从区块链到 Web3

黄华威，杨青林，林建人，郑子彬 著

2023 年 1 月 17 日

人民邮电出版社，暂定 2023 年 4 月出版

三分之一篇幅抢先版

感谢关注！

目录

作者简介

黄华威：中山大学“百人计划”副教授，博士生导师，IEEE 高级会员，中山大学“区块链与智能金融研究中心”副主任，中国计算机学会 (CCF) 区块链专委会执行委员、分布式与并行计算专委会执行委员。2016 年取得日本会津大学“计算机科学与工程”博士学位；曾先后担任日本学术振兴会特别研究员、香港理工大学访问学者、日本京都大学特任助理教授。研究方向包括区块链底层机制、区块链系统与协议、Web3 与元宇宙。研究成果发表在 CCF A 类期刊 IEEE Journal on Selected Areas in Communications（JSAC），IEEE Transactions on Parallel and Distributed Systems（TPDS），IEEE Transactions on Mobile Computing（TMC）与 IEEE Transactions on Computers（TC）等，以及 CCF 推荐 A / B 类国际学术会议 INFOCOM、ICDCS、SRDS、IWQoS 等。曾担任 CCF 推荐 A 类期刊 IEEE JSAC 的区块链专刊的客座编辑（lead guest editor）。主持科技部和广东省重点研发计划课题，主持国家自然科学研究基金面上和青年项目、CCF-华为胡杨林基金区块链专项项目，以及多项广东省和广州市科技计划项目。

杨青林：中山大学助理研究员，IEEE 会员（IEEE member）。2021 年 3 月取得日本会津大学计算机科学与工程博士学位。研究方向包括智能边缘云，深度学习，联邦学习隐私保护，Web3。发表 10 余篇国际期刊与会议论文。曾担任 IEEE Open Journal of Computer Science (OJ-CS) 专刊客座编委成员。参与多项国家重点研发计划课题、国家自然科学基金面上项目的研发工作。

林建人: 资深程序员，在去中心化系统、智能合约语言与虚拟机的设计与实现方面拥有丰富经验。《高伸缩性系统》中文版译者。唬米科技创始人，同时也是中山大学区块链实验室技术指导。访问 https://github.com/Jianru-Lin/ 可以了解他的开源项目。

郑子彬: 中山大学计算机学院教授，软件工程学院副院长、国家优秀青年科学基金获得者、IEEE Fellow、ACM 杰出科学家、国家数字家庭工程技术研究主心副主任、区块链与智能金融研究中心主任。出版 Springer 英文学术专著 2 部、发表论文 200 余篇，论文谷歌学术引用超过 26000 次。获得教育部自然科学二等奖、吴文俊人工智能自然科学二等奖、青年珠江学者、ACM 中国新星提名奖、国际软件工程大会（ICSE）ACM SIGSOFT Distinguished Paper Award、国际 Web 服务大会（ICWS）最佳学生论文奖等奖项；担任数十个国际学术会议的程序委员会主席。

编写委员会其他成员

罗肖飞: 中山大学访问学者，获得日本会津大学“计算机科学与工程”硕士、博士学位，曾参与日本文部省 RFID（无线射频标识）项目的研发等相关工作。目前的研究方向为区块链、支付通道网络，强化学习等等。相关研究成果发表在 CCF A 类期刊 JSAC 及其他知名国际期刊与会议。罗肖飞博士贡献了本书的关于数字加密货币相关章节的写作。

李涛涛: 博士，现任职于中山大学软件工程学院副研究员职位，研究兴趣包括区块链理论与技术应用、应用密码，具体包括侧链技术、跨链协议、轻量级区块链、密码工具在区块链中的应用。参与多项国家/省部级重点研发计划课题，近年来在 CCF 推荐国际学术会议和期刊上发表论文多篇。李涛涛博士贡献了本书关于跨链协议相关章节的写作。

序言

笔者在构思这本书时预设了一个定位：在内容方面我们力求跟市面上大部分关于 web3、区块链与元宇宙的技术书籍都不一样。笔者并不寻求将区块链与 web3 相关的内容“一网打尽”，而是着重于对 web3、区块链与元宇宙的生态方面做出深入思考、总结与展望，以期在这些被誉为“下一代互联网”的技术范式被大众认知的早期阶段，就去启发大众探讨这些技术背后的社会意义。

内容安排方面，本书总共包括六个部分。

第一部分标题为“聊聊 web3”，包括 2 个章节。第 1 章从 web1 与 web2 的发展出发，进而引出 web3 的定义、流派与技术栈，以及 web3 与 web1、web2 的区别等等方面。第 2 章主要讨论 web3 的社会意义。

第二部分主要概述区块链技术与应用，包括 3 个章节。第 3 章从区块链技术的概述出发，引出第 4、第 5 章区块链的两大最有价值的应用形式：数字货币与非同质化通证，并深入讨论二者之间的关系。

第三部分阐述为什么元宇宙不只是虚拟游戏那么简单，内容包括 2 个章节。第 6 章介绍元宇宙基本概念，并结合 AI 技术及区块链讨论元宇宙的发展阶段、核心技术、经济系统、与 AI 技术的融合。第 7 章探讨对元宇宙行业的思索，话题包括行业重要事件的观察与观点、对元宇宙的风险进行解析、探讨元宇宙普通用户与投资人的参与方式与布局的机会。

第四部分回答一个问题：去中心化自治组织（DAO）是什么？内容上包括 3 个章节。第 8 章主要介绍 DAO 的定义和技术架构。第 9 章展示对国内外有代表性的 DAO 项目实践案例的调研发现。第 10 章探讨 DAO 的现存问题，并解析 DAO 未来可能的发展演化趋势。

然后，第五部分探讨 Web3 与区块链的生态，内容包括三个章节。第 11 章从宏观的角度重点探讨 Web3 生态如何“统领全局”，话题包括 Web3 范畴、与区块链的关系、NFT 与元宇宙的关联、web3 与 DAO 的关系、分布式存储、数字身份、如何发展 NFT 产业、以及元宇宙在教育行业的尝试等内容。第 12 章用来回顾区块链生态。特别地，本章对区块链“通证经济”框架之下最新的技术趋势进行梳理，如 Layer1、Layer2 与 Layer3 技术与跨链技术等，也顺带聊了区块链企业 50 强榜单的话题。第 13 章对 web3 与区块链的生态进行综合的总结与展望，比如对比国内外区块链生态发展的路线，展望区块链的下一个五年趋势，并结合国内的政策进行解读国内如何发展 web3 行业。

最后，在第六部分，本书还提供了一个「附录」，选取一部分具有代表性的区块链、web3 与元宇宙的项目、平台、工具、以及重要的参考文献，等等。

本书最大的特点，不是包罗万象，不是把所有的基本知识点都收罗进来，而是带着警惕与批判的眼光对 web3、区块链、与元宇宙行业演化过程中存在的问题进行审视，对蕴含的风险进行剖析，对潜在的机会进行发掘。在帮助读者了解必要概念的同时，理清这些概念之间的关系，警示行业风险，

帮助读者掌握从区块链到 web3 的发展脉络，避免陷入对科技新潮流的盲目跟风。

假如本书的读者对区块链技术原理有一定的了解，那么，读者朋友将会对本书讨论的一些话题会更容易产生共鸣感。所以，为了更好里理解本书所探讨的话题，笔者建议读者预先学习一些区块链的基础知识，比如区块链的底层架构，共识协议，智能合约等等相关的知概念。

本书在写作过程中，得到了很多专家学者的关心与指导。在此，笔者衷心感谢各位专家学者的热心指导与提出的宝贵修改建议。特别感谢全体编辑委员会成员为本书所做出的贡献。

笔者希望通过本书能激发读者朋友积极探索适合于国内 web3 生态发展的路径，并带着开放的心态去思考 web3 可能带来的社会价值。

黄华威
2022 年 12 月 23 日

Part I

聊聊 WEB3

第 1 章　从 Web1 到 Web3

导读：本章节我们首先介绍 web3 的起源与演化历程，然后介绍 web3 的定义、流派，以及对其未来发展趋势的讨论。

1.1　WEB1.0 与 WEB2.0

互联网经过 30 年的发展，经历了从 web1.0 到 web2.0 的重大变革。Web1.0 诞生于九十年代，其主要特点在于用户通过浏览器获取消息；而 web2.0 诞生于 2004 年前后，更注重用户的交互。简单来说，web1.0 到 web2.0 的转变，是从“只读”模式向“读写”并存模式的转变 [1]。Web3 注重的则是“读-写-并且拥有”，“用户对自己数据的所有权”是 web3 最大的特征之一。Web2.0 时代，用户参与内容建设，但是用户的数据和隐私却被互联网巨头占有，用户几乎没有得到自己的数据带来的收益。Web3 更强调帮助用户参与者将数据掌握在用户手中，帮内容贡献者更公平地兑现他们的劳动价值。

在 web2 时代，互联网巨头带来垄断的问题。Web1.0 和 web2.0 本质都属于中心化网络，由各大互联网厂商和公司的服务器占据着网络中心位置。随着网络规模的扩大，中心化网络模式会带来一系列的问题，例如：

- 2017 年亚马逊 AWS 的网络故障导致了美国数百家网站服务瘫痪。

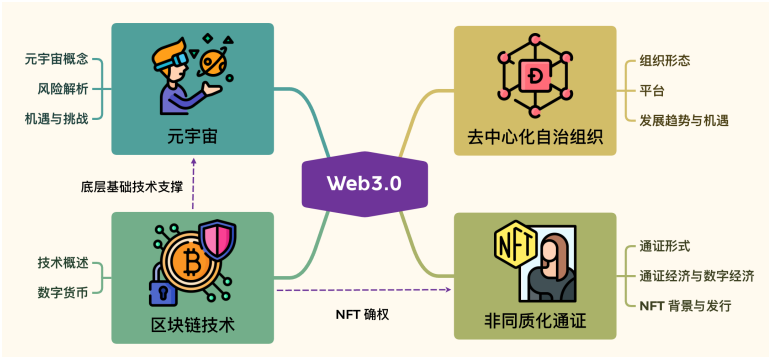

图 1: 本书主要涉及的几个概念之间的脉络关系

- 另外，中心化的中介平台的存在产生了不合理的利益分配，平台获得了比用户更多的利益。

- 互联网巨头通过用户数据创造天量级价值，但用户自己却几乎没有获得任何收益。

- 此外，不透明的互联网在用户隐私保护方面的问题也日趋严重。

因此，web3 逐渐被人们所关注与了解。Web3.0 最早在 2006 年被 Jeffrey Zeldman 提出，而与区块链相关的 web3 概念是由以太坊联合创始人 Gavin Wood 于 2014 年提出。区块链由于具备去中心化分布式存储、以及链上数据可信等等属性，逐渐成为构建 web3 的天然基础设施 [2]。

1.2 WEB3 的定义

Web3 的字面的意思它是被翻译为第三代互联网，目前并没有一个明确的定义。人们可以将它描述为基于区块链技术的去中心化的互联网技术的合集。在这个合集中有新的技术与范式，还有新的组织形式及对应的价值观与世界观。

Web3 这个名词最早是由 HTTP 的发明者叫 Tim Berners-Lee，在互联网泡沫时期提出的，它指的是一个集成的通信框架，互联网数据可以跨越各个应用和系统，实现机器的可读 [3]。

这里笔者简单介绍一下 Tim Berners Lee。他是英国的计算机科学家，被誉为万维网之父，2016 年获得了图灵奖。我们从刚才他所定义的 web3 的概念可以看出来，这个概念是相当有历史感的。因为在他当年的定义中仅仅出现了“通信框架”，以及跨越各个应用与系统实现机器的可读。

其实，我们今天所讨论的 web3 的概念已经跟 Berners Lee 当初提出的概念完全不一样了。现在我们所说的 web3 是指什么呢? 它其实是指 2014 年以太坊的联合创始人、Plokdot 的创建者 Gavin Wood 在一篇名为《DApp：web3.0 是什么?》[4] 这篇博文中给我们重新定义了 Berners Lee 提出的这个词。Gavin Wood 所定义的 web3 是指一种区块链技术，它可以基于无需信任的交互系统，在各方之间实现创新的交互模式。这里所说的“无需信任的交互系统”，其实就是指区块链技术支撑之上的一种系统。

我们再来看一下 web3 的其他观点。一名传统投资合伙人认为 web3 是指基于区块链技术的去中心化在线生态系统。

许多人认为它代表了互联网的下一个阶段，目前的 web3 行业很像 2000 年左右的互联网。这是因为目前 web3 行业逐渐问世了一些雏形产品，比如被视为去中心化的“支付宝” Metamask，就是以小狐狸为头像的一个去中心化的钱包工具；被视为去中心化 QQ 音乐的 Audius；以及全球最大的 NFT 交易平台 Opensea，等等。这些去中心化的应用已经在全球范围内吸引了千百万的用户，这些应用背后的公司也逐渐成为全球最具影响力的公司。

接下来，我们再梳理一下从 web1.0 到 web3 的发展演化路径。最早 web1.0 起源于 1990 年附近。当时比较有代表性的应用是以桌面浏览器才能访问的门户网站，比如说维基百科。当时比较流行的国内的门户网站包括雅虎与新浪这些老一辈的门户网站。可见这些 web1.0 时代的网站，最大的特点就是“可读”或者叫“只读”。因为用户只能被动的从这些网站上获取信息，网站并没有提供一个给用户进行与之交互的渠道。

在 web2.0 时代，网站与应用出现了一些新的变化。最大的变化就是从“可读”模式变为了“可读加可写”模式。比如以博客、推特、微信、抖音这些为代表的新一代的应用，它们的内容可以由用户自己生产，然后这些平台还提供多种多样的用户与平台之间、或者用户与用户之间进行交互的方式与手段。所以，web2.0 的最大的特点是“可读加可写”。

到了 web3，在“可读加可写”模式的基础上又出现了一个新的特性，就是“拥有”。这个“拥有”是指用户产生的内容数据可以由用户自己所主宰。就是说用户对自己的数据具有主权。而不像 web2.0，由用户生产的数据的所有权被平台和

寡头所控制着。可见从 web1.0 到 web3，经历的是底层逻辑的变换。因此，在前后端生态方面会蕴含着产生翻天覆地变化的可能性。究其原因，主要有以下几点：web1.0 与 web2.0 被视为信息互联网，而 web3 则可以被看作是一个价值互联网。Web1.0 与 web2.0 本质是在传递信息，侧重数据或者信息的消费，而 web3 则是在传递着价值以及创造财富。这里的“创造财富”是指用户自己的数据可以创造收益。但是，问题是这些创造的财富是否能回到用户自己手中。这个问题也给 web3 的开发者与创业者提出了一个新的要求：他们需要通过技术手段来保证用户自己创造的价值能够被保护，能够被最终传递到用户手中。因此，一些热切拥抱 web3 的开发者认为当前所有的 web2.0 的应用都值得在 web3 的背景下重新做一遍，从而升级为对应的 DApp。

1.3 WEB3 的流派

Web3 流派是指把对 web3 感兴趣的爱好者或者从业者分为一些类别。这里我们把他们大概分为 5 组，或者叫 5 个圈子，分别是“数据所有权派”、“币圈、链圈派”，“极客技术派”，还有“概念炒作派”，最后是“政商界的 web3 人士”。接下来我们逐个展开解释一下。

第一个流派就是拥护数据所有权的一派人。这一派秉承打破数据垄断与数据独裁的理念，进行保护 web3 应用生态中用户的权益。

第二个流派是指币圈与链圈。他们更多时候所关注的是价值网络，即依靠各种加密货币投资与投机的金融市场。

第三个流派叫做技术极客圈，比如一部分 web3 的技术爱好者想要建立一些去中心化的社区，比如去中心化的知乎。用户在这些去中心化的社区可以发布一些创作者的权益可以被保护的文章。其他形式的社区还包括去中心化的信息网络，可支持发布一些作者或编剧的权益受到保护的一些影视作品或新闻。

下一个流派就是概念炒作派。他们主要的诉求就是炒作各种与 web3 相关的新兴概念，然后从中获取一些利益。比如炒作跟元宇宙相关的一些概念。但是，他们炒作的题材大多时候跟 web3 没有太大的联系。

最后一个流派就是政商界的相关的人士了。这一部分人士可能是出于对某些下发的政策的拥护，不得不积极地了解与学习 web3 业界的相关需求，以及将来发展的前景，然后积极地与前面提到的几个流派进行密切的交流与合作。这种现象当然是好事，至少连这些保守的政商界的人士都看到了 web3 这个时代浪潮的巨轮正在滚滚向前。无论将来国内的“去中心化经济”是使用数字人民还是使用某种合法的代币来计量价值，总之会出现一种法律允许的价值承载工具来疏通面向 web3 与元宇宙的经济系统。政商界人士所期待的 web3 业态如果发展到技术极客派所期望达到的程度，我觉得国内 web3 的生态便会迸发出勃勃生机。

正如一句话说的那样，“不管你是否喜欢，该向前的不会后退”。Web3 各派人士正在悄然展开密切交流与合作。国内的 web3 生态迟早有一天也会枝繁叶茂、大树参天。

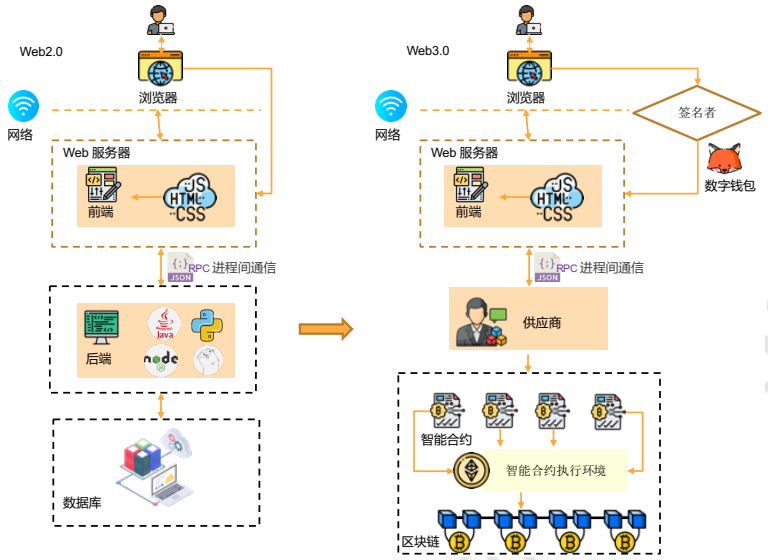

图 2: Web2 与 Web3 开发技术栈对比

1.4 WEB3 的技术栈

本小节介绍 web3 的开发技术栈，以及对比一下与传统“客户端-服务器”模式的技术栈的区别。

首先，我们回顾一下传统的“客户端-服务器”这种形式的技术栈，前端是客户端的浏览器或者 APP，它们使用 HTML 或者 CCS 或者 JavaScript 来实现前端的呈现形式。然后，后端就是服务器。那么，Web3 形式的 APP 或者叫去中心化应用（Decentralized APP，DApp），它们的开发技术栈长什么样呢?

其实，如图 2 所示，web3 的开发技术栈的前端跟传统的 web2 的“客户端-服务器”形式的开发技术栈的前端是一样

的，只是后端从传统的数据库变成了区块链。然后，中间还会有一个 web3 的 service provider，即 web3 服务的提供商，提供一些与 web3 相关的一些功能，比如说 web3 的钱包与身份管理工具。这个钱包的一个例子就是以小狐狸为 logo 的 metamask [5]。

我们进一步分析 web3 形式的开发技术栈。首先是前端，开发者可以开发手机端使用的 DApp，或者开发可以与钱包进行交互的前端呈现的页面。然后，后端如果是需要与大量链下数据进行交互的话，这些数据可以存储在 IPFS（这是一种安全的分布式存储产品）[6]。

如果某些 web3 的 DApp 的业务比较复杂，可能就要借助智能合约来实现。此时需要把相关的智能合约部署在某个支持智能合约的区块链上，如以太坊，当然也可以部署在国内常见的联盟区块链上。这些合约同时又要与中间的 web3 的身份管理工具进行业务交互。

总之，如图2所示，左端是用户的前端，右端是后端区块链，中间是 web3 形式的钱包管理工具或者身份管理工具。有些复杂的场景或应用可能会与多个智能合约产生交互。

1.5 WEB3 与 WEB1、WEB2 的区别

2022 年 4 月 29 日，微信号「量子学派」发表了一篇发题目为《Web3.0，与这片土地无关!》的文章，作者带着批判的思路详细论述了 web3 难以在这片土地上生根发芽的原因与现状。也许这种批判让微信平台的内容管理者感到了些许的不安，最终这篇《Web3.0，与这片土地无关!》被删除了。这件

事情让我们有一种时空错乱的感觉，因为回想起一百多年前新文化运动的先贤们高举“德先生”与“赛先生”两面旗帜，为大众争取民主与科学进行了不屈不挠的抗争。没想到在当今智能化的社会，这种抗争貌似仍然在继续。意识层面的东西我们不便多谈，本小节主要讨论《Web3.0，与这片土地无关》文中第一部分：对 web3 的三种理解。这一部分内容被作者“删繁就简”地指出了从 web1 到 web3 的区别。

那么，究竟什么是 web3 呢？不妨从以下三个方面来理解：

- 第一种理解：Web1.0 是“可读”（read only）；如 web1.0 时代的门户网站 yahoo 与新浪，它们提供信息给用户。Web2.0 是“可读 + 可写”（read+write）；如 web2.0 则以博客、推特、微信、抖音这些平台为代表，平台由用户产生内容。Web3 则是“可读 + 可写 + 拥有”（read+write+own），这是因为 web3 是由用户产生内容数据，并且数据的主权被用户自己拥有，而不是被寡头平台控制。这些看似小小的变动，但却是底层逻辑的更换，也因此蕴藏着产生天翻地覆的变化的可能性。

- 第二种理解：Web1.0 是“半中心化”。因为 web1.0 时代中心化的门户网站与个人网站各占据半壁江山，两者鼎立形成“半中心化”的生态。Web2.0 是“中心化”。这是因为 web2.0 时代的众多寡头平台形成了一个个的信息孤岛，大公司垄断了用户产生的各种数据。Web3 则是“去中心化”。因为 web3 时代则是纯粹“去中心化”，最大的特点是用户生产的数据由用户自己主宰。

- 第三种理解：Web1.0 与 Web2.0 是信息互联网，Web3 则是价值互联网。这是因为 web1.0 与 web2.0 本质上是在「传递信息」，侧重数据或者信息的消费；而 web3 则是在「传递价值」，面向所有的 web3 的用户创造财富。

从技术角度来看，web3 可以简单地理解为基于区块链技术的互联网。它旨在推翻当今互联网“中心化垄断”的现状，帮助用户拿回自己的数据主权，从而在数字世界里重造一个新维度的互联网。这个新维度的互联网世界的一种表现形式可以是元宇宙。

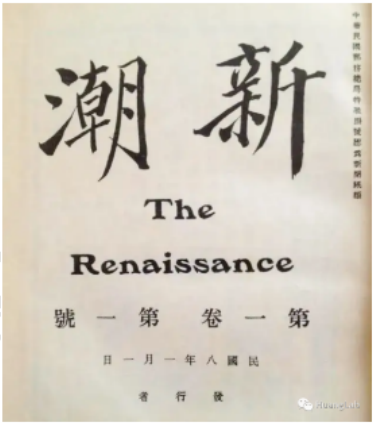

图 3: 《新潮》封面

“旧社会时候，站在时代前沿的改革先贤们进行了若干尝试，他们发现洋务运动救不了中国，辛亥革命也救不了中国，但是新文化运动却唤醒了很多新青年。如果说洋务运动强调发展技术（例如“师夷长技以制夷”），辛亥革命诉求建立新制度，那么新文化运动就是倡导「技术 + 制度 + 思想文化」”。

例如，先贤们为了引领新文化，通过各种途径传播新思想，如图3所示的《新潮》杂志创刊号。

类比先贤们对旧时代的改革，web3 对新时代的“革命”也将遵循“技术 + 制度 + 文化”的范式。如果只发展区块链技术，而不进行“辛亥革命”和“新文化运动”，那么 web3 这把好牌就会被越打越烂。令人欣慰的是，2022 年从国家层面到各地地方政府，顶层设计者纷纷提出了多项政策文件，重视以及鼓励发展基于区块链技术的新型数字经济。相信在不久的将来，中国一定会借助 web3 这股新风潮在世界范围内引领未来 20 年数字经济方向的发展。

Part II

区块链技术与应用

第 3 章　区块链技术概述

导读：本章节将介绍区块链技术与生态相关的一些宽泛话题，包括区块链的起源、对区块链账本原理的解读、区块链技术与数据库的区别、区块链技术对人类社会的意义、以及区块链技术宏观层面的演进趋势。

3.1　区块链的起源：从文字与货币的角度解析

我们从文字与货币的两条主线去解析区块链的起源，如图 5所示。

文字是用来传递信息的，信息代表的是人类某种活动背后的精神。货币是用来传输价值的，价值代表的是人类对某种物质赋予的期望。

文字与货币几乎同时起源于公元前 3000 年左右，地点是在美索不达米亚平原（就是周杰伦《爱在西元前》歌词中提到的美索不达米亚平原），该平原是古巴比伦王国的所在地，在今天伊拉克境内。据说，文字与货币这两者起源于同一个场景，即古巴比伦王国的商人使用楔形文字来记录生意，做生意就是买卖，买卖就需要货币。所以，文字与货币就这样几乎同时起源了。

接下来，我们分别回顾一下它们各自的发展路径。

文字，用来传递信息，那么、信息传递技术的发展路径是：只有发音的语言 -> 基于文字的语言 -> 印刷术 -> 电报

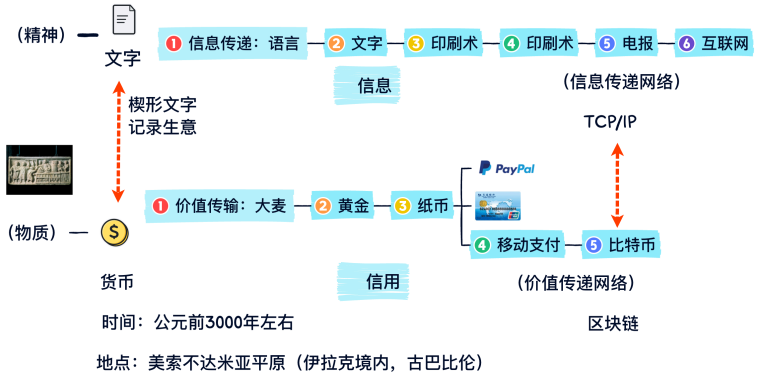

图 5: 从文字与货币的演化过程理解区块链的起源

-> 互联网技术。可见，从口口相传的方式，到基于 TCP/IP 协议的信息传递网络的建立，我们看到了一条完整的技术路线。顺着这条路线，信息传递的手段越来越高效了。

货币，用来传输价值，货币表现形式的发展路径是：以大麦为代表的实物 -> 以黄金为代表的贵金属 -> 纸币 -> 以信用卡、微信支付、支付宝为代表的移动支付 -> 以比特币为代表的去中心化加密货币。到比特币这一步，我们看到了人们基于区块链技术建立起来了高效的价值传输网络。自此以后，在这样一张价值传输网络之上，人类社会的信用就更加有保障了。至于为什么说使用区块链建立起来的价值传输网络就可以更好地保障人类的信用，我们稍后在本书其他章节来慢慢解释。

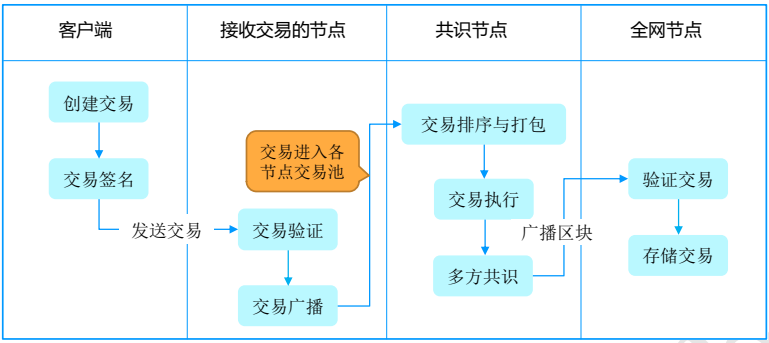

图 6: 区块链交易从提交到上链的流程

3.2 对区块链账本的解读

区块链是一种“分布式账本”，它的主要作用与银行账户数据库一样，用于记录用户的余额及交易记录。在现实中的银行，一定存在一个中心服务器，拥有最高权限，对各个节点的交易记录进行汇总管理，这其实就是一种“中心式账本”。而与之相对的“分布式账本”就不存在这样一个中心服务器。

没有了中心化的角色，那么如何在区块链这个“账本”上生成唯一、真实、可靠的账本记录呢？图 6 展示了区块链交易从客户端创建到上链的整个流程。

假设区块链中的两个客户端之间产生了一次交易，该交易提交到区块链网络后，第一个接收到这条交易的节点会将此次交易的广播到全网，即传送给网络中的所有节点。其他节点收到这条交易之后，就对此次交易进行一次记账，这就是“全民记账”。值得注意的是，区块链的全民记账是以某种预定的周期“一轮一轮”地进行的。

在某一轮记账持续了一段时间之后的某个时刻，几乎每个区块链节点都积攒了一些系统新生成的账目，那么该以谁的账目为准呢？这时就需要全网达成一个共识。全部区块链节点随后会基于某一种共识机制进行“协商”，最终全网会选择一个记账记得最好的节点，该节点就获取了此次记账的记账权。

获得了记账权的该节点就会把自己本次产生的“增量账本”（即新区块）广播给全网其他所有的节点，最终使全网其他节点都获得了此次“增量账本”的一个拷贝。

当一个新区块中的所有交易被全网节点记账后，就相当于全网都对这些新交易进行了“见证”，这就使得上链存储的这些账目几乎无法被篡改。可见，区块链的账本具有极强的可靠性与不可抵赖的特性。一个区块通常可以存储上千条交易记录，每一轮共识产生的新区块按照时序顺序连接起来，就组成了“区块链”。

3.3 区块链与中心化的数据库有何不同？

首先比较一下二者的运行方式。我们知道客户可以将数据上传到数据库进行存储，反过来也可以从数据库去读取数据。当数据上传之后，数据库里面就已经存在这项数据了，而且这份数据在数据库里面是唯一的一份，除非去复制多份拷贝存储在不同的磁盘位置上。另一方面，客户端也可以从数据库里面去读取某项已经存储的数据。但这种中心化的数据库一个很大的缺陷，就是已经存储的数据很容易被攻击与篡改。

内容略去一部分

第 4 章　数字货币（Digital Currency）

导读：随着区块链技术的发展和 Web3 世代的开启，数字货币这类虚拟资产必然发挥越加重要的作用。它摒弃了传统纸币的诸多缺点和中心化电子支付的风险，采用分布式记账而且支持匿名交易。目前，虽然各类山寨币的出现招致了广泛的批评，加密数字货币领域的炒作大于其实用价值，但数字货币是 web3 世界未来发展的基石。本章，让我们了解数字货币的真面目。

4.1　数字货币是什么？

数字货币是一种以电子货币的形式发行的替代货币，是被赋予一定经济价值的数字资产。它属于虚拟货币的一种，但不同于游戏或应用中的虚拟代币，是一种面向真实世界交易用途的虚拟货币。早期出现的中心化的数字黄金货币，以及后来兴起的加密货币都属于数字货币。

4.1.1　数字货币有哪些优点？

在介绍数字货币之前，我们首先介绍原始货币的由来。在货币出现之前，交易一般通过以物易物的方式进行，然而这种以等价商品间的交换实现交易的方式存在缺陷——物品通常

不便携带和不可分割。于是出现了以货币作为等价交换物的交易方式。货币经历了从贵重金属到纸币、信用支付再到移动支付及数字货币的发展历程。在这个过程中，贵重金属的铸币成本较高，纸币虽然避免了高昂的铸币成本，但需要复杂繁琐的防伪工序，而数字货币几乎没有发行成本。

现代在线交易系统的记账方式大多是中心化记账，由第三方可信任的服务供应商提供交易信息的记账。各大银行的在线电子转账记账，淘宝、京东等在线购物平台的交易记账，都是由相应的供应商提供存储服务用来存储用户的交易记录。但这对于部分有隐私交易需求的用户并不友好，用户的交易信息被存储在所谓的“可信任”的第三方，一些敏感的交易信息仍存在泄露风险，比如一些商业合作的机密信息与个人用户的隐私交易等等。只有保证对交易以外的所有人匿名，才能实现真正的安全隐私交易。而以加密货币为代表的数字货币，依托于区块链技术的分布式记账方式，不仅实现了交易匿名，还避免了集中存储可能存在的种种风险。

4.1.2 为什么需要数字货币？

首先我们需要了解货币体系。世界上大多数国家都发行自己的法定货币，即政府承认的具有购买力的货币，其本身并没有价值，只是承载了国家背书之后的价值。在货币兑换出现之前，以商品货币金银为首的贵金属是全球贸易的硬通货，但经由商品货币进行币种之间的兑换略显繁琐，因此出现了外汇。

部分国家或银行将本国的法定货币与外币挂钩来增加和维持外汇储备。美元作为世界储备货币在全球货币体系中占主导地位。当美国为刺激本国经济增长实行量化宽松政策增发货币时，因占据了储备货币发行国的地位，并不会直接引起本国的通货膨胀，而是通过拉动消费、增加商品进口以及将美元贬值缩减债务等手段，将通胀转移到他国 [13]。以加密货币为代表的数字货币就可以避免由单一国家增发货币带来的通胀问题。

在电子支付如此发达的今天，纸币的使用已经越来越少，数字货币与移动设备绑定，方便携带的同时也为人们的移动支付提供了便捷。此外，现有的货币体系在应对金融危机时有短板，人们在面对银行存款被冻结及货币贬值的风险时，更愿意选择部分加密货币或黄金当做避险资产。以纸币为代表的流通货币，由于无法准确确定当前流动资金的体量，造成通货膨胀率难以估计，从而很难实现有效的调控来应对通胀。而数字货币可由发行方精确追踪，因此降低了应对危机实施调控的难度。另外数字货币在反洗钱和反逃税方面也存在诸多优势，因为发行方可追踪交易流水和货币去向，通过技术分析手段可确定是否具有洗钱和逃税的嫌疑。

4.1.3 数字货币的发展

1996 年，第一个基于实物黄金的数字黄金货币 e-gold 诞生，也即是早期的数码货币，其购买力随黄金价格的浮动而变化。2005 年，瑞波（Ripple）币作为一款典型的非加密数字货币出现，它流通于一个开放支付网络 ripple 网络，并常被用于

不同货币间的兑换和汇款。2008 年，中本聪提出了比特币的概念。比特币是一种去中心化的基于密码学原理的加密货币，以区块链作为底层技术进行发币和对交易进行记账。2011 年之后，又相继出现了莱特币、以太坊的以太币，夸克币，狗狗币等等其他几千种加密货币。

随着区块链技术的大热，数字货币开始井喷式的增长，各大互联网巨头也相继推出自己的数字货币，或支持与已存在的数字货币绑定进行交易结算。狗狗币于 2013 年推出，2019 年受到马斯克的支持而火爆，其主要流行于 Twitter，TikTok，Reddit 等社区。2019 年，Facebook 推出自己的加密货币项目 Libra，同时亚马逊和苹果公司也紧锣密鼓地开展着数字货币的研究。随着元宇宙等技术的兴起，可以预见，数字货币也将成为元宇宙中主要流通的货币。

我国对数字货币的发展也高度重视。早在 2014 年就成立了数字货币研究所，中国人民银行在 2020 年推出了第一款数字人民币，目前在试点运行和测试阶段。与去中心化的加密货币不同，数字人民币沿用了纸币的管理体系，在中心化的管理下发行，受到现有的人民币管理条例约束，交易也会受到监控，以便打击非法融资、洗钱和逃税等违法金融行为。

4.2 典型的数字货币介绍

如图 12 所示，当今各种数字货币层出不穷。以下是对几种典型数字货币的介绍。

内容略去一部分

第 5 章　非同质化通证

导读：非同质化通证是区块链技术另一个比较有代表性的应用场景。其中，“通证”表示可流通的加密数字权益证明，每个通证可以代表一个独特的数字作品。非同质化通证可以基于数字文件生成，数字文件可以是画作、声音、影片、游戏中的道具等元素。虽然数字文件本身可以被无限复制，但通过对代表它们的通证在区块链上确认，就可以为买家提供所有权证明。

5.1　NFT 的定义与属性

非同质化通证（Non-fungible Token，NFT），指的是不可替代且可流通的加密数字权益证明 [14]。它具有外在和内在两种价值属性。外在价值属性体现在大众对它的价值的认同程度。而内在价值属性主要体现在一下几点：

- **稀有性（Rareness）**。这是 NFT 几乎最重要的价值。所有的创作者都可以自行决定以某一种艺术形式作为稀缺资源，并且可以决定其发行数量来确保这个 NFT 作品的稀缺性。

- **不可分割性（Indivisibility）**。与其他加密货币不同 [15]，NFT 作品只能以整体的形式来进行交易与流通。每一

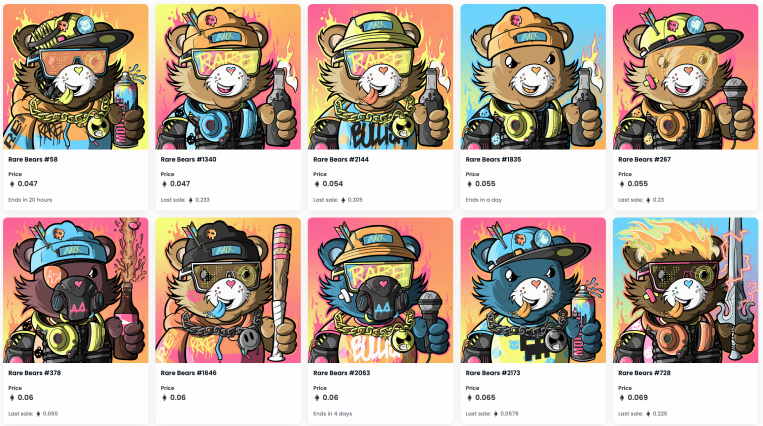

图 13: 稀缺小熊 NFT [17]

个 NFT 都是以一个整体存在，无法像比特币等其他加密货币一样以“1”以下的计量单位流通 [16]。

- **唯一性 (Uniqueness)**。传统艺术作品的数字文件可以被随意复制，NFT 则以区块链确权的方式让这些艺术品获得具有独特标识的“数字身份证”。其创作者可以自行决定某一作品的发行数量并进行编号，流通与交易的每一个环节都通过区块链被完整记录，因而每份 NFT 自身都是独特的。如图 13 展示的是在 Opensea 平台交易的稀缺小熊 NFT。

NFT 具有很强的文化属性和互动属性，参与者购买后就获得了其不可更改的所有权与使用权。而这种购买行为背后具有较强的社交意义，购买者可以借以彰显他们在数字领域独一无二的购买能力、意趣品味甚至社交地位。反过来讲，

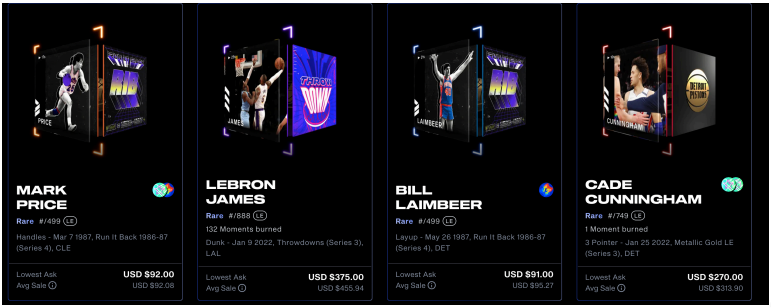

图 14: NBA 官网售卖的 NFT：NBA 尖峰时刻（NBA Topshot）[18]

NFT 的价值也需要丰富的社交活动与一定数量参与者的共识来支持。

NFT 与数字藏品有着千丝万缕的关系。数字藏品实现了虚拟物品的资产化，从而使数字资产拥有可交易的实体。在 web3 时代，数字藏品除了能建立独特标识外，用户还可以享受到数据所有权，数字藏品的价值将更多体现在身份象征和资产媒介方面。数字艺术品作为数字藏品的一种，具有以下特征：

- 形式上：早期的数字艺术指的是将物理艺术品映射到数字世界。
- 创作方式：伴随着 AI 等技术的成熟，创作者可以直接对数字文件进行操作，比如利用生成对抗网络 GAN [1] 等技术作为创作手法。
- 表现形态：在形式上，一方面利用新的媒介和手法，保留或复现已有的艺术元素，另一方面由媒介或技术创造

1 https://github.com/nolan-dev/GANInterface

全新的艺术展现形式；在效果上，通过数字媒介和数字化手段表现的艺术作品，可带给人们全新的审美体验。

5.2 NFT 发展的三个阶段

NFT 的发展具有明显的阶段性特征。下面，笔者以时间为顺序，分为三个阶段来介绍 NFT 的发展历程:

5.2.1 概念的酝酿阶段

1993 年至 2017 年，业界对 NFT 的认识停留在概念的模糊酝酿阶段。NFT 的概念设计可追溯至 1993 年加密货币的先驱哈尔 · 芬尼（Hal Finney）提出的加密交易卡（Crypto Trading Cards）。哈尔 · 芬尼在介绍加密交易卡时称“想到了一个展示购买和销售的数字现金的方法——加密交易卡。密码学爱好者会喜欢这些迷人的密码艺术的例子。请注意，它的完美组合呈现形式是——单向函数和数字签名的混合，以及随机法。这是一件多么值得珍藏和展示给你的朋友和家人的完美作品”。哈尔 · 芬尼的这段话提出依托加密学和数学随机排列组成一个系列的加密纪念卡，这种卡可以兼具艺术品与数字货币的双重属性。2012 年出现的彩色币（ColoredCoin）实现了现实资产的上链。2014 年创建的合约币（Counterparty）实现了点对点开放式交易平台的搭建。可以说，构建 NFT 的基本概念与底层技术在这一阶段逐渐成型。

5.2.2 *NFT* 的诞生阶段

2017 年至 2020 年，NFT 正式诞生，而且借助于加密货币与电子游戏的“东风”茁壮成长。2017 年，同质化代币交易额与参与人数屡创新高，世界上第一个 NFT 项目——加密朋克（CryptoPunks）——作为一款像素角色生成器问世。该项目生产的像素头像被开发者通过区块链传播。由于当时还不具备足够通用性的 ERC20 通证标准作为基础协议，这些头像类的 NFT 只能以以太币进行结算，但是却凭借它的独特性获得了加密圈的大量关注。ERC20 通证标准是通过以太坊创建的一种代币发行的规范。调用者可以通过编写一个智能合约来创建“可互换”的通证，并支持与众多交易所、钱包进行交互，现在已被加密货币行业普遍接受。此后，Dapper Labs 团队受加密朋克的启发推出了专门面向铸造 NFT 的 ERC721 标准（提供发行 NFT 的标准接口），并基于这个标准推出了一款名为加密猫（CryptoKitties）的 NFT 产品。Dapper Labs 团队推出的每一只数字加密猫都是独一无二且不可复制的。这种“以稀缺谋求价值最大化”的思路让加密猫迅速成为加密市场的现象级的作品。自此，NFT 开始以文娱特别是游戏产业为主赛道蓬勃发展。在此期间，OpenSea、SuperRare 等交易平台获得了飞速发展，“蒸汽”（Steam）等游戏平台也依靠 NFT 进行不断创新。与此同时，NFT 行业也得以获得了更加规范的演进，比如进一步规范了交易市场、斩获了大量用户群体、丰富了产品、繁荣了世界范围内的市场。

5.2.3 *NFT* 的爆发阶段

2020 年以来，NFT 借助此前积累下的用户群体与资本实现了爆发，市场热度与社会影响力双线走高。新冠疫情爆发以来，英美等国政府借助滥发货币的方式刺激经济。传统的投资方式失去了吸引力，很多风险投资家的投资变得更加激进，他们将目光投向了 NFT 的蓝海领域。据 NFT 数据网站 CryptoSlam 统计，借助“疫情经济”的东风，“幻想生物”（AxieInfinity）等现象级产品的累计交易量破 10 亿美元，游戏金融（GameFi）性质产品层出不穷且获利颇丰。除了资本市场繁荣之外，NFT 的社会影响力与知名度也不断提升。据谷歌官方搜索趋势数据显示，NFT 相关的关键词搜索量自 2021 年初起呈爆炸式增长。ai de 斯诺登、特斯拉总裁埃隆 · 马斯克、NBA 球星史蒂芬 · 库里等人的积极参与，也为 NFT 市场带来了名人效应。2021 年 11 月 24 日，《柯林斯词典》将 NFT 评为 2021 年度词汇。一个月后的 12 月 20 日，《柯林斯词典》又评出了 2021 年 12 大科技热词，NFT 以第一名入围 [15]。

本章节，我们详细回顾了 NFT 历史上具有代表性的项目、团队和他们的闪耀时刻。这些的高光时刻清晰地篆刻了 NFT 历史发展的里程碑。所有这些故事，都为 NFT 世界的后浪们总结了经验、指出了未来的方向。至于未来 NFT 会发展到什么程度，估计没人能够给出准备的预判。不过，我们可以借鉴先贤的思路窥探一二。意大利学者维柯曾在《新科学》中提出了历史循环的三个阶段，即神权时代、贵族时代、民主时代。历史总是押着相同的韵脚，从更高维度的历史视角去观察，NFT 发展史也基本符合维柯提出的历史三段论的特

征。如今 NFT 在以太坊以及其他公链上遍地开花，普通人能够轻松触及，这正是 NFT 民主时代的开端 [19]。

5.3 NFT 的发行、铸造与价值分配

5.3.1 *NFT 的发行*

NFT 的分类和电影、游戏的分类非常像。我们可以依照电影和游戏的分类来探索 NFT 的发展。NFT 能够以多种形式发行 [20]，举例如下。

- **艺术作品:** 非同质化通证影响最大的应该是艺术行业。如今，人们已经开始在非同质化通证平台上交易艺术作品。有些创作者与艺术家已通过拍卖他们创作的非同质化通证艺术作品而获利。不同的是，大部分数字艺术作品储存在 NFT 交易平台上，而实体艺术品则保存在画廊、博物馆、艺术俱乐部等场所。

- **现实世界物品:** 目前，土地和房地产等现实世界的物品在 NFT 领域逐渐掀起了浪潮。例如，就所有权而言，房屋所有者可以通过发行通证，将物业的一部分出售给投资者。这样，投资者就可以通过分享收益、优先入住、以低廉价格使用物业等方式，获取收益。

- **影像:** NFT 可以将照片实现通证化（如图 14 展示的 NBA 尖峰时刻 NFT）。如果读者是摄影师，可以通过发行证书，出售自己的影像作品的所有权。

内容略去一部分

Part III

元宇宙不只是虚拟游戏那么简单

第 6 章　元宇宙（Metaverse）

导读：元宇宙是融合区块链、人工智能、网络与计算等技术构建的一个与现实世界平行且交互的数字世界。本章，笔者将带领读者了解元宇宙的基础知识，并通过对元宇宙背后核心技术的分析帮助读者解读元宇宙赛道的机遇与挑战。

6.1　元宇宙是什么?

从 2021 年初开始，虽然元宇宙概念火出了天际，但笔者相信大多数人还是分不清楚元宇宙跟沙盒类的网游之间的本质区别，因为多数人仍然认为元宇宙是一个更加开放化的沙盒类网游。本节，笔者通过详细介绍元宇宙和沙盒游戏的特点，帮助读者认清元宇宙与网络游戏之间的异同点。

6.1.1　元宇宙与沙盒游戏的差异

首先，沙盒类游戏（Sandbox Game）是一种电子游戏类型。通常它的游戏地图较大，具有较强的与环境的互动性。另一点，极高的自由度是沙盒类游戏的最大卖点，玩家可以较为自由地探索、创造和改变游戏中的情节与内容。沙盒类游戏大多数是非线性游戏（按照不同顺序完成某些挑战），但也有

按照固定挑战顺序推进的线性模式剧情可供选择，一般不强迫玩家完成指定的目标任务。

对于元宇宙，中纪委网站在 2021 年 12 月 23 日发表的文章《深度关注：元宇宙如何改写人类社会生活》对元宇宙做了以下定义 [26]：“通常说来，元宇宙是基于互联网而生、与现实世界相互打通、平行存在的虚拟世界，是一个可以映射现实世界、又独立于现实世界的虚拟空间。它不是一家独大的封闭宇宙，而是由无数虚拟世界、数字内容组成的不断碰撞、膨胀的数字宇宙”。

元宇宙里用户可以通过化身（Avatar）实现同现实生活中的各种活动，比如开会、工作、购物等，甚至在里面可以开发出各种应用。对比沙盒类游戏，无论是谁在运行元宇宙的特定部分，元宇宙必须提供“前所未有的互操作性”——用户必须能够通过他们的化身与元宇宙中其他化身或者实体进行交互。元宇宙能够给用户提供的体验包括拥有财富、体验第二人生、拥有新的影响力和社会地位，甚至在元宇宙中娱乐与工作。因此，元宇宙并不是我们所常见的沙盒游戏。

举例来讲，如果大家戴个 VR 头盔之类的传感设备，然后仅仅连接进入被设计出来的虚拟空间，增强用户的沉浸式体验，这样跟玩一般的游戏比如说开放世界或者沙盒游戏有什么差别呢？如果从这个角度来看，我们会发现元宇宙它本身跟诈骗没什么两样，无非是旧酒装新瓶罢了。其实，元宇宙最根本的点在于它不单纯是游戏，而是一个可以与物理世界共生交互的虚拟世界。我们所理解的传统游戏，目的就是为了娱乐。以前，我们不会想到有人在游戏里面办公，比如处理 office 文档、编程、开会与工作，甚至是设计新的事物来

满足现实世界的需求。这是因为元宇宙出现之前的时代，人们进入虚拟游戏世界的唯一目的就是为了娱乐。而现在不同了，基于虚拟游戏的技术，元宇宙融合了相关的互联网技术，比如 5G/6G 通信网络、物联网、区块链等技术。这些技术叠加起来构建了一个比传统虚拟游戏要更加复杂的“虚实相生”的世界——元宇宙。

元宇宙的价值在于把现有的互联网提升到了一个全新的体验高度。元宇宙要成功，它必须做的像浏览器一样满足以下两点：

- 构建一个公共的开放世界。
- 任何参与者都可以生产内容，比如，用户生成内容，专业者生成内容与 AI 生成内容。而且，参与者可以将这些内容在这个虚拟世界里开放、交易与流转。

仅仅依靠浏览器的前端技术，基本上已经极其难以实现这些功能了，而现在还要做一个虚拟世界级别的“浏览器”，难度就更大了。不过，业界可以从简单的尝试开始，初期可以构建一系列的小 demo，逐步探索，逐步进步。

6.1.2 元宇宙概念爆火的原因分析

其实，元宇宙并不是一个新概念，早期的科幻作品《雪崩》里面就有虚拟世界的这种设想。电影《黑客帝国》也是把整个世界当做是一个虚拟的游戏。但是，为什么现在又开始炒这个元宇宙的概念呢?

一方面，从技术的发展角度来说，过去的设想开始有一点点的可行性了，也就是说当今的技术发展已经到了一个奇点。过了这个奇点之后就会形成下一波技术浪潮。大数据、人工智能、区块链、物联网等技术都有了一定的发展与积累。在这个基础之上，人们就会融合这些研发成果与技术，构建一个具有广阔市场的新业态。

另一方面，各行各业严重的内卷导致投资人不知道该去投什么项目了。资本、投资人都需要新的赛道，需要新的投资故事。如 2021 年 10 月 28 日，马克 · 扎克伯格在 Facebook Connect 大会上宣布将 Facebook 更名为 Meta（取自元宇宙英文 Metaverse 的前 4 个字母），并于 2021 年 12 月 1 日起以新的股票代码 “MVRS” 进行市场交易，标志着将以元宇宙业务为优先，通过发展 AR、VR 等软硬件及相关生态，最终将公司打造成元宇宙企业 [27]。

那么，如果没有新的赛道出现，没有新的投资故事，大家就不敢投资了。当大家都不敢投资的时候，整个世界的经济就有可能要下滑。所以，元宇宙的叙事背景横空出世。元宇宙的特点，满足资本对于最佳赛道的全部要求，一个重要原因就是资本需要出口，或者说资本需要新的叙事来投资。恰好元宇宙满足了这个条件，它是一个全新的故事，而且很容易判断它的商业模式是非常明确的，并且它未来的市场容量是巨大的，也是很容易估算的。

但是，笔者认为元宇宙的愿景的实现可能需要 20 年以上的时间发展相关的技术。因为回顾之前，从 90 年代互联网兴起到 2000 年互联网泡沫，再到 2010 年附近才正式开始互联网的大蓬勃时代的话，差不多也是 20 年。主要的原因是现有

的游戏开发工具，比如各种游戏开发引擎，例如“虚幻 · 五”这种顶尖的引擎，或者行业里面普遍采用的 unity 之类的工具，它们的整个开发流程的成本很高，而且存在很多的局限性，比如互动性等等。

我们知道 Facebook (Meta 的前身) 一直致力于把 Facebook 社交软件搬到这个虚拟世界里面去。当然，他们面临的挑战也是非常多的。首先，Meta 需要花巨资把虚幻引擎的公司整个买下来，在此基础上，Meta 能不能做出来呢？它可以做出看起来很炫酷的视觉效果，但是实际上离 Metaverse 的概念仍然差得很远。那么，这个差别主要体现在哪儿呢？我们举个小例子，从技术上来讲，玩家在游戏里可以浏览网页吗？其实是看不了的。游戏里边看网页这件事其实是技术上很大的难点。这个问题表面上看像把浏览器的画面在游戏里展示，但实际上需要两种截然不同的技术体系完成融合。

此外，很多人也会质疑为什么要在元宇宙里工作呢？人们很奇怪在元宇宙里浏览网页的行为，为什么不直接使用个人电脑去浏览网页呢？还有，为何要在元宇宙里网购呢？对于有些反感或者抵制元宇宙的人而言，他们可能会怀疑或者犹豫为什么要去加入到元宇宙的世界里。如果对元宇宙完全不感兴趣，可不可以呢？当然可以，我们回看一下历史啊，比如说上世纪九十年代初互联网刚刚诞生的时候，当时华尔街就开始在纳斯达克炒作互联网概念。其实，那个时候的技术才只是几台电脑连接一根网线，那个时候的电脑分辨率还是很低的，大概 640×320。以现在的眼光来看，那些都是马赛克画面。即使在那种情况下，他们就开始开发购物网站，做各种应用。后来互联网发展得怎么样呢？很明显，现在大家谁

还离得开互联网呢？当初那些选择不加入互联网的人，最后他们都不得不进入互联网的世界。就像现在的老年人，如果说不学会操作打车软件，那么他们打车都很困难。因此，我们看到一个社会现象：当技术与社会发展到一定程度，无论人们愿意与否，都会被动卷入这些技术浪潮。

被动卷入的核心原因就是这个世界的发展并不是由大多数人决定的。如果说人类社会像一列火车的话，火车头才是决定火车方向的。这个火车头只是人类世界里面最聪明的一小群人。也就是说整个人类中的大部分人都是盲从的，他们本以为他们有自主意识 [28]，比如说他可以选择做什么，或选择不做什么，其实大家都没有自主选择的能力的，都只能随大流。这个“大流”就是由很少的一群人决定了这个世界的发展方向。因此，对于元宇宙的概念，不需要说服所有人去接受，只要说服最聪明的那群人都跟着“大流”走就可以了，其他的人没办法发展其他的方向，他们只能慢慢涌入其中，于是时代的浪潮就形成了。因此，元宇宙的发展大概率也是这样的一个过程。

但是，一个问题是，如果各个公司单独开发自己版本的元宇宙，那无疑跟诈骗没有两样。元宇宙的发展，必须要像互联网一样，有一个公共标准与规范，就像互联网协议那样。这样可以保证元宇宙不会受到某个公司的控制。目前，部分公司炒作的元宇宙概念与真实的元宇宙有较大差异，读者朋友需要去伪存真、谨慎判断。在业界看来，元宇宙较长一段时间内都将成为下一代互联网发展的目标，这有赖于底层技术和算力层面出现的核心技术的突破。

最后，笔者再分享一位播客听友的问题，作为本节的收尾。

这位听友收听了与本节内容相关的播客之后，提出了一个很有代表性的问题：“元宇宙如果像互联网那样未来会普及，那么对于大众生活来说，它究竟解决了什么痛点?”

笔者回复道：“这是一个好问题！现阶段来看，貌似如果没有元宇宙，人们也可以活的好好的。所以目前来看，元宇宙还处于早期的泡沫期。但这并不代表元宇宙就是一个伪需求，只是人们还没开始意识到未来元宇宙的巨大作用与潜力。就像十年前人们觉得 3G 接入网的服务就够用了，谁料到还有 4G、5G 甚至是 6G 技术的出现，以及这些新一代的通信技术催生了移动互联网时代的繁荣。虽然现在人们还只能在元宇宙里进行非常初级的体验，比如元宇宙游戏、社交、举办活动等等，但是人们很快就会看到元宇宙里爆发巨量的应用与远超现实世界规模的应用生态”。

6.2 元宇宙的 3 个早期发展阶段

本节笔者将简单梳理元宇宙早期发展的三个时期：概念孕育期、形态塑造期与快速发展期。

概念孕育期

首先，我们来看一下元宇宙相关的概念孕育期。从 1992 年开始 Meta 这个词就已经出现在了尼尔斯蒂芬森的科幻小说《雪崩》中。《雪崩》中描述的元宇宙形态是：“戴上耳机和目镜，找到连接终端，就能够以虚拟分身的方式进入由计算机

模拟、与真实世界平行的虚拟空间”。《雪崩》描绘了一个庞大的虚拟现实世界，所有现实世界的人在元宇宙里都有一个网络分身（Avatar），人们用数字分身来进行活动，并相互竞争以提高自己的地位。

令人惊讶的是到了 1993 年日本的一个电子游戏公司叫世嘉，推出了自己的 VR 头盔。这个头盔只能支持当年很火的街机游戏。尽管该头盔产品因为技术等其他原因没有问世，但是他们的概念远远超出了那个时代应该有的产品。

另外一个比较有代表性的支持游戏的头盔产品，就是 1995 年任天堂推出的名为 Virtual Boy 的设备。但是该设备的使用局限性比较大，只能被固定在一个地方，用户需要把眼睛凑上前去，然后才能看见头盔里面所显示的游戏画面，游戏使用视差原理产生立体 3D 的效果。

到了上世纪 90 年代后期，陆续出现了众多的 3D 游戏，特别是以第一视角为特点的射击类游戏的兴起，如 1993 年的“毁灭战士”（Doom），1996 年的 Tom reader 和 1999 年的“无尽的任务”（EverQuest）。这些游戏有一个共同的特点，就是游戏玩家在这些游戏中都有一个以人为具象的身体化身，来帮助游戏玩家感受沉浸感十足的 3D 游戏环境。

形态塑造期

接着，我们再来看元宇宙的形态塑造期。其中标志着该时期开启的一部作品就是 1999 年上映的科幻电影《黑客帝国》。这部精彩的电影展示了人们通过脑机接口技术完美进入了一个虚拟的元宇宙世界。2003 年，“第二人生”（Second Life），成为了第一个现象级的虚拟世界的游戏。到了 2006 年，Roblox

问世了，至 2019 年它的月活用户已经超过了 1 亿。2017 年“堡垒之夜”获得了最佳多人游戏的提名。到了 2018 年 1 月，它的全球的玩家已经超过了 4,500 万。2018 年电影《头号玩家》中展示了一个叫做绿洲的游戏场景，这是对元宇宙的一个很好的具象化。

快速发展期

经历了漫长的形态塑造期，接下来元宇宙进入了快速的发展期。自元宇宙概念第一股 Roblox 于 2021 年 3 月 11 日在美国上市，元宇宙迅速进入人们的视野。科技巨头们也纷纷布局元宇宙，尤其是，Facebook 改名 Meta 全力押注元宇宙。这个标志性的事件掀起了各大科技巨头的“元宇宙热”。以 Facebook、微软、腾讯、字节跳动为代表的科技巨头持续加码元宇宙赛道，围绕 VR/AR 硬件设施、3D 游戏引擎、内容制作平台等与元宇宙相关的多重领域拓展商业版图。因此，也有人把 2021 年称为元宇宙的元年。自此，整个互联网生态随声附和，全球产业遥相呼应，元宇宙概念得以彻底爆发。随后，NFT 概念的出圈，也直接推升了元宇宙的热潮。不过，短期内 NFT 主要涉及对虚拟世界中的艺术品进行数字化确权，和对元宇宙中的数字藏品支持流转交易。对于 NFT 介绍可以参考章节5。

6.3 实现元宇宙的 6 项核心技术

目前，关于元宇宙背后的核心技术的主流说法是包括 6 个方面，如图 18所示。用英文字符可以合称为 BIGANT [29]。其

内容略去一部分

第 7 章　对元宇宙的思索

导读：一个概念的爆火往往会蒙蔽人们的双眼、迷惑人们的心智。读者在挖掘元宇宙潜在的机遇时，也要认清元宇宙背后的各种风险。笔者通过对国内各行业在元宇宙方向的产业布局分析，帮助读者思考应该以什么样的方式参与其中。

7.1　由 LIBRA 破产想到元宇宙

据彭博社报道，由 Meta（原 Facebook）公司支持的 Diem 加密货币协会正在考虑打包出售其相关资产，以退还早期投资者的投资。彭博社还援引知情人士的话称，Meta 拥有 Diem 协会约三分之一的股份 [41]。

公开资料显示，Diem 协会前身为 Libra，于 2019 年 6 月被提出，总部设在瑞士日内瓦。按扎克伯格最初的设想，Libra 将是一种与美元、欧元等主权货币挂钩的稳定币，试图将 Facebook 庞大的用户群体与区块链技术相结合，打造数字经济时代新的储值手段和价值尺度。为此，扎克伯格联合了数十家大型公司一起合作。很多市场分析认为，这是科技巨头们试图改变金融体系。

由于 Libra 计划触碰了主权国家金融体系的根基，因此该计划在全球范围内遭到了监管机构的强烈反对。其中，最大的阻碍就来自美国。不久之后，Libra 失去了包括 Visa 和万事达卡在内的主要支持者。

随后，意识到“发币不易”的扎克伯格不得不尝试“以退为进”的曲线救国路线。在 2020 年 4 月将重心从锚定一篮子货币转为锚定单一货币——美元。同时，扎克伯格在 2020 年 12 月份将 Libra 正式更名 Diem，并做出各种新尝试，竭尽全力打消美国监管机构的疑虑。

2021 年 5 月 13 日，Diem 协会宣布与银行 Silvergate Bank（美联储成员之一）达成战略合作，并将其主要业务从瑞士转移至美国，并计划将该项目完全纳入美国监管范围，尝试简化 Diem 美元稳定币的发行计划。

但美国绝不会放弃巩固了几十年来之不易的“美元霸权”。真正的核心利益，强如扎克伯格也不可染指。因此，扎克伯格的以退为进的策略始终难过美国这一关。到了 2021 年 11 月，美国监管机构终于下定了决心，出具一份报告重点强调以下两点。首先，如果科技公司的庞大用户网络突然开始以新货币进行交易，现有金融体系将遭到冲击。其次，发币人同时也是科技巨头，二者合一“可能导致经济权力过度集中”。在监管的重压下，扎克伯格雄心勃勃的“发币计划”[42] 宣告失败。

不久后，Meta 高管、Diem 项目的联合创建者之一的 David Marcus 在加入该科技巨头七年后选择了离职，而扎克伯格也选择了“元宇宙”赛道进行二次创业。

由以上故事，我们可以发现：

- Libra 不属于去中心化加密货币。它只是由众多机构共同构成的一个联盟链发行的。
- 在 Libra 的联盟链里，没有挖矿发币的概念。加入这个联盟，并不能通过挖矿获得奖励。

- 加入 Libra 联盟链的前提是，需要提供现实资产抵押（可以是主权货币），通过对资产的现实价值在链上新增虚拟资产。

- 因为上一条的原因，所以 Libra 的币值和比特币之类是不同的。如果能发行的话，它的币值将会是相对稳定的。

上述设计的目的是为了实现：

- 提供全球范围内在任何国家都能使用的转账系统。

- 这个系统转账的手续费比现有的跨境转账系统低得多。

Libra 受到的阻力主要来自美国国会。因为 Facebook 的目标是在全球合法运营这个经济系统。刚开始的时候，各大金融机构都生怕错过机会纷纷加入。但是美国国会在听证会上，提出了几个基本的疑问：

- Facebook 如果能够发行 Libra，加之他自身又是互联网巨头，那么这种高度集权的信息平台附加一个中心化的经济系统，会不会带来极大的金融风险？

- Libra 如何解决隐私保护与反洗钱的矛盾？

- 其他一些意识层面的问题。

Facebook 本身在 libra 推出前就已经陷入到了几起丑闻里。比如用户个人信息泄露，青少年沉迷网络等问题。Facebook 已经处于后院失火的状态。因此，美国社会对 Facebook 观感不佳。在这种情况下，就让 Libra 的推进更加困难重重。其实 Libra 如果能成功发行，扎克伯格绝对会成为这个地球

上最富有的人。看来这个世界终究还是会被幕后某种强大的力量所主导，有些秩序不是那么轻易就可以被推翻重建的。

不破不立。虽然让这个世界接受创新没那么容易，但是，只要我们有梦想，终究会从历尽千辛万苦找到的一扇窗户中看到新世界的一缕晨曦。笔者认为，基于区块链技术的元宇宙与 web3 就是不远的未来新世界的这扇窗户。但愿我们每个人都可以从这扇窗户中找到属于自己的光芒。

7.2 元宇宙的去中心化经济系统是必需的吗？

现在业界普遍认为区块链技术可以帮助元宇宙打造虚拟世界里的经济体系。那么，人们很自然地会问一个问题：元宇宙中去中心化的经济系统一定就好吗？在回答这个问题之前，笔者有必要对“制度经济学”进行介绍，因为无论是中心化的还是去中心化的经济系统都是建立在制度之上。

7.2.1 必要的铺垫：制度经济学

制度经济学是经济学的一个子集，与政治学、社会学或历史学相交叉，用经济学的方法研究制度在社会经济背景下的作用 [43]。单个人满足自己愿望的能力是有限的。地球上甚至没有人能够独自生产出一支铅笔，因为这依赖于智利的石墨工人、加拿大的伐木工人、台湾的胶水制造商、德国的生产线制造商、中国的商人以及千百万不知名的人参与合作和作出贡献。在专业化劳动分工精妙复杂的现代社会，人需要与难以计数的陌生人或组织进行交易、合作。人类的相互交往，

尤其是经济生活的相互交往，依赖于信任。信任以秩序为基础，而要维护这种秩序，就要依靠禁止各种不可预见的行为和机会主义行为的规则，我们称这些规则为「制度」[44]。诺思 [45] 将制度定义为一个社会的游戏规则，制度使人们结成各种经济、社会、政治等组织或体制，它决定着一切社会经济活动和基于各种经济关系展开的框架，因此各个社会学科都与制度有着内在的联系，是社会科学的一个共有范畴。

为什么人类社会需要制度？主要原因可以归结为以下方面：人的有限理性（主观的智力资源稀缺），客观环境的不确定性，与人的机会主义倾向。制度让人的行为具备可预见性，在大规模的人类协作中减少协调活动的成本，以便有效地利用资源。我们之所以能将辛苦工作挣来的钱放心交给下一秒就忘记相貌的银行出纳员，将自己的身体安心托付给素未谋面的医生，都是因为他们都受制于制度。回过神来，人类社会太多理所当然的事实际上都垂悬在由制度编制的信任之网上。

制度是演化而来的，与政策不是一回事。当人们发现有更好的、更有效率的制度可以取代现存的制度时，就有可能出现制度变迁。制度约束人与人之间的关系，而人与人之间的关系是一种社会关系之间进行的博弈，利益不一致的情况出现在几乎所有人类活动中，相关各方的最后总是能通过自己的选择以期实现一个对己方有利的结局。经济学家在把经济过程作为博弈过程处理的同时，不仅把制度看作博弈的规则，也把它当做博弈的结果。只要人们反复地发生交易或其他经济关系，就会通过逐步演化或人为有意识地设计规则。当我

们把时间拉长一点来看，历史上所有称为革命、改革、复辟、前进、倒退等等内容，其中最紧要的实质都是制度演变。

对比法学、政治学、伦理学、文化学及社会学甚至人类学，制度经济学对制度关注的层面及视角不一样。制度经济学关心对人类经济影响最深远制度的创造和演变。人类的理性选择将创造和改变诸如产权结构、法律、契约、政府形式和管制这样一些制度，这些制度和组织将提供激励或建立成本与收益，最终这些激励或成本与收益关系在一定时期内将支配经济活动和经济增长。

交易是人类经济活动的基本单位，也是制度经济学的基本分析单位。制度经济学基本理论工具是交易费用理论和产权理论。交易费用范式构成了制度经济学的理论框架，如果没有交易费用，不论生产和交换怎么安排，资源的使用都相同。交易成本从根本上影响着市场上生产什么和什么样的交换会发生，何种组织得以生存以及哪种游戏规则能够持续。交易的前提是产权，没有产权交易无从谈起。交易和交换不同，不是商品买卖而是权利买卖。产权制度是经济运行的根本基础，有什么样的产权制度就会有什么样的组织、技术和效率；

产权方法和交易成本方法存在差别，前者需要一种对个人诱因的分析，而后者则把个人置于一个更广阔的机构框架内，例如容许把公司作为一个组织起来的尸体而加以分析 [46]。

7.2.2 回到问题

现在，回到开头的问题：去中心化的经济系统就一定是好的吗？其实，“中心化”的体制系统是人类文化发展的选择出来的成果。虽然从技术上完全去中心化已经实现了，比如以比特币为代表的区块链技术。但是，人类社会必然还会产生中心化的组织来掌控人类社会，就像埃隆·马斯克对狗狗币的掌控，而且这种掌控是脱离了原本已经成熟的中心化的制度体系。在没有新的制度体系被制定出来的时候，仅仅从技术上实现去中心化可能带来的是灾难。

因此，没有制度配套的去中心化经济系统就像一个“乌托邦世界”一样。人们对去中心化的渴望与向往来源于对自由不受约束的向往。因为元宇宙的构建和参与是以人为主体的，而人之间的差异化（能力、身份、知识等）会在人们在元宇宙中搭建去中心化的经济系统的过程中让实现平等与自由的愿望落空。

人们在搭建元宇宙中的经济系统时，究竟应该选择偏向中心化还是去中心化？这是一个融合制度与技术的逐步探索的过程，类似于对未来加密货币掌权归属问题的讨论 [47]。不过，过去只有一个选项，现在有两个选项，而且这两个选项在一定程度上形成了竞争和制衡。人类的乌托邦理想就像爱情一样永恒，总是不断的往新的乌托邦去发展。因此，笔者认为元宇宙中的制度终究会让我们再度失望，这是因为未来在元宇宙体系里将会诞生的新的不公平。人们对各种规则的不满、矛盾和冲突，仍然会在元宇宙中继续上演。

内容略去一部分

Part IV

去中心化自治组织（DAO）是什么?

第 8 章　DAO 的简介

导读：去中心化自治组织（DAO）依赖于区块链和智能合约技术，被视为未来实行去中心化创新的一种新型自治形式。

8.1　DAO 的定义与概述

去中心化自治组织（Decentralized Autonomous Organization，DAO），最早被称为去中心化自治公司。这个术语在比特币问世后不久就出现了，主要用于加密代币圈的非正式论坛的聊天。后来随着以太坊智能合约的出现，2016 年 4 月诞生了第一个 DAO 项目——The DAO。DAO 背后的技术主要包括两个部分：区块链与智能合约。前者作为去中心化的账本，是 DAO 组织的基础设施；后者可以支持开发丰富的去中心化应用。

我们展开更多细节解释一下这两项技术起到的作用。首先，区块链通过提供一个可审计的去中心化、透明的账本，用来记录 DAO 项目的所有重要的事件，为一个 DAO 项目的社区提供了基本的透明度和信任。其次，智能合约允许自动执行预先编写好的规则，通过代码实现对 DAO 项目事务的执行与治理。这两项技术共同构成了 DAO 的基础。DAO 的组织概览如图 24 所示。

在已出现的 DAO 项目中，有些采用的还是“链下协作为主，链上治理为辅”的方式。其中，链上治理也仅仅涉及投

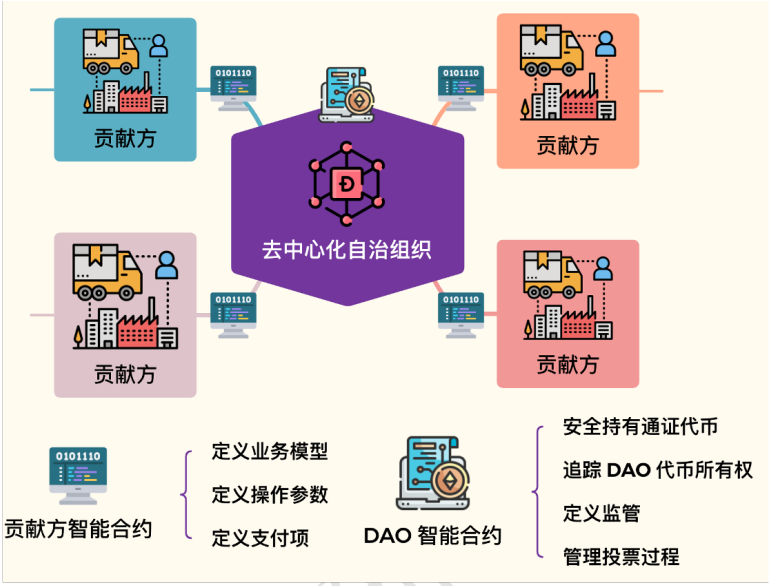

图 24: DAO 的概览

票的过程。有些 DAO 项目很简单，甚至只使用一个简单的智能合约就能实现全部的业务逻辑。

其实 DAO 不一定需要依靠区块链技术才能建立。具有相同理念和共识的一帮人即可形成一个 DAO。而且，人们未必需要借助区块链共识协议才能形成社区的共识。比如，在互联网世界里，当人们强烈认同一个视频或者一篇文章时，即使它们不断被中心化的监管机构删除，人们仍然可以通过自发存储和不停地转载，将其尽力保留在网络上。这样的自发行为其实就是 DAO 的思想和 web3 文化的一种践行。进一步来讲，如果借助区块链的技术，这些人们产生的社会共识，会

更加容易地被记录与分享，从而更好地践行 DAO 与 web3 的理念。

虽然互联网人是最具有创新精神的一个群体，但是能突破旧思维去拥抱新的变化，去参与新赛道，仍然是逆人性的行为，是充满挑战的。不管如何，这个世界唯一不变的真理就是这个世界在一直变化着。任何人都阻挡不了新趋势的发展。总有一个时刻我们会意识到：如果不去主动拥抱变化，就会被新技术的趋势所碾压。

8.2 DAO 的技术架构

如图25 所示，DAO 的底层架构包括三层。底层是区块链，中间层是 DAO 项目的技术栈协议，上层是 DAO 项目应用。每一层都会向上起到支撑作用。比如，区块链可以为技术栈协议层提供分布式账本数据库的功能，技术栈协议可以为应用层提供前端访问的应用程序接口（API）以及其他中间层的缓存功能，应用层可以支持开发者根据应用的业务逻辑编写代码。

关于 DAO 的技术架构早期理论探索，比较有代表性的国内研究是 2019 年中科院袁勇老师团队发表的题为 “Decentralized Autonomous Organizations: Concept, Model, and Applications” [50] 的论文。该论文发表在期刊 IEEE Transactions on Computational Social Systems (TCSS)，主要介绍了 DAO 的概念、特点、研究框架、典型的实现方法、挑战和未来的趋势。特别地，作者在文中提出了一个五层架构的

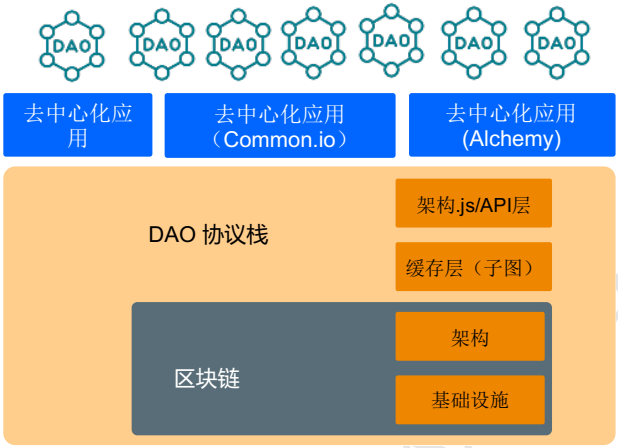

图 25: DAO 的三层技术架构

DAO 参考模型（如图26所示），分别包括“基础技术层”、“治理操作层”、“激励机制层”、“组织形式层”和“表达层”。

其中一些亮点总结如下。

五层架构的“基础技术层”的亮点在于其融合了人工智能、物联网及区块链技术。人工智能技术可以赋能 DAO 中的每个独立节点成为一个自主“代理”（也称为软件代理或者代理机器人）。这些代理具有一定的自主性，因为它们有“目标导向行为”的能力。未来，预计它们将取代人类参与 DAO 组织时的感知、推理、决策和其他功能。另一方面，智能合约的自动执行能力可以赋予 DAO 更多的智能。比如，区块链可以与物联网（Internet of Things, IoT）结合，形成“区块链物联网”（Blockchain IoT, BoT）。区块链物联网可以将智能设备和某些实物资产进行数字化改造成数字资产，然后整合到 DAO 中。BoT 作为一个可靠的物联网服务平台，DAO 将以安全可

图 26: DAO 的五层架构参考模型 [50]

信的方式监控智能设备的整个生命周期，实现设备间的自动交易，并利用智能合约实现智能设备间的互操作性。

“治理操作层”利用 AI 技术可以完成从角色到任务的自动匹配。AI 算法根据参与 DAO 的个人贡献和能力，匹配个人在 DAO 中的位置和角色，然后自动完成任务识别、推荐和匹配。通过这样的方式，人力和知识资源就可以被高效流通起来。

最后，“激励层”中的荣誉评价体系可以对每一个参与 DAO 的个人的工作过程和交付结果进行多维度的评价。评价结果代表个人在 DAO 中的荣誉体系中的级别。不同的级别将享有不同的权益。

内容略去一部分

第 9 章　DAO 的实践案例调研

前文中我们提到了历史上第一个 DAO 项目，即 The DAO。这里我们简单介绍一下 The DAO 项目，它是第一个在以太坊发起的去中心化的众筹项目。但是仅仅 2 个月后，它就遭到黑客攻击，大量众筹来的以太币被黑客盗取。此次攻击事件对 DAO 社区造成了很大的负面影响。这次事件还导致了以太坊的硬分叉与社区分裂（此次事件的来龙去脉请扫图 27）中的二维码收听）。

图 27: The DAO 攻击事件的详解

尽管 DAO 的早期发展遭遇类似黑客攻击这种阻碍，但是 DAO 的爱好者们依然进行着持续的创新与尝试。本章为大家介绍国内外一些具有代表性的 DAO 案例与项目。

内容略去一部分

第 10 章　DAO 的现状与未来

本章梳理 DAO 在早期发展过程中遇到的重要课题，并对 DAO 将来的发展进行思考与探讨。

10.1　DAO 亟需解决的问题有哪些?

本节，笔者认为目前 DAO 亟需解决如下两个问题：激励机制的设计和 DAO 的去中心化治理。

10.1.1　*DAO 的激励机制设计*

DAO 的激励方案是一个 DAO 项目至关重要的组成部分。从上述几个成功的 DAO 案例中我们可以看到它们明确的激励方案。其中，“代币激励”是 DAO 的主要激励手段。通过本书前面相关章节的学习，我们已经知道代币是一种可流通的数字资产，是去中心化应用的权益证明。现实世界中的股票、债券和期权都可以进行数字化而成为数字资产。一般来说，人们认为代币至少整合了股权（具有增值、长期收入等特点）、财产（代表使用权、商品或服务）和货币（在一定范围内流通）的属性。

DAO 的发起人、开发者和其他利益相关者分享系统的产权。对于 DAO 的其他参与者来讲，主要的经济激励是代币。

代币创造的新经济模式被称为代币经济（Token Economy），特指利用加密数字资产的金融属性，将商品和服务使用代币来衡量其价值。目前，常见的代币类型包括支付代币、功能代币、资产代币等。

每个 DAO 可以发行自己的代币，并根据项目属性设置代币系统的发行模式、流通量、质押锁定期等要素。一个 DAO 项目的代币模型的关键是激励机制的设计。其目的是促进参与者的积极参与并做出贡献，实现与 DAO 项目的双赢。一个好的代币模式，一方面可以将货币资本、人力资本和其他资本整合在一起，重塑人与组织的关系，降低 DAO 的运营成本；另一方面，也可以满足项目发起初期的资金需求。当前 DAO 典型的激励方案主要包括以下几种典型方式 [60]：

- **回溯性激励提案**。该方案的贡献者在做出贡献后自主提交奖励申请。奖励金额由贡献者自己提出，同时需要列出他们为 DAO 所创造价值的证据。

- **流支付**。该方案依托软件实现自动化的激励模式。激励奖励像工资一样周期性支付给贡献者。（例如 superfluid 就是一种流支付工资软件）。

- **集体评议奖励**。顾名思义，该方案根据其他人对某成员贡献的评价来决定为贡献者发放多少激励金额。

- **赏金制**。该方案会明确所发布任务的奖励，完成任务即可获得相应的奖励。

10.1.2 *DAO* 的去中心化治理

虽然 DAO 的管理方式是开放的，无许可的，但 DAO 依然需要解决“可以信任谁”、“可以与谁合作”、“奖励应该给谁”的问题。如果采取传统的类似公司面试招聘的方式，这将与 DAO 的“成员共治”的精神相违背。所以我们需要一个“链上声誉系统”来判断谁是可信的、可靠的。

当开发人员开始构建 DAO 的社交相关的产品时，他们需要对产品的“声誉/信用/贡献”进行衡量与设计。这时，开发人员就会自然地面临着需要解决如下问题：如何定义好的声誉与糟糕的声誉？好的声誉将获得什么样的权益激励以及相应的治理权力？声誉等级是否代表着治理权力的等级？由声誉获得的权益等级，又该如何保证参与者的经济收益与治理权力的平衡？声誉权益杂糅了经济利益与治理权力，这样是否会造成一种数字化的腐败？一个声誉系统的监督机制又该如何评估 DAO 治理参与者的道德贡献 [54]？如果一个 DAO 缺失了身份认证的功能，在任务悬赏方面可能出现“自问自答”式的类似“女巫攻击”的问题。

可见，实现 DAO 的去中心化的治理，并非一件容易的事情。甚至，如果 DAO 的某个环节存在漏洞，DAO 还可能遭受严重的攻击。比如，DAO 项目中，智能合约扮演者举足轻重的角色。智能合约的安全问题是不可忽视的。这里，笔者分享一个关于智能合约漏洞引发的著名的“The DAO 黑客攻击事件”。2016 年 6 月 17 日，以太坊创始人维塔利克布特林（Vitalik Buterin）心急如焚，急匆匆在 Reddit 上发了一篇帖子“DAO 遭到攻击，请求交易平台暂停 ETH/DAO 的交

易、充值以及提现，等待进一步的通知。最新的情况会尽快更新 [61]。”这是因为，黑客利用了 The DAO（以太坊平台上第一个 DAO 项目）代码里的一个递归漏洞，不停地从 The DAO 资金池里分离资产。随后，黑客继续利用 The DAO 的第二个漏洞，避免分离后的资产被销毁。黑客利用这两个漏洞，进行了两百多次攻击，总共盗走了 360 万的以太币，超过了该项目筹集的以太币总数目的三分之一。

受“The DAO 攻击事件”的影响，以太坊币价格第二天暴跌约 30%。为解决这次危机，有人提议进行硬分叉，这将意味着重大的技术问题与价值观的问题，因为硬分叉相当于在以太坊的区块链上进行修改规则，从而违背了“区块链上的数据不可篡改”的理念。

经过激烈的讨论，维塔利克不得不支持硬分叉。最后，多数人同意了进行硬分叉。2016 年 7 月 20 日晚，以太坊硬分叉之后，形成了两条链：一条为原链（称为“以太坊经典”，简写为 ETC），另一条为新的分叉链（简称为 ETH）。这两条链各自代表不同社区的共识以及价值观。“以太坊经典”一方认为，区块链的精神就是不可被篡改。已经发生的攻击事件木已成舟，已经生成的历史账本就不应该去修改，这是原则问题。ETH 一方则认为，这是黑客发起的盗窃事件，是违法的行为，必须予以作出回应与回击。

Slock.it 的联合创始人兼首席技术官 Christoph Jentzsch 曾撰文回忆了 The DAO 事件。在文末，他总结了从此次事件中学到的教训 [62]：

- 智能合约的安全问题还需要通过实践来改进。这个领域还处于早期阶段，DAO 的发展得一步一步来完善。

- 对于未知事物要时刻保持警惕。现在已经有不少安全方面的工具可用。他们团队也知道存在很多攻击手段，问题就在于，编写 The DAO 代码的时候没人意识到这点。

- 以太坊的工具还不成熟。形式化验证工具在当时还没有被开发出来。The DAO 事件促进了这些安全工具的开发。

- 去中心化系统的治理和投票机制需要改进。提交意见来指导去中心化治理的软件工具当时还没有被开发出来。一些当时的中心化的论坛，比如 Reddit，并不适合去中心化系统的治理。

- 应该逐步发布产品。The DAO 在发布的时候应该更谨慎一些，逐步地推出不同版本会是更好的选择。类似的项目在早期推出时应该保留部分的中心化，然后逐步去中心化。

- 复杂性应该最小化。虽然 The DAO 的代码只有有 663 行，但是，根据统计经验得知，每 1000 行代码就会有 15-50 个软件缺陷。所以，任何 DAO 项目的智能合约代码要尽可能简单。

为了支撑 DAO 的去中心化治理，DAO 渴望“代码是法律（Code is law）”的理念通过智能合约来践行，但实际上这很难实施。因为，法律规则和智能合约之间存在较大的语义差距。此外，DAO 还涉及很多复杂的法律责任和管辖权的问题，比如如何将 DAO 视为一个法律实体？这些问题，都将启发着 DAO 的实践者与研究者持续思考。

Part V

WEB3 与区块链的生态

第 11 章　Web3 如何统领全局？

Web3 被以太坊的联合创始人 Gavin Wood 定义为一种区块链技术，可以基于“无需信任的交互系统”在各方之间实现创新的交互模式。在笔者看来，可以将 web3 描述为基于区块链技术的、将传统 web2 世界的应用改造为去中心化应用过程中使用的一系列互联网技术的合集。在这个合集中，有新的技术、新的范式，而且会诞生新的组织形式（即 DAO）以及新的价值观与世界观。因此，笔者认为，Web3 将统领下一代互联网的全局。

在笔者看来，本章的内容是本书最大的特色。原因是笔者从专业研究者与技术开发者的视角，解读 Web3 的生态，探讨了若干有趣的话题，而且不少话题源自学生、业界从业者、专业投资人、证券交易操作员的真实问题。笔者把这些问题进一步整理后，汇聚成这些小章节，以飨读者。

11.1 WEB3、区块链与元宇宙哪个范畴最大?

这个问题来自于笔者的一个金融从业的朋友。这个问题无论是从问题本身还是从问题的提出者的社会角色来看，无疑都是很有代表性的，因此笔者将对这个问题的看法整理为这一章节。

11.1.1 概括地理解三个概念之间的关系

其实这个问题包含了三个独立的概念，即 web3、区块链、以及元宇宙。我们先简单粗粒度地探讨一下它们之间的关系，总结为如下三条：

1. Web3 可以不使用区块链，也可以不涉及元宇宙。
2. 区块链可以不涉及 web3、也可以不涉及元宇宙，比如比特币就跟这两者都没有直接关系。
3. 元宇宙可以不使用区块链、也可以不涉及 web3。

当然上述这些完全无关的模式，笔者只是说存在这样的例子，不是说这三个概念就是相互完全无关。具体原因我们稍微展开讨论一下。

首先，笔者认为元宇宙的叙事最宏大。而且，从消费者的角度来说，普通用户对元宇宙的感受也最为直接。毕竟人是视觉动物，而元宇宙呈现给用户的视觉效果特别的新奇，而且这种在虚拟世界中的体验是与现实世界截然不同的。

其次，从产业的角度来说，区块链的影响最深远。这是因为区块链影响的是其他两者的底层经济基础设施，以及创

造了新的经济模式。所以，我们说区块链的影响最深远，但是消费者对区块链技术的感知，其实不会那么强烈。

然后，普通用户可能在不久的将来最先能看到 web3 影响广泛的产品。Web3 的最大价值是通过采用新型数字经济模式提出的全新解决方案来解决现有商业模式的核心矛盾。实际上 web3 的基本诉求是：在商业上做到“去寡头化”。在模式上，web3 尊重个人用户的自主选择。关于现在传统寡头化的商业模式与“去中心化金融”模式之间的矛盾已经很明显了，老百姓其实都能看明白。另一方面，从技术的角度来看，市面上也已经问世了很多 web3 模式的解决方案。因此，笔者认为，web3 是普通用户能够看得见的未来。

11.1.2 进一步地探讨三个概念之间的关联

接下来，笔者进一步系统地探讨一下这三个概念之间的关系。

图 36: Web3、区块链以及元宇宙相互之间的关系

如图36所示，我们从 4 个角度来剖析：从发展历程的角度，从产品分类的角度，从生态体系的角度，以及从技术体系的角度。

首先，无论从哪一个角度来看，区块链无疑都是其他两者底层共同的基础设施，本章后续章节有详细的阐述。所以，我们主要来探讨 web3 与元宇宙之间的关系。

从发展历程上看，web3 与元宇宙沿着各自的逻辑发展，二者的发展早期并无任何的关联。具体来说，web3 的名词首次在 2000 年附近第一次被 Tim Berners Lee 提出。稍后，2006 年 web3.0 的概念被 Jeffrey Zeldman 在一篇抨击 web2.0 的博客中提出。后来，跟区块链相关的 web3 的定义被 Gavin Wood 在 2014 年提出并阐释。反观元宇宙，本书前述元宇宙的章节中曾详细介绍过，早期的元宇宙经历了上世纪 90 年代的概念的孕育期，2000 年后的形态塑造期，以及 2021 年起始的快速发展期。可见，web3 与元宇宙的早期发展历程并无明显的“瓜葛”。

从产业分类的角度来看，web3 跟元宇宙产生了交互。这是因为元宇宙的构建者意识到元宇宙需要一个经济系统，而这个经济系统不是被一家独大的某个企业所控制。恰好，web3 基于区块链技术可以为元宇宙构建去中心化的数字经济系统。

进一步地，乐观的概念主义者把 web3 与元宇宙同时称为“下一代互联网”，而且二者在生态体系的角度看似是几乎重合的。这是一个值得辩证的观点。

最后，在技术开发者的眼里，他们可不认为二者是重合的，而是呈现出一个相互支撑的关系。比如，web3 可以为元

宇宙提供去中心化的经济系统（DeFi）、去中心化的组织形式（DAO）、还有丰富多彩的 NFT，等等。元宇宙可以为 web3 提供可以施展拳脚的空间与平台。

11.2 WEB3 与区块链、DAO 的关系

2022 年上半年网络上出现了一篇流传甚广的文章，题目为《Web3 革命：逃离、信仰、大迁；徙》[64]。文中提到“国内至少六家互联网大厂的高管或高级技术人才，放弃了稳定的高薪和可观的期权，主动探索 web3 世界”。紧接着，作者列举了几个有代表性的践行者在这个新兴赛道的早期探索与尝试。比如，美团的联合创始人王慧文对 web3 学习之后，提出了“区块链撕裂了中国互联网，中国互联网的主要矛盾从巨头与创业公司的矛盾转变成古典互联网与区块链之间的矛盾”的观点 [64]。2020 年他从美团退休，开始探索 web3 新的赛道。另一个具有代表性的 web3 的从业者是前“字节跳动”公司 90 后程序员郭宇。2020 年他实现财务自由后从字节跳动离职，开始专心研究区块链技术与应用，后来全身投入 web3 赛道。可见，从传统互联网企业的高管到年轻人，web3 正在源源不断地吸引传统 web2 互联网人的加入。

那么，web3 究竟有什么魔力？让我们回顾一下 web3 的定义。“Web3 是指基于区块链技术的去中心化在线生态系统。许多人认为它代表了互联网的下一个阶段”。一名传统投资机构合伙人认为“目前的 web3 行业，很像 2000 年的互联网”。

目前，web3 行业也逐渐问世了一些雏形产品，比如被视为去中心化的支付宝 Metamask，被视为去中心化的 QQ

音乐 Audius，以及全球最大的 NFT 交易平台 Opensea，等等。这些去中心化的应用已经在全球范围内吸引了千百万的用户，这些公司也逐渐成为全球最具影响力的公司。

如果用一句话概括一下 web3 与区块链、还有 DAO 之间的关系，笔者认为如下这句话最合适："区块链是一种技术，DAO 是一种制度，web3 则是一种文化" [64]。

目前，web3 与 DAO 已经被应用到了互联网、金融、艺术等等具有代表性的为数不多的几个行业。但是，这场变局已经悄悄铺开了 10 年之久。不用焦虑，社会大众对 web3 文化的了解，远远尚未成熟。未来，这个赛道是一片蓝海。

11.3 NFT 与区块链、元宇宙的关系

人们在弄明白了区块链技术可以为数字艺术品提供新的发布与流转方式之后，开始逐渐认可 NFT 的价值。这是因为数字艺术品被铸造成 NFT 后，就拥有了数字资产的属性。再加上投资界的持续炒作，加速了 NFT 的火爆出圈。尤其是从 2021 年开始，元宇宙的蹿红也直接促进了 NFT 的出圈。

那么，NFT 和元宇宙、区块链之间到底有什么样的关系呢？其实这个问题来自于笔者的一位播客听友曾同学，她是中山大学传播与设计学院的一位研究生。有一天曾同学通过邮件联系了笔者，咨询了如上的这个问题。笔者对这个问题进行了回复。后来曾同学将部分观点转述到她们团队的公众号文章。稍微扩充之后，笔者将对这个问题的观点通过以下三个方面做出更详细的阐述，分享给读者朋友。

内容略去一部分

第 12 章　对区块链生态的探讨

导读：本章节，笔者对区块链生态做出深层次的探讨。内容将包括挖矿与算力的探讨，区块链与加密货币的关联，区块链的分层架构，区块链跨链技术，以及区块链企业榜单的话题。

12.1　POW 挖矿与算力

在比特币挖矿过程中，所谓的“矿工”是指以计算为手段，获得相应的比特币出块奖励与手续费的矿机。一个矿工不会验证一个单独的比特币的转账交易，而是会将一系列的交易打包形成“区块”，并通过计算其块的 hash 值进行验证。比特币采用“工作量证明（PoW）”算法实现共识，即一种对某个特定目标难度值进行计算的共识机制。具体来讲，使用基于 SHA-256 算法的 PoW 机制要求每台矿机通过暴力破解方法解决一个数学难题。当矿机参与 hash 计算后得到一个符合目标难度值的 hash 值时，这台矿机就可以获得“记账权”，并可以获得一定数量的比特币的“出块奖励”。

在 PoW 共识协议中，矿工可以通过获得新币奖励和交易费的收入，这种方式提供了比特币网络的激励机制。同时，全网的算力提供了比特币的安全性。虽然说一个贪婪的攻击者能够通过某种技术手段汇集比诚实矿工节点更多的算力，即可以发动 51% 攻击，但是他将不得不在使用高昂的算力成

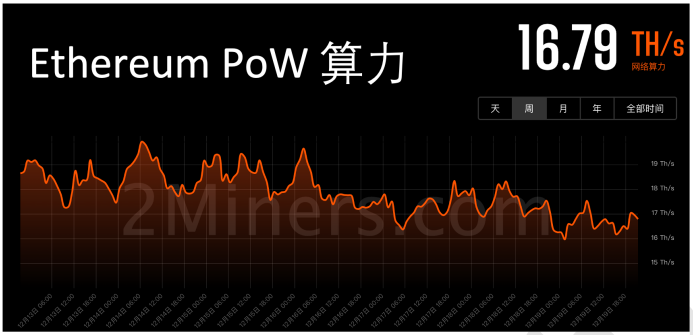

图 41: Ethereum PoW 网络算力反映的是 ethw 网络中所有矿工的整体性能。目前，Ethereum PoW 网络算力为 16.79 TH/s = 16 79 0 903 872 893 h/s。网络算力利用当前网络难度、加密货币网络设定的平均区块查找时间和最新区块的有效区块查找时间计算得出 [96]。

本进行攻击和用其产生新币之间做出选择。从经济学角度考虑，遵守比特币系统规则所获利益在大多数情况下要大于发起 51% 攻击带来的利益。因此，在假设全网矿工都是理智的假设下，比特币的网络是安全的，因为至今为止没有一个实体可以控制超过全网一半以上的算力。

随着计算机硬件技术的发展，矿工的“挖矿”算力越来越强大。从全网的角度看，全网的算力也会得到提升（如图41），从而让潜在的 51% 攻击者的攻击成本也提高了，看似比特币的区块链变得更安全了。但是升级全网的算力也会让区块产生的速度提高。区块产生的间隔变短将会导致比特币的区块链发生更多的“分叉”冲突，从而降低了主链区块的产生速度。这样也会导致攻击者更容易“追上”或者“赶超”主链的

长度，最终可能破坏比特币的区块链。可见，升级矿工的算力也会带来副作用。

现实情况是，在一个去中心化的区块链网络中，没人可以限制矿工升级自己的挖矿设备。在正常的情况下，矿工为了赚取更多的挖矿奖励，他们会自发地升级自己的算力。从历史上看，除去发生了黑天鹅事件，比如受某些国家与地区重大政策的限制或者矿工所在的地区发生了战争，比特币整体的算力是在逐渐增强的。那么，为了维持比特币整体出块的稳定，比特币的区块链将不得不经常改变挖矿难度，来匹配变化的全网算力。

那么，比特币系统中挖矿的难度调整是怎么一回事呢？实际上，比特币每一个挖矿难度的调整周期大概为两个星期的时间。比特币网络可以根据上一周期的出块情况来动态调整挖矿难度（通过调整限制满足难道要求的 hash 字符串的前若干位“0”的数目），来确保整个网络生成一个新区块的时间稳定在 10 分钟左右。比特币的难度调整公式如下：下一周期的难度系数 = 当前周期的难度系数 * (20160 分钟/当前周期 2016 个区块的实际出块时间)。

虽然说，比特币的 PoW 挖矿机制与难度调节机制设计得很巧妙，但是，PoW 共识算法仍然有 3 个广受批评的方面：

- 资源浪费。图42 展示了 PoW 挖矿与算力之间的关系。矿工为求解区块链的 PoW “谜题”，需要进行大量的哈希运算，这需要消耗大量的电力和各种算力资源，而且找到的符合难度要求的哈希值实际上并没有任何的现实使用价值。简单地说，比特币挖矿就是比特币矿工参与算力运算竞争，通过哈希运算，看谁先计算出符合预

图 42: PoW 挖矿与算力

先定义好规则的“幸运数字”，从而获得打包区块链转账交易生成区块的的权利。

- 交易吞吐量低下。因为 PoW 共识算法限制比特币出块的时间是 10 分钟左右，所以每一笔提交到比特币网络的交易至少需要 10 分钟才可能被打包上链。而且，由于比特币遵循“最长链原则”，通常这笔交易还需要等待大概 6 个区块才能被全网一致性确认。这些因素限制了比特币仅支持每秒 7 笔左右的交易处理速度，并不适合高并发的商业应用场景。

- PoW 共识算法算力集中化。目前，“矿池”是比特币网络挖矿的主力，个人矿工基本不可能单独生存下去。算力聚集度高的矿池变得越来越有话语权，进而导致算力的集中化。这一点是有悖于比特币网络去中心化的特点的。

从技术上看，PoW 算法的核心矛盾是区块大小与出块间隔。增加区块容量可以提高吞吐量，但是区块过大会造成网络传输的拥塞，反而会降低节点间共识的效率，结果可能降

低区块链的吞吐量。而减小出块间隔也能增加单位时间内的出块量，但出块间隔的缩短会造成更频繁的区块链“分叉”，这样会带来“双花攻击”的可能性变高，等等安全问题。

随着公有链共识机制的发展，PoW 共识算法产生了许多变种。对现有这些从性能和安全性角度进行提升的方法可以被归为两种，一种是在不改变 PoW 共识机制的基础上，对链的增长方式进行改造，重新分配记账权，减小无序竞争和出块间隔；二是不对 PoW 共识算法内容做修改，通过链下扩展机制，对链上交易量进行卸载，旨在提升主链的效率。

12.2 区块链一定需要加密货币吗？

对于这个问题，首先一定要分清楚是何种类型的区块链。早期以比特币为代表的区块链，还有后续出现的一些类似于比特币的竞争币，如莱特币、点点币等等这些加密货币底层的区块链，根本的功能就是转账。所以，早期的公链肯定是需要加密货币的。

对于后来陆续出现的其他类型的区块链，比如许可链，也叫联盟链。联盟链也是我国现在大力推广的一个战略性方向。联盟链在国内通常被用于与实体经济相关的很多应用场景。在这些应用场景里面，通常不存在加密货币这么一个角色。而且，加密货币的炒作在我国也是被禁止的。由此可见，并不是所有的区块链都发行加密货币。

另外一个衍生的问题是：联盟链既然没有加密货币，那么联盟链是否需要激励机制呢？我想若干个联盟单位建立一条联盟链。比如某大学的几个附属医院之间，以联盟链的形

式组织起来分享病人的数据。在这个场景中应该会存在联盟成员之间的激励问题。比如，假如某些联盟成员不愿意分享自己的数据，该怎么办呢？这个时候就需要联盟链相关的激励机制来发挥作用了。至于如何设计联盟链的激励机制，我想可能有很多的方法，比如可以通过链下的方式去设计针对联盟链成员的激励机制。这里我们就不展开了。

12.3 区块链的 LAYER1, LAYER2 与 LAYER3 简述

由于可信任、防篡改和去中心化的特性，区块链技术保障了交易数据的安全可追溯，但同时也面临着交易吞吐量低的问题。近来年，研究者为了提升区块链的性能，陆续提出了区块链的 Layer1 扩展方案以及 Layer2 和 Layer3 解决方案，如图 43 所示。本小节简单介绍区块链中这些不同 Layer 相关的概念。

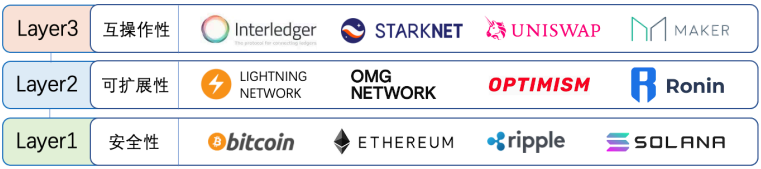

图 43: 区块链不同 Layer 的特性以及代表性案例

12.3.1 *Layer1 介绍*

区块链的 Layer1 是指区块链底层，也即区块链系统本身层面，比如比特币系统的 Layer1 就是比特币的主链。因此，Layer1

内容略去一部分

第13章　未来的展望

13.1　国内外区块链发展路线对比

本节我们简单聊聊国内外对公链和联盟链的发展路线。国内没有直接说不允许公链的发展，公链比较敏感。目前国内发展较多的是联盟链。但联盟链的生态其实步履艰难，主要原因就是应用生态很弱。即使区块链是个好东西，而且有一些项目和产品也落地了，比如长安链、海河智链等区块链项目。但是，一个问题是，就算把区块链做出来，也会发现没有太多“用武之地”。这样就让人看到一个很危险的信号。相比之下，国外的区块链生态发展得非常好，而且是越来越火热，现在几乎成为了国外互联网创新的一个核心基础。

区块链技术通过它的第一个产品比特币被提出来的时候，它的唯一目的是实现具有交易转账功能的数字货币。事实证明，区块链技术的确成功地实现了支持数字货币的目标。但是要注意，区块链技术初始创设起来的时候根本没有“联盟链”的概念与领域，只是后来有人把区块链应用到了一些适合联盟链的场景。

其实区块链技术本身也能支持实现各种的去中心化应用，但是要基于数字货币，或者更严谨一点说基于“加密货币”的基础上去做的各种各样的DApp，包括NFT、DeFi、社交游戏金融（GameFi），等等新型数字经济产物。

事实上，国外的区块链技术并不存在“应该应用到哪里?”这种疑问。有些基于区块链技术的去中心化的应用已经落地并迅速获得了市场的认可。在如何应用区块链技术这个方面，我们会发现国内和国外的观点其实是有较大差别的。在未来几年，笔者猜测国内外的区块链技术与相关行业仍然会按照各自的思路与顶层设计，各自发展。但是，乐观的一方面是，国内的区块链行业也不是一味地埋头苦干，还是有一些企业家会“抬头看路”。希望未来国内的区块链行业会走出自己的特色。

13.2 区块链的下一个五年是什么?

从 2017 年开始，我国监管部门逐渐打击各种雨后春笋般冒出来的加密货币，或者叫山寨币。随后，区块链技术开始在各种政策的积极刺激下，逐渐为各行各业赋能，包括金融、供应链、数字政务等等行业。但是，当时一个亟待解决的问题是：基础设施不完善，没有高性能的底层区块链系统。于是，各个头部大厂如腾讯、阿里、华为，还有国家队长安链等等，甚至包括出身学术界的树图公链 Conflux，纷纷入局建设各自的区块链系统平台。这些头部企业与机构也不负众望，纷纷推出了自己的区块链产品。

经过近 5 年的飞速发展时期，区块链基础设施相当完善了。那么、一个新问题也摆在了人们面前：国内区块链技术在接下来 5 年会有什么样的发展前景?

虽说区块链赋能了很多行业，但是目前为止仍然没有看到一个杀手级的、属于未来的应用。在 2021 年底举行的 CCF

中国区块链技术大会（中国计算机学会旗下最具有权威的区块链技术大会），很多与会专家认为元宇宙将会是区块链的杀手级的应用。但是现在仅仅过去了不到一年的时间，回过头去看，从 2022 年的第二季度开始，大家对元宇宙的热情貌似突然转冷。下半年的情况好一些，但是元宇宙中有说服力的应用仍然没有面世。

那么，将来区块链技术的杀手级的应用会是数字经济吗？即便现在国内有些链企提出了「无币公链」的概念，貌似可以规避监管。但是，不论无币公链如何实现，公众可能仍然会好奇：如果一个区块链公链不发行「代币」，那么这个「无币公链」如何支持通证经济？「无币公链」与国内主推的联盟链，它们的应用场景又有哪些差别呢？这些问题值得我们进一步思考与探索。

13.3 WEB3 发展趋势与展望

Web3 将改变当前互联网架构与生态，将会解决 web2 语境存在的数据隐私泄漏、数据垄断以及算法作恶等问题，让互联网用户真正实现自主管理和拥有数据，帮助用户构建更加开放、安全和普惠的互联网生态。Web3 的视线并不仅仅依靠部分群体的技术创新，而需要大众积极参与，同时更需要社会与国家层面的关注，共同构建更加完善的法律治理体系，为 web3 的建设提供一个合适的土壤。本小节，笔者面对 web3 的创新发展策略，做出以下几个方面的思考。

内容略去一部分

结束语

Web3 构建了一个允许所有参与者共建共享、安全可信的价值互联网。用户通过 web3 的分布式架构，实现自主可控的价值转移，真正帮助用户实现“价值拥有”。

本书从区块链技术出发，结合元宇宙、NFT、DAO 等概念，对基于区块链的 web3 生态进行了技术方面的探讨，并展望了 web3 的未来发展趋势。

区块链作为国家近年来大力倡导的新兴技术，是构建 web3 与元宇宙的引擎。本书重点阐述了区块链技术如何赋能 web3、元宇宙、NFT、DAO，并自底向上地从各个角度对 web3 生态做了详细的剖析。

从技术的角度看，国内 web3 的相关研究起步较慢。在推进 web3 的发展过程中应该借鉴业界前沿的项目和技术，取长补短，抓住历史绝佳机遇，加快建设下一代互联网。从国家发展的角度来看，需要相关部门多一些开放包容的心态，鼓励相关技术创新，同时制定相关的法律和监管政策，保障 web3 的安全可持续发展。

Web3 与元宇宙代表着未来互联网，它们的概念内涵和应用领域还在不断地丰富和扩展。Web3 与元宇宙带给用户新奇体验的同时，也将产生更多的机遇和挑战。我们需要抓住机遇，坦然面对挑战。

若想在未来 20-30 年内不落后于时代，不仅需要社会各个层面的仁人志士明辨方向、有序竞争、创新引领，也需要业界、学界、监管部门集思广益、通力协作、共同建设。

种一棵树最好的时间是十年前，其次是现在。元宇宙已经在这片土地上生根发芽，web3 也必将枝繁叶茂！

参考文献

[1] 徐璐, 曹三省, 毕雯婧, 成于庆, and 柴剑平. Web2.0 技术应用及 web3.0 发展趋势. 中国传媒科技, (5):3, 2008.

[2] S. Ramakrishnan. Web 3.0: The evolution. *ITNOW*, (2):2, 2022.

[3] Victoria Shannon. A More Revolutionary Web. *The New York Times*, 23, 2006.

[4] Gavin Wood. Đapps: What Web 3.0 Looks Like. https://gavwood.com/dappsweb3.html, 9 月 6 日, 2022 年.

[5] MetaMask community. A Crypto Wallet & Gateway to Blockchain Apps. https://metamask.io/, 9 月 6 日, 2022 年.

[6] Lukas Lukac. A Technical Guide to IPFS–the Decentralized Storage of Web3. https://www.freecodecamp.org/news/technical-guide-to-ipfs-decentralized-storage-of-web3, 9 月 6 日, 2022 年.

[7] Jeffrey Zeldman. Web 3.0. *A List Apart*, 16, 2006.

[8] Pooja Dixit, Anuja Bansal, Pramod Singh Rathore, and Manju Payal. An overview of blockchain technology: Architecture, consensus algorithm, and its challenges. *Blockchain Technology and the Internet of Things*, pages 21–46, 2020.

[9] Ali Arjomandi-Nezhad, Mahmud Fotuhi-Firuzabad, Ali Dorri, and Payman Dehghanian. Proof of humanity: A tax-aware society-centric consensus algorithm for blockchains. *Peer-to-Peer Networking and Applications*, 14(6):3634–3646, 2021.

[10] Mostefa Kara, Abdelkader Laouid, Muath AlShaikh, Mohammad Hammoudeh, Ahcene Bounceur, Reinhardt Euler, Abdelfattah Amamra, and Brahim Laouid. A compute and wait in pow (cw-pow) consensus algorithm for preserving energy consumption. *Applied Sciences*, 11(15):6750, 2021.

[11] Mohamed Sabt, Mohammed Achemlal, and Abdelmadjid Bouabdallah. Trusted execution environment: what it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 57–64. IEEE, 2015.

[12] Oasis Protocol Project. The oasis blockchain platform, 9 月 6 日, 2022 年.

[13] 罗兰. 美国“印钞”向他国转嫁通胀. http://finance.people.com.cn/n/2013/0322/c1004-20883307.html, 3 月 22 日, 2013 年.

[14] 魏丽婷, 郭艳, and 贺梦蛟. 非同质化代币 (nft): 逻辑, 应用与趋势展望. 经济研究参考, (4):11, 2022.

[15] 韩亚峰. 数字账本技术非同质化代币的特征与安全挑战. 中国信息安全, (000-001), 2022.

[16] 秦蕊, 李娟娟, 王晓, 朱静, 袁勇, and 王飞跃. Nft: 基于区块链的非同质化通证及其应用. 智能科学与技术学报, (003-002).

[17] RareBearsByEnox. Rare Bears Nft - Official. https://opensea.io/collection/rarebearsnft-official, 9 月 6 日, 2022 年.

[18] NBA Top Shot. Marketplace. https://nbatopshot.com/search?byMomentTiers=MOMENT_TIER_RARE, 9 月 6 日, 2022 年.

[19] ForesightNews. Nft 简史：跨越六十年的 nft 群星闪耀时刻. https://foresightnews.pro/article/h5Detail/17279.

[20] COIN GEEk. 什么是非同质化代币？非同质化代币在加密货币领域的崛起. https://coingeek.com/zh-hans/bitcoin-for-beginners/what-is-nft-the-rise-of-non-fungible-tokens-in-cryptocurrency/, 9 月 6 日, 2022 年.

[21] 欧易交易所. Bitcoin 价格. https://www.okx.com/cn/markets/prices/bitcoin-btc, 9 月 6 日, 2022 年.

[22] Susan Blackmore, Lee Alan Dugatkin, Robert Boyd, Peter J Richerson, and Henry Plotkin. The power of memes. *Scientific american*, 283(4):64–73, 2000.

[23] Nat Eliason. Tokenomics 101: The Basics of Evaluating Cryptocurrencies. https://every.to/almanack/tokenomics-101, 9 月 6 日, 2022 年.

[24] 林永青. 何为通证经济? 金融博览, 1, 2019.

[25] 凯利. 数字货币时代: 区块链技术的应用与未来. 中国人民大学出版社, 2017.

[26] 管筱璞李云舒. 深度关注 | 元宇宙如何改写人类社会生活. https://www.ccdi.gov.cn/toutiaon/202112/t20211223_160087.html, 9 月 6 日, 2022.

[27] 龚才春. 中国元宇宙白皮书. https://www.healthit.cn/wp-content/uploads/2022/01/2022%E4%B8%AD%E5%9B%BD%E5%85%83%E5%AE%87%E5%AE%99%E7%99%BD%E7%9A%AE%E4%B9%A6-%E9%BE%9A%E6%89%8D%E6%98%A5.pdf, 9 月 6 日, 2022 年.

[28] 勒庞. 乌合之众: 大众心理研究. 中央编译局, 2015.

[29] 赵国栋, 易欢欢, and 徐远重. 元宇宙. 商学院, 12:120, 2021.

[30] Aleena Chia. The metaverse, but not the way you think: game engines and automation beyond game development. *Critical Studies in Media Communication*, pages 1–10, 2022.

[31] Qinglin Yang, Yetong Zhao, Huawei Huang, Zehui Xiong, Jiawen Kang, and Zibin Zheng. Fusing Blockchain and AI with Metaverse: A Survey. *IEEE Open Journal of the Computer Society*, 3:122–136, 2022.

[32] Vitalik Buterin. And We Finalized! https://twitter.com/VitalikButerin/status/1570306185391378434, 9 月 6 日, 2022 年.

[33] Uriel Singer, Adam Polyak, Thomas Hayes, Xi Yin, Jie An, Songyang Zhang, Qiyuan Hu, Harry Yang, Oron Ashual, Oran Gafni, et al. Make-a-video: Text-to-video generation without text-video data. *arXiv preprint arXiv:2209.14792*, 2022.

[34] Jonathan Ho, William Chan, Chitwan Saharia, Jay Whang, Ruiqi Gao, Alexey Gritsenko, Diederik P Kingma, Ben Poole, Mohammad Norouzi, David J Fleet, et al. Imagen video: High definition video generation with diffusion models. *arXiv preprint arXiv:2210.02303*, 2022.

[35] Baidu. Ernie-vilg 文生图. https://wenxin.baidu.com/ernie-vilg, 9 月 6 日, 2022 年.

[36] 杨强, 范力欣, 朱军, 陈一晰, 张拳石, and 朱松纯. 可解释人工智能导论. 中文信息学报, 36(5):1, 2022.

[37] Long Ouyang, Jeff Wu, Xu Jiang, Diogo Almeida, Carroll L Wainwright, Pamela Mishkin, Chong Zhang, Sandhini Agarwal, Katarina Slama, Alex Ray, et al. Training language models to follow instructions with human feedback. *arXiv preprint arXiv:2203.02155*, 2022.

[38] Ronald John Johnston et al. *Nature, state and economy: a political economy of the environment.* Number Ed. 2. John Wiley & Sons Ltd, 1996.

[39] 刘哲昕. 系统经济法论: 经济法本质及其与 WTO 关系研究. 系统经济法论: 经济法本质及其与 WTO 关系研究, 2006.

[40] 罗良清 and 龚颖安. 虚拟经济的本质及影响实体经济的机理. 江西财经大学学报, (2):5–9, 2009.

[41] 高智谋. Libra 彻底破产？扎克伯格挑战主权货币完败！. https://wallstreetcn.com/articles/3650695, 9 月 6 日, 2022 年.

[42] 市场咨询. 报道称母公司 meta 面临另一项反垄断调查. https://finance.sina.cn/usstock/mggd/2022-01-15/detail-ikyakumy0467223.d.html, 9 月 6 日, 2022 年.

[43] 卢现祥, 朱巧玲, et al. 新制度经济学, volume 2. 武汉大学出版社, 2011.

[44] 张曙光. 论制度均衡和制度变革. 经济研究, 6:30–36, 1992.

[45] 刘和旺 and 颜鹏飞. 论诺思制度变迁理论的演变. 当代经济研究, (12):21–24, 2005.

[46] Kokii. Web3 的底层逻辑：制度经济学视角. https://foresightnews.pro/article/h5Detail/12662, 9 月 6 日, 2022 年.

[47] Saffron Huang, Josh Stark. Who Will Control Crypto? https://saffron.mirror.xyz/E6UKhw0KAZL1TgAeI_pcWSwkUDHOQ5R28OBHknTzy24, 9 月 6 日, 2022 年.

[48] 每日经济新闻. 清华大学教授沈阳：元宇宙对算力的要求是目前 1000 倍以上，中国有 10 多年窗口期突破核心技术. https://finance.sina.com.cn/chanjing/cyxw/2022-03-10/doc-imcwiwss5271286.shtml, 9 月 6 日, 2022 年.

[49] 天风证券. 一文看懂元宇宙的 6 层框架、4 大赛道. https://www.ccvalue.cn/article/1305599.html, 9 月 6 日, 2022 年.

[50] Shuai Wang, Wenwen Ding, Juanjuan Li, Yong Yuan, Liwei Ouyang, and Fei-Yue Wang. Decentralized autonomous organizations: Concept, model, and appli-

cations. *IEEE Transactions on Computational Social Systems*, 6(5):870–878, 2019.

[51] SeeDAO community. Dao it, do it！. https://seedao.xyz/, 九月 6 日, 2022 年.

[52] GitCoin. Build and Fund the Open Web Together. https://gitcoin.co/, 9 月 6 日, 2022 年.

[53] CULT DAO. Cult.dao the Manifesto. https://cultdao.io/manifesto.pdf, 9 月 6 日, 2022 年.

[54] VION WILLIAMS. 加密精英的傲慢：对 dao 的深层批判/论 dao 的七宗罪/daos 微观权力结构. https://www.panewslab.com/zh/articledetails/1xtizxav.html, 9 月 6 日, 2022 年.

[55] DAO Experts. Govern better, together. build your dao now. https://aragon.org, 9 月 6 日, 2022 年.

[56] WILLY OGORZALY. The Best Way to Build Your Dao. https://colony.io/, 9 月 6 日, 2022 年.

[57] DAOstack. Building Collaborative Networks. https://daostack.io/, 9 月 6 日, 2022 年.

[58] Snapshot. Where Decisions Get Made. https://snapshot.org/, 9 月 6 日, 2022 年.

[59] Btcwbo. Dao 投票平台 snapshot 为啥值得关注？. http://www.btcwbo.com/4975.html, 9 月 6 日, 2022 年.

[60] The SeeDAO. 你真的理解 dao 激励和奖励吗? . https://mp.weixin.qq.com/s/8yltLUMo9Zq0kQ3-LKERUw, 9 月 6 日, 2022 年.

[61] Ethereum. <dao attack> exchanges please pause eth and dao trading, deposits and withdrawals until further notice. more info will be forthcoming asap. https://www.reddit.com/r/ethereum/comments/4oif2x/dao_attack_exchanges_please_pause_eth_and_dao/, 9 月 6 日, 2022 年.

[62] Christoph Jentzsch. The history of the dao and lessons learned. https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5, 9 月 6 日, 2022 年.

[63] E Glen Weyl, Puja Ohlhaver, and Vitalik Buterin. Decentralized Society: Finding Web3's Soul. *Available at SSRN 4105763*, 2022.

[64] 虎嗅 App. Web3 革命：逃离、信仰、大迁徙. https://www.jiemian.com/article/7391325.html, 9 月 6 日, 2022 年.

[65] 李伟. 区块链是 web3.0 时代的核心基础设施. https://mp.weixin.qq.com/s/RmQI07fpTgpP58u50f_nnA, 9 月 6 日, 2022 年.

[66] Opensea Developers. Metadata standards. https://docs.opensea.io/docs/metadata-standards.

[67] Filecoin Slack. What is Filecoin. https://docs.filecoin.io/about-filecoin/what-is-filecoin/, 9 月 6 日, 2022 年.

[68] Web3 智慧空间. Web3 中的数据存储 | 去中心化永久存储：arweave. https://lunjin.net/finance/Z4eGpefc66.html, 9 月 6 日, 2022 年.

[69] CoinYuppie. Arweave: An experiment in permanent storage. https://coinyuppie.com/arweave-an-experiment-in-permanent-storage/, 9 月 6 日, 2022 年.

[70] Laszlo Fazekas. A Brief Introduction to Ethereum Swarm. https://medium.com/geekculture/a-brief-introduction-to-ethereum-swarm-db6d79657e60, 9 月 6 日, 2022 年.

[71] STORJ. Fast, secure cloud storage at a fraction of the cost. https://www.storj.io/, 9 月 6 日, 2022 年.

[72] Hashkey Hub. 万字讲透去中心化存储. https://zhuanlan.zhihu.com/p/107707161, 9 月 6 日, 2022 年.

[73] W3C. Decentralized identifiers (dids) v1.0. https://www.w3.org/TR/did-core/, 19 July, 2022.

[74] W3C. A primer for decentralized identifiers. https://w3c-ccg.github.io/did-primer/, 11 November 2021.

[75] Jia Shi, Xuewen Zeng, and Rui Han. A blockchain-based decentralized public key infrastructure for information-centric networks. *Information*, 13(5):264, 2022.

[76] 张开翔. 数字时代的身份基础设施建设. https://www.ccvalue.cn/article/345969.html, 10 月 11 日, 2021.

[77] AMBER. Decentralized identity: Passport to web3. https://www.ambergroup.io/newsDetail?source=marketNews&id=40237.

[78] BrightID. Bright dao is here! https://www.brightid.org/.

[79] WeIdentity. Weidentity 文档. https://weidentity.readthedocs.io/zh_CN/latest/, 9 月 6 日, 2022 年.

[80] DID 开发者中心. 系统架构. http://did.baidu.com/architecture/, 9 月 6 日, 2022 年.

[81] Cosimo Sguanci, Roberto Spatafora, and Andrea Mario Vergani. Layer 2 blockchain scaling: A survey. *arXiv preprint arXiv:2107.10881*, 2021.

[82] 分散式身份识别. 拥有你的数字身份. https://www.microsoft.com/zh-cn/security/technology/own-your-identity, 9 月 6 日, 2022 年.

[83] DIF. Sidetree v1.0.0. https://identity.foundation/sidetree/spec/, 9 月 6 日, 2022 年.

[84] Wikipedia. Microsoft ion. https://en.wikipedia.org/w/index.php?title=Microsoft_ION&oldid=1055984592, 9 月 6 日, 2022 年.

[85] The Identity Hub. Welcome to the identity hub. https://docs.theidentityhub.com/doc/Index.html., 9 月 6 日, 2022 年.

[86] Phillip J Windley. Sovrin: An identity metasystem for self-sovereign identity. *Frontiers in Blockchain*, page 30, 2021.

[87] Nitin Naik and Paul Jenkins. uport open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain. In *2020 IEEE International Symposium on Systems Engineering (ISSE)*, pages 1–7. IEEE, 2020.

[88] UNIPASS. Your passport to studying overseas. https://unipass.co.ke/.

[89] ARCx. Better borrowing. https://arcx.money/, 9 月 6 日, 2022 年.

[90] RabbitHole. Learn and earn crypto by using the best web3 applications. https://rabbithole.gg/.

[91] 数据治理研究. 腾讯关闭幻核：规避风险，抢占赛道. https://www.yuanyuzhouneican.com/article-152329.html, 9 月 6 日, 2022 年.

[92] 人民邮电报. 《上海市数字经济发展“十四五”规划》发布 2025 年数字经济增加值将达 3 万亿元. https://www.cnii.com.cn/rmydb/202207/t20220719_397536.html, 9 月 6 日, 2022 年.

[93] Haihan Duan, Jiaye Li, Sizheng Fan, Zhonghao Lin, Xiao Wu, and Wei Cai. Metaverse for Social Good: A University Campus Prototype. In *Proceedings of the 29th ACM International Conference on Multimedia*, pages 153–161, 2021.

[94] Chenglin Pua（马来西亚）. 元宇宙大学正在就位. https://www.bitpush.news/articles/3160302, 9 月 6 日, 2022 年.

[95] Nir Kshetri. 在元宇宙中上大学或将面临的 5 个挑战. https://theconversation.com/5-challenges-of-doing-college-in-the-metaverse-189921, 9 月 6 日, 2022 年.

[96] 2MINERS.COM. Ethereum pow 算力. https://2miners.com/zh/ethw-network-hashrate, 9 月 6 日, 2022 年.

[97] Mohammad Musharraf. What is the Blockchain Trilemma. https://www.ledger.com/academy/what-is-the-blockchain-trilemma, 11 月 15 日, 2021 年.

[98] E Buchman Tendermint. *Byzantine fault tolerance in the age of blockchains*. PhD thesis, Master's Thesis at University of Guelph, Ontario, 2016.

[99] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. *White Paper*, 21:2327–4662, 2016.

[100] BIS Innovation Hub. Inthanon-lionrock to mbridge: Building a multi cbdc platform for international payments. https://www.bis.org/publ/othp40.pdf, 2021.

[101] 福布斯. 福布斯发布 2022 年全球区块链 50 强，蚂蚁、腾讯、百度等中国企业上榜. https://mp.weixin.qq.com/s/YteaKOJp2qP58HwTfIO71A, 9 月 6 日, 2022 年.

[102] 区块链大本营. 福布斯：2022 区块链 50 强榜单. https://mp.weixin.qq.com/s/QSjj37_7WzBDwDkzyC85qA, 9 月 6 日, 2022 年.

[103] 树图区块链研究院. 让区块链变成人人可用的工具，上海原创 web3.0 操作系统是如何诞生的. https://mp.weixin.qq.com/s/WS4-ST2M0yS5s42K_HkWCQ.