HZ BOOKS
华章IT

作者是中国企业以太坊联盟联合发起人和核心成员，是国内区块链和以太坊技术的早期布道者

从设计理念、技术架构、共识算法、智能合约、以太坊虚拟机、开发工具、DApp开发、企业以太坊解决方案、跨链技术等9个维度系统、深入讲解以太坊

区块链技术丛书

DIVE INTO ETHEREUM

深入理解以太坊

王欣 史钦锋 程杰 ◎著

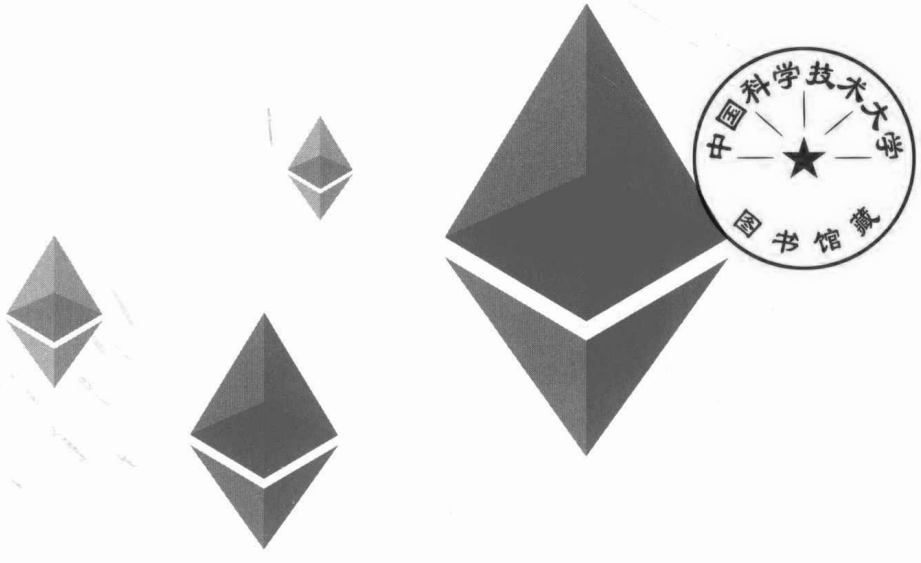
机械工业出版社
China Machine Press

区块链
技术丛书

DIVE INTO ETHEREUM

深入理解以太坊

王欣 史钦锋 程杰◎著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

深入理解以太坊 / 王欣，史钦锋，程杰著 . —北京：机械工业出版社，2019.1
（区块链技术丛书）

ISBN 978-7-111-61492-0

I. 深… II. ①王… ②史… ③程… 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（2018）第 277694 号

深入理解以太坊

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：李 艺 责任校对：殷 虹
印 刷：北京诚信伟业印刷有限公司 版 次：2019 年 6 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：17.25
书 号：ISBN 978-7-111-61492-0 定 价：89.00 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 读者信箱：hzit@hzbook.com

Preface 前　言

2017 年年初，IBM 宣布在德国慕尼黑设立物联网事业部，旨在通过 Watson 物联网技术，从内嵌在机器、汽车、无人驾驶飞机、滚珠轴承、设备部件甚至医院中的数十亿传感器中获取实时数据，围绕区块链、安全，构建全新的物联网。

身处物联网行业，我隐约感觉到区块链将会成为新的研究方向，为传统行业带来新的助力。随后，我查阅了大量的相关资料，以尽可能多地了解区块链。一个偶然的机会，我结识了南京一家区块链初创公司的技术负责人，并受邀加入他们的团队，开始全身心地投入区块链行业。

起初，我的工作围绕以太坊开源项目展开，从白皮书、黄皮书、源码、工具到共识算法、智能合约、雷电网络、零知识证明，无所不含。短短几个月的时间，我所学习的新知识比过去几年加起来还要多。没过几个月，本书的另外两位作者史钦锋和程杰也加入团队，并成立了以太坊技术研究小组。在大家的共同努力之下，我们从理论到实践，完整地总结出一套借助以太坊技术实现区块链应用落地的技术方案。

一路走来，我们深深感受到区块链理论涉及的概念之多，技术涉及的门类之广，对于一个初学者来说实属不易。另外一方面，一些不法分子以区块链技术创新之名，行招摇撞骗、掳掠钱财之实。作为相关从业人员，我们有能力，也有必要尽自己的微薄之力，将所学、所思、所感、所得用文字记录下来，以帮助广大读者客观理性地认识这个新事物。如若读者能就其中一两点产生共鸣，激发创新、创造的热情，那实在是意外的收获。

本书内容仅仅针对以太坊开源项目。回想笔者的工作经历，虽然也接触过其他项目，但总体比较来看，以太坊是比较适合初学者入门的技术栈。因为以太坊技术社区在全球范围较为完善，参考资料多；以太坊核心团队也很具备极客精神，开发速度快；以太坊主网上线运行时间长，经历了严苛的安全性检验；以太坊的目标远大，它要成为世界的计算机。

本书的主线由粗到细，由近及远。全书不仅归纳总结了以太坊项目的整体现状和核心技

术，也对未来的发展和技术走向做了总体的预测和分析。全书各章节主要内容具体如下。

第 1 章　从比特币说起，介绍了以太坊项目的起源，并对项目的整体情况做了概述。

第 2 章　从理论入手，介绍了以太坊知识体系的诸多概念，比如密码学、共识和图灵完备特性。

第 3 章　从架构入手，介绍了以太坊设计的整体思路、模块划分以及核心功能实现。

第 4 章　讨论共识，共识是区块链最核心的问题，共识的设计也是区块链的难点所在。从 PoW 到 PoA，再到 PoS，我们比较了各种共识算法的优缺点，也分析了不同算法的适用场景。

第 5 ～ 7 章　围绕智能合约展开讨论。智能合约是以太坊的最大创新点，其将区块链变成了可以服务于任何行业、任何场景的可编程平台。从开发步骤、技术原理到底层实现，这三章覆盖了智能合约软件支持的方方面面。对于偏向区块链技术应用的开发者，我们建议将学习重点放在第 5 章；对于偏向底层区块链协议的开发者，相信第 6 章和第 7 章会带给你不少收获。

第 8 章　指导读者熟练掌握以太坊周边的工具，在不开发代码的情况下，完成与以太坊网络的交互。

第 9 章　介绍了以太坊技术的企业级应用以及企业以太坊联盟的标准化进展。

第 10 章　对跨链方案进行了探讨。由于目前跨链技术还没有达到成熟的阶段，本章仅对大体的技术方向做了介绍。跨链也被视为后以太坊时代的区块链技术热点，将引领区块链 3.0 时代的到来。

第 11 章　分析了以太坊现阶段面临的发展瓶颈，并对可能的解决方案进行了展望。

本书内容包罗万象，具体包括项目概述、架构设计、实现细节和开发方法，适合对区块链理论和实现感兴趣的读者阅读，也适合作为技术手册，供读者遇到具体问题时查阅参考。由于区块链技术发展迅速，笔者水平有限，书中难免存在错误或不当之处，希望得到广大读者批评指正。后续，笔者将通过线上专栏或技术社区的方式，与读者保持沟通，并针对感兴趣的话题进行讨论。

感谢带领笔者进入区块链行业的技术大咖 Denny，感谢曾经一起工作的同事，也感谢为本书出版费尽心血的华章的各位老师。本书的编写占用了笔者陪伴家人的很多时间，但笔者得到了家人充分的鼓励与支持，在此深深地感谢他们。

王欣

Contents 目　录

第 1 章 Chapter 1

以太坊概述

本章将主要概述以太坊技术的历史背景、发展过程和技术特性。1.1 节从比特币的起源引入区块链的概念及其商业价值；1.2 节描述了以太坊项目的历史发展过程；1.3 节重点分析了以太坊的核心技术——智能合约和 PoS 共识算法；1.4 节对以太坊的架构进行了总体概述；1.5 节介绍了以太坊社区的协作方式；1.6 节回顾了以太坊的路线图并介绍了现阶段的发展目标；最后是本章小结。

1.1 区块链起源

2008 年，通货膨胀造成的经济危机在全球范围爆发。当人们还在为货币的未来感到担忧时，一位名叫“中本聪”（Satoshi Nakamoto）的人悄无声息发表的一篇名为《比特币：一种点对点的电子现金系统》的论文引起了金融界的广泛关注。文中提出了一种点对点的数字货币，该货币可以独立存在于任何国家、任何机构之外，不受第三方机构管束，且因其数字算法的特殊性，很难被不法分子伪造，这就是后来为人们所熟知的“比特币”。

中本聪的论文中首次出现了区块链（Blockchain）的概念，并给出通过时间戳和工作量证明（Proof of Work）共识机制解决双花（Double Spending）和拜占庭将军问题的设计思路，即保证同一笔比特币不会同时出现于两个地址，与此同时，所有节点都可以让其他节点接收到自己的真实意图，以保持行动一致。2009 年，理论变成了现实，比特币网络成功创建，“创世区块”也由此正式诞生。

为了避免出现双花问题，一笔交易的接收人必须要能够证明在当前交易发生之前，交易发起人并没有将同一笔交易发给另外一个人，这就要求接收人知道交易发起人的所有交

易记录。因此，在区块链上所有交易必须公开，并且这些交易数据必须被网络证明是真实有效的。

区块链中每个包含时间戳的交易数据块被计算出 Hash 值，同时将该 Hash 值存入下一包含时间戳的交易数据块中，如此反复，生成链式数据结构（如图 1-1 所示）。这样，一旦下一个区块确认生成，之前所有的区块信息（包括交易的内容和交易顺序）就都不可修改了，否则将导致 hash 验证失败。区块生成，也就是我们通常所说的记账，在比特币网络中是通过工作量证明来保证的。当网络中多个节点同时生成最新区块时，长度最长的链会作为选择结果，因为最长的链代表投入算力最多，最能代表大多数节点的意志。所以多个最新区块的信息将被保留一段时间，直到判断出哪一条链更长。

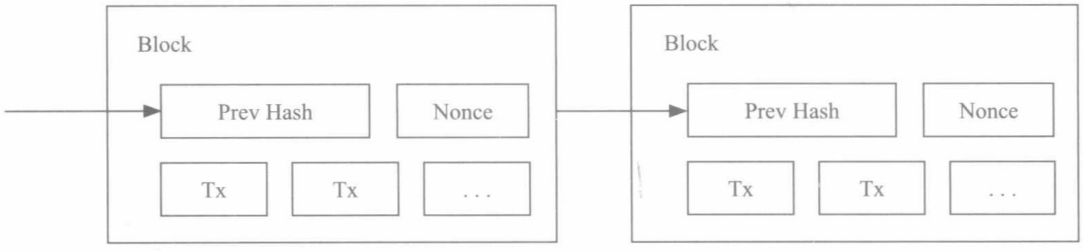


图 1-1 区块链的哈希链式结构

一个节点必须拥有网络中 51% 以上的算力才有能力篡改一个区块并重新生成后面所有的区块，它还需要保证后面区块产生的速度比其他节点更快。在庞大的比特币网络中，能拥有如此惊人的算力几乎是不可能的。

比特币系统设计得非常精妙：没有中心化的管理方，数据很难被篡改，抗攻击能力强。回看历史，在比特币诞生之前，人们在这一领域不断探索，其中许多学术贡献也为比特币的成型铺平了道路。

- 比特币实现的基于零信任基础且真正去中心化的分布式系统，其实是为了解决 30 多年前由 Leslie Lamport 等人提出的拜占庭将军问题，即将军中各地军队彼此取得共识，决定是否出兵的过程延伸至运算领域，设法建立具有容错特性的分布式系统，即使部分节点失效仍可确保基于零信任基础的节点达成共识，实现信息传递的一致性。
- 工作量证明机制则是采用由 Adam Back 在 1997 年所发明的 Hashcash 算法，此算法依赖成本函数的不可逆特性，实现容易被验证但很难被破解的特性，该算法最早应用于过滤垃圾邮件。
- 隐私安全技术可回溯到 1982 年 David Chaum 提出的注重隐私的密码学网路支付系统，之后 David Chaum 在 1990 年基于这个理论打造出不可追踪的 eCash 中心化网络。
- 交易加密采用的椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm，ECDSA），可追溯回 1985 年 Neal Koblitz 和 Victor Miller 提出的椭圆曲线密码学（Elliptic curve cryptography，ECC）及加密算法。相较于 RSA，采用 ECC 算法的好

处在于可以使用较短的密钥达到相同的安全强度。到了 1992 年，Scott Vanstone 等人提出了 ECDSA。

- 最后，再来看共识机制。1990 年，Leslie Lamport 提出了具有高容错特性的数据一致性算法 Paxos。1991 年，Stuart Haber 与 W. Scott Stornetta 提出了用时间戳保证数字文件安全的协议。1998 年，Wei Dai 发表匿名的分散式电子现金系统 B-money，引入了工作量证明机制，强调点对点交易和不可篡改特性。然而 B-money 中并未采用 Adam Back 提出的 Hashcash 算法。同年，Nick Szabo 发表了去中心化的数字货币系统 Bit Gold，参与者可贡献算力。到了 2005 年，Hal Finney 提出了可重复使用的工作量证明机制（Reusable Proofs of Work，RPoW），结合 B-money 与 Adam Back 提出的 Hashcash 算法来创造数字货币。

综上所述，区块链是用分布式数据库识别、传播和记载信息的智能化对等网络，其包含以下几个主要特性。

- 分布式去中心化：区块链中每个节点和矿工都必须遵循同一记账交易规则，而这个规则是基于密码算法而不是信用的，同时每笔交易都需要网络内其他用户的批准，所以不需要一套第三方中介机构或信任机构背书。
- 无须信任系统：区块链网络通过算法的自我约束，使欺骗系统的任何恶意行为都会遭到其他节点的排斥和抑制。参与人不需要信任任何人，随着参与节点的增加，系统的安全性也会得到增加，同时数据内容可以做到完全公开。
- 不可篡改和加密安全性：区块链采取单向哈希算法，同时每个新产生的区块都将严格按照时间线形顺序推进，时间的不可逆性将导致任何试图入侵篡改区块链内数据信息的行为都很容易被追溯，因此会被其他节点排斥，从而限制相关的不法行为。

区块链最重要的是解决了中介信用问题。在过去，两个互不认识的人要达成协作是很难的，必须要依靠第三方。比如支付行为，过去任何一次转账行为，都必须要有银行或者支付宝这样的机构存在。但是通过区块链技术，通过比特币，人类第一次实现了在没有任何中介机构参与的情况下，完成双方可以互信的转账行为。这是区块链的重大突破。

并非所有的区块链项目都会采用类似于比特币这样的“工作量证明”方式，其更多地出现在早期的区块链项目中。如果采取其他证明机制，如“权益证明”（Proof of Stake，PoS）“股份授权证明机制”（Delegate Proof of Stake，DPoS），则不需要采取这样的挖矿方式。

区块链是比特币的底层技术，但其应用的真实价值远远超过电子货币系统。我们认为比特币是区块链 1.0 系统，当通过智能合约（Smart Contract）实现货币以外的区块链应用时，即进入了区块链 2.0 系统。

1.2　以太坊发展之路

比特币是第一个可靠的去中心化解决方案。随后，人们的注意力开始迅速转向如何将

比特币底层的区块链技术应用于货币以外的领域。以太坊就是这样一个开放的区块链平台。它与比特币一样，是由遍布全球的开发者合作构建的开源项目，其不依赖于任何中心化的公司或组织。但与比特币不同的是，以太坊更加灵活，可以为开发者带来更方便、更安全的区块链应用开发体验。

2013 年年底，以太坊的创始人 Vitalik Buterin 提出了让区块链本身具备可编程能力来实现任意复杂商业逻辑运算的想法，并随后发布了以太坊白皮书。白皮书中描述了包括协议栈和智能合约架构等内容的具体技术方案。2014 年 1 月，在美国迈阿密召开的北美比特币大会上，Vitalik 正式向外界宣布以太坊项目的成立。同年，Vitalik Buterin 联合 Gavin Wood 和 Jeffery Wilcke 开始开发通用的、无须信任的下一代智能合约平台。2014 年 4 月，Gavin 发表了以太坊黄皮书，明确定义了以太坊虚拟机（EVM）的实现规范。随后，该技术规范由 7 种编程语言（C++、Go、Python、Java、JavaScript、Haskell 和 Rust）实现，获得了完善的开源社区支持。

在软件开发之外，发布一个新的数字货币及其底层区块链需要协调大量的资源，包括建立由开发者、矿工、投资人和其他干系人组成的生态圈。2014 年 6 月，以太坊发布了以太币的预售计划，预售的资金由位于瑞士楚格的以太坊基金会经营管理。从 2014 年 7 月开始，以太坊进行了为期 42 天的公开代币预售，总共售出 60,102,216 个以太币，接收到比特币 31,591 个，折合市场价值 18,439,086 美元。该笔资金一部分用于支付项目前期法务咨询和开发代码的费用，其他部分则用于维持项目后续的开发。根据 CoinTelegraph 的报道，以太坊作为最成功的众筹项目之一，将会被载入史册。

在以太坊成功预售之后，开发工作由一个名为 ETH DEV 的非盈利组织进行管理，Vitalik Buterin、Gavin Wood 和 Jeffery Wilcke 出任总监职务。ETH DEV 团队的工作非常出色，频繁向开发社区提交技术原型（Proof-of-Concept）以用于功能评估，同时在讨论版发表了大量的技术文章介绍以太坊的核心思想。这些举措吸引了大量用户，同时也推动了项目自身的快速发展，为整个区块链领域带来了巨大的影响。时至今日，以太坊的社区影响力也丝毫没有减弱的趋势。

2014 年 11 月，ETHDEV 组织了 DEVCON-0 开发者大会。全世界以太坊社区的开发者聚集在德国柏林，对各种技术问题进行了广泛讨论。其中一些主要的对话和演示为后续的以太坊技术路线奠定了坚实的基础。

2015 年 4 月，DEVgrants 项目宣布成立。该项目为以太坊平台以及基于平台的应用项目开发提供了资金支持。几百名为以太坊做出贡献的开发者获得了相应的奖励。直到今天，这个组织还在发挥作用。

经历了 2014 年和 2015 年两年的开发，第 9 代技术原型测试网络 Olympic 开始公测。为鼓励社区参与，以太坊核心团队对于拥有丰富测试记录或成功侵入系统的开发者安排了重金奖励。与此同时，团队也邀请了多家第三方安全公司对协议的核心组件（以太坊虚拟机、网络和 PoW 共识）进行了代码审计。正因如此，以太坊的协议栈正在不断完善，各方

面的功能也变得更加安全、可靠。

2015 年 7 月 30 日，以太坊 Frontier 网络发布。开发者们开始在 Frontier 网络上开发去中心化应用，矿工开始加入网络进行挖矿。矿工一方面通过挖矿得到代币奖励，另一方面也提升了整网的算力，降低了被黑客攻击的风险。Frontier 是以太坊发展过程中的第一个里程碑，虽然它在开发者心目中的定位是 beta 版本，但在稳定性和性能方面的表现其远远超出了任何人的期望，从而吸引了更多的开发者加入构建以太坊生态的行列。

2015 年 11 月，DEVCON-1 开发者大会在英国伦敦举行，在为期 5 天的会议内举办了 100 多项专题演示、圆桌会议和总结发言，共吸引了 400 多名参与者，其中包含开发者、学者、企业家和公司高管。具有代表性的是，包含 UBS、IBM 和微软在内的大公司也莅临现场并对项目展示了浓厚的兴趣。微软还正式宣布将在其 Azure 云平台上提供以太坊 BaaS 服务。通过这次盛会，以太坊真正让区块链技术成为整个行业的主流，同时也牢牢树立了其在区块链技术社区的中心地位。

2016 年 3 月 14 日（π 日），以太坊平台的第二个主要版本 Homestead 对外发布，其同时也是以太坊发布的第一个正式版本。它包括几处协议变更和网络设计变更，使网络进一步升级成为可能。Homestead 在区块高度达到 1,150,000 时，系统会自动完成升级。Homestead 引入了 EIP-2、EIP-7 和 EIP-8 在内的几项后向不兼容改进，所以其是以太坊的一次硬分叉。所有以太坊节点均需提前完成版本升级，从而与主链的数据保持同步。

2016 年 6 月 16 日，DEVCON-2 开发者大会在中国上海举行，会议的主题聚焦在智能合约和网络安全上。然而，出乎所有人意料之外的是，在会议的第二天发生了区块链历史上最严重的攻击事件。The DAO 项目编写的智能合约由于存在重大缺陷而遭受黑客攻击，导致 360 万以太币资产被盗。最终通过社区投票决定在区块高度达到 1,920,000 时实施硬分叉，分叉后 The DAO 合约里的所有资金均被退回到众筹参与人的账户。众筹人只要调用 withdraw 方法，即可用 DAO 币换回以太币。The DAO 是人类尝试完全自治组织的一次艰难试验，因为在技术上存在缺陷，理念上和现行的政治、经济、道德、法律等体系不能完全匹配，最终以失败告终。The DAO 也为我们提供了很多可借鉴的经验，例如智能合约漏洞的处理，代码自治和人类监管之间的平衡等。

The DAO 事件之后，以太坊的技术体系更加趋于完善。2017 年年初，摩根大通、芝加哥交易所集团、纽约梅隆银行、汤森路透、微软、英特尔、埃森哲等 20 多家全球顶尖金融机构和科技公司成立企业以太坊联盟。2017 年 9 月 18 日，以太坊开发团队开始测试“大都会”（Metropolis）版本的第一阶段：拜占庭分叉。2017 年 10 月 16 日，主网在 4,370,000 区块高度成功完成拜占庭分叉。此次硬分叉将为智能合约的开发者提供灵活的参数；同时，为后期大都会升级引入 zkSnarks 零知识证明等技术做了准备；延迟引爆难度炸弹，将冰河期推迟 1 年；也使挖矿难度显著降低，从而明显提高了以太坊平台的交易速度，使对应的矿工们挖矿的收益从每区块 5 个以太币降低到 3 个。而大都会版本的第二阶段——君士坦丁堡硬分叉也已经在 2019 年 3 月顺利完成。

2017 年 11 月 1 日，DEVCON-3 开发者大会在墨西哥海边小城坎昆召开，历时 4 天。参会人数爆增到 1800 人，是 DEVCON-2 的两倍。大会上 Vitalik Buterin 对 PoS 共识和分片的开发现状做了介绍。其余参会者的主题演讲也十分精彩，共达 128 场之多，覆盖 PoS 共识、形式化证明、智能合约、zkSNARKs 零知识证明、Whisper 和 Swarm 组件、数字钱包、DApp 等重要技术方向。

以太坊规划的最终版本为 Serenity。在此阶段，以太坊将彻底从 PoW 转换到 PoS（权益证明）。这似乎是一个长期过程，但并不是那么遥远。PoW 是对计算能力的严重浪费。从 PoW 的约束中解脱出来，网络将更加快速，对新用户来说更加易用，更能抵制挖矿的中心化等。这将与智能合约对区块链的意义一样巨大。转换到 PoS 以后，之前的挖矿需求将被终止，新发行的以太币数量也会大大降低，甚至不再增发新币。

1.3 以太坊核心技术

1.3.1 智能合约

以太坊是可编程的区块链。它并不是为用户提供一系列预先设定好的操作（例如，比特币交易），而是允许用户按照自己的意愿创建复杂的操作。这样一来，以太坊就可以作为通用去中心化区块链平台。20 世纪 90 年代，Nick Szabo 首次提出了智能合约的理念。由于缺少可信的执行环境，智能合约并没有被应用到实际产业之中。自比特币诞生后，人们认识到比特币的底层技术区块链天生可以为智能合约提供可信的执行环境。以太坊首先看到了区块链和智能合约的契合，并致力于成为智能合约的最佳运行平台。

从技术方面来看，以太坊利用图灵完备的虚拟机（EVM）实现对任意复杂代码逻辑（即智能合约）的解析。开发者能够使用类似 JavaScript（Solidity）或 Python（Serpent）的语法创建出可以在以太坊虚拟机上运行的应用。结合点对点网络，每个以太坊节点都运行着虚拟机并执行相同的指令。因此，人们有时也形象地称以太坊为“世界电脑”。这个贯穿整个以太坊网络的大规模并行运算并没有使运算更高效，而是使在以太坊上的运算比在传统“电脑”上更慢更昂贵。然而，这种架构可以带给以太坊极强的容错性，保证区块链上的数据一致、不可篡改。

从应用方面来看，智能合约是一种用计算机语言取代法律语言去记录条款的合约。如果区块链是一个数据库，那么智能合约就是能够使区块链技术应用到现实当中的应用层。传统意义上的合同一般与执行合同内容的计算机代码没有直接联系。纸质合同在大多数情况下是被存档的，而软件会执行用计算机代码形式编写的合同条款。智能合约的潜在好处包括：降低合约签订、执行和监管方面的成本；相比其他合约，智能合约可以极大地降低人力成本。

图 1-2 就是一个智能合约模型：一段代码被部署在分布式共享账本上，它可以维持自己

的状态，控制自己的资产和对接收到的外界信息或者资产进行回应。

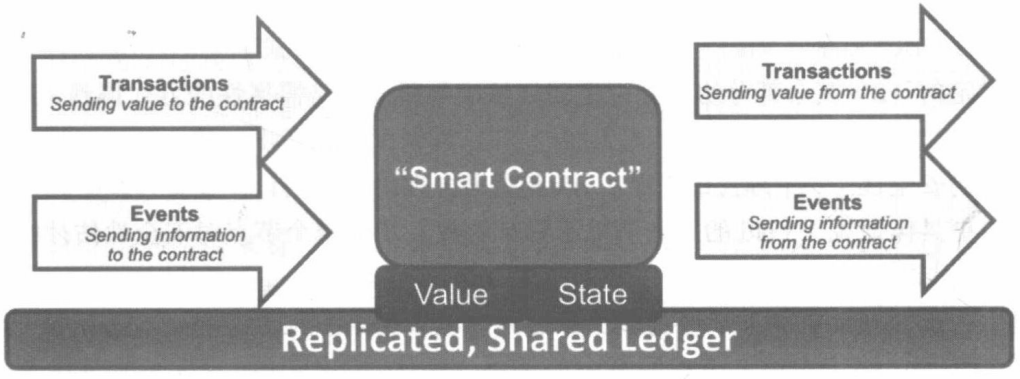


图 1-2　智能合约模型示意

1.3.2　PoS

以太坊另一个重要的核心技术就是共识算法的改进。比特币在区块生成过程中使用了工作量证明（Proof of Work）共识机制，一个符合要求的区块 Hash 由 N 个前导零构成，零的个数取决于网络的难度值。要得到合理的区块 Hash 需要经过大量的枚举计算，计算时间取决于机器的 Hash 运算速度。在股权证明（Proof of Stake）共识中，验证人轮流提议新块并对下一个块投票，每个验证人的投票权重取决于其持币量的大小（即股权）。验证人为区块链网络提供出块服务，网络也会对验证人返回奖励，而且这种奖励也实现了对攻击者的经济制约。

PoS 的明确优点包括安全性、降低集权风险和提高能源效率。PoS 可以灵活地、明确地设计对拜占庭行为（即不遵循协议）进行的惩罚。这使得协议设计者能够对网络中各种行为的不对称风险和收益回报情况进行更多的控制。提高安全性的另一个方面是增加网络攻击的成本，因此具有明确惩罚（可能在比 PoW 更严重的级别上）的能力可以增加网络的安全性（即经济安全）。在 PoS 的情况下，一美元就是一美元。这样的好处是，你不能通过汇集在一起，使得一美元的价值变得更多。你也不能开发或购买专用集成电路（ASIC），从而在技术上占有优势。所以，PoS 不同于 PoW 挖矿收入的累计分配方式，采用了比例分配（成熟的去中心化的身份管理服务使得按比例分配收益成为可能）。

以太坊要实现的 PoS 机制被命名为 Capser（名字源于 20 世纪 90 年代的一部电影《鬼马小精灵》），它实际上是由以太坊团队正在积极研究的两个主要项目组成，即 Casper FFG 和 Casper CBC。虽然是独立的两套实现，但它们有着一样的目标：将以太坊的工作量证明转到 PoS。

友好的终结工具 Casper FFG 又名“ Vitalik's Casper”，是一种混合 PoW / PoS 的共识机制，它是以太坊首个通向 PoS 的候选方法。更具体地说，FFG 在工作量证明（如以太坊的 Ethash PoW 链）的基础上，实施了权益证明。简单地说，区块链将用熟悉的 Ethash PoW