第1篇：区块链技术指南

第1章

重新认识区块链

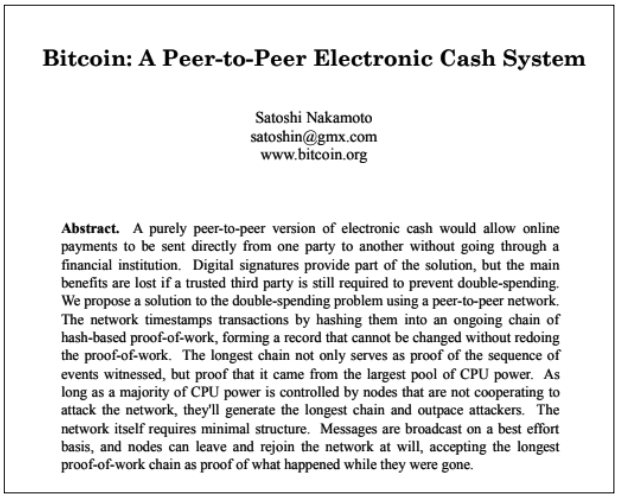
当你看不懂区块链技术的发展时，就看看区块链的历史吧！因为历史或许会给你答案。当你搞不懂区块链的时候，或许是区块链的光环蒙蔽了你的双眼。其实它并不神秘，你需要给自己一个重新认识它的机会。

1.1 以史为鉴，才能在区块链的世界中走得更远

通过比特币的发展历程，你需要掌握一个非常重要的思维方式，一方面我们要学会拥抱变化，但同时也要清醒地知道任何一项新技术的发展都没有想象的那么容易，它需要经历很长时间的发展才能产生真正的价值。

1.1.1 比特币的发展历程

2008 年 11 月 1 日，一个化名为中本聪（Satoshi Nakamoto）的密码极客发表了比特币白皮书——《比特币：一种点对点的电子现金系统》（图 1–1），至此，比特币展开了一次人类历史上伟大的数字货币实验。



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.

图 1-1 比特币：一种点对点的电子现金系统

去中心化的数字货币概念，早在几十年以前就已经被提出来。在比特币之前，数字货币经过了几代的演变，这期间包括 ECash、

Hashcash、B-money 等上百种数字货币，但只有中心化的 Paypal（一个总部位于美国加利福尼亚州圣荷西市的互联网第三方支付服务商）和去中心化的比特币走到了今天。下面我们通过几个典型的数字货币案例来揭开比特币的神秘面纱，也让我们对比特币技术的发展有一个更清晰的认识。

1983 年，大卫·乔姆（David Chaum）提出的 ECash 是第一个真正意义上的数字化支付系统，也是第一个应用加密技术的数字货币项目，后来美国和芬兰的几家银行都使用了这个系统。但由于没有说服更多的银行和商家使用，同时由于这种数字货币系统只支持用户和商家之间的交易，不支持用户与用户之间的交易，以致最终项目失败。

1997 年，亚当·贝克（Adam Back）提出了一个 Hashcash 体系，通过计算数学难题来防止用户发送垃圾邮件。由于这个算法需要付出一定的工作量和成本（计算数学难题需要耗费时间，并消耗一定的电力），这就可以给数字货币赋予商品属性，并可以有效控制货币通胀，之后被数字货币广泛使用。

比特币的工作量证明机制（Proof of Work，PoW）与 Hashcash 比较类似，并在此基础上做了大量的改进。

1998 年，戴维（Wei Dai）提出的 B-money 是首个去中心化的数字货币系统，在其设计中融合了数学计算和可信时间戳（timestamp）（用数学算法控制新币的产生，用可信时间戳记录交易信息和防止双重支付（double spending）），遗憾的是，他没有提出具体的实现方法。

2005 年，尼克·萨博（Nick Szabo）也提出了一个类似于 B-money 的方案，称为比特黄金（BitGold）。

2005 年，哈尔·芬尼（Hal Finney）引入了“可重复使用的工作量证明机制”（reusable proofs of work），同时使用 B-money 的思想和 Adam Back 的计算哈希现金（Hashcash）难题来创造加密货币。但是，这种概念再次迷失于理想化，因为它依赖于可信计算作为后端（依赖于可信计算提供的共识机制需要可信硬件的支撑才可以发展起来）。

直到 2009 年 1 月比特币横空出世，才真正实现了去中心化的、账务公开的数字货币系统，正式开启了区块链技术的发展历程。

在比特币系统中，中本聪对之前的数字货币做了大量改进并真正意义上实现了它。

在“比特币白皮书”中，中本聪使用了大量篇幅来描述防止双重支付（double spending）的原理，这是价值传递和互联网信息传递的根本区别。

信息传递可以重复流通，但价值传递却要保持唯一性。同一个信息可以让很多人阅读，这也是为什么知识付费时代成就了很多大 IP 的原因。即使阅读一篇文章的价格很低，但其拥有庞大的用户群，因此收益也非常高。但价值传递却恰恰相反，我的一元钱给了你，就不能再给别人了。生活中使用实物（例如纸币）交割很容易解决双重支付的问题，一旦价值数字化后，由于信息很容易复制，同一笔数字资产有可能被重复使用。在比特币中，每笔经过验证的交易都会加盖时间戳（一笔交易发生的时间），所有交易按照时间顺序存储在账本中。由于每笔交易都有一个唯一的可信时间，这样就杜绝了一笔交易同时发生的可能性，也就解决了价值传递的唯一性问题。

在比特币体系中，解决数学难题并不产生货币，只是用来保证区块链的安全，时间戳用来保存区块和交易的先后顺序。比特币从根本上融合了用数学计算来控制新币的产生和用安全的时间戳来记录信息，防止双重支付（double spending）的发生。

1.1.2 区块链的发展历程

很多人分不清比特币与区块链，以为比特币就是区块链，区块链就是比特币，其实比特币只是第一个成功的区块链应用。你可以将区块链理解为智能手机，而比特币仅是智能手机上的一个应用软件而已。随着比特币价格的不断飙升，十年内价格上涨了几万倍，比特币背后的区块链技术逐渐进入了大众视野。比特币价格（2013 年 4 月 29 日 –2018 年 12 月 2 日）的变化曲线如图 1–2 所示。

关于区块链概念最早的研究要追溯到 1991 年，斯图亚特·哈伯 (Stuart Haber) 和斯科特·斯托内塔 (W. Scott Stornetta) 使用区块链实现了一个不可篡改的文档时间戳系统。哈伯和斯托内塔在设计中加入了默克尔树的概念（Merkle trees），将多个文档收集在一个区块中，从而提升了系统效率。

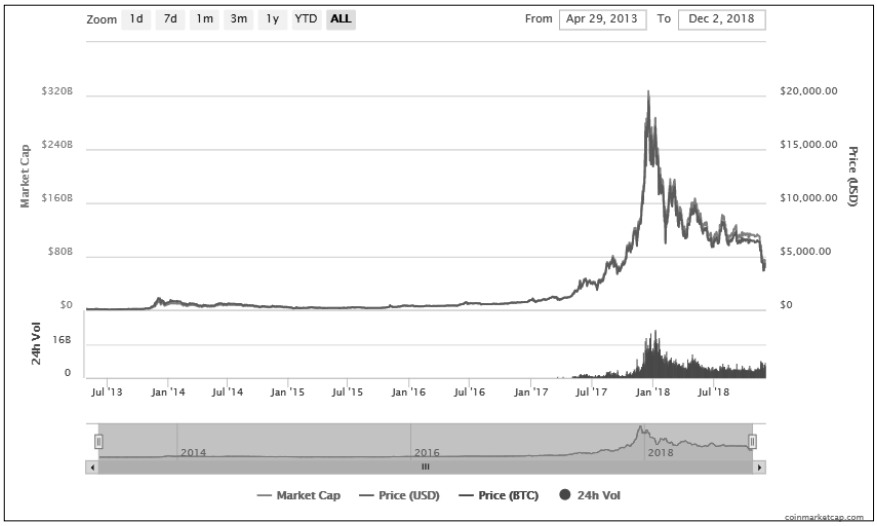


图 1-2　比特币的价格曲线（2013 年 4 月 29 日—2018 年 12 月 2 日）

（数据来源于 coinmarketcap.com）

由于比特币受到更多人的关注，因此，大家公认的第一个区块链是中本聪发明的比特币。通常大家将区块链技术的发展划分为 3 个阶段，分别是比特币时代的区块链 1.0 时代，以太坊时代的区块链 2.0 时代和以 EOS 为代表的区块链 3.0 时代。区块链演进路线图如图 1–3 所示。

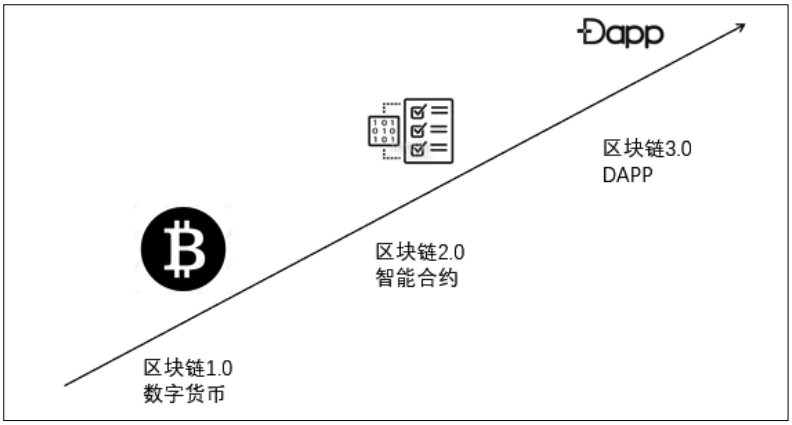


图 1-3　区块链演进路线图

比特币开启了数字货币时代，解决了货币和支付手段的去中心化，被称为区块链 1.0 时代。在没有中心化机构的情况下，比特币实现了一

个面向全球、账务公开的数字货币网络系统。在过去 10 年中，账本已经从当初的几十吉比特达到了现在的上百吉比特（计算机中表示容量的单位，也就是 GB）。

就像互联网早期的 TCP/IP 协议【由 TCP（传输控制协议）和 IP（网络协议）组成的网络通信模型】一样，只能简单地进行计算机之间的通信，但随着技术的不断发展，基于 TCP/IP 协议发展起来的 HTTP（超文本传输协议）协议成了浏览器现在使用的标准协议。之后，随着 HTTP 协议的发展，像域名系统（Domain Name System，DNS）、电子邮件、搜索引擎、网页和其他互联网服务（SaaS、PaaS、IaaS）技术都是在这个网络模型基础上发展出来的产品，TCP/IP 协议将人类带入到了互联网时代。

与基于 TCP/IP 协议的互联网革命一样，比特币底层的区块链技术也会像互联网技术一样发展，成为一种新的技术协议，最终重构互联网。与 TCP/IP 协议不同的是，TCP/IP 是一个信息传输协议，而区块链是一个价值交换（Value-Exchange ）协议。

在比特币之后，市场上出现了各种各样的基于比特币底层的区块链技术加密的数字货币，例如，域名币、彩色币、元币、狗狗币、莱特币等。

由于比特币是一种脚本语言，普通程序员无法进行编程，要开发一个区块链应用难度非常大。随着各种竞争币的相继出现，人们发现比特币背后的区块链技术可以为智能合约提供可信执行环境。

智能合约是在 20 世纪 90 年代由尼克·萨博（Nick Szabo）提出的理念，几乎与互联网同龄。由于缺少可信的执行环境，智能合约并没有被应用到实际产业中。以太坊创始人 V 神（Vitalik Buterin），一个 1994 年出生的俄罗斯小伙，对比特币、竞争币的概念进行整合和提高，发布了白皮书《以太坊：下一代智能合约和去中心化应用平台》，并一直致力于将以太坊打造成最佳智能合约平台。至此，区块链进入到了 2.0 时代。一个形象的说法就是，以太坊将区块链从功能机时代进化到了智能机时代，用户通过以太坊可以方便地开发自己的去中心化应用（Decentralized APPlication，DAPP）。

以太坊通过建立抽象的基础层，内置有图灵完备的编程语言，使

任何人都可以创建智能合约和去中心化应用。类似域名币的主体框架只需要两行代码就可以实现，诸如货币和信誉系统等其他协议，也只需要不到 20 行代码就可以实现。智能合约不仅可以创建一些满足条件的合约，还可以开发一些功能非常强大的去中心化应用。但由于以太坊是基于比特币架构实现的，在实际应用过程中存在效率低下、手续费高等问题，所以，目前主要的用途是用去中心化的方式来注册、确认、转移各种不同类型的资产和合约。所有的金融交易，包括股票、私募股权、众筹、债券等都可以被改造，并在链上使用。

为了解决区块链的效率和收费等问题，以 EOS 为代表的公有链提出了超越货币、经济和市场的去中心化应用，即区块链 3.0 时代。联盟链方面，以 Fabric 为代表的超级账本（Hyperledger）发展得也非常迅速。随着区块链技术的不断发展和演进，区块链在金融、供应链、数字版权、公共事务、共享经济等方面的应用已经正式拉开了帷幕。

1.1.3 中本聪：神秘的比特币创始人

中本聪的英文名是 Satoshi Nakamoto，自称是日裔美国人，是比特币的创造者。图 1–4 是网络上流传的中本聪的照片。

图 1-4 网络上流传的中本聪的照片

中本聪在 2007 年 5 月开始编写“比特币”，2008 年 5 月注册 bitcoin.org 域名，2008 年 10 月公开发表白皮书，2009 年 1 月 3 日“挖”出了创世区块（在区块链中将第一个区块称为创世区块），得到了 50 个比特币的奖励，他在创世区块中写上了这样一句话：

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

这句话来源于当时的英国财政大臣正在考虑实施的第二次财政救援计划，而这条消息当时就刊登在英国的《泰晤士报》上（图 1–5）。

图 1-5 《泰晤士报》（*The Times*）

随后的两年时间，中本聪与许多人进行邮件交流，并回答人们关心的问题。这两年期间，中本聪对比特币代码进行了多次修改，于 2010

年 11 月将比特币项目交接给了核心社区成员，而他却不再出现。但在 2018 年 11 月 29 日，P2P 基金会（p2p foundation）网站上一个与中本聪有关联的账户更新了自己的状态，发布了一个单词——nour，这个单词在阿拉伯语中是光的意义，这也引发了比特币追随者的各种猜想。图 1–6 是中本聪（Satoshi Nakamoto）在 P2P 基金会网站上的主页。

图 1-6　中本聪（Satoshi Nakamoto）的主页

从发表比特币论文以来，中本聪的身份一直是一个谜。P2P 基金会网站的个人资料中，中本聪自称是居住在日本的 37 岁男子。然而，这一点被广泛怀疑，他的英文书写如同母语般流利，却从未使用过日语。用他的名字在网上搜索，无法找到与他相关的任何信息。各种迹象表明，中本聪可能是一个虚构的身份，背后极有可能是一群人。

对于中本聪身份的猜测非常多，其中有人怀疑是美国中情局的一个特勤小组，也有人怀疑是日本数学家望月新一，但是后来的各种推测都被一一否认。发表自 2015 年 5 月的一篇文章中，尼克·萨博（Nick Szabo）在谈到比特币的发明人时提到，他所认识的人里面，对数字货币足够感兴趣，并且能付诸实施的，本来只有他自己、戴维和哈尔·芬尼三个人，后来中本聪出现了。

关于中本聪匿名的原因有很多，在中本聪活跃的“密码朋克”和“密码学”邮件组中，大家都普遍采用匿名的方式来发表文章。此外在中本聪公开发表比特币的时候，电子黄金（e–Gold）的创始人被指控洗钱并最终认罪，这也可能是他匿名的一个原因。另外，数字货币的一些技

术当时是受专利保护的，为了避免侵权，采用匿名的方式研发比特币也是一种可能的考虑。

中本聪在编写比特币代码的时候得到了很多人的帮助，这在比特币早期论坛中可以看到关于比特币的一些进展情况。这些文章中，中本聪将大卫·乔姆（David Chaum）等人提出的数字货币失败原因归结于中心化控制上，他发明的比特币是一个去中心化匿名的数字货币系统。中本聪在发明比特币的时候，不是先写理论再写代码，而是完成比特币代码的编写之后，才开始写白皮书。他在具体实现比特币的时候，大量参考了之前数字货币的设计方式，在早期比特币白皮书中引用了一些密码学、时间戳的论文，也引用了 Hashcash、B-Money、比特黄金（e-Gold）的成果。在比特币最初的定义中，他是这样描述的：

“比特币是 B-money 和比特黄金（e-Gold）的具体实现。”

1.1.4 V 神：以太坊创始人

维塔利克·布特林（Vitalik Buterin），1994 年 1 月 31 日出生，是一位出生于俄罗斯的加拿大籍程序员、作家、以太坊联合创始人，业内都称他为“V 神”。图 1-7 是以太坊创始人维塔利克·布特林。

图 1-7 以太坊创始人维塔利克·布特林

V 神出生于俄罗斯莫斯科一座叫科洛姆纳（Kolomna）的古老小镇，他在这里一直生活到了 6 岁，当时父母为了寻求更好的工作机会移居加拿大。他在加拿大上三年级的时候，被安排到天才儿童班，并开始对数学、编程和经济学产生了浓厚的兴趣。

后来，V 神上了一所位于多伦多的私立高中，在那里他对学习产生了极大的兴趣。他曾经说，高中生活是他生命中最有趣且成长最快的年代，那里学生与教师之间的联系非常紧密，通过高中的学习让他学会了如何思考、推理和学习。

V 神在 17 岁时从计算机科学家的父亲那里了解到了比特币，对于这种新鲜事物，他表现出了浓厚的兴趣。为了更好地理解比特币背后的技术，布特林开始学习比特币论坛中的技术资料并开始给博客写文章赚取比特币，虽然当时比特币缺乏主流关注，但布特林却意识到比特币背后的技术，并非限于加密货币，各行各业都适用。后来他还创建了比特币杂志（*Bitcoin Magazine*），被称为加密货币领域第一本严肃的出版物，随后被 BTC Media 收购。

18 岁的时候，他在国际奥林匹克数学竞赛中获得了铜牌。 19 岁的时候，他进入了滑铁卢大学。该大学在加拿大排名第三，并且是北美洲最优秀的学校之一，其数学、计算机科学和工程学的教学水平居世界前列。

2013 年年底，布特林在白皮书中首次描述了以太坊。他认为比特币需要一种脚本语言来开发应用程序，但没有达成一致，所以他提议使用一种更通用的语言开发去中心化应用。

2014 年 1 月 23 日，布特林在自己任编辑的比特币杂志上发表了《以太坊：一个下一代加密货币和去中心化应用平台》（Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform）（图 1-8）。

关于以太坊项目，布特林说：“我真的很感激有机会在一个有趣和跨学科的领域中工作，有机会与这些领域中突出的密码学家、数学家和经济学家互动和学习，帮助构建影响全世界数亿人的软件和工具”。

图 1-8　以太坊：一个下一代加密货币和去中心化应用平台

以太坊在设计之初就规划了 4 个阶段，分别是前沿（Frontier）、家园（Homestead）、大都会（Metropolis）和宁静（Serenity）。2015 年 7 月发布了以太坊初期版本——前沿，2016 年 3 月发布了以太坊的第一个正式版本——家园，目前以太坊处于大都会阶段，到宁静阶段，以太坊性能将会得到大幅度提升。

1.1.5　BM：EOS 的缔造者

Daniel Larimer（丹尼尔•拉里莫）是一名软件程序员和加密货币企业家，2003 年获得弗吉尼亚理工学院和州立大学的计算机科学学士学位，业内都称他为 BM（ByteMaster）。图 1–9 是 Daniel Larimer（丹尼尔•拉里莫）。

2009 年，在比特币的初期阶段，BM 就对区块链产生了兴趣。2010 年 7 月，BM 在 bitcointalk（比特币论坛）中曾经与中本聪进行了针锋相对的争论，指出相对银行系统，比特币 10 分钟一次的交易确认时间显得太长了，提出需要改变共识机制才可以提升效率，而中本聪则霸气十足地回复了那句名言：“看不懂就算了，我没时间搭理你，不好意思”。

“If you don’t believe me or don’t get it, I don’t have time to try to convince you, sorry.”

图 1-9　EOS 缔造者——BM

在与比特币社区未达成共识的情况下，BM 研发了石墨烯（Graphene）技术框架。石墨烯技术框架中设计和实现了区块链的基本功能，如 DPOS 共识、P2P、对象模型、存储、插件机制等多方面的内容。在石墨烯框架上，结合业务进行二次开发，可以实现满足特定业务功能的区块链。

自 2004 年以来，BM 一直是一位连续创业者，作为自由市场的倡导者，一直在为建立高质量、工业级、低费用的区块链技术平台而奋斗。

2014 年，他创建了世界上第一个去中心化数字货币交易所——比特股（BitShares）。比特股是一个全球化的交易网络，具有去中心化属性，平均每 3 秒确认一次交易，可以承载 10 万次 / 秒的交易，也是代理权益证明机制（Delegate Proof of Stake，DPoS）的鼻祖。在比特股上任何个人和机构都可以自由地进行转账、借贷、交易，以及发行资产、智能货币、期货等。同时比特股底层的石墨烯技术可以快速搭建去中心化、高性能的去中心化交易所。图 1–10 是数字货币交易所比特股系统的主界面。

2015 年，他与父亲一起创办了区块链技术咨询公司 Cryptonomex。现在，Cryptonomex 已经是一个拥有由数千名支持者组成的全球社区，通过共享收入来源，共同发展区块链生态。

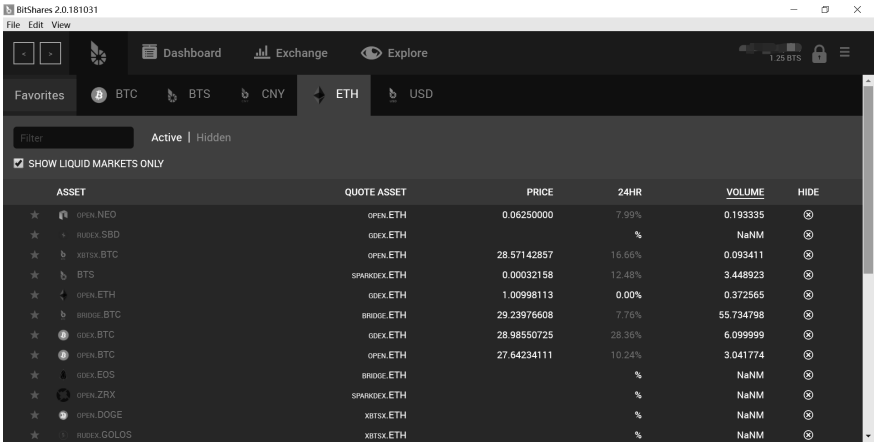


图 1-10　比特股主界面

2016 年，他作为联合创始人参与了世界上第一个基于区块链的社交平台 Steem。Steem 首次采用了脑力挖矿（Proof Of Brain）的方式。与传统社交平台不同的是，用户可以通过在平台上发布内容、点赞、回复赚取 Steem 代币。Steem 的目标是识别每个人对社区的贡献，这其中包含了内容输出和社群活动的组织。一个长期看好平台发展的用户，通过在平台上写作、参加社区建设可以获得相应奖励。图 1–11 是 Steem 的主界面。

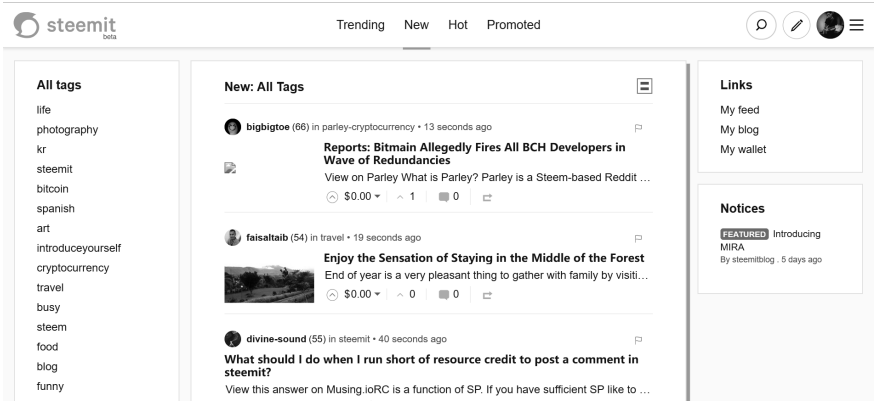


图 1-11　Steem 主页面

2017 年，BM 加入 BlockOne 公司，成为 BlockOne 公司的 CTO，负责 EOS 开发。EOS 被誉为区块链 3.0 时代的代表，是 BM 基

于之前的两个成功的项目比特股和 Steem 开发的公有链。经过近一年的研发，2018 年 6 月已经主网上线，随着 EOS 技术的不断迭代，将会为众多区块链应用提供一个可靠、稳定的底层公有链，也会将区块链技术从货币、经济时代升级到 DAPP 时代。

2018 年 2 月，福布斯估计 BM 的净资产在 6~7 亿美元。

1.2 10 分钟搞懂区块链，你信不信?

珍珠项链、打麻将，这些貌似与区块链风马牛不相及的事情恰恰是你认识区块链的基础。一个形象的说法，区块链就是一群人共同维护的一个大账本。

区块链是一种分布式账本技术（DLT，Distributed Ledger Technology），通过共识机制发动节点来共同记账。为防止共识信息被篡改，通常情况下，区块链会采用链状数据结构，使用密码学技术进行数据存储。

技术从来都不是独立存在的，这一点在区块链技术中体现得淋漓尽致。区块链第一次创造性地将密码学、分布式、博弈论、P2P 协议等技术有机地组合在一起，使其具备去中心化、账务公开、不可篡改、可追溯等特点。

区块链最大的创新是第一次用技术解决了人类的共识问题，用理性的技术为人类建立信任提供了方法。

1.2.1 区块链并没有你想象的那么难懂

区块链是“化名”为中本聪 (Satoshi Nakamoto) 的一个人或者一群人智慧的结晶。从 2018 年以后，区块链逐渐被大众所津津乐道，每个人都在问区块链是什么?

区块链诞生于比特币，随着区块链技术的不断发展，区块链技术在商业中的价值已经超过了数字货币本身。

区块链是什么，有点类似一串珍珠项链，其中每颗珍珠都有固定的位置，拿走任何一颗珍珠，其他珍珠的位置都会发生变化。每颗珍珠

就相当于一个区块，将珍珠用线串起来就形成了区块链。当然这样的比喻不是非常贴切，只是为了方便大家理解。

第一个区块链应用——比特币，它的工作原理类似打麻将，4 个矿工自发地组织在一起，通过掷骰子（碰撞一个随机数）确定谁来记账，谁获得了记账权谁就得到了相应的奖励，其他 3 个矿工对这笔账目进行确认。

一个形象的说法，区块链就是一群人共同维护的一个大账本。

这个账本与我们之前使用的账本不同，由于它是一群人来记账，因此修改这个账本的难度会比较高。

我们传统的信息系统，无论是银行系统，还是我们熟悉的支付宝、微信，使用的数据库都是集中式、中心化的，所有的数据安全都依赖于某一个组织（例如阿里）的可信度，以及这个组织背后的技术是否过硬，管理是否足够严格。

而区块链则不同，它是通过共识机制发动大量的节点来共同记账，并且这些节点之间地位平等。由于区块链采用了一群人共同记账的方式，使数据难以篡改。在区块链技术中，要修改数据必须得到半数以上节点的同意才可以修改数据，相对于传统中心化单个节点说了算的记账方式，使用区块链技术进行记账可以提高大家的信任度，而这种信任机制的建立不依赖于某个组织、个人，而是依赖于区块链技术本身。图 1–12 展示的是中心化账本与分布式账本的区别。

举一个例子，在一个村子里，张三借给李四 1 万元人民币，原来的方式就是张三给李四打一张借条，或者找一个双方都信得过的人作为见证人。现在有了区块链，同样是张三借给李四 1 万元人民币，我们会发动所有的人都来记账，每个人都会在自己的本子上记一笔账“张三借给李四 1 万元人民币”。按传统的记账方式，一旦李四的借条丢了，或者张三贿赂了这位见证人，这笔借款都有可能收不回来。但有了区块链，由于全村人都记账，这笔借款就变得无法抵赖了。

所以，区块链实际上就是分布式账本技术（DLT，Distributed Ledger Technology）。

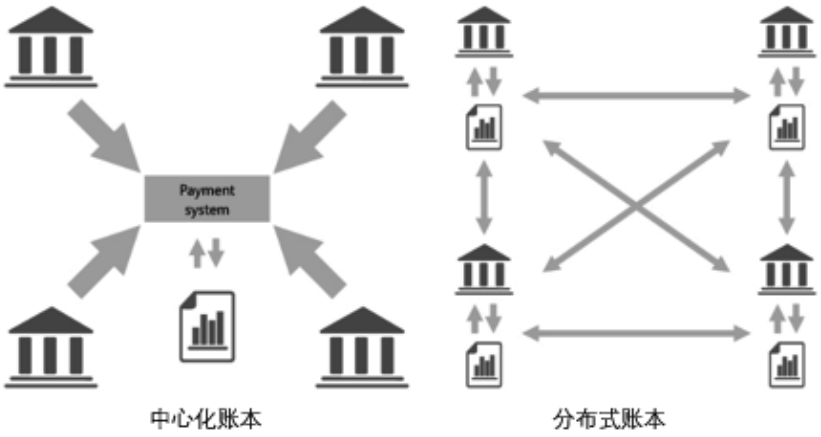


图 1-12　中心化账本与分布式账本

那么，问题来了，凭什么全村人都帮李四来记这一笔账，只是人缘好是不能让全村人都来记账的，我们必须有一套机制来奖励这些人。这就有点像农村的红白喜事，全村人都来帮忙，原因是以前大家生活条件都不好，只要村中有红白喜事，当事人都要大摆宴席答谢村里人，这其实就是一种奖励机制。

同样，区块链要让一群不相干的人来共同记账，因此需要一套奖励机制，也就是经济刺激，让参与记账的人可以获得经济上的回报。但问题是，只要有经济刺激，就会有人作弊。为了防止有人作弊，区块链引入了共识机制，以确保参与者无法作弊。比特币和现在的以太坊使用的共识机制是工作量证明机制（Proof of Work，PoW）；Bitshares、Steem、EOS 采用的是代理权益证明机制（Delegate Proof of Stake，DPoS）。

为防止共识信息被篡改，典型的区块链会采用链状数据结构进行数据存储（图 1–13）。

图 1-13　区块链数据结构

区块链是一个连续增长的数据结构，每个区块都包含了前一个区块的哈希值。为了保证区块链的安全性，区块之间按照时间顺序，结合密码算法进行数据存储。

因此，区块链也是一个 “历史记录不可篡改的数据库”。

传统数据库可以增、删、改、查（CURD），而区块链只能增加和查询，不能修改、不能删除。

去中心化是区块链最重要的特征，指的是区块链在不依赖中心化组织的条件下，参与方（节点）可以通过共识机制达成一致，使区块链天然具备信任的基础。账务公开是区块链技术中一个常用方法，为了使参与方都可以记账和验证，通常情况下会将账务公开广播给全网。可追溯特性是基于密码学的区块链链状数据结构保证的。为了确保交易的唯一性，有效防止双重攻击，使用时间戳技术为每一笔交易加盖时间戳。

技术从来都不是独立存在的，这一点在区块链技术中体现得淋漓尽致。区块链第一次创造性地将密码学、分布式、博弈论、P2P 协议等技术有机地组合在一起，使其具备去中心化、账务公开、不可篡改、可追溯等特点。

区块链最大的创新是第一次用技术解决了人类的共识问题，用理性的技术为人类建立信任提供了方法。

1.2.2 区块链只能发币吗?

作为一个分布式账本技术，除了加密货币本身的应用之外，智能合约是区块链现在一个主要的发展方向。全世界的精英都将重心放在了智能合约的大规模应用上。

智能合约（Smart Contract）是在 20 世纪 90 年代由尼克·萨博（Nick Szabo）提出的理念，由于缺少可信的执行环境，一直没有被应用到实际产业中。区块链技术的出现给智能合约带来了新的契机。

由于区块链是一个历史记录不可篡改的数据库，因此将计算机代码写在链上就可以让代码具备“智能”的特点。智能合约本质上就是一段运行在区块链上的代码，这段代码具备去中心化、公开透明、不可篡改等特点。

现实生活中，甲乙双方要进行一笔交易，我们需要签订一个合同，在合同中约定合同标的、内容、权利、义务等合同法规定的条款，双方盖章签字，一式两份。以买卖合同为例，一旦双方签订一份项目合同，后续就要按照合同要求执行。但现实中，由于大家的法律观念意识不强，经常会出现合同违约，即使签订了合同也不会按照合同执行，此时合同就变成了一张废纸，对双方都没有约束力。一旦出现纠纷，就要诉诸法律，由法院来进行强制执行。

那么，有没有一种更有效的办法来确保合同的执行呢？答案是将上面的合同内容写在智能合约中，一旦智能合约中某个条件达成，合约就会自动执行。由于区块链信任的特点，使合约的执行不依赖于人和现有的中心化机构，这样就可以有效解决传统合同出现纠纷的问题。

无论是显式的合同，还是日常生活中的各种交易都是一种契约关系。传统契约需要签字、盖章才具备法律效应。你可以将智能合约想象为一个自动售货机，使用智能合约就是不依赖人和现有中心化机构，合约可以根据预设的条件自动执行。

基于以太坊进行发币只是智能合约最初级的应用，现在流行的DAPP（去中心化应用）实际上就是将应用系统中部分核心业务代码放在链上执行。从金融方面开始，区块链智能合约技术已经扩展到政府、供应链、溯源、公共服务等行业，是未来数字经济发展不可或缺的技术之一。

1.2.3 揭开区块链神秘的面纱

从字面上理解，区块链就是区块连接成的链，英文是 Block Chain，Block 就是区块的意思，Chain 是链的意思，合起来就是连接在一起的区块。比特币白皮书中，区块和链是两个独立的单词，直到 2015 年以太坊出现后区块链这个词才流行起来。

本解决方案起步于一种时间戳服务器。时间戳服务器是这样工作的：为一组（block）记录的哈希打上时间戳，而后把哈希广播出去，就好像一份报纸所做的那样，或者像新闻组（Usenet）中的一个帖子。显然，时间戳能够证明一个数据在某个时间点之前已然存在，否则该数据哈希也就无法生成。每个时间戳在其哈希中包含之前的时间戳，因此构成了一个链（chain），每一个新的时间戳被添加到之前的时间戳之后。

去中心化作为区块链一个重要的特点，指的是区块链在不依赖中心化组织的条件下，参与方可以通过共识机制达成一致，使区块链天然具备信任的基础。去中心化的英文是 decentralized，原意如下：

① 将权力从中央转移到地方政府。

② 将大型组织部门的管理权，从单一集中管理转移到其他部门，通常情况下给予它们一定程度的自主权。

判断一条链是否去中心化，可以以节点数量、节点的容错性和有多少人（组织）能够控制系统来衡量。节点数量越多，系统可以容忍崩溃的节点越多；参与节点的人（组织）越分散，就代表一条链的去中心化程度越高，反之，一条链就趋向于中心化。

去中心化有时候很容易和无政府主义思想混为一谈，根据英文原意，将去中心化理解为多中心化更为合适。

区块链也不是有些人所宣称的那样，什么都可以做。事实上任何一项技术都不可能包打天下。以互联网技术为例，除 TCP/IP、HTTP、HTML 相关技术外，经过这么多年的发展，互联网已经融合了云计算、大数据、人工智能等许多技术才走到今天，才让一项当初只能发邮件、浏览网页、玩游戏的技术演变成一项改变人类文明进程的技术。

区块链作为一个分布式账本技术，可以应用在很多地方，但在具体业务上，需要和云计算、大数据、人工智能、物联网等技术结合起来才能满足实际业务需求。

例如，在商品溯源中，区块链可以从商品源头信息采集、原料来源追溯、生产过程、加工环节、仓储信息、检验批次、物流周转到第三方质检、海关出入境、防伪验证的全过程进行追溯；将商品信息采用分布式结构存储在各个节点上，使数据受多方监管，保证链上商品信息记录过程的真实性。区块链数据不可篡改的特点，可以有效保证上链商品信息无法篡改，使商品溯源的可信程度大幅度提升，但要避免源头造假，还需要借助物联网技术进行数据采集。

1.3 玩转区块链，搞定密码学、分布式、共识机制和 P2P 网络即可

区块链起源于密码学，毫不夸张地说，密码学占据了区块链的半壁江山。

区块链是分布式系统，但不是说分布式系统都是区块链。

共识机制不是区块链的特权，但共识机制的确是区块链的灵魂，共识算法也必然要经历一个不断完善、不断进化的过程。

密码学、分布式、共识机制固然重要，但 P2P 才是区块链的根基。

1.3.1 密码学——密码极客的最爱，区块链的起源

密码学是一个大家熟悉又陌生的学科。提到密码大家一定会想到银行卡密码、WiFi 密码、手机密码等，毫不夸张地说，我们的生活已经离不开密码了。

密码学可以分为古典密码学和现代密码学，分水岭是第二次世界大战。一般情况下，我们将第二次世界大战之前出现的密码学称为古典密码学，第二次世界大战之后的密码学称为现代密码学。

古典密码学只关注信息的保密书写和传递，通常会比较依赖于设计者的创造技巧。

古典密码学中经常会用到两个重要的技巧，分别是将字母重新排序和替换字母（符号）。例如，blockchain 可以倒序就成为 niahckcolb，将每个字母用下一个字母代替就成了 cmpdldibjo。但这些都只是技巧性的，不足以保证信息的机密性，一旦敌人明白了原理就很容易破解。在第二次世界大战之前，由于战争和国家安全的需要，还出现了维吉尼亚加密法、恩尼格玛密码机（ENIGMA），其中恩尼格玛密码机就是被计算机科学家、数学家图灵破解。

第二次世界大战以后，计算机技术的发展促使了更为复杂的密码算法。由于计算机可以加密任何二进制形式的数据，不再限于书写的文字，以语言为基础的加密技术因此失效。在密码学领域，加密和解密一直是不断较量的一个过程，正所谓“道高一尺魔高一丈，魔高一尺道高

一丈”。

现代密码学除了关注信息的保密书写和传递，还涉及信息的完整性、不可抵赖性，以及分布式计算中内部和外部攻击者的所有信息安全问题。由于更注重理论研究，也使密码学成为一种系统而严格的学科。

密码学在区块链中的应用非常广泛，占据了区块链的半壁江山。例如，在链状数据结构和工作量证明机制中使用了哈希算法，保证了数据的不可篡改性；在交易数据上加盖时间戳，确保了交易的唯一性，有效防止双重攻击；对交易数据使用私钥进行数字签名，保证交易身份的唯一性；采用加密算法对交易数据进行加密，有效保护数据隐私。总之，区块链与密码学的血缘关系非常近，所以才有人怀疑比特币的发明者有可能是一群密码领域造诣极深的专家。

密码学属于数学和计算机学科的分支，也是专门研究密码算法和密码破译的技术学科。在密码学中，目前常用的密码算法有哈希（Hash）、对称加密、非对称加密、数字信封、时间戳、零知识证明等技术，这些都属于密码算法的应用。密码学是一群高智商人群的博弈，例如，MD5 哈希算法、RSA（1024）算法都已经被破解，未来量子密码学（Quantum cryptography）会对现有密码算法造成威胁，但同时也会出现新的量子加密算法。

虽然密码学非常深奥，但对于大多人来说我们不需要过多了解密码算法的实现原理，只需掌握密码算法的应用就可以了。

1. 哈希（Hash）

哈希也称为散列算法、摘要，是对一段数据进行加密计算，形成一个定长的字符串，由于哈希可以代表一段数据的唯一特征，有点类似人类的指纹，所以大家也经常把哈希称为数字指纹，常用的算法有 SHA-256。

从图 1-14 中可以看出，无论输入的字符串有多长，最终输出的都是一个定长的字符串。图中的“你好”加上感叹号后，两者的哈希就彻底不同了。

图 1-14　哈希算法

区块链是基于哈希指针构建的一个有序的、反向链接的交易块链表，也就是说在区块链中，每个区块都包含了上一个区块的哈希值（图 1–15）。在区块链中使用 SHA–256 算法对区块进行哈希计算而得到的数字指纹（32 个字节哈希值）被称为区块哈希值。图 1–16 中比特币第 554347 个区块中包含了第 554346 个区块的哈希。

图 1-15　区块链数据结构

Block #554347

Summary	
Number Of Transactions	2176
Output Total	6,669.95107828 BTC
Estimated Transaction Volume	1,336.68119658 BTC
Transaction Fees	0.21349756 BTC
Height	554347 (Main Chain)

Hashes	
Hash	00000000000000000022d14dfdc77d3f8be8e8a8ec302eb830490489ec9e16db
Previous Block	00000000000000000001ee8666d4453b3b1da908c5cd12a47b9b4ef16a7f78372
Next Block(s)	第554346区块的哈希
Merkle Root	0b595087bec5796510e1294768eaf20641728bafb13416a870fa3ccad6d53c76

Block #554346

Summary	
Number Of Transactions	701
Output Total	890.471575 BTC
Estimated Transaction Volume	201.42557129 BTC
Transaction Fees	0.03437079 BTC
Height	554346 (Main Chain)

Hashes	
	当前区块的哈希
Hash	00000000000000000001ee8666d4453b3b1da908c5cd12a47b9b4ef16a7f78372
Previous Block	00000000000000000002ae9ee04124233376d3a608d702866213613b5163fb0d9
Next Block(s)	00000000000000000022d14dfdc77d3f8be8e8a8ec302eb830490489ec9e16db
Merkle Root	32417ea9e2fd2d404955946f8d045bc941a89e1b8a3c509593738a828a9e50f8

图 1-16　第 554347 个区块中包含了第 554346 个区块的哈希

（数据来源于 blockchain.info）

由于每个区块都包含了大量的交易数据，随着时间的增长，区块的

高度不断增加，导致交易信息查找变得异常低效，因此，区块链中采用了默克尔树(Merkle tree)的方式来组织区块内的交易数据(图 1–17)。

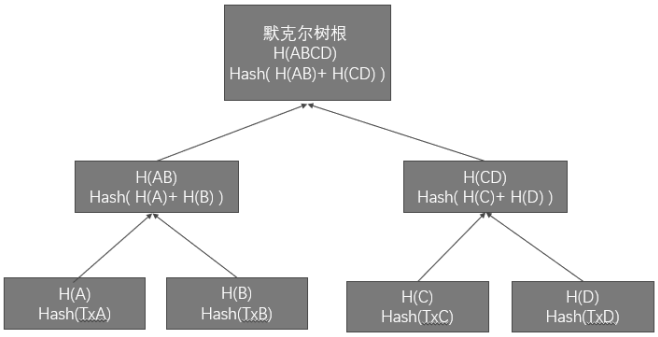


图 1-17　默克尔树

默克尔树有时候也被称为哈希树，顾名思义，就是存储哈希值的一棵树。默克尔树是一种二叉树数据结构，它的叶子是数据块，非叶子节点是两个子节点的哈希。一个默克尔树是自下而上构建的，通过不断计算两个节点的哈希值，直到头部只有一个默克尔树根。区块链中，这种数据结构的特点是通过数学算法，可以非常方便地验证区块中的交易数据。

2. 对称加密

密码学中有两类加密算法，分别是对称加密和非对称加密。我们可以将加密理解为家里的保险箱。对称加密与我们生活中的概念是相同的，使用同一把钥匙对保险箱进行上锁、开锁。非对称加密与我们日常生活不太一样，是用一把钥匙上锁后，用另外一把不同的钥匙来开锁。

对称加密的加密密钥和解密密钥是相同的。由于对称加密使用了相同的加密密钥对数据进行加密，因此加密效率非常高。但在实际使用中，由于很难保证密钥在传输、保存过程中不被截获，因此对称加密的安全性比较低。常用的加密算法有 DES、AES、 SM4。

实际应用中，有时候也会遇到一些让人哭笑不得的案例。有些安全厂商的软件宣称使用了非常安全的加密算法，但实际上就只是使用了对称加密算法。更有甚者还将密钥与密文存放在一起，一旦密钥被黑客攻击，所有密文实际上就变成了明文。看似安全的技术手段，实际上却

非常脆弱。

图 1–18 采用了对称加密算法 DES，使用了密钥 1234567890 将明文数据“你好”加密成密文 U2FsdGVkX1/pez1V1Wa8LNCP9hlXhJFs，再用相同的密钥 1234567890 将密文 U2FsdGVkX1/pez1V1Wa8LNCP9hlXhJFs 解密成明文“你好”。

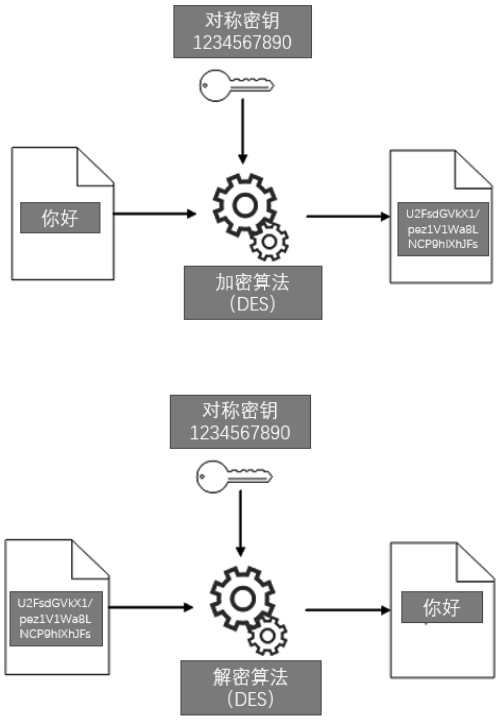


图 1-18　对称加密

3. 非对称加密

由于对称加密非常脆弱，很容易被破解，因此，催生了非对称加密算法。顾名思义，非对称加密的意思就是加密密钥与解密密钥不同，这样就使加密的安全性大幅提高。

非对称加密是由椭圆曲线算法生成的一对公私钥对组成，公钥对外公开，任何人都可以获取，私钥自己持有，不能给任何人看。由于公钥是对外公开的，我们可以用接收者的公钥对数据进行加密，只有持有

公钥对应私钥的人才能进行数据解密。反过来，如果使用自己的私钥对数据加密，用公钥进行解密，我们称为签名。由于私钥是自己持有的，公钥是对外公开的，因此采用私钥加密公钥解密的方式，可以验证身份的唯一性，确定某段数据已经得到某个特定组织、个人的认可，或者确定某段数据由某个组织、个人持有。常用的算法有 RSA、SM2。

还是以安全保险箱为例。在非对称加密中，上锁和解锁使用了两把不同的钥匙，一把称为私钥，另一把称为公钥。当我们用公钥上锁安全保险箱时，只有对应的私钥才可以开锁，但由于私钥只有保险箱的主人持有，因此我们把这个过程称为加密。如果我们将上面的顺序反过来，用私钥上锁，公钥解锁，由于公钥是对外公开的，因此任何人都可以打开安全保险箱，这种方式就不能用作加密，但由于只有保险箱的主人持有私钥，所以只能由保险箱主人的私钥对应的公钥解锁，因此可以起到确认身份的作用。

图 1–19 使用了接收者的公钥对明文进行加密，接收者使用自己的私钥进行数据解密。

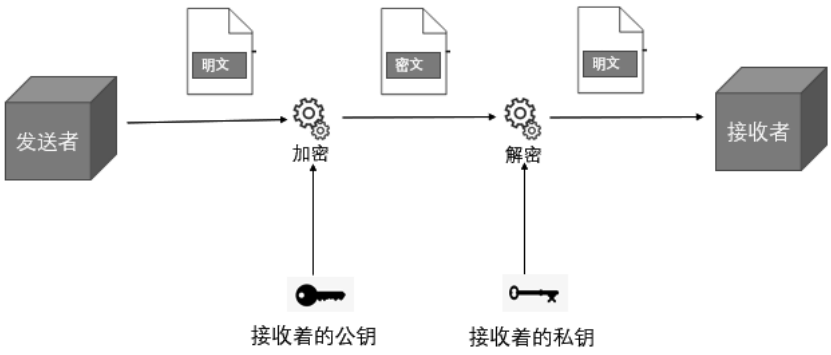


图 1-19　非对称加密

如果发送者（签名者）用自己的私钥对数据加密，将数据发送给接收者（验证者），接收者（验证者）用发送者（签名者）的公钥进行解密，这个过程就是验证签名的过程。如果验证通过，代表这个数据没有被篡改，否则代表数据被篡改。图 1–20 就是一个完整的签名和验证签名的过程。需要注意的是，为了提高签名的效率，通常会对数据做一个哈希，用私钥对哈希进行签名。验证签名的时候，用对应的公钥对数

据进行解密，将得出的哈希与原数据的哈希进行对比，如果哈希相同则代表验证通过，否则验证失败。

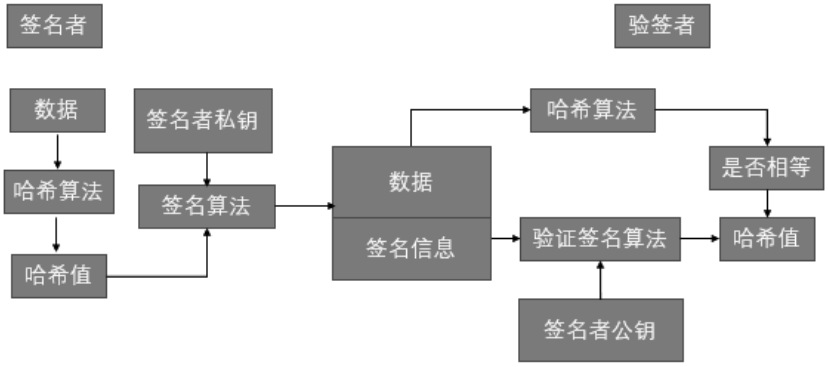


图 1-20　验证签名

4. 数字信封技术

虽然非对称加密的安全性很高，但加解密的效率太低。实际应用中会采用数字信封技术对数据进行加密。数字信封技术是用对称加密算法对明文数据进行加密，用非对称加密算法对对称密钥进行加密，这样既可以提升加密效率，又可以有效保护数据安全。

数字信封技术主要包括数字信封打包和数字信封拆解两个过程。数字信封打包指的是信息发送方采用对称密钥加密信息原文，然后使用接收方公钥加密对称密钥，之后将密钥和密文一起发送给接收方；数字信封拆解指的是，接收方先用对应的私钥打开数字信封，得到对称密钥，然后使用对称密钥解开加密信息得到明文数据。具体过程见图 1–21。

1.3.2　区块链是分布式系统，但不是说分布式系统就是区块链

对区块链最常见的误解是“区块链就是分布式系统”。虽然区块链是一种分布式系统，但不是说所有的分布式系统都是区块链。区块链作为一种分布式记账技术与传统的分布式系统相比，具有更好的容错性，具有数据难以篡改的特性，这是传统分布式系统无法媲美的地方。

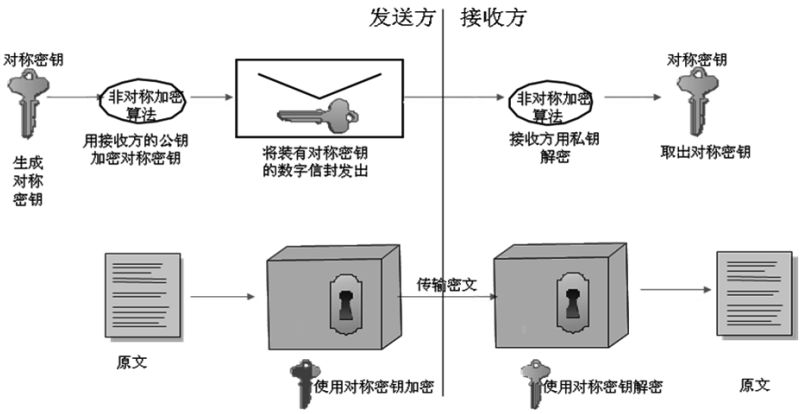


图 1-21　数字信封技术

传统的分布式系统是单组织（单中心）系统。例如，腾讯分布在全球各地的服务器都隶属于腾讯，这就导致腾讯的权利过大，利益比较集中。区块链是由很多组织（多中心）共同维护的一个系统，这些组织之间地位平等，可以很好地保护所有参与者的权益。

1. 传统分布式系统

在计算机理论科学中，CAP 定理指的是系统的一致性（Consistency）、可用性（Availability）和分区容忍性（Partition Tolerance）不能同时得到保证（图 1–22）。

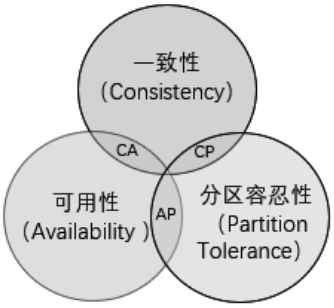


图 1-22　CAP 定理

» 一致性：每一次数据读取操作都是最新写入的数据，数据的读取不存在任何延迟，这里指的是数据的强一致性。

» 可用性：每次系统请求都会收到正常响应，但不确保是最新的数据。
» 分区容忍性：网络分解为相对独立的子网，节点之间的通信不可保障。

基于 CAP 定理，分布式系统在设计时需要弱化其中某个特性。由于系统设计上的缺陷、黑客攻击、服务器宕机等原因导致网络无法正常通信，我们把这类问题统称为网络故障。在网络故障的情况下，系统要么牺牲一致性，要么牺牲可用性。当对系统一致性要求很高的情况下，设计上要牺牲可用性，当对系统可用性要求比较高的情况下，设计上要牺牲一致性。

举一个例子，金融系统对系统一致性要求很高，当网络出现故障时，系统会拒绝向用户提供服务。对一致性要求不高的系统，当网络出现故障时，系统会牺牲一致性，继续向用户提供服务，待网络恢复正常，系统才会更新数据。我们经常使用的微信等社交网络就属于这类，在网络故障时，系统会放弃一些用户请求，但大部分用户的使用还是正常的。

理论研究往往和工程领域有所不同，理论研究是非常严密的学术研究。实际生活中，传统分布式系统在设计上对系统容错的要求都不是很高，除非一些极端情况，例如 SpaceX 的火箭发射系统。

实际上，信息系统的建设都会采用双线路方式、防火墙、负载平衡、冗余备份等手段确保网络的可靠性。

2. 拜占庭容错机制

传统分布式系统在设计时，只考虑系统中存在的故障，但不存在恶意攻击情况，因此，在共识机制上采用了非拜占庭的共识机制（例如 Paxos、Raft）。

区块链在设计上采用了拜占庭容错机制（Byzantine Generals Problem，BFT），拜占庭容错是一种对一致性要求极高的共识机制，在完全开放的环境下，实现了数据的一致性和安全性，为业务提供了一个可信的环境。

1982 年，Leslie Lamport 提出的“拜占庭将军”问题是解释一致性问题的一个虚拟模型。拜占庭是古东罗马的首都，由于地域宽广，守卫的将军需要通过信使传递消息，达成一致的决定。但由于将军中可

能存在叛徒，这些叛变的将军可能会发送错误的消息，干扰大家的决议。图 1–23 左图是所有将军达成一致的情况下攻城成功，右图是将军中存在叛徒的情况下攻城失败。

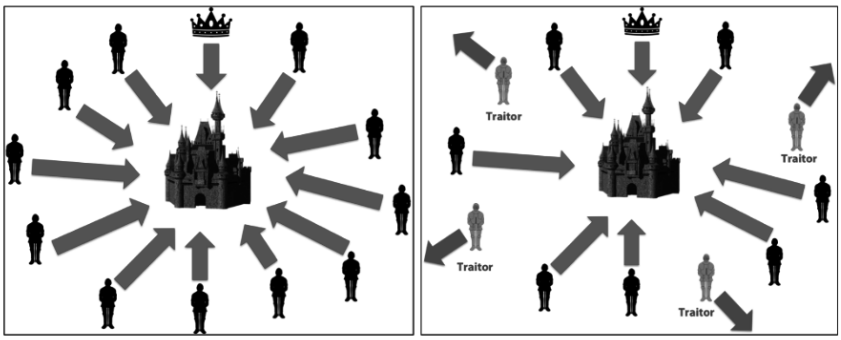


图 1-23　拜占庭将军问题

拜占庭问题的提出是为了解决上述情况下，怎样让忠诚的将军们达成一致的决议。这个问题演变到计算机领域，就是在互联网中不同计算机通过通信怎样达成一致。与拜占庭将军类似，实际过程中有些计算机可能出现错误，有些计算机有可能被黑客攻击，怎样保证网络上的计算机对某个事物达成一致就是这个理论模型要解决的问题。拜占庭问题是区块链技术中共识机制的基础。正因为有了这样的理论基础，才使区块链技术有了发展的科学基础。

区块链是一种分布式系统解决方案，但不能说分布式系统就是区块链。除了两者采用的共识机制不同，数据隶属权也不同。区块链数据隶属于各个参与的节点，而传统分布式数据只隶属于单一的组织。

1.3.3　持续演进、持续进化的共识机制

前面我们已经提到了区块链与传统分布式最重要的区别——即采用了拜占庭共识机制。共识机制是区块链技术中一个很重要的技术，一条公链是否足够去中心化、足够可信，取决于共识算法的合理性，而共识算法是否合理取决于区块链使用场景的需要。

共识机制不只是区块链的特权，在人类历史发展的长河中，已经产生了许多的共识机制，例如国家、宗教、道德、科学等。我们对于一件事情好坏的判断，都基于各自的生活环境和认知水平，这也能很好地

说明为什么价值观相同的人容易达成共识，同一个地域的人容易达成共识。

计算机中让不相干的人达成共识需要有一套新的理论模型。区块链中的共识机制可以让系统在限定时间内完成对交易的验证和确认，对一笔交易，如果利益不相干的若干个节点能够达成共识，我们就可以认为全网对此也能够达成共识。

区块链信任的特点主要体现在区块链上的用户无须信任交易的另一方，无须信任任何一个中心化的机构，只需信任区块链提供的软件系统就可以实现交易，这种自信任的基础就是区块链的共识机制。在一个互不信任的市场中，要使各节点达成一致，其充分必要条件是每个节点出于对自身利益最大化的考虑，都会自发、诚实地遵守协议中预先设定的规则，判断每一笔交易记录的真实性，最终将验证通过的记录写入区块链。区块链技术正是运用一套基于共识的数学算法，在计算机之间建立了一套“信任”的网络，通过技术背书而非中心化信用机构来进行全新的信用创造。

共识机制起源于拜占庭理论，经历了数字货币的历史演进，目前主流共识有工作量证明机制（Proof of Work，PoW）、权益证明机制（Proof of Stake，PoS）和代理权益证明机制（Delegate Proof of Stake，DPoS）。这些共识机制其实都是技术和经济的合体，在计算机世界中加入了现实世界的经济博弈。工作量证明机制锚定的是算力，权益证明机制和代理权益证明机制锚定的是权益（Token）。类似于工作量证明机制的挖矿机制，大家可以将权益证明机制想象为虚拟挖矿。

在工作量证明机制下，用户需要花费一定的金钱购买矿机，每天消耗着巨额的电费，其随机获得挖矿收益与消耗的电力大致成比例。在权益证明机制下，用户花费金钱购买代币（Token），在网络中分配一定的计算资源，系统验证区块产生的奖励大致与购买代币的成本成一定的比例，达到了与工作量证明机制同样的效果，而且不消耗电力，效率也会大幅度提升。

为了能够清楚地理解共识机制，我们需要搞清楚共识机制中的区块、生产者、验证者 3 个核心概念。以篮球比赛为例，在篮球比赛中比赛成绩就是区块，运动员是区块的生产者，裁判员是区块链的验证者。如果裁判徇私舞弊就会产生信任危机，无法保证比赛成绩的真实性，因

此共识机制的关键就是保证区块生产和验证的安全。

共识机制的核心是记账权的争夺，设计思路是让恶意节点的攻击成本远远大于诚实节点的受益，基于利益的考虑，大家与其作恶白白损失金钱还不如老老实实地记账。

工作量证明机制（Proof of Work，PoW）中，全网通过竞猜随机数获取生产区块的资格，一旦某个节点作恶就会白白损失算力，无法成为合格的区块生产者，也无法获得奖励。工作量证明机制并非完美，其中被指责最多的主要有两点，一是浪费能源，二是风险和收益博弈必然导致联合挖矿，而大算力矿池可能会对系统的去中心化构成威胁。

比特币采用的是工作量证明机制。图 1–24 是比特币主要算力分布情况。由于比特币长期缓慢的发展，导致 65% 的算力已经被 5 个矿池所占有。理论上上讲，5 大矿池联手可以对比特币网络发起 51% 的攻击。

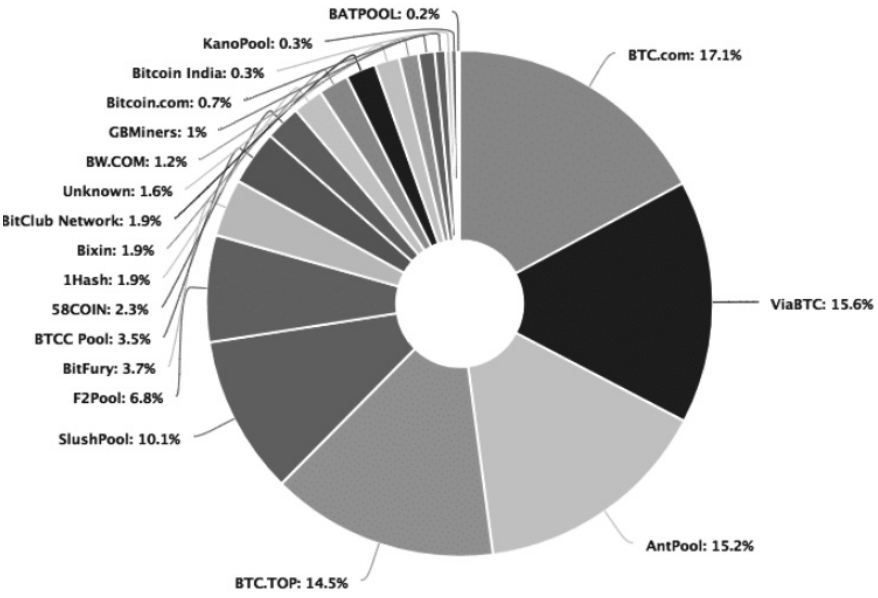


图 1-24　比特币主要算力分布图（来源于 blockchain.info）

权益证明机制（Proof of Stake，PoS）中，节点被称为验证者，没有挖矿，节点通过验证交易则获取交易手续费，验证错误则没收押金。每次系统会根据抵押代币数量来随机选择验证者，抵押代币越多则被选

为验证者的概率越大。举一个例子，如果 A 节点抵押了 100 个代币，B 节点抵押了 10 个代币，那么 A 节点相对 B 节点就有 10 倍的验证机会。

为提高以太坊的工作效率，以太坊 2.0 将会采用权益证明机制。

代理权益证明机制（Delegate Proof of Stake，DPoS）有点类似人民代表大会制度，由持币者选取 21 个节点参与区块生产和验证，每次参与记账的区块生产者是由持有代币的人选举产生的，如果节点作恶，会被系统自动“投出”。在目前的区块链技术条件下，代理权益证明机制采用了部分“人治”弥补了区块链技术在效率上的缺憾。两害相权取其轻就是这个意思。

EOS 采用的是代理权益证明机制，在目前已知的去中心化共识算法中，只有该算法经证明可以满足区块链应用的性能要求。

需要说明的是，现阶段脱离实际业务谈共识机制的优劣没有太大意义。对于一个去中心化的全球货币，工作量证明机制是目前最好的共识机制。对于一个去中心化应用平台，权益证明机制和代理权益证明机制是目前比较好的共识机制。工作量证明机制虽然效率低下，但由于节点匿名，使分布式拒绝服务攻击（Distributed Denial-of-service attack，DDoS）（通过大量合法的请求占用大量网络资源，以达到瘫痪网络的目的）变得非常困难。代理权益证明机制虽然效率比较高，但由于只有 21 个节点，有被 DDoS 攻击的可能性。

关于共识机制更全面的理解，将会在相应章节做进一步介绍。

1.3.4 区块链的根基——P2P 网络

首先要澄清的是，P2P（peer to peer）网络是一种分布式应用架构，不是大家认为的 P2P 网络借贷，中文称为对等网络（也称点对点网络）。除区块链外，规模最大也最成功的 P2P 技术应用是在文件分享领域，Napster 是该领域的先锋，BitTorrent 是其架构的最新演变，国内的迅雷、快播都是 P2P 技术的领导者。

P2P 网络中每一个节点彼此对等，各个节点共同提供服务，不存在任何特殊节点。P2P 网络中不存在任何服务器、中心化服务及层级结构，P2P 网络具有天生的伸缩性、去中心化和开放的特点。图 1-25 是 P2P 网络的示意图。

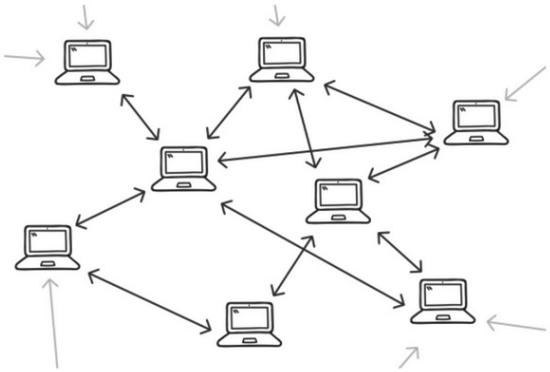


图 1-25　P2P 网络示意图

P2P 网络中，节点之间可以直接使用资源（CPU、存储、带宽），而不需要中心服务器的协调。相对传统中心化架构（客户端 / 服务器）下资源供应者和消费者的分离，P2P 网络中各个节点既是资源的供应者也是消费者。

举一个例子，你通过微信给朋友老王发了一句话“在吗？”，这时老王会在自己的手机上看到这条信息。你以为这条消息是直接发给了老王，其实背后的流程是：你先将这条信息发给了微信服务器，然后微信服务器再将这条消息发给老王。在你完全不知情的情况下，有一个中间人在参与你们的交流，这个人就是微信服务器，它在帮你转发那条消息。节假日，如果微信服务器繁忙，它有可能会罢工，这时候可能这条消息就一直无法发送。

但是，如果采用 P2P 网络，你和老王之间就可以直接通信了。由于在 P2P 网络中不存在特殊节点，因此，其他任何节点出现问题都不会影响你和老王之间的通信。

从上面的例子可以看出，P2P 网络架构既是区块链去中心化核心特性的反映，也是该特性的基石。

1.4 公有链、联盟链、私有链，谁才是真正的区块链？

区块链会在公有链和联盟链得到长足的发展。从长远来看，公有链和联盟链在技术上会趋向融合，界限也会越来越模糊。

区块链的分类有点类似信息网络中的公网、专网、局域网的划分。公网也称为互联网（Internet），我们现在使用的支付宝、微信、滴滴出行、美团外卖都基于互联网；专网是一个比较私密的网络，应用最广泛的就是金融、公安等信息安全级别较高的机构；局域网一般指的是企业内部的网络。

按照区块链准入机制，区块链被分为公有链、联盟链、私有链3种（图1-26）。相对来说，越靠近公有链，对节点的认证和权限管理要求越少，去中心化程度越高。越靠近私有链，对节点的认证和授权管理程度越高，中心化程度越高。

图 1-26　区块链的分类

公有链是一条独立运行，且人人都可以参与记账的区块链。公有链有独立运行、人人参与记账交易、账本公开、代码开源等特点。公有链上任何人都可以通过区块链网络发送交易，将有价值的交易信息记录在区块链上，任何人都可以通过区块链浏览器查看交易信息，区块链上的交易信息是透明的，但身份具有匿名性。为了保证公有链机制可审查，公有链一般都会将代码开源在Github网站上，任何人都可以查看、下载、运行代码。

一个公有链的流行程度取决于这条链的节点是否足够分散，节点越分散，代表权利越分散，也就保证了这条链的可信程度。公有链除了共识机制等技术优势，社区运营发展也是成功的关键要素之一。一条公有链参与的开发者、使用者越多，这条公有链的影响力就越大；反之，这条公有链有可能会被大家抛弃。公有链一般会通过代币机制鼓励参与者竞争记账，来确保数据的安全性。主流的公有链有比特币、以太坊、

EOS 等，都是在特定时期解决了不同的问题。比特币是世界上第一个成功去中心化的数字货币系统，以太坊在比特币基础上提出了一种可编程、可运算的智能合约公有链，EOS 提出了超越货币、经济的去中心化应用操作系统。

联盟链是一个以组织形态运作的区块链基础设施。相对公有链，联盟链节点需要经过认证才能参与到区块链网络中。联盟链节点都是预先选定的且节点数有限，因此联盟链的交易速度更快，具有更高的扩展性，并能很好地保护交易隐私。联盟链主要应用在企业级应用中，一般不需要代币作为激励机制。例如，政府部门之间和企业之间的业务，通过区块链技术为各部门之间建立一个公开透明的账本，可以大幅度提升部门之间的工作效率。在这种情况下，每个部门作为记账节点出现，其实激励已经演变成为跨部门之间业务协同给大家带来的经济效益。

联盟链的代表是超级账本（Hyperledger）。该项目是首个面向企业开放的区块链技术，在 Linux 基金会的支持下，吸引了包括 IBM、Intel、摩根等在内的众多科技和金融巨头的参与。

私有链是在某一领域、某一企业运行的区块链。相对公有链、联盟链，私有链相对比较封闭。在一个组织机构比较复杂的企业中，将各个部门作为节点出现，可以解决部门之间的信任问题；在一个组织机构相对简单的企业中，区块链更多的是作为一个分布式数据库使用，当一个节点崩溃的时候，其他节点可以正常工作，不会导致系统服务中断。

从区块链数据公开透明的特点来看，区块链会在公有链和联盟链得到长足发展。从长远来看，公有链和联盟链在技术上会趋向融合，界限也会越来越模糊。一般是将需要信任的数据放在公有链上，而一些行业数据、私有数据放在联盟链上。