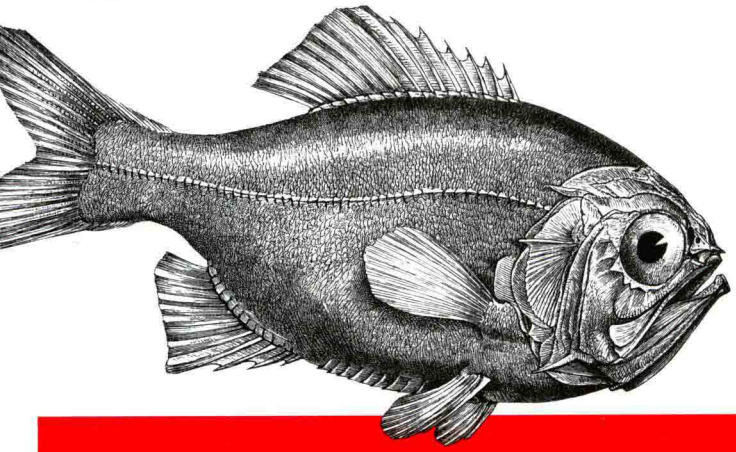
O'REILLY®

TURING 图灵程序设计丛书



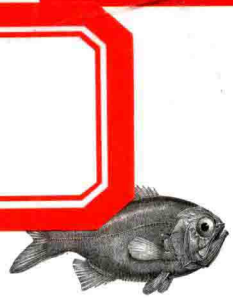
去中心化应用

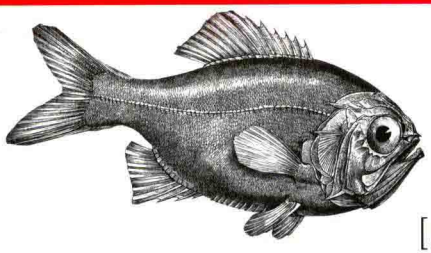
区块链技术概述

Decentralized Applications

帮助读者全面理解并创建dapp

实现超越Web应用的安全性、隐私性、灵活性





[美] Siraj Raval 著

吴海星 译

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

TURING 图灵程序设计丛书

去中心化应用：区块链技术概述

Decentralized Applications:
Harnessing Bitcoin's Blockchain Technology

[美] Siraj Raval 著
吴海星 译

Beijing • Boston • Farnham • Sebastopol • Tokyo O'REILLY®

O'Reilly Media, Inc.授权人民邮电出版社出版

人民邮电出版社
北　京

图书在版编目（CIP）数据

去中心化应用 : 区块链技术概述 / (美) 西拉杰·拉瓦尔 (Siraj Raval) 著 ; 吴海星译. -- 北京 : 人民邮电出版社, 2018.5
(图灵程序设计丛书)
ISBN 978-7-115-47930-3

Ⅰ. ①去… Ⅱ. ①西… ②吴… Ⅲ. ①电子商务－支付方式 Ⅳ. ①F713.361.3

中国版本图书馆CIP数据核字(2018)第032942号

内 容 提 要

在这本实用指南中，作者解释了为什么去中心化应用（dapp）将比现在流行的 Web 应用得到更广泛的使用以及实现更多盈利，展示了如何使用现有工具来创建可用的 dapp 及其市场，并研究了目前两个成功的 dapp 案例。读者将了解到区块链的加密存储台账、scarce-asset 模型和点对点技术如何提供比当前软件模型更灵活、更具激励性的结构。

本书读者对象为对区块链感兴趣的开发人员。

◆ 著　[美] Siraj Raval
译　吴海星
责任编辑　杨　琳
责任印制　周昇亮

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路11号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
大厂聚鑫印刷有限责任公司印刷

◆ 开本：880×1230　1/32
印张：3.75
字数：123千字　2018年5月第1版
印数：1－3 500册　2018年5月河北第1次印刷
著作权合同登记号　图字：01-2017-9358号

定价：39.00元

读者服务热线：(010)51095186转600　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

版权声明

O'Reilly Media, Inc.介绍

O'Reilly Media通过图书、杂志、在线服务、调查研究和会议等方式传播创新知识。自1978年开始，O'Reilly一直都是前沿发展的见证者和推动者。超级极客们正在开创着未来，而我们关注真正重要的技术趋势——通过放大那些“细微的信号”来刺激社会对新科技的应用。作为技术社区中活跃的参与者，O'Reilly的发展充满了对创新的倡导、创造和发扬光大。

O'Reilly为软件开发人员带来革命性的“动物书”；创建第一个商业网站（GNN）；组织了影响深远的开放源代码峰会，以至于开源软件运动以此命名；创立了*Make*杂志，从而成为DIY革命的主要先锋；公司一如既往地通过多种形式缔结信息与人的纽带。O'Reilly的会议和峰会集聚了众多超级极客和高瞻远瞩的商业领袖，共同描绘出开创新产业的革命性思想。作为技术人士获取信息的选择，O'Reilly现在还将先锋专家的知识传递给普通的计算机用户。无论是通过书籍出版、在线服务或者面授课程，每一项O'Reilly的产品都反映了公司不可动摇的理念——信息是激发创新的力量。

业界评论

“O'Reilly Radar博客有口皆碑。”

——*Wired*

“O'Reilly凭借一系列（真希望当初我也想到了）非凡想法建立了数百万美元的业务。”

——*Business 2.0*

“O'Reilly Conference是聚集关键思想领袖的绝对典范。”

——*CRN*

“一本O'Reilly的书就代表一个有用、有前途、需要学习的主题。”

——*Irish Times*

“Tim是位特立独行的商人，他不光放眼于最长远、最广阔的视野，并且切实地按照Yogi Berra的建议去做了：‘如果你在路上遇到岔路口，走小路（岔路）。’回顾过去，Tim似乎每一次都选择了小路，而且有几次都是一闪即逝的机会，尽管大路也不错。”

——*Linux Journal*

前言

排版约定

本书使用下列排版约定。

- 等宽字体（`constant width`）
  表示广义上的计算机编码，包括变量或函数名、数据库、数据类型、环境变量、语句和关键字。
- 等宽粗体（**`constant width bold`**）
  表示应该由用户按照字面输入的命令或其他文本。
- 等宽斜体（*`constant width italic`*）
  表示应该由用户替换或取决于上下文的值。

代码示例

补充材料（包括代码示例、练习题等）可以从 https://github.com/oreillymedia/decentralized_applications 下载。

本书旨在帮助你做好工作。一般来说，你可以在程序和文档中使用本书的代码。除非你使用了很大一部分代码，否则无须联系我们获取许可。例如，使用来自本书的几段代码编写一个程序不需要许可。销售和分发 O'Reilly 书中用例的光盘需要许可。通过引用本书用例和代码来回答问题不需要许

可。把本书中的大量用例代码并入你的产品文档需要许可。

我们很希望但不强求注明信息来源。一条信息来源通常包括书名、作者、出版社和 ISBN。例如："*Decentralized Applications* by Siraj Raval (O'Reilly). Copyright 2016 Siraj Raval, 978-1-4919-2454-9"。

如果你感到对示例代码的使用超出了正当引用或者这里给出的许可范围，请随时通过 permissions@oreilly.com 联系我们。

Safari®在线图书

Safari Books Online（http://www.safaribooksonline.com）是应运而生的数字图书馆。它同时以图书和视频的形式出版世界顶级技术和商务作家的专业作品。技术专家、软件开发人员、Web 设计师、商务人士和创意专家等，在开展调研、解决问题、学习和认证培训时，都将 Safari Books Online 视作获取资料的首选渠道。

对于组织团体、政府机构和个人，Safari Books Online 提供各种产品组合和灵活的定价策略。用户可通过一个功能完备的数据库检索系统访问 O'Reilly Media、Prentice Hall Professional、Addison-Wesley Professional、Microsoft Press、Sams、Que、Peachpit Press、Focal Press、Cisco Press、John Wiley & Sons、Syngress、Morgan Kaufmann、IBM Redbooks、Packt、Adobe Press、FT Press、Apress、Manning、New Riders、McGraw-Hill、Jones & Bartlett、Course Technology 以及其他几十家出版社的上千种图书、培训视频和正式出版之前的书稿。要了解 Safari Books Online 的更多信息，我们网上见。

联系我们

请把对本书的评价和问题发给出版社。

美国：

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472

中国：

北京市西城区西直门南大街 2 号成铭大厦 C 座 807 室（100035）

奥莱利技术咨询（北京）有限公司

O'Reilly 的每一本书都有专属网页，你可以在那里找到本书的相关信息，包括勘误表、示例以及其他信息。本书的网站地址是：

http://shop.oreilly.com/product/0636920039334.do

对于本书的评论和技术性问题，请发送电子邮件到：

bookquestions@oreilly.com

要了解更多 O'Reilly 图书、培训课程、会议和新闻的信息，请访问以下网站：

http://www.oreilly.com

我们在 Facebook 的地址如下：http://facebook.com/oreilly

请关注我们的 Twitter 动态：http://twitter.com/oreillymedia

我们的 YouTube 视频地址如下：http://www.youtube.com/oreillymedia

电子书

扫描如下二维码，即可购买本书电子版。

目录

第1章

什么是去中心化应用

有一种用于构建可伸缩、盈利性大型应用的新模型已经崭露头角。比特币以其加密存储台账、稀缺资产模型和对等网络技术开辟了一条新路，为这种称作**去中心化应用**（decentralized application，简称为 dapp）的新型软件提供了构建基础。虽然 dapp 刚刚得到媒体的关注，但我相信，终有一天它的应用范围会变得更加广泛，并将远远超过目前最流行的 Web 应用。它更灵活、更透明、更分散、更有弹性。与当前的软件模型相比，它的结构有更好的激励性。如果你想了解并亲自创建这样的应用，这是第一本能为你提供帮助的书。

1.1 预备知识：什么是比特币

在深入介绍 dapp 之前，我们先来聊聊比特币[1]和 Web。在过去 10 年间，我们亲眼目睹了 Web 以数量级计的急剧增长。随着与互联网连接的设备逐渐遍及全球，互联网用户的数量达到了数十亿。乍一看，互联网协议套件有着良好的通信标准：链路层将一些数据放在电线上；网络层对数据进行路由；传输层将数据持久化；应用层以应用的形式提供数据抽象。这 4 个协

注 1：在中国，比特币、以太币等“虚拟货币”不具有与货币等同的法律地位，不能在市场上流通使用。本书内容仅代表作者个人观点。——编者注

议层在数据交换上的合作天衣无缝，但可惜它们交换的不是价值。对于价值交换而言，比特币充当了这 4 层之上的第 5 个协议层。

我们现在确实已经有了在 Web 上进行支付的方法，但问题是，它们无一例外地跟效率低下的遗留系统搅在一起，比如在互联网出现之前设计的自动清算所系统（automated clearing house，ACH）。这些传统的支付系统需要依赖集中式的清算系统，因此慢得让人难以忍受。机器不应该为了清算一笔支付等上好几天。它们在持续不断地相互通信，应该有能力将数十亿的小额支付发送给对方，以计量电力和存储空间等资源，并且无须负担高额的中间商交易费用。比特币解决了这个问题。

随着比特币的出现，即时、去中心化、匿名的价值转移终于变成了现实。神秘的比特币缔造者，那个自称中本聪（Satoshi Nakamoto）的人，有效地解决了困扰密码研究几十年的**拜占庭将军问题**。这里引用定义拜占庭将军问题的论文（Lamport，1982）：“（假设）拜占庭军队的一些将军率队在敌人的城市周围安营扎寨。他们相互之间只能依靠信使通信，而且必须在作战计划上达成一致。然而，他们中间可能会有一个或几个想要迷惑其他人的叛徒。那么我们要解决的问题是，找到一种算法来确保忠诚的将军能达成一致意见。”在比特币中达成去中心化的共识，意味着任何一方都无须信任参与信息分享的其他各方，也无须通过一个中央权威来分享信息，其中包括以价值交易形态存在的信息。

比特币和其他“加密货币”将有助于定义互联网的第 5 层协议，让机器像传递数据那样快速有效地传递价值。比特币是很有用的在线价值传递工具，但它最有价值的贡献是其革新性的底层技术：**区块链**（blockchain）。这一技术首次将去中心化共识变成了现实。

区块链是对发生在比特币网络中的所有交易进行大规模复制的数据库。它采用了一种称为工作量证明（proof-of-work）的共识机制，以此来防止在网络中出现双重消费（double-spending）。双重消费问题困扰了密码研究学者几十年，指的是坏人可以对第一次交易予以否认，从而达到将同一笔资金重复使用两次的目的。

工作量证明解决这一问题靠的是在网络中引入**挖矿机**（miner），用其硬件进行加密证明。挖矿机是验证交易的比特币网络节点，会通过自己的区块链

历史来检查交易。区块链历史包含所有曾发生在网络中的交易，是一条带有时间戳的记录。从理论上讲，区块链历史可以修改，但因为有工作量证明，还需要使用网络上的大部分计算力进行验证。因为目前比特币网络所拥有的计算力已经远超世界上所有超级计算机的计算力总和，所以攻破比特币网络极其困难。

从电力消耗和计算负载角度来看，工作量证明需要付出高昂的代价，但它是目前已知能够阻止女巫攻击（Sybil attack）的唯一机制。女巫攻击是指坏人在网络中宣称拥有多个身份，并获取他们不应有的资源来进行攻击。一次成功的女巫攻击极有可能导致比特币完全贬值，因为人们将不再相信它的稳定性。虽然工作量证明代价高昂，但到目前为止，它是唯一经过大规模验证的有效机制。

我们拥有了这样一个称作区块链的新工具，它是一个大规模复制交易数据库，能阻挡女巫攻击。区块链让我们第一次无须使用中心服务器就能达成去中心化共识。你可能想知道这有什么用，也确实应该知道。接下来，我要用很大的篇幅帮你考虑所有的可能性，以及实现它们的方法。不过眼下的重点是让你明白，有众多数据结构能帮你创建出可以盈利的去中心化应用，这只是其中的一种。

1.2 什么是去中心化应用

大多数人熟悉“应用”（application）这个术语是因为它与软件有关。应用软件是指定义了明确目标的软件。目前使用中的应用软件多达数百万，而绝大多数 Web 应用软件都采用集中式的服务器 – 客户端模型。另外有一些是分布式的，还有很少一部分新的应用是去中心化的。图 1-1 直观地展示出了这三种软件模型。

集中式系统是目前最流行的应用软件模型。集中式系统直接控制各个单元的操作，并且信息流源自一个中心。所有单元都要直接依靠中心点来发送和接收信息，以及接受命令。Facebook、Amazon、Google 和其他主流互联网服务用的都是这个模型。我们将这些巨型服务称为“服务栈”。这些服务栈很有用，因为它们为我们提供了有价值的服务。不过它们也有巨大的缺陷，我会在第 2 章展开讨论。

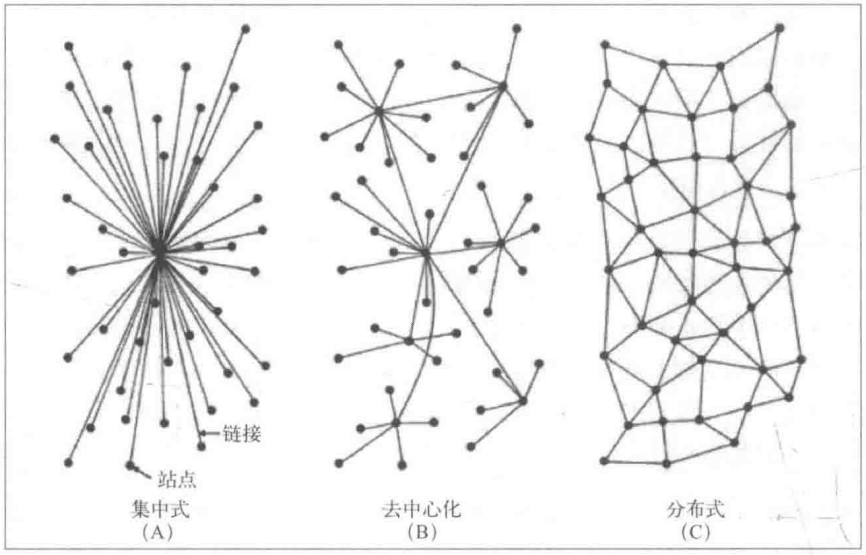


图 1-1：应用软件的三种类型

那么，去中心化和分布式有什么区别呢？

分布式意味着计算不是在一个节点上，而是分布到多个节点上完成的。去中心化的意思则是，任何一个节点都不会对其他节点的工作指手画脚。很多像 Google 这样的服务栈都在内部采用分布式架构，以加快计算速度，降低数据延迟。也就是说，集中式系统同时也可以是分布式的。

那么，去中心化系统可以是分布式的吗？

可以。比特币就是分布式的，因为它盖有时间戳的公共账目（区块链）就是驻留在多个计算机上的。同时它也是去中心化的，因为如果某个节点失效了，整个网络还可以照常运转。也就是说，任何使用区块链和其他端到端工具的应用都可以是分布式的去中心化系统。

那为什么本书不叫作《分布式的去中心化应用》呢？

集中式系统也可以是分布式的。能够达成去中心化共识的应用软件才是真正的革新成果。

那么，有去中心化共识是成为去中心化应用的唯一要求吗？

dapp 领域是一片刚刚开始开垦的沃土，有很多聪明人正在用新的模型进行各种尝试。对于究竟什么是 dapp，不同的开发人员有不同的看法。一些人认为只要没有能导致整个系统失效的中心点就够了，但也有人觉得还要加上其他要求。本书的重点是讨论能够盈利的 dapp，即能让开发人员和用户赚钱的 dapp。之所以关注盈利，是因为利润为成功、健壮、可持续发展的 dapp 奠定了基石。开发人员构建应用，用户保持忠诚，以及矿工维护区块链，都是靠激励措施维持的。接下来介绍所有能够盈利的 dapp 都应该具备的 4 个特性。

1.2.1 特性1：开源

去中心化的闭源应用要求用户相信该应用的去中心化程度确如核心开发人员所说，并且用户不会通过一个中心源来访问自己的数据。因此，闭源应用会让用户望而却步，不敢使用。尤其对于那些会收取、持有或转移用户资金的应用，闭源更让人排斥。尽管确实可以推出一款闭源的去中心化应用，但从一开始就会面临艰难的局面，而且用户会更加青睐开源的竞争对手。将 dapp 开源会改变它的商业行为结构，因此互联网才会变成共同点，而不是孤岛链（见图 1-2）。

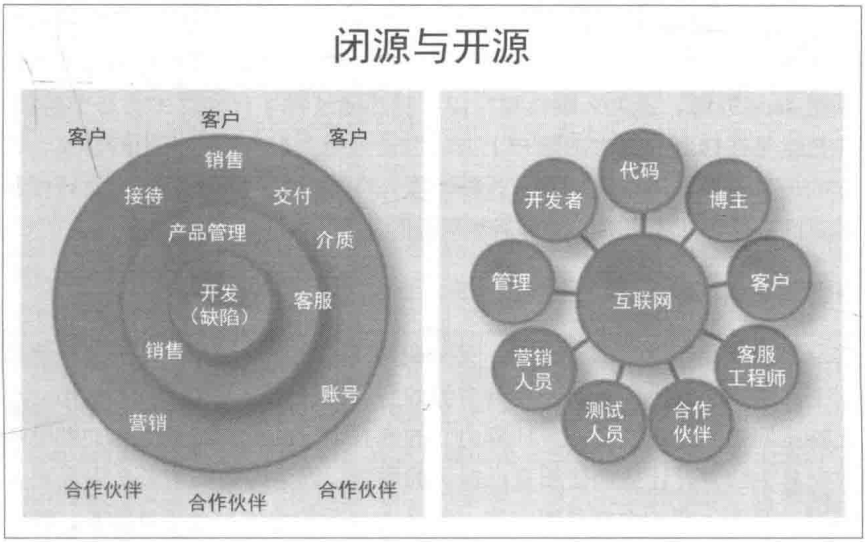


图 1-2：闭源商业计划与开源商业计划的对比

所有应用都能开源，但为什么不这样做呢？

如果研究一下传统的商业模型，就会发现它们全都要求所销售的产品或服务要超过竞争对手。如果把产品开源，竞争对手就能窃取你的工作成果，改头换面后当成他们自己的产品销售。

那么，是什么原因促使开发人员把希望从中盈利的应用开源呢？

从让开源 dapp 的创建者盈利这个角度来看，比特币树立了一个很好的榜样。中本聪保留了最初的一部分比特币，然后让其他人使用其余的部分。因为有数量上的限制，并且比特币网络的工作量证明机制为社会提供了巨大的价值，所以比特币的价值开始增长，从而为中本聪创造了财富。通过开源吸引开发人员为其做出贡献，该应用达成了网络自行完善所需的透明性，并赢得了用户的信任，最终使得比特币在现实世界中有了价值。开源 dapp 能让它赢得潜在用户的信任。任何人都可以从你的 dapp 创建分支，但他们挖不走你的开发团队。用户希望让最合适的人，通常也就是最初的那些开发者，来维护 dapp。

1.2.2 特性2："内部货币"

在 dapp 圈，总会有人问怎么靠它赚钱。集中式应用的传统赚钱模式包括交易手续费、广告收入、推荐佣金、访问用户数据的权力以及订阅服务。如果把 dapp 开源，该怎么赚钱呢？你可能想通过程序自动产生交易手续费，并把这笔钱转到开发者的账户上去，但是可能会有人创建应用的分支，把你的佣金拿走，所以这样是不行的。嵌入广告、订阅服务以及其他任何集中式商业模型所采用的方法都是不可行的。

开源的 dapp 开发者要怎么赚钱呢？

答案是用稀缺令牌，即 App 币，来分配网络中的稀缺资源。用户如果想用这个网络，就需要 App 币。稀缺资源的所有者得到别人支付的 App 币。在比特币网络中，稀缺资源（计算力）的拥有者（矿工）直接从用户那里获取交易手续费，让他们使用自己提供的服务。因为网络的增长会引入更多用户，而 App 币的总额是固定的，所以 App 币的价值也会不断增长。我们可以把这个模型应用到所有 dapp 上。稀缺资源可以是存储空间、交易、图