HZ BOOKS 华章IT

宏观上分析了Hyperledger Fabric的整体架构、设计逻辑和运行机制，微观上剖析了各核心模块的设计理念与实现原理

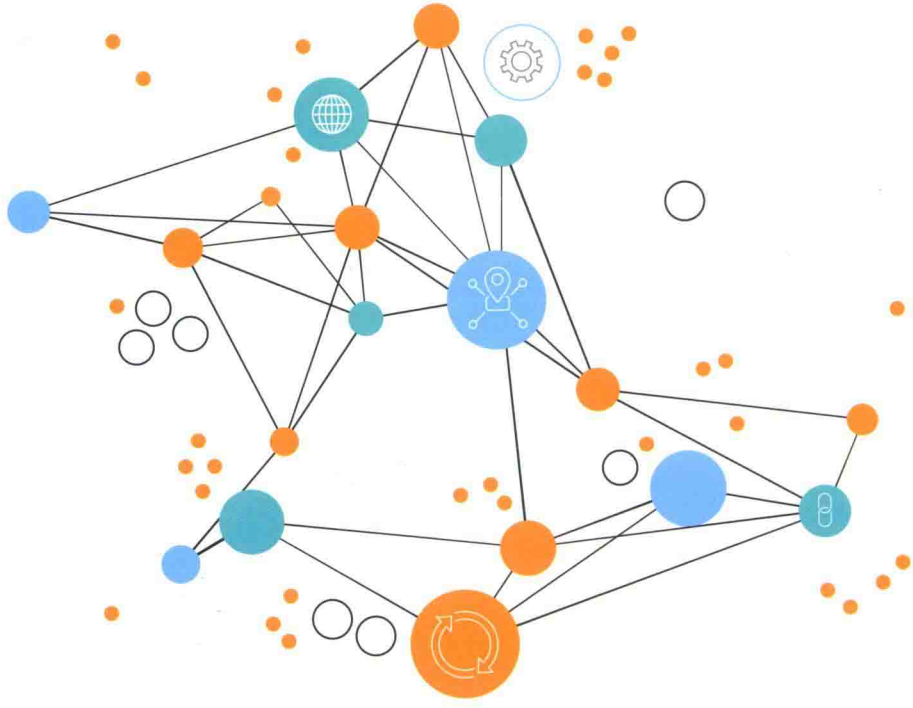
从源代码角度展示Hyperledger Fabric内核和全景图，同时为底层系统研发和上层应用开发提供指导

区块链技术丛书

Hyperledger Fabric 技术内幕

架构设计与实现原理

李鑫 ◎ 著



HYPERLEDGER FABRIC INTERNALS

ARCHITECTURE DESIGN AND IMPLEMENTATION PRINCIPLES

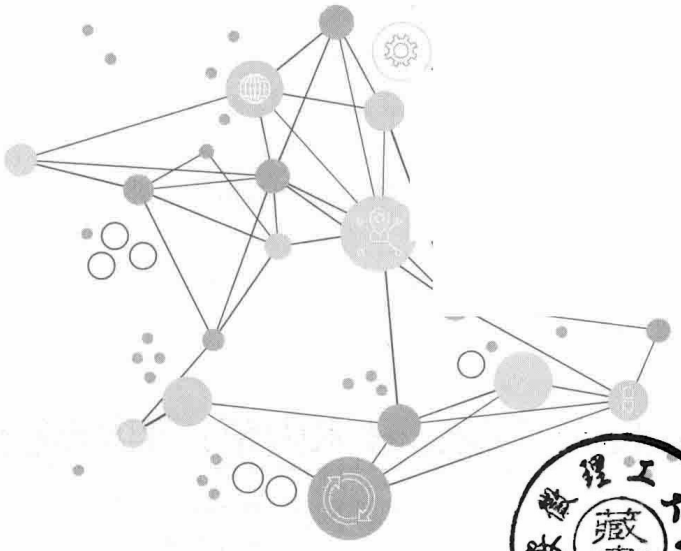
机械工业出版社
China Machine Press

区块链
技术丛书

Hyperledger Fabric
技术内幕

架构设计与实现原理

李鑫◎著



HYPERLEDGER FABRIC INTERNALS

ARCHITECTURE DESIGN AND IMPLEMENTATION PRINCIPLES

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Hyperledger Fabric 技术内幕：架构设计与实现原理 / 李鑫著 . —北京：机械工业出版社，2019.1
（区块链技术丛书）

ISBN 978-7-111-61856-0

I. H… II. 李… III. 电子商务 - 支付方式 - 研究 IV. F713.361.3

中国版本图书馆 CIP 数据核字（2019）第 018577 号

Hyperledger Fabric 技术内幕：架构设计与实现原理

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码：100037）
责任编辑：张锡鹏 责任校对：李秋荣
印 刷：北京市荣盛彩色印刷有限公司 版 次：2019 年 3 月第 1 版第 1 次印刷
开 本：186mm×240mm 1/16 印 张：40.5
书 号：ISBN 978-7-111-61856-0 定 价：129.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzit@hzbook.com

Preface 前 言

2016 年 12 月，“区块链”（BlockChain）被列入国家十三五规划，并作为未来重点突破与发展的六大关键技术之一。2018 年 5 月，两院院士大会将区块链的发展趋势表述为“以人工智能、量子信息、移动通信、物联网、区块链为代表的新一代信息技术加速突破应用”。区块链领域正在以前所未有的速度聚集着社会资源，加速技术应用与关键技术的突破，并受到国家、企业、资本等各方的广泛关注。当前，区块链作为风口概念受到国内外媒体的火热炒作，同时受到大量 VC 风投的极力热捧。

根据产业创新创投数据平台 Innov100 的数据统计，2017 年全球 ICO（Initial Coin Offering，首次代币发行）融资金额高达 350 亿元。2018 年 1 月至 5 月，ICO 融资规模为 118 亿美元。博链研究发布的《全球区块链 + 创投报告》指出，截至 2017 年 4 月底，全球 455 家区块链公司累计获得融资金额达 19.47 亿美元。在获投公司数量上，中国共有 61 家位列全球第二。2018 年第 1 季度，“俄罗斯微信”Telegram 进行了两轮 ICO 融资分别获得 8.5 亿美元共 17 亿美元。中国平安旗下金融管理门户金融壹账通获得 SBI 投资（思佰益）和 IDG 资本的 6.5 亿美元融资，成为 2018 年第 1 季度中国区块链行业融资额最高的项目。2018 年 6 月，Block.one 推出的加密数字货币 EOS 结束了为期 350 天的众筹活动，总融资额近 42 亿美元。

截至 2018 年 3 月底，我国以区块链业务为主营业务的区块链公司数量已经达到了 456 家，区块链产业初步形成规模。同时，区块链明星创业公司如井通科技、智链、量子链、小蚁、趣链、布比等如雨后春笋般纷纷出现并迅速成长，国内 BAT、小米等互联网巨头与众安保险等新型互联网公司相继投入资源，研发核心技术与探索应用落地，传统行业巨头如中国平安、万向集团等也耗巨资，成立新型网络科技公司或实验室，研究区块链技术与应用。这些企业都试图在未来的科技竞争中弯道超车，抢占先发优势，积累资源与技术壁垒。鉴于国内行业发展的碎片化，以及应用存在一定的盲目性，国家工信部在区块链产业整合上积极引导，由中国电子技术标准化研究院牵头，联合国内典型区块链企业成立中国区块链技术和产业发展论坛，共同制定我国区块链技术的相关标准与推动产业发展。该组织于 2016 年 10 月 18 日发布了《2016 年中国区块链技术和应用发展白皮书》；2017 年 5 月

与12月分别提出了我国区块链技术和产业发展论坛标准《区块链参考架构》与《区块链数据格式规范》，其中，《区块链参考架构》已处于国家标准立项阶段；2018年5月发布了《2018年中国区块链产业白皮书》，2018年6月拟筹建全国区块链和分布式记账技术标准化技术委员会，推进区块链标准体系框架工作，提出了基础、业务和应用、过程和方法、可信和互操作、信息安全等标准，并初步明确了21个标准化重点方向及相关标准化方案。同时，2016年12月以来，中国信息通信研究院联合数据中心联盟等单位相继发布了可信区块链系列标准《第1部分　区块链技术参考框架》《第2部分　总体要求和评价指标》《第3部分　评测方法》等，2018年4月9日，牵头与158家企业联手启动了“可信区块链推进计划”，截至2018年9月初，推进计划成员已发展至225家，陆续成立了标准与评测、知识产权、云服务等10个工作组，积极推动国内外企业的可信区块链标准以及产品评测工作。另外，中国电子产品可靠性与环境试验研究所、中国银联电子支付研究院与同济苏州区块链研究院、贵阳区块链测试中心等都在研究与提供相应的区块链平台测评服务。国内的这些工作都在积极推动和促进国内区块链产业的发展，并积极与国际标准（ISO/TC 307等）、ITU-T FGDLT组与SG16研究组等进行接轨及交流，这有利于统一对区块链新兴技术的认知和共同解决区块链关键技术问题，对我国区块链产业的发展具有重大意义。

与此同时，国际上影响力较大的主流区块链开源平台逐渐融合发展，互相借鉴，目前已经涌现出数个典型的生态体系及平台。

- 以比特币为代表的“虚拟货币”平台开源社区生态体系。比特币就是以区块链作为底层技术进行设计与研发的，中本聪（Satoshi Nakamoto）在2008年发表的论文《Bitcoin: A Peer-to-Peer Electronic Cash System》中就曾指出，比特币是通过随机哈希值为全部交易加上时间戳，并将它们融入不断延伸的、基于随机哈希值的工作量证明链条中作为交易记录（即区块），除非重新完成全部的工作量证明，否则形成的交易记录将不可更改。这种独特的记账方式使得比特币的发行可以不依赖于任何政府与货币机构的公信力，而是根据特定共识算法并通过大规模计算来生成的，由全系统所有节点共同背书，其记账权由全网51%的算力决定，第一次在全球范围内实现了一个去中心化的真实的点对点电子现金系统。这完全颠覆了以往人们对“货币”的认知，点燃了以比特币为代表的“虚拟货币”风口。
- 以以太坊（Ethereum）为代表的支持可编程智能合约的公有链或公链平台开源社区生态体系。其核心理念是将区块链作为可编程的分布式信用基础设施，支持自动化运行的智能合约应用，并将平台交易内容扩展到金融、股权、债务凭证等领域。Vitalik Buterin等创始人于2013年12月开始发起以太坊项目，并迅速激发了人们在可信平台上交易金融资产的热情与创造力，现在应用方面有超过上千个DApp上链（https://www.stateofthedapps.com/），已经成为具有国际影响力的开源公链平台。
- 以超级账本Hyperledger Fabric为代表的联盟链平台开源社区生态体系。其目标是完全面向企业级应用场景的许可区块链（Permissioned Chain），用以解决多个弱信任

企业主体之间的信任问题，以降低企业间复杂繁琐业务流程带来的信任成本，实现在可控主体范围内共享敏感数据，从而有效提升企业主体之间大规模协作活动的效率。Hyperledger Fabric 开源社区提供带有身份权限认证的商用区块链平台，采用模块化插件的灵活设计架构，避免了比特币类公链平台与以太坊类公链平台交易效率低下、缺乏完善的身份认证模块等问题，能够广泛应用于金融资产存管、供应链、共享经济等领域。Hyperledger Fabric 自 2015 年底开源以来发展迅速，已经成为主流的联盟链开源平台。另外，值得注意的是，企业以太坊联盟（Enterprise Ethereum Alliance，EEA）、蚂蚁金服、腾讯、百度、BCOS（由微众银行、万向、矩阵元共同发布的开源联盟链平台）、众安、趣链、CITA（秘猿科技）等都是其潜在的竞争对手或产品。企业级 BaaS（Blockchain as a Service）平台作为基础设施服务亦是未来国际企业市场的竞争焦点，国际巨头 IBM、微软等已经在此领域深耕发力多年，以实现高效动态的部署跨域区块链网络的能力，从而提供高质量的商用企业级服务。

此外，目前还涌现出 IPFS（InterPlanetary File System，星际文件系统）、石墨烯（Graphene）、哈希图（Hashgraph）、Blockstack、侧链、DAG、分片技术（Sharding）、抗量子攻击算法、高性能跨链技术、新型共识机制（如拜占庭协商 BA-VRF、DDPOS、HyperPOW 等）等众多的新型区块链平台、新型底层支撑技术以及相关方向，以着力解决当前区块链系统面向领域应用中遇到的关键技术问题（如指数量级提升单链或多链交易处理性能），积极探索新型技术落地与大规模应用场景，这些都是未来具有前景与值得关注的潜在技术。

本书重点介绍了 Hyperledger Fabric 系统架构的设计与实现，根据 Hyperledger 的官网介绍，超级账本旨在通过创建企业级的开源分布式账本框架，协助组织扩展、建立行业专属的应用程序、平台和硬件系统来支持交易业务，是全球跨行业领导者的合作项目，覆盖金融、银行、物联网、供应链、制造行业和技术领域。Hyperledger Fabric 作为联盟链的典型架构，逐渐得到了国际主流公司与研究机构的青睐与大力支持。截至 2018 年 2 月底，已经有 260 个组织机构加入了 Hyperledger 社区阵营，包括 IBM、Intel、Oracle、思科、摩根大通、富国银行、百度、阿里巴巴、腾讯、联想、小米、迅雷、华为等，分为高级会员、标准会员与联盟会员；另外还有一种学术性机构联盟会员，如剑桥大学贾吉商学院、北京大学、浙江大学等。Hyperledger 项目设有理事会、技术指导委员会、市场委员会和用户顾问团等，代码许可协议采用 Apache License Version 2.0，以满足大多数商业用途需求。截至 2018 年 7 月底，超级账本亚太副总裁 Julian Gordon 声称超级账本中 20% 的会员（50 多个中国会员，百度属于高级会员）与 10% 的贡献都来自中国。目前，Hyperledger 开源社区包括 11 个商业区块链和分布式账本项目，其中 3 个项目是中国企业与个人首先发起或提供主要工作的，包括 Hyperledger Caliper（区块链性能测试平台，华为等）、Hyperledger Cello（区块链平台部署和运行管理项目，Oracle 区块链首席架构师杨保华博士等）以及 Hyperledger Explorer（区块链数据可视化工具项目，上海旺链科技等）。另外，中国企业与个人也为 Hyperledger Fabric 等项目做出了重大贡献。

Hyperledger Fabric 得益于模块化插件架构等良好特性，近年来的发展异常迅速，已经开始在很多国内外机构和大公司的实际 PoC（Proof of Concept，概念验证）项目以及实际应用系统中推广使用，如民生银行贸易金融领域产品即国内信用证信息传输系统目前支撑数十亿级别的交易业务量，以及智链 ChainNova 航运物流行业项目等。Hyperledger Fabric 所在的 GitHub 开源社区也非常活跃，Meetup 以及国内外会议上的相关研讨交流同样异常频繁。自 2017 年 3 月正式发布 1.0 测试版本以来，GitHub 代码更新速度飞快，经过 2016 年 0.6 技术预览版本的升级之后，1.0 版架构重新分离出 Orderer 节点与 Committer 节点，以提高系统的可扩展性与并发性，并且引入模块插件化的共识算法，整个系统架构日臻成熟实用。Hyperledger Fabric 于 2017 年 7 月在社区正式发布了 1.0 正式版代码，在这个过程中约有 27 个组织、159 名开发者、3500 多个代码修改以及超过一年的协作和测试。发布 1.0 版是超级账本社区真正的里程碑事件，用户和技术供应商可以基于 Hyperledger Fabric 来推进产品的部署和运营。这标志着 Hyperledger Fabric 已经能够作为一个较为独立完整的开源软件被集成到其他系统中，提供给全世界的开发者进行研究。然而，Hyperledger Fabric 开源社区并没有在 1.0 版本中发布 sbft 等支持拜占庭容错的重要共识机制模块，而是谨慎地推迟了该模块加入发布的时间，因此，Hyperledger Fabric 还有很长的路要走。但是作为一个开源区块链系统，Hyperledger Fabric 已经可以作为一个有影响力的典型联盟链范例来进行深入研究，这对于普及推广区块链技术有着积极意义。

作为 Blockstream、Digital Asset Holdings 与 IBM 贡献给开源社区的许可联盟链平台，Hyperledger Fabric 是一个模块插件化的链式区块数据共享账本平台，支持自动化智能合约。更准确地说，它是利用密码学特征将构造成区块的交易数据集合基于区块哈希值链接起来，按时间戳顺序形成以区块对象为基本单元的“链”，并在参与节点之间共享该“链”，同时链上内容根据共识机制由参识节点集体维护，而不再由单一节点决定记账权，关于其来源在本书中会有更详细的探讨。总体来说，Hyperledger Fabric 具有如下鲜明的技术特点：

- 支持可插拔的架构；
- 基于 PKI 体系与 X.509 标准身份证书的安全管理体系；
- 支持多通道、隐私数据集合等多粒度的数据隐私保护特性；
- Peer、Orderer 等节点可扩展性良好；
- 支持多种链码（智能合约）开发语言（Node.js、Go、Java 等）；
- 基于 Docker 容器技术提供链码运行时环境等。

这些特点使得 Hyperledger Fabric 能够具备提供高效可靠的企业级区块链平台服务能力的潜质，并真正从研究走向实用，企业界与开源社区对 Hyperledger Fabric 异常热情，纷纷表示热烈拥抱与接纳。除了 Fabric 项目外，Hyperledger 还包括 Burrow（支持以太坊虚拟机）、Indy（提供去中心化的身份管理机制）、Iroha（关注移动特性的账本平台项目）、Sawtooth（区块链平台）、Caliper（区块链性能测试平台）、Cello（提供区块链平台部署和运行管理）、Composer（提供面向链码开发的高级语言支持）、Explorer（区块链数据可视化工具）、Quilt（关

注账本互操作性）、uRSA（共享加密库项目）等，这些项目构成了相对完善的区块链生态系统。

笔者正是在了解 Hyperledger Fabric 源码中逐渐熟悉其系统架构与实现机制的，并选择 1.1.0 正式版作为剖析对象，能够体现当前 Fabric 架构设计发展的主流新特性（隐私数据集合等）演变，并兼顾 Fabric 1.2（1.2.0 与 1.2.1 版本）与 Fabric 1.3（1.3.0 版本）中架构与功能升级的源码，以帮助读者能够深入了解整体架构的演变，让读者在应用 Hyperledger Fabric 时有所参考，从而对推进项目落地能够有所帮助。

本书面向的读者

- 区块链应用开发人员
- 区块链底层开发人员
- 区块链技术爱好者
- 分布式计算方向研究人员

如何阅读本书

限于篇幅，本书没有深入介绍比特币、以太坊等主流平台体系架构以及 Docker、gRPC、protocol buffer、yaml 配置文件、现代密码学等常用系统知识。本书不是一本初级入门资料，所以需要读者具备相关的基础知识。同时，Hyperledger Fabric 知识体系非常丰富，本书也不试图成为一部能够兼顾所有方面的百科全书式的权威指南，例如本书就没有重点分析 Fabric CA 与 Fabric SDK 等相关模块。

本书介绍了 Hyperledger Fabric 的架构设计与实现原理，基于源码剖析了 Hyperledger Fabric 核心模块，以 Hyperledger Fabric 系统运行流程为主线展开分析，是一部面向 Hyperledger Fabric 系统架构的技术专著。因此，本书更适合于 Hyperledger Fabric 底层架构开发者与应用开发者，以及对 Hyperledger Fabric 感兴趣的技术爱好者。

希望读者学习相关知识（现代密码学、X.509 标准等），搭建实验环境以配合源码阅读学习（推荐 JetBrains GoLand 或 IDEA 编程开发环境阅读源码与编写 Go 程序）。Hyperledger Fabric 官方网站提供了非常不错的入门教程与背景资料，介绍了 Hyperledger Fabric 的专业知识与示例。如果读者对现代密码学和 PKI 安全体系有所了解，将更容易理解 Fabric 的身份权限控制机制，有兴趣的读者可以进一步参考相关资料。当然，最重要的学习资源还是源代码本身，正如大师所言，“源码面前，了无秘密”。

研究底层架构需要把握真正有价值的整体系统架构，应该将研究的关注点集中在理解系统设计的逻辑思路、重要原理与机制、核心模块接口等方面，如果不是为了改进和优化专用模块，则不必过分关注局部实现细节，从而丢失全局架构设计的宏观视野。因此，结合整体系统架构去研究核心模块会更容易理解 Hyperledger Fabric 系统设计的精髓。

对于区块链应用开发者，推荐按照交易处理流程的顺序阅读本书。对于区块链底层开发者，推荐按照本书章节的正常顺序进行阅读。对于区块链技术爱好者，推荐除了核心模块章节之外，可以尝试研究第 6 章 Gossip 消息模块，该模块是通道上组织节点间通信的基础，提供了高效数据分发与状态的同步机制，属于更底层的基础服务，实现机制相对比较复杂。如果读者更关注 Hyperledger Fabric 其他层次的主题，则可以暂时跳过不作深入了解。

本书结构

本书分为 7 个正文章节与附录。第 1 章介绍区块链的基本概念、Hyperledger Fabric 架构等基础知识。第 2 章至第 7 章分别介绍 Orderer 排序节点、Peer 节点、Endorser 背书节点、Committer 记账节点、Gossip 消息模块、公共功能模块等核心模块的底层细节，使得读者可以完整了解 Hyperledger Fabric 架构的设计思想与实现机制。

第 1 章介绍了区块链的基本概念、Hyperledger Fabric 架构与流程，并以 e2e_cli 为例介绍 Fabric 系统部署流程，帮助读者搭建实验环境进行研究。

第 2 章介绍了 Orderer 排序节点，包括 Orderer 服务节点启动流程、Broadcast 交易广播服务、Orderer 共识排序服务、Deliver 区块分发服务等。

第 3 章介绍了 Peer 节点功能模块，包括 Peer 节点启动流程与 Peer 命令模块（Channel 通道子命令、chaincode 链码子命令等）。

第 4 章介绍了 Endorser 背书节点的背书处理流程，负责启动链码容器提供链码服务，对模拟执行结果签名背书并返回提案响应消息。

第 5 章介绍了 Committer 记账节点的功能模块。其中，交易验证器用于验证交易数据，并调用 VSCC 验证背书策略的有效性，账本提交器执行 MVCC 检查以标记交易的有效性，

并提交数据更新账本。

第 6 章介绍了 Gossip 消息功能模块，包括 Gossip 消息模块的启动流程、消息通信与处理机制、节点管理机制、数据分发与状态同步机制、反熵算法等，可以支持节点的动态加入与退出，提供高效的数据分发与状态同步机制。

第 7 章介绍了 Hyperledger Fabric 中常见的公共功能模块，包括账本数据存储模块、安全服务模块、Events 事件模块等。

附录包括 Hyperledger Fabric 相关文件的解析，包括 orderer.yaml 配置文件、core.yaml 配置文件、e2e_cli 示例相关文件等。

关于本书代码

本书分析的代码版本为 Hyperledger Fabric 1.1.0 正式版（2018 年 3 月发布），研究思路是以 Hyperledger Fabric 运行流程为主线展开分析，重点解析 Hyperledger Fabric 的架构设计与实现原理，完整代码请从 Github 官网 https://github.com/hyperledger/fabric 下载。

致谢

非常感谢 Hyperledger Fabric 开源社区贡献者以及本书所有文献引用的原作者，开源共享促进社会与技术进步！

非常感谢机械工业出版社华章分社的编辑杨福川、张锡鹏以及背后的工作人员，是你们的专业精神、严格要求与辛勤付出使得本书的出版成为可能！

在撰写本书的同时，本人获得了互联网上众多区块链开发人员以及高校、企业同行们的无私支持，他们对技术的执着追求令人印象深刻，是值得尊敬与学习的资深领域专家。同时本人也得到很多领导、同事与朋友的热情帮助，如果没有他们的默默支持，本人是无法完成本书的，在此一并致谢。

因时间仓促与水平有限，本书难免有错误遗漏之处。欢迎读者批评指正，将错误与不当之处发送至邮箱 xinli@nudt.edu.cn，或者通过 QQ 交流群 491318059 以及微信群与笔者（QQ 号 / 微信号 501319508）交流，以便重印或再版时及时更正。同时，本书在撰写过程中参考了大量文献与互联网资料并标注了引用出处，在此表示感谢，如果存在疏漏或版权问题，请发送邮件或直接联系笔者，以便及时更正。

李鑫

目 录 *Contents*

第 1 章 Chapter 1

区块链基础与 Hyperledger Fabric 架构

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.

2009 年 1 月 3 日，（英国）财政大臣正处于实施第二轮银行紧急援助的边缘。（在比特币创世区块中记录的永不修改的话）

——中本聪

本章将从区块链产生的背景开始介绍比特币、以太坊等热点词汇，探讨区块链当前与未来的发展趋势，并逐步介绍区块链的基本概念与核心技术，进而分析 Hyperledger Fabric 的架构与核心机制。另外，读者可以在本章中学习到如何搭建 Hyperledger Fabric 实验环境，尝试运行并查看实验结果。

1.1 区块链背景、概念与现状

本节将介绍区块链产生的背景及研究热潮、区块链的概念与核心技术，并分析目前国际上影响力较大的主流区块链开源平台。

1.1.1 区块链产生的背景及研究热潮

近年来，比特币（Bitcoin）无疑是最热门的投资品词汇，其价格最高时突破了两万美元，成为投资者眼中的新宠和竞相追逐的“真金白银”。比特币一词最初来源于 2008 年中本聪（Satoshi Nakamoto）在 metzdowd.com 网站发表的《 Bitcoin: A Peer-to-Peer Electronic Cash System 》[1]（《比特币：一个点对点的电子现金系统》），这是比特币与区块链理论形成中重要的奠基性论文，并真正开启了虚拟数字货币与区块链应用的人类社会新时代。

中本聪在这篇论文中解决了之前发行虚拟数字货币存在的货币伪造、双重支付（或称“双花”，Double Spent）、匿名化交易、中心化货币发行等挑战，可以不依赖第三方信用机构进行背书，无须基于中心化货币发行体系，在全球范围内实现了点对点交易的可靠记账。比特币持续 9 年多不间断的正常运行表明，这种分布式架构在适当的激励机制与共识算法的作用下拥有支撑全球范围交易的潜力，为当前金融领域造价不菲的中心化架构提供了新的解决思路。因此，在比特币的“挖矿”产业生态中，每个人都可以参与记账，充分利用非对称加密、哈希算法等现代密码学技术确保比特币交易不可伪造、不可篡改且可溯源的特性，并通过记账奖励的方式激发每个节点参与记账的积极性，这就使得黑客的攻击成本非常高昂，还不如“挖矿”参与社区贡献。正是这种结合正反馈奖励机制与博弈心理学的巧妙设计，使得比特币交易系统迅速发展为一个国际共享的分布式账本系统，比特币也一跃成为当下最热门的投资品种之一。但是，比特币没有类似于传统货币相应对等的背书信用标的物作担保，缺乏全社会认同的货币价值基础。因此，比特币相继被各国进行监管并禁止流通兑现或接受为可交换的“货币”。时至 2018 年，比特币已经运行了 9 年多的时间，支持过单笔上亿美元的交易，截至 2018 年 11 月，比特币交易系统已经累计生成超过 55 万个区块（https://www.blockchain.com/en/explorer）。虽然遭到无数次黑客攻击，但从未停止运行，总市值一度超过了上千亿美元，毫无疑问，比特币已成为人类历史上最有影响力的虚拟数字资产之一。

以太坊去中心化自治组织（Decentralized Autonomous Organization，DAO）项目的想法极具天才般的创造性，它旨在构造一个完全去中心化的自治服务平台，并基于超过一定比例的虚拟实体或股东（如 67%）来决定投资或修改运行机制，完全透明且无须人类集中式管理。2016 年 5 月，DAO 项目通过分布式众筹在 28 天内筹集了超过 1.52 亿美元，一举成为当时人类历史上的最大单笔金额众筹项目，同日在各大数字货币交易所开始交易。然而，半个多月后，黑客利用智能合约中递归调用等漏洞盗走了近三分之一众筹所得的以太币，震惊了整个 DAO 社区，公众也由此对去中心化自治系统的安全性与可行性产生了质疑。项目开发者通过研究发现该漏洞不是出现在 DAO 架构本身，而是智能合约出现了问题。这迫使开发者对 DAO 项目强行“硬分叉”，即在挖出第 192000 个区块后的分支上消除被盗走的货币，并决定最终在提取分发完后自动解散 DAO 项目。该事件引起了极大的社会争论与媒体关注，但是，以太坊 DAO 项目无疑是人类社会在去中心化自治系统上具有深远影响力的一次伟大的创新尝试。

近年来，这些创新项目与事件已经开始深刻影响和改变着人类社会，各种琳琅满目的数字虚拟货币以及“去中心化”的分布式应用纷纷出现，虚拟货币交易所在全球遍地开花，追逐企业“币改”与“链改”的大潮席卷而来，而“区块链”就是比特币、以太坊 DAO 等项目采用的底层核心技术，人们发现它不仅可以作为比特币这种“虚拟货币”诸多优良特性的技术基础，而且还可以用来构筑开放信用体系与资产确权的基石，被认为可能开启人类社会基于互联网与虚拟平台传递价值的时代。

区块链技术通过去中心化方式建立起点对点的信任关系，可能会影响甚至改变决定人类社会组织形式与现象的基本作用力，包括生产力水平、生产资料和生产成果的分配总量

与速率、权力的中心化程度等[2]，尤其是弱化了权力集中与运作方式，直接改变了生产资料和生产成果的分配方式，进一步提高了生产力水平。因此，人们普遍认为区块链技术具备改变当前很多领域的潜力，可以与电力、互联网等技术革命相提并论，甚至被《华尔街日报》誉为五百年来最具影响力的金融创新之一。与此同时，区块链已经成为社会与科研人员关注的热点，在金融服务、供应链管理、文化娱乐、智能制造、社会公益、教育就业、医疗健康等垂直领域都引起了人们的广泛关注和强烈兴趣。

目前，区块链被普遍认为是一种具有“颠覆性”的新兴技术，它可能会带来公共与私营服务实现方式上的创新，其最大的“颠覆性”就是重构弱信任主体之间的信用体系，从而避免传统信用体系依靠第三方中介证明的方式。这种信用体系是建立在程序化的区块链共识算法与安全加密算法的基础上，而不是基于单个人或单个系统。同时，数据记录的生成与记录保存需要全网络参识节点按照共识算法进行确认并且不易篡改，如比特币获得 51% 以上的全网计算能力，就可能拥有记账权并修改账本。

因此，区块链摆脱了传统信任体系中需要第三方信息验证的信用确认模式，能够有效降低信用体系构建成本，提高跨组织体系要素的协同效率，同时提高链上资产的真实性、可信性与安全性，天然适合于松耦合的去中心化应用场景，在协调大规模跨组织活动中能显著降低集中式系统带来的复杂性、安全风险、信息不透明度等问题。人们甚至认为，区块链可以帮助建立去中心化的全球信用体系，让互联网价值传递可以像互联网信息传递一样具有低成本与高效率的特点。这样，人们就能够基于区块链技术，通过去中心化的方式重构新型的经济生态体系，促进个体行为与社区生态之间的高效协调和可持续发展，引入合法的激励机制与监管手段，鼓励个体创造社区价值与协作交换，更加强调点到点的直接个性化服务，连接与盘活互联网的巨量边缘资源，大幅降低社会经济活动成本，从而培育可持续发展的垂直领域社区价值生态，以激发潜在的用户场景需求（如存储、泛娱乐、即时通信、物联网支付等）。同时，区块链也可以为弱信任主体间提供可信平台支持共享敏感数据，以提升行业上下游甚至跨行业大规模协作的效率，减少企业联盟间繁冗业务流程的生产成本，提高信息监管透明度，避免高度中心化系统中单点故障带来的系统失效，降低黑客攻击风险。因此，区块链具有改变未来社会生产与生活形态的潜力，赋能产业经济推动共享经济的普及与发展，催生新的区块链产业与促进相关产业升级，创造社会经济价值。

事实上，研究区块链相关技术与应用场景结合，为生产经济、国防安全、科学研究、社会稳定等领域构建高效、稳定、安全的区块链基础设施，提供高效动态的部署跨域区块链网络的能力，从而抢占战略制高点与商业市场，已经成为目前人们竞相研究区块链相关科学与工程问题的基本动机。区块链的应用场景所引起的有别于传统数据库的核心问题，如互联网大规模数据存储与同步技术、高效共识算法、高强度密码安全技术、高性能跨链技术、新型匿名隐私安全技术等正面临着一场深刻的技术变革，可能会孕育爆发出“区块链 +”时代的到来。

但是，人们也应该看到，区块链技术只能确保链上数据的真实性与可信性，可防止不被

轻易攻击且不易被随意篡改，却无法解决链下虚假数据或真实数据“转移”到链上数据过程中的真实性问题。同时，以比特币为代表的“虚拟货币”或 Token（通证）数字资产也带来了风险定价与管理、价值锚定与信任体系缺失、区块链经济系统顶层设计等新挑战仍然是在各国法律框架和行业监管需求内挑战人类智慧与技术极限的重大难题。

如图 1-1 所示，2008 年以来的区块链典型事件表明，区块链作为一种可能会重塑社会运作方式的“颠覆性”创新技术，已得到越来越多的关注与研究，且已经发展成为具有较大影响力的生态体系。

2008年
- 中本聪首次在《比特币：一个点对点的电子现金系统》论文中提出区块链的概念。

2009年
- 1月，创造诞生了世界上第一个区块“创世区块”，基于区块链的比特币正式诞生。

2010年
- 5月22日美国佛罗里达程序员Laszlo Hanyecz用10 000个比特币交换了两块价值25美金的披萨。这是比特币第一次在现实世界获得公允汇率，按2017年6月20日价格计算，这两块披萨价值2000多万美元。

2012年
- 瑞波币（Ripple）基于比特币区块链思想实现去中心化的支付与跨国清算转账系统，其目标是挑战国际银行间支付清算SWIFT系统。

2013年
- 3月，比特币区块链出现硬分叉，强迫大型矿池采用0.7旧版本后使得分叉又重新合并。
- 8月，德国联邦财政部承认比特币和外汇一样，但不能用于法定支付手段。
- 12月，中国五部委联合发布《关于防范比特币风险的通知》，禁止第三方支付参与比特币交易。

2014年
- 以太坊（Ethereum）项目启动众筹，试图将区块链技术运用到智能资产注册与交易等领域。
- 6月，美国加州通过法案允许使用比特币等数字货币进行消费。

2015年
- 《华尔街日报》称区块链为五百年来金融领域最重要的创新。
- 1月，Coinbase获准成为美国第一家持牌比特币交易所。
- 10月，《经济学人》发表封面文章《信任机器》（The Trust Machine）。
- 12月，纳斯达克与合作伙伴Chain.com首次在个股交易商中使用区块链技术平台Linq。
- 12月，Linux基金会启动“超级账本”Hyperledger Fabric项目。

2016年
- 1月，中国人民银行在京召开数字货币研讨会或推出央行数字货币。
- 3月，Blockstream和DAH公司在黑客松编程活动将各自代码融合到IBM提供给开源社区的Open Blockchain代码中，形成Hyperledger Fabric雏形。
- 5月，日本首次批准数字货币监管法案，并定义比特币为财产。
- 7月，比特币产量第二次减半。
- 12月，Hyperledger开源社区发布Fabric 0.6.0-preview技术预览版本。

2017年
- 1月，中国人民银行宣布数字货币试运行试验成功。
- 3月，Hyperledger开源社区发布Fabric 1.0.0-alpha测试版。
- 5月，中国《区块链参考架构》标准发布。
- 5月，全球爆发比特币WannaCry“勒索”病毒，其利用微软系统本身漏洞实施的攻击，并强制要求使用昂贵的比特币充值来解锁硬盘文件，与比特币本身安全性毫无关系。
- 7月，Hyperledger开源社区发布Fabric 1.0.0正式版。
- 9月，中国人民银行、中央网信办、工业和信息化部等7部委共同发布公告表示，停止各类代币发行融资活动，并清退已完成的代币发行，合理保护投资者权益。
- 10月，以太坊“拜占庭”硬分叉顺利进行。以太坊客户端钱包parity发现严重漏洞，导致约50万枚以太币被冻结，在白帽黑客协助下找回37.7万枚以太币。
- 12月，根据coinmarketcap数据显示17日上午4:19分左右比特币价格达到历史最高20 089美元。

2018年
- 2月~3月，“俄罗斯版微信” Telegram的ICO连续两轮融资都获得了8.5亿美元，共17亿美元。
- 3月，Hyperledger开源社区发布Fabric 1.1.0正式版。
- 6月，加密数字货币EOS总融资额近42亿美元。
- 7月，Hyperledger开源社区发布Fabric 1.2.0正式版与Fabric 1.1.1正式版。

图 1-1　区块链典型事件