# 自序

在区块链与 Web 3 的世界里，十年可以是一段沧海桑田般的旅程。从比特币的白皮书发布，到以太坊开启智能合约平台，再到 NFT、DeFi、DID、RWA 与零知识证明的持续迭代，这个领域的技术与理念在不断重塑着金融、互联网乃至制度形态。我有幸在近十年的研究与观察中，一次又一次见证了这些浪潮的兴起、高潮与回落，也见证了人们在“去中心化”与“信任重构”的实验中一次又一次对边界的试探。

在此之前，我已经出版过多部相关著作，包括思想札记式的《回归常识——高博士区块链观察》，面向技术解析的《区块链技术本质与应用》《区块链中的密码技术》《Web 3中的零知识证明》，以及面向大众普及的《Web 3时代——NFT、元宇宙、区块链和去中心化网络的未来》《与每个老百姓密切相关的稳定币》《RWA：现实世界资产的链上革命——资产逻辑、金融制度与信任结构的重构》等图书。这些图书分属不同类型，有的是观察者的随笔，有的是工程师的技术手册，有的是公共知识的通俗读本，但始终缺少一本能够系统串联技术原理、架构演进、制度逻辑与应用案例的“全景式”著作，既能在深度上支撑高年级本科生和研究生教学，又能在广度上覆盖区块链核心生态的多个维度。

这本《从比特币到 Web 3——去中心化系统的技术原理与架构演进》正是为填补这一空白而写。我希望它具备三个特征。一是跨学科整合。区块链并非单一技术的呈现，而是密码学、分布式系统、博弈机制、金融工程、制度设计等多个领域知识交汇的产物。本书从技术内核到经济机制、再到制度与应用，力求呈现一个立体、连贯的知识地图。二是体系化与前瞻性。本书不仅详解 PoW、PoS、EVM、跨链协议、账户抽象等成熟技术，也探讨去中心化身份、零知识证明、模块化区块链、可编程法律等前沿方向，兼顾“已经落地的现实”与“尚在探索的未来”。三是可持续更新。这一领域的变化之快，意味着任何一本纸质书都可能很快过时。因此，我决定将本书全文开源于 GitHub，让它不仅是一个静态成果，更是一个可以被更新、被批注、被改进的知识仓库。

全书 50 余万字，历时半年多完成。对我而言，这不仅是一次学术写作，更是一次整理与反思近十年学习和研究成果积累的过程。写作的难处，不仅在于技术的复杂性，更在于如何在复杂性中寻找秩序，在多个学科的交汇中保持逻辑自洽，让读者既能看到细节的精确，又不迷失在技术术语的丛林。

我深知，这本书不可能覆盖区块链与 Web 3 的全部面向。它是一份在特定时间节点上的全景扫描，也是一次开放邀请——希望更多研究者、开发者、学生、爱好者能在这个开源项目中补充案例、修正细节、提出质疑，共同推动这一领域的公共知识建设。

技术终将过时，理念与方法才会长存。

我愿把这本书献给所有关注、参与、推动去中心化系统演化的人们。

高承实

2025年 孟秋