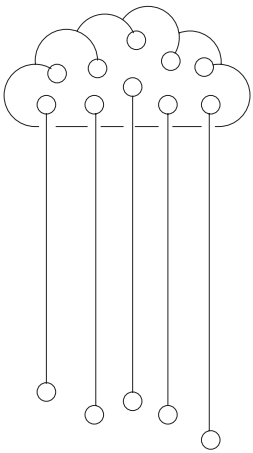


第 1 章
从莎草纸到区块链——Web3.0 的发展历史

公元前 3000 年左右，一种名为“莎草纸”（Papyrus）的文字记录工具被尼罗河三角洲的古埃及人发明，他们将纸莎草的根茎抽出，揉碎之后摊开成片，晒干之后，这堆纤维便成为了人类历史的一部分。运气好一点，我们或许还能在大英博物馆看一眼实物，感受一下时间流逝的沧桑。

2008 年 11 月 1 日，中本聪发表了一篇题为《比特币：一种点对点式的电子现金系统》的论文，文中详细描述了如何创建一套去中心化的电子交易体系，且这种体系不需要创建在交易双方相互信任的基础之上。次年 1 月，比特币创世区块诞生。在这个区块上，中本聪留下了当天《泰晤士报》的头版文章标题：*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*（2009 年 1 月 3 日，财政大臣正处于实施第二轮银行紧急援助的边缘）。

当这些看似无意义的数据被哈希算法加密之后，一个全新的媒介传播载体——区块链便诞生了。同莎草纸相比，区块链的存在是看不见摸不着的，但违反常识的是，它却可以比莎草纸保存得更为持久，甚至于直到永恒。如果我们能有幸穿越到未来，只要我们手里还能找到对应的哈希密码值，我们便能通过一定的手段找到几千年，或者几万年以前我们存储在区块链的一段文字，或者一段照片，而我们却几乎感受不到岁月的洗礼。

中心化网络时代的高潮尚未结束，但一场去中心化的 Web3.0 范式革命正式拉开了序幕。

1.1 规律捕捉：信息传播社会发展趋势总结——从 Web1.0 到 Web2.0，再部落化的二次探索

1.1.1 互联网时代之前：从部落化到集权化——中心化制度的胜利

人类文明的发展历程，本质上就是一个中心化与去中心化之间此消彼长的过程。在人类的漫长历史中，在生产力没有足够发展的情况下，中心化的制度和组织形式曾经长期占据主导地位，在政治、经济、文化和社会等方面，中央集权、等级制度和权力集中的模式曾经是主流。在古代，人类社会的政治、经济和文化中心主要在一些大国和帝国，如古埃及、古希腊、古罗马等。这些国家和帝国以中央集权、等级制度、权力集中为主要特征，政治和经济的决策权掌握在少数人手中，而普通人民缺乏参与决策的权利。

尽管在人类的历史长河中，也曾出现过诸如小国寡民或雅典城邦民主制等积极的去中心化组织制度的积极设想与尝试，但无一例外都走向了失败。在这些失败中，内部的组织矛盾与外部的侵略压迫固然是十分重要的原因，但若究其根本，**传播系统与生产力的局限才是导致这些尝试走向失败的核心因素**。

雅典去中心化治理与罗马中央集权的制度碰撞

雅典是古希腊最著名的城邦之一，也是古代世界中最早实行去中心化民主制度的城邦之一，其组织模式至今仍能在各种去中心化自治组织（DAO）中找到存在的身影。在雅典民主制中，政治权力分散在所有自由男性公民之间，公民们通过集会、投票等方式参与政治决策。雅典的民主制有以下几个特点：

- 扁平化的政治权利：雅典民主制中的政治权力是分散与扁平的，所有自由男性公民都有平等的权利，可以参与政治决策。此外，雅典民主制中还有一些民众代表机构，如议会、陪审团等，这些机构也都是通过选举产生的，代表了广大公民的意志。
- 民主投票政治决策：雅典政治制度之所以有其先进性，与其“众生”平等的民主投票制度是密不可分的。雅典民主制中的政治决策通过集会和投票等形式进行，公民们在集会上讨论政治议题，进行投票表决。这种直接民主的形式，使得政治决策更加民主化、权力更加分散。
- 有限制的“民主”：雅典的民主与公平并不是毫无节制的公平，相反，为了保障管理机制的合理性与有效性，雅典民主制中还有一些限制政治权力的机制。例如，公民只有在完成义务的前提下才能享受权利，而义务包括服兵役、纳税等。此外，公民还必须接受审查，以确保他们的身份符合资格。这些限制机制可以有效遏制政治权力的滥用，保证政治决策的公正性和合法性。

与雅典的“小国寡民”相比，罗马帝国的中央集权化制度则显得天差地别。罗马帝国的中央集权制度在政治方面的构建是一个漫长而复杂的历程，经历了许多阶段的发展和演变。在共和时期，罗马政治制度基于贵族制和民主制相结合的模式，政治权力分散在不同的政治机构和阶层之间。但随着罗马帝国的扩张和内外威胁的增加，共和政治制度逐渐失去了有效性，政治腐败和内部分裂加剧，导致罗马陷入了动荡和混乱。于是，罗马的政治领袖逐渐意识到，为了维护帝国的长期稳定和统一，必须建立一个强大而高效的中央政府，实现政治权力的高度集中和控制。

罗马帝国的中央集权制度主要体现在皇帝对政治权力的高度控制上。皇帝不仅是政治和军事的最高领袖，还是全国官方文化的代表和宣传者。皇帝的形象与地位被广泛宣传和推广，作为罗马帝国的象征和文化标志，这种宣传和推广对维护罗马帝国的长期稳定与统一起到了非常重要的作用。此外，罗马帝国还建立了一套完善的法律制度，由中央政府制定和执行，确保全国法律和政策的一致性。

罗马中央集权制度与雅典民主政治迥然不同，清晰地昭示了人类社会组织管理的两种形态：去中心化与中心化制度，而时间也很贴心地将两种制度的优劣势通过血淋淋的历史形式告诉给我们。

罗马中央集权制度相对于雅典民主制度的优势在于其高度的集中和控制力度。罗马帝国的中央政府通过建立一个强大而高效的中央政府，实现政治权力的高度集中和控制，确保政治和行政的高效率。然而另一方面，罗马过于集中管理的政治制度使得国家机器缺乏政治自由和民主参与，政治权力过于集中和垄断，导致政治腐败和专制，而制度的僵化则成为了击碎这个“利维坦”[①]的最后一击。

与之相比，雅典民主制度的核心优势便在于其创新性与灵活性——正是因为充分尊重每一个政治个体的认知与意见，雅典民主政治治理的有效性才得以更好地发挥出来，这也是去中心化制度的核心优势所在。然而问题在于“人人发声”的政治制度仅在组织人数较少或者传播速度足够快时才能正常运转，一旦组织群体过于庞大，完全的“去中心化”将会对于组织效率形成极大的桎梏。

① 利维坦：一种威力无比的海兽，可用以比喻君主专制政体。

1.1.2 互联网 Web1.0 的诞生：媒介的去中心化赋权——从中心化到去中心化的二次转折点

当美国国防部决定启动阿帕网研究计划时，他们或许怎么也不会想到，这个为了抵御苏联核弹危机而研发的战略网络，会在未来直接改变全人类的科技发展格局。阿帕网的内核，归根到底是一种去中心化的传播机制——当某个控制中心与其他控制中心失去联系时，由于分布式传播；整个网络不会受到过大的影响，也正是在此刻，“去中心化”开始被植入进整个世界的认知当中。

彼时的阿帕网还只是一个雏形，互联网真正的开端是在 1989 年的欧洲粒子物理研究所，如图 1-1 所示。TimBerners 和其他在欧洲粒子物理实验室的人提出了一个分类互联网信息的协议，这个协议，1991 年后被称为 WWW（World Wide Web），是基于超文本协议——在一个文字中嵌入另一段文字的——连接的系统，当你阅读这些页面的时候，你可以随时用他们选择一段文字链接。至此，Web 互联网正式面世。

图 1-1 1989 年的欧洲粒子物理研究所

此后的二三十年的时间里，人类对于互联网的探索从未止步，而在摩尔定律的技术规律加成下，互联网的应用边界更是不断被

突破，成功渗透并影响着世界上的每一个角落。也有一部分人意识到，那个驱使互联网诞生的“去中心化”理念正在被这光怪陆离的虚拟世界不断消弭。怀揣着这个思想，他们成为了互联网新一轮的开拓者与革新者，而 Web1.0 时代，也正从此刻开始拉开序幕。

Web1.0 是指互联网的早期阶段，是互联网发展历程中的一个重要阶段。这个时期大约从 20 世纪 90 年代中期到 21 世纪初期，也被称为静态 Web 时代。在这个时期，互联网主要是由一些静态网站组成，网站的内容主要是文字、图片和少量的动画，如图 1-2 所示。这些网站的交互性和个性化定制程度都比较低，用户只能被动地浏览网页上的信息，无法与网站进行交互并进行个性化定制。

图 1-2 Web1.0 时代的网页

在 Web1.0 时代，网站的设计和开发主要以展示信息为主，网页的布局和设计也比较简单，一般采用静态 HTML 页面来展示内容，如图 1-3 所示。由于当时互联网技术的限制和硬件设备的限制，网站的响应速度也比较慢，用户需要等待很长时间才能打开一

个网页。此外，由于缺乏相应的技术支持和标准，网站的兼容性和安全性也存在一定的问题。

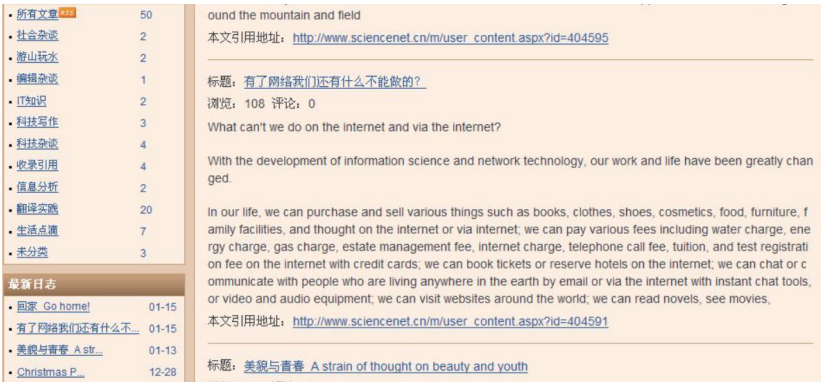


图 1-3　Web1.0 时代的网页布局

尽管 Web1.0 时代的网站交互性和个性化程度较低，但是它也为互联网的发展奠定了基础。在这个时期，互联网技术得到了快速的发展，网络基础设施得到了高速迭代，使得互联网在全球范围内得到了广泛的普及。

更为关键的是，Web1.0 为互联网的发展提供了一个全新的展示平台，改变了人们信息交流与传播的方式。在 Web1.0 互联网出现以前，人类社会的媒体传播资源被大型专业电台与企业所垄断，大众媒介信息的生产对于普通人而言几乎是触不可及的事。

但在 Web1.0 诞生之后，大众媒体的信息传播范式被迭代——尽管操作或许还有些困难，但一个普通人只需要花费一些时间和精力即可拥有属于自己的网页与博客，而这些网页与博客可被互联网的所有人看见。

Web1.0 是不完美的，但却是颠覆性的，传承了千年的中心化社会组织与生产制度，开始被互联网一点点消弭与瓦解。

1.1.3 Web2.0：媒介赋权的深度尝试——移动互联网的开拓

尽管 Web1.0 时代是一个静态的、信息消费为主的时代，用户只能被动地浏览网站上的信息，但 Web1.0 的诞生还是为互联网的发展奠定了基础，也为后来的 Web2.0 时代的网站提供了有价值的经验和启示——用媒介赋权的形式重新尝试去中心化的组织运行是可行的，这启发了人们去探索更加开放、民主、去中心化的网络模式。此后十余年间，互联网的去中心化趋势不断明晰，移动互联网与众多 UGC（User Generated Content，用户生产内容）平台的崛起让大众个体在网络中得到了更大的自主权利，“人人拥有话筒”逐渐成为现实。

Web2.0 时代的到来，使得互联网的去中心化趋势不断明晰。Web2.0 时代的“个人门户”模式是以“个人节点”为中心，关系为链接，本质特征是参与、展示和信息互动。在 Web2.0 时代，用户不再是单纯地消费信息，开始拥有了信息生产者的权利。用户在网络空间传播信息，展现自我信息和观点的同时，也无形中影响了社会信息传播和舆论导向。

用户可以通过各种媒介发布自己的信息和观点，而这些信息可以被其他用户接收、评论和转发。这种去中心化、自由化的网络环境，让个体获得了更多的话语权，也促进了信息的自由流动和互动。

社交媒体的崛起拉开了 Web2.0 时代的序幕。社交媒体的出现改变了人们获取信息和互动的方式，使得人们可以更加轻松地分享信息、建立社交网络以及与其他人互动。在 Web2.0 时代，用户不再被动地接收信息并作为内容的接收者，而是成为了内容的创造者和发布者。这种模式被称为用户生成内容（UGC）。社交媒体平台

让用户可以轻松地共享他们的想法、观点以及图片、视频和音频等多种形式的内容，而且这些内容可以迅速地传播和分享。其中，Facebook 是最具代表性的社交媒体平台之一。Facebook 让用户可以轻松地创建个人资料，分享内容并与其他人互动，包括点赞、评论和分享等。它也成为了企业和品牌营销的一个重要平台，例如，许多企业和品牌会在 Facebook 上创建官方页面，通过发布内容和与粉丝互动来提高品牌知名度及产品销售量。

紧接着，苹果手机的发布加速了移动互联网的时代革命，大众的媒介赋权被提升到了一个全新的高度。苹果的 iPhone 于 2007 年发布，如图 1-4 所示，这款智能手机引领了移动互联网时代的到来。iPhone 的操作系统 iOS、触摸屏技术和应用程序生态系统，使得用户可以方便地使用各种应用程序，实现多种功能，这些功能包括：社交媒体、搜索引擎、电子邮件、在线购物、地图和导航、游戏等。iPhone 的成功让用户可以在任何时间、任何地点使用互联网，扩大了人们获取信息和互动的范围，改变了人们的生活方式。

图 1-4　乔布斯与苹果手机发布

此外，一批新兴的互联网企业正在崛起。他们凭借数据、技术与资本优势，获得了整个 Web1.0 到 Web2.0 的时代红利，最终成为新一代的互联网巨头。这些新兴的互联网企业包括了谷歌、

Facebook、亚马逊、阿里巴巴等公司。这些公司在 Web1.0 时代就已经开始发展，他们的创始人拥有敏锐的商业嗅觉和技术能力，在当时互联网行业的空白中迅速崛起。这些新兴互联网企业的崛起，推动了全球数字经济的发展，也对传统行业和企业造成了冲击。随着互联网的不断发展和创新，这些企业也在不断地进行战略调整和创新，以适应新的市场和技术环境。

1.2 痛点分析：Web3.0 之前——中心化的网络出现了什么问题

1.2.1 不可避免的单点故障

在传统互联网架构中，大多数应用和服务都是通过中心化的服务器提供的。这种中心化架构存在一些问题，其中最严重的是单点故障。在这种架构下，少数的中心化服务器承担着大量的服务和应用，一旦这些服务器出现故障或遭到攻击，就会导致整个服务和应用无法正常运行。发生单点故障后，用户将无法访问服务和应用，甚至可能会造成严重的经济损失。

出现单点故障不仅仅是因为中心化服务器的数量较少，还因为这些服务器通常是由少数组织或企业所掌控和管理。这些组织或企业可能会出于自身利益考虑，对服务和应用进行限制或控制，从而影响用户的自由和权利。此外，中心化服务器集中在少数机房或地区，存在地理位置集中的问题，该问题也会导致服务和应用在某些地区的访问速度较慢或不稳定，从而影响用户体验感和满意度。另外，中心化服务器的集中也会导致资源浪费和能源消耗。由于服务器需要大量的电力和空间来运行和维护，中心化架构可能会导致能

源浪费和资源浪费的问题。

1.2.2 中心化的数据垄断危机

除了单点故障外，中心化架构还存在另一个严重问题，即中心化服务器由少数机构控制和管理，这些机构通常拥有对用户数据和资产的控制权，一旦这些机构出现问题，就会给用户的数据和资产带来很大的风险。

首先，黑客可以攻击中心化服务器，并窃取用户数据和资产。这种攻击可能会导致用户的个人信息、支付信息和其他敏感信息泄露，使用户遭受经济损失和信用风险，这对于金融、电子商务、社交媒体等产生严重影响，因为这些应用通常需要用户输入大量的个人信息和支付信息，一旦这些信息泄露，用户将面临极大的风险和损失。

其次，中心化机构可能会滥用用户数据和资产，对用户的隐私和权益造成侵犯。这种滥用可能包括出售用户数据、擅自使用用户数据、向第三方泄露用户数据等行为，这些行为可能会导致用户的隐私和权益受到侵犯，对用户产生不良影响。例如，某些公司可能会收集用户的浏览记录、搜索记录、购物记录等信息，然后将这些信息出售给广告商或其他第三方，从而产生侵犯用户隐私和权益的现象。这种滥用用户数据和资产的行为，可能会导致用户失去对自己数据和资产的控制权，从而对用户的自由和权益产生负面影响。

另外，中心化机构可能会因为经营不善、违法犯罪或其他原因而破产或关闭，导致用户的数据和资产遭受损失。例如，用户在某个中心化交易所购买了加密货币，但该交易所由于经营不善或其他原因破产或关闭，导致用户的加密货币无法取回而遭受损失。如遇

到这种情况，用户将面临无法收回自己的资产、无法获得赔偿或补偿等风险。

而比技术问题更为严重的，是个人数据主权的保护问题。

1.2.3 个人数据主权的保护失效

在传统互联网架构中，用户的数据和资产通常存储在中心化服务器中，由少数机构控制和管理。这种集中化的控制存在一些问题，其中最为严重的是安全和隐私隐患问题。由于用户的数据和资产集中存储在少数中心化服务器上，一旦服务器出现问题，例如被黑客攻击、遭到破坏或出现故障，用户的数据和资产就会受到威胁。这将导致用户的数据和资产无法得到保护，甚至可能遭受损失。例如，2017 年，Equifax 公司就因为其服务器被黑客攻击，导致超过 1.4 亿用户的个人信息泄露，给用户带来了巨大的经济和信用风险。

除了安全问题之外，集中化控制还可能导致用户的隐私和权益被侵犯。这些机构可能会滥用用户的数据和资产，例如出售用户数据给第三方、将用户数据用于商业行为或者滥用用户数据进行广告投放等。这些行为可能会对用户的隐私和权益造成侵犯，特别是在用户没有授权的情况下使用其数据和资产，会让用户感到不安和不满。此外，集中化控制也可能导致机构或个人滥用权力，例如篡改或删除用户数据等行为，这将导致用户数据与资产受到威胁或遭受损失。

集中化控制还可能导致数据与资产的不可控。由于用户的数据与资产存储在中心化服务器上，用户无法直接控制和管理自己的数据与资产。这可能会导致用户无法保障自己的隐私和权益，也无法对自己的数据与资产进行有效的控制和管理。

1.2.4 信息茧房与围墙花园

美国学者尼葛洛庞帝，在 20 世纪 90 年代提出的“我的日报”概念，已经在今天的数字化时代成为现实。个人用户可以通过社交媒体、新闻应用、其他在线平台获取为他们量身定制的新闻、文章、娱乐和其他信息。这种个性化的服务不仅能够满足用户的需求，还能帮助用户更好地掌握信息并与他人分享和交流。

尼葛洛庞帝提出的概念揭示了数字化时代个性化信息服务的趋势和潜力，随着互联网技术和数字化的发展，个人用户将能够享受到更加符合自己兴趣和需求的定制化信息服务。

越来越多的互联网企业和应用程序开始采用个性化算法及推荐系统，为用户提供符合其兴趣和需求的信息服务，其中的佼佼者——字节跳动更是凭借抖音与今日头条荣登新一代的互联网巨头宝座。

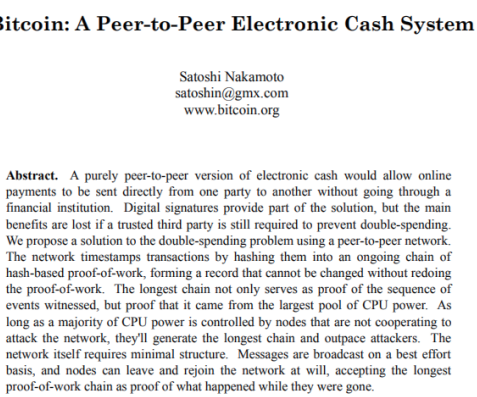
但这种极具个性化的信息推荐方式对大众真的友好吗？网络社区超越了物理和地理的限制，提供了与志同道合的人保持联系的新机会，还能够避免与不感兴趣的人和事接触。但如果人长期倾听与自己相像的观点，会变得更加极端和自信，甚至可能发生群体极化、两极分化。而这种情况导致我们生活在虚幻的“奶头乐”中，而 Web2.0 并不允许我们去打破这个虚幻的美梦。

1.3 从中本聪到以太坊——Web3.0 如何从区块链中诞生

1.3.1 中本聪与比特币：Web3.0 真正意义上的起点

2008 年的一天，一位名叫中本聪的用户在某个密码学交流社区上发布了一篇名为《比特币：一种点对点式的电子现金系统》论

文，如图 1-5 所示，并在该论文中提出了一种无须可信第三方的电子支付系统——比特币，它的发行总量为 2100 万枚，且永不增发。这篇论文的发布，标志着 Web3.0 时代从此刻开始启航。



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 1-5　中本聪跨时代意义的白皮书

在这篇论文中，中本聪对比特币的技术原理与设计思想进行了清晰的阐述，虽然全文不过 9 页，但去中心化的颠覆式思想已经跃然纸上。关于比特币的技术原理，中本聪对从生产、流通到记录的种种流程进行了详细的模型解释。

（1）比特币的生产。

比特币的生产是通过“挖矿”（Mining）这一过程实现的。挖矿的本质是利用计算机程序解决一个复杂的数学题，也被称为“工作量证明”（Proof of Work，PoW），以验证交易并将新的区块添加到区块链中。挖矿需要消耗大量的计算资源和能源，因此挖矿的难度会随着时间的推移而逐渐增加，以保持比特币供应的稳定性。根据中本聪的设计，比特币的总量为 2100 万枚，并且不会增发。

（2）比特币的交易。

比特币的交易是点对点的，也就是说，用户可以直接将比特币

转移给其他用户，而无须经过任何中介机构。比特币的交易是由比特币网络中的节点共同维护的，每个节点都会对交易进行验证，并将其广播到全网中。

（3）比特币的交易验证。

当一笔比特币交易发生时，该交易将会被广播到全网的节点中，并由节点进行验证。节点通过比对交易数据和交易历史记录，以确保交易的真实性和合法性。如果交易被验证通过，则会被记录到一个新的区块中，并被加入区块链中。

（4）比特币的交易记录。

比特币的交易记录是由区块链技术实现的。区块链是一种去中心化的公共账本，用于记录比特币网络中发生的所有交易。每个区块包含一定数量的交易记录，每个区块都有一个唯一的标识符，并按照一定的顺序连接在一起，形成一个链条。区块链的去中心化特点意味着没有任何一个人和机构可以单独控制或篡改其内容，这是比特币网络的一个重要优势。

2009 年 1 月 3 日，中本聪将比特币的设想落地到了现实，创立了区块链上的所谓“创世区块”。比特币是一种去中心化、开放式、匿名性的数字货币，它不依赖任何中央机构或第三方信任机构，而是通过区块链技术实现点对点的交易和账本管理。比特币的创造者中本聪提出了一套完整的区块链协议和加密算法，保证了比特币的安全性和去中心化特性。

比特币使用区块链技术实现账本的分布式存储和管理，每个节点都可以参与区块链的维护和交易。另外，比特币的开源性也是货币经济学的一种突破性尝试。比特币使用开源代码，任何人都可以查看比特币的代码和技术，从而提出改进建议和参与比特币的发展与运营。

比特币的出现，是对传统金融制度和货币体系的挑战，它通过去中心化的方式，实现了点对点的交易，没有中心化机构参与其中，使得交易更加安全、透明和高效。比特币的技术基础是区块链，区块链是一种去中心化的数据库技术，能够确保数据的安全性和不可篡改性。区块链的出现，彻底颠覆了传统的中心化数据库管理方式，为全球数字经济的发展开辟了新的道路。

如果仅仅是在金融领域进行革新，或许并不能很好地体现出比特币和区块链的创新价值。比特币和区块链最大的价值，是让世界看到了一条鲜有人尝试的去中心化路径——用密码学来解决信任与管理问题。区块链技术提供了一种基于密码学、分布式共识、不可篡改性的新型数据结构和算法，这种技术可以让用户在不需要第三方信任机构的情况下进行安全可靠的信息传播。

比特币的成功证明了区块链技术的可行性，为 Web3.0 的发展提供了重要的技术支持。相比于虚无缥缈的“郁金香”金融骗局，伴随着比特币一起出现的区块链技术，才是让人类生产方式发生另一种变革的启明星所在。

比特币在国家层面的应用探索

- 阿根廷：由于阿根廷的通货膨胀率较高，许多人开始使用比特币作为一种防止通货膨胀的手段。2018 年，阿根廷的通货膨胀率超过了 40%，这使得人们开始寻找一种能够保护其财产免受通货膨胀影响的方式。比特币作为一种去中心化数字货币，不受政府和央行的控制，因此被认为是一种抗通货膨胀的投资工具。此外，由于比特币的交易速度快、手续费低且可以进行跨境汇款，许多人开始将比

特币用于跨境汇款，以避免央行汇率和汇款手续费的高昂成本。比特币的匿名性和去中心化的特点，也有助于保护用户的隐私和安全性。因此，越来越多的人开始将比特币作为一种抗通货膨胀的投资工具和跨境汇款的支付方式。

- 日本：2017 年 4 月 1 日，日本政府正式承认比特币作为一种合法的支付方式，这使得比特币在日本的应用得到了进一步推广。根据日本的法律规定，比特币被视为一种资产或商品，而不是货币。这意味着，比特币交易需要缴纳消费税，但不需要支付所谓的货币交换税。这一政策的推出，促使比特币在日本的普及和接受程度的提高。一些日本商家也开始接受比特币付款，包括餐厅、超市和电子商务网站等。例如，日本的一些餐厅和咖啡馆开始接受比特币付款，并且在菜单上标注了比特币的价格。此外，日本的一些电子商务网站也开始接受比特币付款，例如日本的亚马逊和乐天市场等。
- 委内瑞拉：委内瑞拉的通货膨胀率长期较高，导致人民的财产受到了严重的侵蚀。为了保护财产，一些人开始将比特币等加密货币作为一种抗通货膨胀的投资工具。由于比特币的去中心化特点，使其不受政府或金融机构的控制，因此被认为是一种安全的财富保值方式。2018 年，委内瑞拉政府推出了一种名为“石油币”的数字货币。石油币与委内瑞拉的石油储备挂钩，一定数量的石油币可用于购买石油和其他商品。政府希望通过推出石油币来促进国内经济发展，同时减轻人民的通货膨胀压力。然而，石油币的推出并没有得到广泛的认可和接受。

由于委内瑞拉政府一直存在信用危机和政治危机，石油币的可信度和稳定性受到了质疑。相比之下，比特币等加密货币因为其去中心化特点和全球性的接受度，更受人们信任。

- 美国：比特币在美国的应用也相对较为广泛，一些知名企业和机构也开始探索比特币的应用，例如 PayPal、微软、星巴克等。此外，比特币也被用于购买房产和艺术品等高价值商品。如 PayPal 于 2020 年 10 月宣布将支持比特币等加密货币的买卖和使用。这意味着 PayPal 的用户可以使用比特币等加密货币进行在线支付，也可以将比特币等加密货币转换成法定货币存入 PayPal 账户。

1.3.2 Vitalik 与以太坊：用共识搭建 Web3.0 的应用生态创新

中本聪与他的比特币成为互联网迈向去中心化世界的第一步，他的论文和发明激发了人们对区块链技术的兴趣和研究。比特币的出现，标志着 Web3.0 时代正式启航，这种去中心化的数字货币为全球数字经济的发展开辟了新的道路，也正如中本聪自己所言，比特币是一个完完全全的去中心化系统，以至于他自己都没有 100% 的权利对比特币作出决定。

尽管大众很期待中本聪能对比特币系统或其应用层面进行更深层次的创新，但事实上中本聪本人也在文章发表后一直处于一种半消失的状态。同时，比特币生态的发展往往是由社区力量来推动的，这种去中心化的模式虽然具有一定的优势，但也带来了一些问题。例如，比特币的扩容问题、网络安全问题、治理问题等，都需要社区共同协作来解决，但在缺乏前期社区规划和领导者的情况

下，想要让大众自行形成一个完备的组织体系显然是不现实的，这也体现了去中心化社区的弊端。

当对去中心化货币应用的需求开始涌现时，历史必然会把革新者放在一个合适的位置，而这一次的幸运儿便是 Vitalik 与以太坊，如图 1-6 所示。

图 1-6　以太坊，实现更具有功能性的生态应用

2013 年，Vitalik Buterin 发布了一篇名为《以太坊：下一代加密货币和去中心化应用平台》的白皮书，其中详细阐述了以太坊的愿景和设计原则。Vitalik Buterin 在白皮书中指出，比特币虽然是一种非常成功的去中心化电子现金系统，但其功能仍然受到了限制。比特币只能进行简单的交易，无法实现更复杂的应用程序。而以太坊的目标是打造一种更为通用的去中心化应用平台，使得开发者可以构建各种类型的应用程序，并将其部署到区块链上。

在以太坊白皮书中，Vitalik Buterin 对于去中心化应用生态的组成进行了详细且富有想象力的描绘，并在白皮书中首次提出了智能合约与去中心化应用等经典 Web3.0 概念。而在治理方面，以太坊同样沿用去中心化的治理架构，不依赖中央机构或第三方信任机构，整体决策是由社区中的参与者共同决定，从而保证了去中心化和分散治理的原则。

以太坊的关键技术与应用概念

- 智能合约：以太坊的智能合约是一种可以自动执行的计算机程序，它们存储在区块链上，并由以太坊网络中的节点执行。智能合约可以实现各种复杂的业务逻辑，如转账、投票、协议、预测市场等。相比于传统合约，智能合约的最大特点及优势便是其自动性与去中心化特性。智能合约通过区块链技术实现自动化执行，避免了传统合约需要人工介入的问题。这使得智能合约具有更高的效率和准确性。同时，智能合约的执行结果和代码都将永久存储在区块链上，不可篡改，这将极大地保证智能合约的安全性。
- 去中心化应用：去中心化应用是指基于区块链技术的应用程序，其核心特点是去中心化和不可篡改。以太坊的目标是成为一个开放、透明、安全、可扩展的专门用于构建去中心化应用的平台。以太坊为开发者提供一个可编程的区块链平台，使得开发者可以构建各种类型的应用程序，并将其部署到区块链上。
- Solidity 智能合约语言：Solidity 是一种高级语言，类似于 JavaScript 或 Python，它可以用于定义各种数据类型、函数、类、结构体等，从而实现各种复杂的智能合约业务逻辑。其语言特点是简单、安全、可靠、可扩展。它支持面向对象编程，可以定义类、继承、接口等，同时还支持事件、异常处理、库等特性。Solidity 语言代码可以被编译成 EVM（以太坊虚拟机）的字节码，在以太坊网络上执行。
- 以太币（ETH）：以太坊是一个区块链平台，其本地加密货币是以太币（Ether），也被称为 ETH。以太币是以太坊网络中的基础货币，是实现去中心化应用和智能合约的重

要基础。按照官方设定，以太币的供应量是有限的，总量为 1 亿个，且随着时间推移，以太币的发行量会逐渐减少。以太币的价格是由市场供求关系决定的，随着以太坊平台的发展和应用场景的不断拓展，以太币的价格也在不断变化。

- 以太坊虚拟机（EVM）：以太坊虚拟机是以太坊网络中的计算引擎，是实现智能合约的核心组件之一。EVM 是一个基于栈的虚拟机，其指令集包括各种算术运算、比较运算、位运算、逻辑运算等。EVM 可以根据智能合约的代码自动执行各种操作，例如转账、存储数据、触发事件等。另外，EVM 还提供一种名为“油费”的机制，用于限制智能合约的执行次数和效果。

以太坊自 2015 年上线，至今已经成为世界上最大、最活跃的去中心化平台之一。以太坊网络由全球各地的节点共同维护，这些节点遍布全球，共同维护着以太坊的区块链的底层数据运转。截至 2023 年 2 月，官方数据显示，以太坊网络有 1.3 万至 1.4 万个节点，这些节点在维护以太坊网络的同时，也保护着网络的安全性和去中心化特性。在应用生态方面，以太坊上有超过 4000 个去中心化应用（DApps），包括去中心化金融（DeFi）平台、去中心化交易所（DEX）、NFT 市场、游戏、市场预测工具等。这些应用程序不仅可以实现区块链技术的价值传递，还可以为用户提供更多的服务和体验。特别是在去中心化金融领域，以太坊生态系统中的各种应用程序，为参与者提供了更加安全、高效、低成本的金融服务，使得金融领域的创新和进步更为快速与便捷。如图 1-7 所示为以太坊官方网页。

图 1-7 以太坊官方网页

除了构建去中心化应用程序，以太坊还支持发行和交易非同质化代币（Non-Fungible Token，NFT），这种数字资产在以太坊生态系统中得到了广泛的应用。NFT 可用于艺术品、音乐、游戏及其他数字内容的所有权证明和交易，这种数字资产的出现，为数字内容的所有权和交易提供了更好的保障及便利。

当前，以太坊正在进行一系列升级，以实现更高的性能、安全性和可扩展性，这些升级被称为以太坊 2.0（ETH 2.0）。ETH 2.0 的主要升级包括从工作量证明（PoW）共识机制切换到权益证明（PoS）共识机制，以及引入分片技术来提高交易吞吐量。ETH 2.0 预计将在未来几年逐步推出。