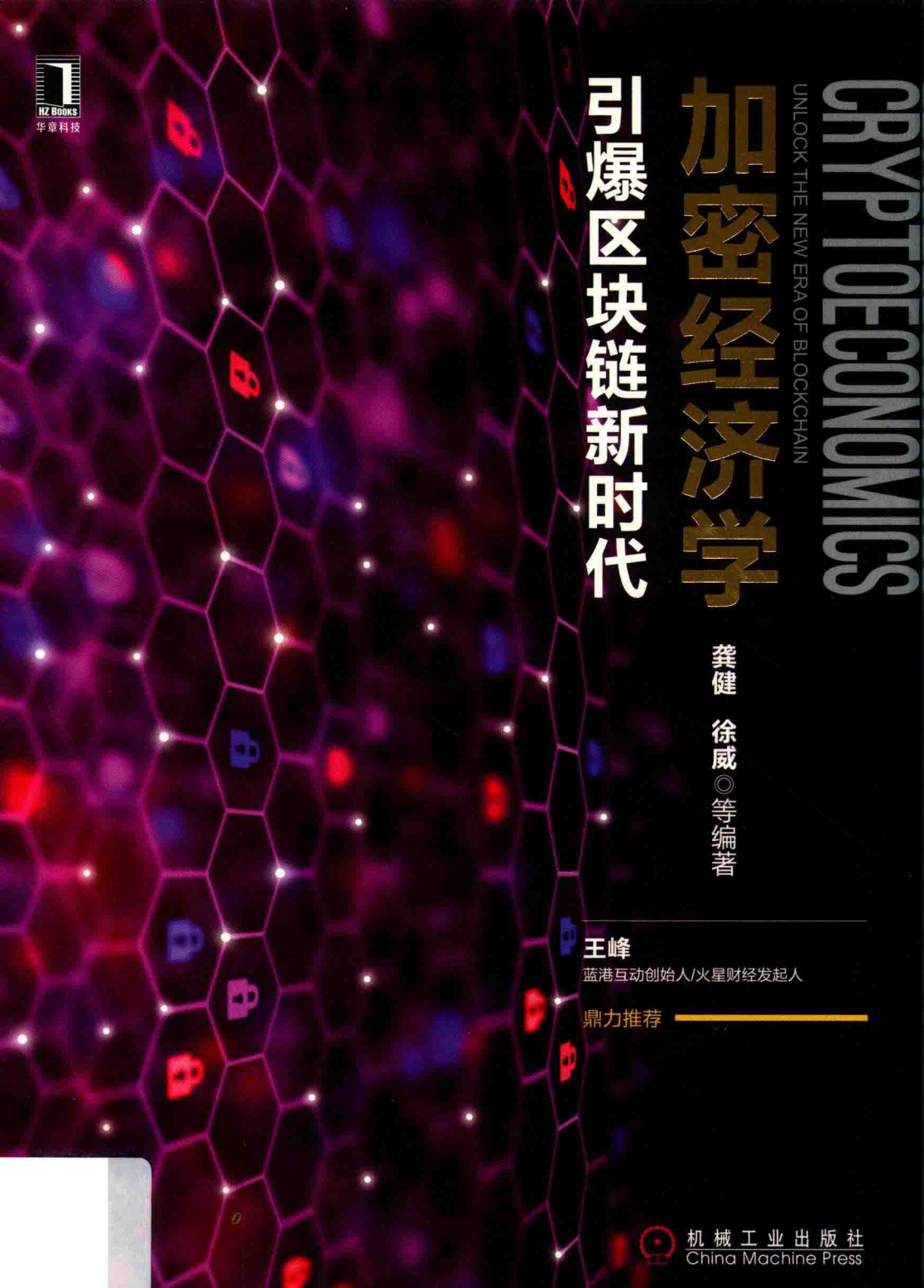
HZ BOOKS
华章科技
CRYPTOECONOMICS
加密经济学
UNLOCK THE NEW ERA OF BLOCKCHAIN
引爆区块链新时代
龚健 徐威◎等编著
王峰
蓝港互动创始人/火星财经发起人
鼎力推荐
机械工业出版社
China Machine Press

加密经济学

引爆区块链新时代

龚健 徐威 阳昊 张森 行走的翻译C 方媛媛◎编著

CRYPTOECONOMICS

UNLOCK THE NEW ERA OF BLOCKCHAIN

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

加密经济学：引爆区块链新时代 / 龚健等编著 . —北京：机械工业出版社，2019.1

ISBN 978-7-111-61590-3

I. 加… II. 龚… III. 电子商务 - 电子支付 IV. F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 281827 号

加密经济学：引爆区块链新时代

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：罗丹琪
责任校对：殷　虹
印　　刷：北京文昌阁彩色印刷有限责任公司
版　　次：2019 年 1 月第 1 版第 1 次印刷
开　　本：147mm × 210mm　1/32
印　　张：5.75
书　　号：ISBN 978-7-111-61590-3
定　　价：59.00 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

FOREWORD
推荐序

为什么要读这本书?

从 2014 年投资 OKCoin 开始算起，我接触区块链已经有 4 年了。在这期间，OKCoin（OKEx）已经成为全球最大的数字货币交易所之一，但我必须说，我是从 2017 年年底创办火星财经开始，才真正在区块链世界找到感觉的。

很多人不能一眼看到区块链的巨大机会。因为区块链足够颠覆，足够复杂，它看上去是 20 年前“去中心化互联网”的升级版，好像只是一个技术创新。但事实上，区块链建立了一个新的信任体系，并由此把技术、经济、文化乃至人性裹挟进来，把一切链化，打一个比方，它更像八爪鱼。我相信这是一次远大于互联网的机会，这是一次“掀桌子”的机会。

对这样一个复杂和全新的事物，单从技术角度理解已经完全不够了。所以，在火星财经的社群里，很多人讨论问题稍一深入，就会进入货币学、经济学范畴，甚至哲学和神学也经常被纳入讨论议题。

当下，“比特币”“区块链”“智能合约”“挖矿”这些名词已经走入大众的视线。很多人关注区块链技术是由于加密数字货币市值的暴涨，而非体会到区块链技术颠覆了我们已有的认知，并将要带来一场全新的革命。

我很喜欢“加密经济学”这个提法，我相信这个尚未被大家所熟知的名词，将会在区块链中占有相当重要的地位。本书的作者之一龚健，是比特币社区的早期参与者，2011 年开始接触挖矿，也是《哈佛商业评论》和《华尔街见闻》等的专栏作家。他所著的这本书比较系统地梳理了区块链衍生的经济模式的架构和来龙去脉，是一本科普类的加密经济学书籍。书中用通俗易懂的语言，讲述了加密经济学及与其相关联的博弈论和行为经济学等。

区块链通过技术解决信任问题，而加密经济学的机制被写成代码之后，能通过一系列的奖励和惩罚措施来约束区块链上每个

人的行为，这是一种伟大的创新机制，自动、安全、有共识。

我相信未来关于加密经济学的讨论会更多、更深入，加密经济学对于区块链的影响也会越来越大，让我们共同期待那一天的到来。

王峰，蓝港互动集团 (HK.8267) 创始人、
火星财经发起人、极客帮创投合伙人

PREFACE

前言

加密经济学如何引爆区块链新时代

相信你对“区块链”已经再熟悉不过了。区块链技术颠覆了我们已有的认知，并将带来一场全新的革命。

加密经济学是一个不被大家所熟知的名词，但是它在区块链中的地位相当重要。以太坊社区开发者弗拉德·赞菲尔（Vlad Zamfir）对这一术语进行了解释：这是一门独立的学科，旨在研究去中心化数字经济学中的协议，这些协议被用于管理商品及服务的生产、分配和消费。它也是一门实用科学，重点研究对这些协议的设计和界定方法。

本书比较系统地梳理了区块链衍生的经济模式的架构和来龙去脉，用实际案例说明了加密经济学与区块链的必然联系。

区块链通过技术解决信任问题，而加密经济学的机制被写

成代码之后，能通过一系列的奖励和惩罚措施来约束区块链上每个人的行为，这是一种伟大的创新机制。加密经济学的最大意义在于保证去中心化共识系统的安全、稳定、积极和有序。这里面我们提到了四个词语，其中安全和稳定主要依靠密码学机制来实现，而积极和有序则依靠经济学机制来实现。

本书还对当前最流行的各种共识算法和这些共识算法的优化机制进行了详细探讨，对有志于参与区块链浪潮的朋友来说，非常有参考意义。同时，本书还探索了博弈论、行为经济学这些经济学机制在区块链上的映射，也列举了一些浅显易懂的例子，以帮助大家轻松理解。

CONTENTS
目录

01

第1章

什么是加密经济学

什么是加密经济学？以太坊社区开发者弗拉德·赞菲尔说：

“加密经济学是一门独立的学科，旨在研究去中心化的数字经济中管理商品和服务生产、分配及消费的协议。加密经济学是一门专注于这些协议的设计和特性的实用科学。”

如果把加密经济学的概念分解一下，正如其名，它来源于两个词汇：密码学（Cryptography）和经济学（Economics）。

1.1 密码学基础

古典密码学主要关注信息在保密形式下的书写和传递，以及与其相对应的破译方法。而现代密码学则起源于20世纪末出现的大量相

关密码理论，是数学和计算机科学的分支，同时大量涉及信息论。现代密码学不只关注信息保密问题，还同时涉及信息完整性验证，信息发布的不可抵赖性（即数字签名），以及在分布式计算中产生的来自内部和外部攻击的所有信息安全问题。

现代密码学的发展促进了计算机科学的发展。如今，密码学已被应用在日常生活中，包括 ATM 的芯片、计算机访问密码、电子商务等领域。

区块链技术中使用了多项密码学内容，主要包括**哈希算法、密钥加密和数字签名。**

1.1.1 哈希算法

哈希（Hash）函数有多种叫法，如密码散列函数、消息摘要函数、杂凑函数，它不一定使用密钥，但它和许多重要的密码算法相关。它将输入数据（通常是一整份文件）输出成较短的固定长度散列值，这个过程是单向的，两个不同的输入产生相同的散列值这种情况的发生概率非常小。

简而言之，哈希算法是将任意长度的字符串映射为较短的固定长度的字符串。例如，比特币使用的是 SHA-256 摘要算法，对任意长度的输入给出的是 256 位的输出。

那么，加密货币中哈希算法的应用有哪些呢？

1. 加密哈希函数

加密哈希函数有如下特性。

- 确定性：无论在同一个哈希函数中解析多少次，如果输入的内容相同，得到的总是相同的输出。
- 高效运算：计算哈希值的过程是高效的。
- 抗原像攻击，即隐匿性：对一个给定的输出结果，不可逆推出输入。
- 细微变化影响：任何输入端的细微变化都会对哈希函数的输出结果产生剧烈影响。

加密哈希函数对区块链的安全性和挖矿有巨大的作用。

2. 数据结构

密码学中，有两种数据结构对于理解区块链非常重

要：链表和哈希指针。

链表是依次按顺序连接而成的数据区块，如图 1.1 所示。

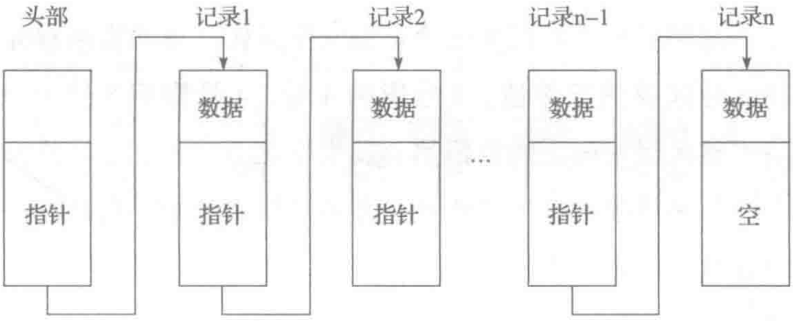

图 1.1

链表中的每一个区块都通过指针指向另一个区块。

区块链本质上是一个链表，其中的每个新区块都包含一个哈希指针。指针指向前一区块及其含有的所有数据的哈希值。正因如此，区块链拥有了不可更改的重要特性。

那么，区块链是如何实现不可更改性的呢？

假设有人尝试篡改区块中的数据，我们先看加密哈希

函数的第三条特性——“细微变化影响：任何输入端的细微变化都会对哈希函数的输出结果产生剧烈影响。”那么，即便有人尝试对 1 号区块里的数据进行细微的改写，也会使得存储在 2 号区块里的 1 号区块的哈希值产生巨大的变化，这将导致 2 号区块的哈希值发生变化，进而影响存储在 3 号区块的哈希值。3 号影响 4 号，4 号影响 5 号……最终整条区块链上的数据都会发生变化。这种通过冻结整条链条来修改数据的方式几乎是不可能做到的。因此，区块链被认定具有不可更改性。

每个区块都有自己的梅克尔根（Merkle Root）。如图 1.2 所示，如果每个区块里都包含多笔交易，将这些交易按线性存储，那么在所有交易中寻找一笔特定的交易会变得非常麻烦。这就是我们使用梅克尔树的原因。

如图 1.3 所示，在梅克尔树中，所有个体交易通过哈希算法都能向上追溯至同一个根，这会使搜索变得非常容易。因此，如果想要在区块里获取某一特定的数据，我们可以直接通过梅克尔树里的哈希值来进行搜索，而不用进行线性访问。