CAICT 中国信通院

白话区块链

——兼论产业和趋势

2018年3月14日

个人简介

卿苏德，博士，毕业于北京邮电大学网络与交换国家重点实验室，师从长江学者廖建新教授，教育部颁发的博士研究生国家奖学金获得者。

现任**中国信息通信研究院（CAICT）**云计算和大数据研究所区块链主管，高级工程师，可信区块链联盟办公室主任，国际电信联盟ITU-T FG DLT分布式账本焦点组评估准则牵头人。

- ✓《“十三五”国家信息化规划》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
- ✓ 中国信通院《全球区块链应用十大趋势》、《区块链在物联网中的应用》等报告的核心编制人员
- ✓ 参加韩国第18届世界知识论坛，发表区块链主旨演讲，该论坛由联合国前秘书长潘基文致辞，美国前国务卿希拉里和法国前总统奥朗德发表主旨演讲。

郑重声明

谨代表个人观点，与单位无关

如有雷同，肯定别人抄袭我的

讲的不好，请随时给我白眼提示

比特币的出现是为了抵御08年经济危机带来的通货膨胀

2008年11月1日，一个自称中本聪(Satoshi Nakamoto)的人发布比特币的白皮书《一种点对点的电子现金系统》

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks
2009年1月3日首相第二次对处于崩溃边缘的银行进行紧急救助

```
00000000  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E  ....;£íýz{.²zÇ,>
00000030  67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA  gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040  4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C  K.^J)«_Iÿÿ...¬+|
00000050  01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D  ......ÿÿÿÿM.ÿÿ..
00000080  01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F  ..EThe Times 03/
00000090  4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C  Jan/2009 Chancel
000000A0  6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20  lor on brink of
000000B0  73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66  second bailout f
000000C0  6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05  or banksÿÿÿÿ..ò.
000000D0  2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27  *....CA.gŠý°þUH'
000000E0  19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6  .gñ¦q0·.\Ö¨(à9.¦
```

比特币创世区块（ genesis block ）

2013年是个分水岭：币圈的沉寂和链圈的萌芽

区块链≠比特币

区块链≈windows操作系统

比特币≈系统里的迅雷软件

”Blockchain”这个单词不在比特币的白皮书里？！

什么是区块链呢？

区块链是一种多方维护、全量备份、信息安全、可编程的分布式数据库技术。

分布式网络，共享账本

集中记账 → **分布记账**

共识与激励，公平记账

单方决策 → **多方共识**

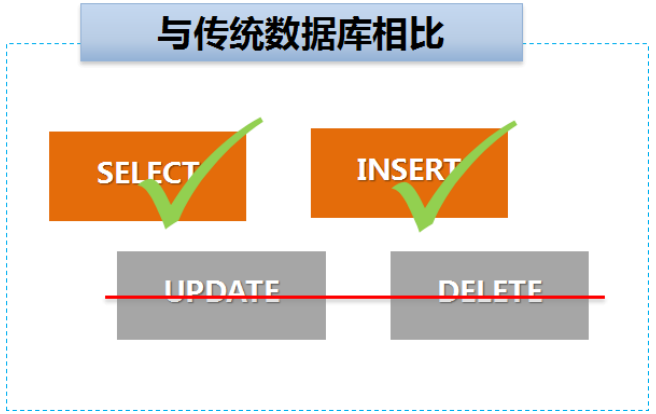
块-链式数据结构，密码可信

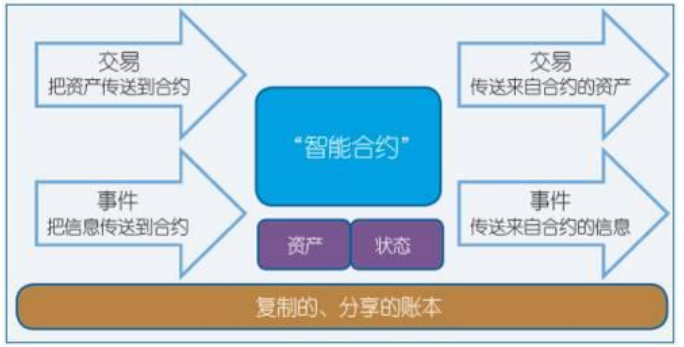
增删改查操作 → **难以篡改**

传统合同代码化，智能合约

外挂合约 → **内置合约**

只有我自己知道，中国银行的账户里有1万元存款
但全世界都知道，我的比特币钱包里有1个比特币





白话区块链

区块链(Blockchain)

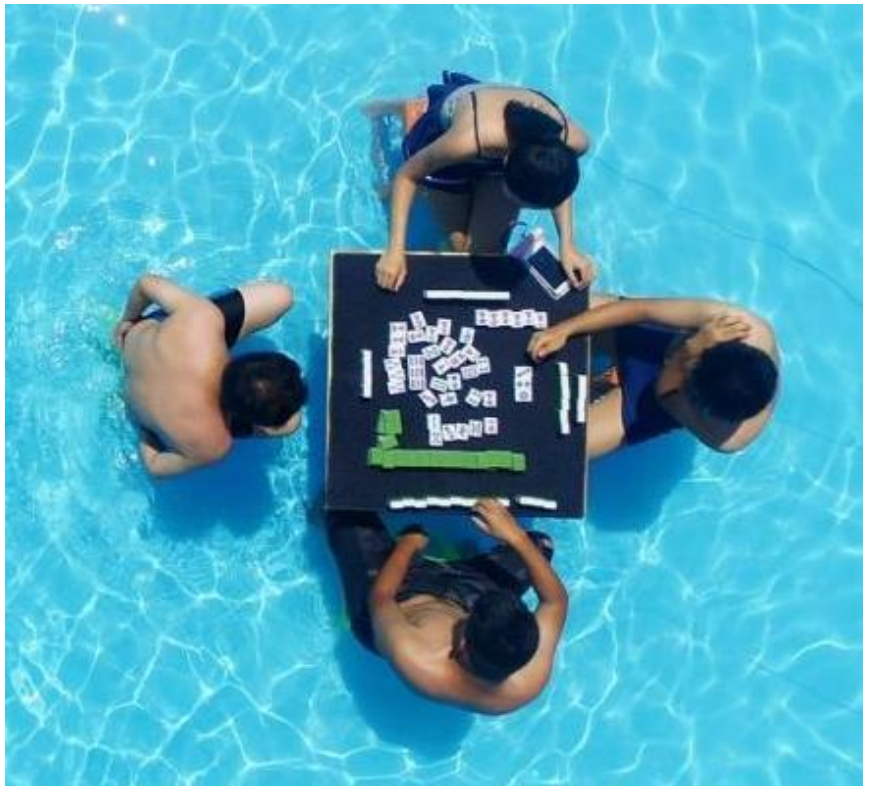
=

区块(Block) + 链(Chain)

为了学区块链，我们打几把麻将！

赵薛忆

卿苏德



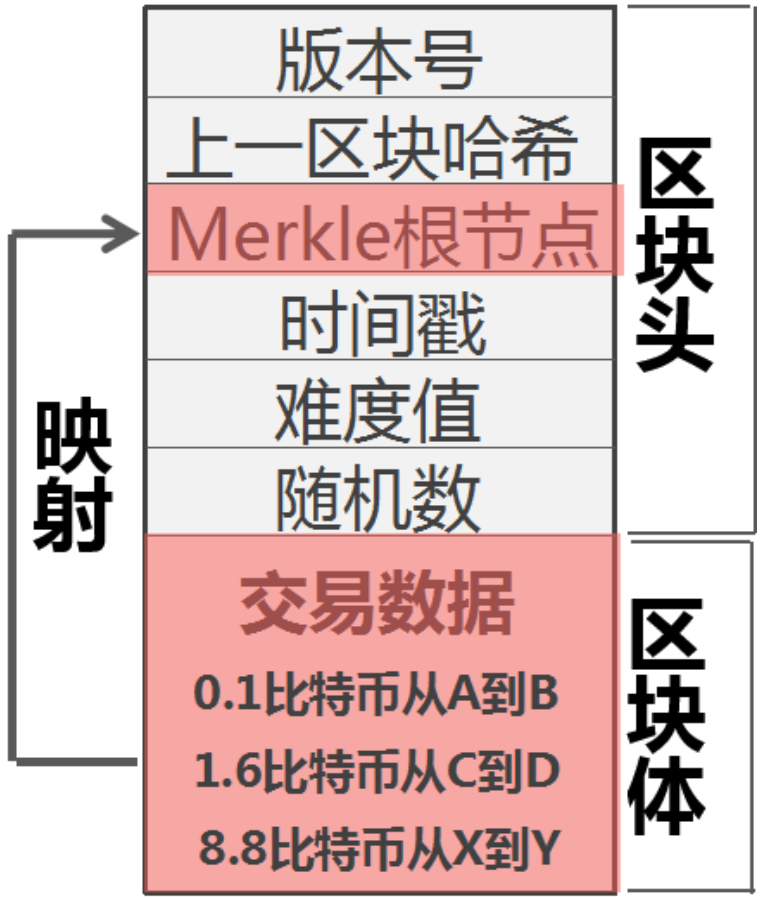
廉志鹏

艾 锋

区块链的“区块”

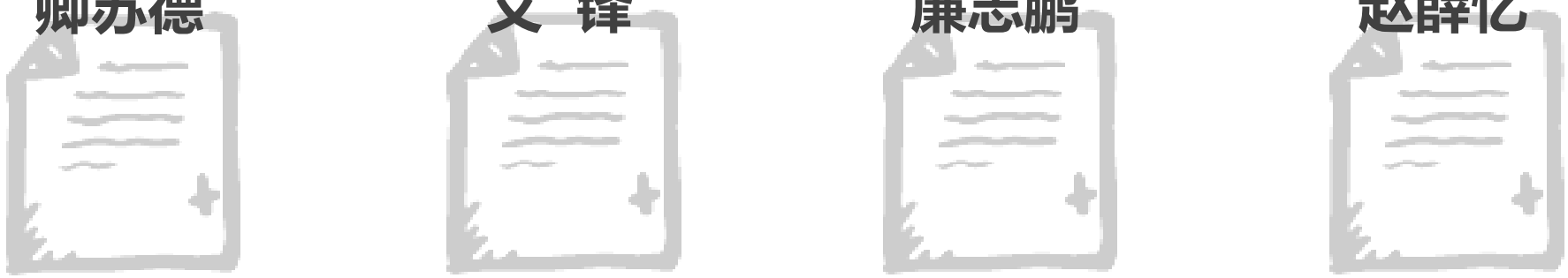
一页账本

区块N



亲兄弟明算账：复式记账法的尴尬症犯了

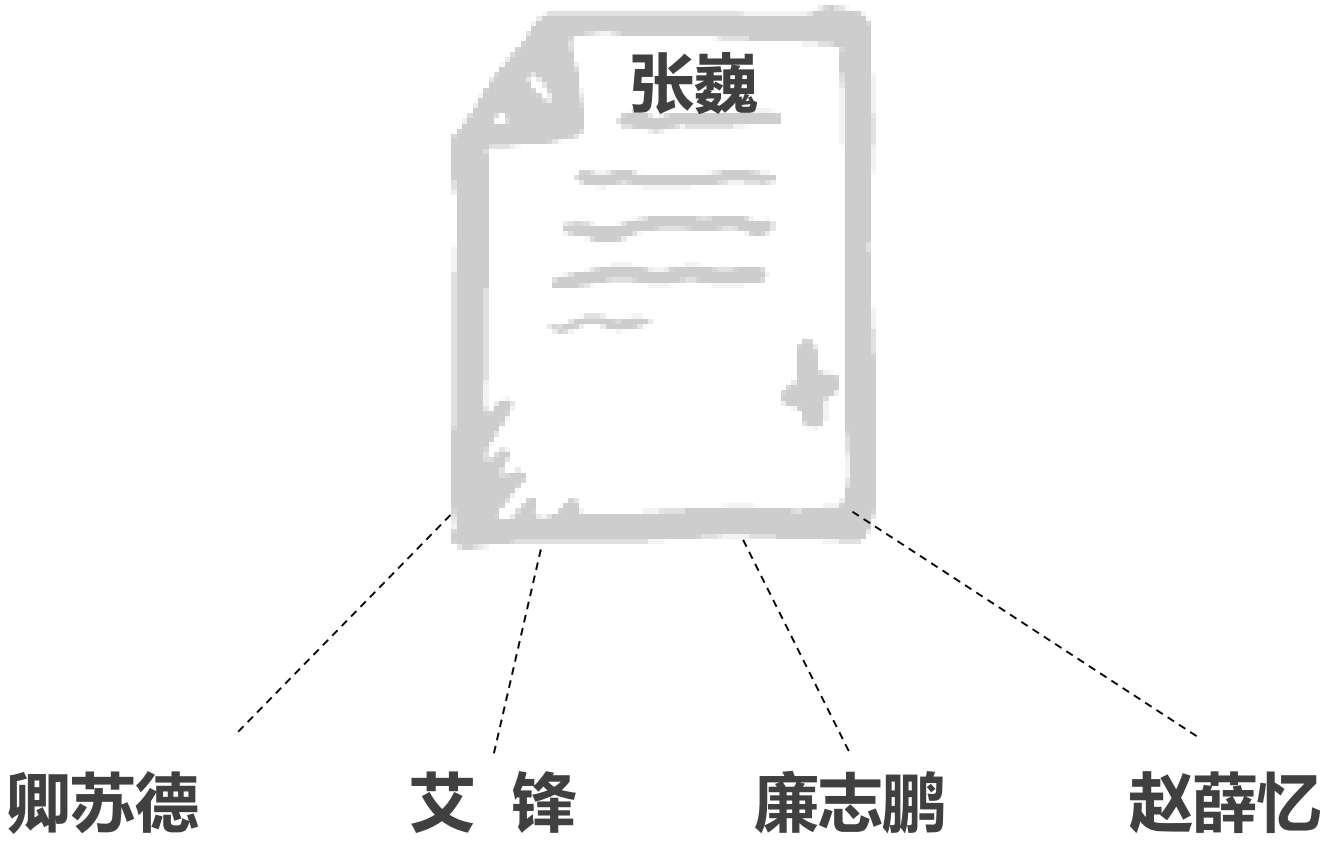
卿苏德　　艾　锋　　廉志鹏　　赵薛忆



卿苏德：赵薛忆欠我100元

赵薛忆：欠卿苏德1元

找一个中心节点信用背书：领导专治各种不服



中介费用高昂：我们四个人打麻将，还要承担张巍晚上的吃住，张巍可能还要加顿夜宵

中介制造信息不对称：张巍说晚上有事（其实是累了），我们支付了额外的10元加班费

中介的效率低：所有的后续牌局都要等张巍审核完，签完字

自己动手丰衣足食：一种貌似完美的解决方案

记账

分而治之，又遇分歧；统一记账，篡改怎办？

卿苏德

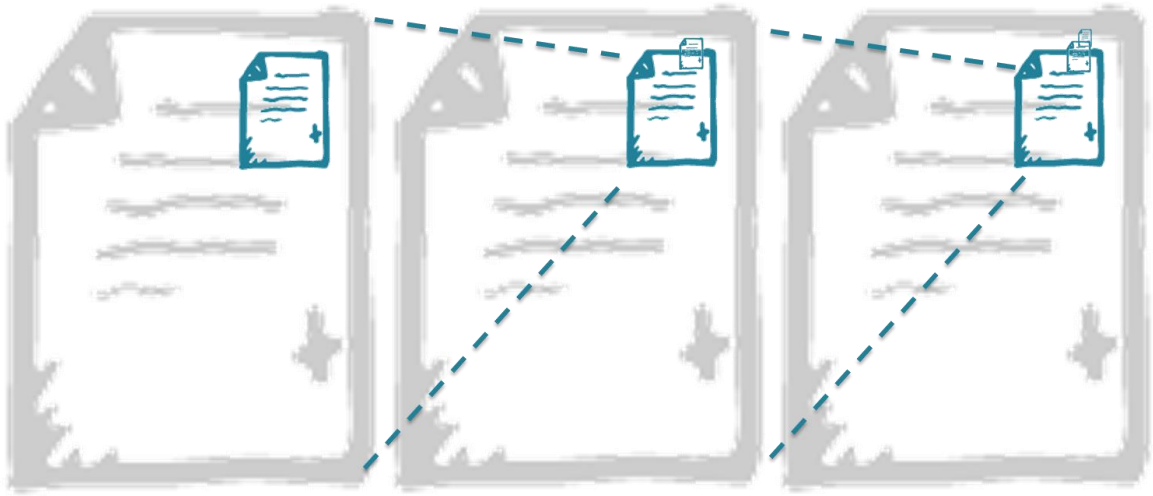
廉志鹏

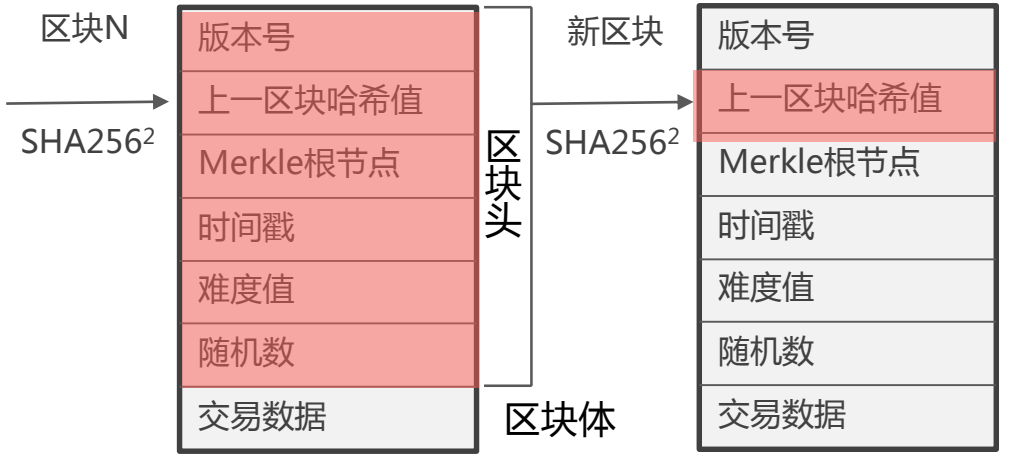
记账

赵薛忆

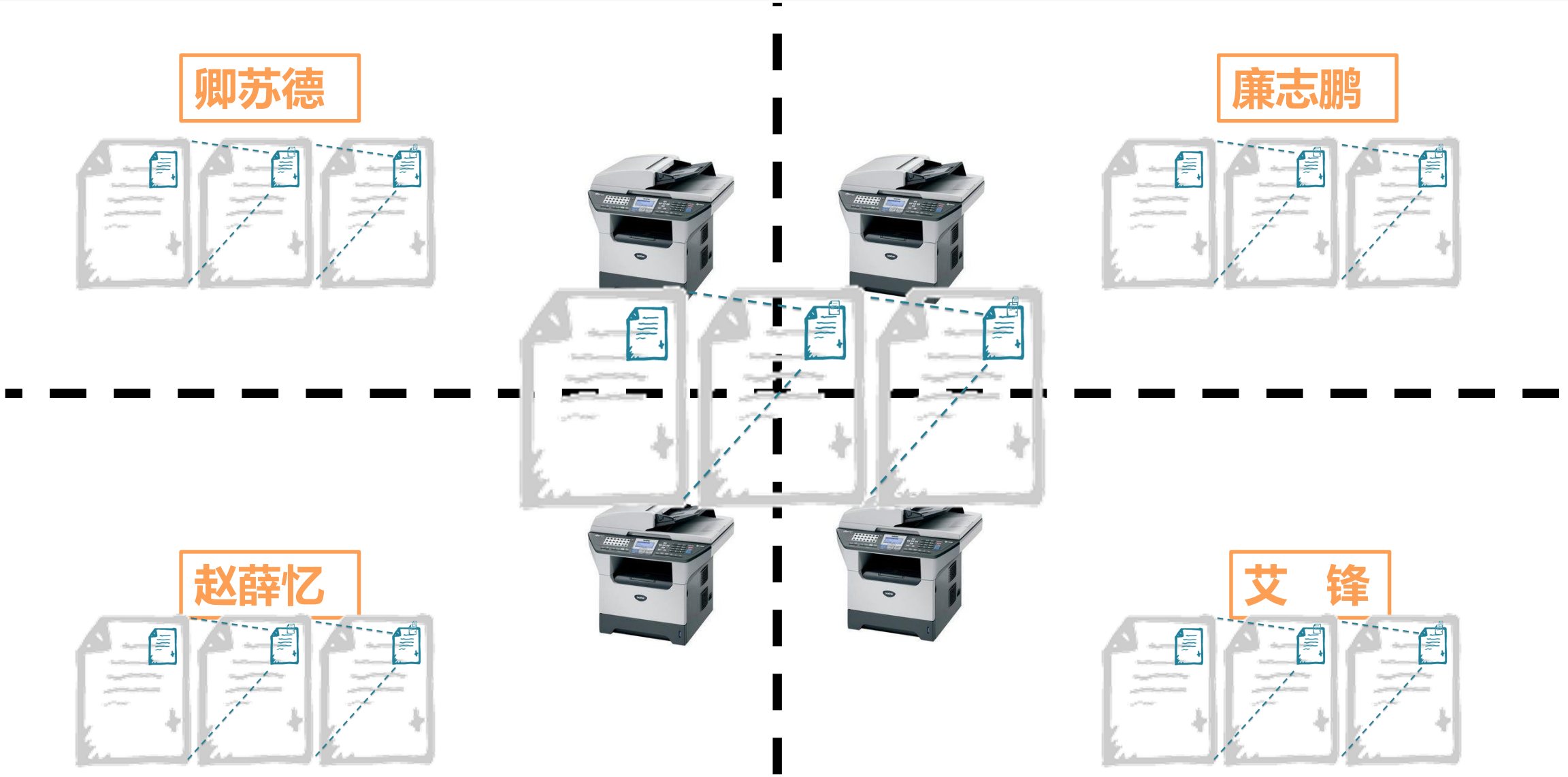
艾　锋

区块链的“链”



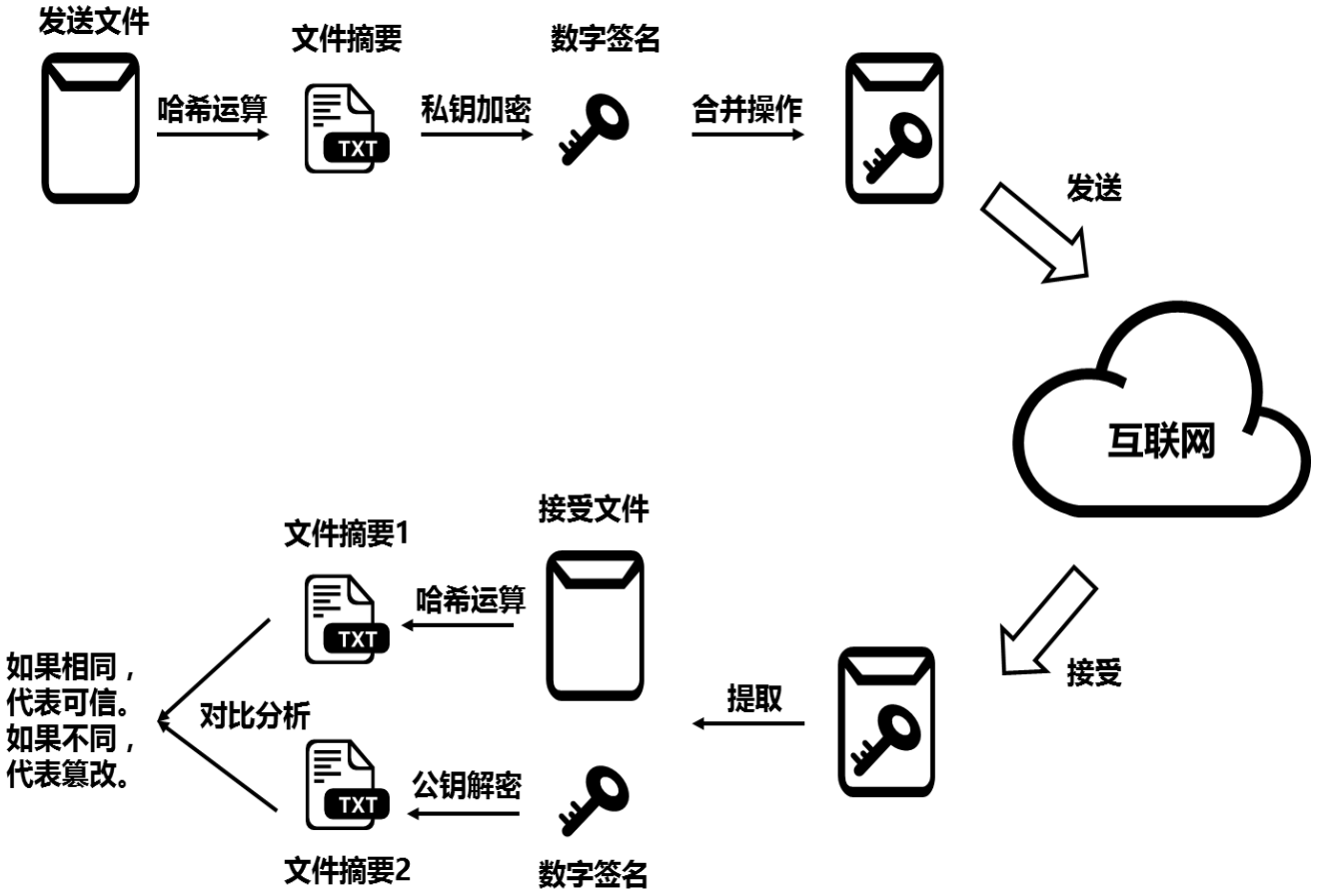

区块N
SHA256²
版本号
上一区块哈希值
Merkle根节点
时间戳
难度值
随机数
交易数据
区块头
区块体
新区块
SHA256²
版本号
上一区块哈希值
Merkle根节点
时间戳
难度值
随机数
交易数据

复印机：全量备份，人手一份



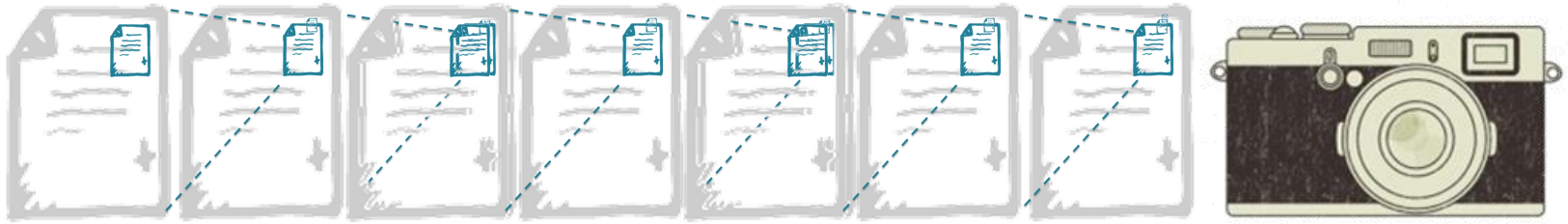
事不关己高高挂起？保险柜保证通信安全

- 要给A传递账本，首先向A申请一个只有A指纹才能打开的保险柜。保险柜有一个缝，可以塞进相片。
- 对要传递的账本拍照，将带相片的下一页账本塞进保险柜。
- 将保险柜和账本原件一起寄给A。
- A收到后，打开保险柜，取出带相片的账本。核对相片与上一页账本的所有信息，如果正确，则追加到账本的最后一页。



区块链的技术架构-1

数据层



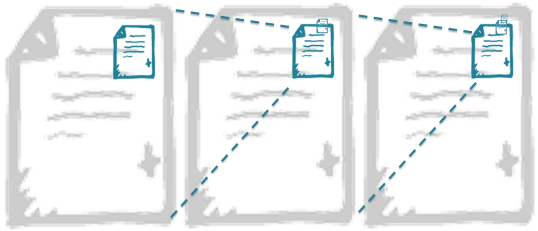
共识层

人手一个副本，验证靠少数服从多数

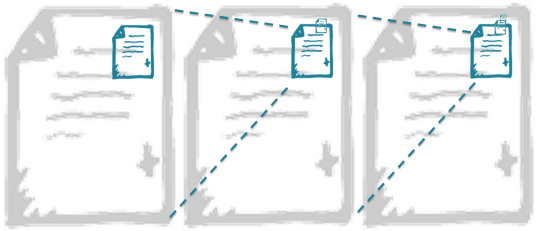
网络层

新的问题：如果全球都来打麻将，如何结算？

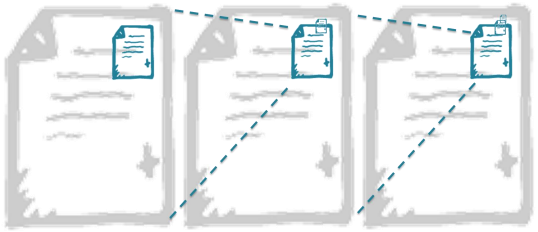
中国人



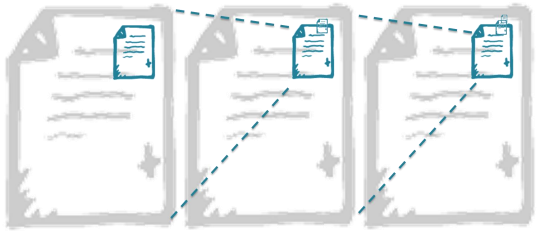
日本人



美国人



德国人



引入代币（筹码）

比特币

比特币是如何利用区块链技术进行价值传递？

预留在比特币中A的指纹

①获取B的指纹

B的指纹

1个比特币

0.9个比特币

0.1个比特币
是矿工手续费

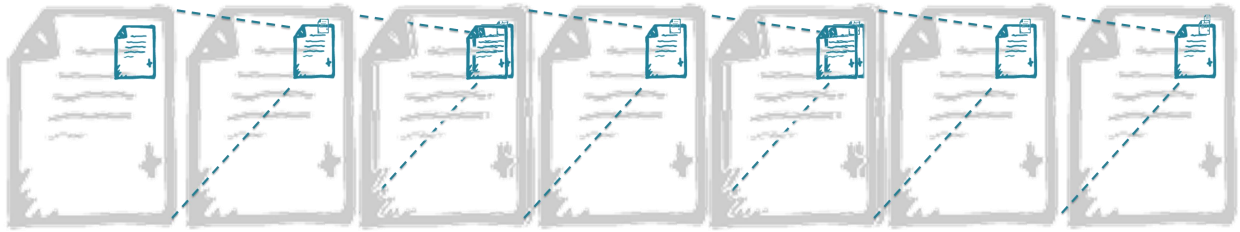
②按上A的指纹，匹配成功后，发送交易

区块的确认记账以后

区块链的技术架构-2

应用层

数据层



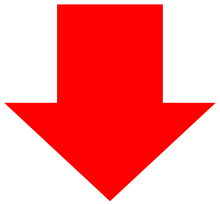
共识层

少数服从多数

网络层

新的问题：联合篡改，如何防止？

双王闯+清一色+三个杠+自摸……



不能指定记账人：疲劳驾驶+容易作假

给予记账人奖励：形成正向激励机制

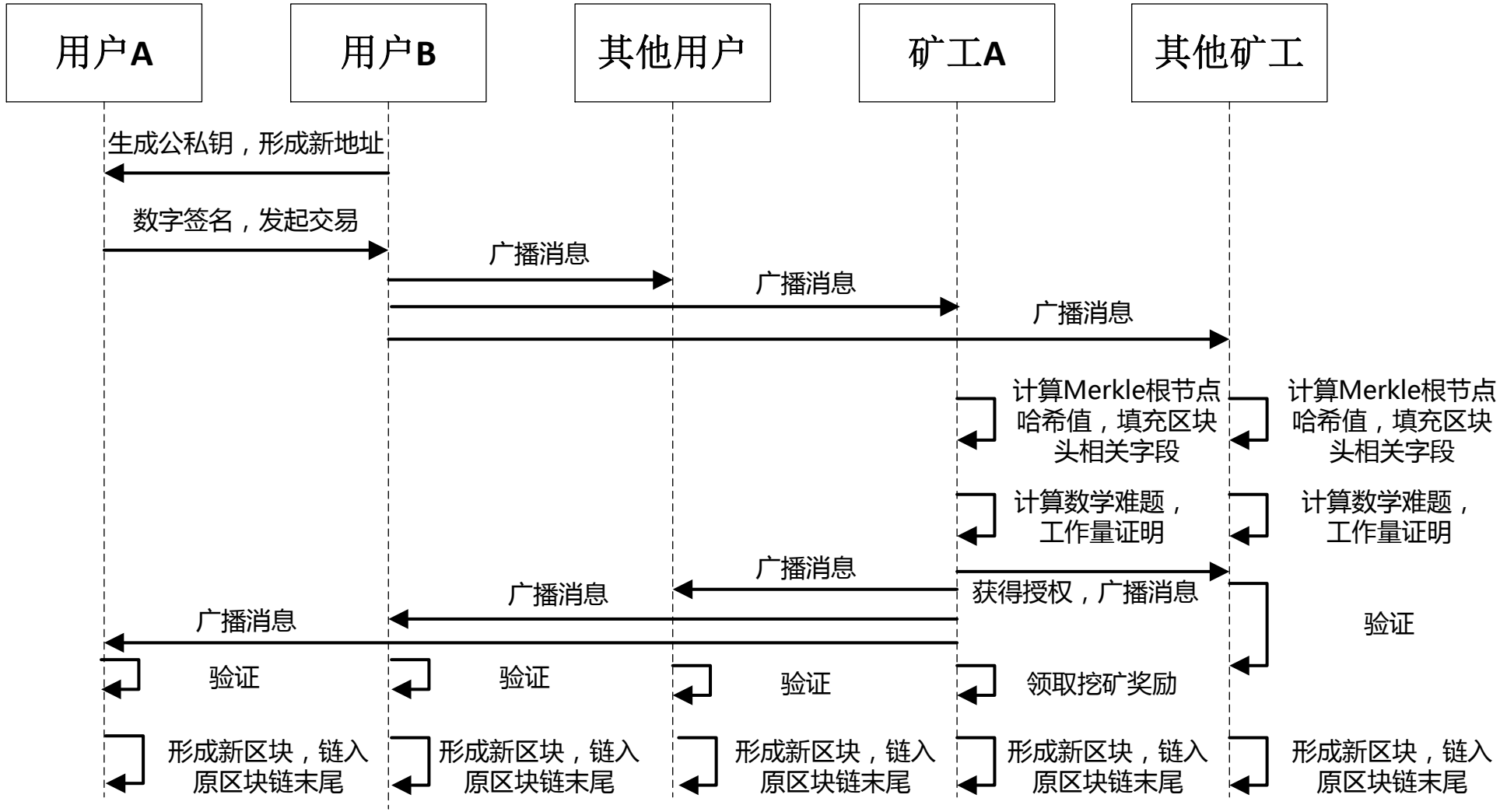
里应外合作假：某大行39亿票据案，用报纸代替纸票贴现，资金拿去炒股导致巨额亏损

前呼后应造假：根据新华网2015年5月报道，五常大米年产105万吨，在售1000万吨

挖矿：公平争夺记账权，用算力证明你的正直

- **工作量证明**：把拍的上一页账本的相片完全打散，要求还原这幅图
- **难度值**：打散程度，主要是为了控制生成区块的时间间隔（十分钟）
- **激励**：拼图完成的，能够得到相应代币（比特币）奖励，可以作为打麻将的筹码

区块链的运转机制

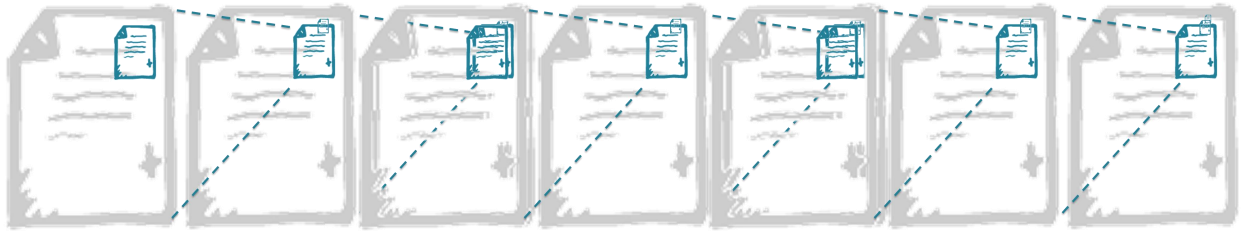

用户A
用户B
其他用户
矿工A
其他矿工
生成公私钥，形成新地址
数字签名，发起交易
广播消息
广播消息
广播消息
计算Merkle根节点哈希值，填充区块头相关字段
计算Merkle根节点哈希值，填充区块头相关字段
计算数学难题，工作量证明
计算数学难题，工作量证明
广播消息
广播消息
广播消息
获得授权，广播消息
验证
验证
验证
验证
领取挖矿奖励
形成新区块，链入原区块链末尾
形成新区块，链入原区块链末尾
形成新区块，链入原区块链末尾
形成新区块，链入原区块链末尾
形成新区块，链入原区块链末尾

区块链的技术架构-3

应用层

加密数字货币

数据层



共识与激励层

少数服从多数

网络层

对于区块链的共识，我们没有形成共识

- POW：劲大的
- POS：钱多的
- DPOS：代理人

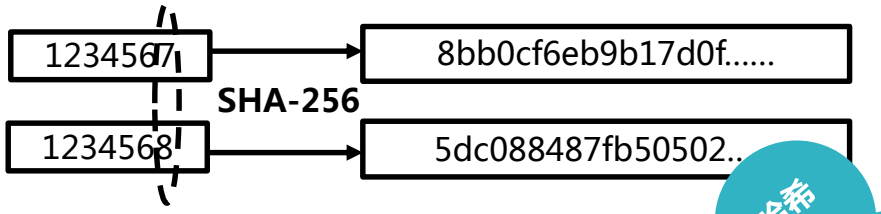
特性	POW	POS	DPOS	PBFT	RBFT
节点管理	公开	公开	公开	准入机制	准入机制
交易延时	高（分钟）	低（秒级）	低（秒级）	低（毫秒级）	低（毫秒级）
吞吐量	低	高	高	高	高
节能	否	是	是	是	是
安全性	<50%算力	<50%股权	<50%验证	>33.3%恶意节点	>33.3%恶意节点
代表应用	bitcoin、ethereum	peercoin	Bitshare	Fabirc	Hyperchain
扩展性	好	好	好	差	差

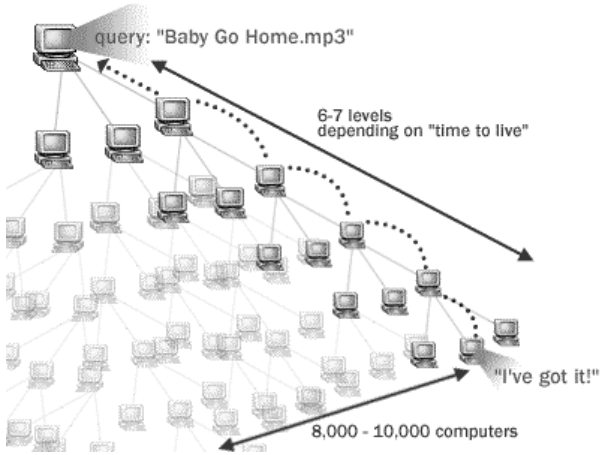
	联动优势	腾讯	复杂美	布比	博晨	智链	太一云	趣链	中兴通讯
共识机制	PoW	BFT-Raft	DLS	dPaxos/PBFT	PBFT改进的LBFT	SOLO/KafKa	PoW/PoS	RBFT	改进的KafKa

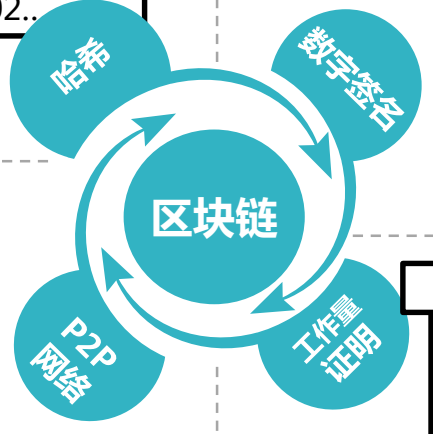
区块链的技术图谱：多种技术的集成创新

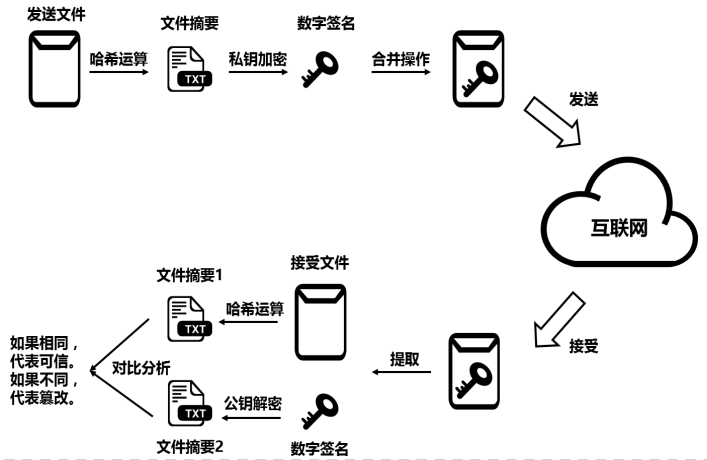
区块链主要运用了四个基础技术，分别是**拍照（SHA256哈希运算）、指纹（数字签名）、复印机（P2P网络）**和**拼图（选举记账人，工作量证明PoW）**

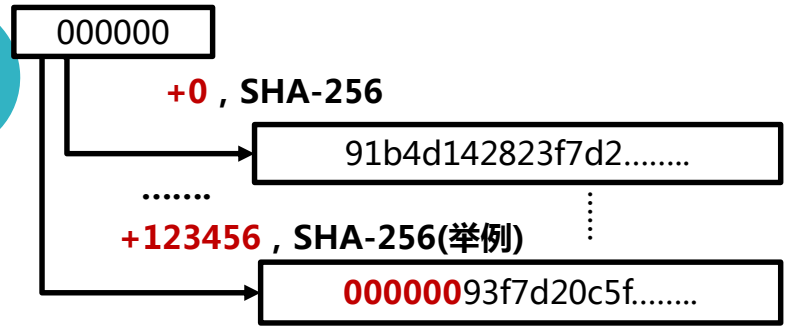
技术的集成创新











区块链行业正处在从1.0到2.0的过渡阶段

区块链1.0 – 数字货币

加密数字货币

2009年

区块链2.0 – 智能合约

加密数字货币 + 智能合约

ethereum

HYPERLEDGER

2020年

区块链3.0 – 价值互联网

成为成熟的数字经济基础设施

分布式商业　数字孪生城市

Token经济　个人信用体系

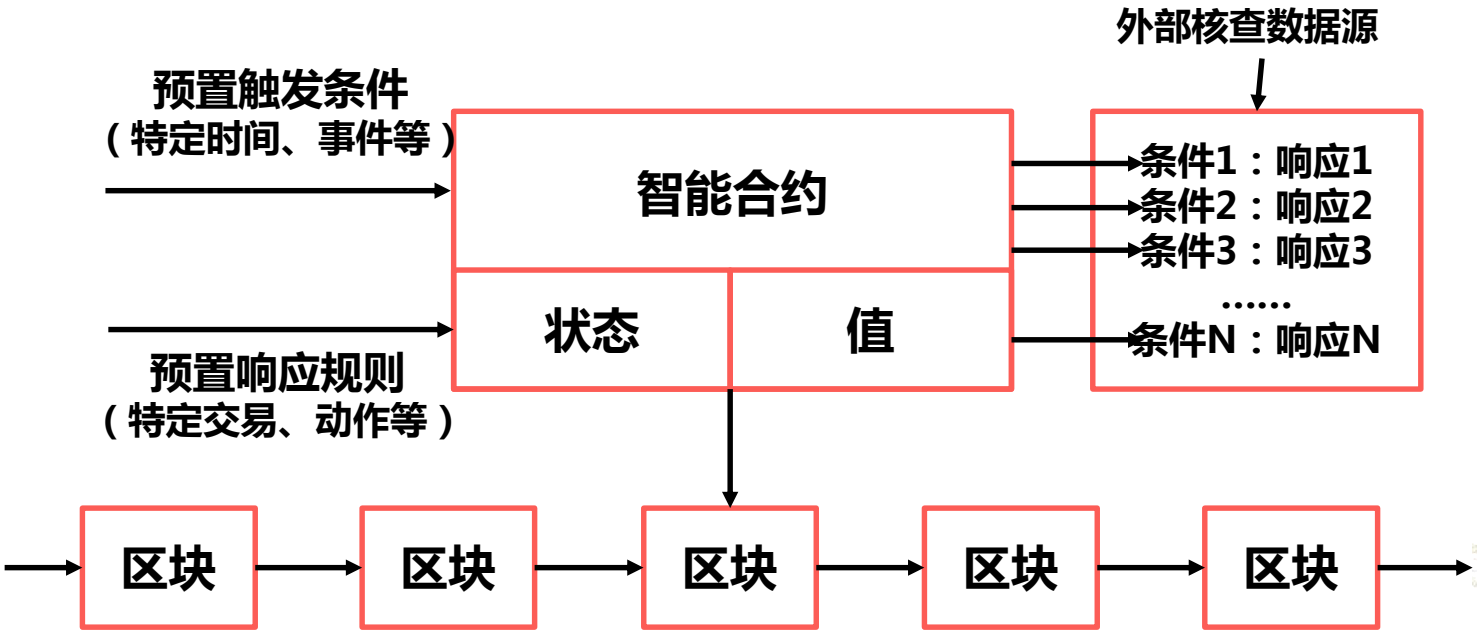
版权

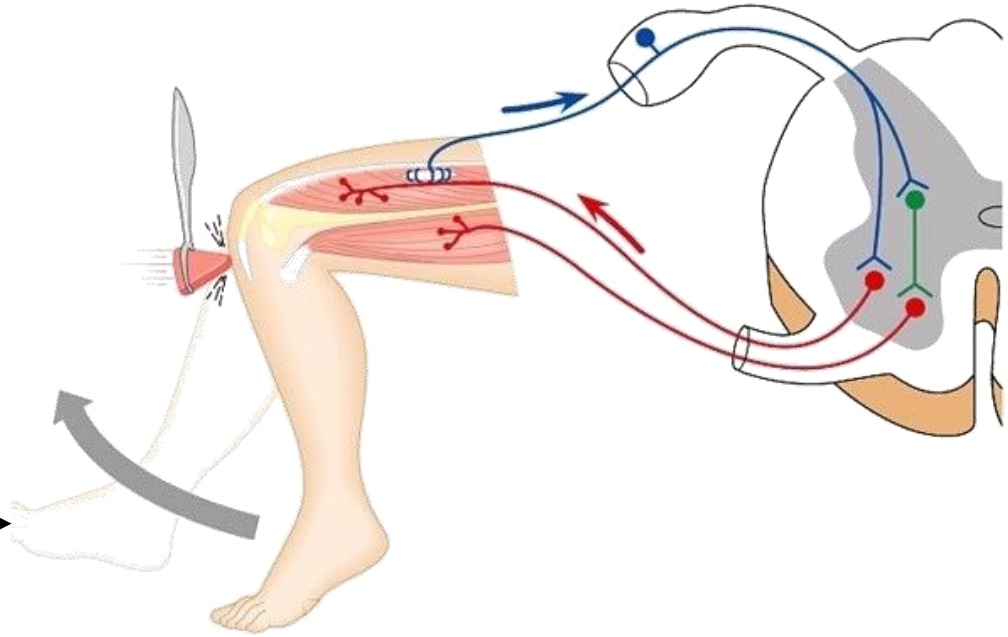
供应链　互助保险

2030年

智能合约：代码即法律（Code is Law）

智能合约是由事件驱动的、具有状态的、存储和运行在区块链上的程序。





智能合约的一个简单例子

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（根据新华社报道），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

区块链的技术架构-4

应用层

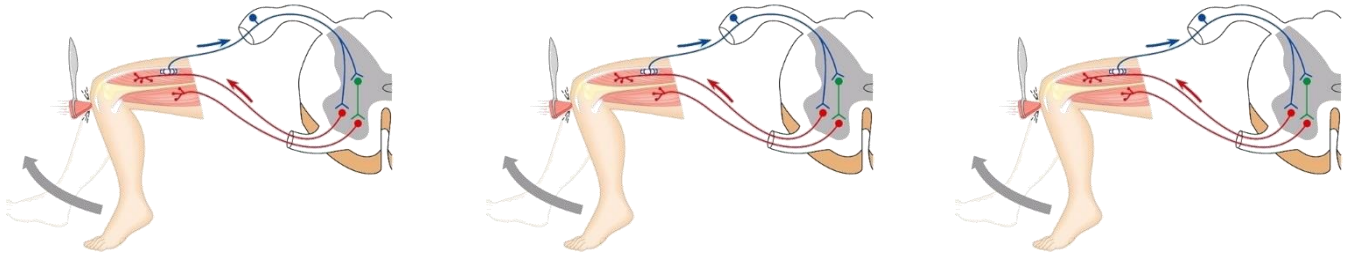
智能合约层

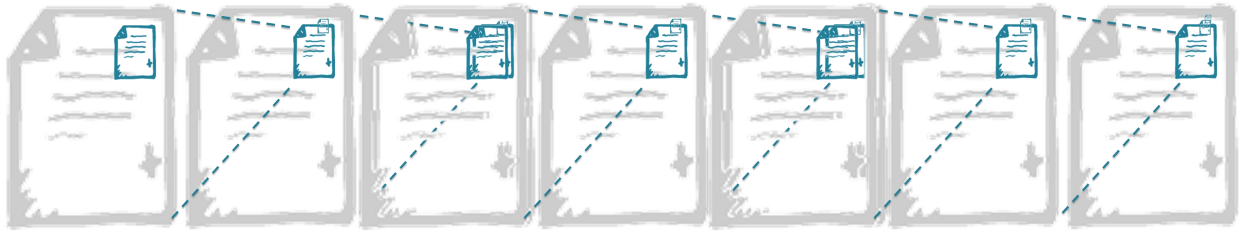
数据层

共识与激励层

网络层

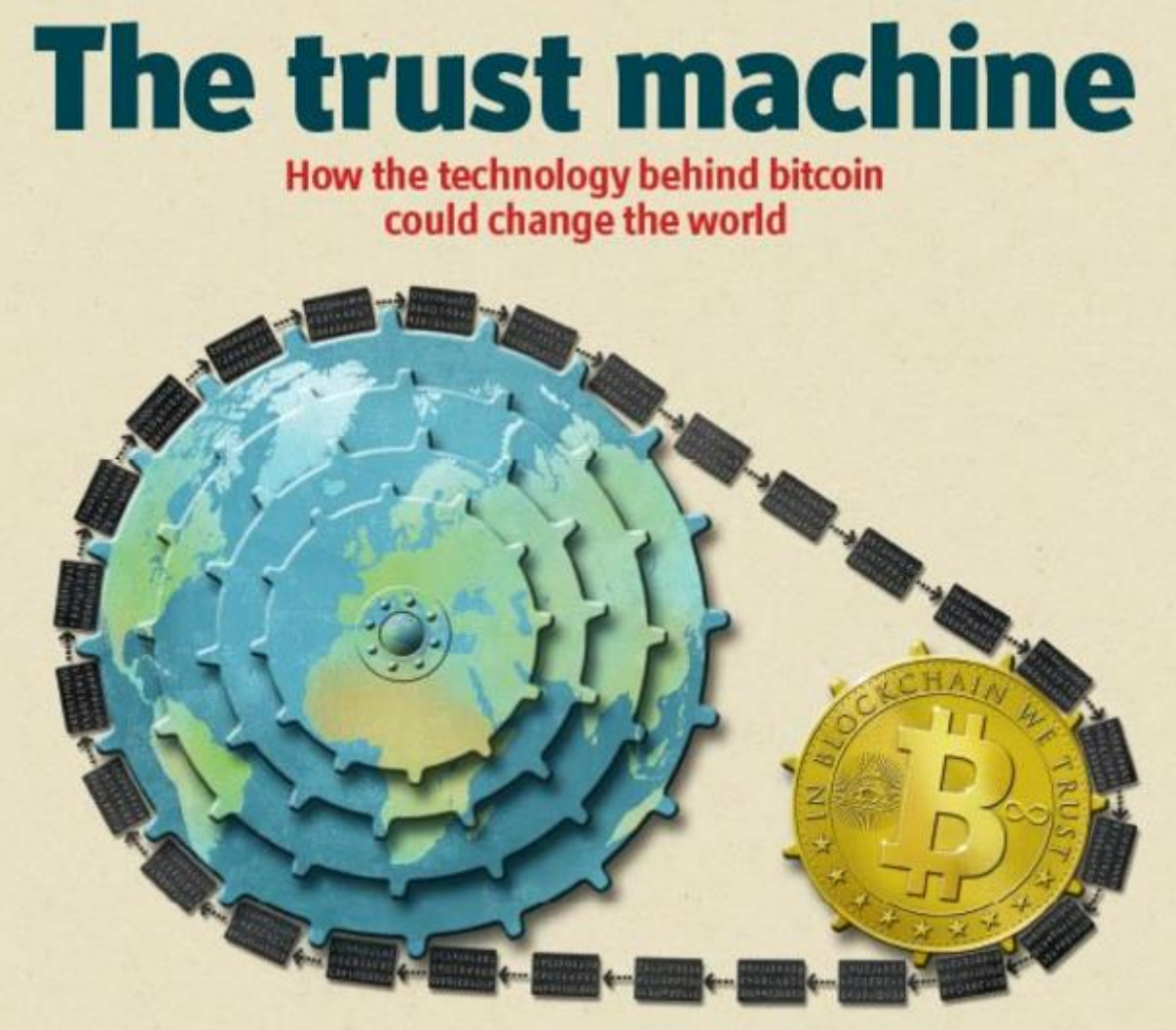
加密数字货币





少数服从多数

区块链是信任建立的机器



区块链是一种多方共同维护，用高度冗余的数据实现低成本的信任，用密码学保证信息安全和权属安全，用共识机制和网络通信形成防篡改、防作伪的信任建立机制和新型协作范式。

本质上，区块链提供了一种在不可信网络中进行价值传递交换的可信通道。

用区块链实现价值传递：数字经济时代的基础设施

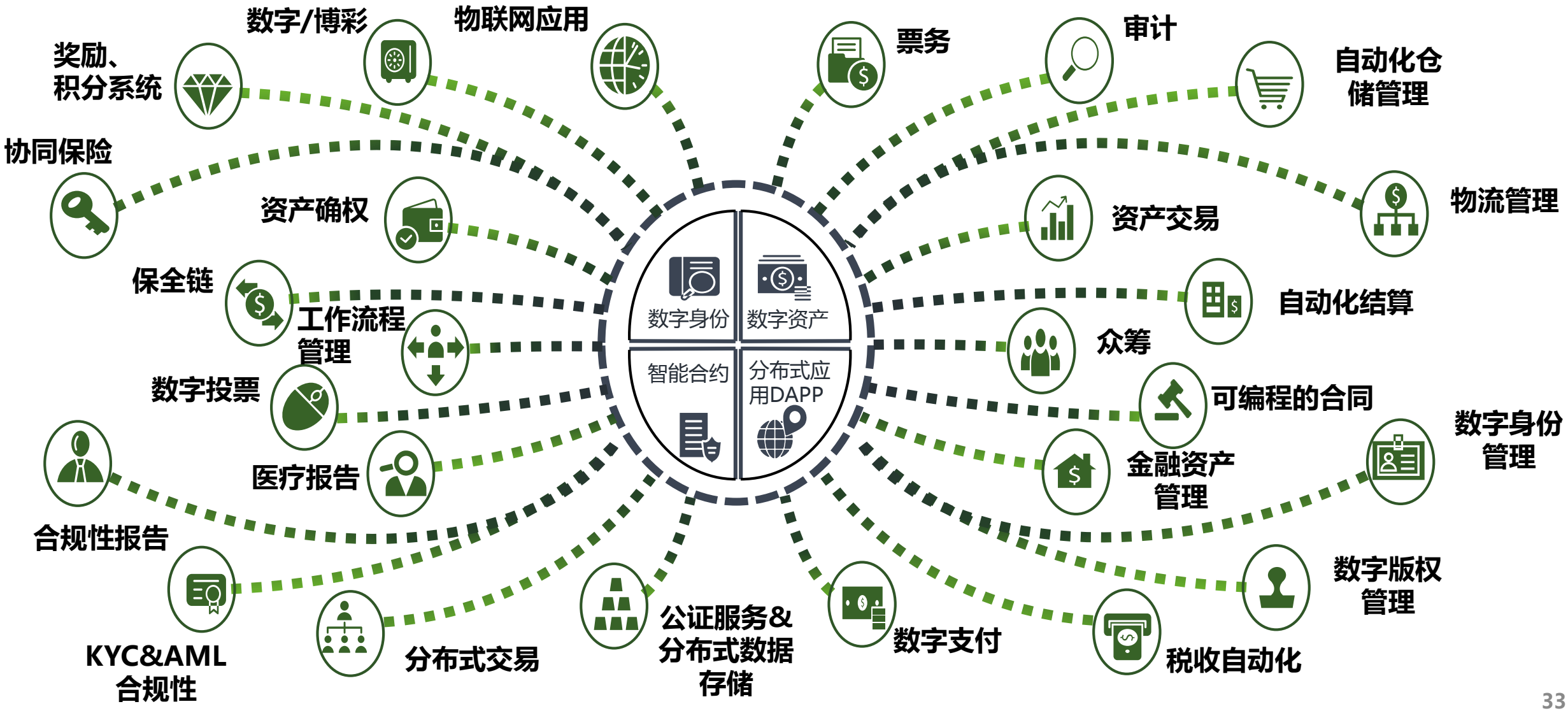
	信息互联网	传递价值互联网
传递对象	数据即信息	数据即资产/价值
技术要求	信息要广泛传播	价值禁止复制、防止双花

区块链技术是现有互联网技术的补充，可以不依赖任何中心化的信用中介机构就能实现可靠的点对点的价值传递。

缺乏信任的问题 → 加速金融数字化，提升信息透明可信 → 建立信任的机制

信息流和资金流分离 → 即时清结算，节省成本，提升效率 → 整合信息流和资金流

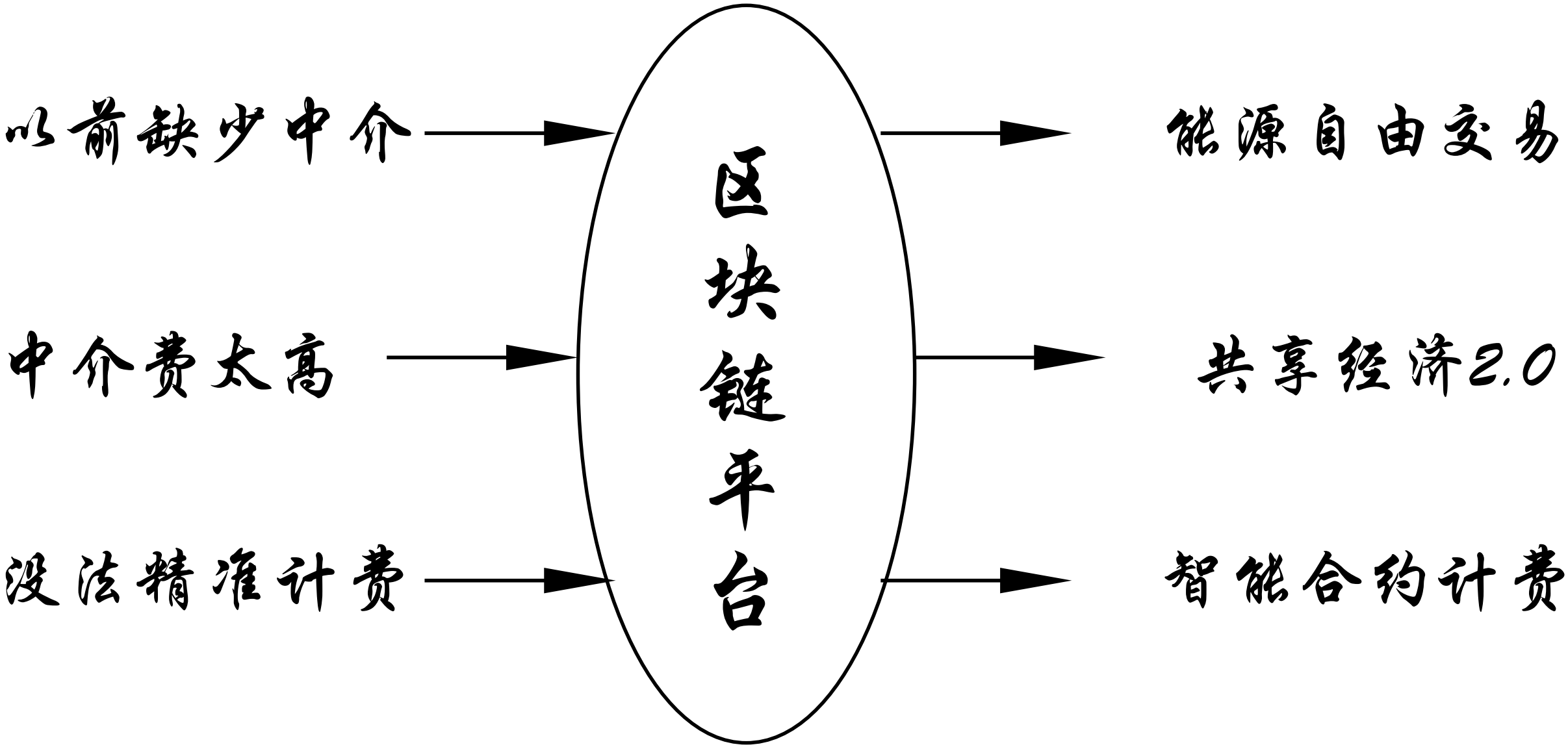
目前区块链技术的主要应用场景



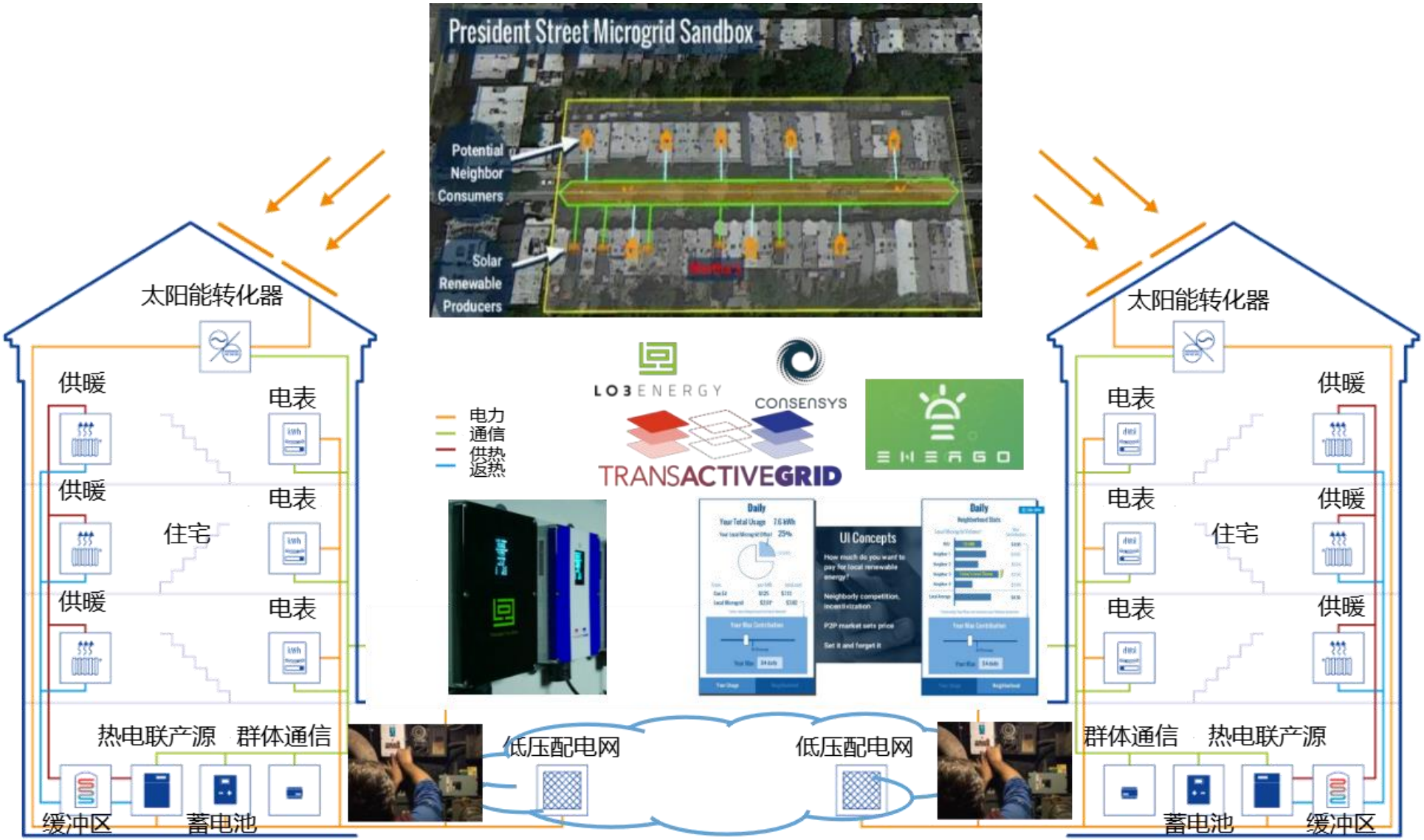

CAICT
Automatic
Connective
Intelligent
Convergent
Traceable

联 智 融 源

说是去中介，结果自己成了新中介

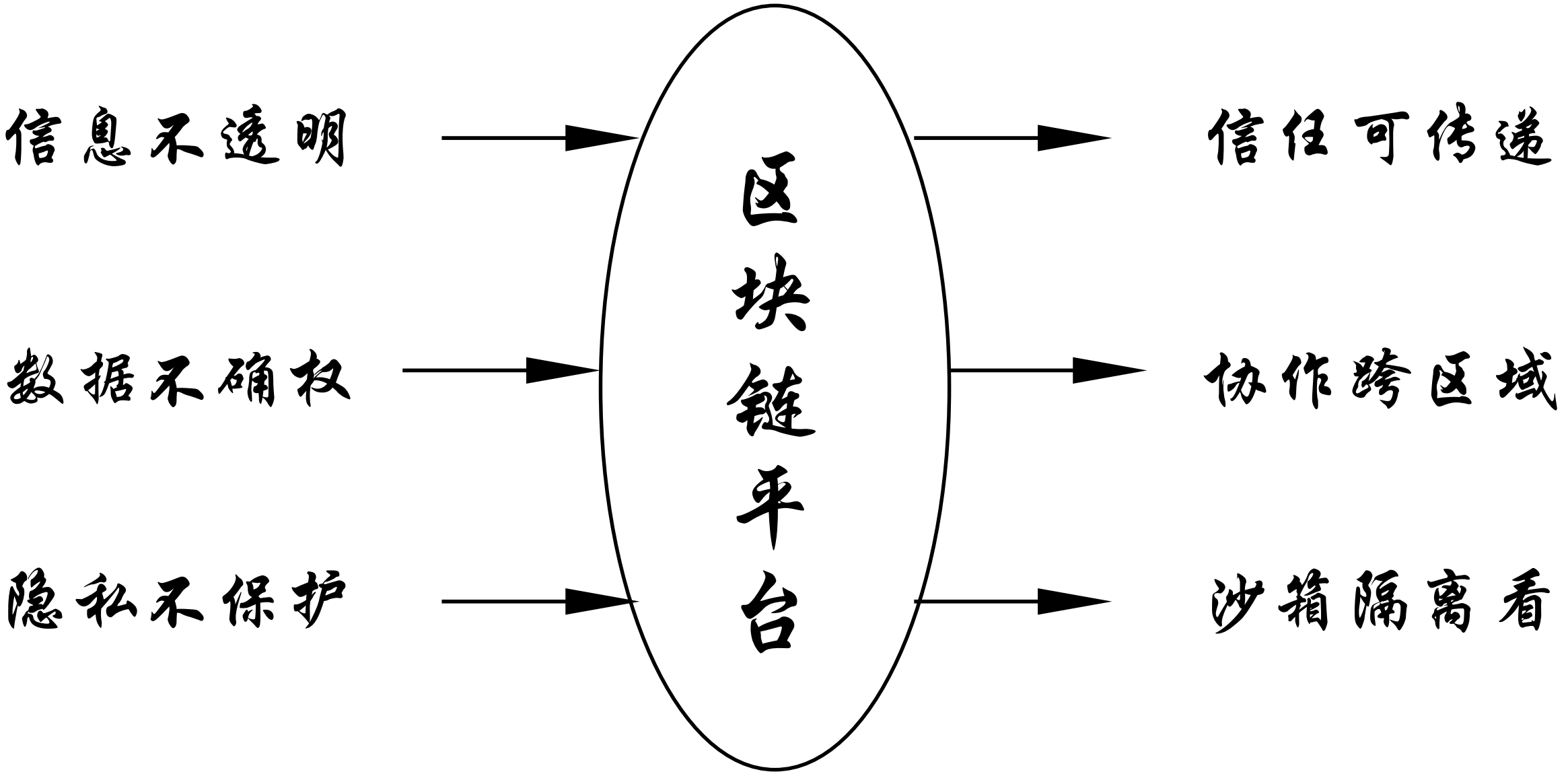


能源的自由交易

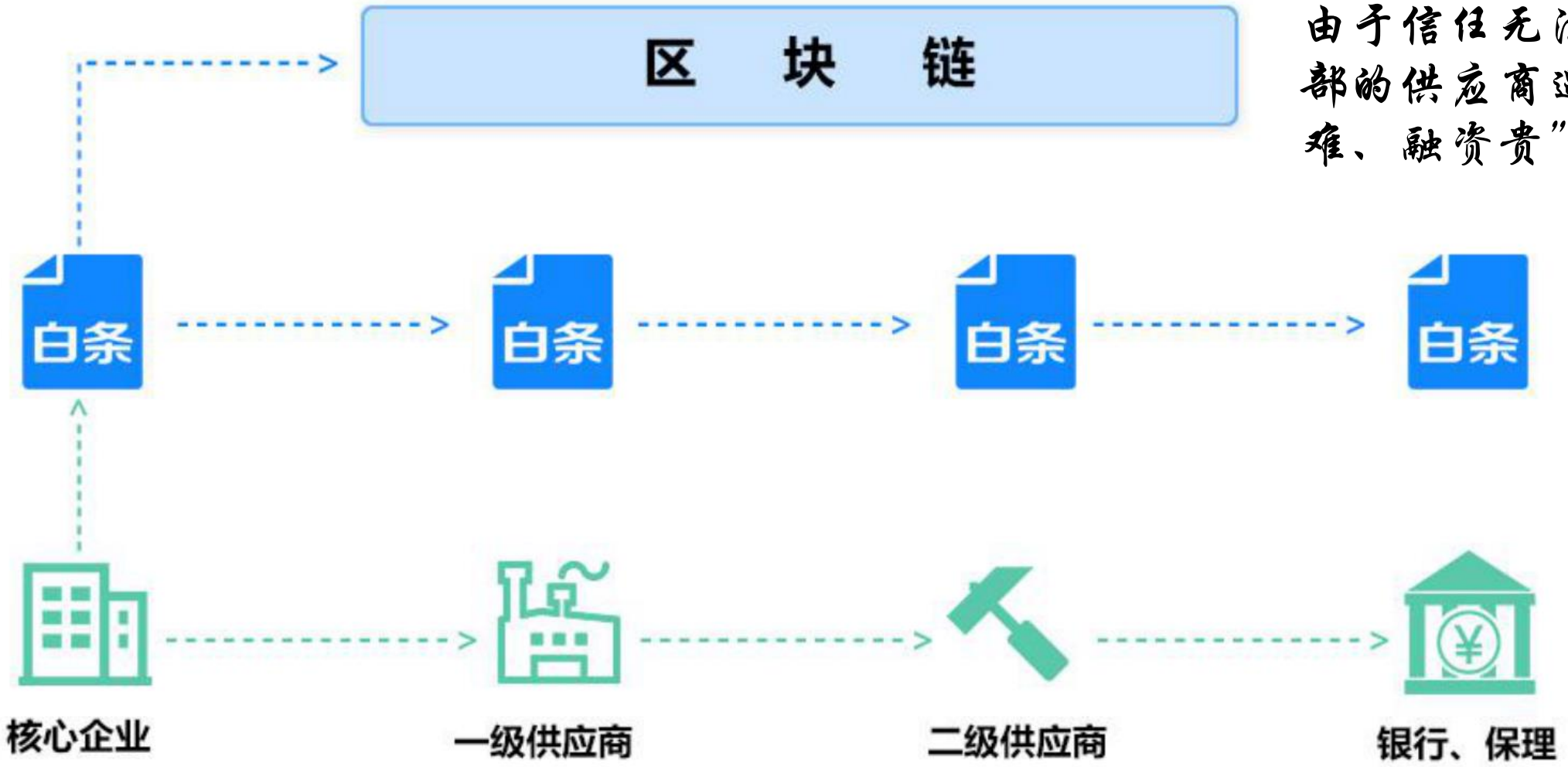

President Street Microgrid Sandbox
Potential
Neighbor
Consumers
Solar
Renewable
Producers
太阳能转化器
供暖
电表
住宅
热电联产源
群体通信
缓冲区
蓄电池
低压配电网
电力
通信
供热
返热
LO3ENERGY
CONSENSYS
TRANSACTIVEGRID
ENERGO
UI Concepts
Daily


CAICT
Automatic
Connective
Intelligent
Convergent
Traceable
联 智 融 源

信息的冗余确保了低成本地建立信任



供应链金融的融资



由于信任无法传递，尾部的供应商遇到“融资难、融资贵”的难题

数字白条，在供应链金融的区块链上流转

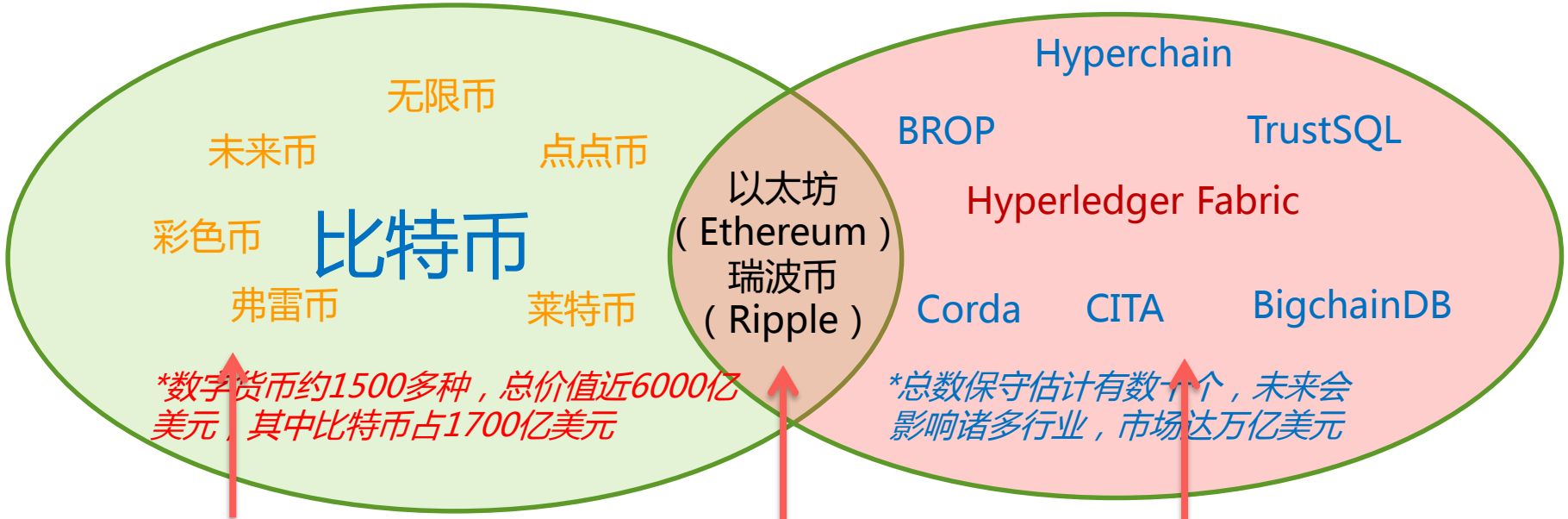
产业现状：发展区块链两大阵营——币圈和链圈

币圈

在区块链上发行加密数字货币，进行价值交换

链圈

用区块链技术解决企业信息化问题，传递信任



公有链用币做激励

有重合的地方

联盟链可以没有币

空气币可以没有链

我国在芯片、矿机、矿池的先发优势

矿机

矿机异军突起，影响芯片制造的现有格局

- ✓ 当前全球三大比特币挖矿机厂商均为中国企业
- ✓ 2017年12月，比特大陆向台积电10nm晶圆订单已超华为海思
- ✓ 带动芯片设计发展，比特大陆于2017年11月发布首款面向AI应用的张量处理器（TPU），对标谷歌，直接叫板寒武纪、深鉴科技等

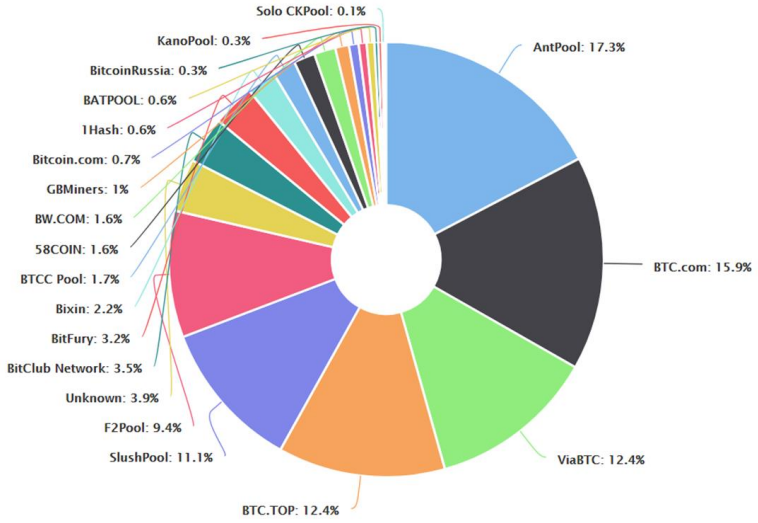
能源消耗和社会影响巨大

- ✓ 根据18年1月数据，挖矿每年约用31Twh，已超爱尔兰全年用电量
- ✓ 挖矿导致显卡脱销，不论是Nvidia还是AMD显卡，价格接近翻倍
- ✓ 每台矿机收益约80-120元，平均6-8个月回本，90后辞职挖矿成时髦

矿池和矿场

中国矿池全球领先，彰显先发优势

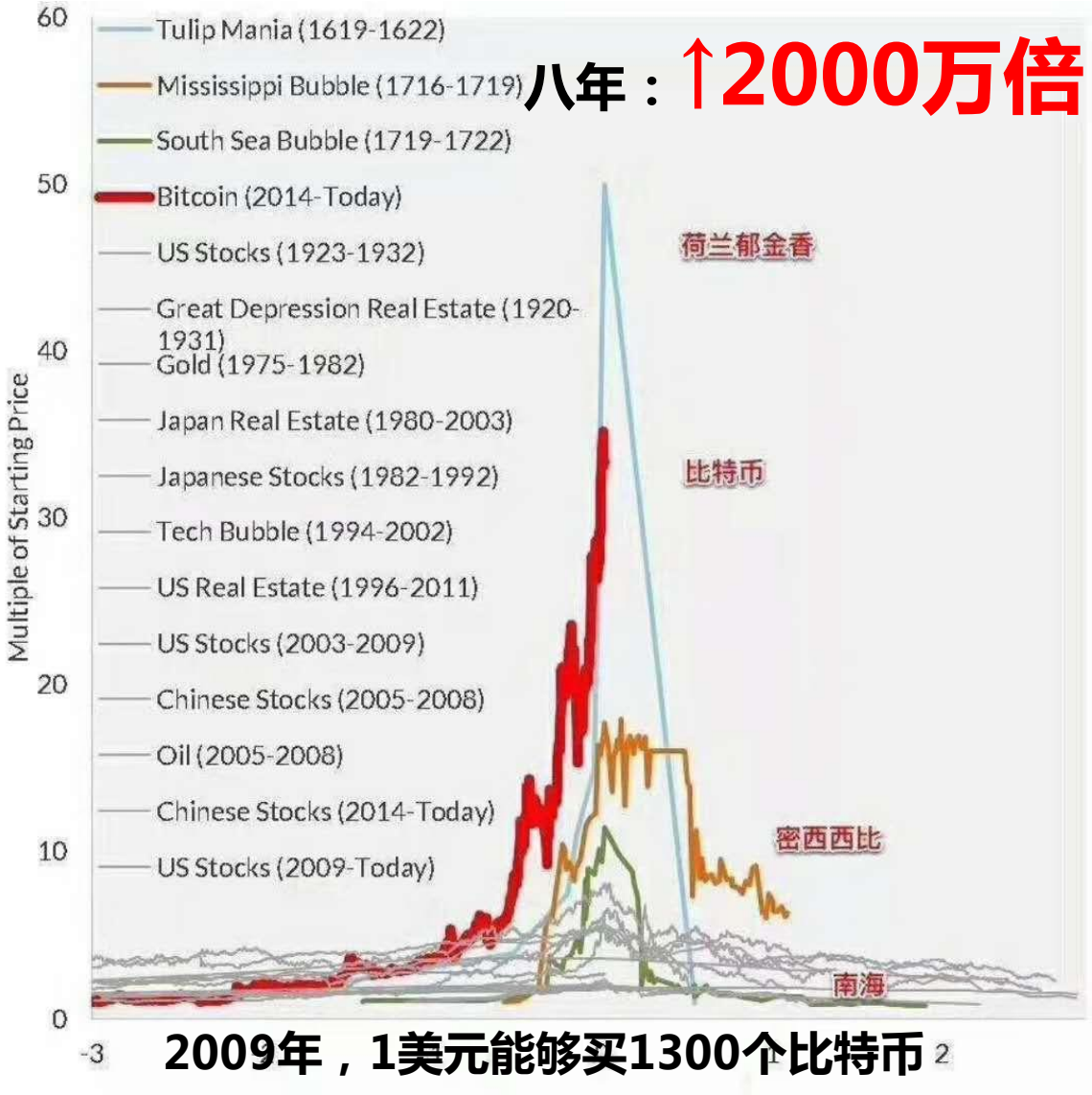
- ✓ 18年1月数据，全球算力排名前三的都是中国矿池
- ✓ 矿场分布在新疆、内蒙、四川等地，随季节（发电站蓄水量）迁徙，逐步向北欧、俄罗斯迁移



算力越发集中化，违背初衷

- ✓ 全球共19个大矿池，有中心化趋势
- ✓ 矿池运营、挖矿软件手续费高昂

比特币为什么一路飙升，逐渐成为弱国躲避经济制裁的工具



2009年，1美元能够买1300个比特币

2017年12月，2万美元买1个比特币

The Telegraph HOME | NEWS | SPO

News

UK | World | Politics | Science | Education | Health | Brexit | Royals | Investigations

News

North Korea may have made as much as $200 million from Bitcoin, according to expert

share

North Korea may have amassed hundreds of millions of dollars in Bitcoin

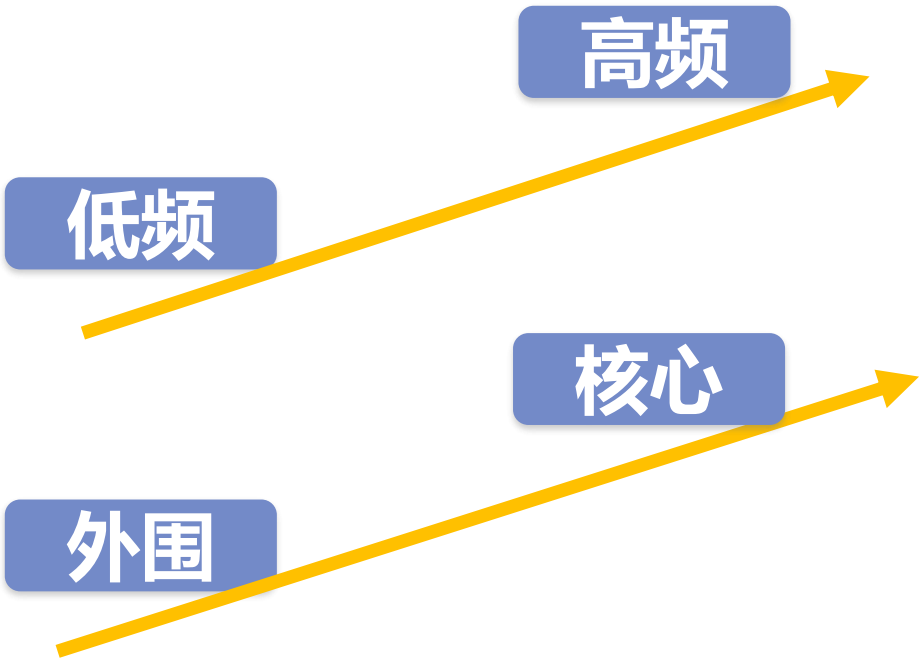
By **Nicola Smith**, TAIPEI

5 MARCH 2018 • 4:10AM

North Korea may have raked in more than $200 million in digital cryptocurrency transactions last year, diluting the impact of stiff international sanctions over its nuclear and missiles programme.

国内金融机构积极试水区块链应用

基本上都处在概念验证阶段，尚未大规模商用。



部分金融机构的区块链试点项目

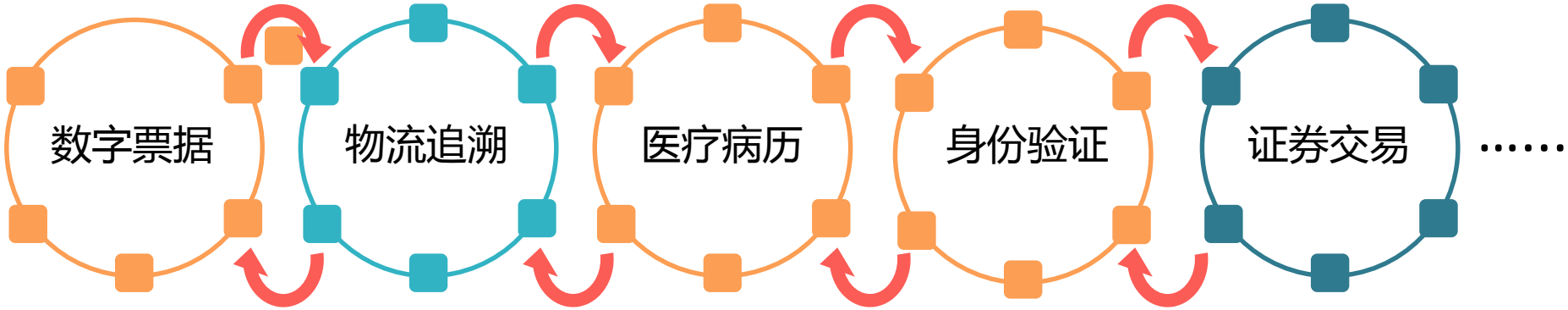
典型应用	机构
基于区块链的数字票据	上海票据交易所
应收账款管理	浙商银行
信用证	民生银行、中信银行
资产证券化ABS	京东、百度
精准扶贫	工商银行、众安保险
积分管理	泰康保险
人民币现钞管理	人民银行南京分行
数字保单与保单质押登记	上海保险交易所

区块链技术持续迭代更新，跨链互通需求增多

技术迭代

链上	解决性能低下的问题	链下
单链	解决扩展适配的问题	多链
孤链	加速价值流通增值	跨链
区块链	区块树、区块图的出现	分布式账本

跨链流通



跨链：价值要在不同区块链系统中流通、增值

可信区块链标准：因为透明，所以可信

区块链的
需求侧

- ✓围绕最终用户视角
- ✓构建统一话语体系
- ✓行业的最高水准
- ✓可实现、可验证
- ✓与技术架构中立

区块链技术
供给侧

不同区块链厂商由于解决方案不一样，技术架构、通信协议和实现方法都不一致，在将解决方案大规模部署至生产环境之前，系统的性能、可扩展性、安全性、稳定性和可维护性等都需要严格的测试验证

国内首个可信区块链标准与评测

《可信区块链第1部分：区块链技术参考框架》
《可信区块链第2部分：总体要求和评价指标》
《可信区块链第3部分：评测方法》

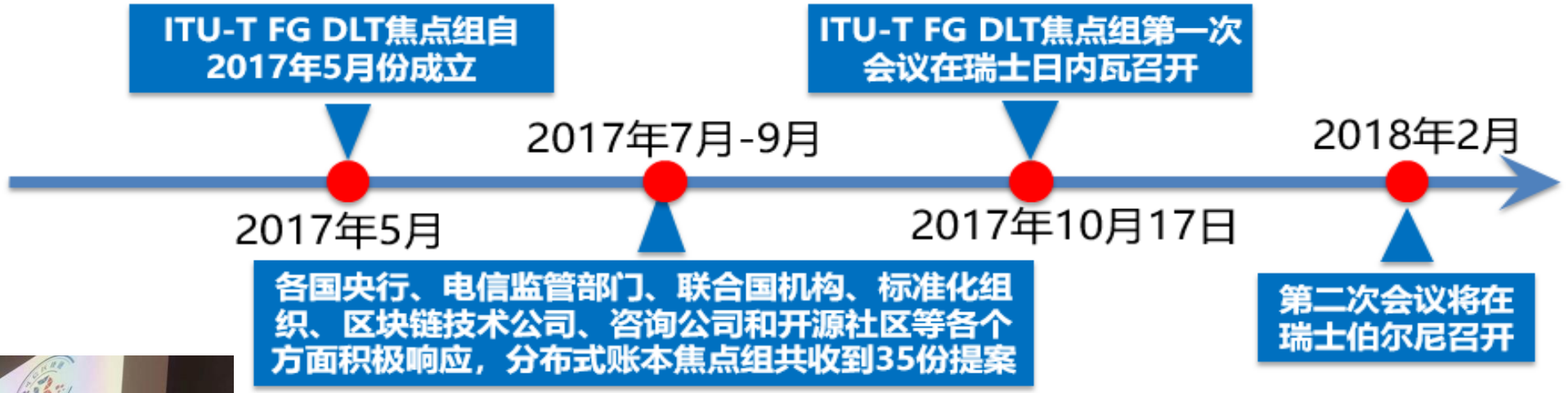
（企业）信息披露 → （测试机构）测试验证 → （专家）公证评审 → （联盟）大会颁证

严格按照《可信区块链》系列标准进行测试

全国4个城市，9家企业开展实地测试

邀请行业专家、科研机构和参与厂商组成评审团队

可信区块链标准从国内走向国际舞台



由中国信息通信研究院和人民银行数字货币研究所，代表我国产业界联合在ITU-T分布式账本焦点组提交了“可信区块链：一个分布式账本技术评估框架”的技术提案，得到各方的热烈响应。

目前，中国信通院的魏凯主任当选该组副主席，卿苏德博士当选测试评估准则的牵头人。

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

谢谢！

可信区块链联盟（筹）已有140+家企业申请加入！
期待与您在联盟里的相遇！

共同研讨，携手共进！
卿苏德
邮箱：qingsude@126.com
我也不太懂，我们一起弄懂