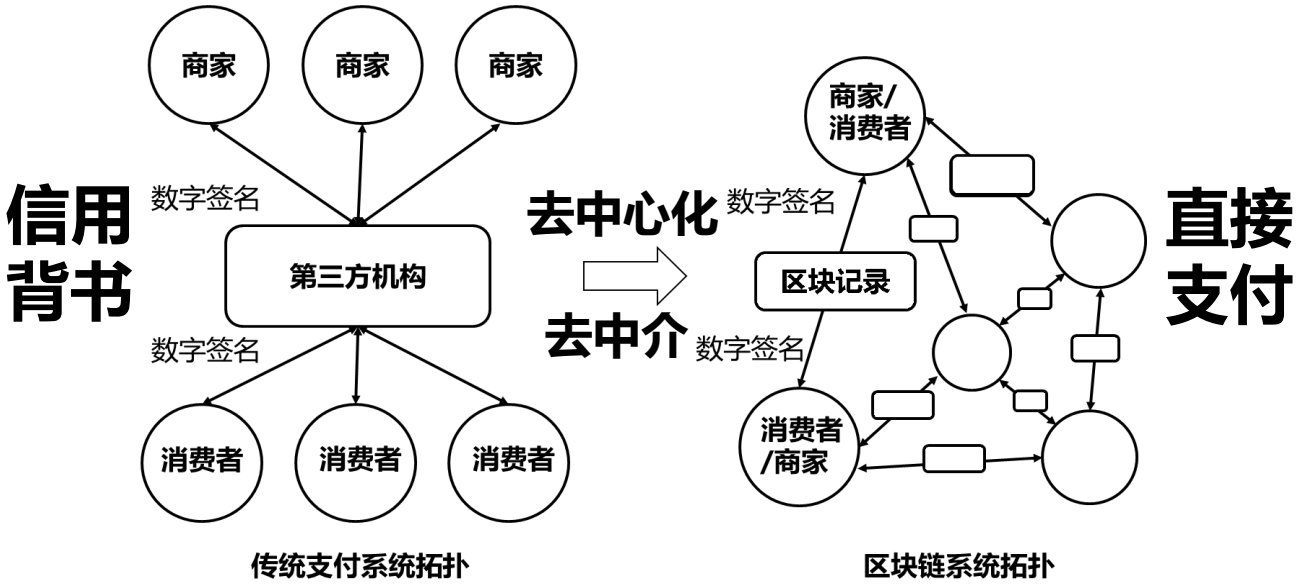
账本复印给所有人进行核对

添加进备忘录后不可修改

区块链的特点

技术定义：区块链是一种**分布式数据库**，通过**去中心化、去信任**的方式，**集体维护**一个**可靠数据库**。

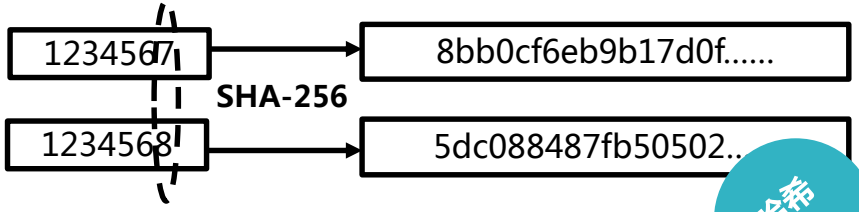


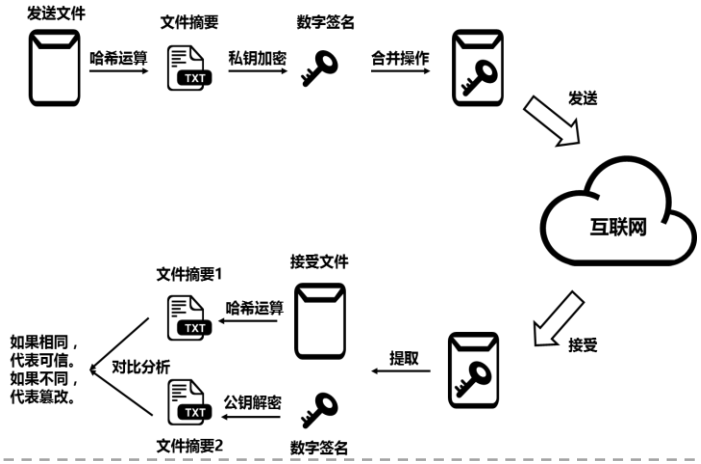


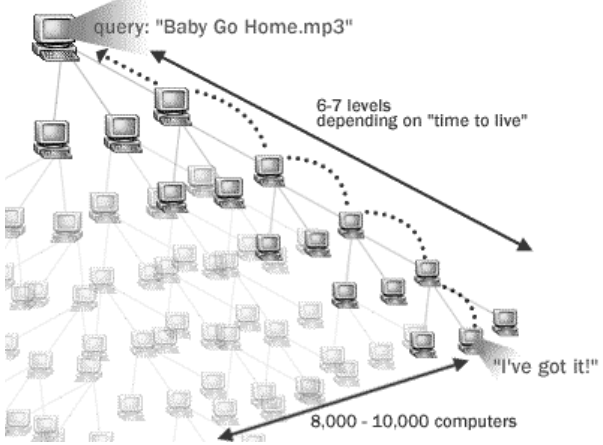
- 去中心化
- 公开透明
- 开放共识
- 安全可靠

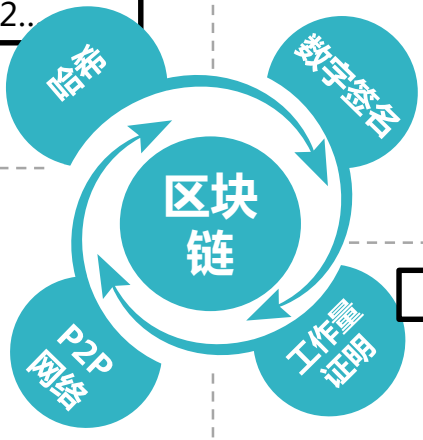
区块链的技术原语

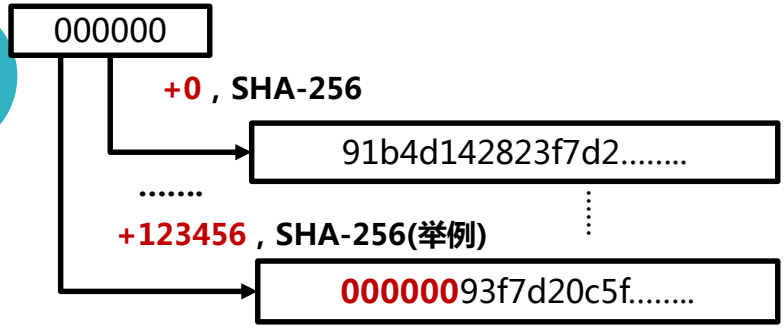
区块链主要运用了四个基础技术，分别是**哈希运算（SHA256）、数字签名、P2P网络和工作量证明（PoW）**。



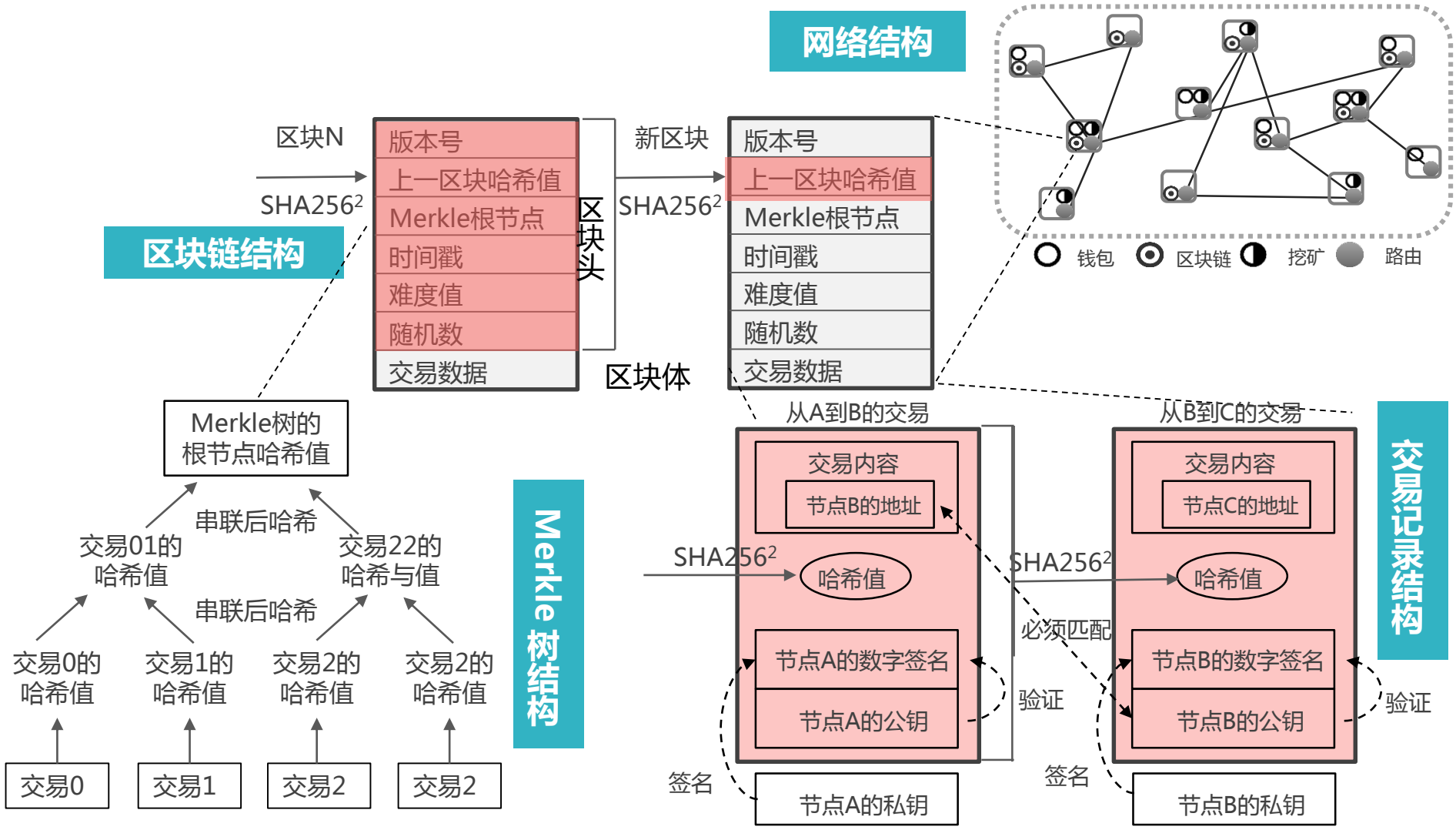




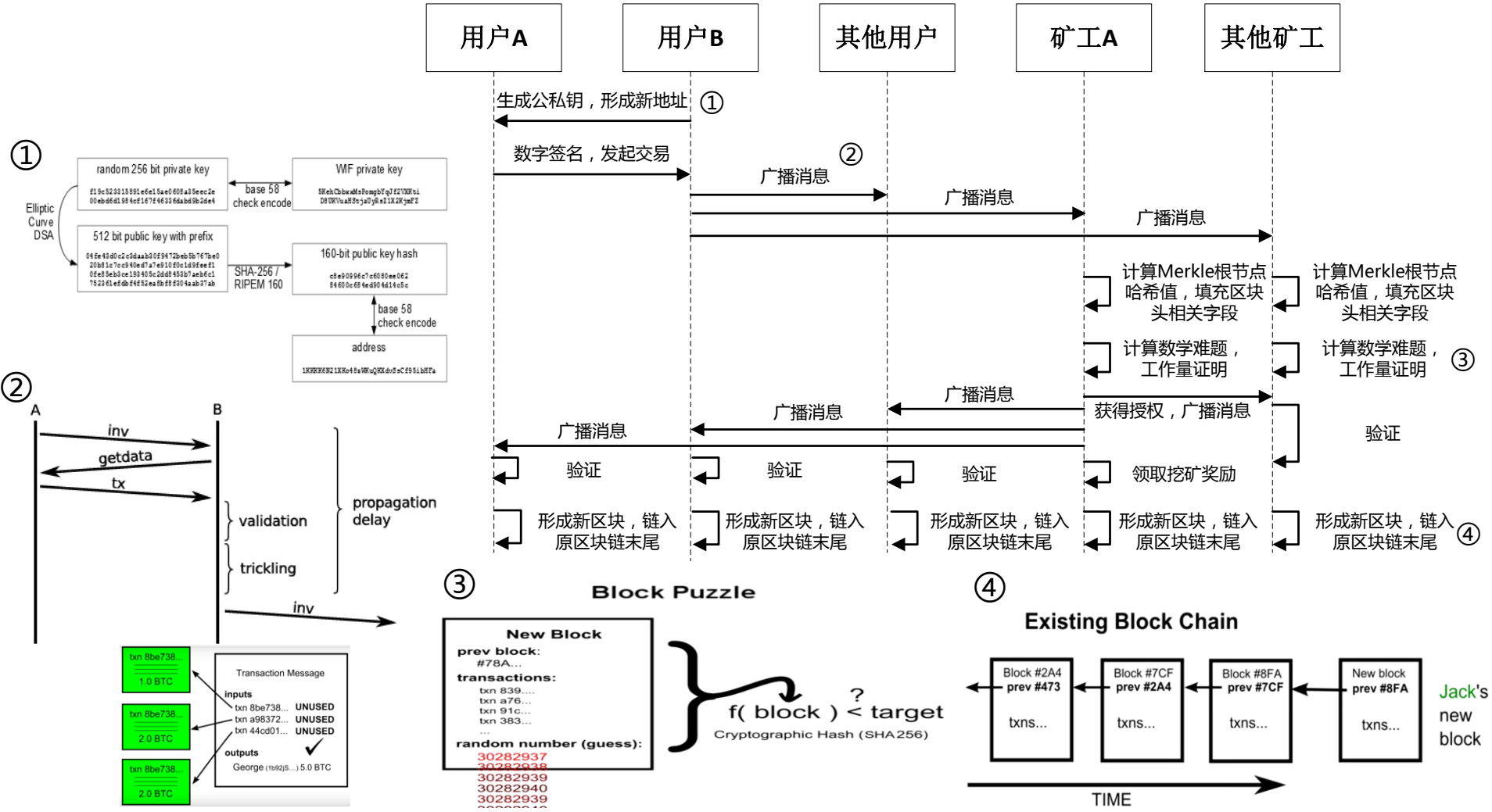




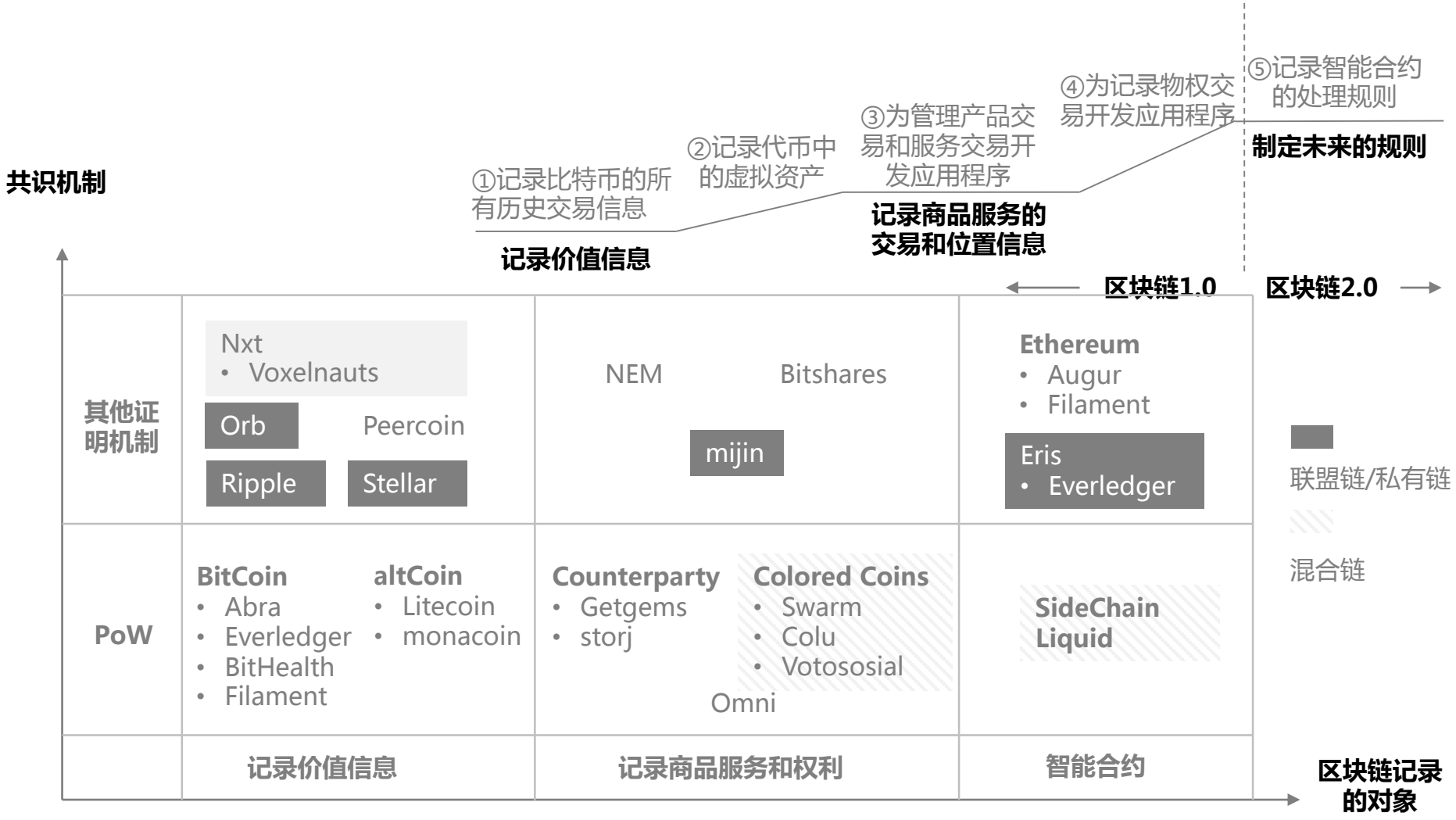
区块链的数据结构


网络结构
钱包
区块链
挖矿
路由
区块链结构
区块N
SHA256²
版本号
上一区块哈希值
Merkle根节点
时间戳
难度值
随机数
交易数据
区块头
区块体
新区块
SHA256²
版本号
上一区块哈希值
Merkle根节点
时间戳
难度值
随机数
交易数据
Merkle树的
根节点哈希值
串联后哈希
交易01的
哈希值
交易22的
哈希与值
串联后哈希
交易0的
哈希值
交易1的
哈希值
交易2的
哈希值
交易2的
哈希值
交易0
交易1
交易2
交易2
Merkle 树结构
从A到B的交易
交易内容
节点B的地址
SHA256²
哈希值
节点A的数字签名
节点A的公钥
签名
节点A的私钥
必须匹配
验证
从B到C的交易
交易内容
节点C的地址
SHA256²
哈希值
节点B的数字签名
节点B的公钥
签名
节点B的私钥
验证
交易记录结构

区块链的运转机制


用户A
用户B
其他用户
矿工A
其他矿工
生成公私钥，形成新地址 ①
数字签名，发起交易 ②
广播消息
广播消息
广播消息
计算Merkle根节点哈希值，填充区块头相关字段
计算Merkle根节点哈希值，填充区块头相关字段
计算数学难题，工作量证明
计算数学难题，工作量证明 ③
广播消息
广播消息
获得授权，广播消息
广播消息
验证
验证
验证
验证
领取挖矿奖励
形成新区块，链入原区块链末尾
形成新区块，链入原区块链末尾
形成新区块，链入原区块链末尾
形成新区块，链入原区块链末尾
形成新区块，链入原区块链末尾 ④
①
random 256 bit private key
base 58 check encode
WIF private key
Elliptic Curve DSA
512 bit public key with prefix
SHA-256 / RIPEM 160
160-bit public key hash
base 58 check encode
address
②
A
B
inv
getdata
tx
validation
trickling
propagation delay
inv
txn 8be738...
1.0 BTC
2.0 BTC
2.0 BTC
Transaction Message
inputs
txn 8be738... UNUSED
txn a98372... UNUSED
txn 44cd01... UNUSED
outputs
George (1b92jS...) 5.0 BTC
③
Block Puzzle
New Block
prev block:
#78A...
transactions:
txn 839....
txn a76...
txn 91c...
txn 383...
...
random number (guess):
30282937
30282938
30282939
30282940
30282939
f(block) < target ?
Cryptographic Hash (SHA256)
④
Existing Block Chain
Block #2A4
prev #473
txns...
Block #7CF
prev #2A4
txns...
Block #8FA
prev #7CF
txns...
New block
prev #8FA
txns...
Jack's new block
TIME

区块链正从1.0向2.0演进

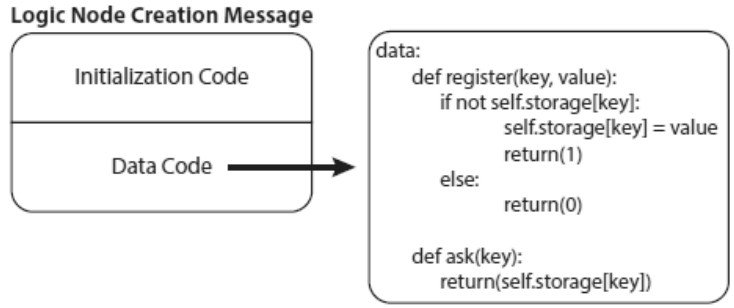


区块链1.0的局限

Stack	Script
	sigBob pubKeyBob OP_DUP OP_HASH160 pubKeyBobHash OP_EQUALVERIFY OP_CHECKSIG
sigBob pubKeyBob	OP_DUP OP_HASH160 pubKeyBobHash OP_EQUALVERIFY OP_CHECKSIG
sigBob pubKeyBob pubKeyBob	OP_HASH160 pubKeyBobHash OP_EQUALVERIFY OP_CHECKSIG
sigBob pubKeyBob pubKeyBobHash	pubKeyBobHash OP_EQUALVERIFY OP_CHECKSIG
sigBob pubKeyBob pubKeyBobHash pubKeyBobHash	OP_EQUALVERIFY OP_CHECKSIG
sigBob pubKeyBob	OP_CHECKSIG
true	

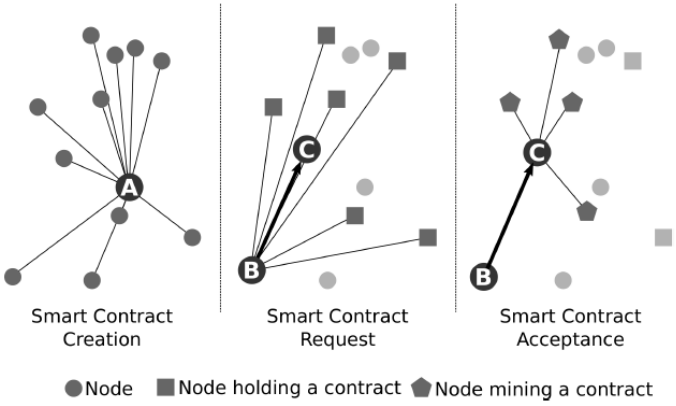
非图灵完整

不支持循环



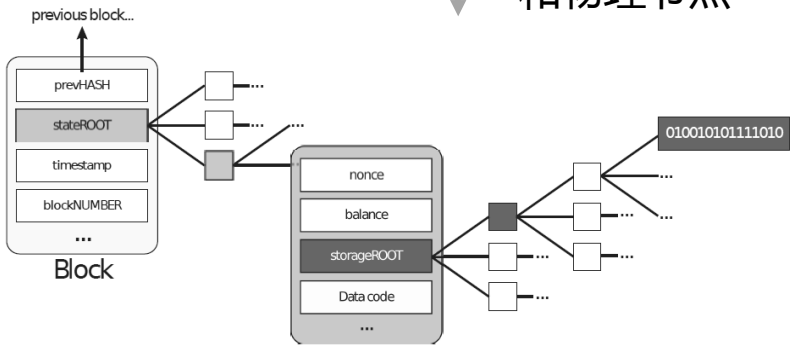
修改区块链结构

划分为逻辑节点和物理节点

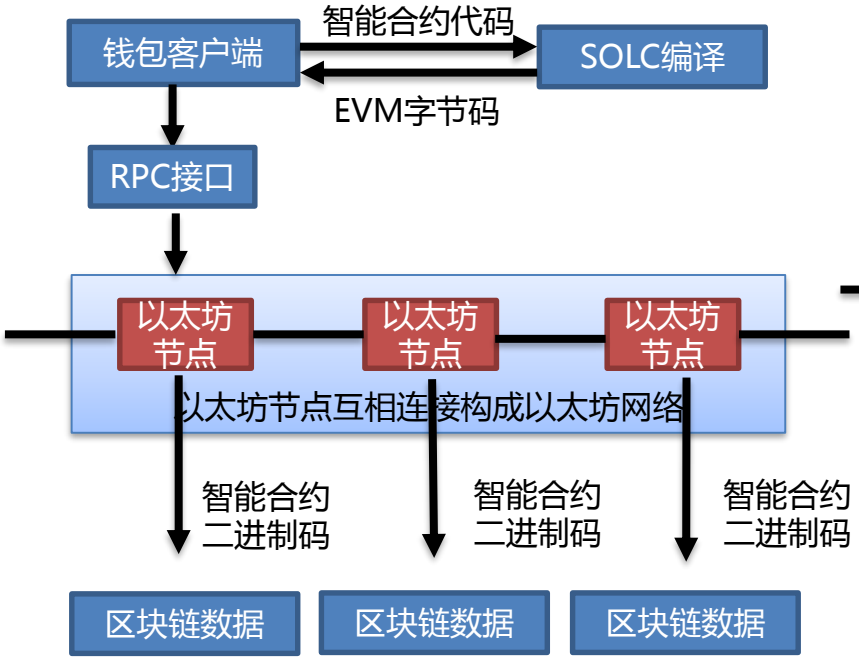


运行机制

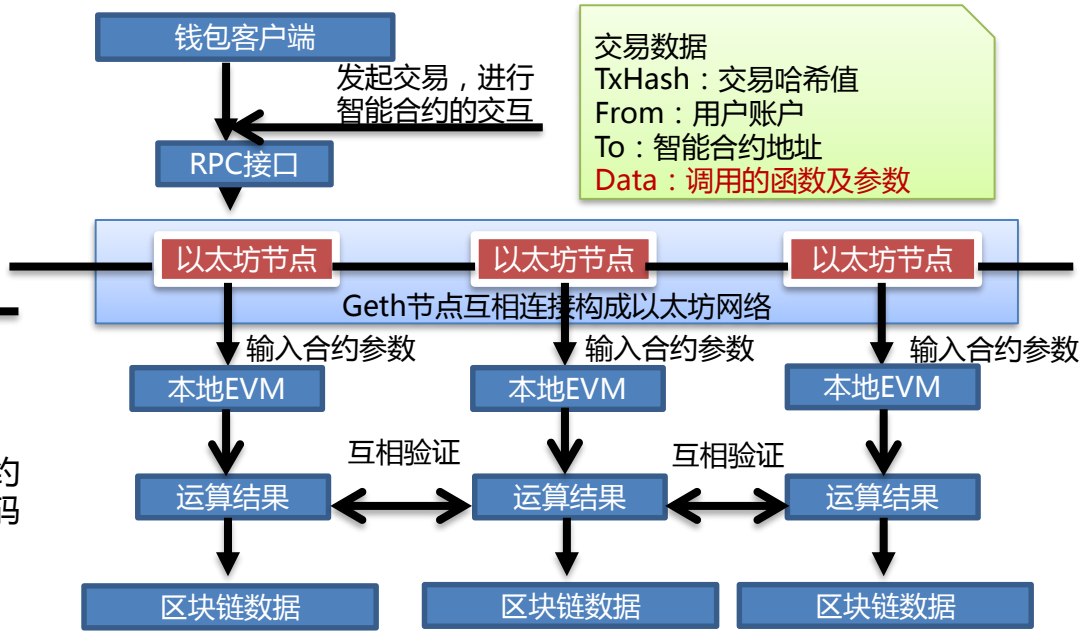
划分为创建合约、请求合约和接受合约



智能合约的原理



部署原理



运行原理

来源：李赫《区块链技术详解》

智能合约的例子

今天凌晨2:45，欧冠皇马VS拜仁慕尼黑

↓

发布一个智能合约，皇马赢，小明给我1000元；拜仁赢，我给小明1000元。

↓

比赛结果发布，皇马4:2拜仁。触发智能合约响应条件。

↓

履行智能合约，将小明的1000元打入我的账户

目录

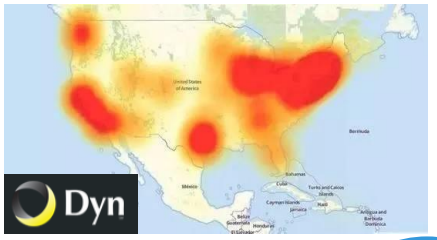
物联网发展中的行业痛点

UEC GROUP LTD

IT大咖说 知识分享平台

设备安全

Mirai创造的僵尸物联网（Botnets of Things），DDos攻击域名解析服务商Dyn， Twitter、PayPal 等诸多人气网站暂时瘫痪。



个人隐私

中央服务器管理者在未经授权情况下可能使用其存储和转发隐私数据。成都的266个监控摄像头，被网络“直播”。

通信兼容

全球物联网平台缺少统一的语言，这很容易造成多个物联网设备彼此之间通信受到阻碍，并产生多个竞争性的标准和平台。

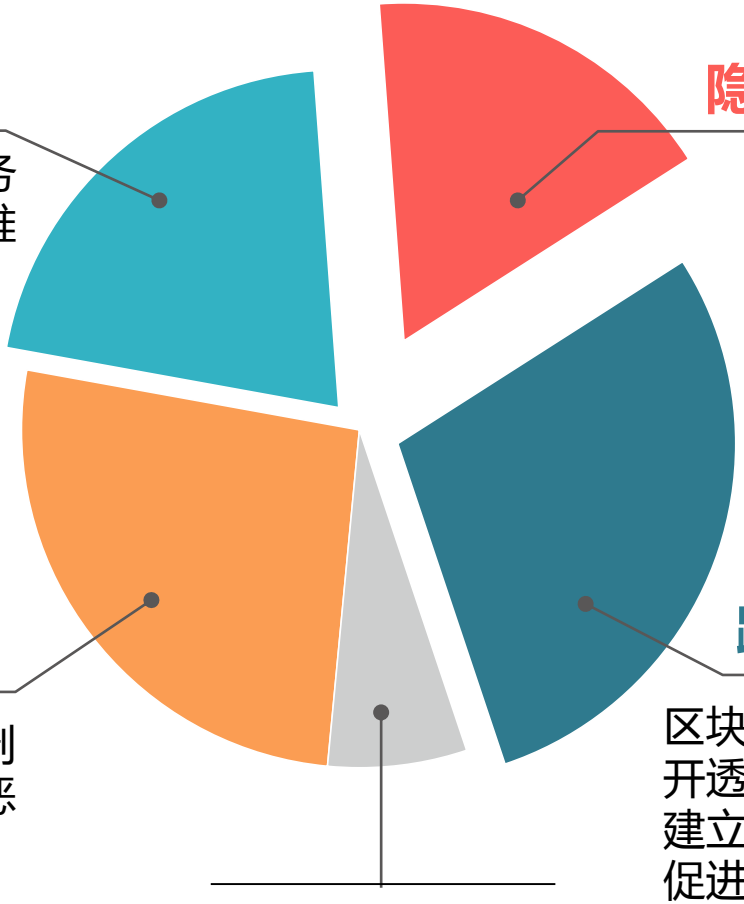
架构僵化

目前的物联网数据流都汇总到单一的中心控制系统，随着设备几何级数增长，中心化服务成本难以负担

多主体协作

目前，很多物联网都是运营商、企业内部的自组织网络。涉及到跨多个运营商、多个对等主体之间的协作时，建立信用的成本很高。

区块链+物联网带来的改进



降低成本

区块链无需中心服务器，规避昂贵的运维费用。

隐私保护

区块链中的所有传输的数据都经过严格的加密处理，用户的数据和隐私将会更加安全。

身份鉴权

区块链的验证和共识机制有助于避免非法甚至是恶意的节点接入物联网。

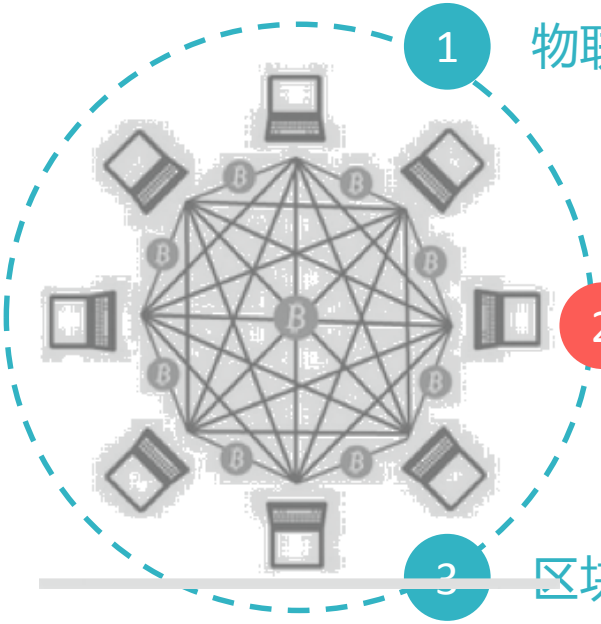
跨主体协作

区块链的分布式对等结构和公开透明的算法，能够以低成本建立互信，打破信息孤岛桎梏，促进信息横向流动和多方协作。

可证可溯

数据只要经过共识写入区块链，就难以篡改，还能依托链式结构追本溯源。

目录



现状一：物联网龙头纷纷布局区块链

IBM 2016年10月，IBM推出了Bluemix云平台上的区块链服务（BaaS）。

PREDIX 2016年10月，通用电气（GE）和爱立信合作，在GE Predix云上提供基于区块链的“数字指纹”存证服务。

Microsoft 2016年8月，微软区块链服务正式向Azure云平台用户开放。

亚马逊 amazon.cn 2016年5月，亚马逊选择与数字货币集团（DCG）进行合作，为企业提供区块链实验环境。

CISCO 2017年4月，Cisco开始探索如何使用区块链来登记设备标识。

SAP 2017年5月，SAP发布了Leonardo生态系统，提供区块链云服务，希望整合物联网、机器学习等前沿科技

IBM、微软、亚马逊和SAP主要是在各自的云平台上提供区块链服务，通用电气和思科更多地是关注设备的标识和存证问题。

数据来源： Forrester Wave：物联网软件平台（2016年第4季度）

现状二：传统行业和初创公司

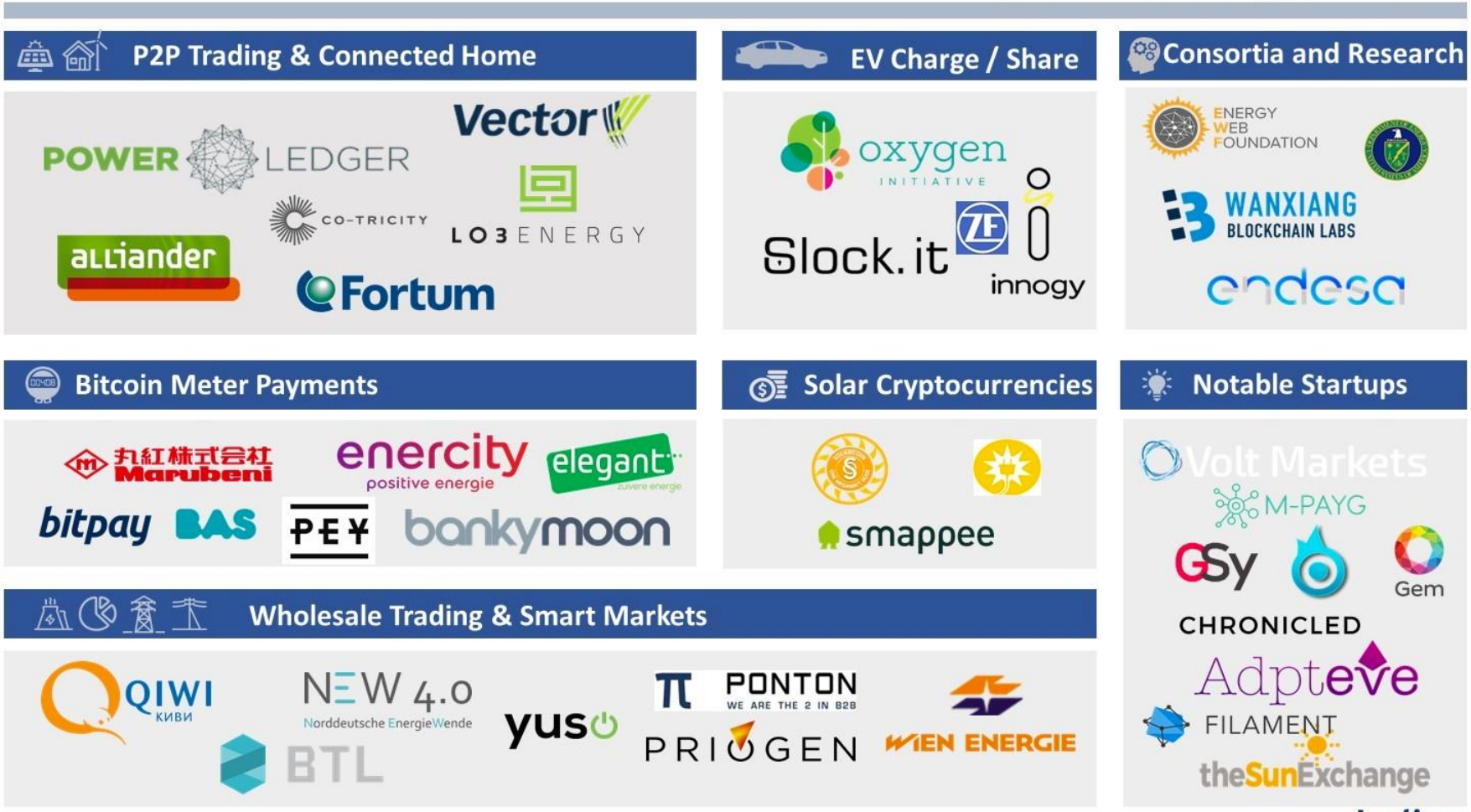
	分布式能源系统		新型交易模式	认证和交易市场	
电力公司	fortum	VATTENFALL 瑞典国营电力公司瀑布电力	RWE The energy to lead / innogy		
初创企业	LO3 ENERGY TRANSACTIVEGRID / CONSENSYS / oneup	powerpeers energie van elkaar 荷兰初创公司	slock.it	SOLARCOIN ONE MEGAWATT HOUR	GrünStromJeton
项目	**布鲁克林微电网** 基于区块链的10户可再生能源交易试点	**电力共享平台** 让消费者能自由选择购买的绿能电力来源	**BlockCharge** 通过点对点的、无中介的方式，让电动汽车选择可用充电桩进行充电	**Solar-Change** 用太阳币记录太阳能发电量，通过交易平台交易太阳币以实现能源交易	基于区块链的绿色能源认证服务。主要聚焦在需求侧的认证。
硬件设备	Raspberry Pi		Smart Plug	BITMAIN ANTMINER	

传统电力公司通过与初创公司合作、成立子公司、甚至买下初创公司等方式，投资不同的试点项目，打造分布式能源系统和点对点的能源交易平台。

初创公司从分布式能源系统、新型交易模式、认证和交易市场等不同角度切入区块链领域，开始初步涉及相关的物联网硬件制造，不断丰富区块链+的产业生态。

现状三：垂直行业的生态格局已初步形成

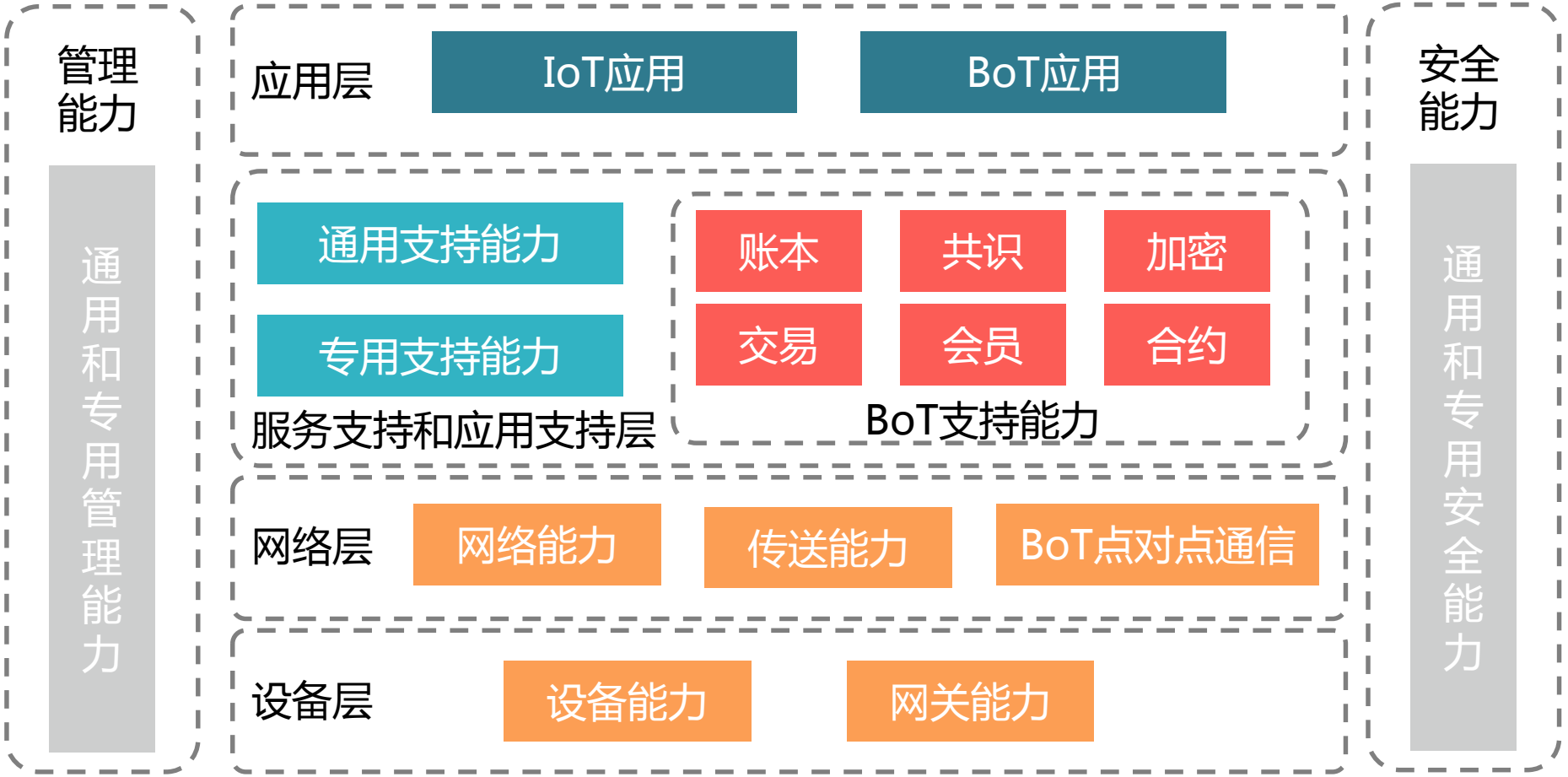
以电力行业的区块链+物联网应用举例，从终端支付（加密数字货币）、能源交易市场、技术支撑+行业组织、智能家居点对点交易、打造智慧城市等方面已形成良好生态格局。



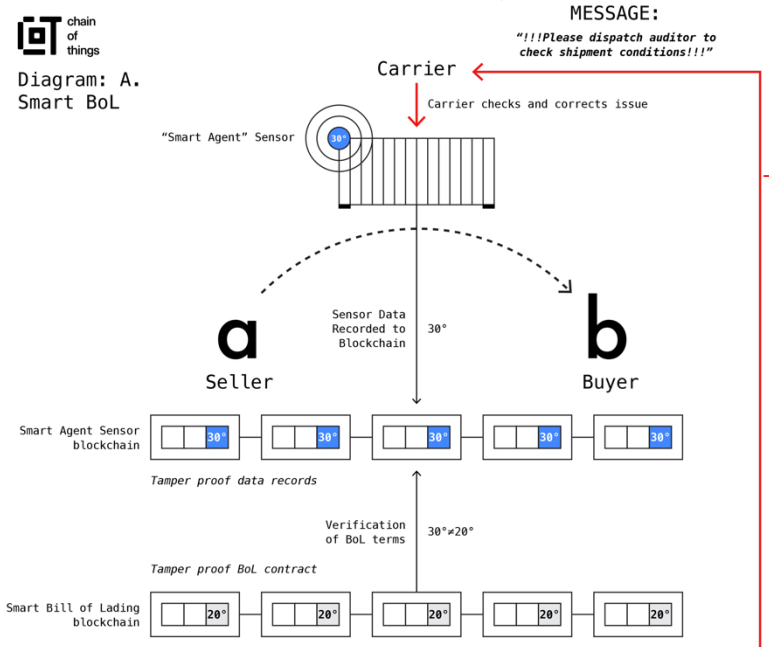
资料来源 :Indigo

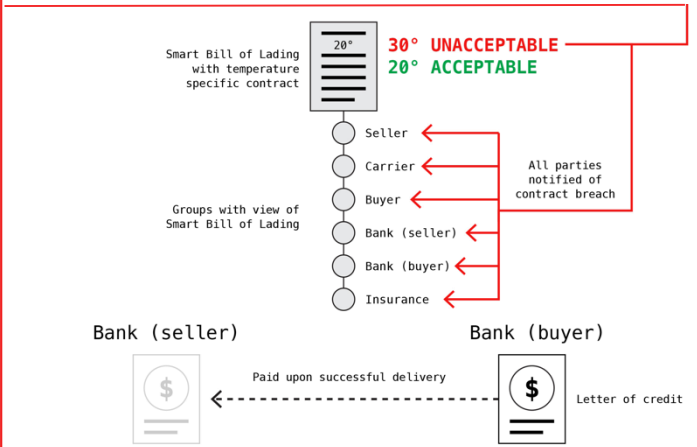
现状四：区块链+物联网国际标准

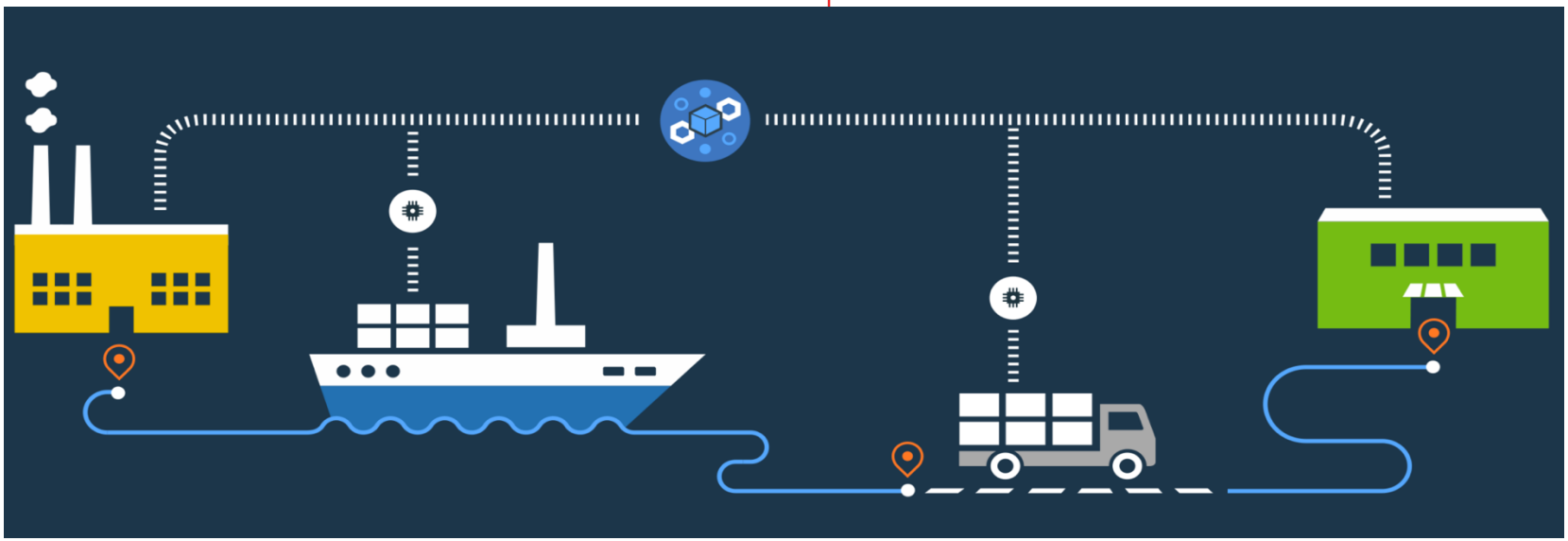
2017年3月，中国联通联合众多公司和研究机构在ITU-T SG20成立了全球首个物联网区块链（BOT，Blockchain of Things）标准项目，定义了去中心化的可信物联网服务平台框架。



应用场景一：传感器数据的存证[illegible]

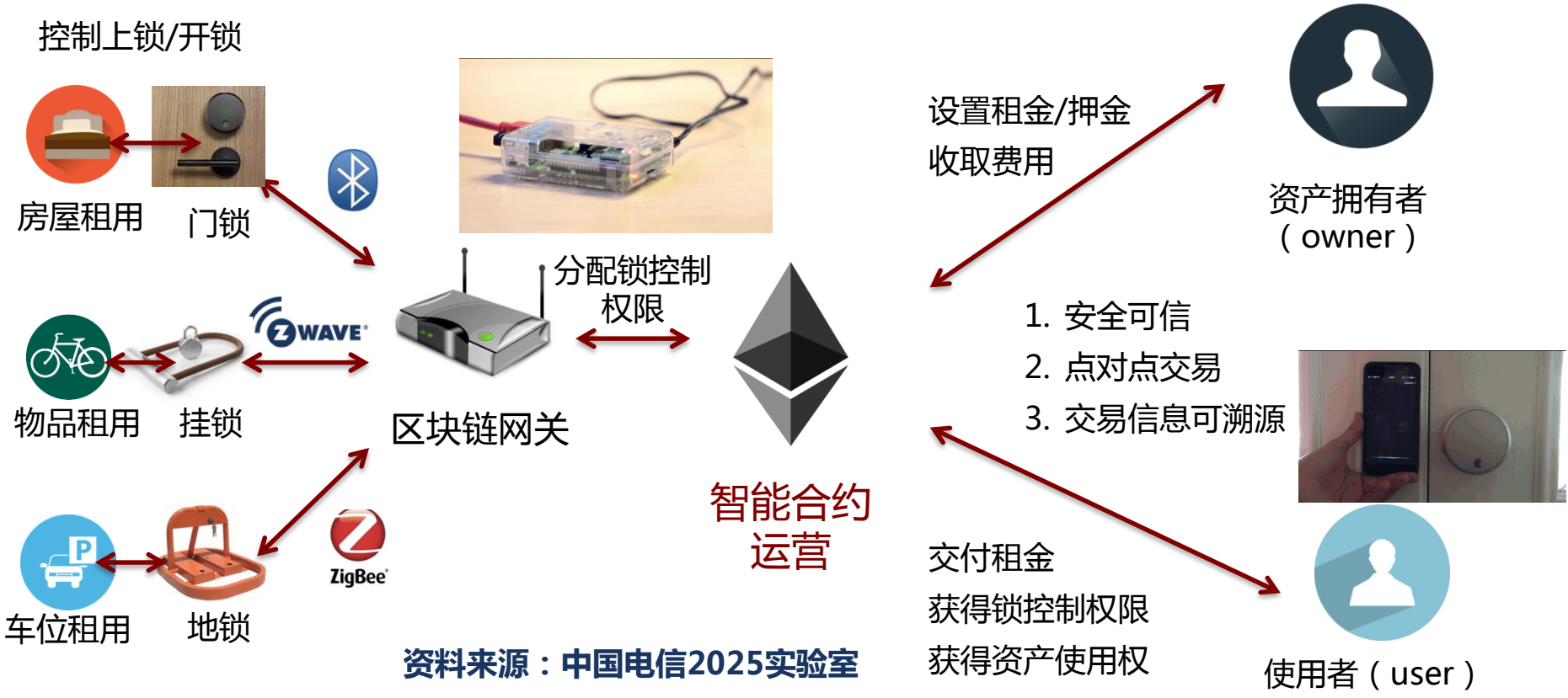






应用场景二：新型“共享”经济

完成各类锁与资产的绑定。区块链网关是区块链的节点，在区块链上运行智能合约，由智能合约操控锁的控制权限转移；资产拥有者与使用者交易双方通过智能合约的前端应用——Dapp来完成交易，拥有者获得租金与押金，使用者获得控制权限，以此获得资产的使用权。



资料来源：中国电信2025实验室

应用场景三：基于智能电表的能源交易

太阳能转化器

供暖

电表

住宅

热电联产源

群体通信

缓冲区

蓄电池

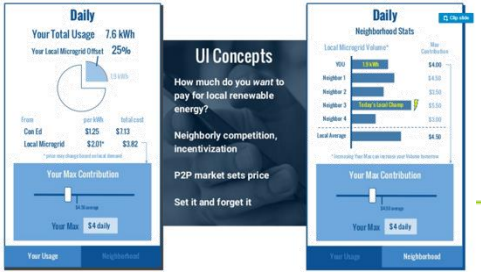
电力
通信
供热
返热

LO3 ENERGY

CONSENSYS

TRANSACTIVEGRID

ENERGO



低压配电网

低压配电网

太阳能转化器

供暖

电表

住宅

热电联产源

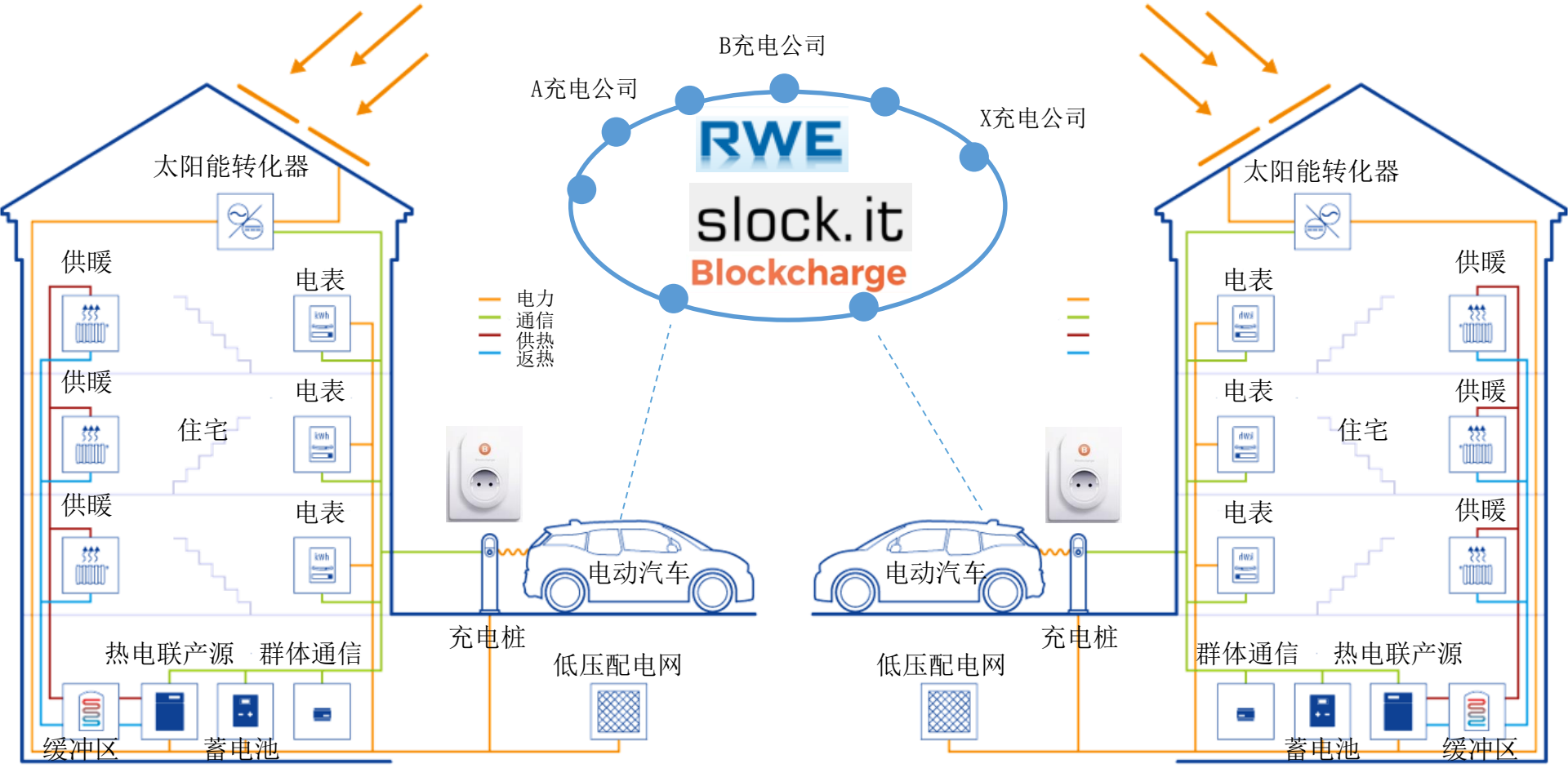
群体通信

缓冲区

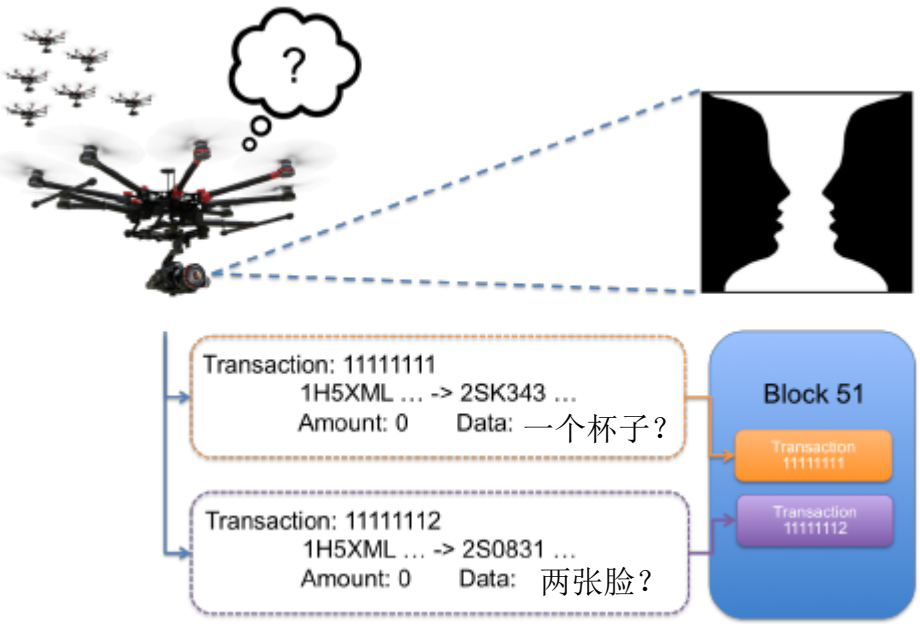
蓄电池

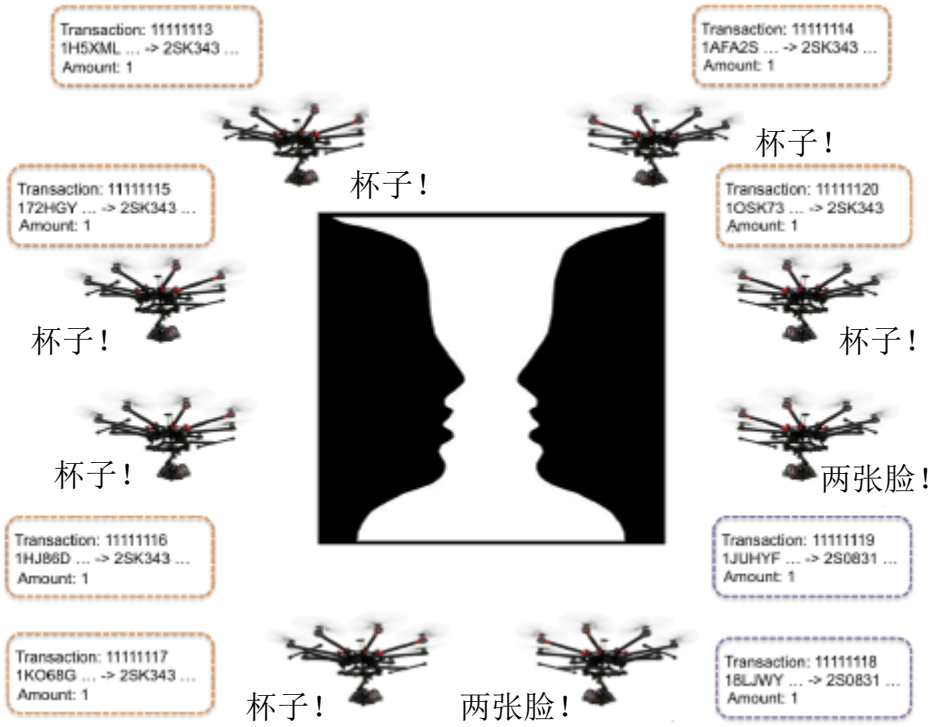
应用场景四：电动汽车的即时充电

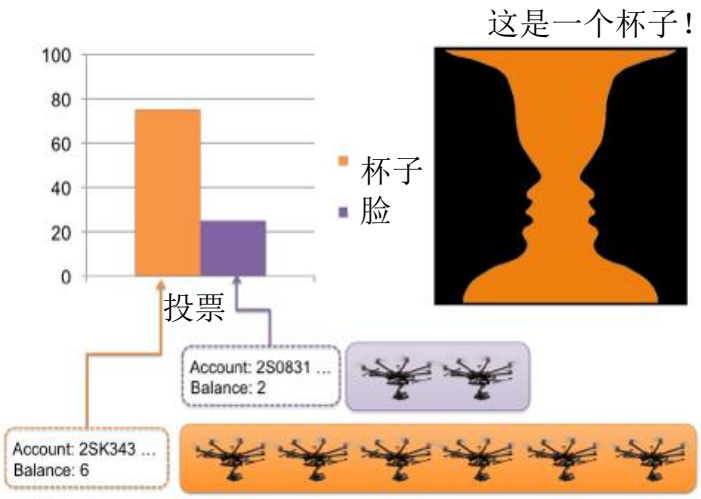
首先，在智能手机上安装Share&Charge APP。在APP上注册你的电动汽车，并对数字钱包进行充值。需要充电时，从APP中找到附近可用的充电站，按照智能合约中的价格付款给充电站主人。APP将与充电站中的接口通信，后者执行电动车充电的指令。



应用场景五：无人机的安全通信



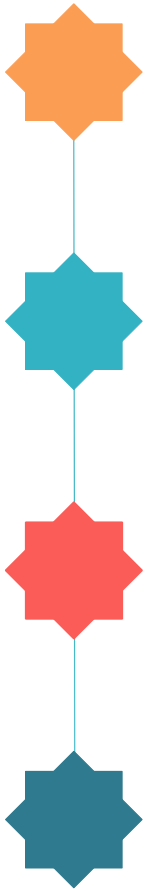




一方面，每个无人机都内置了硬件密钥。基于数字签名的通信确保安全交互，基于私钥的ID增强了身份鉴权，阻止伪造信息的扩散和非法设备的接入。

另一方面，基于区块链的共识机制，未来区块链与人工智能的结合点——群体智能，充满了想象空间，MIT实验室已经在这个交叉领域展开了深入研究。

区块链+物联网的应用阻碍



资源消耗

比特币的PoW是资源耗费高的共识机制，而IoT设备普遍存在计算能力低、联网能力弱、电池续航短等问题。

数据膨胀

随着区块链的不断增长，IoT设备是否有足够存储空间？例如，比特币运行至今，需要100G物理存储空间。

性能瓶颈

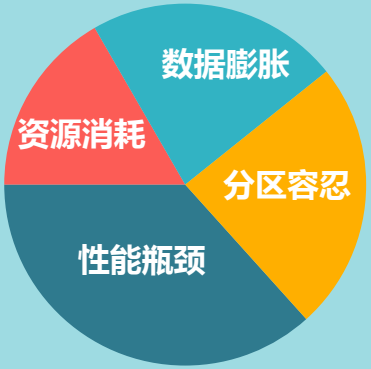
传统比特币的交易是7笔/秒，再加上共识确认，需要约1个小时才写入区块链，这种时延引起的反馈时延、报警时延，在时延敏感的工业互联网上不可行。

分区容忍

虽然工业物联网强调节点“一直在线”，但是，普通的物联网节点失效、退出网络是司空见惯的事情，容易产生大量网络带宽消耗，甚至出现“网络割裂”的现象。

区块链+物联网的改进思路

从区块链角度



- 不使用基于挖矿的共识机制，使用投票的共识机制（例如PBFT等）
- 使用简单支付交易方式(SPV)，支持重型节点和轻型节点。
- 不使用链式结构，采用有向非循环图（DAG）。采用主链-侧链等跨链技术，进行划区划片管理。
- 改为支持链上链下交易，尤其是离线的交易，支持多个CPS集群。

从物联网角度

- 低功耗广域网（LPWA）解决传输质量、传输距离、功耗、蓄电量的问题。
- 随着摩尔定律，存储成本下降，物联网存储能力持续上升。
- 随着MEMS传感器、SiP封装工艺等新技术、新工艺、新架构的不断成熟、成本降低，小体积、低功率的传感节点有望广泛应用。

可信是区块链+物联网的核心要[illegible]
准规范的重要性日趋凸显

智能合约
智能合约的执行率、执行结果和有效性需要第三方中立机构评估

共识机制
检验系统中的各个节点是否最终一致，尤其在“网络割裂”的情况下

私钥安全
评估系统保护用户私钥的安全等级

权限管理
确认系统支持多角色分类和权限管理

信息披露
为了炒作，区块链公司经常披露一些不实的信息，需要甄别清楚

区块链以算法和软件来承担信任基础，仍然需要规则来规范。未来将从用户的角度、以业务为导向，提出标准规范，增强区块链的可信程度， 给区块链的信任增加砝码。

可信区块链工作组未来展望

1、标准制定和输出。

国际标准 — 国际电联：SG16

中国通信标准化协会 China Communications Standards Association

行业标准 — CCSA：TC1

2、标准的试点评估。 区块链开放实验室、区块链测试平台建设。

3、区块链行业纵向和横向交流。 项目落地；区块链与物联网、云计算等结合。

未来的工作

- ✓可信区块链预测试的全面开展
  - ◆ 9月19日召开可信区块链峰会，成立可信区块链联盟，并对测试通过的厂商颁发评测证书，宣布十大区块链应用案例。
  - ◆ 根据可信区块链预测试的结果和经验，不断丰富和迭代可信区块链标准
- ✓区块链测试平台的搭建
  - ◆完成许可型的区块链测试平台搭建（含联盟链和私有链）
- ✓区块链测试工具的研发
  - ◆研发支持多种区块链系统接入的交易模拟发送器

CAICT 中国信息通信研究院
China Academy of Information and Communications Technology

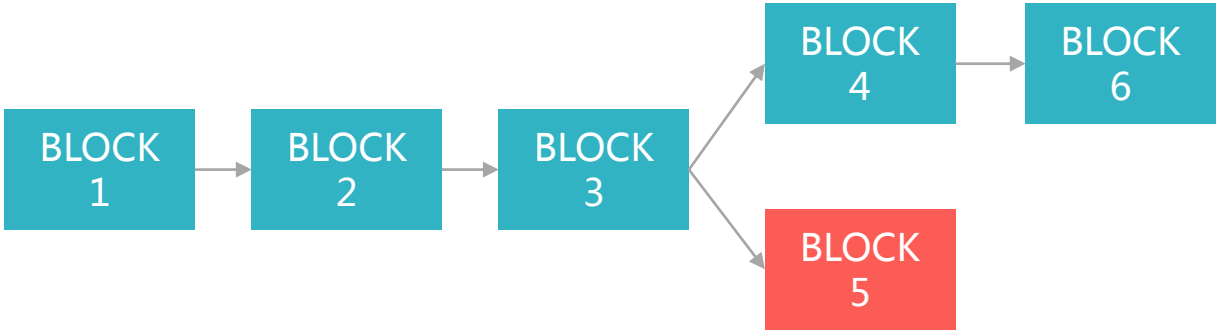
厚德實學　興業致遠

政府高端专业智库

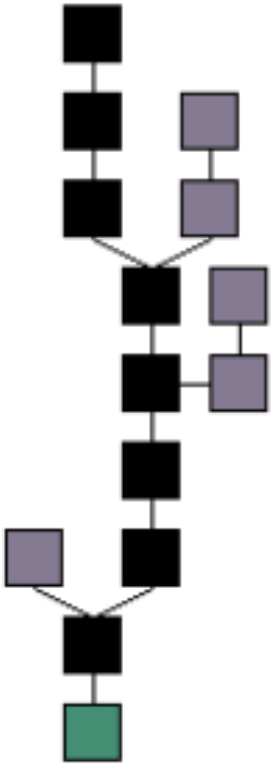
行业创新发展平台

区块链的分叉

区块链的分叉：同一时间段内全网不止一个节点能计算出随机数（拼出拼图），即会有多个节点在网络中广播它们各自打包好的临时区块（都是正确的拼图）。



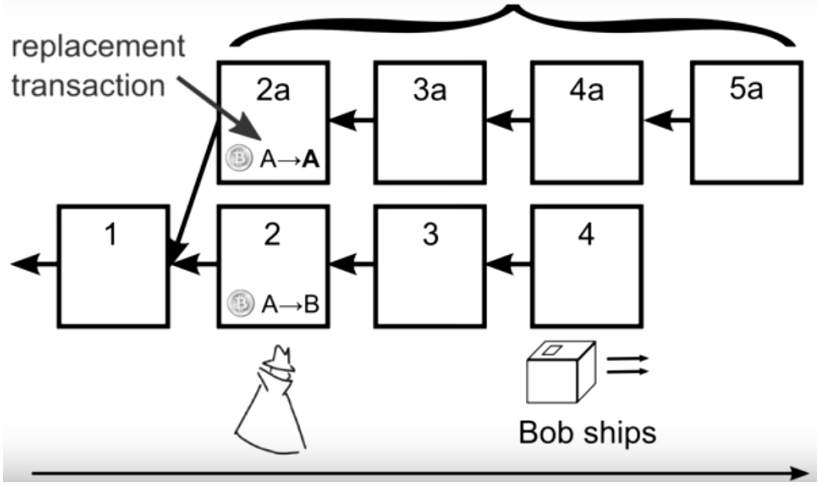
共识基础：区块链主链选择标准



- 工作量最多的（区块高度最高）是主链
- 高度相同的，难度最大的是主链
- 高度、难度都一致，时间最早的是主链
- 高度、难度、时间都一致，按照网络接受顺序选出主链

双花问题和51%攻击

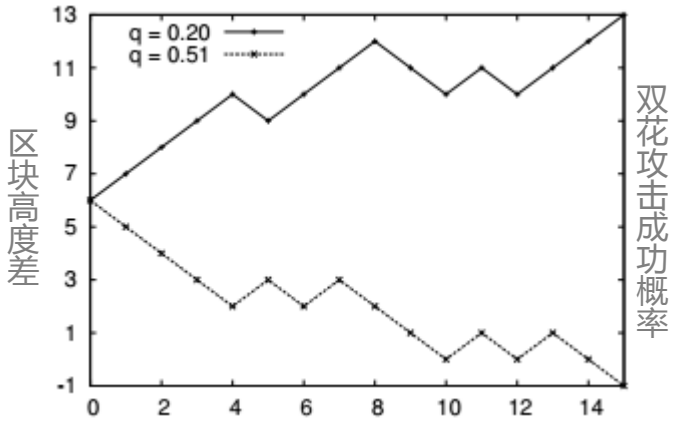
双花问题，即双重支付问题，是指同一笔钱同时用作不同交易。



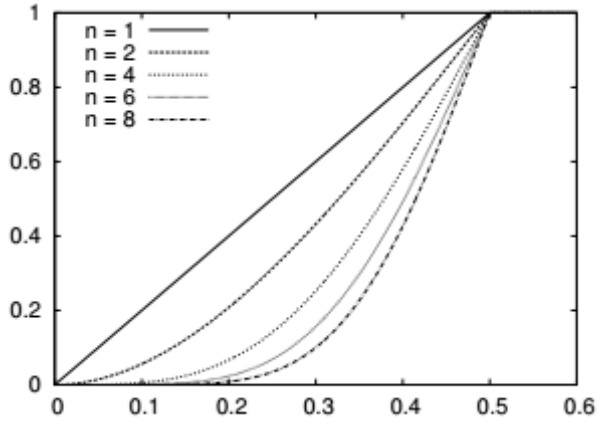
建模成二项式随机过程（binomial random walk）。一个诚实节点创建新区块的概率为p，攻击者创建新区块的概率为q，p+q=1.

$$z_{i+1}=\begin{cases} z_i+1 & \text{概率p} \\ z_i-1 & \text{概率}q \end{cases}$$

51%的由来



延迟6个区块确认的由来



物联网在区块链+能源中的比重

10%

Metering

Data exchange between stakeholders of Smart Grid applications, intelligent control systems, as well as the standardization of data transfers

20%

Grid management

Value exchanged between devices in the form of data, network access, currencies, compute cycles, contracts for ongoing service, trusted introductions to other devices

40%

Decentralized Generation

Development of EV Charging Stations that use blockchain based smart contracts to authenticate users and managing the billing process

20%

EV Charging

Real-time metering of local energy generation and P2P transaction management

10%

IoT

Continuous identification of new applications of blockchain for IoT and the Connected Home markets

Indigo ADVISORY