

深入浅出区块链

核心技术与项目分析

梁 伟◎编著



中国工信出版集团

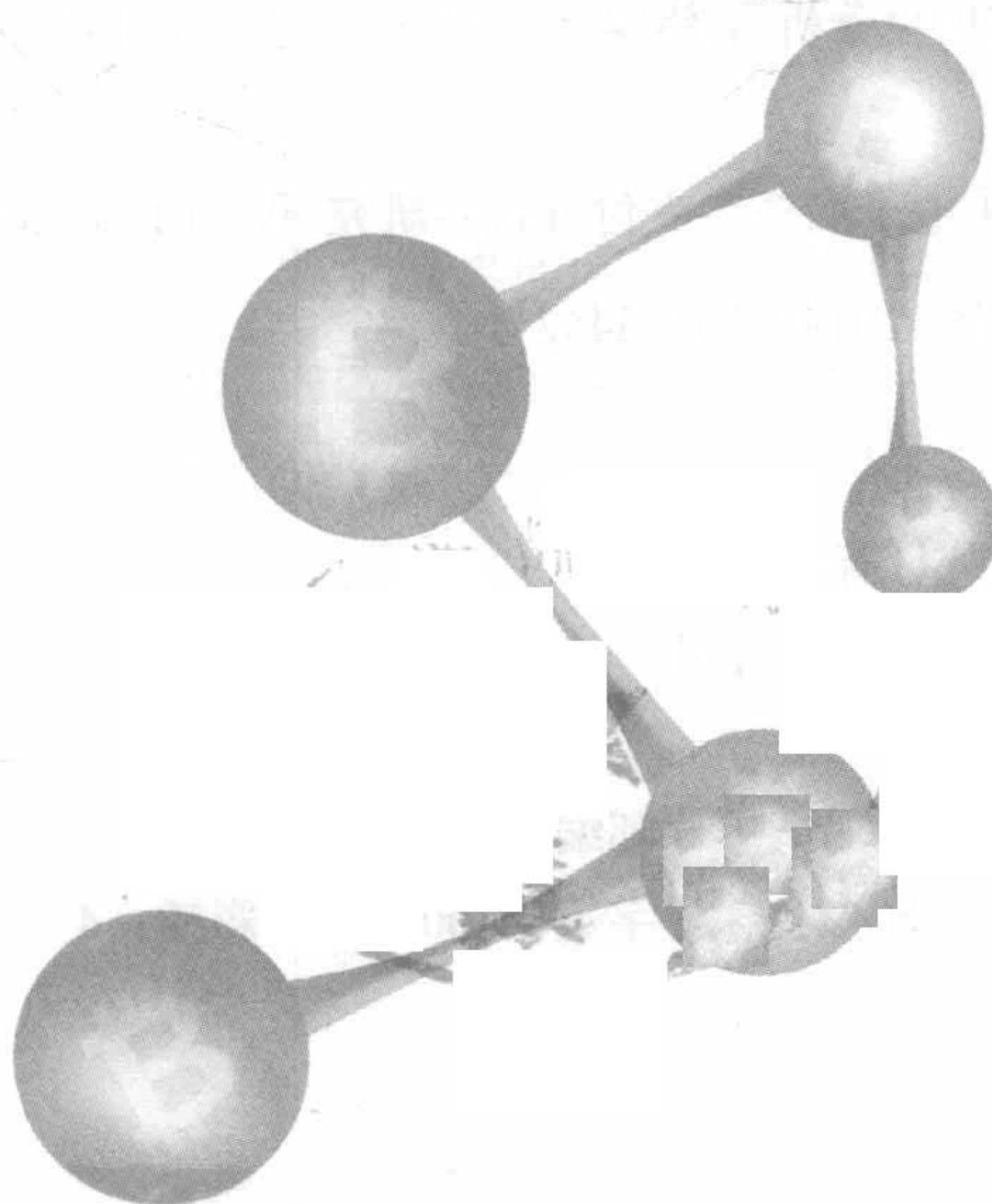


电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

深入浅出区块链

核心技术与项目分析

梁 伟◎编著



电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内容简介

区块链技术作为未来价值互联网的雏形，世界经济论坛预测，到2025年，全球GDP的10%将由区块链技术承载。作为继蒸汽机、电气化、计算机之后第四次工业革命的重要成果之一，区块链是集合了分布式存储、P2P网络、共识、安全加密等技术的综合创新。

本书通过透视优质的代表性区块链项目，可以让读者全面了解区块链产业发展现状，并加深对区块链新技术的理解。本书不求大而全地泛泛而谈，也不谈“币圈”乱象，而是针对区块链具体的核心技术点为读者建立起区块链技术体系的知识树，并从核心技术的视角向读者展示理念超前、工作扎实的一些优秀项目，这有利于提升读者对区块链领域的投资和从业认知。

本书适合区块链从业人员阅读，具体包括开发人员、CTO、决策者、解决方案专家、售前人员等。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有，侵权必究。

图书在版编目（CIP）数据

深入浅出区块链核心技术与项目分析/梁伟编著. —北京：电子工业出版社，2019.9

ISBN 978-7-121-33750-5

I. ①深… II. ①梁… III. ①电子商务—支付方式—研究 IV. ①F713.361.3

中国版本图书馆CIP数据核字（2019）第163442号

责任编辑：李利健

印 刷：三河市双峰印刷装订有限公司

装 订：三河市双峰印刷装订有限公司

出版发行：电子工业出版社

北京市海淀区万寿路173信箱 邮编：100036

开 本：720×1000 1/16 印张：15 字数：300千字 彩插：4

版 次：2019年9月第1版

印 次：2019年9月第1次印刷

定 价：69.90元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

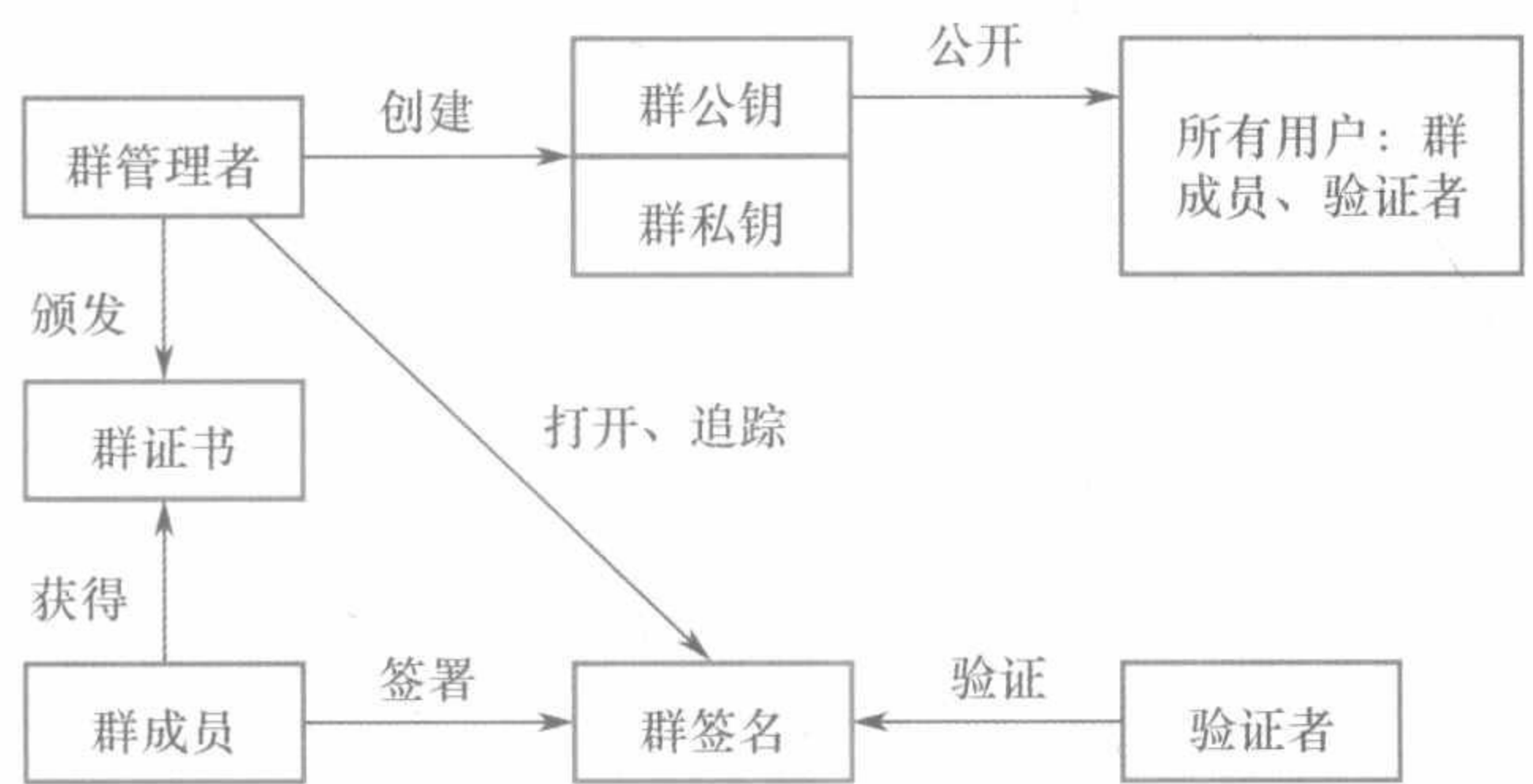


图 2-8 群签名的一般流程

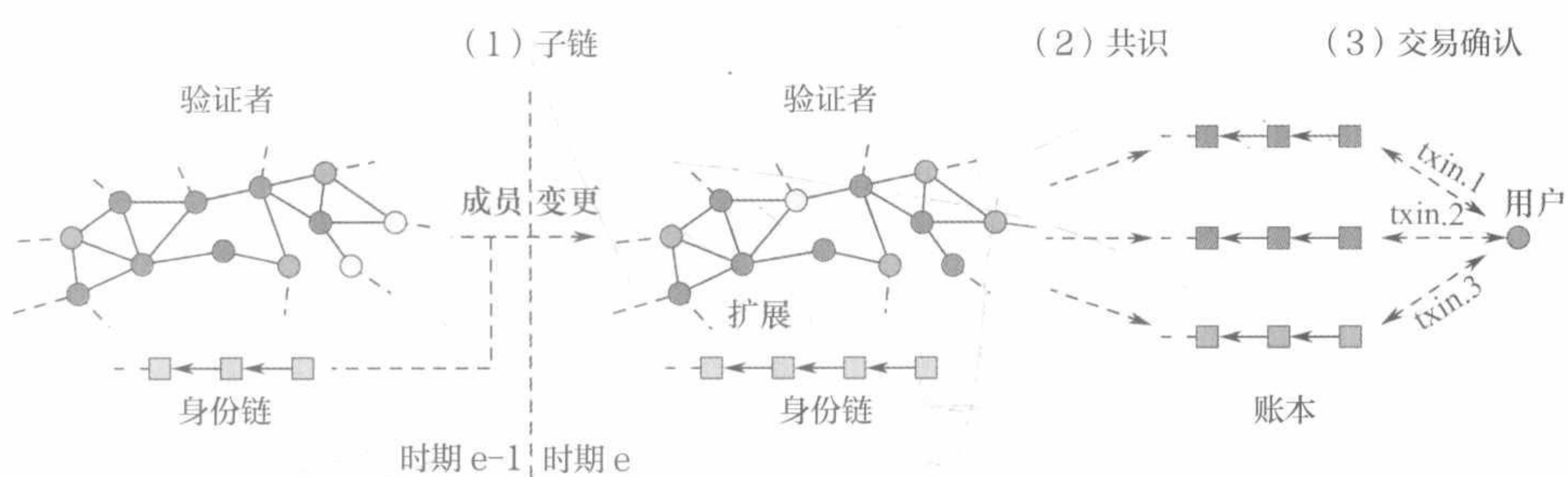


图 2-10 OmniLedger 的总体架构和设计重点

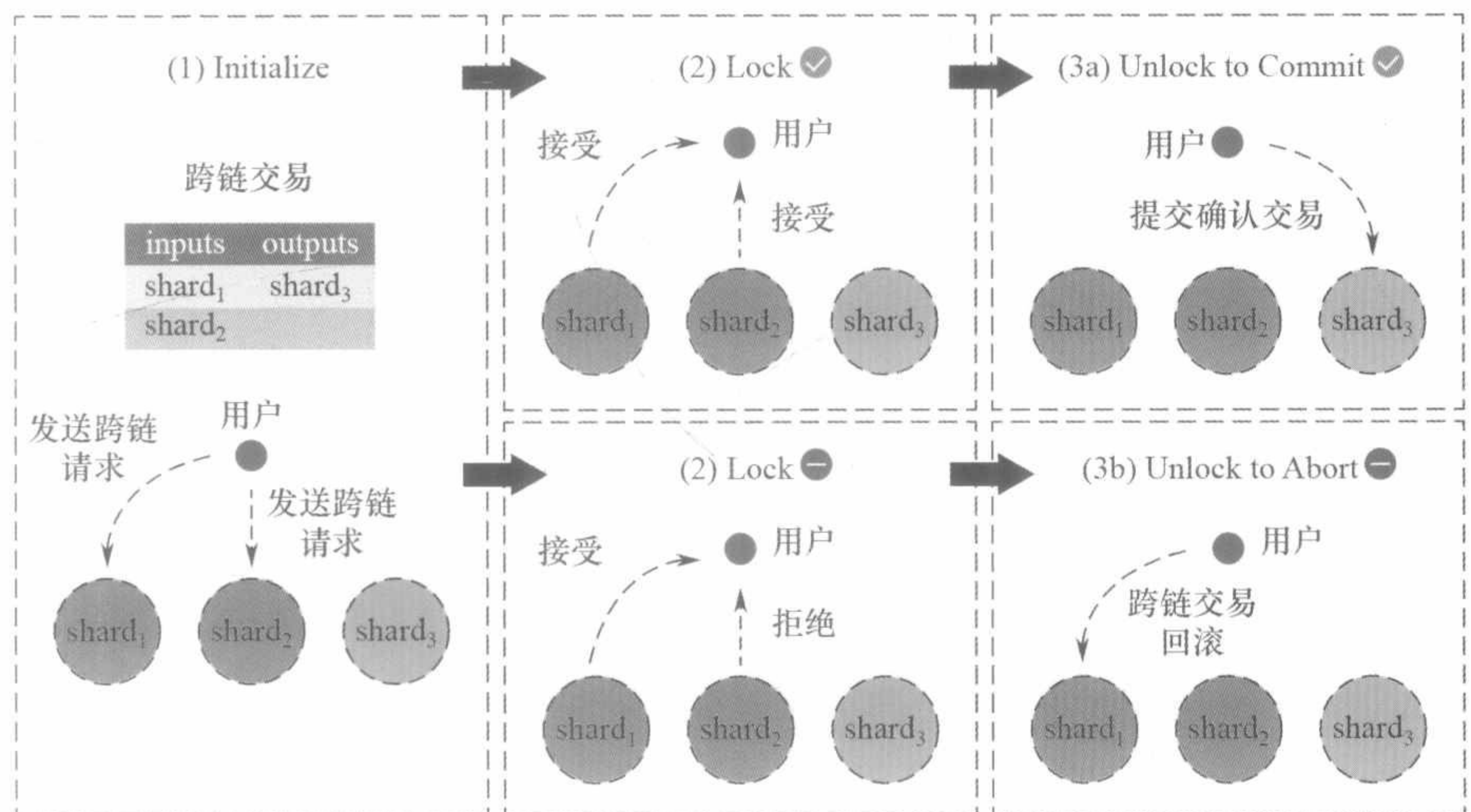


图 2-11 OmniLedger Atomix 协议

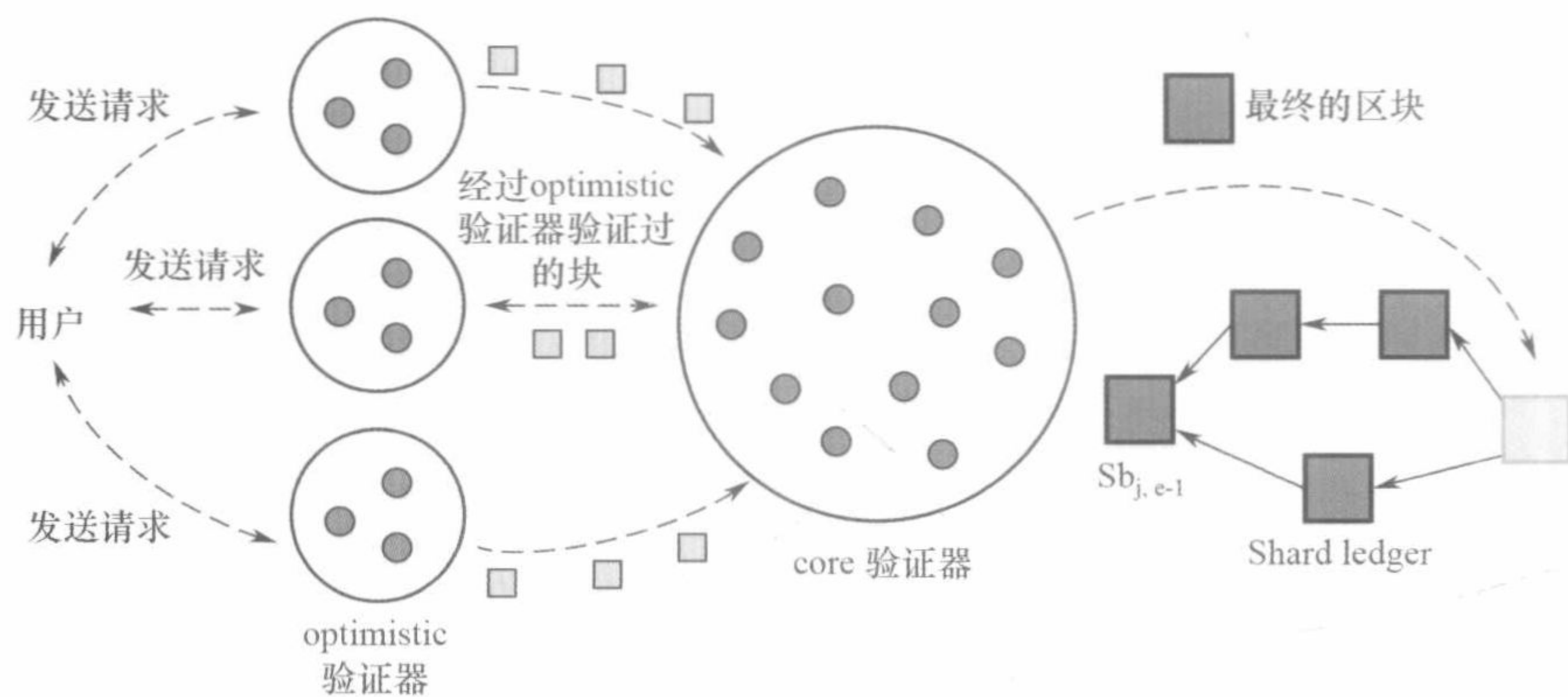


图 2-12 OmniLedger 分层处理机制

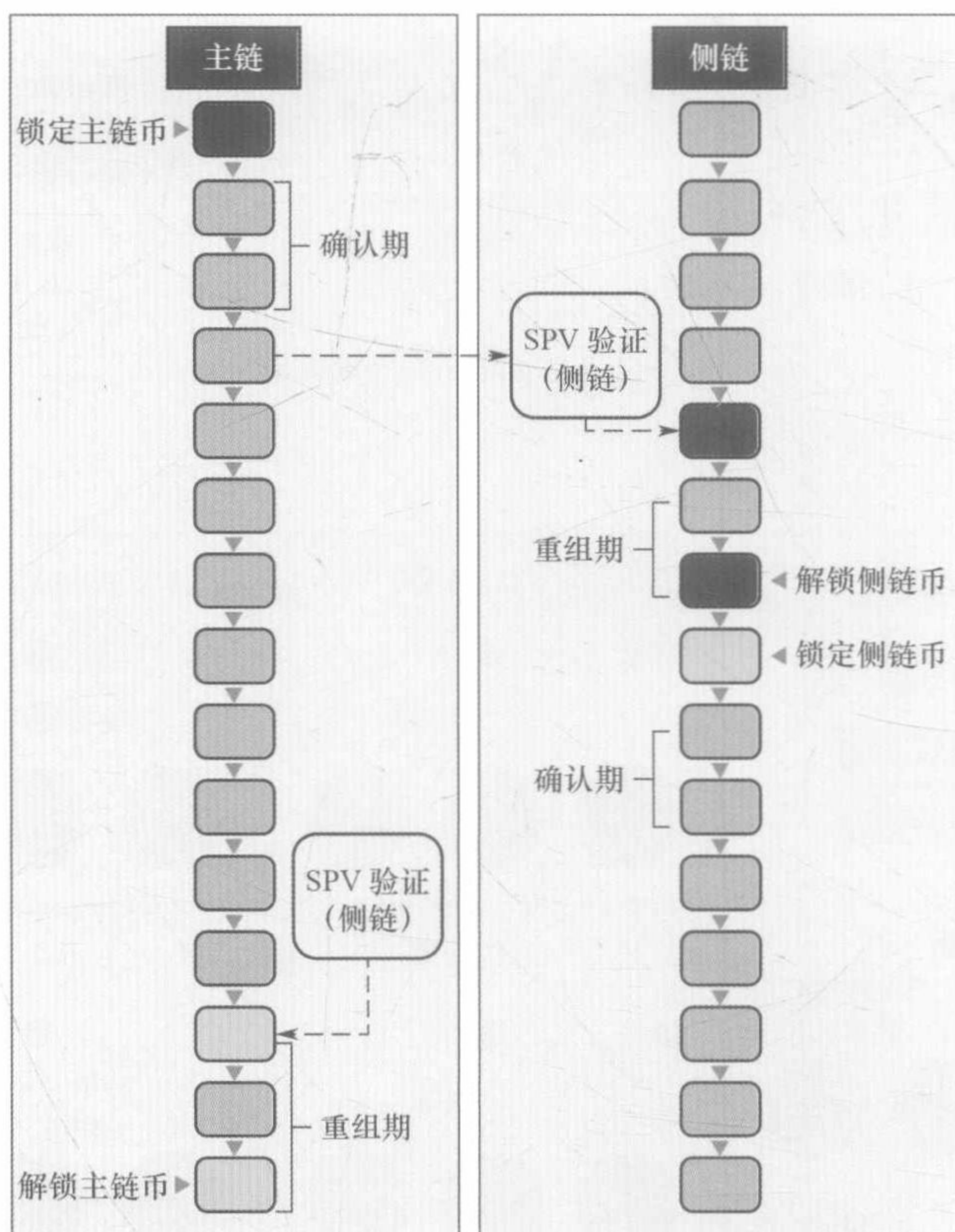


图 2-13 双向锚定技术

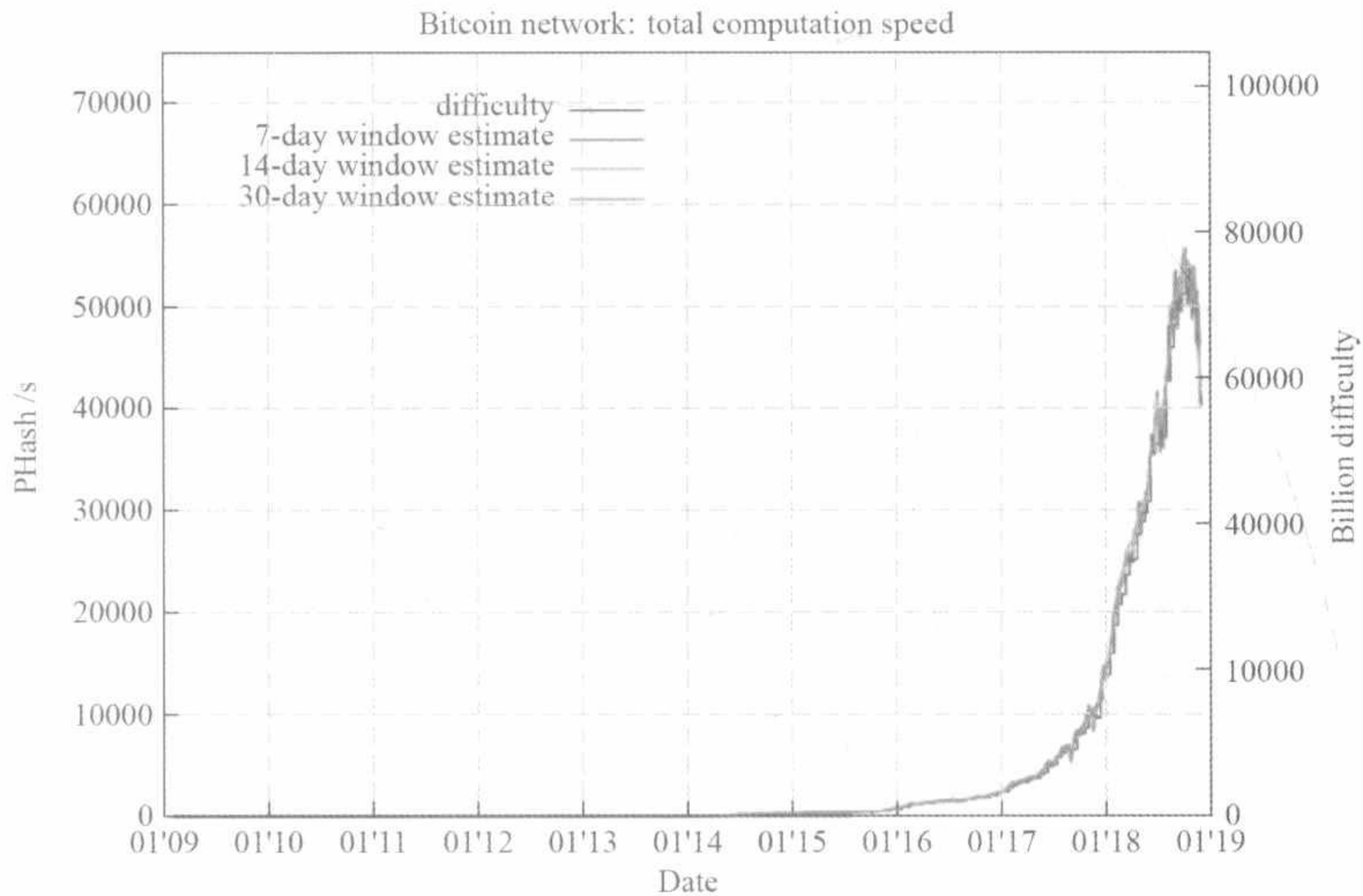


图 2-14 比特币挖矿算力技术图

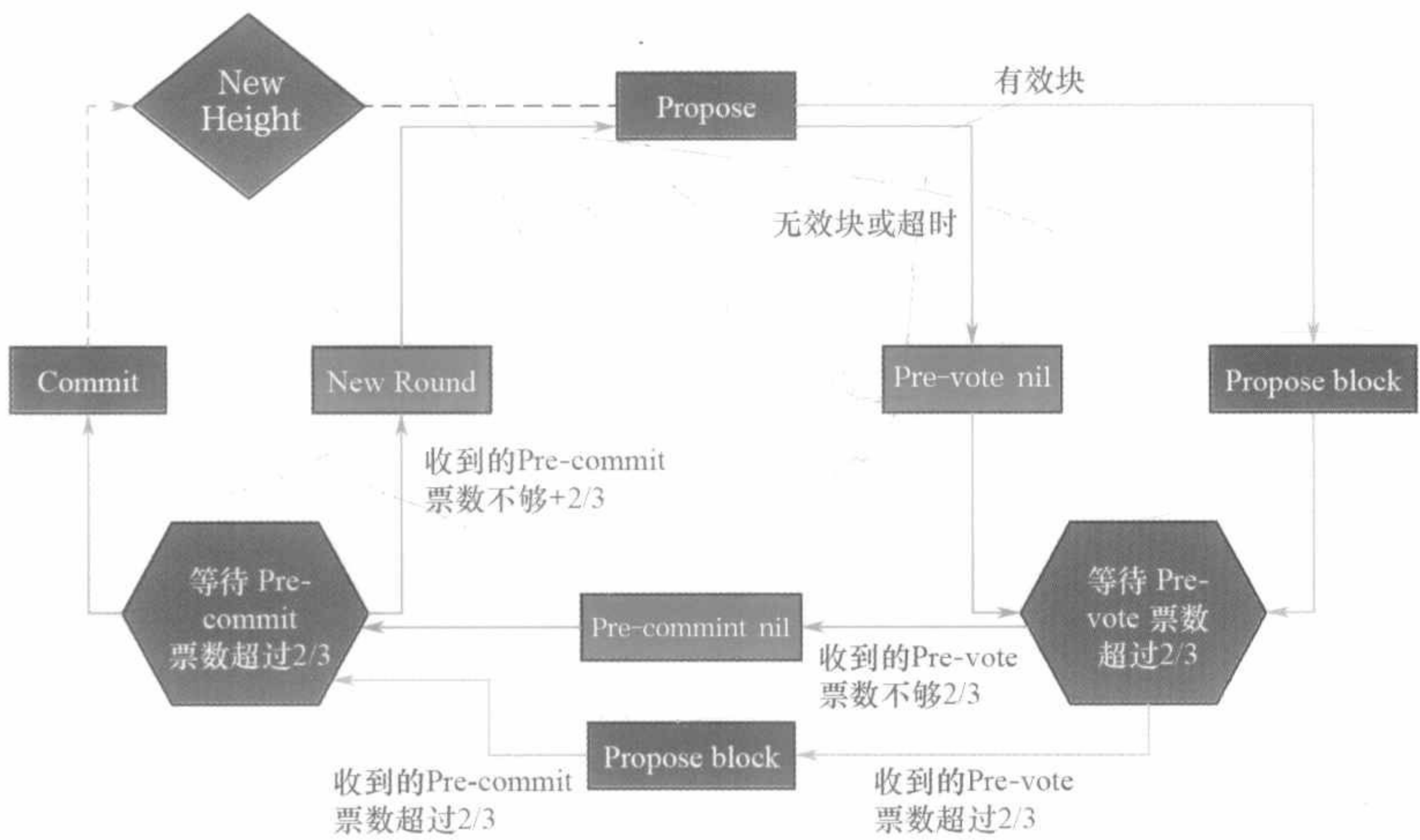


图 2-21 Tendermint 核心算法流程

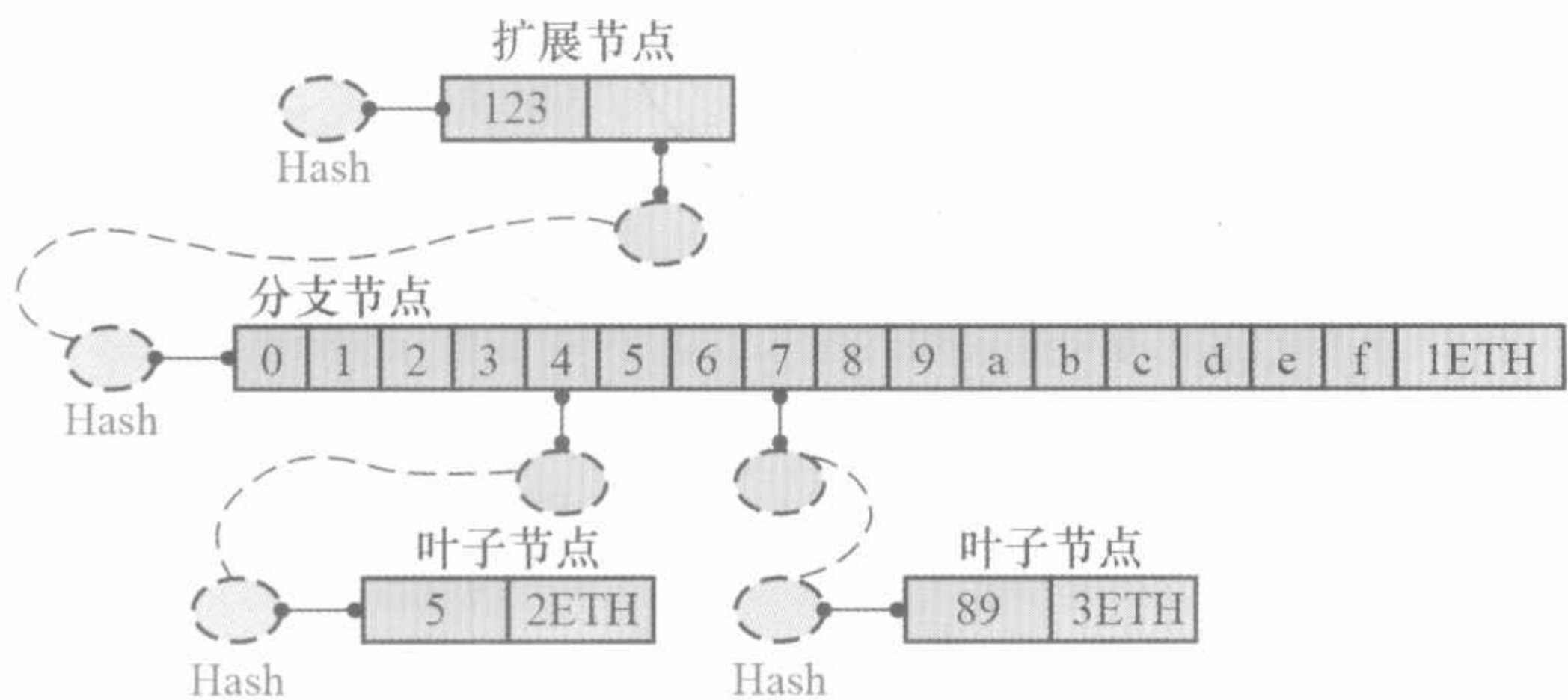


图 3-5 散列索引图

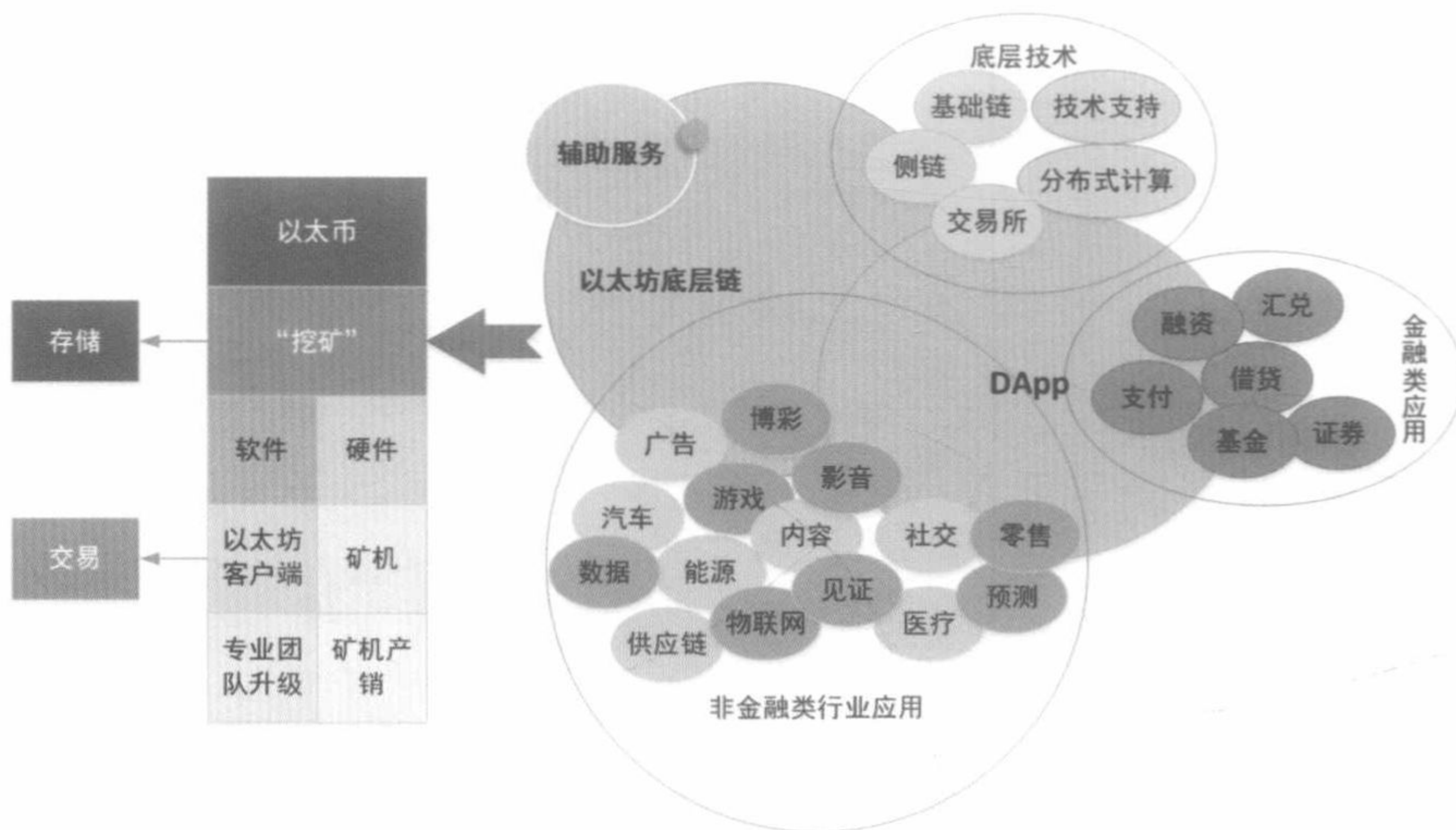


图 3-7 以太坊的生态系统

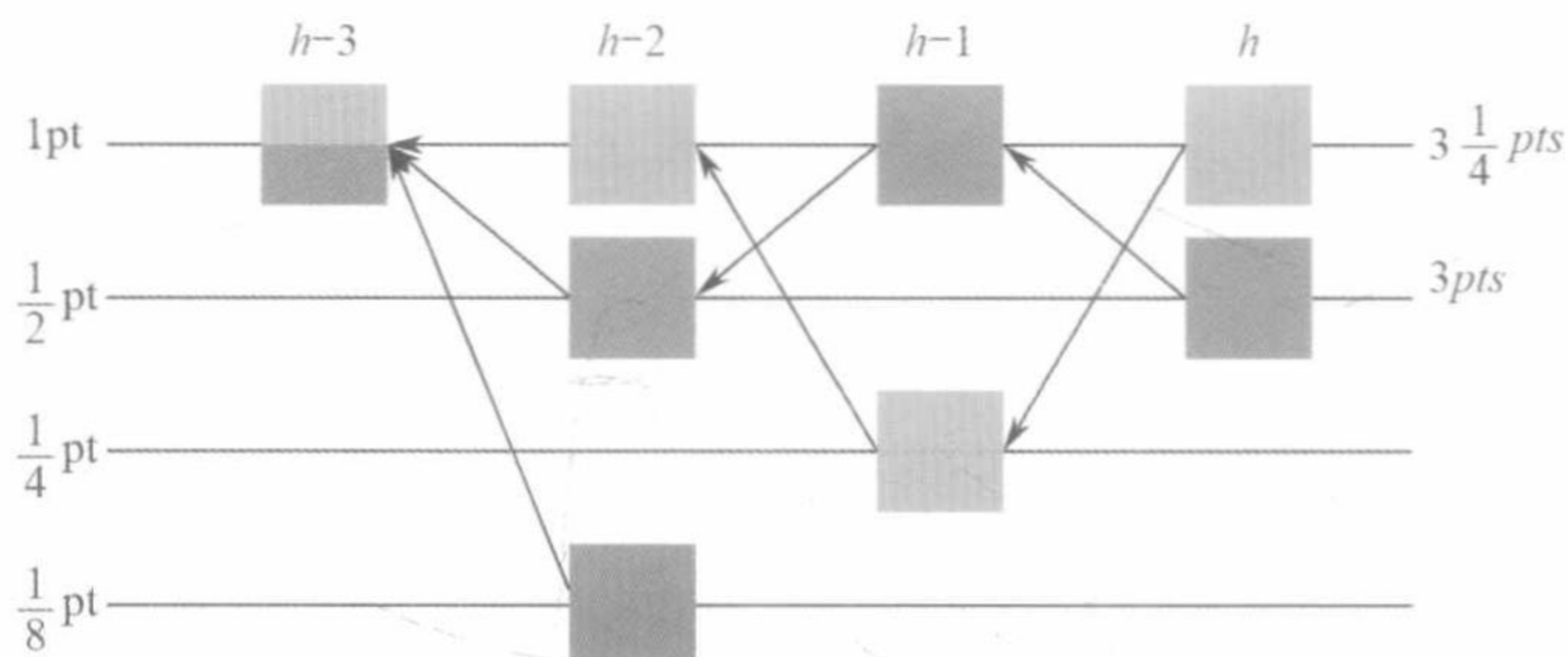


图 3-11 链的权重

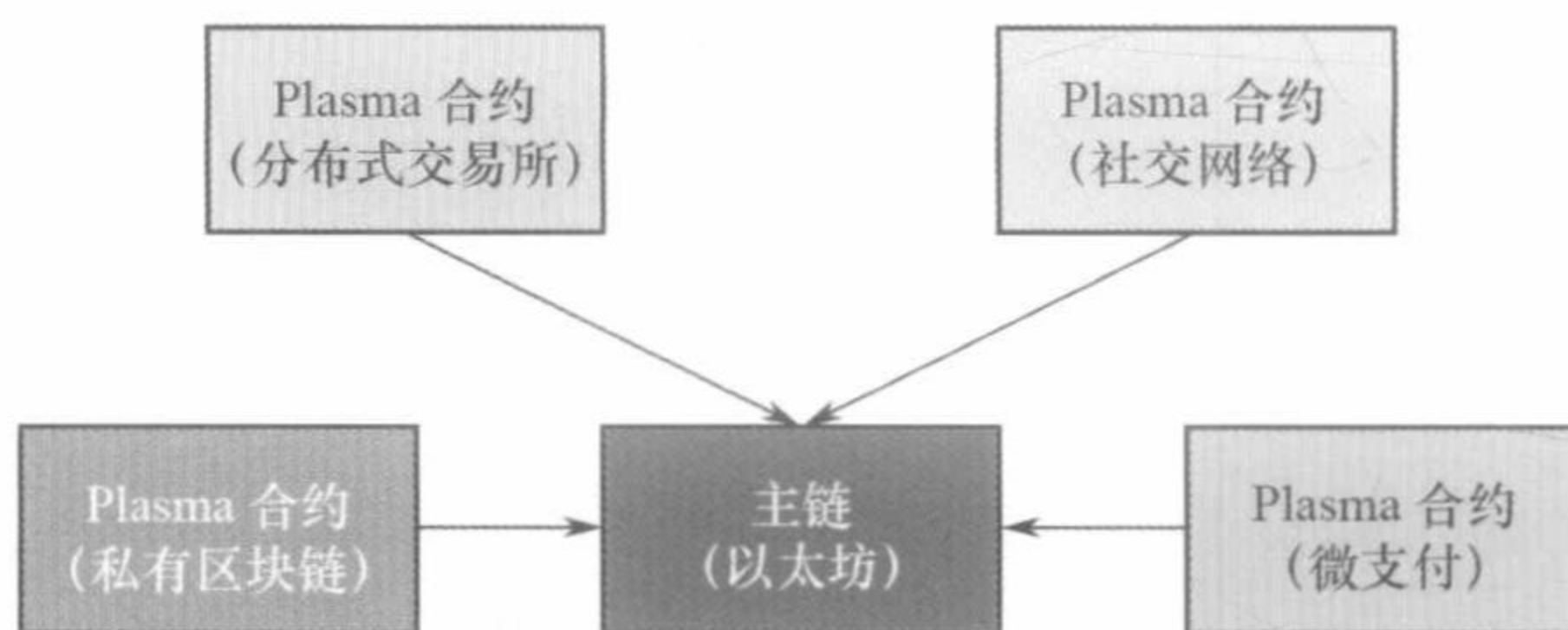


图 3-19 Plasma 链下扩容方案

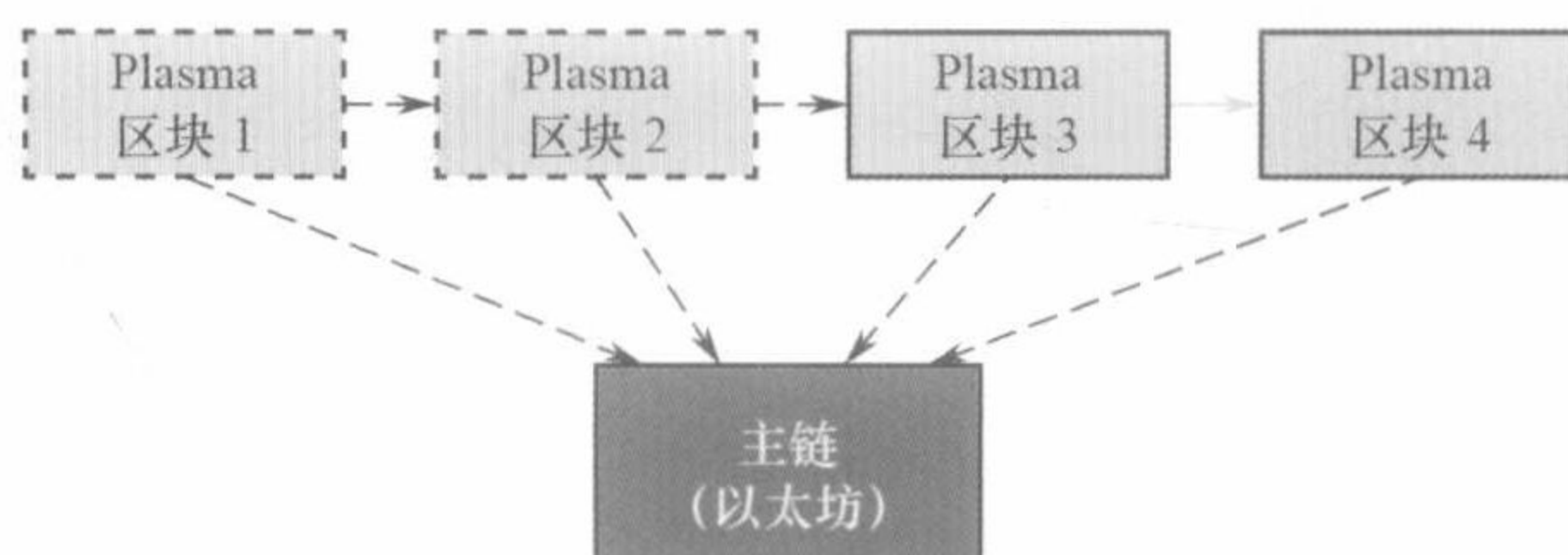


图 3-20 Plasma 节点的欺诈证明

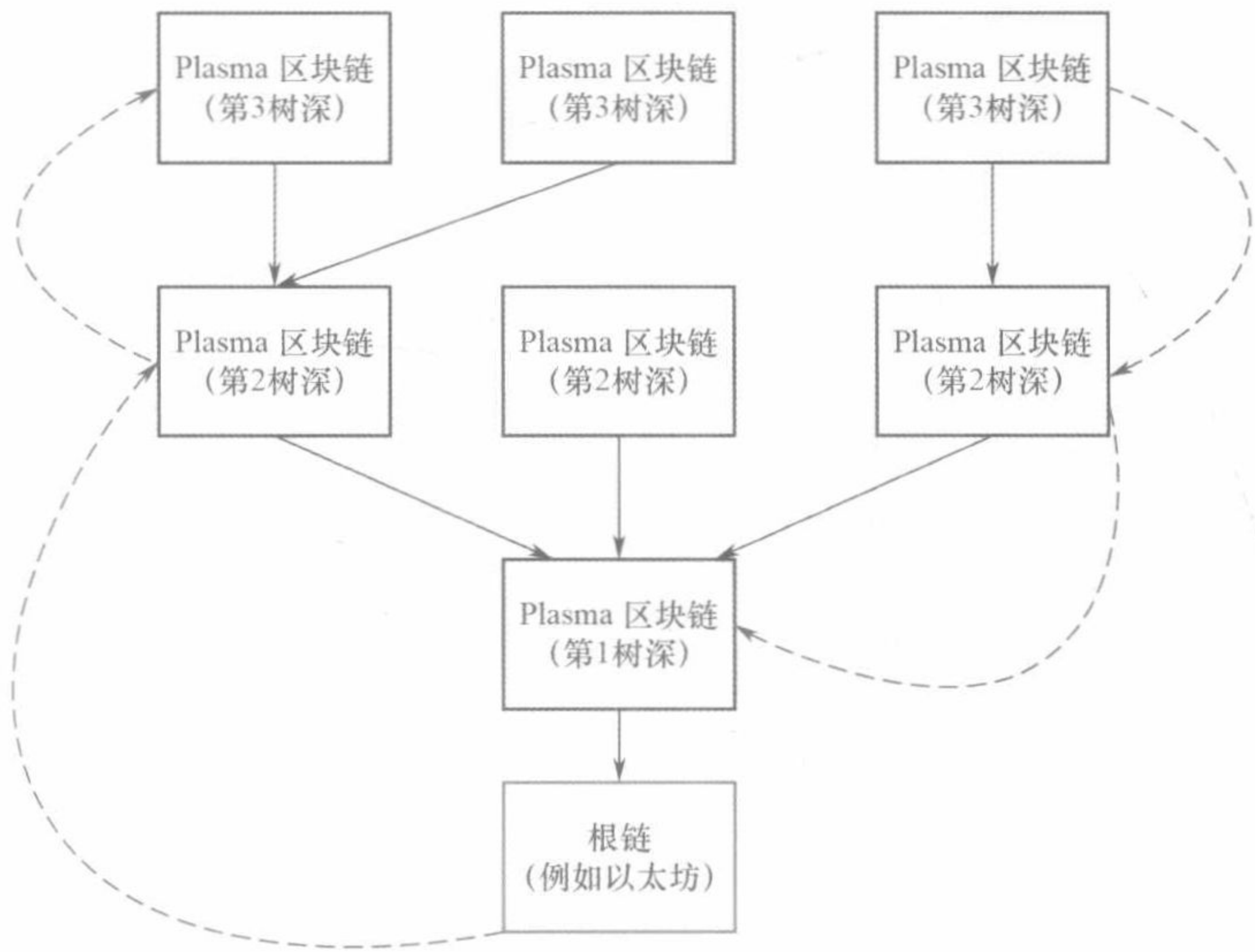


图 3-21 MapReduce 高扩展计算流程图

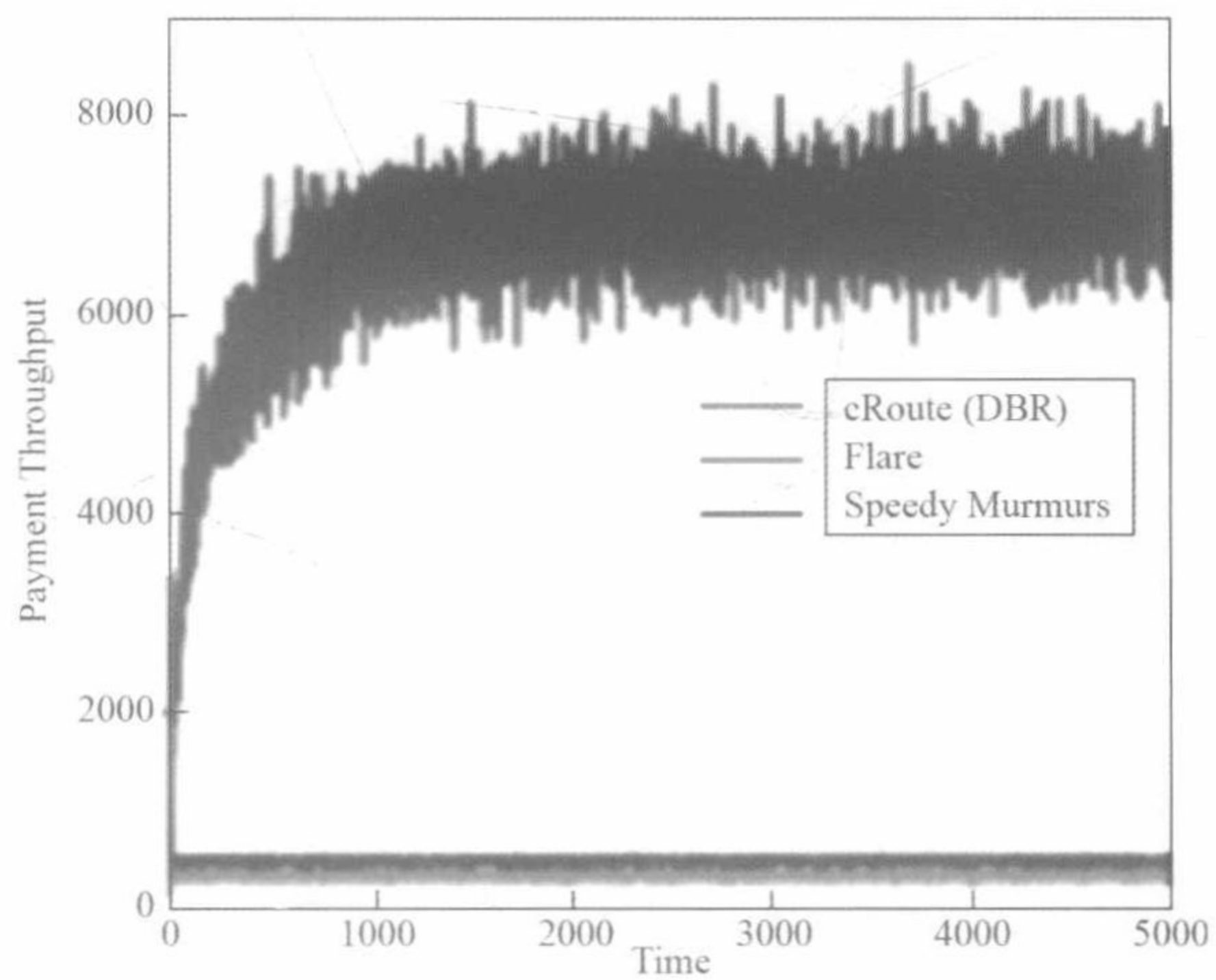


图 3-24 线下支付路由算法性能

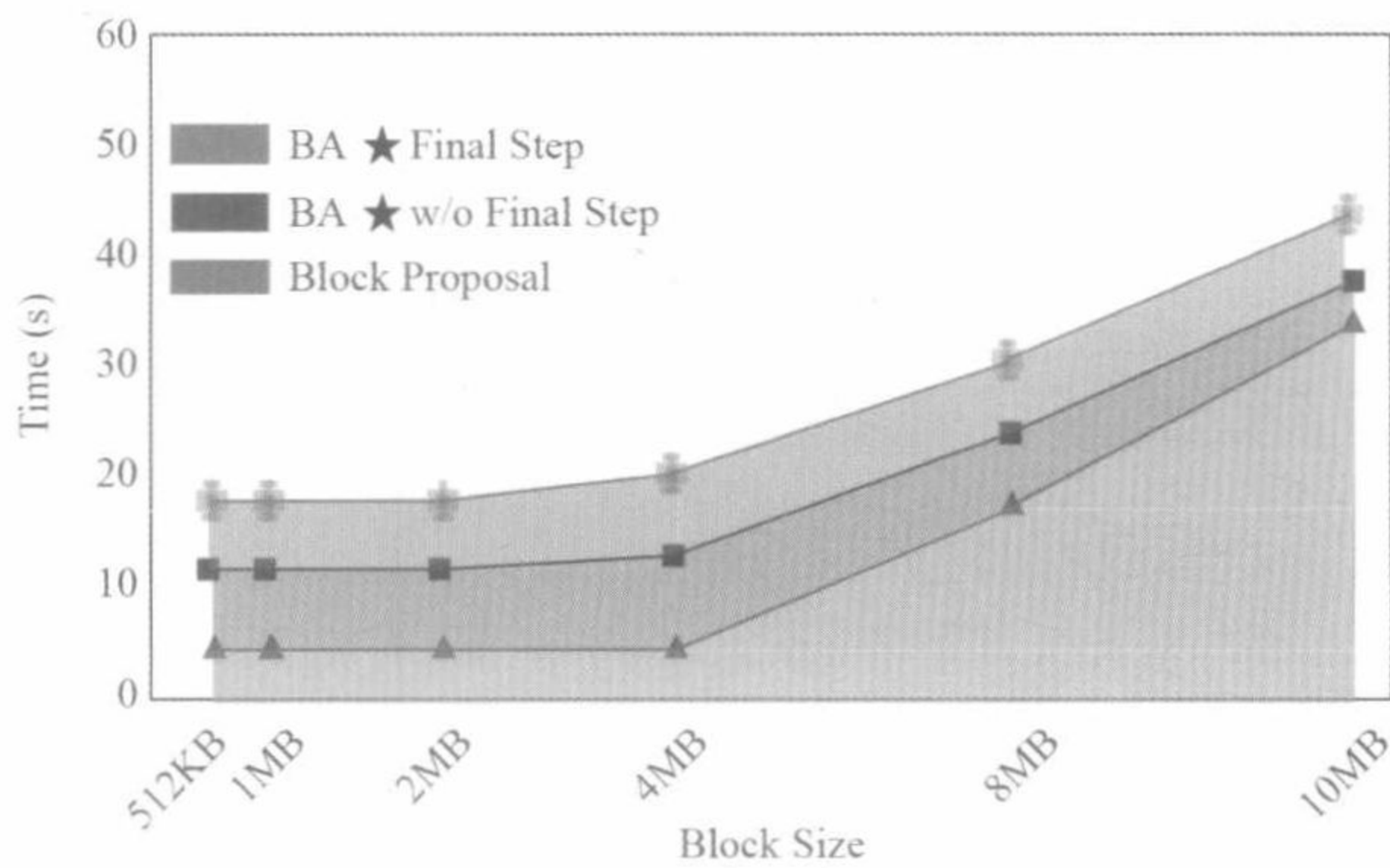


图 3-27 区块大小对通量影响关系图

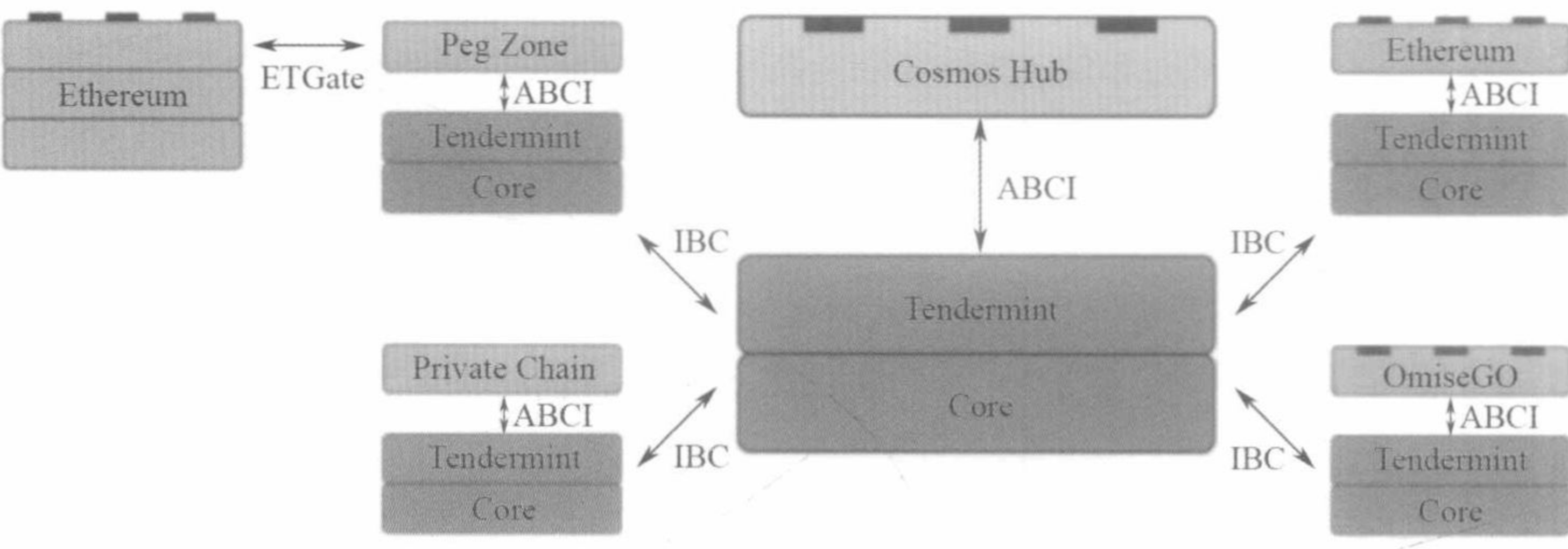


图 3-35 Cosmos 生态框架

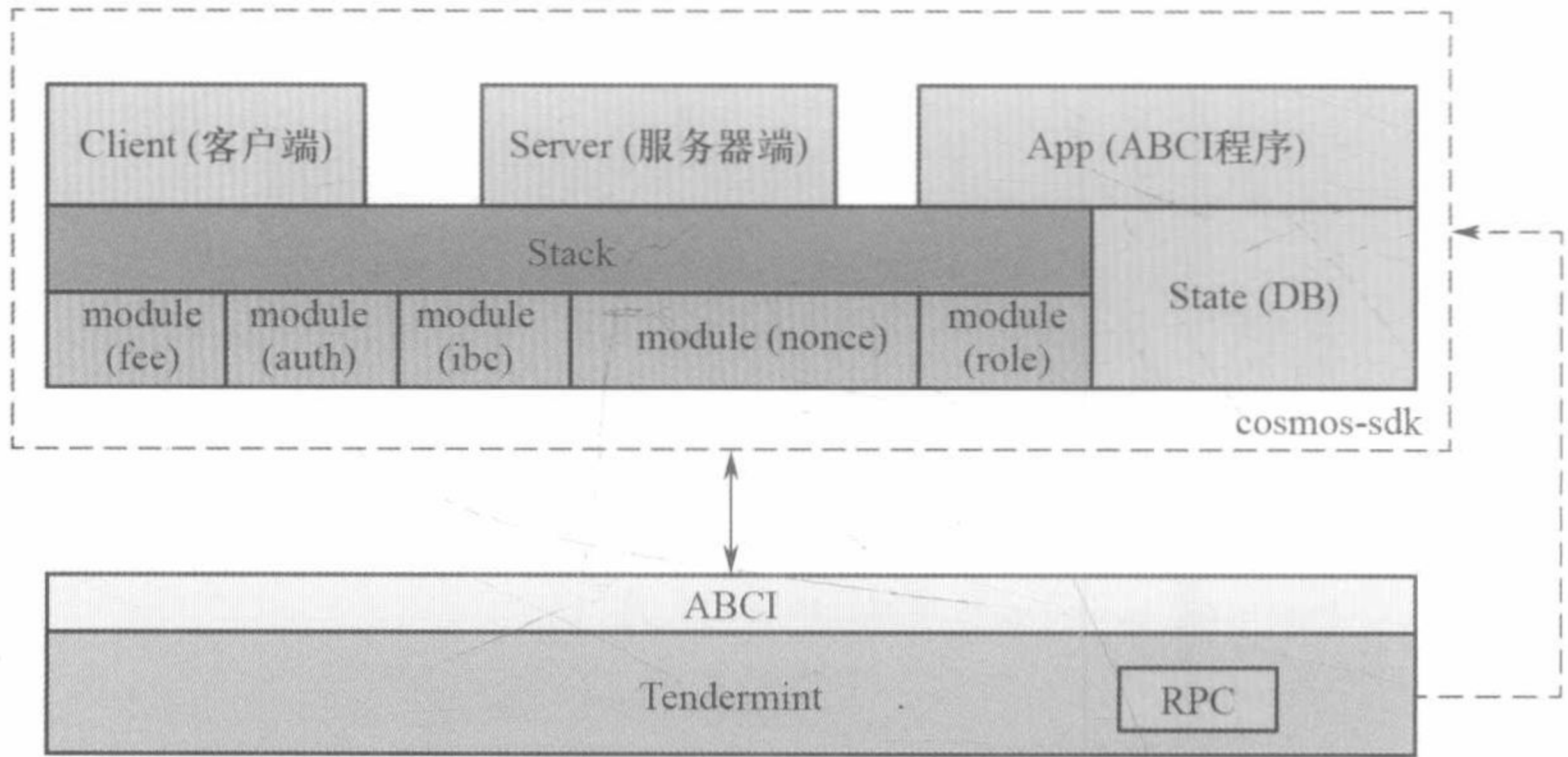


图 3-36 Cosmos SDK 的框架

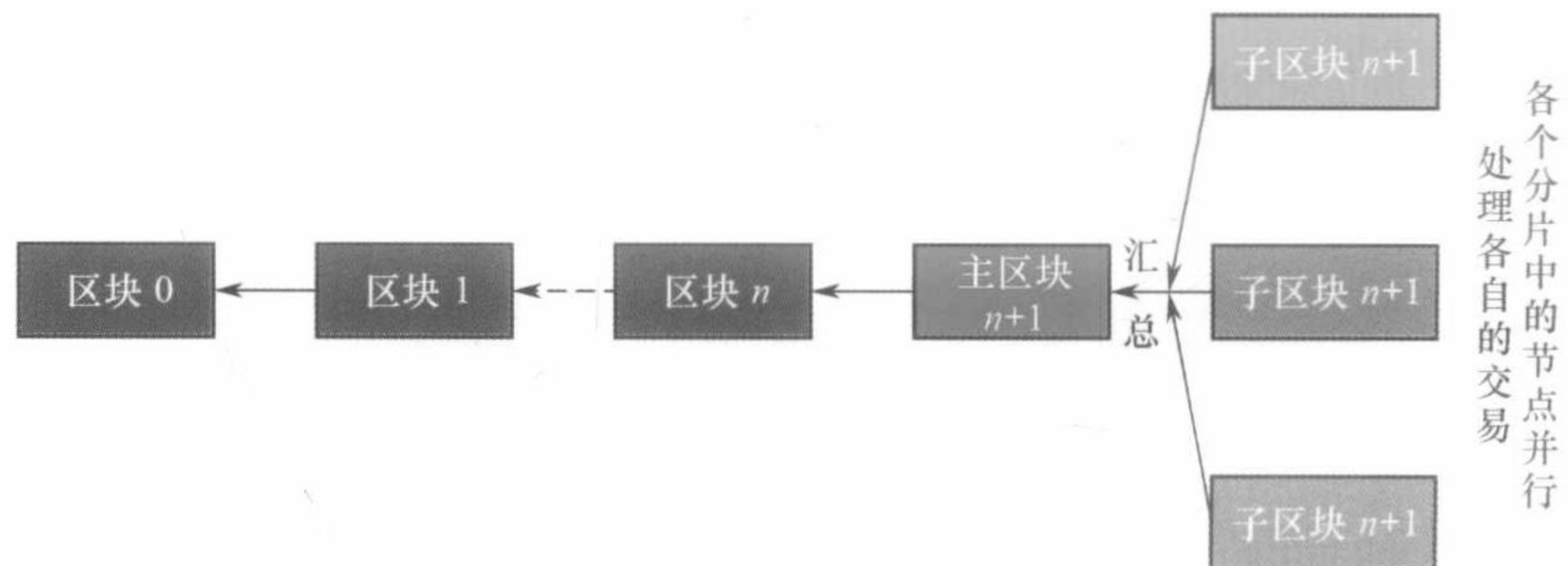


图 3-58 Zilliqa 分片网络处理交易过程示意图

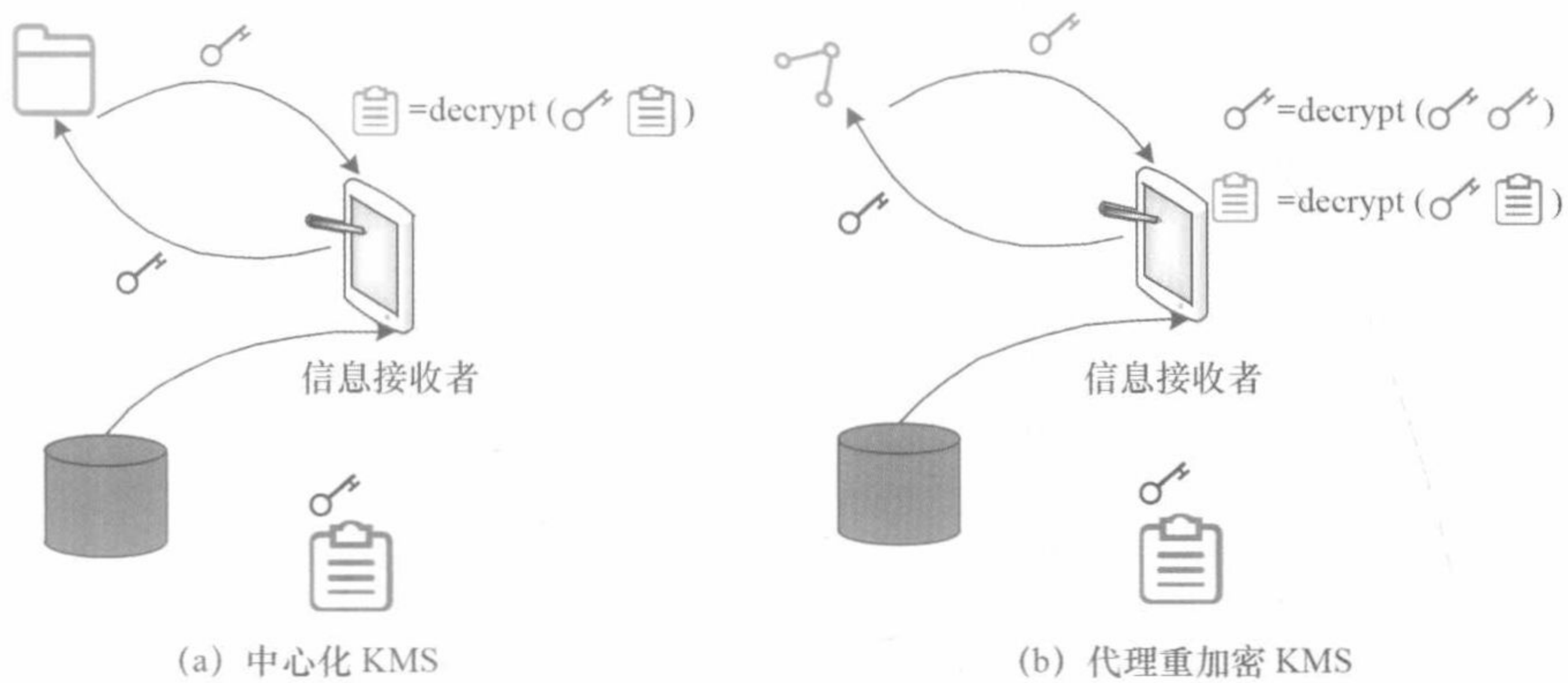


图 3-69 中心化密钥管理系统 (KMS) 与代理重加密 (PRE) 密钥管理系统的区别

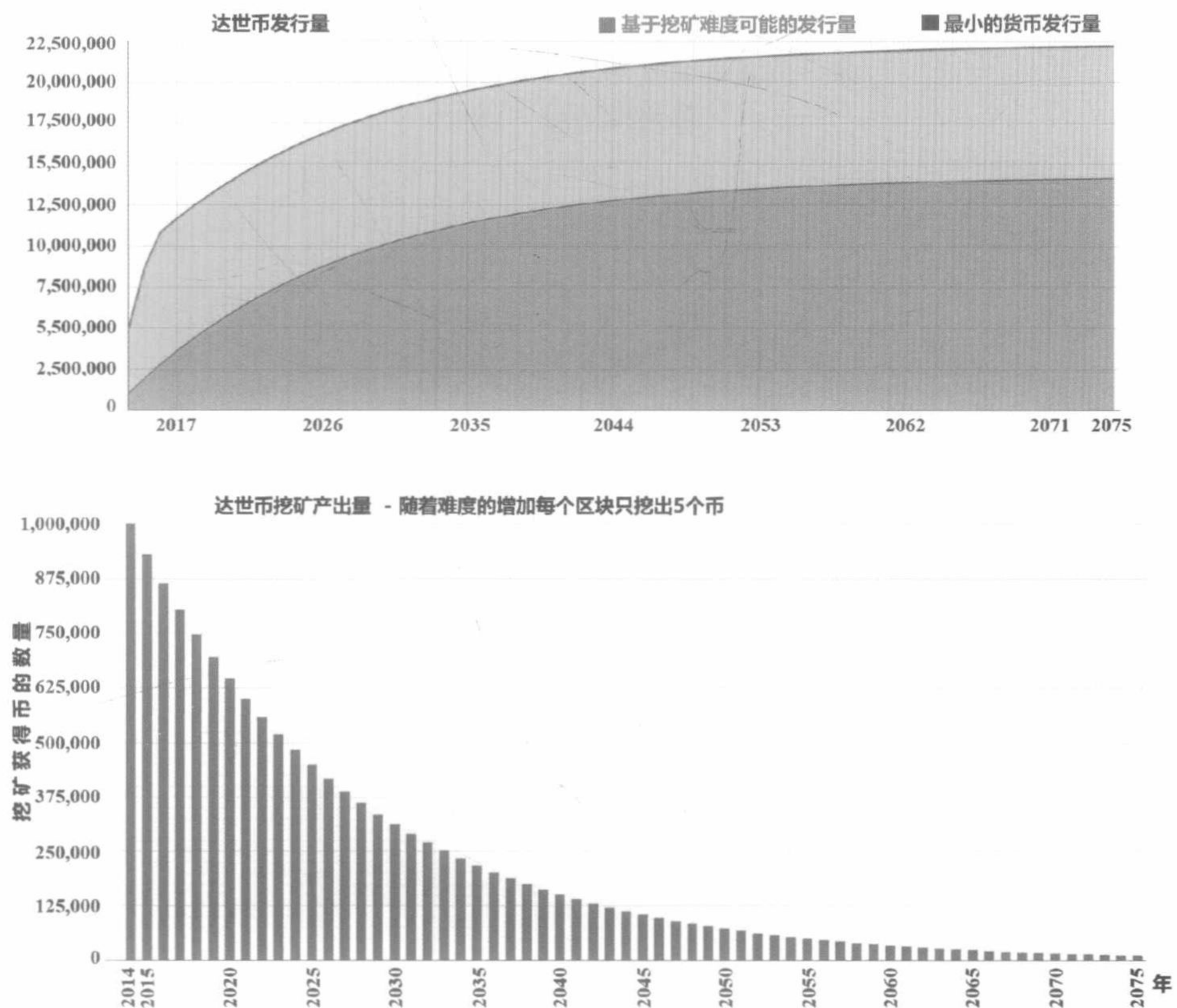


图 3-73 DASH 挖矿奖励模型

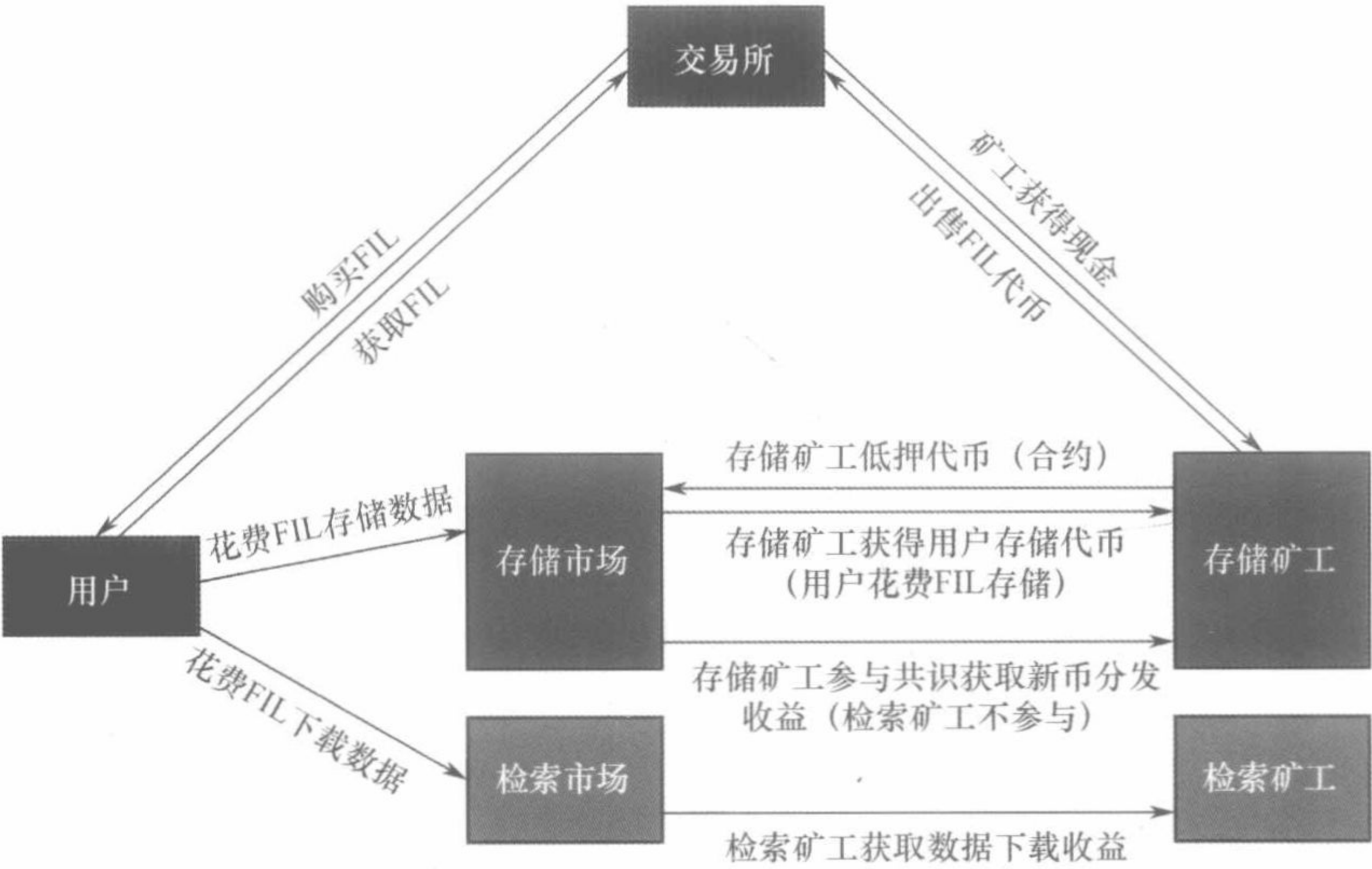


图 3-74 Filecoin 体系中价值与代币转移图示



图 3-75 Filecoin 发展路线图

推荐序 1

区块链是分布式数据存储、多中心点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。区块链技术的第一时段始于 2009 年，代表性应用就是比特币，主要解决了支付手段的去中心化。区块链技术的第二时段始于 2013 年，核心技术是以以太坊为标志的智能合约，着眼于应用的去中心化。区块链技术目前处于第三时段——联盟区块链的阶段，其共识过程由多家机构节点共同参与，具有更高的可扩展性，并且接纳监管。

我国“十三五规划”将区块链与量子通信、人工智能等技术同列为“重大任务和重点工程”。2018 年 5 月，习近平总书记在“两院院士大会”¹上的讲话指出，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。在政策、技术、市场的多重推动下，区块链技术正在加速与实体经济融合，助力高质量发展。

作为新兴信息技术之一，区块链也面临着技术发展参差不齐、框架缺乏标准等多重挑战，期待本书的出版能为区块链技术的普及添砖加瓦，也希望全球区块链技术研究和产业应用给数字经济带来新的发展。

中国工程院院士 陈纯

2019 年 7 月于杭州

1 指中国科学院第十九次院士大会、中国工程院第十四次院士大会。

推荐序 2

区块链技术对电信运营商来说，既是机遇，也是挑战。区块链的去中心化、防篡改以及多方共识等技术特性，决定了其在解决电信行业合作中需要多方共同决策并建立互信机制、优化运营商之间及与上下游产业链的合作协同等方面具有重要的价值。电信运营商可以利用自身在网络资源和终端资源上的优势，布局区块链新型生产模式，对内提升传统业务效能，对外促进客户价值提供。

国内外主流运营商已开展区块链相关业务，包括美国 AT&T 构建区块链行业解决方案套件，西班牙电信 Telefonica 使用区块链技术跟踪并记录国际呼叫，韩国电信 SK Telecom 推出基于区块链的客户身份认证平台，中国移动在基于区块链的 PKI 安全基础设施、国际漫游清结算方面进行了应用示范等。

区块链是中国电信的重点工作领域之一。中国电信集团正在加快区块链的技术储备、产品创新和产业布局。梁伟博士作为中国电信区块链重点研发课题的负责人，正在带领团队积极探索区块链等新兴信息技术在电信行业的特色应用场景，目前已在区块链底层基础设施，区块链加密 SIM 卡，基于区块链的电子招投标、数字资产管理、农业溯源等方面进行了初步实践。这本书是他们在该领域深入研究的结晶。期望这本书能帮助读者建立区块链技术知识体系，并为相关工作与实践提供参考。

中国电信研究院院长 何志强

2019 年 7 月

推荐序 3

我们不仅生活在一个自然世界中，也生活在一个技术世界中，尤其是当下数字技术革命时代，移动互联网、云计算、大数据、人工智能、区块链等技术突飞猛进，也让我们所处的技术世界加速变化。然而区块链与云计算、大数据、人工智能不同，它是一种“草根式”的重大技术创新。云计算需要海量的服务器，才可能产生资源利用的规模效应；大数据则需要海量的“非结构化”数据，才可能发现新的价值；人工智能不仅需要海量的并行计算能力，还经常需要训练海量的数据后，才能习得新智能。

区块链创新技术的特点是分布式，而且从边缘市场开始。“草根式”创新的另一个代表是互联网，它就是从当时很小众的计算机网络开始，分布式地连接每台计算机和网络，低调、大气、不奢华，从而在监管机构和电信机构的“眼皮”底下取得成功。所以，“草根式”创新在一些不起眼的地方“搞事情”，且以分布式合作的方式，取得了颠覆性成功。但区块链和互联网也有不同，互联网的设计初衷是计算机通信，用来传递数字信息；区块链致力于为价值传递制造信任，为大规模社会化协作提供新的技术与商业范式。

另外，区块链只是信息技术的一个“区块”，必须与其他技术和场景“链”起来，才可能占据一个生态位。产业界也在不断地实践，区块链技术正在与物联网、人工智能、5G 通信等技术融合，共同解决数字经济和实体经济中的问题。

我和梁伟博士是中科院计算所的校友，很高兴能为梁博士的新书作序，也希望该书的出版能帮助读者增长见识、拓展视野。

中国信通院云计算与大数据研究所所长 何宝宏

2019 年 7 月于北京

推荐序 4

数字社会的核心在于数据规管能力。从国际数据法律法规的构建与修改的发展趋势看，数据的所有权，以及数据使用的人权、事权、物权正在快速地进行法律界定。以拥有数据为目标，以集中数据为手段的“数据圈地”模式很快会出现法律和规模的双重瓶颈。

区块链技术有利于实现可信数据交换，释放数据价值。区块链开启了一个时代，一个真正的信用时代，通过所有智能设备的记账实现多方共识，通过智能合约由数据提供方和使用方共同约定数据共享的规则，无须中间过程，即可进行不可抵赖、不可篡改的数据交换、协同处理。

我们和梁博士的团队在政务服务、智能医疗等方面进行了广泛而卓有成效的合作，综合运用区块链、大数据、人工智能、加密算法、协同计算等技术，为数字经济的产业赋能提供解决方案。我很高兴能为梁博士的新书作序，希望该书的出版能为我国数字经济的发展添砖加瓦。

中组部“千人计划”青年学者，北京航空航天大学教授 朱晔罡

2019年7月于北京

推荐序 5

我因录制北京电视台定期播出的《解码区块链》电视栏目与梁博士相识，彼此有点相见恨晚的感觉。梁博士是我在众多投资调研项目过程中见过的为数不多的对区块链从理论到实践都有较多积累的人，更难得的是，他带领的团队在区块链与电信运营商领域深度融合做出了用户友好的创新产品和解决方案。因为我们有着共同的创新观念，因为我们温暖彼此，让我们在创业路上不孤单。所以，当接到邀请为这本书作序的时候，我更是感觉义不容辞，更当鼎力支持。

从大学时代的互联网创业开始，到移动互联网时代某卫视频道歌曲选秀官方App的200万+用户，再到区块链时代，我亲自参与了这三个阶段的创新创业投资。尤其是在2013年开始对互联网金融的研究实践，在清华大学五道口金融学院担任互联网金融专题班的辅导员时，我深刻体会到互联网对金融在线化、份额化、风控的改变。从权属确认到资产定价等互联网没有做到的，区块链这部“信任机器”做到了，并且智能合约提供的资产的可编程性将在包括金融在内的多领域激发出千姿百态的创新形式。

随着区块链技术广泛应用于银行、保险、通信、教育、版权、供应链管理、娱乐、智能制造、社会公益、政府管理等经济社会领域，它将优化各行业的业务流程、降低运营成本、提升协同效率，为经济社会转型升级提供系统化的支撑。

区块链投资需要关注长期价值，除了要研究清楚项目解决什么问题、这个问题是否真实存在、区块链在这个领域的独特价值，还要看项目的赛道方向、自身技术、经济模型、市场营销和团队积累等。本书遴选了一些成功的区块链项目，并从多维度进行了分类介绍，有利于读者开拓产业视野，提高投资认知。

链石资本创始合伙人 薄胜

2019年7月

推荐序 6

这是一个正在加速数字化的世界，在这个几乎无盲区的全社会数字化进程中，IoT、5G 和 AI 技术正在数据的自动化采集、传输和处理领域解决各自的问题，而我们也面临一个新的课题，即面对加速增长的海量数据，是否可能基于数据本身而不是基于预设的信任关系来建立协作？区块链技术会是一种新的免信任的分布式协作的利器吗？

自 2009 年 1 月 3 日比特币诞生，区块链已迈过了 10 个年头。回头重新审视区块链的发展历程，分析其核心技术体系，回顾国内外的亮点项目，对我们更深刻地理解区块链技术内涵大有裨益。当然，总体而言，区块链作为一项颠覆性的新技术，仍处于发展的初期阶段，面向未来，我们更需要以开放的心态来接受区块链技术自身的进化。不忘记初心，不拘于成见，即使有一天，区块链变得既非“区块”，也无“链”，也无损它的重要价值。

与梁伟博士的结识源于中国计算机学会区块链专业委员会，他的专注、热情和踏实都深深地感染了我。很高兴看到国内的区块链领域有像梁伟博士这样务实的专业人士一直埋头耕耘在技术的百草园，耐得住寂寞，沉得下心，采来百花酿出蜜。

是为序。

中钞区块链技术研究院院长 张一锋

2019 年 7 月于杭州