区块链技术与应用

计算机科学与技术学院　李京

00章 课程介绍和要求

课程介绍和要求

- 课程名称：区块链技术与应用 CS4004
- 课程属性：专业方向
- 课程对象：本科三年级
- 上课时间：3~16周，周四（8、9、10）
- 上课地点：西区教三楼3A 206
- 学时：40+20 2.5学分
- 教师：李京　　lj@ustc.edu.cn
- 助教：张灏文

教学目标

掌握区块链系统的基本理论和相关技术，了解区块链前沿以及典型应用场景，掌握如何构建区块链系统和设计区块链应用，进而掌握解决问题和完成相关研究的方法，从而具备区块链领域创新和独立思考的意识。通过本课程的学习，学生应达到如下目标：

① 掌握区块链系统中涉及的P2P技术、密码学原理、分布式一致性算法和共识协议、智能合约等基础知识，了解区块链基础设施服务的构建方法；

② 熟悉去中心化应用Dapp的应用场景，如数据确权、身份认证、预测市场、去中心化金融等，准确分析社会各行业中存在的去中心化信任、公开透明、不可篡改、不可伪造以及跟踪溯源等问题，能够设计和开发相关区块链应用，实现互联网上的价值与信任。

课程主要内容

1. 了解区块链的前沿发展及其研究的主要内容，掌握区块链的主要知识体系、基本理论；
2. 熟悉区块链主流平台搭建的步骤，掌握区块链系统的运行原理，包括区块链上的数据查询和存储管理、智能合约等；
3. 掌握基于智能合约的区块链应用编程技术，熟悉其开发流程和设计方法 。

参考教材


Blockchain
Theory and Method
区块链
理论与方法
清华大学出版社


区块链
原理、架构与应用
Blockchain
Principle, Architecture and Application
清华大学出版社


区块链
原理、设计与应用
第2版

课程主要内容

一、概述和基础知识

- 概述
- 区块链数据层（区块结构和关键技术）
- 分布式一致性和共识算法

二、典型区块链系统和编程

- 比特币系统
- 以太坊系统
- 开源分布式账本平台：超级账本（Hyperledger Fabric）

三、区块链技术应用案例

四、区块链研究与发展

授课和考核方式

- 采取教师课堂教学和学生动手实践相结合
- 综合参考教材进行课堂教学，后续部分章节会邀请业界专家与我共同讲授
- 实践内容由每位学生独立完成
- 课程考核方式：
  - 到勤率：10分
  - 作业和实践：40分
  - 期末考试：50分

01章 区块链技术概述

目 录

信息学科在新时代的基石技术：ABCD

- **近十年，随着IT技术进一步发展，新的技术纷纷涌现，其中，人工智能、区块链、云计算、大数据等均已登场。科技界人士将其简称：ABCD**

人工智能（AI）、区块链技术（Blockchain）、云计算（Cloud Computing）、数据科学（Data Science）

人工智能：生产力的变革 → 大数据： 生产资料的变革 → 区块链： 生产关系的变革

在区块链技术的基础上，人类的市场有很大的提升空间，即构造信任，减少欺诈和交易成本；提高效率，从而形成高速、自动化和智能化的市场系统。以AlphaGo为代表的人工智能侧重于发展生产力，而以区块链为代表的人工智能侧重于改造生产关系，构造公正、高效、创新的人工市场。区块链通过构造一个市场机器来制造信用和实现交易的“大爆炸”。

1.1 区块链起源和定义

- 互联网上的贸易，借助可信赖的**第三方信用机构**来处理电子支付信息，受制于“基于信用的模式”。

- 区块链技术通过构建区块链网络，任何达成一致的**无信任双方直接交易**，不需要第三方中介的参与。

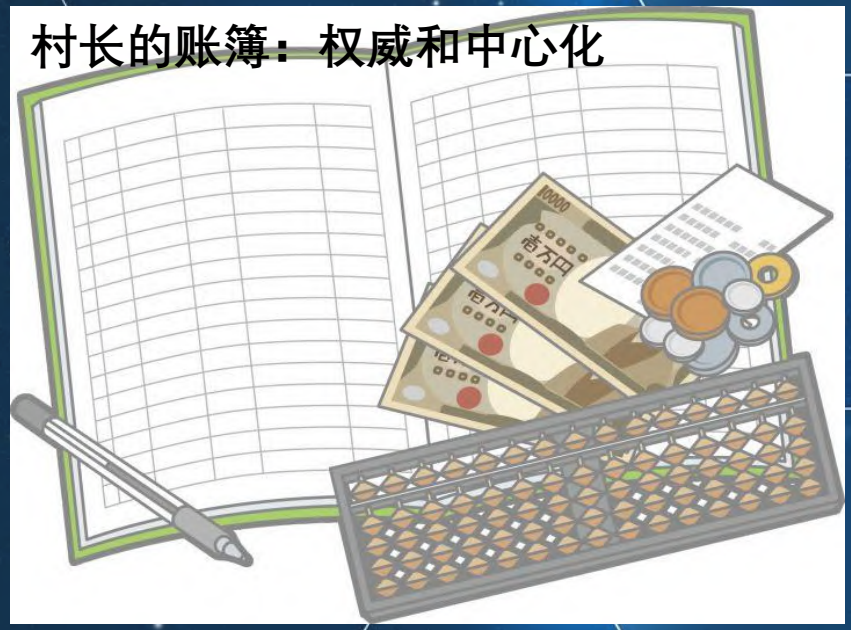
中心化账簿

村长记账：

1. 老王借给张三1000块钱，张三赖账不还
2. 老王找到村长，村长协调还钱

存在问题：

1. 村长年事已高，万一有个三长两短**不在了**，那大家的那本账簿怎么办？
2. 村长爱财如命，每次找他记账，他都要向大家收取**手续费**，而且一年比一年高。
3. 村长最近掉钱眼儿里了，为了谋取利益，将大家的钱**借给别人**。万一大家向他要钱，他拿不出来怎么办？
4. 村长掌握着大家的所有信息，万一他**把大家卖了**怎么办。
5. 村长**速度太慢了**，转个钱要好几天才行。
6. 村子里面最近有小偷出现，万一**偷走村长的那本账簿**怎么办。
7. 村长生病的时候，连个人都**找不到**哇。



去中心化账簿

全村人记账：

1. 村民们聚集在一起开了个会。决定给**每家每户都发一个账簿**，任何人之间转账交易，都通过村里的大喇叭**向全村的人通告**。
2. 收到通知以后，村民们就在**自己家**的账簿上记录下来**每一笔交易记录**。

记账优势：

1. 如果有一天村长的账簿丢了，那也没关系，村里老王、老李、老赵、老张...他们都有一个**备份**。
2. 如果小偷来村子里偷账簿怎么办呢？当然没关系，除非他可以一次偷走所有村民的账簿，否则这些记录就一直存在，丢的人可以去别人家再备份。
3. 而且无论换多少任村长，只要家家户户都有这本账簿，这里面的记录是绝对安全的，村长是无法篡改的，里面的钱该是谁的就是谁的。这本账簿到底属于谁呢？它并不属于某一个人，而是属于**整个村子**的。

全村人的账簿：去中心化

加密账簿+激励

安全和有序记账：

1. 村上请来了一个先生，他的工作就是把每位村民每一页的交易记录，转化成**加密过后**的密文，更加**方便**村民们的**记账；**
2. 村民们也会给这位先生一些小小的**报酬。**

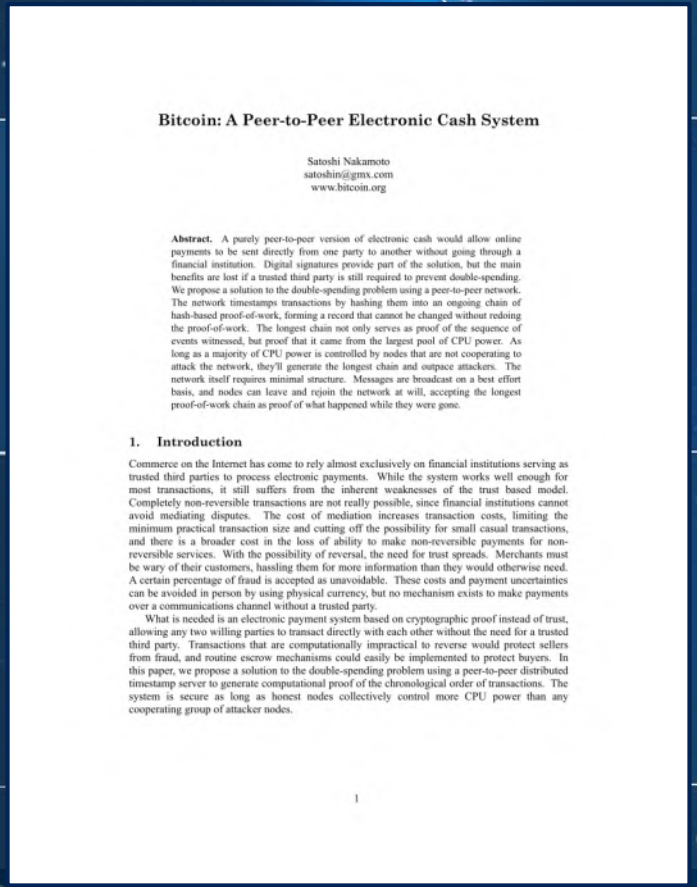
区块链：

1. 故事中的账簿上的每一页纸，其实就是**区块**，这本账簿的本身，就是**区块链**。
2. 村长一人掌握账簿是**中心化的运营**，所带来的问题，就是前文村民反映村长的问题。而村里每家每户都有账簿则是**去中心化的运营环境**。
3. 村里请来的先生，则是区块链中不可缺少的人物：**矿工**。
4. 村民们给他的报酬，就是他为区块链**提供算力**记录交易的酬劳：比如说比特币、以太币等。

什么是区块链

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链（Blockchain），是比特币的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。

《比特币：一种点对点的电子现金系统》



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

区块链定义

区块链技术是在不完全可信的环境中，通过构建点对点网络，利用链式数据结构来验证与存储数据，借助分布式共识机制来确定区块链结构，利用密码学的方式保证数据传输和访问的安全，利用由自动化脚本代码组成的智能合约来编程和操作数据。

简单来说，**区块链**是一种去中心化的分布式数据库。

1.2 区块链的体系结构

区块链3.0
区块链3.0是价值互联网的内核，基于区块链技术的应用扩展到任何有需求的领域，进而到整个社会。

区块链2.0
区块链1.0只能够支撑一些简单的指令集。2013年以太坊提出了智能合约，所谓智能合约实际上是一组决定区块链如何传递信息的可编程规则或程序指令，很多场景可以采用智能合约的形式来运转，无需第三方进行担保和信任。

区块链1.0
2008年比特币诞生，其核心是区块链技术，通过区块链的分布式记录存储，建立了真正意义上的数字货币。人们将以比特币为首的数字货币和支付行为组成的区块链技术阶段，称作区块链1.0。

袁勇、王飞跃2016年提出

数据层

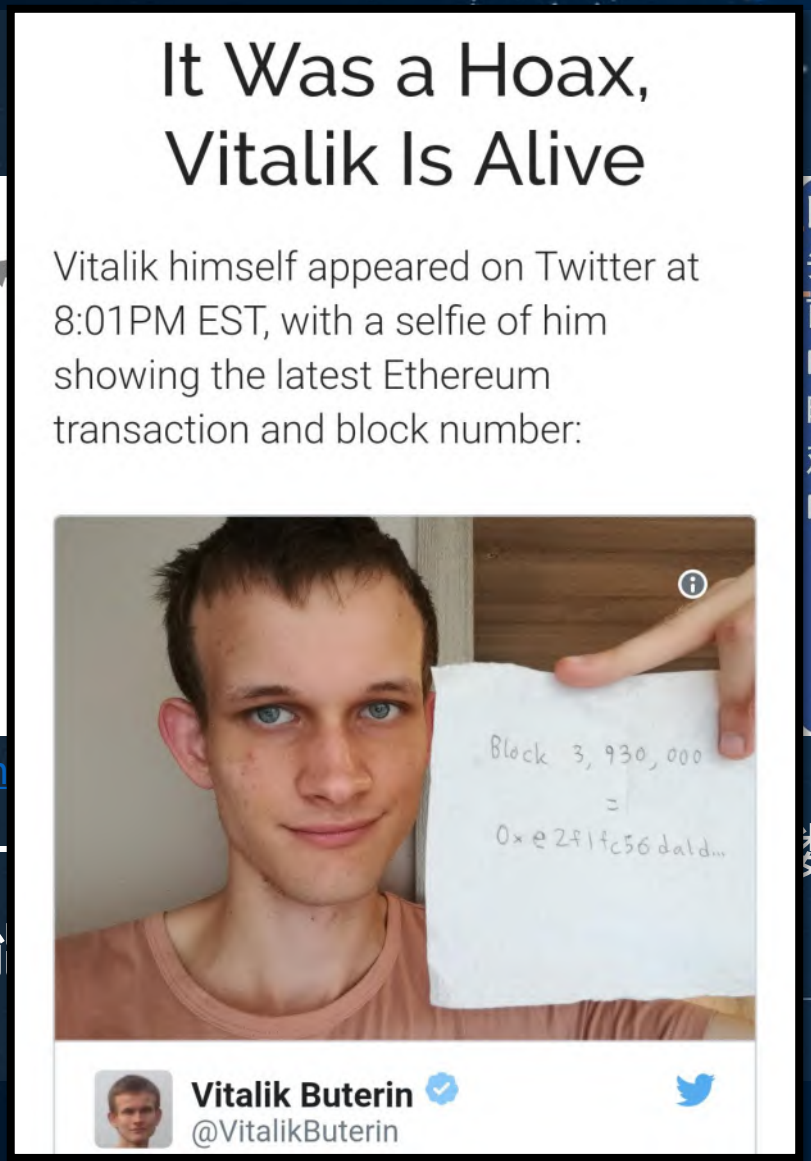
- 数据层封装了区块链的底层数据存储和加密技术。每个节点存储的本地区块链副本（数据账本）可以被看成三个级别的分层数据结构：区块链、区块、区块体（封装交易）。每个级别都需要不同的加密功能来保证数据的完整性和真实性。

数据层

链式数据结构

区块高度: 602243
头块哈希: ae1d7012
前块哈希: 05406e23
Merkle根: 109f6558
时间戳: 2019-11-04 7:53 AM
难度: 13,691,480,038,694.45
Nonce: 2,772,982,680
当前区块包含的交易数据

*数据来源：https://www.blockchain.com



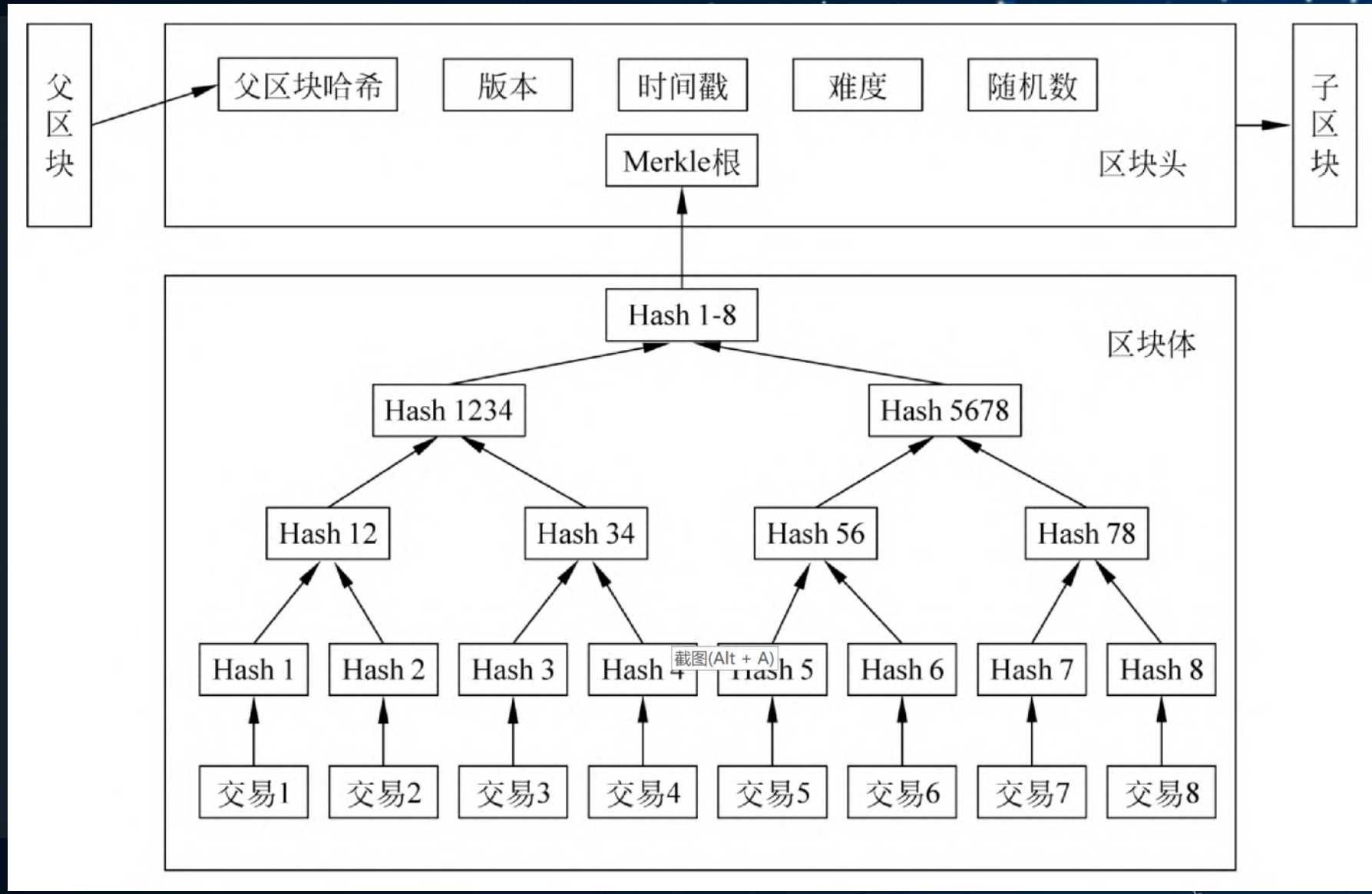
区块高度: 602245
头块哈希: 28f4662e
前块哈希: 10b4e49d
Merkle根: 86724ef0
时间戳: 2019-11-04 8:12 AM
难度: 13,691,480,038,694.45
Nonce: 1,882,559,396
当前区块包含的交易数据

- 区块链：每一个区块包含前一
- 不可变数据：只能添加、不能
- 不可变数据 + 时间刻度 →

数据结构

无法篡改

数据层（区块结构）

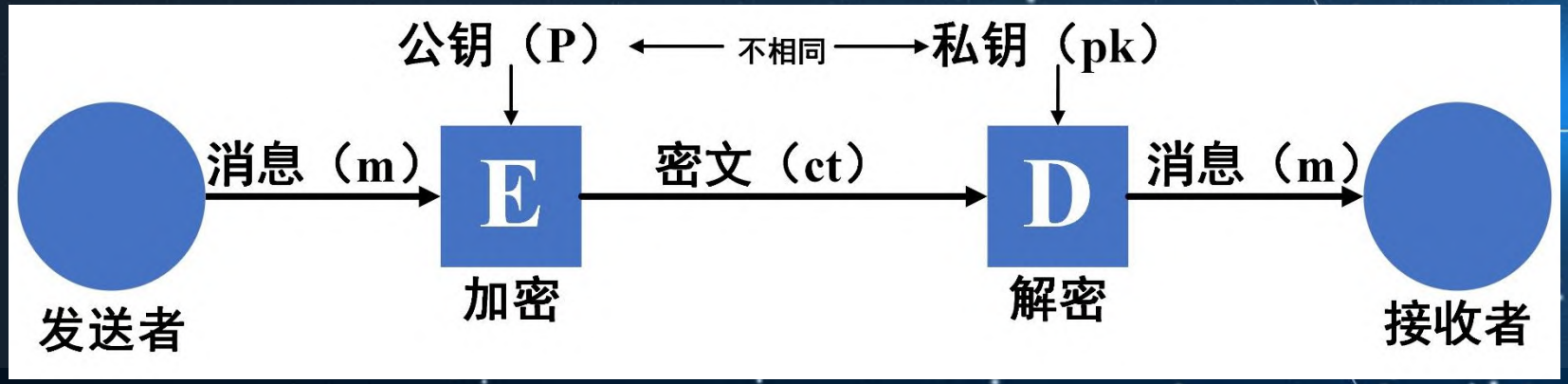

父区块
父区块哈希
版本
时间戳
难度
随机数
Merkle根
区块头
子区块
Hash 1-8
区块体
Hash 1234
Hash 5678
Hash 12
Hash 34
Hash 56
Hash 78
Hash 1
Hash 2
Hash 3
Hash 4
Hash 5
Hash 6
Hash 7
Hash 8
交易1
交易2
交易3
交易4
交易5
交易6
交易7
交易8

数据层

基于密码学体系

- PKI公私钥
- 数字指纹、数字签名
- 零知识证明
- ……

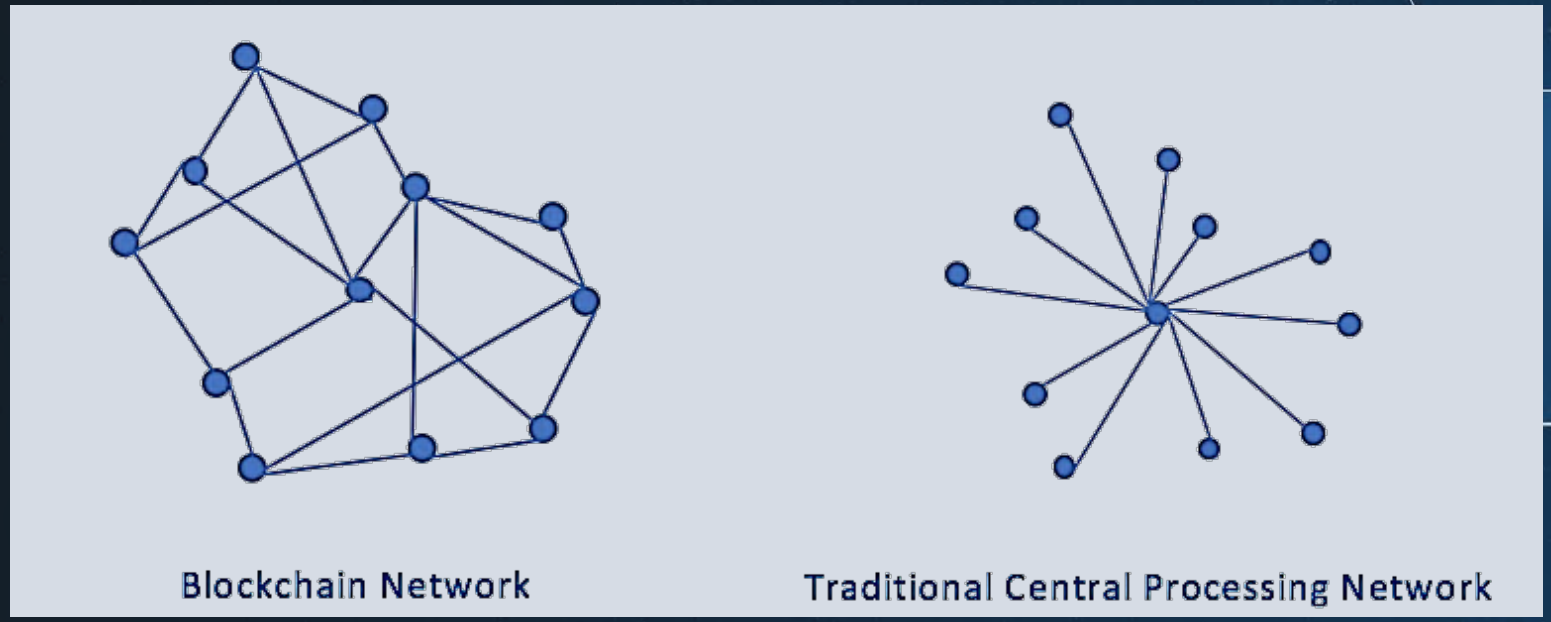
哈希（数字指纹）示意图



非对称加密示意图

网络层

- 网络层封装了区块链系统的组网方式、消息传播机制和验证机制。
- 组网方式通常采用点对点（P2P）方式

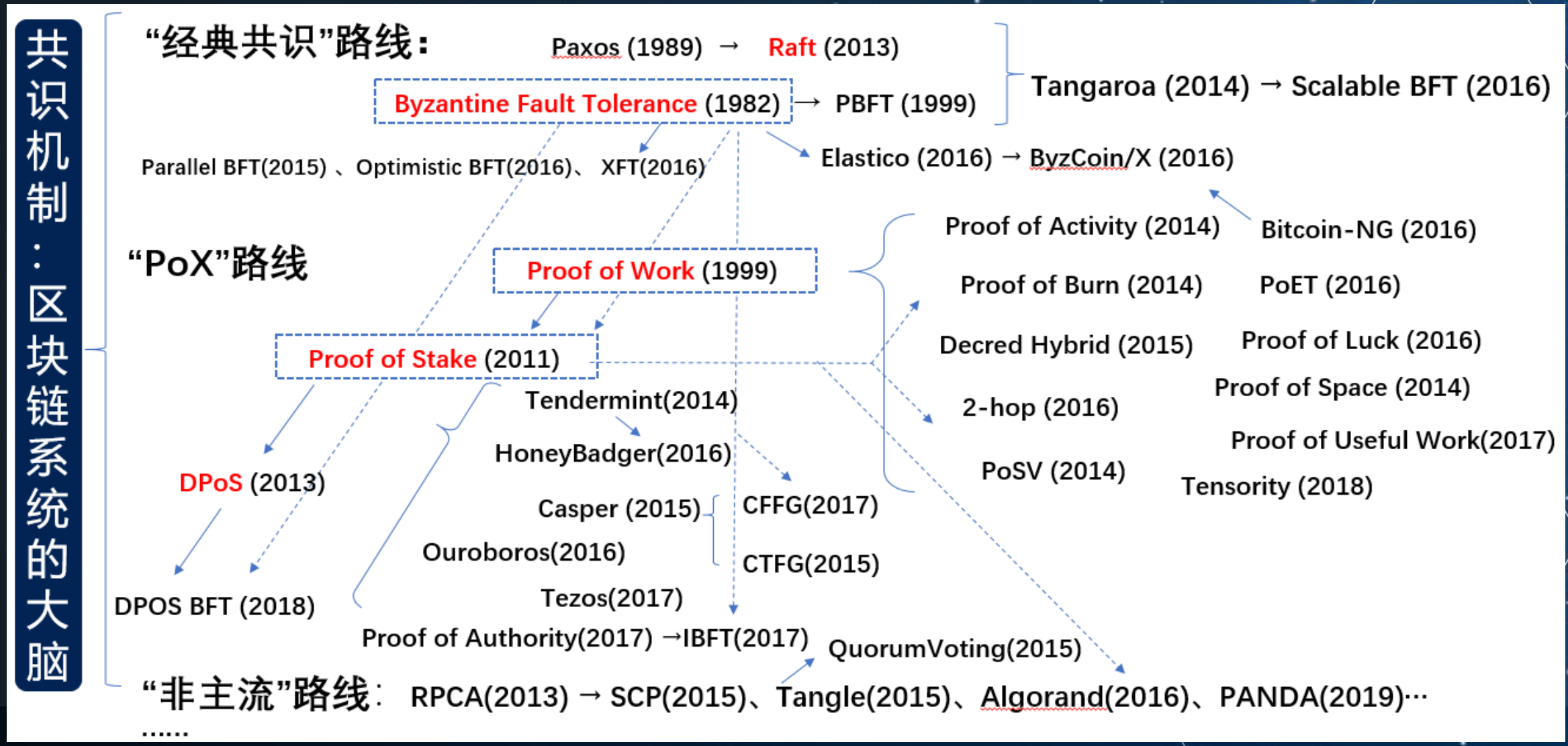


- 网格网络(Mesh) vs 轴辐网络（Hub-and-Spoke)
- 权限对等、数据公开 vs 中央服务器分配权限
- 数据分布式、高冗余存储 vs 多点备份、中心化管理

共识层

- 共识层主要封装区块链系统使用的各类共识算法。
- 如何在分布式系统中高效地达成共识是分布式计算领域的重要研究问题。正如社会系统中“民主”和“集中”的对立关系相似，决策权越分散的系统达成共识的效率越低、但系统稳定性和满意度越高；而决策权越集中的系统更易达成共识，但同时更易出现专制和独裁。区块链技术的核心优势之一就是能够在决策权高度分散的去中心化系统中使得各节点高效地针对区块数据的有效性达成共识。常见共识算法有：工作量证明共识（PoW）、权益证明共识（PoS）、拜占庭共识机制（BFT）、授权股份证明共识机制（DPoS）。早期的比特币区块链采用高度依赖节点算力的工作量证明 (Proof of work, PoW) 机制来保证比特币网络分布式记账的一致性。
- 共识协议因不同的区块链网络而存在差异。

共识算法的发展路线图


共识机制：区块链系统的大脑
“经典共识”路线：
Paxos (1989) → Raft (2013)
Byzantine Fault Tolerance (1982) → PBFT (1999)
Tangaroa (2014) → Scalable BFT (2016)
Parallel BFT(2015) 、Optimistic BFT(2016)、 XFT(2016)
Elastico (2016) → ByzCoin/X (2016)
“PoX”路线
Proof of Work (1999)
Proof of Activity (2014)
Bitcoin-NG (2016)
Proof of Burn (2014)
PoET (2016)
Decred Hybrid (2015)
Proof of Luck (2016)
Proof of Space (2014)
2-hop (2016)
Proof of Useful Work(2017)
PoSV (2014)
Tensority (2018)
Proof of Stake (2011)
Tendermint(2014)
HoneyBadger(2016)
DPoS (2013)
Casper (2015)
CFFG(2017)
Ouroboros(2016)
CTFG(2015)
Tezos(2017)
DPOS BFT (2018)
Proof of Authority(2017) →IBFT(2017)
QuorumVoting(2015)
“非主流”路线：
RPCA(2013) → SCP(2015)、Tangle(2015)、Algorand(2016)、PANDA(2019)…
……

激励层

- 激励层是将经济因素集成到区块链技术体系中来，包括经济激励的发行机制和分配机制等，主要在公有链当中出现。在公有链中必须激励遵守规则参与记账的节点，并且惩罚不遵守规则的节点，使得节点最大化自身收益的个体理性行为与保障去中心化的区块链系统的安全和有效性的整体目标相吻合，才能让整个系统朝着良性循环的方向发展。
- 对私有链系统，则不一定需要进行激励，因为参与记账的节点往往是在链外完成了博弈，通过强制力或自愿来要求参与记账。

激励层

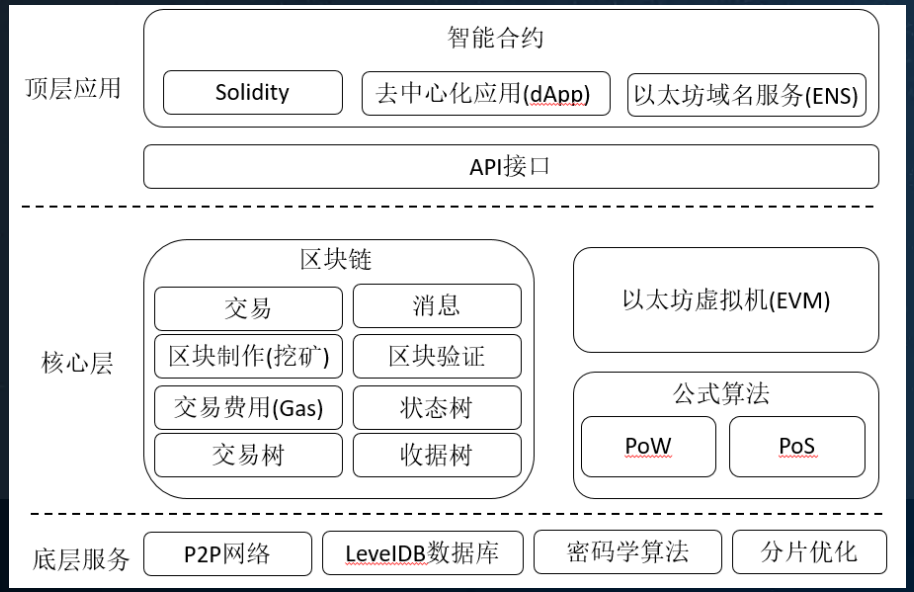
以比特币为例：

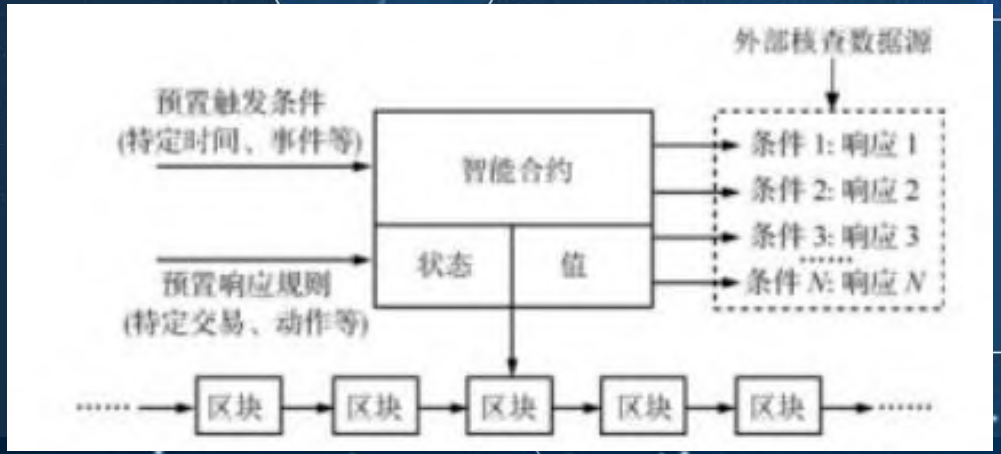
比特币起初由系统奖励给那些创建新区块的矿工，该奖励大约每四年减半。刚开始每记录一个新区块，奖励矿工50个比特币，该奖励大约每四年减半。依次类推，到公元2140年左右，新创建区块就没有系统所给予的奖励了。届时比特币全量约为2100万个，这就是比特币的总量，所以不会无限增加下去。

另外一个激励的来源则是交易费。新创建区块没有系统的奖励时，矿工的收益会由系统奖励变为收取交易手续费。例如，你在转账时可以指定其中1%作为手续费支付给记录区块的矿工。如果某笔交易的输出值小于输入值，那么差额就是交易费，该交易费将被增加到该区块的激励中。只要既定数量的电子货币已经进入流通，那么激励机制就可以逐渐转换为完全依靠交易费，那么就不必再发行新的货币。

合约层

- 合约层封装区块链系统的各类脚本代码、算法以及由此生成的更为复杂的智能合约。如果说数据、网络和共识三个层次作为区块链底层“虚拟机”分别承担数据表示、数据传播和数据验证功能的话，合约层则是建立在区块链虚拟机之上的商业逻辑和算法，是实现区块链系统灵活编程和操作数据的基础。





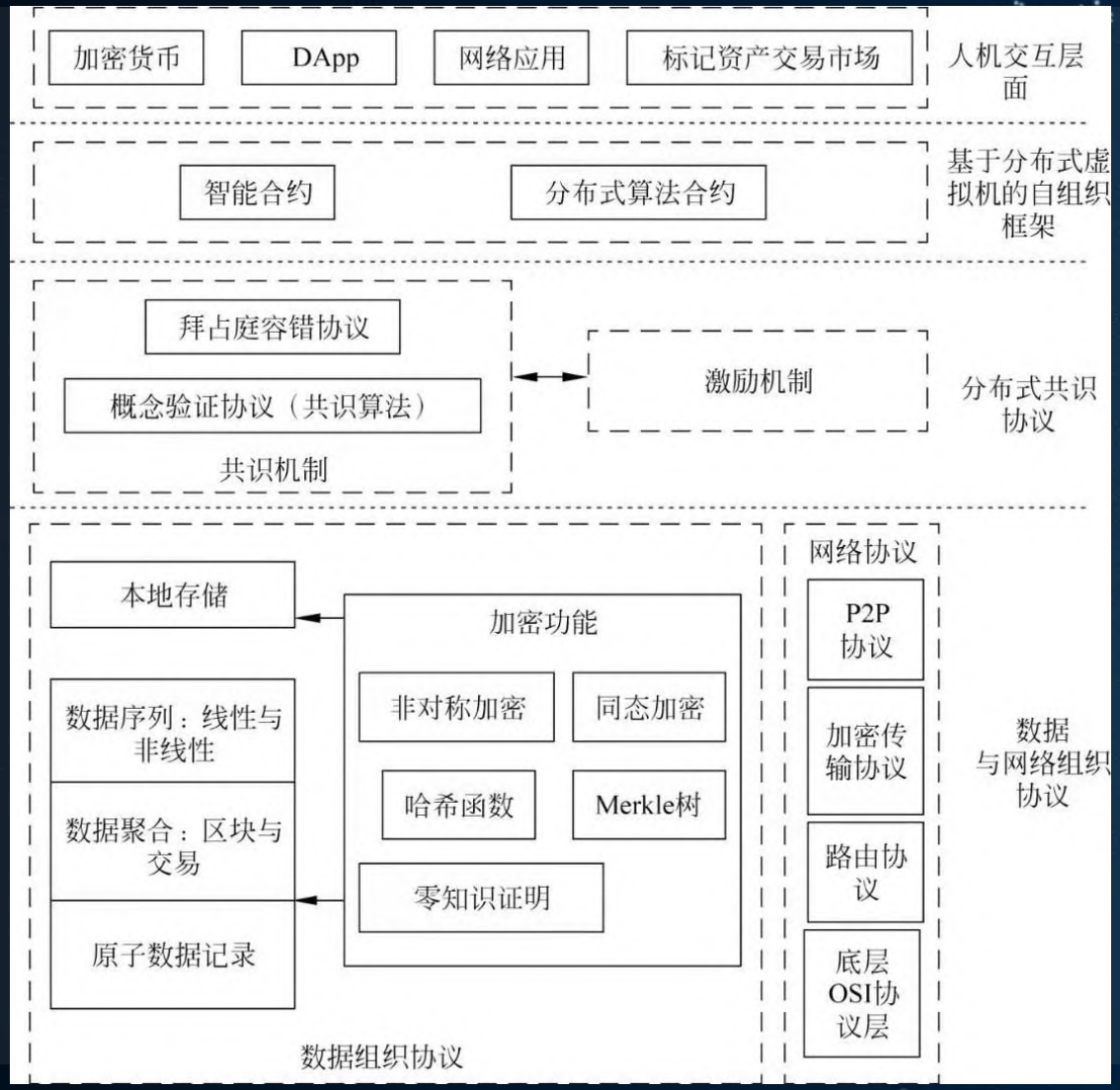
合约层

例如，可以编写智能合约以规定运输物品的成本，其中运费根据物品到达的速度而变化。根据双方同意并写入账本的条款，当收到物品时，相应的资金会自动转手。

应用层

- 区块链技术是具有普适性的底层技术框架，除可以应用于数字加密货币外，在经济、金融和社会系统中也存在广泛的应用场景。
- 区块链3.0支撑“可编程社会”。

四层体系结构模型


加密货币
DApp
网络应用
标记资产交易市场
人机交互层面
智能合约
分布式算法合约
基于分布式虚拟机的自组织框架
拜占庭容错协议
概念验证协议（共识算法）
共识机制
激励机制
分布式共识协议
本地存储
加密功能
非对称加密
同态加密
哈希函数
Merkle树
零知识证明
数据序列：线性与非线性
数据聚合：区块与交易
原子数据记录
数据组织协议
网络协议
P2P协议
加密传输协议
路由协议
底层OSI协议层
数据与网络组织协议

1.3 区块链特征

- **去中心，去信任**
  - 区块链由众多节点共同组成一个端到端的网络，不存在中心化的设备和管理机构。节点之间数据交换通过数字签名技术进行验证，无需互相信任，只要按照系统既定的规则进行，节点之间不能也无法欺骗其它节点。
- **开放，共识**
  - 任何人都可以参与到区块链网络，每一台设备都能作为一个节点，每个节点都允许获得一份完整的数据库拷贝。节点间基于一套共识机制，通过竞争计算共同维护整个区块链。任一节点失效，其余节点仍能正常工作。

1.4 区块链特征

- **交易透明，双方匿名**
  - 区块链的运行规则是公开透明的，所有的数据信息也是公开的，因此每一笔交易都对所有节点可见。由于节点与节点之间是去信任的，因此节点之间无需公开身份，每个参与的节点都是匿名的。
- **不可篡改，可追溯**
  - 单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非能控制整个网络中超过51%的节点同时修改，这几乎不可能发生。区块链中的每一笔交易都通过密码学方法与相邻两个区块串联，因此可以追溯到任何一笔交易的前世今生。

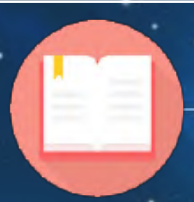
1.4 区块链分类

公有链

无官方组织及管理机构，无中心服务器，参与的节点按照系统规则自由接入网络、不受控制，节点间基于共识机制开展工作。

联盟链

由若干机构联合发起，介于公有链和私有链之间，兼具部分去中心化的特性。



私有链

建立在某个组织内部，系统的运作规则根据组织要求设定，修改甚至是读取权限仅限于少数节点，同时仍保留着区块链的真实性和部分去中心化特征。

按去中心化程度

- 无许可区块链（Permissionless Blockchain）：一种完全去中心化的分布式账本技术，允许节点自由加入和退出，无需通过中心节点注册、认证和授权，节点地位平等，共享整个账本。
- 许可区块链（Permissioned Blockchain）：存在一个或多个具有较高权限的节点，可以是可信第三方，也可以是协商制定有关规则，其他节点只有经过相应授权后才可访问数据，参与维护。

1.4 区块链分类

	公有链	联盟链	私有链
参与者	任何人，无需许可	联盟成员，许可加入	个体或公司内部，许可加入
共识机制	POW/POS/DPOS...	分布式一致性算法	分布式一致性算法
记账人	所有参与者	联盟成员协商确定	内部自定义
激励机制	有	通常无	无
中心化程度	去中心化	多中心	中心化
主要特点	安全性高	效率和成本优化	可控性最强，不对外公开
承载能力	通常为几笔-几十笔/秒	1000-1万笔/秒	1000-10万笔/秒
典型场景	数字货币、智能合约平台	金融、政务、司法等行业	审计、日志等内部场景

不同区块链系统性能比较

分类	交易系统	吞吐量(tps)	交易延迟	共识机制
公有链	BTC(比特币)	3~7	10min	PoW
	BCH(比特币现金)	24~224	10min	PoW
	LTC(莱特币)	7~28	2.5min	PoW
	EOS	3600	0.5s	DPoS
	ETH(以太坊)	30~40	15s	PoW+PoS
联盟链	Fabric	3560	0.5s	Kafka
	Quorum	1650	1s	Raft
传统交易处理系统	Visa	5.6万	<1s	
	支付宝	49.1万	<1s	

1.5 数字货币简史

区块链1.0旨在解决交易速度、挖矿公平性、能源消耗、共识方式以及交易匿名等问题，参照物为比特币（BTC）。

比特币——数字货币的诞生

中心化系统：

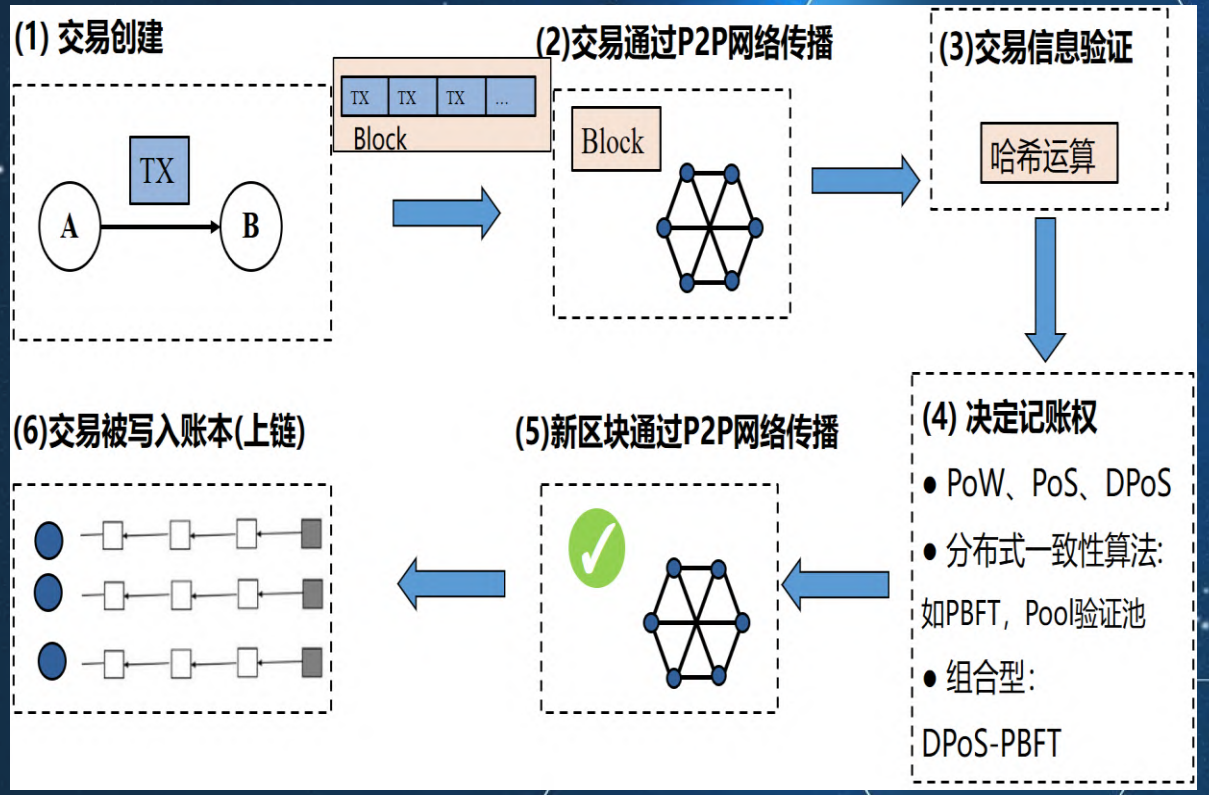
由政府、大企业和公司控制，容易受到黑客攻击、信息不够透明、信息容易出现堵塞。

比特币系统：

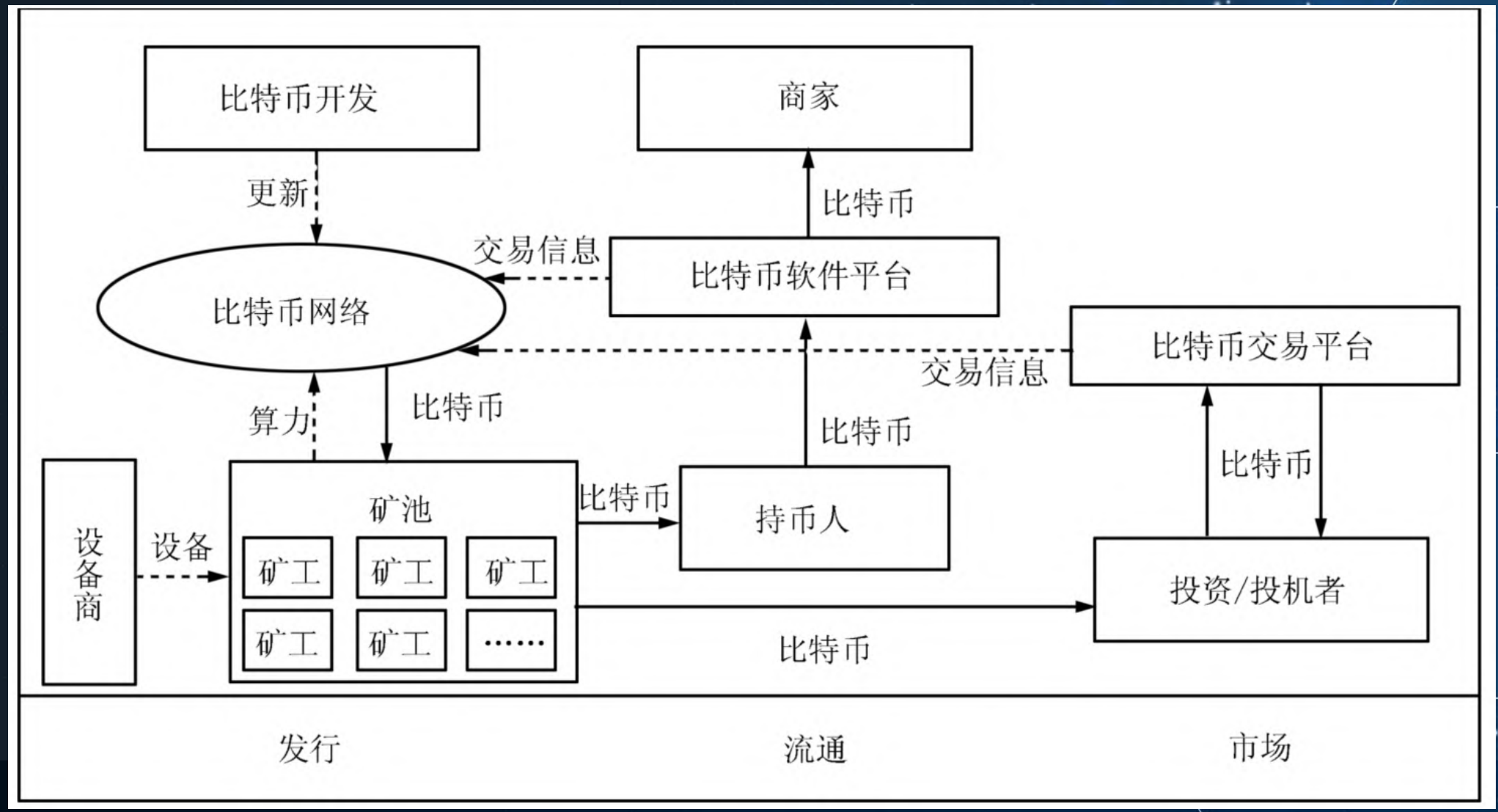
每个用户都有一个地址存储自己的比特币，这个地址叫做钱包。用户每次交易就是比特币由一个地址转移到另一个地址上，几乎不可篡改。

比特币——运行机制

1. 产生新交易。
2. 通过P2P网络被广播到所有的参与节点。
3. 各节点都会将新交易进行验证，并各自形成一个等待上链的区块。
4. 通过共识算法选出拥有记账权的节点。
5. 获得记账权的矿工通过P2P网络广播它的新区块，全网其它节点核对该区块记账的正确性。
6. 超过一定数量的节点验证新区块无误后，就可以将这个区块连接到上一个区块上组成区块链。



比特币——生态圈


比特币开发
商家
更新
比特币
交易信息
比特币软件平台
比特币网络
比特币交易平台
交易信息
算力
比特币
比特币
比特币
矿池
比特币
设备商
设备
持币人
矿工
矿工
矿工
矿工
矿工
……
投资/投机者
比特币
发行
流通
市场

冰火比特币

2008年11月，中本聪发布论文《比特币：一种点对点的电子现金系统》提出比特币概念

2008

2009

1月3日第一块区块产生，称为“创世区块”中本聪挖矿获得50个比特币
1月12日中本聪送密码学家哈尔.芬妮10比特币，产生第一笔交易

2010

5月21日，弗罗里达一个程序员用1W比特币买了25美元比萨优惠券

2012

Ripple币用于向各国转移外汇

2013

“芦山地震”收到233个比特币

2016

2018

中国人民银行数字货币研究院成立
将区块链纳入《“十三五”国家信息化规划》

2019

币圈跌宕起伏
而区块链技术风向已定

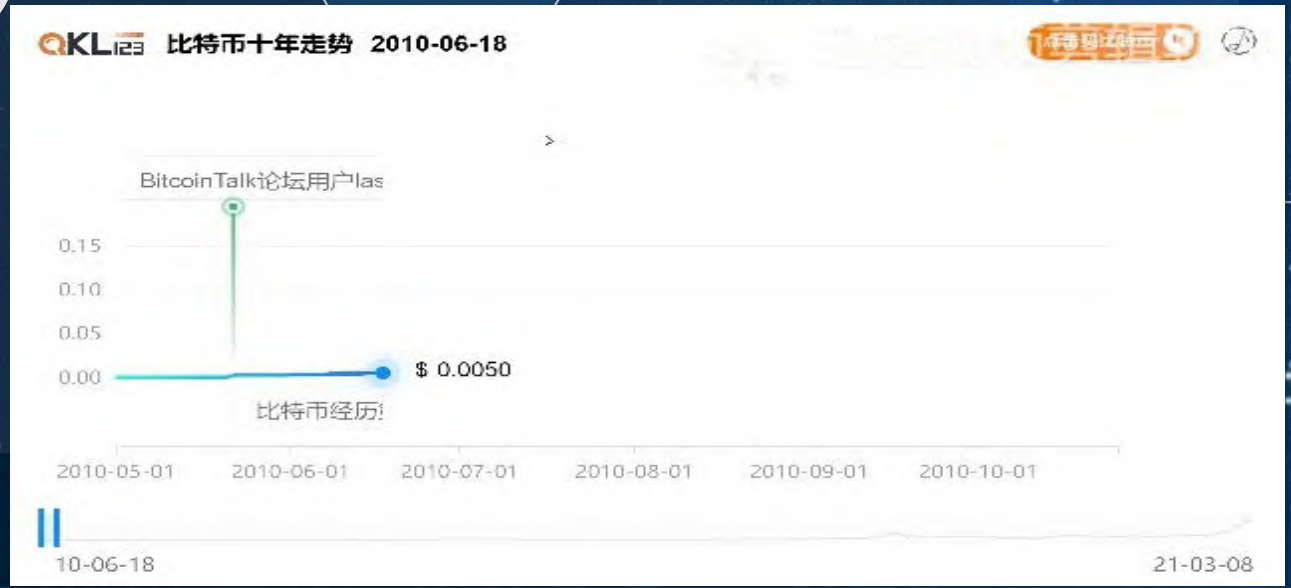
2020

中共中央政治局10月24日下午就区块链技术发展现状和趋势进行第十八次集体学习

国内开始大规模探讨基于联盟链构建的区块链应用；去中心化金融场景落地

2021

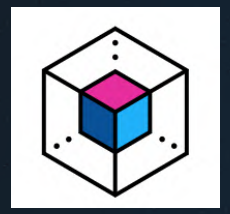
国外传统资本投资区块链，包括twitter、微策略、特斯拉等

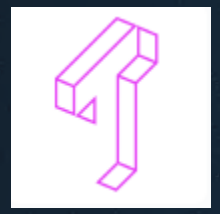


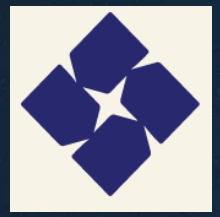
区块链2.0

区块链2.0旨在解决数据隐私、数据存储、区块链治理、高吞吐量、域名解析、合约形式化验证等问题，参照物为以太坊（ETH）。

数据隐私


Engima


Taxa


Starkware


ARPA


Nucypher

链上治理


Tezos

数据存储

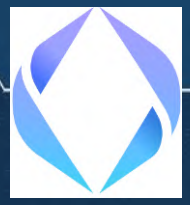

Arweave

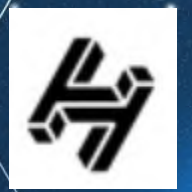

IPFS


Storj


Sia

域名解析


ENS


Handshake

高吞吐量


NEAR


AVA


Elrond


ETH2.0

合约形式化验证


ADA


CertiK


Tezos

以太币

2013年末，Vitalik受比特币启发后开发了以太坊，以太坊和比特币有着相似的运行交易机制，以太坊最大的优势是加入了**部署智能合约功能**，每个人可以根据需求发布自己的智能合约。

以太坊网络中的每笔交易都需要支付一定的手续费。无论是转账交易还是部署智能合约，所支付的手续费越高，该交易就越快地被打包进区块中，这也是以太币最主要的价值。

智能合约

一种旨在以信息化方式传播、验证或执行合同的计算机协议，它允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

数字钱包

数字钱包是一个形象的概念，因为拥有私钥就拥有对应地址的数字货币，因此人们把**管理密钥的软件**称为“钱包”

全节点钱包

全节点钱包在使用时需要下载所有节点的信息。

轻钱包

轻钱包在使用时不需要下载节点信息，但这种方式相比于全节点钱包，交易速度会降低。

数字钱包

Blockchain钱包

Blockchain钱包是比特币专用的钱包，它是一个轻钱包，通过网页打开就可以随时使用，也可以下载手机客户端，不用在本地同步节点信息。但是目前只支持比特币、以太币和比特币现金的业务。

Mist钱包

Mist钱包是专为以太坊用户和开发人员设计的钱包，它可以存储用户的以太币。通过Mist可以部署智能合约。

imToken钱包

imToken是手机钱包，同时也是轻钱包，imToken支持多种数字货币，包括BTC、ETH、EOS等，是目前最流行的手机钱包之一。

火币Pro钱包

火币Pro准确的说应该是一个交易所，用户在交易所上购买后直接可以存在交易所的钱包里。

数字货币市场现状

比特币的稀缺性、去中心化和全球性流通的特性，吸引了越来越多的人关注数字货币市场。

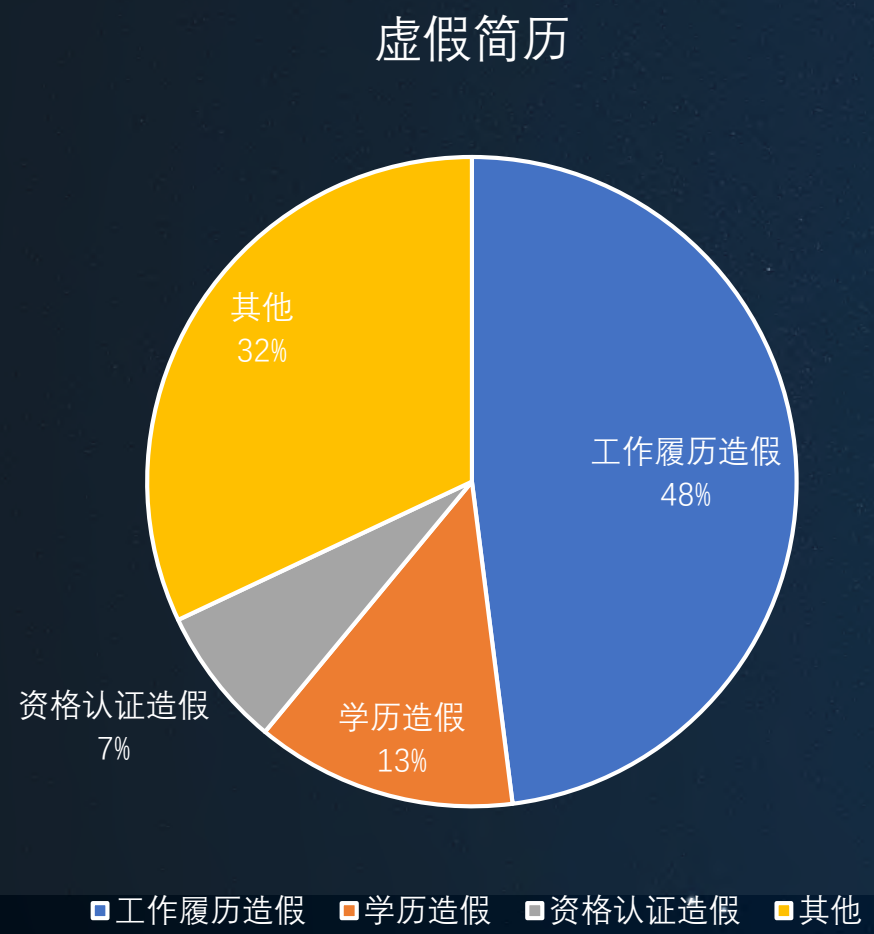
现在全球市场上的数字货币大约有3000多种，根据央视前两天的报道，此前国内比较流通的数字货币大约在1600种左右，目前市值排名比较靠前的数字货币有比特币、以太坊、瑞波币、柚子、莱特币。

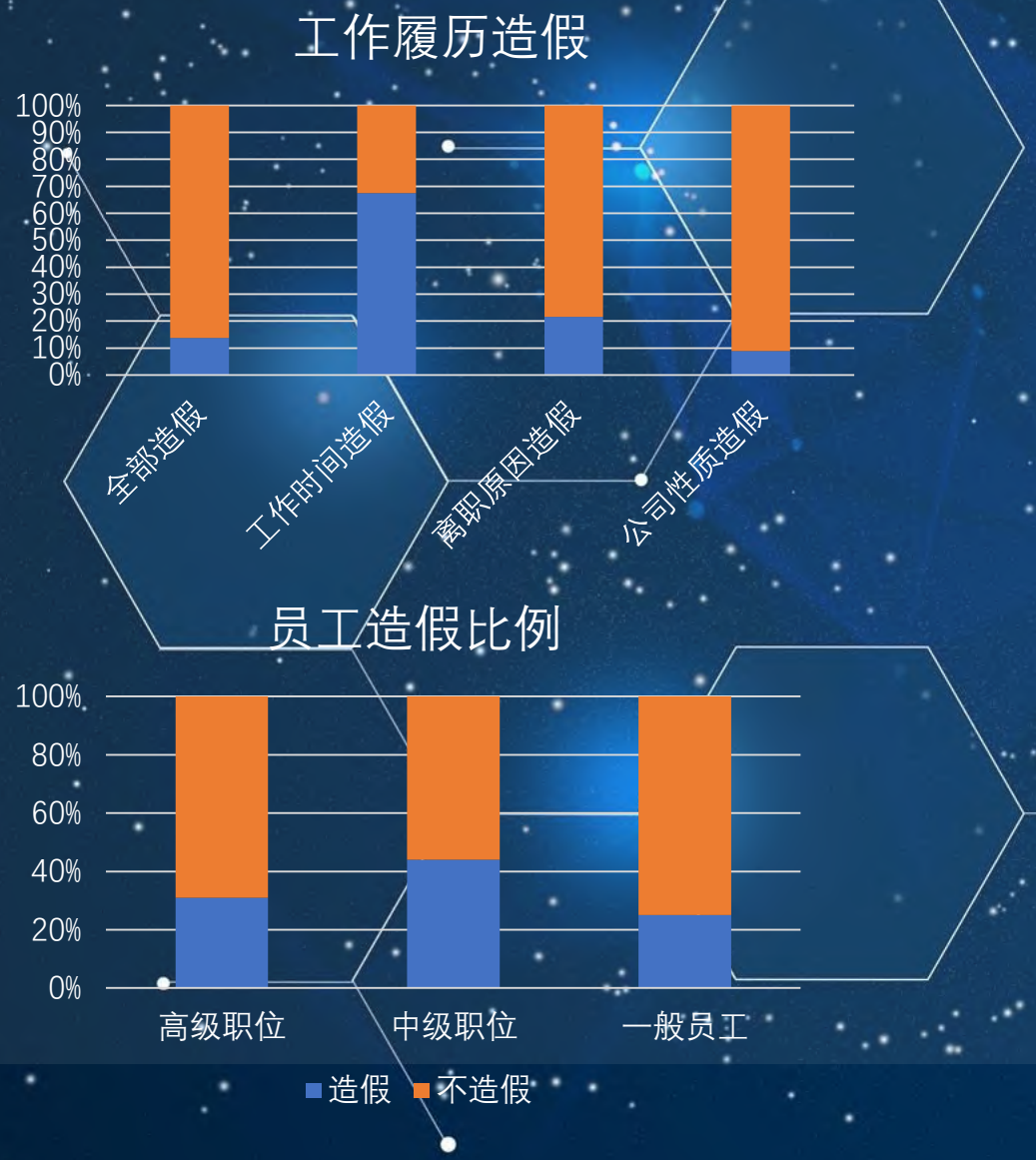
随着各种数字货币的发行、完善和推广，数字货币将成为更多人所接受的数字资产。未来，私人数字货币或将与法定数字货币共存，成为人类货币形态发展的新阶段，也将重构货币制度体系和金融机构体系。

1.6 区块链典型应用场景

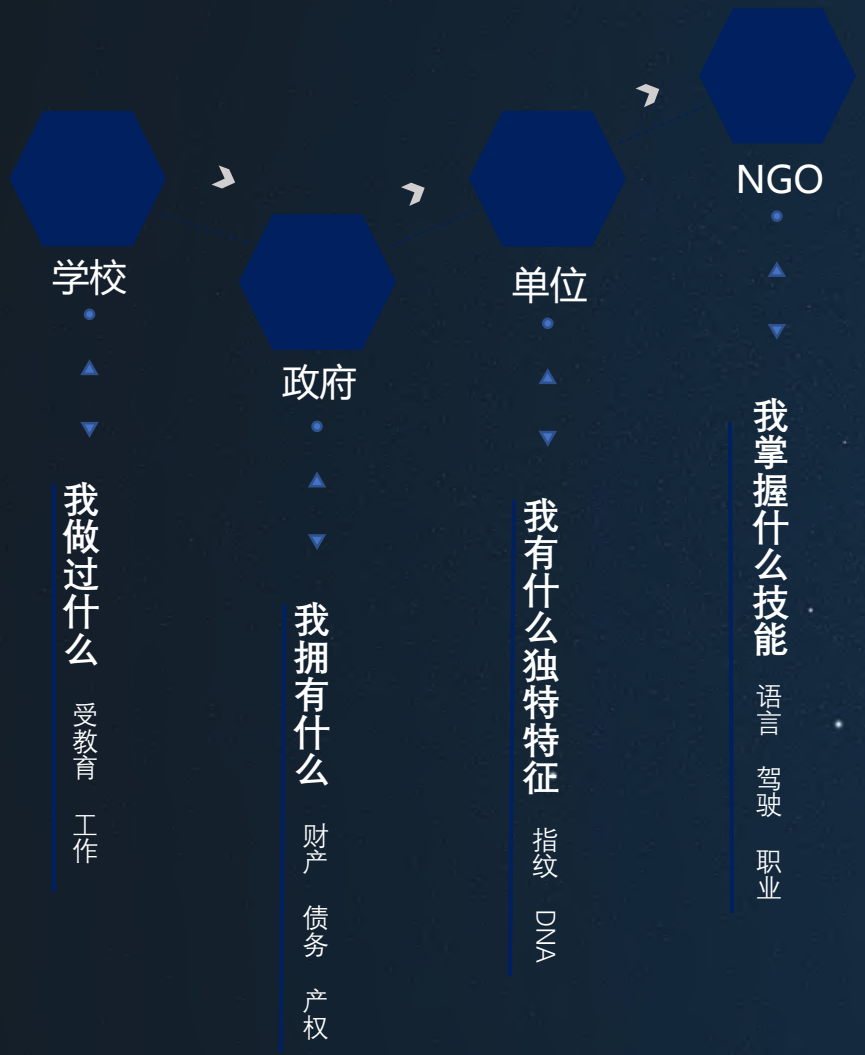
适用场景：多源身份认证

招聘场景中的简历造假现象





适用场景：多源身份认证



多源身份认证

多源认证

多个不同的认证方从不同的角度、不同的方面对同一个人进行多源认证

完整画像

可从与主体有关联的各个组织机构及个人收集各种证明数据来描绘主体的各个维度

可信追踪

认证均经过认证方的签名，具有不可伪造、不可抵赖的特性。

适用场景：分布式声誉体系

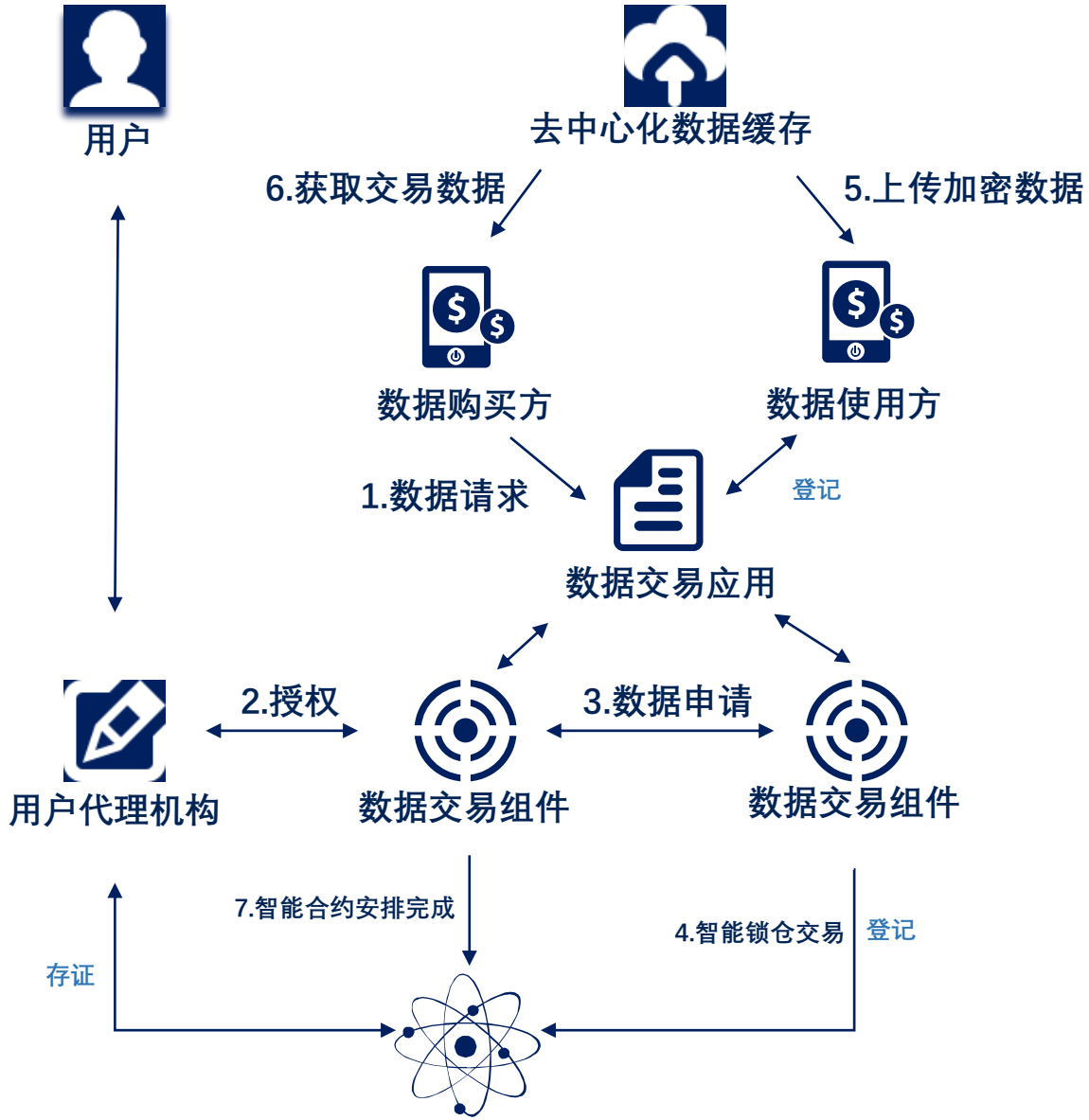
分布式声誉体系

1.机构对个体进行本地信任的计算。

2.区块链对个体进行综合信任（全局信任）的计算。

3.建立分布式信用数据管理体系。

适用场景：数据协同与交换



数据协同与交换

数据发现

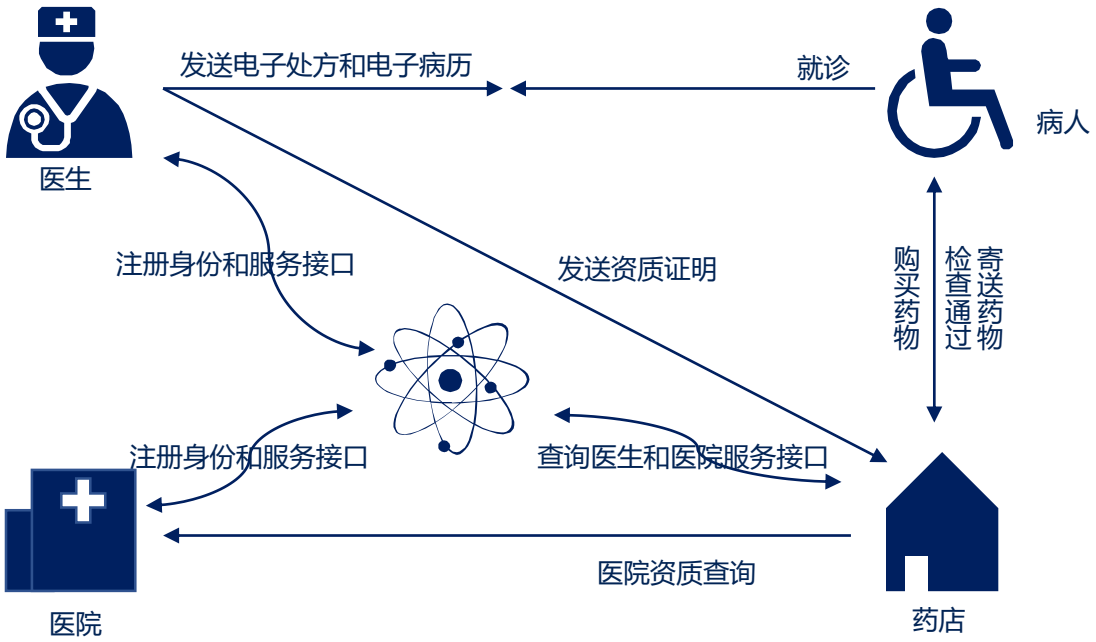
需要使用数据的应用可从用户出发，根据用户身份ID同样授权访问用户的数据

数据交易模型

数据使用方发出获取数据的请求。请求发送到用户的客户端，由用户进行授权。

适用场景：分布式流程协作

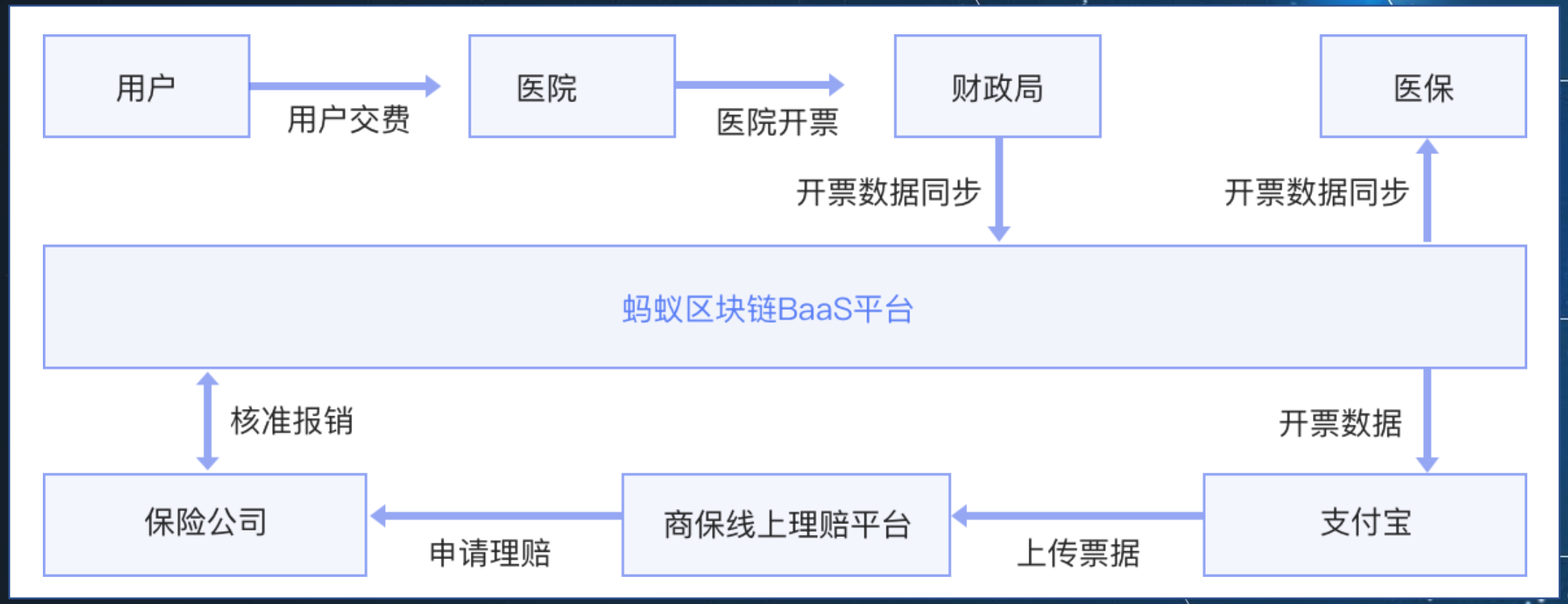
示例：处方药的认证购买



人的多源可信认证	形成对医生身份、购/用药主体身份的可信认定，降低购药环节的相关风险
购药各方责任的明晰	各参与者的职责和权限由多方记录及确认
购药流程的记录	购药的每一个流程的推进均在链上记录
购药结果的可信	医院对其开具的处方及后续购药者的购药行为进行认证与背书
声誉体系的形成	基于区块链设计声誉体系管理。形成对药店、医院声誉管理的综合评价。

区块链 + 金融科技

阿里-区块链电子发票解决方案



区块链 + 智慧旅游

智慧旅游

行业痛点

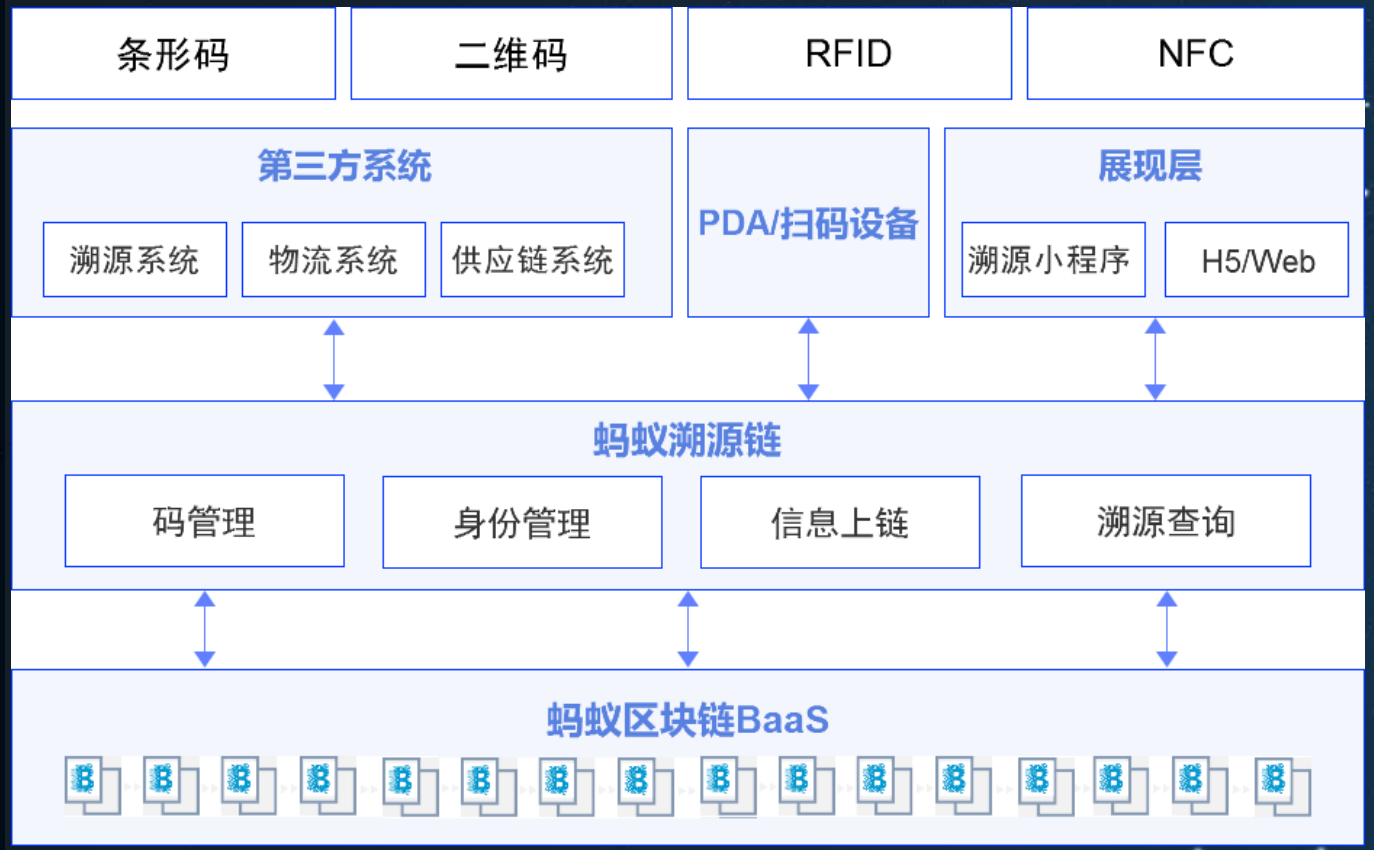
- 收取中介费用
- 推广徒有其名的项目
- 刷单
- 删差评
- 用户隐私泄露

区块链解决方案

利用区块链技术将客户、旅游供应商、第三方服务商连接在一起。使用区块链技术框架搭建了一个去中心化模式的文旅生态服务系统，利用区块链各节点权利与义务的对等性，从根本上解决当前在线旅游行业中的信用、隐私、成本等行业症结。

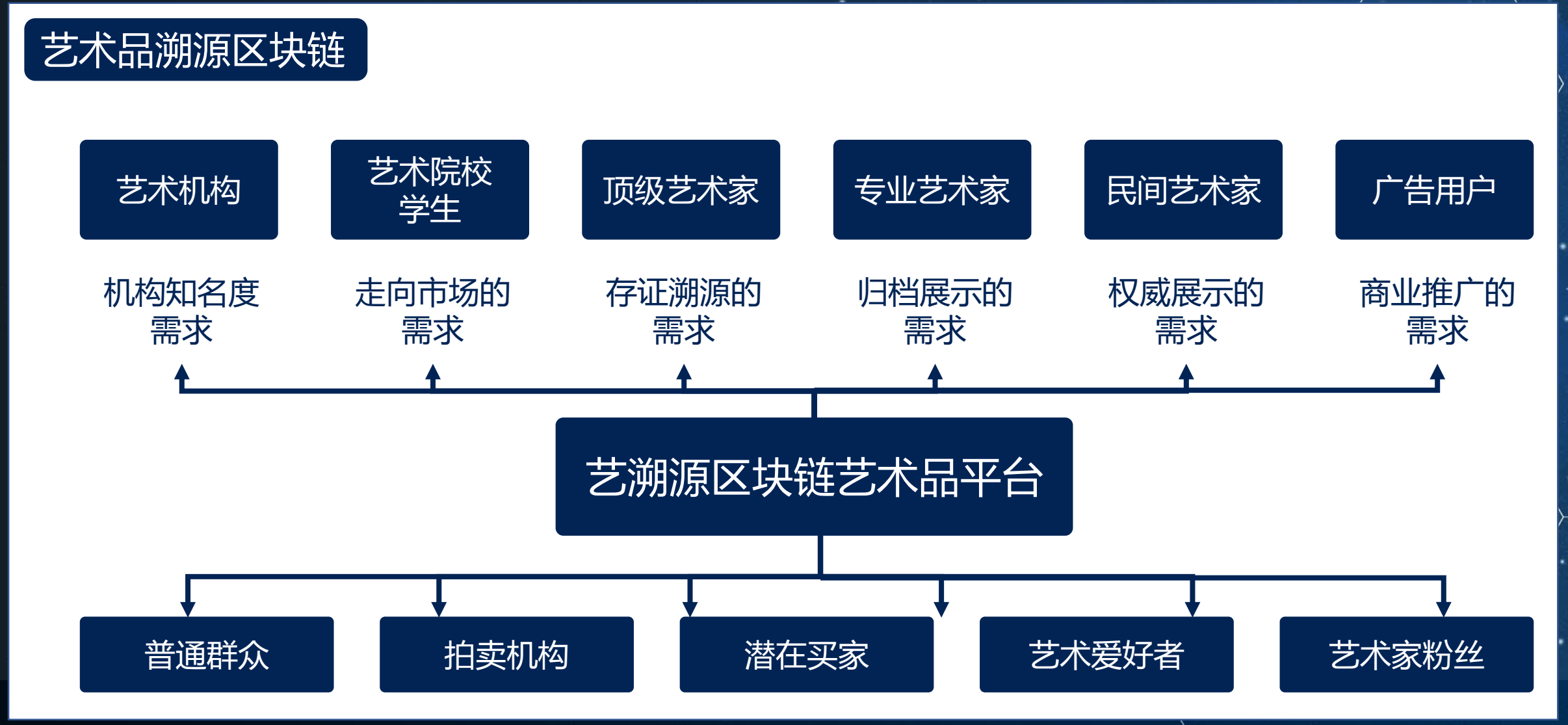
区块链 + 品质溯源

阿里-蚂蚁区块链品质溯源



从2018年 9 月 30 号开始，五常大米天猫旗舰店销售的每袋大米都有一张专属“身份证”。消费者打开支付宝扫一扫，就可以看到这袋米具体的种植地，种子、肥料、物流一目了然。源头的质量检测由五常市质检部门负责，“一检一码”。相关的物流信息、种植信息后续将写入蚂蚁金服的区块链中，以保证信息不可篡改。

区块链 + 品质溯源


艺术品溯源区块链
艺术机构
艺术院校学生
顶级艺术家
专业艺术家
民间艺术家
广告用户
机构知名度需求
走向市场的需求
存证溯源的需求
归档展示的需求
权威展示的需求
商业推广的需求
艺溯源区块链艺术品平台
普通群众
拍卖机构
潜在买家
艺术爱好者
艺术家粉丝

区块链+教育应用场景

示例：MIT 数字证书项目

信息上链 — 学生信息的提交（学位证、毕业证、成绩单……）

信息认证 — 个人确认/官方认证（→ 个人身份 + 官方身份）

线上验证 — 查询信息 / 验证信息

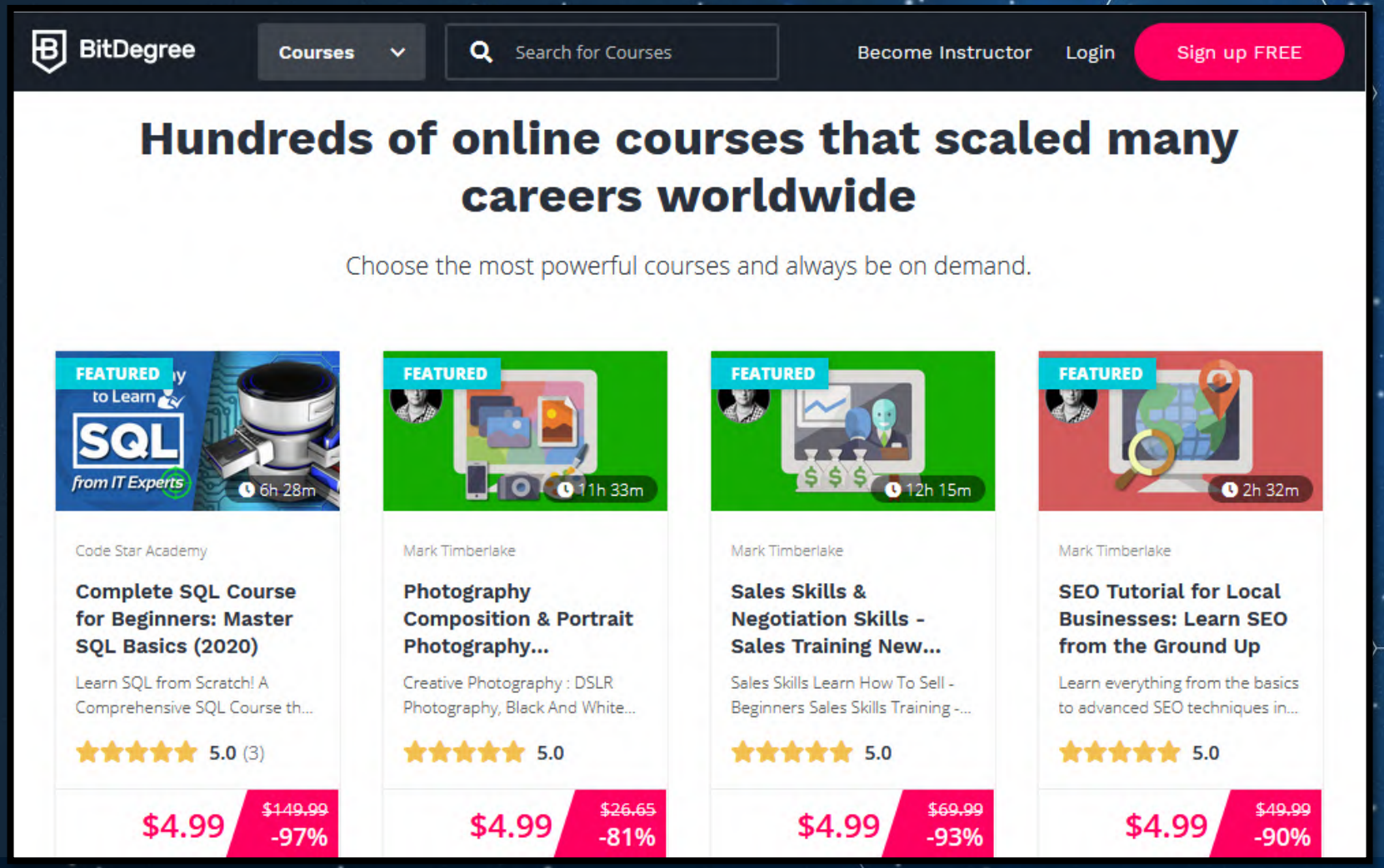
https://news.mit.edu/

区块链+教育应用场景

示例： BitDegree

基于区块链的在线教育平台，提供奖学金和技术人才招聘。

2018年6月，这家初创公司的学生人数从3月的900人增加到54,000人。



区块链 + 教育应用场景

示例：区块链数字档案平台

区块链 + 教育应用场景

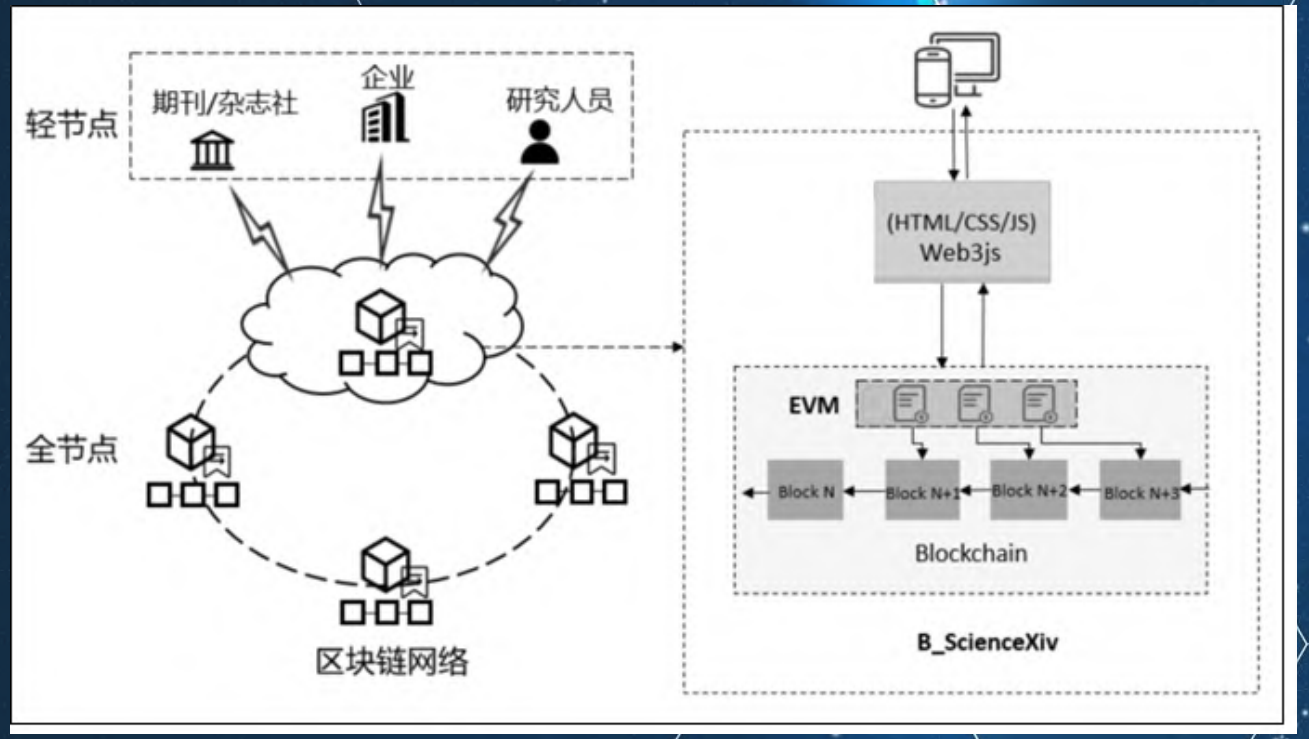
示例：区块链科研成果预发布平台

成果存证

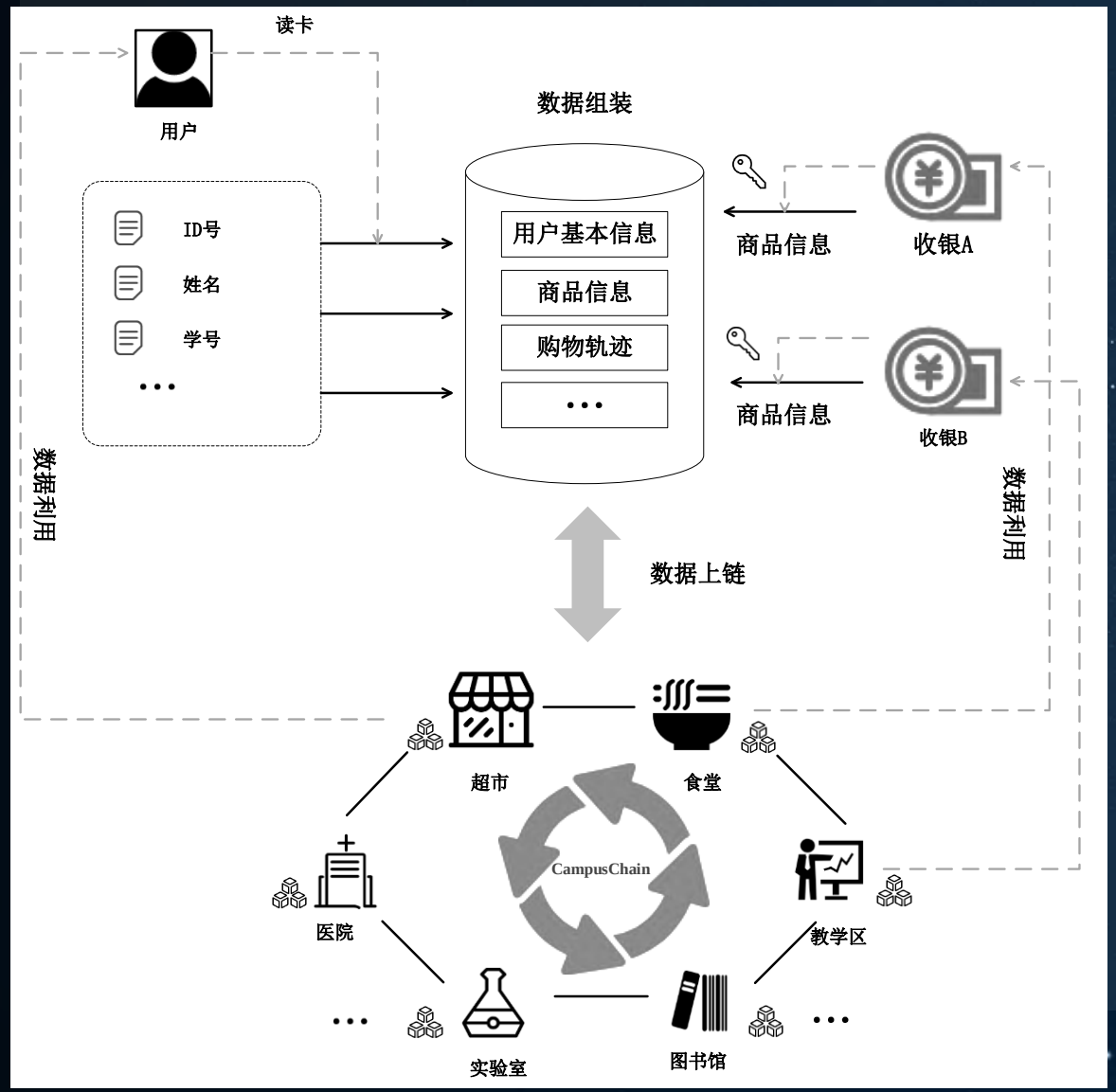
成果检验、追溯

成果授权、转让

基于智能合约的成果资产变现和收益自动化分配



区块链 + 教育应用场景



示例：CampusChain 校园区块链

- 跨部门协作：对接校内多个单元实现多主体协作
- 学业全流程记录：完成从入学到毕业的全面记录
- 学位登记校验：链上颁发毕业证、学位证，杜绝造假
- 积分激励：勤工俭学/公益服务/献血记录等链上奖励
- 可信数据利用：链上数据用来进行真伪效验，数据追溯，数据恢复，校园大数据分析等。

小结

- 区块链是什么？

定义

区块链是一个**分布式账本**，一种通过去中心化，去信任的方式集体维护一个可靠数据库的技术方案

数据角度

区块链是一种几乎不可能被更改的**分布式数据库**，分布式不仅体现在对数据的分布式存储，也体现在对数据的分布式记录

业务角度

区块链是多种技术的整合的结果，通过**新的数据结构**、**分布式共识机制**、**哈希加密算法**以及独特的运行机制，使得去中心化的信任构想成为现实。

小结

- 区块链特征

开放，共识

任何人都可以参与到区块链网络，每一台设备都能作为一个节点，每个节点都允许获得一份完整的数据库拷贝。节点间基于一套共识机制，通过竞争计算共同维护整个区块链。任一节点失效，其 余节点仍能正常工作。

去中心，去信任

区块链由众多节点共同组成一个端到端的网络，不存在中心化的设备和管理机构。节点之间数据交换通过数字签名技术进行验证，无需互相信任，只要按照系统既定的规则进行，节点之间不能也无法欺骗其它节点。

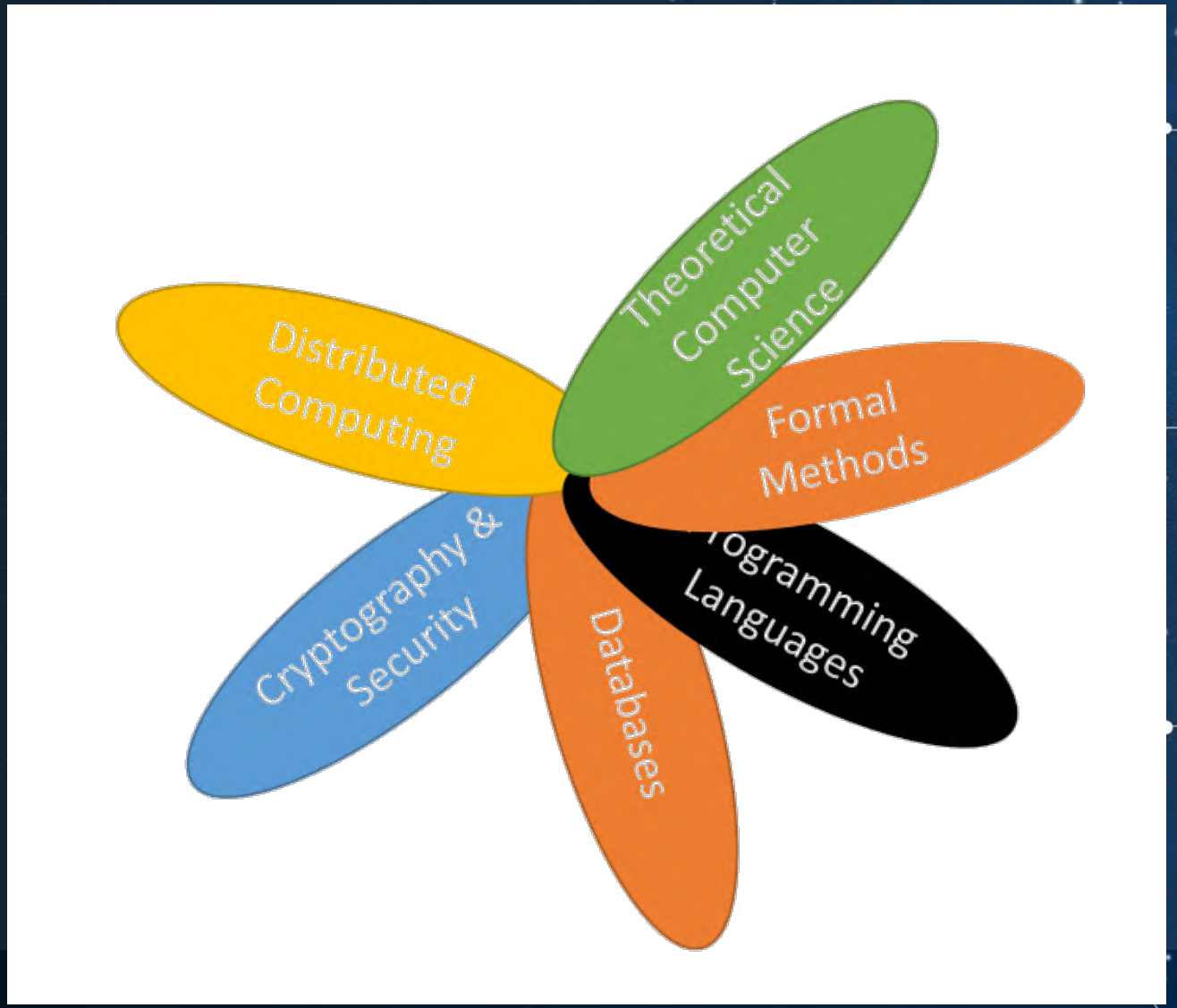
不可篡改，可追溯

单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非能控制整个网络中超过51%的节点同时修改，这几乎不可能发生。区块链中的每一笔交易都通过密码学方法与相邻两个区块串联，因此可以追溯到任何一笔交易的前世今生。

交易透明，双方匿名

区块链的运行规则是公开透明的，所有的数据信息也是公开的，因此每一笔交易都对所有节点可见。由于节点与节点之间是去信任的，因此节点之间无需公开身份，每个参与的节点都是匿名的。

区块链技术中涉及到的计算机学科



区块链面临的挑战

基于区块链的应用探索一直在加速推进，跨链、隐私保护、安全监管等区块链关键技术也正在成为研究热点。然而，区块链技术仍处于初级阶段，各方面仍面临挑战。

- 区块链技术在系统稳定性、应用安全性、业务模式等方面尚未成熟，主要在性能、能耗、生态、安全、监管方面存在问题

技术成熟

应用场景

- 区块链的应用模式仍在探索中，还没有找到真正的“杀手级”应用，区块链的“不可替代”优势还未体现

- 区块链底层系统架构设计人才要掌握多项交叉学科的专业技能，并深入理解区块链底层设计原理，兼备系统架构设计的经验

专业人才

法律法规

- 对区块链技术的治理、监管和标准等仍不健全，主要体现在两方面：一是法律主体不明确，二是链上规则不明确

谢谢!