# 内容介绍

《从比特币到 Web 3——去中心化系统的技术原理与架构演进》是一部系统性、跨学科、面向研究生及研究者的区块链与 Web 3 教材。全书 50 余万字，覆盖从密码学基础到去中心化应用、从分布式共识到跨链互操作、从经济机制到制度设计的完整知识体系。

第 1–2 章从信任机制的演化切入，深入解析区块链的技术基石，包括非对称加密、哈希函数、Merkle 树、公私钥签名、PoW/PoS/PBFT 等主流共识机制，并探讨分布式系统的根本性难题。

第 3–4 章完整剖析比特币与以太坊两大核心系统的架构、运行机制与技术治理，涵盖 UTXO 模型、Nakamoto 共识、EVM、Gas 定价、链重组等关键技术。

第 5–8 章以工程实践为导向，讲解智能合约开发、安全审计、钱包架构、账户抽象、DApp 三层架构、去中心化身份与存储、用户交互安全等应用层技术。

第 9–11 章深入分析 DeFi 协议设计、DAO 治理机制与 RWA（现实世界资产上链）连接机制，结合典型案例探讨金融制度创新与链上经济安全。

第 12–13 章聚焦零知识证明、隐私增强技术与跨链互操作方案，涵盖 zkSNARK/zkSTARK、匿名交易、Cosmos IBC、Polkadot XCM、模块化区块链等前沿方向。

该书特色与亮点，一是跨学科整合，融合了密码学、分布式系统、博弈论、金融工程、法律制度等多领域知识，帮助读者建立全景式理解；二是技术深度与可读性兼顾，既有代码与协议层面的细节解析，也有制度背景与案例分析，适合学术研究与工程实践双重需求；三是前沿与可持续更新，覆盖账户抽象、可编程法律、ZK Coprocessor、跨 Rollup 通信等最新发展方向，并以开源形式在 GitHub 持续维护更新。

无论你是从事区块链研发、研究去中心化制度，还是希望系统掌握 Web 3 技术与架构的全貌，这本书都将是你构建知识体系与前瞻视野的重要参考。