



北京大学

PEKING UNIVERSITY

区块链课程

孙惠平

sunhp@ss.pku.edu.cn



北京大学 软件与微电子学院

School of Software and Microelectronics, Peking University



北京大学
PEKING UNIVERSITY



PART 第一章

区块链简介

- --科技让信任变简单

目录

CONTENTS



- 01. 区块链从哪里来？
- 02. 加密货币的崎岖之路
- 03. 从比特币到区块链
- 04. 区块链原理
- 05. 区块链现状

第一节

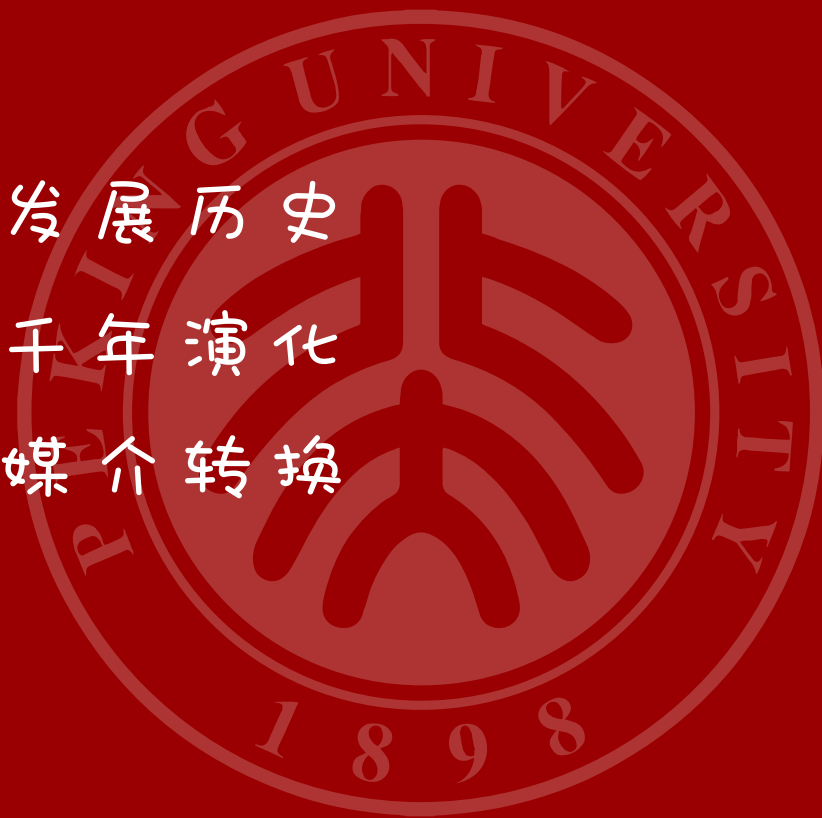
区块链从哪里来？

——人类文明的发展旅途

01 信息存储的发展历史

02 记账科技的千年演化

03 价值流通的媒介转换



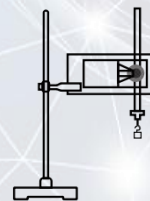
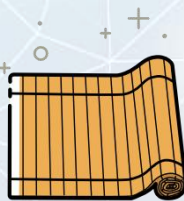
区块链从哪里来？——人类文明的发展旅途



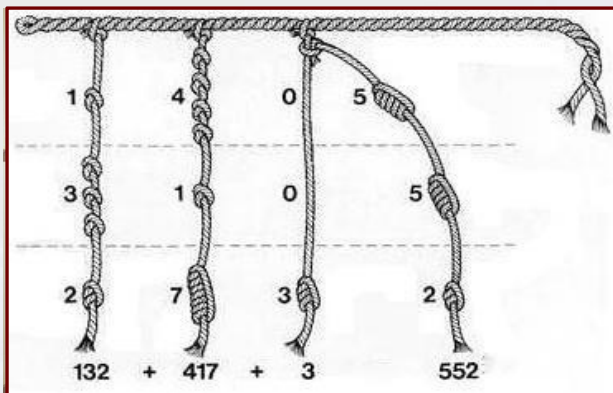
新生事物往往不是凭空而来，发展和演化也很少一蹴而就。

认识新事物，首先要弄清楚他的来龙去脉。知其出身，方能知其所以然。

区块链是信息存储与共识的载体，在了解区块链发展前，我们先了解信息存储的历史发展。



1.1 信息存储的发展历史



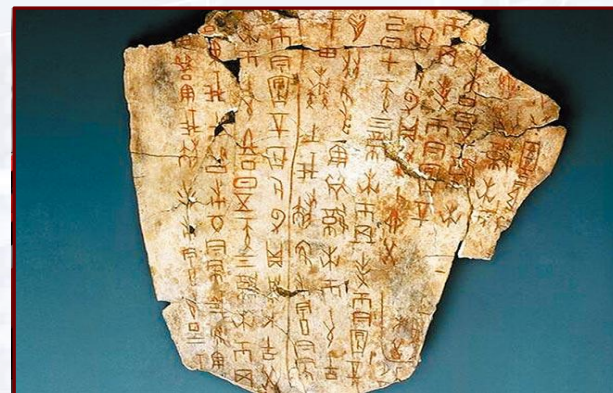
结绳记事法

在远古时候，人类为了生存聚在一起生活，一块劳动共同对抗大自然的不确定性和外界的威胁。那个时候，由于最多的活动是打猎，捕到猎物会用绳子一个个地拴起来。当时人们发现，结越多，就代表着猎物越多，结越少，就代表猎物越少。就这样，人类开始使用打结来表示数量上的不同。



刻痕记事法

在古代北欧地区，牧羊人利用刻痕计数法来记录自己的羊群数量。英语单词score就源自北欧语skor，本意是“刻痕”。由于当地人采用20进制，一条刻痕代表20，所以score也就含有“20”的意思。



甲骨文记事法

夏、商、西周三代时期，数字元号逐渐规范。公元前十四至十一世纪的殷墟甲骨文卜辞中有许多数字。其中有13个记数单字、1-9、10、100、1000、10000。

1.1 信息存储的发展历史

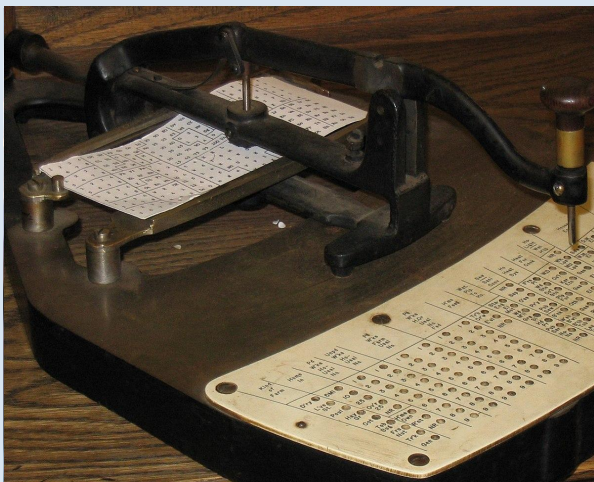
造纸术的发展

西汉（公元前202年—8年）初期，中国人发明了造纸术（此前靠龟甲、兽骨、金石、竹简、木牍、缣帛等记录文字）。纸的出现让信息的能被记录、传播和继承，带来了革命性的进步，促进了人类文化的传播。纸也为打孔卡奠定了基础。



1.1 信息存储的发展历史

打孔卡的发展历史



打孔卡

1725年法国人Basile Bouchon发明了打孔卡（穿孔卡），他用在纸上打孔的形式来存储图案，用于控制纺织机进行图案织造。



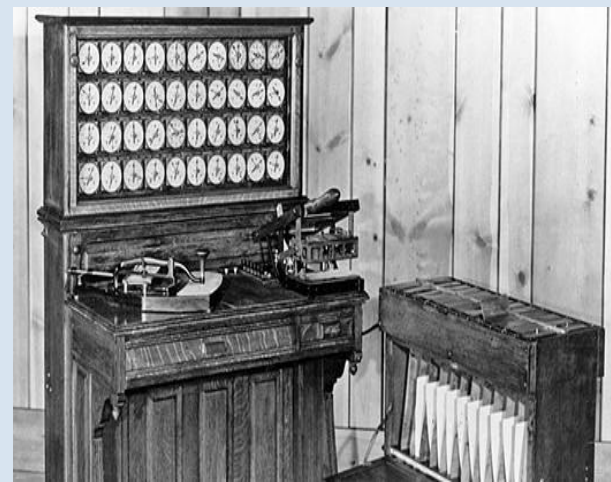
提花织机

1801年Joseph Marie Jacquard将打孔卡顺序捆绑在一起用于提花织机，这是打孔纸带（Punched Tape）的雏形。



打孔纸带

1846年Alexander Bain使用打孔纸带发送电报。

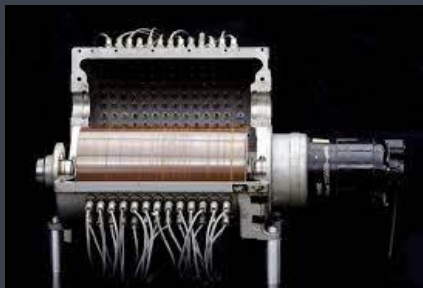


打孔卡制表机

1890年，Herman Hollerith发明了打孔卡制表机，用于收集并统计人口普查数据，标志着半自动化数据处理系统时代的开始。这种机器不仅统计速度更快，而且能够以新的方式理解信息，很快便应用到了各个行业。

1.1 信息存储的发展历史

随着存储设备的逐渐升级，同体积的硬件存储的容量呈指数级增长，出现了磁带、磁鼓、机械硬盘、固态硬盘等硬件存储设备。由于区块链需要非常大的存储量，这些硬件存储设备成为了区块链存储的根基。



在计算机领域，存储是极为重要的应用。以数据库为例，上层应用在存储数据时只需要和数据库或其他数据管理系统打交道，而数据的具体存储方式不需要应用和开发者担心。目前的应用很多都依赖单一的数据库，有些则依赖于集群部署和多地部署的数据库。但无论如何，这些数据库都由公司或机构管理。

1.1 信息存储的发展历史

场景案例

在一个食品供应链领域，食品的生产、加工、运输和零售都来自不同的企业。每个企业都管理着自己的数据库，维护着自己关心的数据。

比如：生产方关注产品生产的原料消耗、制作时间、制作成本等；加工方关注产品的采购价格、采购时间、加工价格、加工时间等；运输方关注产品的运输时间、预期交付时间、运输位置、温度等；零售方关注产品的销量、进货时间、销售时间等。



然而，当各方拥有的数据分开，会带来两个问题



数据造假追责较难

谁都有可能修改自己的数据库。一旦修改，各方难以达成共识找出足够的证据证明具体是谁改的



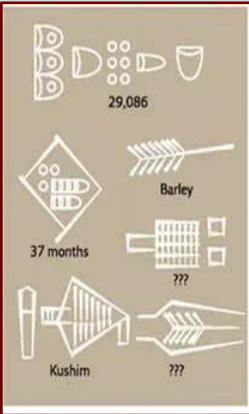
数据生态难以形成

由于各方的数据彼此隔离，想要使用这些全方面的数据实现更高的数据价值就非常困难

1.2 记账科技的千年演化

如果说信息存储是人类文明薪火相传的重要支柱，那么记账科技则是保障社会文明的核心基石

人类文明的整个发展历史，都伴随着账本科技的持续演化



简单账本

公元前3500-15世纪

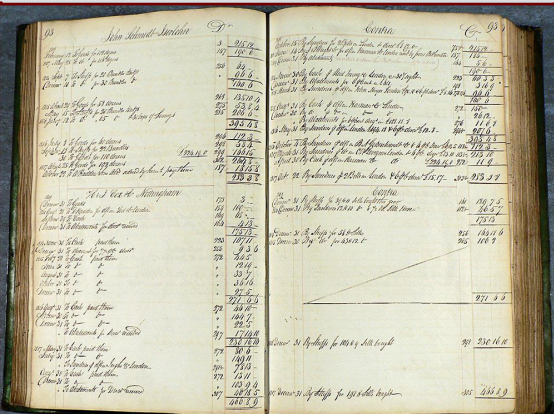
- 优点：**简单记账法自然易用，适合小规模简易账务
- 缺点：**在应对大规模的账务、涉及多个实体的复杂需求时，容易出错或被篡改



复式账本

15世纪-20世纪中期

- 优点：**将单一中心记录分拆为多个科目，极大提高了账目的可靠性，一旦发现问题，方便追查根源。
- 缺点：**仍然无法解决多方之间账本的可信互通问题。



数字化账本

20世纪中期-21世纪初

- 优点：**数字媒介的出现使得账本的规模、处理的速度、账本的复杂度，都有了翻天覆地的提升。
- 缺点：**仍然是中心化模式，数据一旦丢失则无法找回。



分布式账本

2009年-未来世界

- 优点：**由交易多方共同维护同一个共享的分布式账本；打通交易在不同阶段的来龙去脉；凭借分布式技术，进一步提高记账的规模、效率、可靠性及合规性。
- 缺点：**仍然处于发展的初期，还存在不少尚未解决的问题。

1.2 记账科技的千年演化

账本科技的未来

账本科技历经千年发展愈发弥新，由简单到复杂、由粗糙到精细、由中心化到分布式，这与业务需求的不断变化密不可分。大规模、高安全、易审计等特性将越来越受到关注。

随着社会文明特别是商业活动的进一步成熟，分布式记账的需求将更加普遍，分布式账本科技也将更加繁荣。



1.3 价值流通的媒介转换

从货币说起

货币是人类文明发展过程中的一大发明，最重要的职能包括价值尺度、流通手段、贮藏手段。很难想象离开了货币，现代社会庞大而复杂的经济和金融体系还能否持续运转。

历史上，货币的形态经历了多个阶段的演化，包括实物货币、金属货币、代用货币、信用货币、电子货币、数字货币等。货币自身的价值依托也从实物价值、发行方信用价值，到今天出现的对信息系统（包括算法、数学、密码学、软件等）的信任价值。



1.3 价值流通的媒介转换

货币的功能



交易媒介

在任何经济社会中，货币的作用之一就是交易媒介，用于购买商品与服务。采用货币来进行购买商品与服务的交易，会大幅减少交易成本，从而提高整个社会的经济效率。



记账单位

货币的第二个作用是作为记账单位，用来衡量商品与服务价值。这个作用跟用“千米”来衡量距离，“千克”来衡量重量一样。试想一下，如果没有货币作为记账单位，我们如何在超市里对商品标价。



价值存储

人们尽量将商品在还有价值的时候卖出去来获得货币，等以后需要的时候，再使用货币获得需要的商品。这就是货币的价值存贮作用。

1.3 价值流通的媒介转换

物物交换



- 贝壳、羽毛、牲口等实物货币
- **特点：**实物货币是货币发展的最初阶段，用一种人们都认可且易于交换的物品作为媒介进行交换，这种媒介就是最原始的货币。

金属货币



- 黄金、白银等贵金属
- **特点：**金属货币早期以金属块作为交易媒介，随着交易经验的积累，权力机构便发展出标准铸币。铸币的价值固定，保存方便，克服了更多的交易困难，还可以储藏、保值、积累财富。

纸币



- 早期纸币、银票、交子、廉价金属货币
- 纸币本位货币、国家法币
- **特点：**纸币是代替金属货币执行流通手段的由国家（或某些地区）发行的强制使用的价值符号。

中心化电子货币



- 在线支付，例如微信、支付宝、PayPal等
- 银行卡，VISA信用卡
- Q币、点券等游戏货币
- 电子现金
- **特点：**用一定金额的现金或存款从发行者处兑换并获得代表相同金额的数据或者通过银行及第三方推出的快捷支付服务，通过使用某些电子化途径将银行中的余额转移，从而能够进行交易。

去中心化数字货币



- 比特币
- 以太坊
- 莱特币
- 瑞波币
- 狗狗币

1.3 价值流通的媒介转换

商品货币时代

- 货币价值主要取决于贵金属的发现和冶炼

信用货币时代

- 货币本身没有价值而取决于对发行机构的信任

去中心货币时代

- 货币价值取决于人们对算法、系统的认可

有人认为信用卡相对纸币形式更方便。相对于信用卡这样的集中式支付体系来说，货币提供了更好的匿名性。另外，一旦碰到系统故障、断网、没有刷卡机器等情况，信用卡就不可用了。

无论是货币，还是信用卡模式，都需要额外的系统（例如银行）来完成生产、分发、管理等操作，带来很大的额外成本和使用风险。诸如伪造、信用卡诈骗、盗刷、转账等安全事件屡见不鲜。

1.3 价值流通的媒介转换

很自然的，如果能实现一种数字货币，保持既有货币的这些特性，消除纸质货币的缺陷，无疑将带来巨大的社会变革，极大提高经济活动的运作效率。



BLOCKCHAIN
TECHNOLOGY

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed
diam nonummy nibh euismod tincidunt ut laoreet dolore
magna Lorem ipsum dolor sit amet, consectetur adipiscing

1.3 价值流通的媒介转换

2008年11月1日，一个自称中本聪的黑客在一个密码学邮件列表中发布了一篇论文《Bitcoin: a peer to peer electronic cash system》，勾画了比特币系统的基本框架。

2009年1月3日，他为该系统建立了一个开放源代码项目，在位于芬兰赫尔辛基的一个小型服务器上挖出了第一批50个比特币，正式标志着比特币的诞生。

2010年5月，第一笔比特币支付的真实交易产生：一个佛罗里达的程序员花1万比特币（当时约25美元）买了两份披萨。

2010年7月，第一个比特币交易所在日本成立。

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.

—Satoshi Nakamoto,
“Bitcoin: a peer to peer electronic cash system”, 2008

第二节

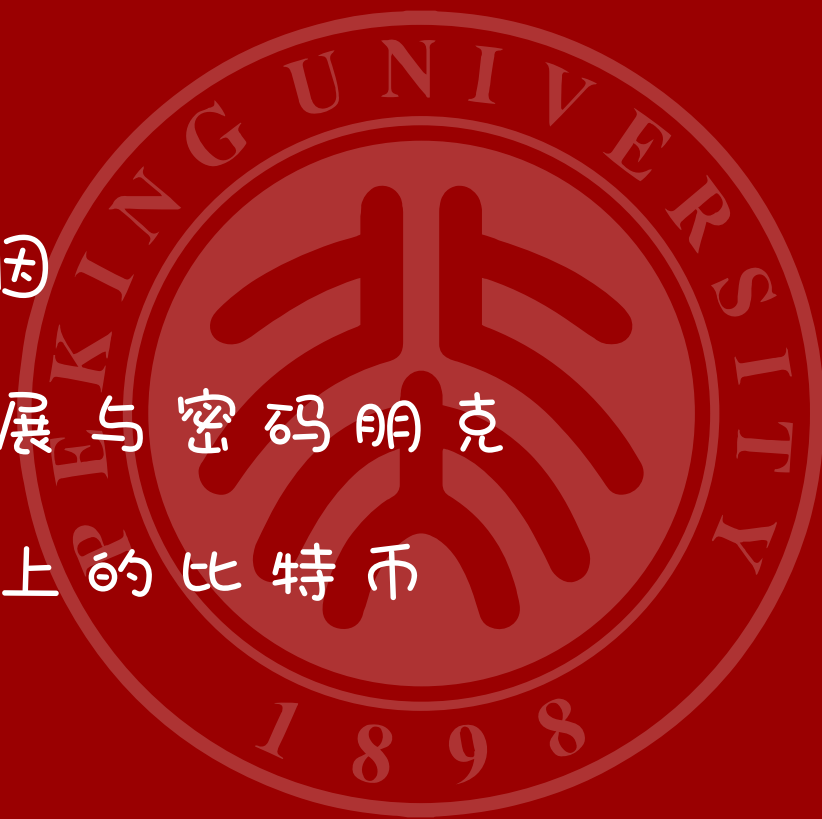
加密货币的崎岖之路

—区块链思想的摇篮

01 加密货币的基因

02 加密技术的发展与密码朋克

03 站在前人肩膀上的比特币



加密货币的崎岖之路——区块链思想的摇篮

CRYPTO COIN WITH GROWTH CHART

Sed ut perspiciatis unde omnis
Sint dicta abhorreant id quo
Vid n rationibus suscipiantur

“我们将要公开发布我们的代码，让密码朋克战友们能够使用软件。我们的代码，对全球所有人免费。如果你们要封杀我们所写的软件，我们也毫不在意。我们清楚，软件是无法被销毁的，彻底的分布式系统永不停机。”

——《密码朋克宣言》

2.1 加密货币的基因

中本聪的生日 - 为什么是 1975 年 4 月 5 日



美国大萧条时期的失业工人

1933年4月5日，针对美国遇到的大萧条，万恶的美国总统罗斯福法案，宣布进入紧急状态并禁止美国人民储藏黄金，所有美国公民必须上缴自己存储的黄金，否则处以1万美元以下罚款和五至十年的有期徒刑。

当万恶的美国政府以20.67美元每盎司强制收购美国人民手中的黄金之后，立刻将黄金价格提高至35美元每盎司在国际市场进行交易，一夜之间，美国人民的黄金财产损失超过40%。

1975年，那是万恶的美帝国主义政府重新允许人民拥有黄金的年份，福特总统签署“黄金合法化”法案，美国人民可以再一次合法拥有黄金。



罗斯福正在签署黄金禁令法案

2.1 加密货币的基因



货币的去国家化：自由主义的思考

1933年，美国政府强制兑换人民手中黄金的价格：20.67美元/盎司。

1934年，美国政府在国际市场交易黄金的价格：35美元/盎司。

1944年，美国政府承诺在布雷顿森林体系下与黄金挂钩：35美元/盎司。

1971年，美国停止向外国政府用美元兑换黄金。

1973年，布雷顿森林体系瓦解，美国宣布美元与黄金正式脱钩。

1975年，美国人民买回自己的黄金的价格是140美元/盎司。五年后，黄金价格达到590美元/盎司。

任何有理性、有良知的学者都不得不思考这一赤裸裸的掠夺。

针对布雷顿森林体系的瓦解，自由主义大师哈耶克在1976年出版了《货币的非国家化》一书。遵循他一贯的观点，哈耶克认为西方政府并不值得相信，历史一再证明，西方政府如果垄断某种商品一定会导致无效率。他梳理了西方政府发行货币的历史，无一不以西方政府失信、货币贬值终结。



英国自由主义学者哈耶克

2.1 加密货币的基因



自由货币的猜想



货币发行未必一定由国家垄断，干嘛不模仿商品的生产，搞一下竞争呢？哈耶克认为，私人货币，比黄金要好得多。私人货币相对于法定货币将展现出两个优势：

(1) 币值稳定

(2) 币值的稳定将减少经济周期波动的不利影响。

哈耶克的最终理想是国家将货币的权利还给人民。关键则是自由竞争产生稳定的币值。

2.2 加密技术的发展与密码朋克

加密货币诞生的基础——密码学技术的发展

加密货币系统包含了计算机科学过去20多年的成果：计算机网络P2P、算法、数据库、分布式系统、计算机密码学，等等。其中，计算机密码学又是重中之重。离开现代密码学和信息安全技术，人类社会将无法全面步入信息时代。

DH密钥交换技术

- 1976年，Diffie和Hellman的《密码学的新方向》提出非对称加密技术，实现了在不安全的互联网上安全进行加密通信。

RSA非对称加密算法

- 1978年，Ron Rivest、Adi Shamir、Leonard Adleman 共同提出，非对称加密算法有效解决了安全分发密钥的问题。

Merkle-Tree

- 1980年，斯坦福大学博士Merkle Ralf正式提出了Merkle-Tree这种数据结构和相应的算法的数据结构。

ECC椭圆曲线加密算法

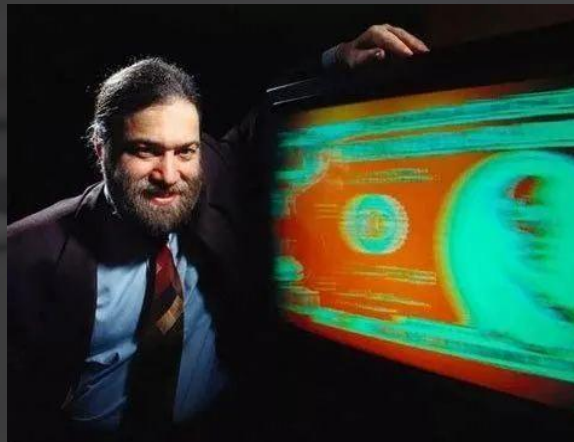
- 1985年，Neal Koblitz 和 Victor Miller分别独立提出了椭圆曲线加密算法——
- Elliptic Curve Cryptography (ECC)，ECC算法具有多种国际标准，具备较高的安全性。

2.2 加密技术的发展与密码朋克



拜占庭将军问题

1985年, Leslie Lamport等人提出的拜占庭将军问题 (Byzantine Generals Problem)。用来解决公开网络上的信任问题。1982 年Leslie Lamport 把军中各地军队彼此取得共识、决定是否出兵的过程, 延伸至运算领域, 设法建立具容错性的分布式系统, 即使部分节点失效仍可确保系统正常运行, 可让多个基于零信任基础的节点达成共识, 并确保资讯传递的一致性。



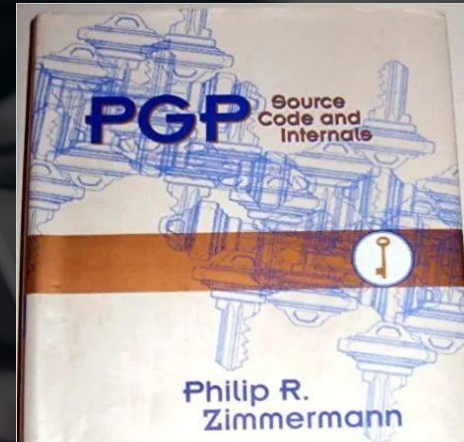
不可追踪加密网络支付

1982年和1985年, 被后人成为数字货币先锋的David Chaum 分别发表了两篇论文, 提出了不可追踪的密码学网络支付系统, 阐述了数字货币的构想, 为后来孕育出区块链诞生的“密码朋克”奠定了技术基础



时间戳技术

- 1991年, 密码朋克成员Stuart Haber与W.Scott Stornetta 提出了一个用 时间戳的方式来保证数字文件安全的协议。该协议用时间戳表达文件创建的先后顺序, 并要求在文件创建后其时间戳不能改动, 从而使得文件被篡改的可能性为0。



PGP

1991年, Philip Zimmerman 发布 PGP, PGP 是用来做邮件加密的, 它是一个基于 RSA 公钥加密体系的邮件加密系统, 能够保证邮件内容不被篡改, 同时让邮件接受者信任邮件来自发送者。

2.2 加密技术的发展与密码朋克

朋克运动-对传统的反抗



20世纪六七十年代，社会思潮风起云涌。西方的年轻人热衷于反抗，以消除心中的不满与苦闷。朋克运动应运而生，最初的形式是一些搞乐队的酷小孩，穿着奇装异服，弹唱暴躁而反叛的摇滚。后来，朋克成了一种精神，成了年轻人对抗传统，发泄不满，甚至反对一切、为了反对而反对的精神。朋克精神就是反抗传统。然而时间久了，反抗本身也成为了一种传统，由此流传下来。



到了20世纪80年代，个人计算机开始流行，网络崭露头角。另一个新发明——非对称加密，也进入了实用阶段。那些缺少音乐细胞，搞不了摇滚，因而偏爱理工科继而被视为书呆子的年轻人，终于有了自己的武器与阵地。他们骨子里的那种反抗精神终于有了发泄的途径。

至此，朋克精神进入技术与网络领域



2.2 加密技术的发展与密码朋克

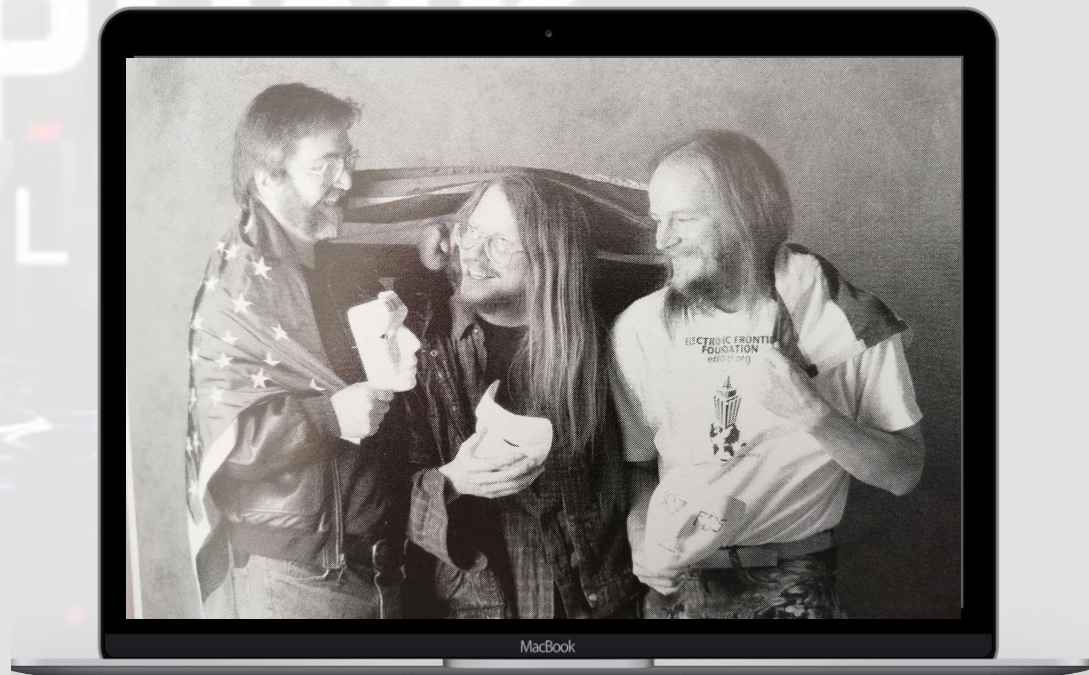
密码朋克 - 对隐私的追求

1992年，三位退休技术大咖——加利福尼亚大学伯克利分校数学家埃里克·休斯（Eric Hughes）、退休的英特尔员工蒂姆·梅（Tim May）、以及曾是Sunmicrosystems第五位员工的计算机科学家约翰·吉尔摩（John Gilmore）邀请了二十位最亲密的朋友参加了一次非正式会议，期间他们讨论了一些看似最令人头疼的程序和密码问题，加密货币的神秘大门也正是从这个时候开始，被他们这个组织打开了。

这个组织的创始人并不多，他们痴迷密码学，但不想让外界知道自己的身份，也不想参加线下聚会。而如果在公开的网络上发表信息就立刻被别人知道，根本没办法保护因此，因此，早期密码朋克成员之间大多只是通过匿名邮件列表进行点对点的沟通。

匿名邮件列表最大的特点就是匿名性，大家可以隐藏身份进行交流，越来越多有价值的讨论就出现了。如何形成合力，建立组织共识？

1993年，经过多轮讨论和商议，终于形成了一个共识。埃里克·休斯起草了《密码朋克宣言》，标志着“密码朋克”组织的诞生，这也是“密码朋克”一词第一次出现。



2.2 加密技术的发展与密码朋克

■ 从密码朋克到加密货币

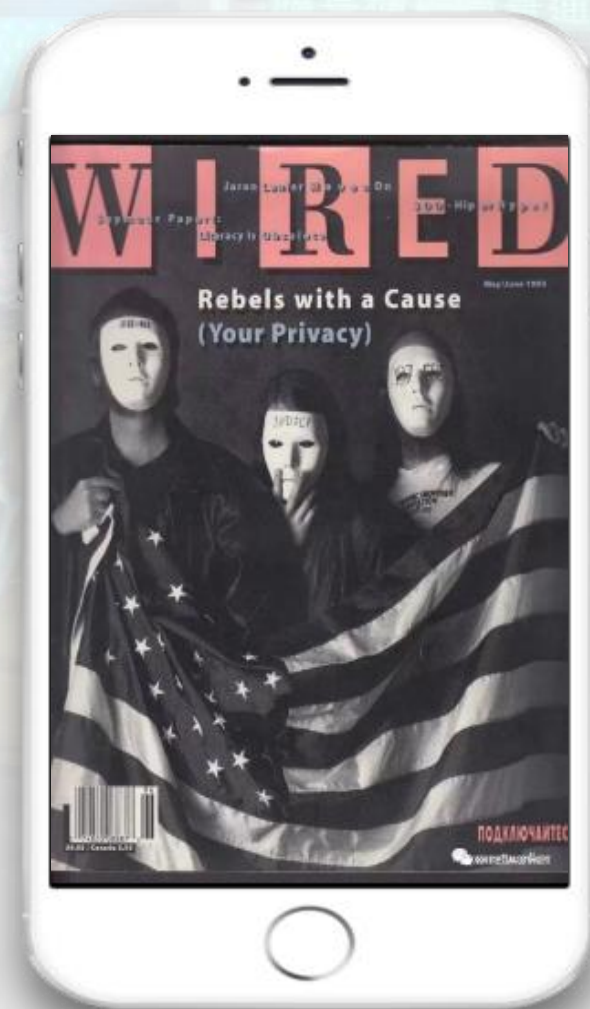
很快，匿名邮件列表中的成员数量就突破了1400人。讨论的话题包括数学、加密技术、计算机技术、政治和哲学，也包括私人问题。

早期的成员有非常多的IT精英，比如维基解密的创始人阿桑奇，BT下载的作者布拉姆-科恩，万维网发明者蒂姆-博纳斯-李爵士。提出了智能合约概念尼克萨博；Facebook的创始人之一肖恩-帕克，当然还包括比特币的发明人中本聪。

密码朋克们都是密码学家，有的只是密码学知识，编写代码的技能和他们心中的梦想。因此，

他们只有一条路可走，那就是用他们的才能，架构出一个基于密码学的匿名加密货币系统，这就是比特币诞生的根源。

据统计，比特币诞生之前，密码朋克的成员讨论发明过失败的数字货币和支付系统从多达数十个。



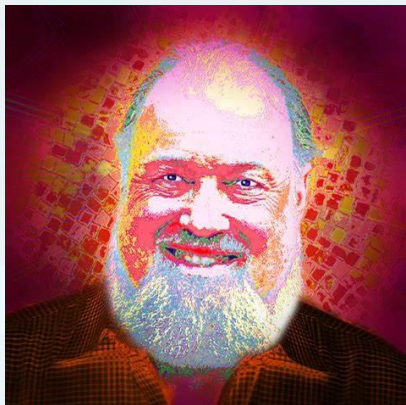
2.3 站在前人肩膀上的比特币

通往比特币的漫长之路

上世纪50年代计算机出现后，人们就尝试利用信息技术提高支付系统的效率，开发除了使用电子支付手段的各种银行卡。自80年代起，随着密码学技术的发展和密码朋克运动的兴起，那些追求隐私的密码学家们，开始利用他们密码学的知识，来完成他们心中的梦想

——用他们的才能，架构出一个基于密码学的匿名加密货币系统

加密货币前后经历了三十多年的探索，比较典型的成果包括e-cash, HashCash, B-money和BitGold等。



1982年David Chaum与Ecash



1997年Adam Back与Hash Cash



1998年戴伟与B-money



2005年Nick Szabo与BitGold



2008年中本聪与Bitcoin

2.3 站在前人肩膀上的比特币



David Chaum与Ecash

1983年，荷兰密码学家大卫·乔姆（David Chaum）提出不可追踪的密码学网络支付系统，被认为是比特币设计思想的雏形。8年后，他将此想法扩展为密码学匿名现金系统，即Ecash。

ecash 系统是首个尝试实现不可追踪（untraceable）的匿名数字货币，基于 David Chaum 自己发明的盲签名技术，曾被应用于部分银行的小额支付系统中。

然而，ecash 虽然不可追踪，但仍依赖中心化机构（银行）数据库的协助，才能验证一笔钱是否已经花掉



Ecash 的优势与缺陷

- 优势：使用盲签名隐私保护技术，是首个尝试实现不可追踪的匿名数字货币，为未来几十年的大量创新和研究奠定了基础。
- 缺陷：依然依赖一个中心化数据库的协助。本质上与银行没有区别

密码朋克真正追求的是一个没有中心组织的匿名货币系统！



E-cash Registers

2.3 站在前人肩膀上的比特币

对抗垃圾邮件的办法：POW-工作量证明机制

1990 年代早期，电子邮件系统方便了无数互联网人，但当时的互联网先驱们，意识到了电子邮件系统有自己的问题。

发送电子邮件很简单、成本也很低，而且你还可以向许多人发送同样的消息，那一定会招致滥用”，IBM 的研究员 Cynthia Dwork 博士和 Moni Naor 博士在他们发表于 1992 年的白皮书中这么解释。该白皮书名为“**以任务处理施加代价，打击垃圾邮件**”。

- 为此，他们提出了这样的方案：发送电子邮件的人，每逢发送一份邮件，都要在邮件中附加一些数据。这些数据需是一个数学问题的解，而且每封邮件提出的问题都是独一无二的。
- 要给电子邮件添加一个解并不难，理想情况下只需一台普通计算机的处理能力，算个几秒钟就行，：然而对发广告的、搞诈骗的和黑客来说，会累积出高昂的成本，因为他们都想一次性发送几千乃至几百万条消息。



Cynthia Dwork

2.3 站在前人肩膀上的比特币

Adam Back 与 Hash cash



就在 Dwork 和 Naor 出版他们白皮书的同一时间，密码朋克成员，埃克塞特大学的博士后 Adam Back 也一直在思考用类似的方法来对抗垃圾邮件。

1997 年 3 月 28 日，密码朋克邮件列表的 2000 多个订阅者收到了一封邮件，开头就是左图的引文。在 Hashcash 中，邮件的元数据（如“发送者地址”、“收件人地址”、发送时间，等）都被形式化为一个协议。此外，电子邮件的发送者必须给这部分元数据加入一个随机数字，称作“nonce”。所有这些元数据，包括这个“nonce”，（输入哈希函数后）可得出一个哈希值。



- **优势：**首个提出 POW 方案的货币，POW 方案所提供的，乃是数字货币研究的一个全新的基础。后来的大多数重要的数字货币方案，都建立在 Hashcash 之上。
- **缺陷：**
 - 1、Hashcash 并不能很好地担当一种成熟的现金，他只能用来对抗垃圾邮件。
 - 2、接收者“收到”的工作量证明，对他来说没有任何用处
 - 3、计算机的性能日益提高，相同的时间里，它们可以生成越来越多的证明——Hashcash 会遭遇超级通胀。

2.3 站在前人肩膀上的比特币



戴维与B-money

1998 年，刚大学毕业的华人 Wei Dai（戴维）提出了 B-money 的设计，这是首个不依赖中心化机构的匿名数字货币方案。B-money 引入工作量证明的思想来解决数字货币产生的问题，指出任何人都可以发行一定量的货币，只要他可以给出某个复杂计算问题的答案，货币的发行量将跟问题的计算代价成正比。并且，任何人（或部分参与者）都可以维护一套账本，构成一套初级的 P2P 网络，使用者在网络内通过对带签名的交易消息的广播来实现转账的确认。B-money 是去中心化数字货币领域里程碑式的成果，为后面比特币的出现奠定了基础。从设计上看，B-money 已经很好地解决了货币发行的问题



B-money 的优势与缺陷

- 优势：B-money 是首个不依赖中心化系统而使用分布式思想的匿名数字货币方案，分布式思想是比特币的重要灵感来源，在比特币的官网上，B-money 被认为是比特币的精神先导。
- 缺陷：未能解决“双花”问题，也未能指出如何有效、安全地维护账本，而戴维本人由于始终未能解决货币的稳定性问题，最终未能实现。

B-money — 1998年，比特币的精神先导

戴维 (Wei Dai)



2.3 站在前人肩膀上的比特币



尼克·萨博与Bit-Gold

1998年，密码朋克早期成员，前DigiCash员工尼克·萨博设计出了一种叫“比特黄金” (bit gold) 的去中心化的数字货币机制(所谓：《比特黄金白皮书》)，被公认为是比特币的最直接先驱。

在 DigiCash 工作期间，萨博便认识到了 eCash 中心化系统的风险。于是，他便想要创建出一种能够媲美黄金等贵金属的加密货币，使得它兼具数字性和稀缺性，而且其稀缺性不依赖于对第三方的信任。——这，就是比特黄金。

比特黄金使用了**工作量证明机制**来解决数字货币的产生问题，使用**时间戳技术**来对抗通胀问题



BitGold™



BitGold 的优势与缺陷

- 优势：Bit Gold 是比特币的早期雏形。除了基于公钥密码学的所有权记录共享数据库之外，工作量证明哈希链也与比特币的区块链设计有着惊人的相似之处。
- 缺陷：未能解决“双花”问题，也未能指出如何有效、安全地维护账本，而戴维本人由于始终未能解决货币的稳定性问题，最终未能实现。

2008年4月，萨博决定将他的想法变为现实，并在博客上写道：“演示版本和试验市场能让Bit Gold获益良多，有人能帮忙写代码吗？”

2.3 站在前人肩膀上的比特币

比特币—金融危机中开拓新的时代

2008年年末，源自美国的金融危机已经演变为世界金融危机，形成全球性恐慌，很多国家做出了过激反应。同时，现存的世界货币金融体系，以及对这一体系有至关重要影响的国际货币基金组织遭受普遍质疑。很多经济学家预测此次金融危机可能超过20世纪30年代的大危机。

就在这一年的11月，一篇署名中本聪（Satoshi Nakamoto）的研究报告“Bitcoin: A Peer-to-Peer Electronic Cash System”发表。不到两个月，即2009年1月3日，经中本聪对其提出的比特币理论系统的实际运行，即所谓的“挖掘”过程，第一个比特币的区块横空出世，其中包含50枚比特币。



比特币发明者——中本聪，日裔美国人，数学家，精通密码学，身份神秘。拥有100万个比特币。比特币初期，通过加密电邮与论坛中的比特币粉丝交流，2011年不再回复消息，将比特币域名、比特币客户端交给加文·安德列森（比特币基金会首席科学家）。

2.3 站在前人肩膀上的比特币

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 payments to be sent directly from one party to another without the need for a central authority or financial institution. Digital signatures provide part of the security, but the main proof is that a transaction is only valid if it is confirmed by the network. Benefits are lost if a trusted third party is still required to process transactions. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into a proof-of-work, forming a record that cannot be changed without the consensus of the network. The longest chain not only serves as proof of the fact that a transaction has been included in the blockchain but also serves as a proof of the fact that a majority of CPU power is controlled by honest nodes. The network itself requires minimal structure, no centralized server or authority, and nodes can leave and rejoin the network at any time. The proof-of-work chain as proof of what has been done in the past.

Introduction

Electronic payments on the Internet has come to a point where third parties to process electronic transactions, it still suffers from the inherent problem of being completely non-reversible transactions, mediating disputes. The current practical transaction system has a broader cost in terms of time and money. With the increasing number of their customers, a certain percentage of firms are avoided in person-to-person communications. What is needed is a system that is needed in any two-way transaction. Transactions are not subject to fraud, and the system is not subject to any central authority. In this paper, we propose a peer-to-peer electronic cash system. The main idea is that a transaction is only valid if it is confirmed by the network.

比特币白皮书

本文提出了一种完全通过点对点技术实现的电子现金系统。他使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。

解决传统货币的根本问题 ——bitcoin的特性

中本聪选择在2008年全球金融危机的时候将比特币公布于世，在介绍他的创新时说道：

传统货币最根本的问题在于信任。中央银行必须让人信任他不会让货币贬值，但历史上这种可信度从来都不存在，银行必须让人信任他能管理好钱财，并让这些财富以电子货币形式流通，但**银行却总是用货币制造信贷泡沫**，使私人财富缩水。



中心化问题

比特币是点对点的支付系统，没有经过任何中心化机构，比如银行。

对应比特币的特性



通胀问题

比特币的发行总量恒定为2100万枚，不存在货币增发情况，比如美元。

中本聪十分清楚，自己将颠覆很多统治阶级的既得利益，所以他在比特币白皮书里对政治只字未提，但处处含沙射影，这也从一个侧面印证了他创造比特币是为了改变传统政治货币的桎梏。

比特币，就是为了对抗政府信用失信和银行信贷泡沫而出现的。

哈耶克在《致命的自负》中说：“**我们的文明，不管是它的起源还是他的维持，都取决于这样一件事情，他的准确表述，就是在人类合作中不断扩展的秩序。**”

比特币作为一种支付体系，将人们从对第三方的信任的依赖中解放出来，扩展了人们的社会协作，为数字时代的社会秩序提供了新的工具。

Our civilization, both its origin and its maintenance, depends on one thing, as he accurately describes it, the expanding order of human cooperation.

《The Fatal Conceit》

—— *Friedrich August von Hayek*

第三节

从比特币到区块链

——思想与技术的绚烂化学反应

01 区块链定义

02 区块链特性

03 区块链分类





2008年11月1日，中本聪在密码朋克邮件列表中发布了文《Bitcoin: a peer to peer electronic cash system》，勾画了比特币系统的基本框架。

然而，在这篇论文中，并没有区块链（Blockchain）一词，而是频繁出现单独的“区块”与“链”两个词。

2009年1月9日，那个神秘的男人中本聪，在密码朋克邮件组里，发布了比特币0.1版本。这个基于C++语言的程序在Windows上可以运行，并在磁盘上创建了名为“Blockchain”的目录。

至此人们称比特币的技术为

“区块链”
(BlockChain)



3.1 区块链定义

从2008年中本聪提出比特币以来，区块链得到了产业界和学届的广泛关注，相关的学术论文和文献大量出现，有很多不同的区块链的定义

国际标准化组织 (ISO: International Organization for Standardization)

区块链是使用密码链接将证实的块按照只增序列化链式组织形成的防止篡改分布式账本。

美国国家标准与技术研究院 (NIST: National Institute of Standards and Technology)

区块链是一种分布式数字账本，账本中每一个块包括一组被密码签名的交易，每一个块通过验证和进行共识决定形成，并通过密码链接到前面的块以防止篡改。当新的块被增加后，越旧的块变得越难于被修改，新的块被网络中的记账节点复制，任何冲突能根据预先确立的规则自动解决。

IBM公司

区块链是一个共享的分布式账本，旨在促进业务网络中交易记录和资产跟踪流程。

定义

3.1 区块链定义

通过上述12个区块链定义，我们可以看出区块链包括如下一些含义：

区块链是一个区块结构

区块链是区块按照链式结构连接在一起的一种数据结构，这种结构具有只增、防止篡改、难于修改的特征，这是相对狭义的定义。



区块链是一个密码使能系统

区块链需要标明实体的身份、需要证明和验证交易、需要构造区块链结构，这些都需要密码学的支持，比如公钥密码、数字签名、数字哈希等密码学函数和功能。



区块链是一个分布式账本

区块链是一种分布式系统，通过将交易处理、传播、验证、存储等功能分布到不同的账本节点上，形成了一个记账节点之间共享的分布式账本，通过账本复制提高了账本抵御安全攻击的能力。



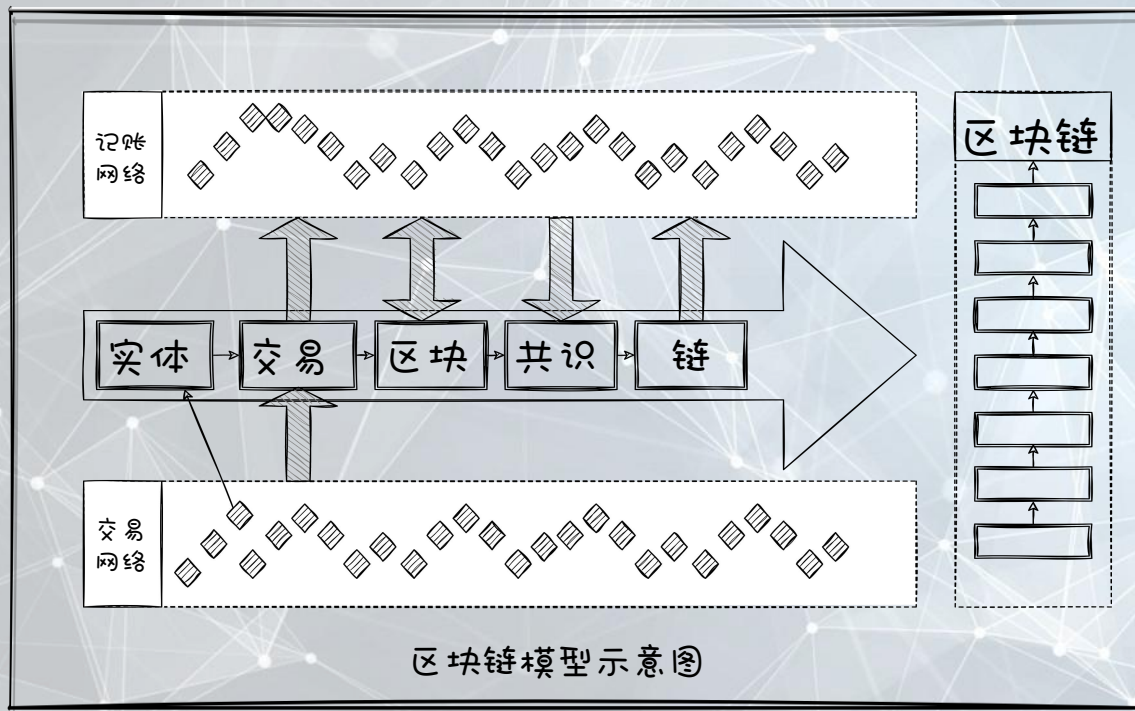
区块链是一个交易处理基础设施

区块链的目的是高效安全的交易处理，和中心化的交易处理系统相比，分布节点通过共识机制来保证交易的更新和维护，可以为广泛的应用提供一种数据不可篡改、业务逻辑自动可新的计算基础设施。



3.1 区块链定义

根据上面的区块链定义和分析，我们将区块链抽象成如图所示的模型，该模型包括交易网络、记账网络、区块链、实体、交易、区块、共识和链等概念，每个概念的含义具体如下：



交易网络

互相之间发生交易的实体构成的网络。一般通过对等网络连接。



记账网络

记账节点构成的网络。和交易网络一样，一般也是通过对等网络连接。有些系统中记账网络和交易网络是重叠的，节点既可以发生交易也可以记账，有些系统中交易网络和记账网络是分离的。但实际运行中基本上记账网络和交易网络均是分离的。



区块链

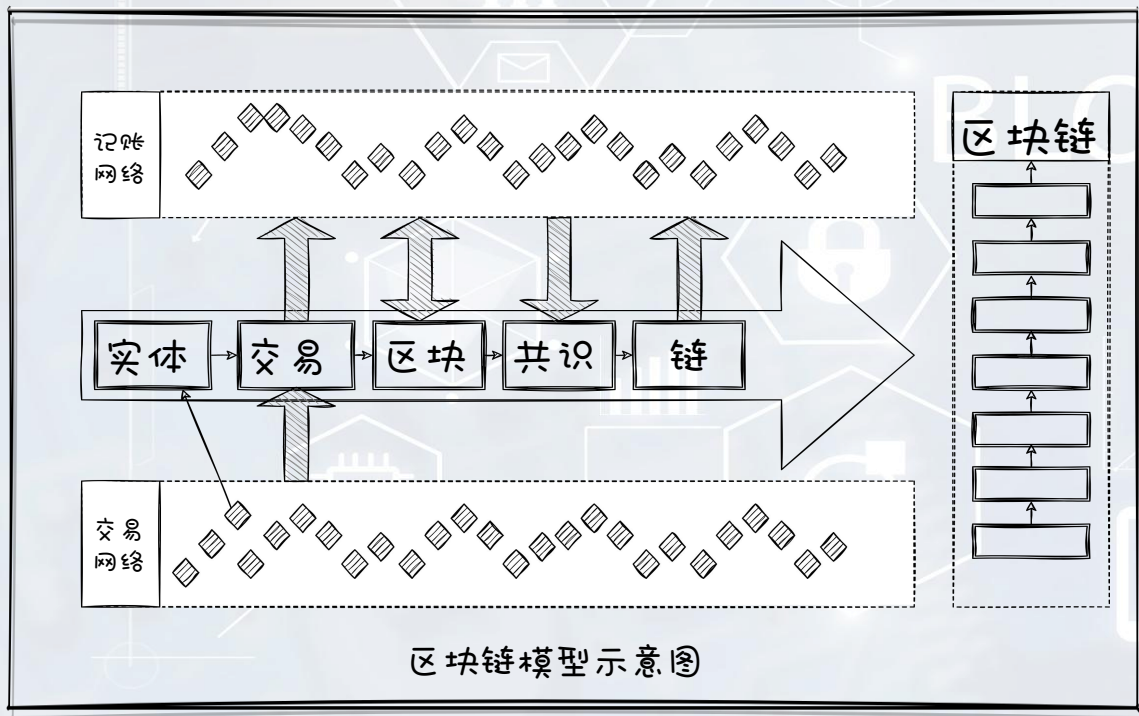
链式结构连接的区块数据形成的数据结构。区块链的实际存储有很多方式，可以存储在关系数据库、KV数据库、分布式存储等存储系统中。

3.1 区块链定义



链

指的是基于哈希指针的链式结构，一个新的经过记账节点的共识形成的区块，通过链式结构假如区块链的尾端。



实体

可以发生交易的个体。实体一般通过公私钥机制来进行身份管理和认证，根据需要这些实体可以匿名的，也可以是实名的，实名和匿名的程度主要看隐私保护的要求。



区块

多个交易数据按照某种方式组织的一个数据结构。



交易

记账节点构成的网络。和交易网络一样，一般也是通过对等网络连接。有些系统中记账网络和交易网络是重叠的，节点既可以发生交易也可以记账，有些系统中交易网络和记账网络是分离的。但实际运行中基本上记账网络和交易网络均是分离的。



共识

记账节点对交易和区块的真实性，乃至任何一种状态和行为的一致性的认定。区块链指的共识一般是拜占庭容错的共识，也就是分布式节点中存在恶意破坏系统的节点。

区块链特性

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。任一节点失败，其余节点人能正常工作。

去中心化，去信任

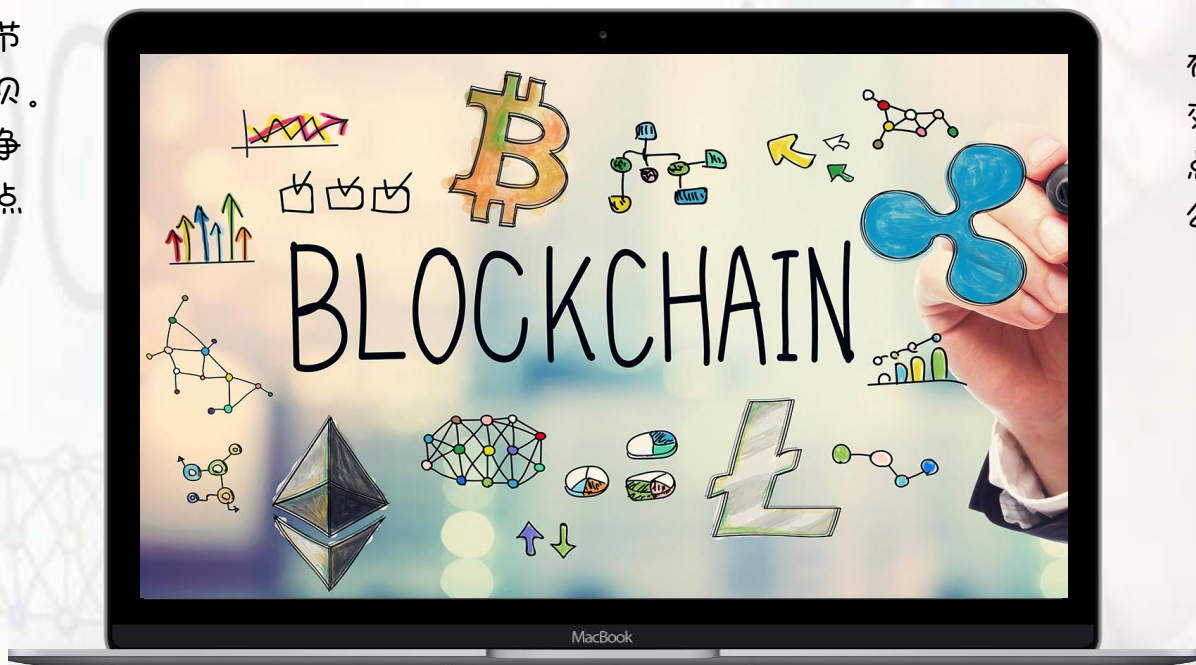
区块链由众多节点共同组成一个端到端的网络，不存在中心化的设备和管理机构。节点之间数据交换通过数字签名技术进行验证，无需互相信任，只要按照系统既定的规则进行，节点之间不能也无法欺骗其他节点。

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心超过51%的节点同时修改，这几乎是不可能发生的。区块链中的每一笔交易都通过密码学方法与相邻的两个区块串联，因此可以追溯到任何一笔交易的前世今生。

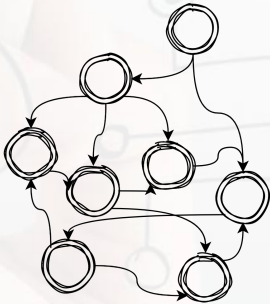


区块链的分类

并不是所有区块链都和比特币一样。根据节点的准入规则，可以将它们分为公有链、联盟链和私有链

- 公有链对所有人开放，任何人都能参与，如比特币、以太坊等。
- 联盟链对特定的组织团体开放，如Fabric、BCOS、蚂蚁链等。
- 私有链对单独的个人或实体开放，通常由公司或个人内部使用。

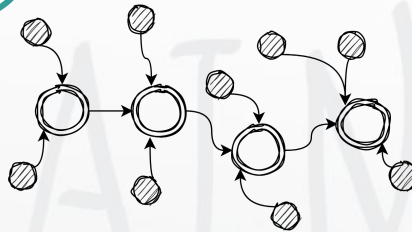
公有链



任何人都可加入网络访问/写入
数据

- 每秒3-20次数据写入
- 需要给挖矿者激励

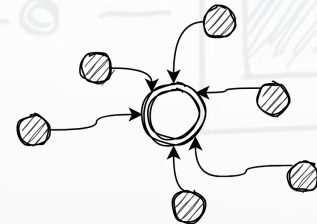
联盟链



授权公司和组织才能加入网络

- 每秒1000次以上数据写入
- 机构间互利共赢，无需激励

私有链



• 单个公司和组织管理的网络

- 每秒1000次以上数据写入
- 无需激励

3.3 区块链分类

著名区块链项目介绍



比特币 (Bitcoin) 是一种基于去中心化, 采用点对点网络与共识主动性, 开放源代码, 以区块链作为底层技术的加密货币。比特币由中本聪 (网名) (Satoshi Nakamoto) 于2008年10月31日发表论文提出。



以太坊 (Ethereum) 是一个去中心化的开源的有智能合约功能的公共区块链平台。以太币 (ETH) 是以太坊的原生加密货币。截止 2021 年 8 月, 以太币是市值第二高的加密货币, 仅次于比特币。



蚂蚁链是蚂蚁集团智能科技业务对外品牌, 致力于用科技链接信任。通过融合交叉区块链、AIoT、数据分析和智能风控等技术, 为产业互联网提供可信、高效的技术解决方案。构建数字时代的可信链接网络, 促进产业协作和价值创造。

第四节

区块链原理

- 01 交易实例
- 02 哈希指针
- 03 链式结构
- 04 区块结构
- 05 分布账本
- 06 为什么去中心化？
- 07 区块链历史
- 08 区块链未来



4.1 交易实例

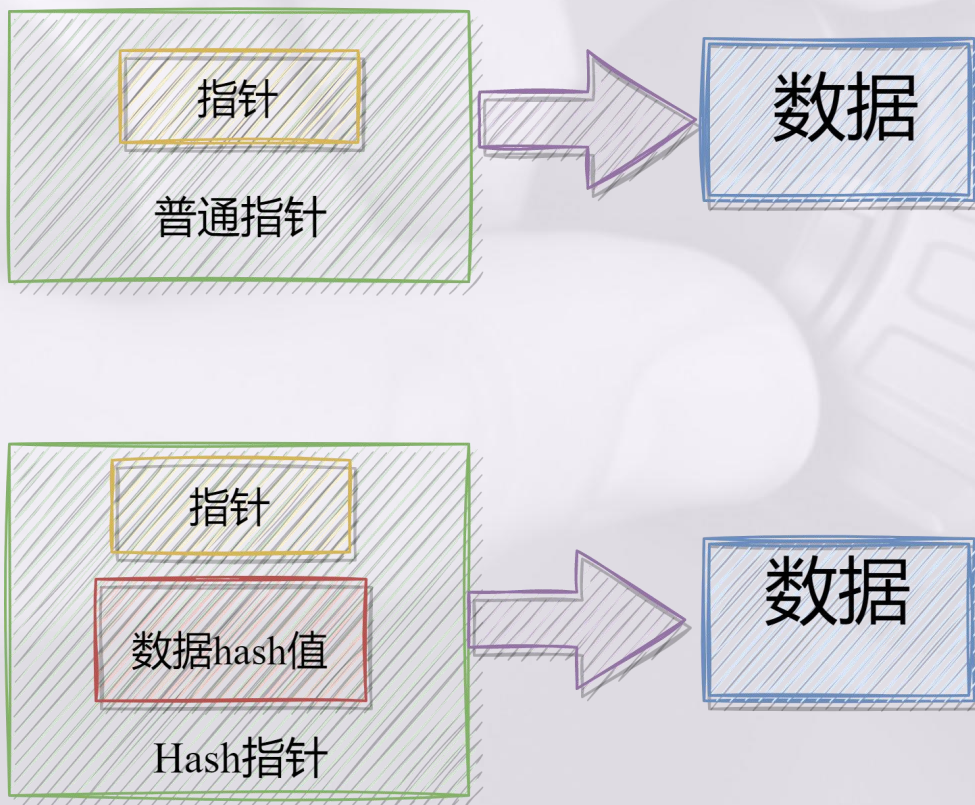
交易网络存在 n 个实体，分别为 $E1$ 、 $E2$ 、...、 E_n 。每个实体有自己的账户，账户有该实体的余额（假设单位为元）。该交易网络中存在一系列的交易，分别为 $T1$ 、 $T2$ 、...、 T_m ，交易内容包括该交易涉及的实体和交易数额。例如交易 $T1$ 是实体 $E1$ 向实体 $E2$ 转移20元。

序号	实体	账户
01	E1	88
02	E2	120
03	E3	65
04	E4	20
05	E5	320
06	E6	56
07	E7	95
08	E8	177
...	...	...

序号	交易	内容	交易数额
01	T1	E1 E2	20
02	T2	E4 E6	8
03	T3	E8 E4	45
04	T4	E6 E7	32
05	T5	E5 E4	14
06	T6	E7 E8	21
07	T7	E2 E5	30
08	T8	E5 E6	100
...	...	...	...

如果采用传统的数据库的存储方式，如图所示构建两个表，一个表是实体账户余额表，另一个是交易表。这种序列存储方式无法提供较好的数据完整性保证，攻击者获得表的访问权限后可以任意修改每一个表的字段，修改任一记录的复杂度是 $O(1)$ 。

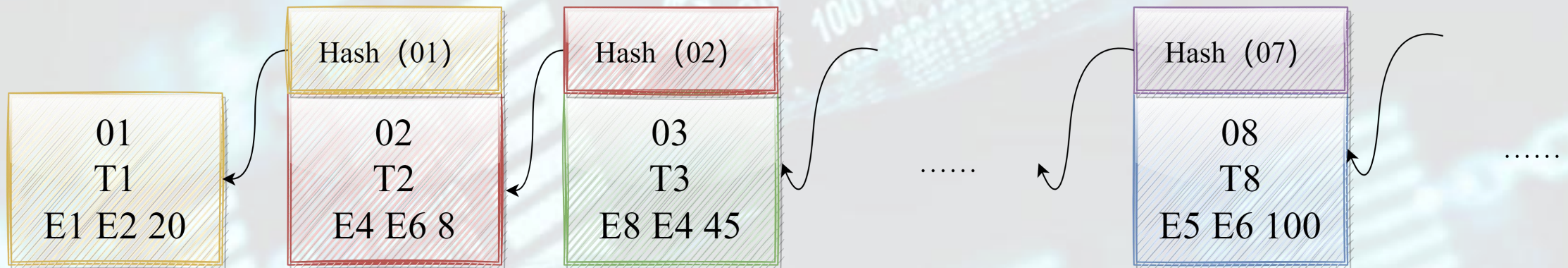
4.2 哈希指针



区块链为了更好的数据完整性保证，使用和哈希指针（Hash Pointer）的技术。如图所示，Hash指针将指针和Hash函数相结合，哈希指针不仅包括数据存储的指针（即地址），还包括所指数据的哈希值。知道一个数据的指针可以取回该指针所指的数据，知道一个数据的哈希指针不仅可以取回该指针所指的数据，还可以判断该数据是否已经修改。

4.3 链式结构

在上述交易数据的平板结构上，可以通过增加一系列哈希指针来构建余个链式的交易数据存储，假设交易是按照序号不断发生的，如图所示，将T1交易数据的哈希指针存在T2交易中，将T2交易数据和携带的T1的哈希指针生成一个新的哈希指针存在T2交易中，按照这样的处理方式，新发生一个交易，就将上一个交易的数据生成哈希指针存在新交易中。



4.3 链式结构

和上一节的平板结构对比，链式结构的修改难度是 $O(n)$ ， n 表示链的长度和要修改的交易位置之差，比如当前交易为 T_8 ，要修改 T_1 ，需要修改6个交易数据，如果 n 很大，我们可以发现做一个交易数据修改就相当于重构一遍所有涉及的交易，交易很多很频繁的情况这种修改是不可能的，需要耗费非常大的存储和计算资源。



数据不可篡改

链式结构使得交易数据的存储难于修改，这就是我们常说的区块链的只增和不可篡改，只增和不可篡改值得是难于修改，不是真的不能修改，交易数据是可以修改的，但是修改后不被发现比较困难，需要修改者付出较大的代价。

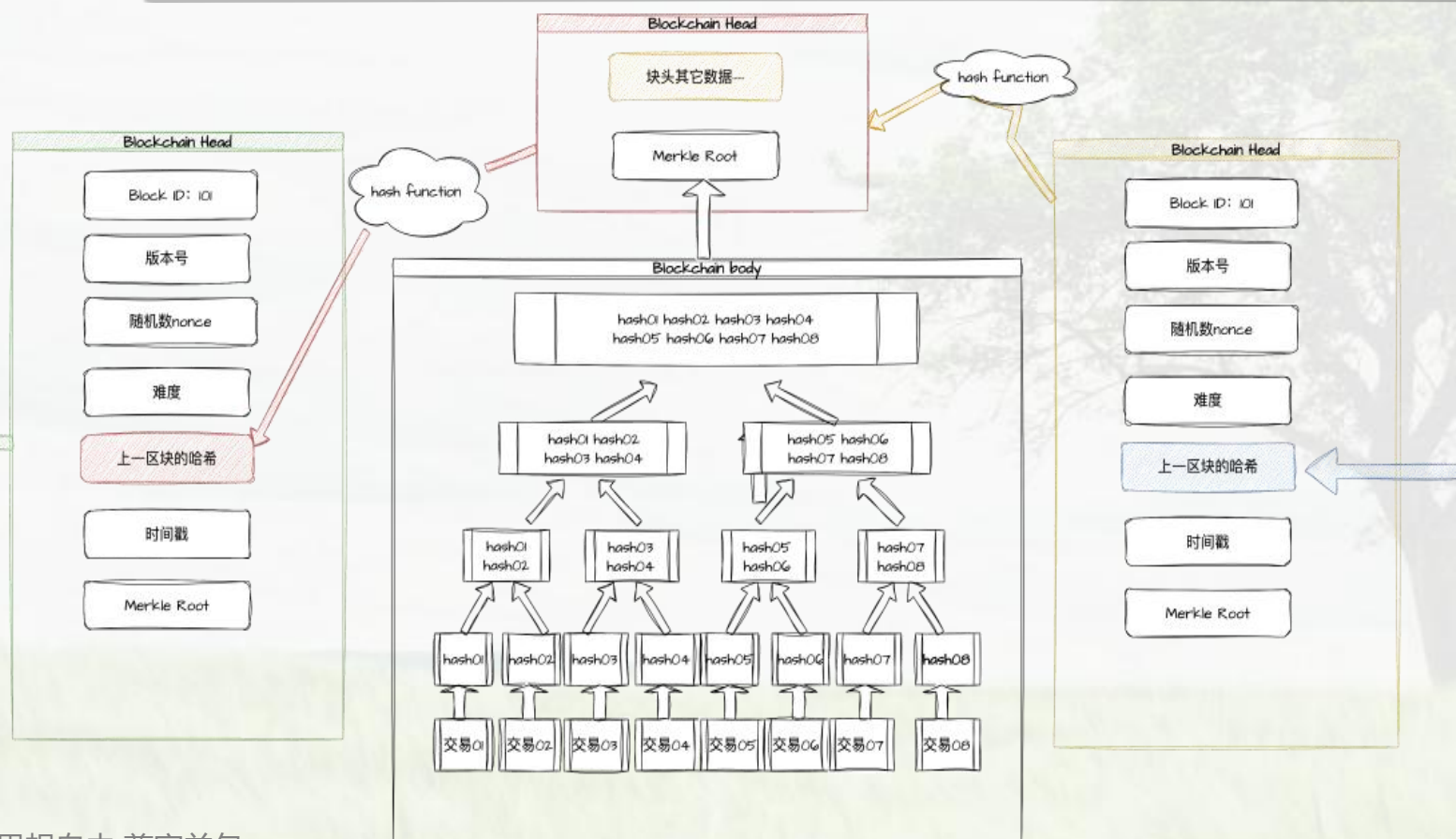


数据完整性保护

链式结构可以提供较好的数据真实性和完整性保证，在原来的平板结构下数据的真实性和完整性需要其上的应用来保证，数据库本身并不提供，区块链借助于链式结构可以在系统层面提供数据真实性和完整性保证，应用开发简单。

4.4 区块结构

区块由区块头和区块主体构成，区块头负责实现区块链的基本功能，区块主体包含了交易信息。区块间为链式存储，每个区块都包含前一个区块的哈希值，相当于把上一区块的指纹放在下一区块里，彼此串在一起。



可想而知，一旦有人篡改某个交易信息，所有的区块都需要进行修改，否则哈希验证无法通过，节点数据就出现问题。此外，如果哈希算得很快，那么节点可以推倒重新算一遍。反之如果算哈希需要几十分钟的时间，那么想要修改数据可谓难比登天。这里的时间就是难度，是后面会讨论的问题。

4.4 区块结构

大小	字段	描述
4字节	版本	版本号，用于跟踪软件/协议的更新
32字节	父区块哈希值	引用区块链中父区块的哈希值
32字节	Merkle根	该区块中交易的Merkle树根的哈希值
4字节	时间戳	该区块产生的近似时间
4字节	难度目标	该区块工作量证明算法的难度目标
4字节	Nonce	用于工作量证明算法的计数器

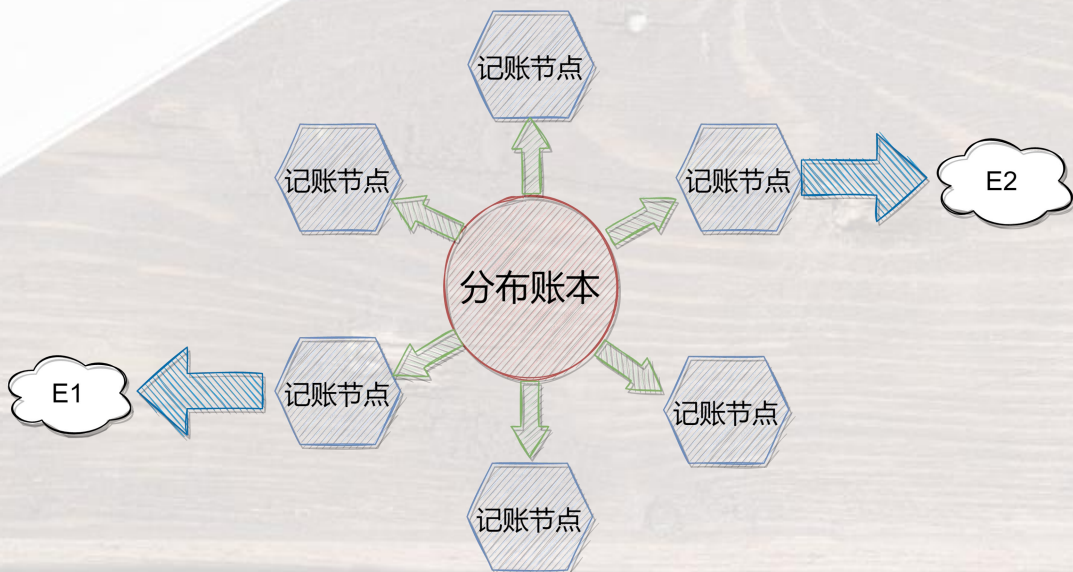
4.5 分布账本

我们通过前面的介绍知道区块链是一种分布式账本，和分布式账本对应的是中心化账本，也就是交易记录存在一个中心化的系统中，如图上方所示，实体E1和实体E2发生一次交易，如果是中心化账本，就是有一个集中账本来记录E1和E2的交易。中心化账本存在单点失败和中心作恶问题：



· 单点失败问题

因为所有交易都存储在中心化系统中，一旦系统被攻击，系统就面临单点失败问题，抗毁性非常差。同时数据仅有一个备份，一旦丢失无法恢复。

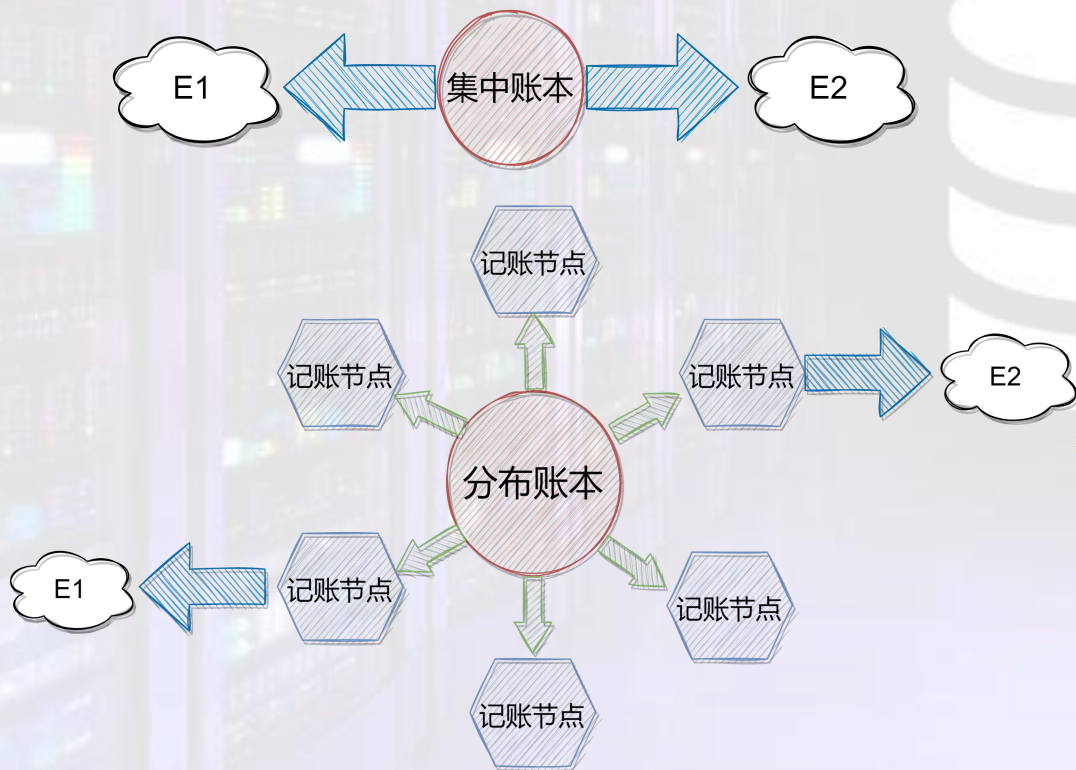


· 中心作恶问题

所有交易信息都被中心账本存储，中心账本拥有较大的权限，如果中心作恶将使得系统无法正常运行，运行中心账本的实体有可能通过作恶来为自己提供收益。

4.5 分布账本

和中心账本相对应，分布式账本可以较好的解决单点失败和中心作恶问题，如图下方所示，如果是8个记账节点组成的分布账本，首先因为所有交易数据都存储在8个节点上，就算单个节点出现问题，还有剩余7个节点，并不影响系统的运行，更严重一些，就算一般节点出现问题，剩余的节点依然可以提供服务。分布账本依靠数据复制解决了单点失败和中心作恶，但是数据复制带来了数据一致性和代价效率问题。



· 数据一致性问题

因为所有节点需要存储所有交易数据，任意时刻每个节点的数据一般情况下是不一致的，因为交易产生会首先被一个节点发现，然后传播给其余节点，这个时刻该交易仅存在该节点上，其余节点没有，这就造成了数据一致性问题，一般来说区块链中只有经过一顿时间的交易数据才能一致。

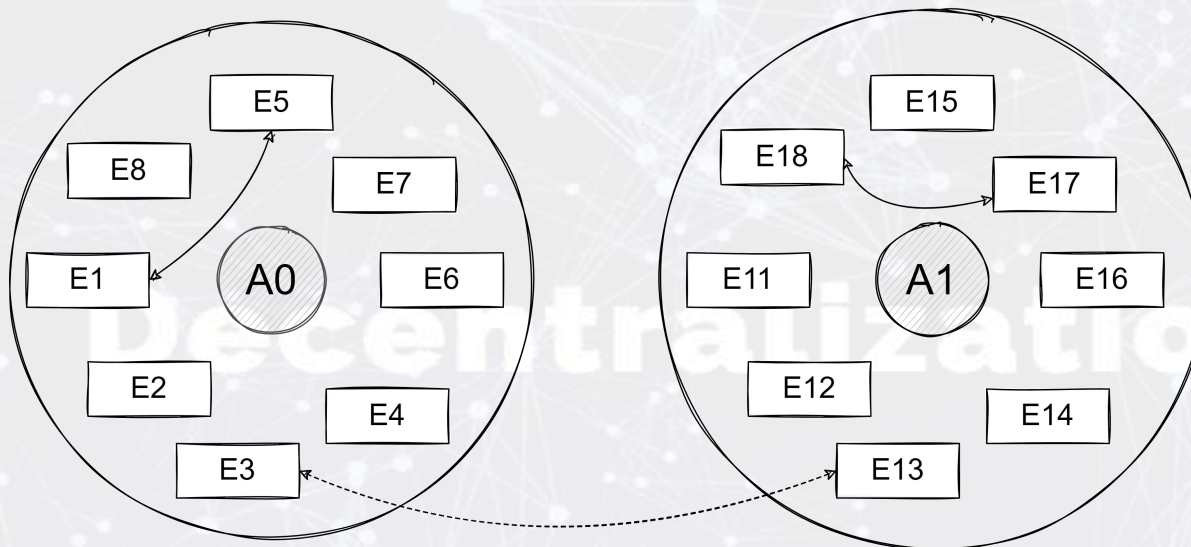


· 代价效率问题

中心账本仅需一份数据存储，分布账本需要多份数据存储，还需处理数据在不同节点的传输，还需要运行共识协议来解决错误节点和恶意节点。所以分布账本需要付出存储、计算和通信成本，代价比中心账本高。数据复制同步和共识通信都需要付出额外的工作，效率也比较低，一般说来分布账本要比中心账本的效率低。

4.6 为什么去中心化?

中心账本具有更好的效率，但是存在单点失败问题和中心作恶问题，单独采用链式结构不使用分布账本是否可以取得更好的效果呢？



答案是否定的。采用链式结构的中心账本和单纯的中心账本比，具有更好的数据的完整性和真实性，但是依然不能防止中心作恶，中心是没办法篡改数据了，但是可以有选择性的区分节点，可以威胁节点。

4.7 区块链历史

从区块链 1.0 到区块链 3.0



区块链 1.0 时代见证了整个去中心化概念的迭代，它集中体现在加密货币的演进上。

区块链的最初出现始于比特币（BTC）的诞生和发展。

区块链 1.0 技术包括用于加密货币的区块链核心、钱包软件、采矿设备和采矿软件等组件。

区块链 1.0 可以定义为第一代区块链技术，其主要聚焦于去中心化和加密货币。



Smart contracts

— Simply explained —

区块链 2.0 是以以太坊（ETH）为代表的区块链 1.0 的升级版。

区块链 2.0 主要体现在在以太坊的崛起和智能合约的整合上。以太坊是为了构建去中心化应用而建立的。区块链 2.0 以它为中心。它为开发人员以开源和无需许可的方式将智能合约部署到以太坊区块链，提供了更宽的道路。

区块链 2.0 可以定义为专注于智能合约的第二代区块链技术。



BLOCKCHAIN
SOCIETY

区块链 3.0 的潜力集中在为加密货币之外的服务和行业提供解决方案。

随着区块链技术的不断发展，将其集成到供应链、网络安全、投票、医疗保健、Web 服务、物联网等领域已成趋势。

区块链 3.0 是区块链 2.0 的升级版本，旨在通过使用去中心化应用程序提高技术能力。它专注于解决区块链技术存在的问题，同时促进更快、更具成本效益和高效地交易。

4.8 区块链未来

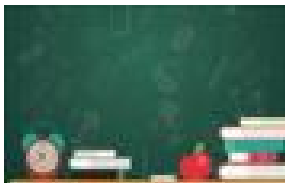
支付、交易清结算、贸易金融、数字货币、股权、私募、债券、金融衍生品、众筹、信贷、风控、征信。



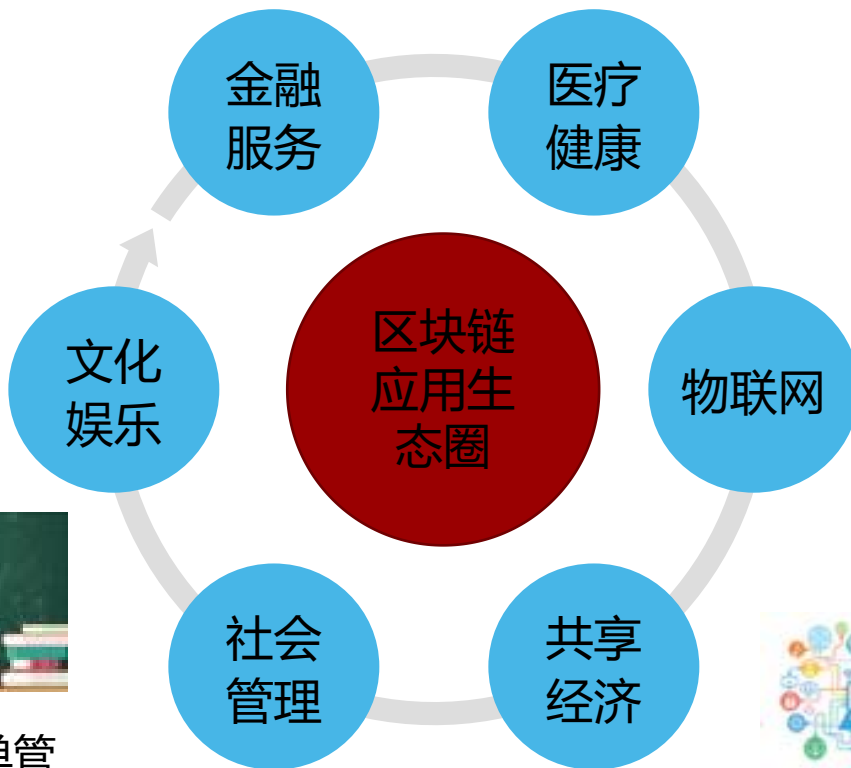
数字病历、隐私保护、健康管理。



视频版权、音乐版权、软件防伪、数字内容确权、软件传播溯源。



代理投票、身份认证、档单管理、公证、遗产继承、个人社会信用、工商管理。



物品溯源、物品防伪、物品认证、网络安全性、网络效率、网络可靠性。



租房、租车、知识技能。

第五节

区块链现状

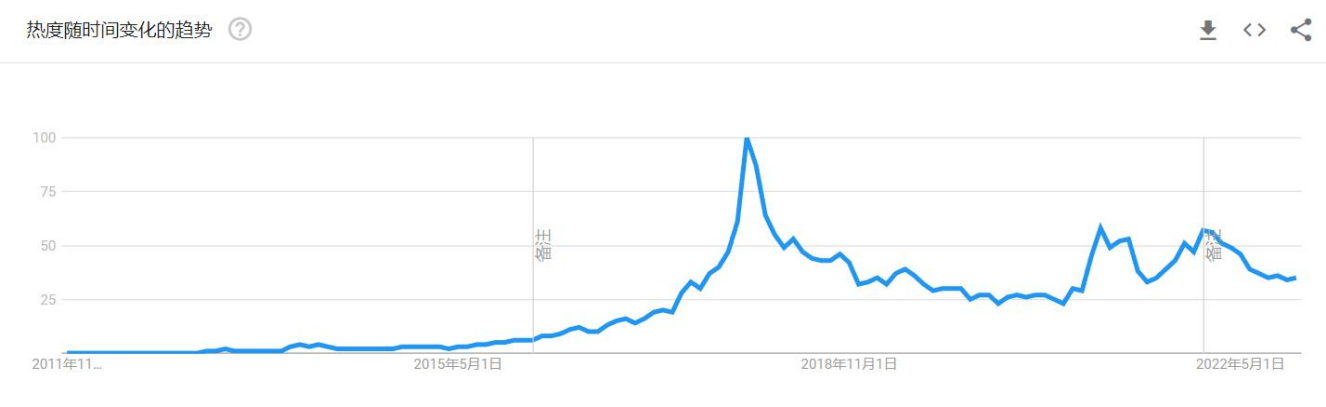
01 发展态势

02 各国战略

03 我国政策



5.1 发展态势

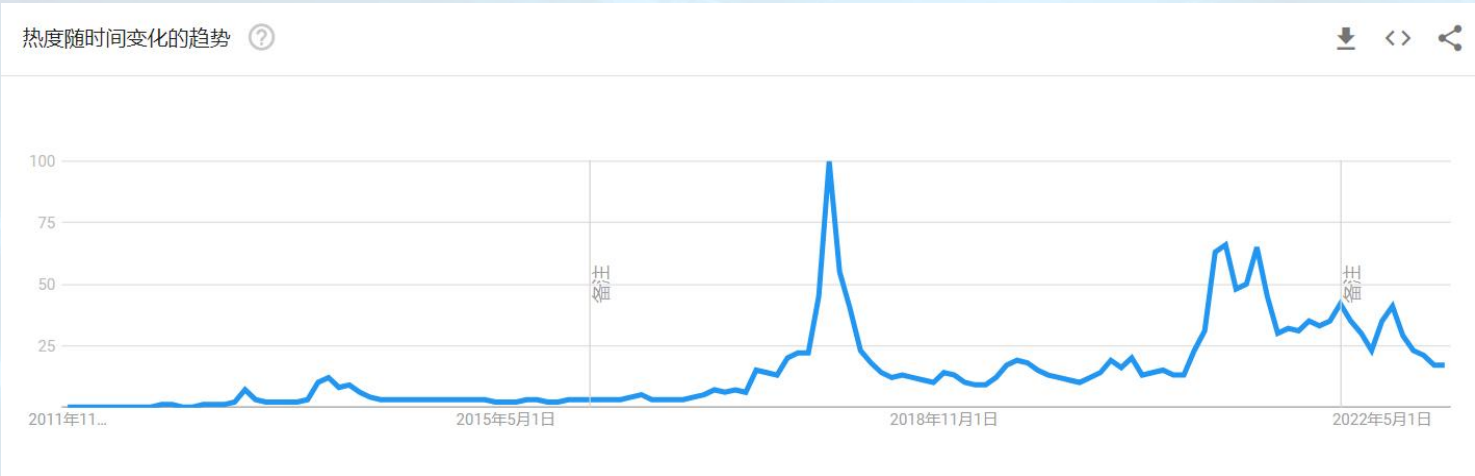


" blockchain " 在Google的搜索热度变化

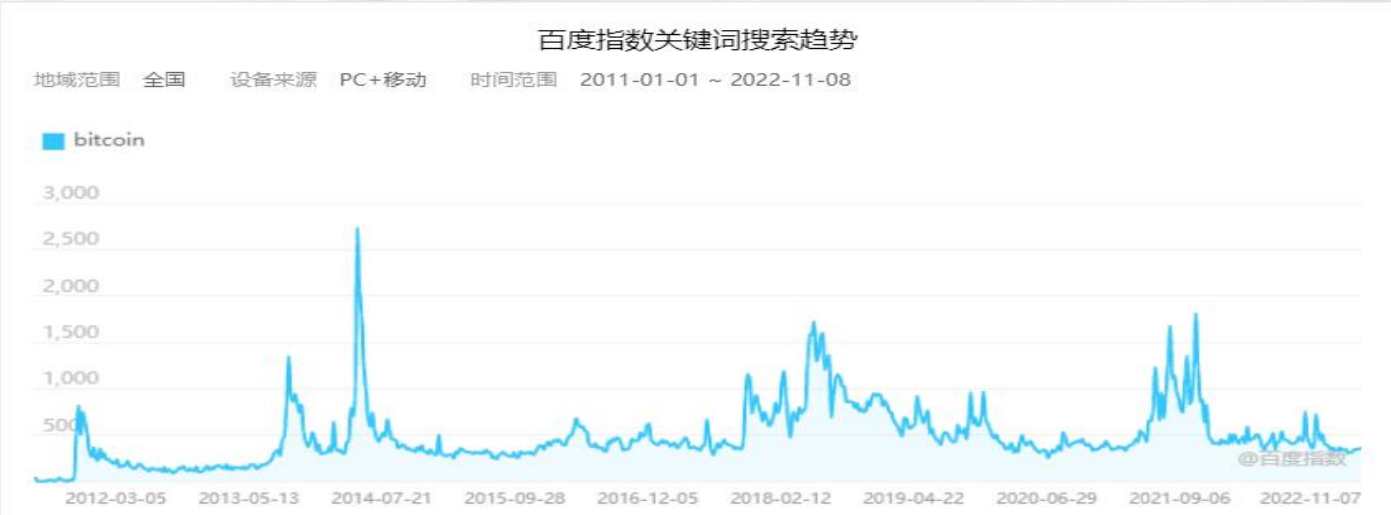


" blockchain " 在百度的搜索热度变化

5.1 发展态势



" Bitcoin " 在Google的搜索热度变化



" bitcoin " 在百度的搜索热度变化

5.1 发展态势



Policy

2021年3月11日第十三届全国人大四次会议表决通过《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》。十四五期间要打造数字经济新优势，加快推动数字产业化，推动产业数字化转型，提出“培育壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业”。提出“推动智能合约、共识算法、加密算法、分布式系统等区块链技术创新，以联盟链为重点发展区块链服务平台和金融科技、供应链管理、政务服务等领域应用方案，完善监管机制。”



区块链成为数字经济重点产业

5.1 发展态势

区块链成为国家战略



Policy

2021年是“十四五”的第一年，产业区块链写入国家十四五规划，表明产业区块链成为了国家战略，在该规划指引下，2021年度国家和各省市出台了上千份政策文件鼓励支持产业区块链的研发和应用。

2021年6月，工信部和网信办联合发布《关于加快推动区块链技术应用和产业发展的指导意见》，明确指出到2025年，区块链产业综合实力达到世界先进水平。



产业区块链的应用挑战

产业区块链的技术挑战



核心技术原创不足

区块链的核心技术包括密码算法、分布式算法、网络路由算法、共识算法、性能扩展机制、智能合约技术、激励机制、跨链技术等，在这些核心技术方面国内发表在高等级会议和期刊上的相关论文大幅增加，但和我国产业区块链规模相比还很不匹配，特别缺少有影响力的技术和在产业的应用。



自主底层平台薄弱

国内产业区块链和国外区块链相比有自己的特殊性，平台主要以联盟链为主，当前超级账本和以太坊依然是国内产业区块链主要的技术平台，国内虽然产生了很多联盟链技术平台，但与超级账本和以太坊在规模和范围上相比还有较大差距，需要在智能合约语言、区块链开发工具、区块链安全、分布式计算和存储等领域进一步加强自主的区块链底层平台与工具。



应用技术研究缺失

产业区块链关注区块链和实体产业的融合，当前区块链在很多领域的应用处于初始阶段，基本上采用通用的区块链平台和技术，但每个领域均有自己特定的需求，需要针对不同领域的不同要求定制不同的区块链技术。同时需要研究区块链如何和大数据、云计算、物联网、人工智能等新技术有机融合，也需要研究区块链如何和操作系统、数据库、信息安全等传统技术相结合。

产业区块链的应用挑战

产业区块链的应用挑战



应用领域和范围规模有待突破

产业区块链已经应用到了很多行业和领域，但是大多数应用的规模都较小，体现为：用户数量少、服务节点少、覆盖范围小，业务比较单一、业务量较低等。同时大量传统的行业和领域还没有应用区块链，如何在这些行业应用区块链有待突破，可以大规模商业应用的案例还不足。当前已有的区块链应用之间互联互通也存在较大问题，不同部门机构之间不同的区块链应用如何跨链也亟待解决。



产业区块链技术应用人才匮乏

区块链涉及密码、计算机、分布式、经济等多个学科，因为人才培养的滞后性，区块链技术开发和应用人员奇缺，远远不能满足产业的需要。产业区块链发展迅速，即懂区块链技术又懂特定行业的人才更是难寻。



商业模式和发展路线不够清晰

受国家政策影响，各部委各省市均出台了区块链相关的鼓励和扶植政策，区块链成为了包办百病的良药，产生了不少为了用链而建设的区块链应用，哪些场景适用区块链在商业模式上还不够清晰。同时一些地方没有充分的考虑自身基础和条件，投入大量资源重复建设了一些价值不大的平台和应用，反而阻碍了产业区块链的发展。

Weeklys[®]
Challenge

5.1 发展态势

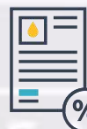
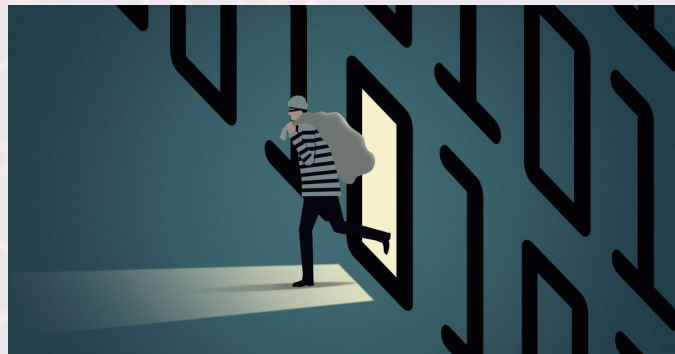
产业区块链的应用挑战

产业区块链的监管挑战



区块链领域相关犯罪频发

，随着区块链特别是数字加密货币和数字资产的快速发展，和区块链相关的洗钱、逃税、赌博、诈骗、传销等犯罪案件频发，2021年公安机关破获相关案件259起，收缴虚拟货币110亿余元。



监管政策制度有待健全

区块链具有分布、去中心、用户匿名和数据不可修改等特性，这些特性使得当前的监管政策制度的执行面临困难，用户和行为的追踪审计、数据和合约的有效合规安全等监管要求难于实现。

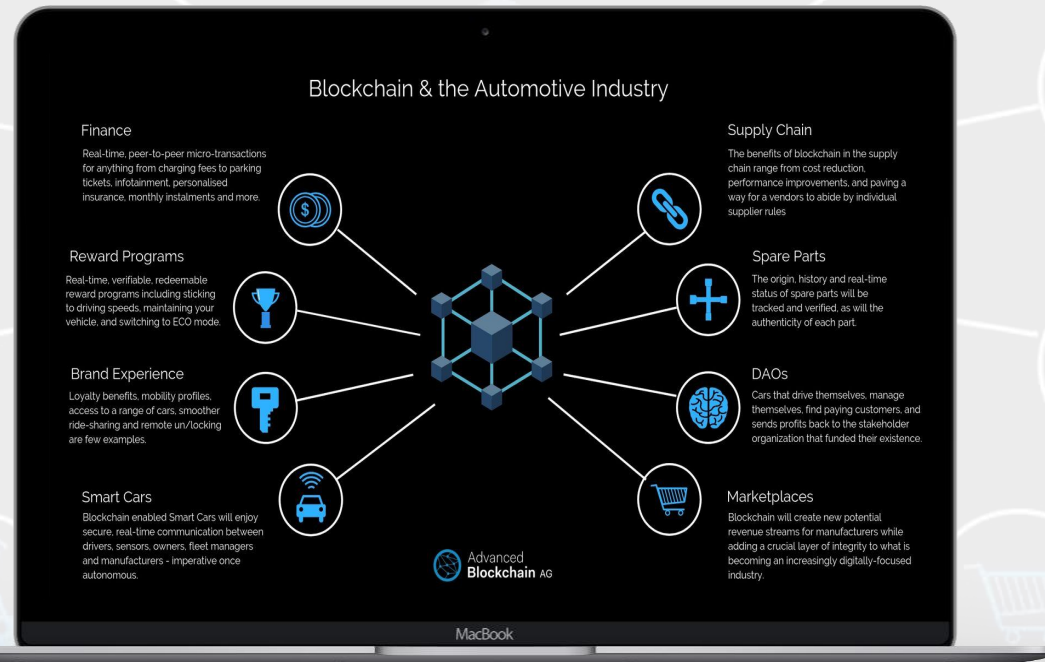
5.1 发展态势

Blockchain & the Automotive Industry

产业区块链深度融合各领域

区块链和产业持续融通

2021年区块链和各产业进一步相互融合发展，在防伪溯源、数据共享、供应链管理、存证取证、城市治理、智慧城市、政务服务等领域持续发展，隐私保护、碳达峰碳中和、元宇宙、数字藏品NFT等领域是2021年产业区块链的热点，2021年也是数字人民币应用推广、用户普及和应用拓展的一年，累积开设钱包过亿，交易金额超过500亿，应用场景超过300万。



区块链创新应用试点启动

2022年初网信办等18个部委发布了《关于国家区块链创新应用试点入选名单的公示》，共发布了15个综合试点164个特色领域试点，涵盖区块链+制造、区块链+能源、区块链+法制、区块链+税费服务、区块链+审批、区块链+检察、区块链+版权、区块链+民政、区块链+人社、区块链+教育、区块链+贸易金融、区块链+风控管理、区块链+股权市场、区块链+跨境金融等领域。要求在2023年年底形成一批区块链创新应用典型案例和推广经验，推动数字中国和数字化经济建设。

5.2 各国战略

美国区块链战略

美国是区块链产业的引领者，比特币、以太坊等主流的区块链平台大多都产生于美国，美国在信息技术和金融方面拥有全球近半数的科研机构、研发人员和产业集群，是区块链相关技术的主要输出者，同时也是区块链产业的主要目标市场，2019年区块链相关融资占全球的39%，区块链相关的论文发表和专利申请多年排名第一。

政府积极支持

美国政府积极支持区块链技术，关注区块链对于美国政治、经济和社会的潜在影响，从国会、联邦各部门到各州都积极参与了区块链的调研论证，并积极推动区块链技术研发、应用创新和产业布局

企业推动

企业和产业联盟是美国区块链产业发展的最主要的推动者。2019年2月摩根大通发布了用于跨境实时支付的数字稳定币，发布后170多个国家银行有意参与。2019年6月Facebook牵头发布了Libra项目，希望建立可以为数十亿人服务无国界金融基础服务，一经宣布得到了全球各界的广泛关注和讨论。

协作监管

美国政府一方面认可区块链的应用潜能，另一方面提出应该密切关注该技术对监管带来的挑战，确保收益和风险的平衡。区块链监管由联邦多个机构和各州政府互相协作，在各自职权范围内执行相应的监管机制和政策，重点关注虚拟货币行业和区块链在金融领域的应用。

高校普及

区块链涉及计算机、信息安全、金融、经济、法律等多个领域，进入门槛较高，麻省理工学院、普林斯顿、伯克利等美国知名高校自2015年开始陆续开设了区块链相关的课程，极大推动了区块链知识的普及。

5.2 各国战略

英国区块链战略

英国高等教育和研究机构众多，也是欧洲计算机研发的中心，在商业、金融和法律方面享有全球影响力，拥有较为成熟的区块链社区，是区块链潜在的领导者，区块链初创企业数量全球第二，区块链企业活跃于各个领域，包括银行、保险、教育、娱乐、体育、健康等。

政府推动

2016年英国科技部发布《分布式账本技术：超越区块链》白皮书，肯定了区块链的价值。2017年发布的数字策略中提到要开展区块链项目试点，通过创新英国投入1000万欧元用于区块链验证项目，将区块链纳入2000万欧元的政府科技分析基金支持。2018年，英国财政部、金融行为监管局和英格兰银行共同组建“加密资产专项工作组”。2020年英国央行发布《央行数字货币：机遇、挑战与设计》，明确对央行数字货币持开放态度。

综合监管

英国金融行为监管局FCA明确应该为区块链设立一个监管框架，并综合考虑融合传统的制度监管和新出现的技术监管和监管科技。目的是降低金融风险、保护消费者、保护和维护英国金融服务的一致性和完整性、促进金融服务竞争的有效性。2014年宣布加密资产交换适用反洗钱监管，2018年发布了一系列关于区块链的监管措施，2019发布了《加密货币资产指南》，明确规定了加密资产的类型、属性、使用范围等，拟定了针对加密货币市场的监管框架。

德国区块链战略

德国是第一个承认加密货币的国家，对区块链技术的应用一直持较为开放的态度，是欧洲区块链产业的先行者，2019年德国经济与能源部和财政部联合发布《德国国家区块链战略》，为德国制定了全面的区块链发展战略，提出了德国区块链的发展目标、遵循原则和相关行动计划。德国政府认为区块链技术是未来互联网的核心，可以为产业和社会的数字化转型提供支持。

金融管理

- 在金融领域保障稳定并推动创新，开放电子证券乃至区块链上发行证券的立法，并制定加密货币的监管要求

技术应用

- 推进区块链试点项目和监管沙盒以促进区块链技术从创新走向成熟，支持面向实践的能源区块链的研发和应用示范，

制度监管

- 建立清晰可靠的投资安全保障，包括涉及区块链的证明提供、艺术品、公司法、分布式协作、国际仲裁等方面的法律法规框架，

公共管理

- 应用区块链到数字化公共管理服务中，推动个人数字身份体系的建立和电子信任管理服务的建设，

促进交流

- 扩大信息和知识传播、互联和合作，将开展一系列区块链相关的技术对话促进信息交流和数据共享，并推动区块链方面的教育培训和产学研合作。

5.3 我国政策

2019年10月24日下午，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习。中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。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。

习近平在主持学习时发表了讲话。他指出，区块链技术应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域。目前，全球主要国家都在加快布局区块链技术发展。我国在区块链领域拥有良好基础，要加快推动区块链技术和产业创新发展，积极推进区块链和经济社会融合发展。



5.3 我国政策

据中国物流与采购联合会区块链应用分会与产业区块链研究院不完全统计，2021年国家部委和地方发布的和区块链相关的政策超过1000项，区块链政策对我国产业区块链的发展有着重要的导向作用，2021年十四五规划确定区块链为国家战略，各级政府对产业区块链日益重视，区块链相关政策增长迅速，大大超过了2019年和2020年。



5.3 我国政策

2021年国务院发布产业区块链相关政策16项，具体名称和重点内容见表3-1。其中《“十四五”规划与2035 年经济远景目标纲要》是2021年产业区块链最有影响力的政策，明确了区块链是十四五数字经济重点产业之一，表明了产业区块链是国家发展战略。

序号	时间	名称	重点
1	1月31日	《建设高标准市场体系行动方案》	推动区块链等新技术基础设施建设
2	2月10日	《防范和处置非法集资条例》	讲虚拟货币纳入非法集资调查认定范围
3	3月3日	《〈优化营商环境条例〉实施情况 第三方评估发现的部分创新举措》	运用区块链技术构建公共资源交易平台
4	3月13日	《“十四五”规划与2035 年经 济远景目标纲要》	推动区块链创新、发展区块链服务平台和领域 应用方案，推进数字货币研发
5	6月25日	《全民科学素质行动规划纲要 (2021—2035年)》	推进科普与区块链等技术深度融合
6	10月10日	《国家标准化发展纲要》	加强区块链技术标准研究



本章从区块链的发展历史展开

第一节从信息存储，记账科技，货币三个维度的历史展开，引出了区块链产生的原因。

第二节从万恶的美国政府抢夺人民黄金开始，引出社会对于加密货币的需求。然后，沿着密码学的发展历史，引出密码朋克组织的成立，以及密码朋克组织成员创造的比特币之前的加密货币：E-Cash、HashCash、B-money、bitgold。最后，从比特币的诞生，引出加密货币的意义——文明，取决于在人类合作中不断扩展的秩序。

第三节从比特币引出区块链，介绍了区块链的定义和特性，并介绍了公有链、私有链和联盟链的特性。

第四节介绍了区块链的原理，从交易示例出发，介绍了区块链的哈希指针，链式结构，区块结构，回答了为什么要去中心化的问题。

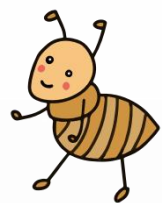
第五节介绍了区块链的现状，美国，英国，德国的区块链政策以及我国的政策，对区块链的未来进行了展望。

感谢您的观看，祝您学习进步，课程满分！~~~





北京大学
PEKING UNIVERSITY



感谢观看

