目录

[从比特币到Web 3 1](#_Toc976465696)

[CIP页用中文图书简介 2](#_Toc388922298)

[作者简介 2](#_Toc1824324665)

[内容简介 1](#_Toc1800616436)

[自序 2](#_Toc620886328)

[第1章 去中心化与信任的重构 3](#_Toc613473923)

[1.1 中心化信任机制的局限 3](#_Toc587234614)

[1.1.1 从加密朋克到赛博货币 3](#_Toc1964799533)

[1.1.2 信任危机的历史与案例 5](#_Toc529711212)

[1.1.3 中心化架构的三重瓶颈 7](#_Toc1536623269)

[1.2 比特币的信任创新与制度实验 9](#_Toc388943261)

[1.2.1 建立在密码学 + 博弈机制基础上的“去信任”系统发明 10](#_Toc29166159)

[1.2.2 比特币的制度构造解析 11](#_Toc569362797)

[1.2.3 思想演化与现实影响 14](#_Toc93398147)

[1.3 Web 1.0到Web 2.0再到Web 3 的演化路径 16](#_Toc2079594319)

[1.3.1 Web 1.0 16](#_Toc1445364508)

[1.3.2 Web 2.0 19](#_Toc2053754739)

[1.3.3 Web 3 21](#_Toc951240142)

[1.3.4 批判视角与挑战声音 25](#_Toc1624798326)

[1.4 Web 3 栈的概念、架构、争议与未来图景 27](#_Toc583409830)

[1.4.1 Web 3技术架构的典型分层 27](#_Toc2106164255)

[1.4.2 基础设施与范式转移的动因 30](#_Toc1329680284)

[1.4.3 争议与路径分歧 33](#_Toc1221702506)

[1.4.4 未来技术、制度与思想的三维演化 35](#_Toc1062869375)

[本章小结 37](#_Toc876609879)

[第2章 密码学基础与共识机制 39](#_Toc1444417933)

[2.1 非对称加密、哈希函数与Merkle树 39](#_Toc1177054243)

[2.1.1 密码学在区块链中的角色定位 39](#_Toc131305937)

[2.1.2 以RSA和ECC为代表的非对称加密 41](#_Toc1393177690)

[2.1.3 哈希函数的单向性、抗碰撞性和雪崩效应 44](#_Toc1123232589)

[2.1.4 Merkle树结构与验证逻辑 47](#_Toc1788866193)

[2.2 公私钥签名验证与交易结构 50](#_Toc703047751)

[2.2.1 公钥、私钥与地址生成 50](#_Toc668525263)

[2.2.2 数字签名与验证流程 53](#_Toc269654137)

[2.2.3 以比特币为例的交易数据结构 56](#_Toc886585389)

[2.3 共识机制的分类与基本模型 59](#_Toc1599090037)

[2.3.1 “共识”在去中心化系统中的含义 60](#_Toc148409654)

[2.3.2 PoW机制详解 62](#_Toc1092540611)

[2.3.3 PoS与变体机制 64](#_Toc1344867227)

[2.3.4 PBFT与拜占庭容错算法 67](#_Toc918099514)

[2.4 FLP不可能定理与拜占庭容错问题 70](#_Toc828528103)

[2.4.1 分布式系统的根本性难题 70](#_Toc787859973)

[2.4.2 拜占庭将军问题与容错模型 73](#_Toc178398809)

[2.4.3 现代BFT算法演化 76](#_Toc461611651)

[本章小结 80](#_Toc1596085393)

[第3章 比特币系统详解 82](#_Toc1188965474)

[3.1 UTXO数据模型与交易链 82](#_Toc607386183)

[3.1.1 账户模型与UTXO模型的对比与取舍 82](#_Toc1349803490)

[3.1.2 UTXO链与交易历史追踪 84](#_Toc130009522)

[3.1.3 一个典型比特币交易的生命周期 88](#_Toc1079167255)

[3.2 区块结构与Nakamoto共识稳定性 92](#_Toc2064655870)

[3.2.1 区块组成与元数据结构 92](#_Toc1630438864)

[3.2.2 Nakamoto最长链规则的设计哲学 94](#_Toc894651528)

[3.2.3 分叉与最终性概率 97](#_Toc1875218449)

[3.3 矿工激励、难度调整与分叉机制 100](#_Toc326468971)

[3.3.1 挖矿原理与工作量证明 100](#_Toc143277512)

[3.3.2 挖矿激励机制与减半周期 102](#_Toc735975897)

[3.3.3 难度调整算法（Difficulty Adjustment） 104](#_Toc41094159)

[3.3.4 分叉的分类与治理含义 108](#_Toc1327279626)

[3.4 比特币脚本语言与Taproot升级 110](#_Toc1676032793)

[3.4.1 Bitcoin Script 的设计哲学 110](#_Toc540154252)

[3.4.2 脚本验证流程与安全性 113](#_Toc959137495)

[3.4.3 Schnorr签名与Taproot升级成为比特币演进的里程碑 115](#_Toc1211624083)

[本章小结 119](#_Toc1326022127)

[第4章 以太坊与智能合约平台 121](#_Toc2016083570)

[4.1 EVM架构与运行模型 121](#_Toc1319578624)

[4.1.1 以太坊的设计目标与范式跃迁 121](#_Toc1094310999)

[4.1.2 EVM（Ethereum Virtual Machine）结构概览 124](#_Toc1035007285)

[4.1.3 智能合约运行生命周期 128](#_Toc749898295)

[4.2 账户模型（EOA与合约账户）与Gas定价 131](#_Toc2106603469)

[4.2.1 账户类型与状态结构 131](#_Toc121615394)

[4.2.2 交易结构与发送流程 134](#_Toc1732978661)

[4.2.3 Gas机制与资源定价模型 137](#_Toc1999134813)

[4.3 状态存储、事件机制与链重组处理 140](#_Toc2077144776)

[4.3.1 状态存储机制 140](#_Toc1078084600)

[4.3.2 日志与事件系统（Event / Log） 143](#_Toc1048342461)

[4.3.3 链重组（Chain Reorganization）与状态一致性 146](#_Toc1535902039)

[4.4 EIP演进过程与技术治理机制 148](#_Toc1152132533)

[4.4.1 EIP与ERC标准体系 148](#_Toc31437132)

[4.4.2 社区治理结构与升级路径 151](#_Toc82900362)

[4.4.3 技术升级的激励博弈 153](#_Toc1736980878)

[本章小结 155](#_Toc544919228)

[第5章 智能合约开发与安全性分析 157](#_Toc1587194188)

[5.1 Solidity语法和开发工具 157](#_Toc2078338329)

[5.1.1 Solidity语言基础与版本管理 157](#_Toc1810777048)

[5.1.2 编译器与语言演进 162](#_Toc1739084099)

[5.1.3 在线与本地开发工具 165](#_Toc1534016223)

[5.1.4 合约部署与交互流程 168](#_Toc1669477726)

[5.2 合约设计模式 172](#_Toc2038292827)

[5.2.1 模块化与可维护性设计理念 172](#_Toc928406445)

[5.2.2 Proxy模式详解 176](#_Toc110942013)

[5.2.3 工厂模式与Clone合约 179](#_Toc586606895)

[5.2.4 其他设计范式 181](#_Toc4660888)

[5.3 常见攻击分析 184](#_Toc1026133324)

[5.3.1 重入攻击（Reentrancy） 184](#_Toc1929091058)

[5.3.2 溢出与下溢 187](#_Toc1672793047)

[5.3.3 闪电贷攻击（Flash Loan） 189](#_Toc1924318052)

[5.3.4 逻辑漏洞与配置错误 190](#_Toc909776144)

[5.3.5 攻击面与攻击路径分类 192](#_Toc524085568)

[5.4 安全审计流程与工具 195](#_Toc1475705029)

[5.4.1 安全开发生命周期（SDL）与风险评估流程 196](#_Toc885783200)

[5.4.2 静态分析工具 198](#_Toc1001601396)

[5.4.3 审计报告撰写要点 201](#_Toc1937837386)

[5.4.4 社区最佳实践与合规指导 204](#_Toc495956100)

[本章小结 206](#_Toc1150138693)

[第6章 钱包架构与账户抽象 208](#_Toc880706604)

[6.1 钱包是用户与链的接口 208](#_Toc1578598304)

[6.1.1 钱包的基础定义与功能层 208](#_Toc1488720290)

[6.1.2 钱包在 Web 3 生态中的角色演变 209](#_Toc589942833)

[6.1.3 钱包与账户的技术映射 210](#_Toc237196032)

[6.1.4 钱包进化路径与多链兼容趋势 210](#_Toc824060992)

[6.2 助记词与分层确定性钱包 212](#_Toc871053041)

[6.3 钱包分类与架构差异 217](#_Toc392438488)

[6.3.1 热钱包与冷钱包 217](#_Toc791387879)

[6.3.2 硬件钱包原理与实现 220](#_Toc1489856482)

[6.3.3 多重签名钱包 222](#_Toc358568954)

[6.4 合约钱包原理与代表性项目 224](#_Toc629296396)

[6.4.1 合约钱包概念解析 225](#_Toc227566097)

[6.4.2 代表性合约钱包项目 227](#_Toc35016972)

[6.5 账户抽象的概念与演化路径 229](#_Toc119729126)

[6.5.1 为什么需要账户抽象？ 229](#_Toc95243443)

[6.5.2 账户抽象的定义与技术目标 231](#_Toc881229486)

[6.6 ERC-4337的账户抽象标准化尝试 233](#_Toc1776741490)

[6.7 账户抽象的其他提案与对比 237](#_Toc934110895)

[6.7.1 EIP-3074以OPCODE 方式实现账户抽象 237](#_Toc1496352695)

[6.7.2 EIP-5003、ERC-6900 等演化方向 239](#_Toc18754848)

[6.8 钱包设计中的安全性与用户体验平衡 242](#_Toc1680117874)

[6.9 钱包未来演进方向与研究前沿 245](#_Toc478633915)

[本章小结 247](#_Toc2073951390)

[第7章 DID与自主权的数字身份革命 250](#_Toc1093937273)

[7.1 DID 的基本概念与核心价值​​ 250](#_Toc1196245344)

[7.1.1 从中心化身份到去中心化身份的演进​​ 250](#_Toc553593394)

[7.1.2 DID 的技术特征​​ 253](#_Toc1345014154)

[7.1.3 DID 在 Web 3 中的战略地位​​ 255](#_Toc1240017956)

[7.2 DID 的技术标准与规范 257](#_Toc1800476004)

[7.2.1 W3C DID 规范解析​​ 257](#_Toc408129351)

[7.2.2 DID Methods的设计与实现​​ 261](#_Toc367233739)

[7.2.3 可验证凭证（VC）与可验证呈现（VP）​​ 264](#_Toc229449895)

[7.2.4 去中心化标识符与区块链的绑定机制​​ 267](#_Toc1631238900)

[7.3 DID 的身份数据模型与存储​​ 269](#_Toc1455954698)

[7.3.1 身份数据的模块化设计​​ 269](#_Toc1801935368)

[7.3.2 分布式存储方案与链上锚定​​ 271](#_Toc1313339982)

[7.3.3 隐私保护设计​​ 273](#_Toc1468153608)

[7.4 DID 的验证与交互流程​​ 275](#_Toc670585626)

[7.4.1 身份验证的核心机制​​ 275](#_Toc538436726)

[7.4.2 DID 解析与解析器的设计​​ 278](#_Toc9965424)

[7.4.3 用户与 DApp 的交互流程​​ 281](#_Toc2132640349)

[7.5 DID 的应用场景与实践案例​​ 284](#_Toc1784277213)

[7.5.1 DeFi 中的 KYC 与合规​​ 284](#_Toc885472183)

[7.5.2 社交与内容平台的用户数据主权​​ 286](#_Toc69305971)

[7.5.3 跨平台身份互操作​​ 288](#_Toc889317923)

[7.5.4 政府与企业级应用​​ 289](#_Toc280148741)

[7.6 DID 的挑战与未来方向​​ 291](#_Toc1175735763)

[7.6.1 技术挑战​​ 291](#_Toc1593932694)

[7.6.2 监管与合规​​ 293](#_Toc1515775380)

[7.6.3 生态发展​​ 295](#_Toc38307299)

[7.6.4 与其他技术的融合​​ 297](#_Toc1733163840)

[本章小结 299](#_Toc816470972)

[第8章 Web 3 协议栈与用户交互层 301](#_Toc7122074)

[8.1 DApp 前端、后端与链上部分的三层架构 301](#_Toc1589097133)

[8.1.1 DApp 定义与演化路径 301](#_Toc1848880239)

[8.1.2 DApp 的技术架构概览 304](#_Toc41804783)

[8.1.3 以 Uniswap 和 Lens Protocol 为例的示例解析 308](#_Toc385835312)

[8.1.4 DApp 的数据流与调用路径 313](#_Toc1480958491)

[8.2 区块链上的身份与命名系统 315](#_Toc1133889507)

[8.2.1 以太坊命名服务系统ENS 315](#_Toc511060671)

[8.2.2 Soulbound Token 与声誉系统 318](#_Toc1609593144)

[8.3 去中心化存储与数据索引 321](#_Toc580469949)

[8.3.1 为什么需要链下存储 321](#_Toc2087708169)

[8.3.2 IPFS 与 Filecoin的内容寻址与激励机制 324](#_Toc375888050)

[8.3.3 数据索引协议The Graph 327](#_Toc1801050523)

[8.4 钱包交互标准与签名流程 332](#_Toc1474135596)

[8.4.1 钱包与 DApp 的通信桥梁 332](#_Toc278126533)

[8.4.2 WalletConnect、MetaMask、RainbowKit 等标准 335](#_Toc1548224259)

[8.4.3 签名类型与 EIP 分化 337](#_Toc2093253961)

[8.5 用户体验与交互安全性分析 340](#_Toc1242217373)

[8.5.1 签名钓鱼成为Web 3 UX 的信任陷阱 340](#_Toc111371877)

[8.5.2 权限管理与用户教育 342](#_Toc1368880202)

[8.5.3 钱包确认界面与 UX 改进路径 345](#_Toc777244703)

[8.5.4 安全性增强方案探索 347](#_Toc8698620)

[本章小结 350](#_Toc168818344)

[第9章 DeFi 协议与金融机制设计 351](#_Toc504009921)

[9.1 借贷协议设计原理 351](#_Toc1219238479)

[9.1.1 去中心化借贷的基本逻辑 351](#_Toc452156879)

[9.1.2 抵押机制与清算路径 355](#_Toc1603522267)

[9.1.3 借贷利率模型 356](#_Toc1626455266)

[9.1.4 示例协议剖析 359](#_Toc514312999)

[9.2 AMM 模型与 DEX 机制 362](#_Toc436895018)

[9.2.1 去中心化交易的基本构成 362](#_Toc647978433)

[9.2.2 AMM 模型比较与迭代 367](#_Toc683949494)

[9.2.3 LP 的角色与激励设计 372](#_Toc1806666914)

[9.2.4 路由与聚合器协议 374](#_Toc1379538665)

[9.3 流动性激励、预言机机制与治理代币设计 376](#_Toc1672889643)

[9.3.1 流动性挖矿机制 376](#_Toc1400323377)

[9.3.2 预言机设计与数据安全 378](#_Toc961709766)

[9.3.3 治理代币的功能、设计演进与系统性影响 381](#_Toc1494109840)

[9.4 经济安全性建模与攻击分析 382](#_Toc977796509)

[9.4.1 去中心化协议的攻击面 382](#_Toc1281059919)

[9.4.2 闪电贷与 DeFi MEV 385](#_Toc103013811)

[9.4.3 模型化分析方法 390](#_Toc481301995)

[9.4.4 安全防御与设计范式 393](#_Toc1819215363)

[本章小结 395](#_Toc1827923602)

[第10章 链上治理与DAO制度设计 397](#_Toc10924832)

[10.1 DAO 的基本概念与历史演进 397](#_Toc1077541429)

[10.1.1 什么是 DAO？ 397](#_Toc509202052)

[10.1.2 历史回顾与典型案例 399](#_Toc436554669)

[10.1.3 DAO 与传统组织的对比 402](#_Toc1370183731)

[10.2 DAO的组织结构与治理Token模型 404](#_Toc1210820136)

[10.2.1 DAO的模块化结构 404](#_Toc698986780)

[10.2.2 治理 Token 的功能与设计 407](#_Toc1135262370)

[10.2.3 治理 Token 的风险与挑战 410](#_Toc2109932642)

[10.3 投票机制设计与激励博弈 412](#_Toc240451183)

[10.3.1 投票机制类型 412](#_Toc1846292674)

[10.3.2 投票过程管理 414](#_Toc1649756415)

[10.3.3 投票激励机制 416](#_Toc1294700488)

[10.3.4 治理攻击分析 418](#_Toc1726790412)

[10.4 治理最小化与协议自治趋势 420](#_Toc1072448926)

[10.4.1 治理最小化的理念来源 420](#_Toc818850011)

[10.4.2 治理参数的自动化调节机制 422](#_Toc1336924901)

[10.4.3 治理结构的渐进分权 424](#_Toc575412546)

[10.5 DAO的法律结构与运营实践 426](#_Toc839798181)

[10.5.1 DAO 的法律地位问题 426](#_Toc1225499983)

[10.5.2 法律包层与链下执行 428](#_Toc462555904)

[10.5.3 DAO 的财务运营与会计问题 431](#_Toc286276388)

[10.5.4 实践案例剖析 433](#_Toc1083883836)

[本章小结 437](#_Toc1879337798)

[第11章 RWA与链下世界的连接 438](#_Toc840890910)

[11.1 链上金融为何需要RWA？ 438](#_Toc263643463)

[11.1.1 去中心化金融的流动性瓶颈与纯加密资产局限 438](#_Toc796918880)

[11.1.2 RWA 现金流、安全性与多样性的引入逻辑 440](#_Toc2107593468)

[11.1.3 从 NFT 到 RWA的资产 Token 化谱系 442](#_Toc1728143058)

[11.2 RWA资产的链上映射机制 445](#_Toc184050131)

[11.2.1 Token 化资产的基本架构 445](#_Toc954100037)

[11.2.2 RWA 的数字映射方式 452](#_Toc298929710)

[11.2.3 链下事件与链上状态同步机制 455](#_Toc1147385637)

[11.3 法律包层、合规问题与审计机制 458](#_Toc1854734646)

[11.3.1 RWA规模化面临的合规挑战 458](#_Toc1800059117)

[11.3.2 法律包层机制解析 460](#_Toc1991444130)

[11.3.3 审计、托管与真实世界接口 462](#_Toc1668854415)

[11.4 链上RWA先锋项目案例分析 465](#_Toc152239438)

[11.4.1 MakerDAO的RWA子金库机制 465](#_Toc1035210889)

[11.4.2 Centrifuge RWA资产池的模块化架构 467](#_Toc2024387076)

[11.4.3 Maple Finance 与链上信贷 469](#_Toc1290166911)

[11.4.4 新兴案例简览 471](#_Toc692889418)

[11.5 RWA的可编程性与“链上执行”的挑战 474](#_Toc1736114292)

[11.5.1 可编程法律的愿景 475](#_Toc1012593855)

[11.5.2 可编程支付与收益分配机制 477](#_Toc2004502157)

[11.5.3 链下执行的“最后一公里问题” 479](#_Toc2091782210)

[11.6 RWA的制度意义与未来潜力 481](#_Toc128818433)

[11.6.1 从链上金融走向链上制度 481](#_Toc387887255)

[11.6.2 全球南方的新机会？ 483](#_Toc1608226140)

[11.6.3 与国家金融体系的协同与竞争 485](#_Toc1227553838)

[本章小结 487](#_Toc621958537)

[第12章 零知识证明与隐私增强 489](#_Toc1454221410)

[12.1 零知识证明基础与主流构造 489](#_Toc587851363)

[12.1.1 零知识证明的基本原理 489](#_Toc1593081741)

[12.1.2 zkSNARK 的数学构造与工程实现 493](#_Toc98710191)

[12.1.3 zkSTARK 与新一代透明证明系统 496](#_Toc1164804653)

[12.1.4 Bulletproofs、Plonk、Halo 2等新型证明系统 498](#_Toc410876919)

[12.2 匿名交易与隐私币机制解析 500](#_Toc1448452528)

[12.2.1 Tornado Cash链上匿名交易的典型路径 500](#_Toc267015704)

[12.2.2 Zcash的隐私币架构与隐私设计 502](#_Toc1639598545)

[12.2.3 Aztec Protocol 与 Noir隐私合约的新路径 504](#_Toc222587511)

[12.3 匿名性的链上设计挑战与监管张力 510](#_Toc111784303)

[12.3.1 匿名性技术的设计维度与系统难题 511](#_Toc1858073043)

[12.3.2 匿名交易与全球监管冲突 514](#_Toc2073922674)

[12.3.3 可选择合规路径与未来设计方向 516](#_Toc611307461)

[12.4 零知识证明在链下计算与 Rollup 中的应用 518](#_Toc682729779)

[12.4.1 ZK-Rollup链上扩容的结构与工作原理 518](#_Toc634269732)

[12.4.2 ZK-EVM的兼容性与工程挑战 521](#_Toc62562016)

[12.4.3 ZK 在跨链与预言机中的应用拓展 523](#_Toc1360299529)

[12.4.4 ZK Coprocessor 与未来链下计算路径 525](#_Toc443277941)

[本章小结 527](#_Toc551582944)

[第13章 跨链互操作与未来范式 529](#_Toc1915119356)

[13.1 跨链互操作的技术背景与需求动因 529](#_Toc926115056)

[13.1.1 链间孤岛问题与资产碎片化现状 529](#_Toc254272736)

[13.1.2 跨链的核心问题与设计挑战 531](#_Toc69416422)

[13.1.3 跨链设计模型分类 533](#_Toc598184233)

[13.2 跨链桥与通用消息传递机制 537](#_Toc1311452424)

[13.2.1 跨链桥（Bridge）的工作机制与主流分类 537](#_Toc1956221007)

[13.2.2 主流桥接协议剖析 540](#_Toc231829079)

[13.2.3 桥接机制的安全挑战与攻击案例 544](#_Toc815995095)

[（3）社区与标准化动向 545](#_Toc598991923)

[13.3 Cosmos IBC、Polkadot XCM 与模块化互操作设计 546](#_Toc2001396372)

[13.3.1 Cosmos 在跨链互操作中的架构优势与 IBC 协议分析 546](#_Toc1432461243)

[13.3.2 Polkadot 跨链互操作架构与标准化探索 548](#_Toc2084428231)

[13.3.3 Cosmos 与 Polkadot 跨链互操作架构的比较 551](#_Toc1084544906)

[13.4 Rollup设计与跨Rollup互操作问题 553](#_Toc105039406)

[13.4.1 Rollup 的核心原理与技术分类 553](#_Toc165738808)

[13.4.2 Rollup与L1的交互方式 556](#_Toc285855897)

[13.4.3 跨 Rollup 通信的探索与难点 558](#_Toc459142540)

[13.5 模块化区块链范式与未来互操作路径 560](#_Toc899926109)

[13.5.1 模块化区块链概念解析 561](#_Toc330788142)

[13.5.2 模块化架构下的互操作创新 563](#_Toc1868624158)

[13.5.3 Web 3 互操作的未来走向与标准化趋势 566](#_Toc1165369778)

[本章小结 568](#_Toc1318998206)

[后记：在浪潮与暗流之间 570](#_Toc2076643908)