一本言简意赅、系统介绍区块链开发的自学教程，零基础入门区块链，读这本书就够了。

范凌杰　编著

自学·区块链

原理、技术及应用

- 简明扼要介绍区块链核心概念与原理
- 实例引导快速上手区块链项目开发（以太坊、超级账本、EOS等）
- 融会贯通各类主流开发技术（Python、Solidity、Go、Docker、前端开发等）

机械工业出版社
CHINA MACHINE PRESS

自学区块链

——原理、技术及应用

范凌杰　编著

机械工业出版社

本书是一本系统介绍区块链理论知识和应用开发的教程。全书共 8 章，主要包括两部分的内容，区块链理论知识（第 1～3 章）：区块链概述、区块链中的密码学以及区块链的核心机制；区块链应用开发（第 4～8 章）：打造自己的第一个区块链——基于 Python、以太坊之 DApp 开发实战、超级账本开发实战、EOS 开发实战以及区块链综合应用开发实践。本书在系统介绍区块链理论知识的基础上，结合丰富的案例进行实践操作的讲解，力求引领读者在实践中深入理解区块链技术，具备基于主流的区块链平台开发区块链实际应用的能力。

本书可以作为区块链开发者的自学用书，也可作为开设区块链开发相关课程的各类院校、培训机构的教材。

本书相关代码可以在 https://github.com/flingjie/learning-blockchain 获取。

图书在版编目（CIP）数据

自学区块链：原理、技术及应用 / 范凌杰编著. —北京：机械工业出版社，2019.5
ISBN 978-7-111-62601-5

Ⅰ. ①自… Ⅱ. ①范… Ⅲ. ①电子商务－支付方式－教材 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字（2019）第 080505 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：王 斌 责任编辑：王 斌
责任校对：张艳霞 责任印制：孙 炜
北京中兴印刷有限公司印刷
2019 年 6 月第 1 版 • 第 1 次印刷
184mm×260mm • 13.5 印张 • 312 千字
0001－3000 册
标准书号：ISBN 978-7-111-62601-5
定价：49.80 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
服务咨询热线：（010）88361066
读者购书热线：（010）68326294

网络服务
机 工 官 网：www.cmpbook.com
机 工 官 博：weibo.com/cmp1952
金 书 网：www.golden-book.com
教育服务网：www.cmpedu.com

前言

区块链技术是近些年来最热门的前沿技术，被认为是未来十几年对金融、物联网、医疗等诸多领域产生最大影响的“黑科技”之一。

“区块链”这个概念是由一个网名为中本聪的人在2008年发表的《比特币：一种点对点的电子现金系统》中提出的。随后他实现了一个比特币系统，并发布了加密数字货币——比特币，接下来出现了以太坊和超级账本这样的大型区块链项目。区块链技术在全球范围内引起了广泛关注，并势不可挡地影响着多个行业的发展趋势。

目前，区块链正处于迅猛发展阶段，急需区块链方面的技术人才。本人根据自己的实践经验，尝试写了这本易懂实用的区块链教程，希望能够帮助想学习区块链技术的朋友。

内容组织与阅读建议

本书主要分为两部分，第一部分是理论知识，介绍区块链技术的概念、原理、架构设计和发展历程；第二部分是应用开发，在掌握理论知识的基础上结合丰富的实践案例进行操作，在实践中深入理解区块链技术，通过学习和实践主流的区块链平台和框架，掌握区块链实际应用开发能力。

- **第1章：区块链概述**：从区块链的概念和运行原理说起，继而介绍区块链的技术构成、逻辑架构和分类，然后介绍区块链的发展历程和典型应用。学完这一章可以对区块链有一个整体的认识，明白区块链是什么，能做什么。
- **第2章：区块链中的密码学**：学习区块链中的密码学知识，掌握区块链技术原理，包括对称加密算法和非对称加密算法、椭圆曲线密码学、Merkle树、数字签名和数字证书等知识。
- **第3章：区块链的核心机制**：这一章介绍了区块链核心技术，包括共识机制、账户交易和智能合约等。
- **第4章：打造自己的第一个区块链——基于Python**：从本章开始进入动手实践区块链的阶段，本章基于Python实现一个功能完备的区块链系统。
- **第5章：以太坊之DApp开发实战**：以太坊是专注于智能合约，开发并运行DApp的区块链平台，这一章介绍了以太坊中DApp（去中心化应用）的概念和开发，并实现了两个完整的DApp（猜拳游戏和宠物商店）。
- **第6章：超级账本开发实战**：超级账本是一个开源项目，它提供了一个成熟的商用区块链框架。这一章介绍了它的概念、学习安装和使用，并通过超级账本中的几个实例学习掌握超级账本的开发过程。
- **第7章：EOS开发实战**：EOS是一个区块链操作系统，这一章介绍了什么是EOS，以及它的框架和特点，并介绍了搭建一个EOS本地开发环境的过程，在此基础之上，

通过实例（Hello World 智能合约和许愿树 DApp）介绍了 EOS 的开发流程。

- **第 8 章：区块链开发综合应用实践**：通过讲解几个综合性的区块链开发实例，以太坊数据查询分析系统、ERC20 代币、数字资产“加密猪”的开发，进一步介绍区块链技术的应用。

本书特色

本书一大特点是，结合区块链的开发实践，介绍了包括 Python 语言、Solidity 语言、Go 语言、Docker 容器技术和前端开发技术在内的多种实际开发中经常用到的技术和工具。通过本书的学习，读者朋友不仅能快速上手开发区块链项目，更能初步了解、掌握多种实用的软件开发技术，非常有助于读者建立基本的开发能力，打下从事多种应用领域开发的基础。

需要说明的是，本书在介绍各类开发技术时重在实现功能，完成任务，并未花费大量篇幅介绍相关理论和知识体系，为零基础或者有一定基础的读者朋友，打开通往区块链开发乃至软件开发精彩世界的大门才是本书要达到的目标。

本书适用读者

本书可以作为零基础区块链爱好者自学用书，也可作为开设区块链开发相关课程的各类院校、培训机构的教材。

配套资源

本书配有所有案例的相关代码，读者都可以访问 https://github.com/flingjie/learning-blockchain 自行获取。

致谢

感谢每一位在茫茫书海中选择了本书的读者朋友，衷心祝愿您能够从本书中受益，学到真正需要的知识。同时也期待每一位读者的热心反馈，随时欢迎您指出书中的不足，并通过电子邮箱 fanlingjie.cn@gmail.com 与作者沟通和交流。

范凌杰　于上海

2018 年 11 月

目录

第1章 区块链概述

区块链（Blockchain）是近些年来极为热门的前沿技术名词，区块链技术被认为是未来十几年对金融、物联网、医疗等诸多领域产生影响最大的“黑科技”之一。

本章将介绍区块链的基本概念、技术构成与逻辑架构、区块链的分类、特点、发展历程、典型应用，区块链技术的现状及展望。通过学习本章的内容，读者可以对区块链有一个整体的认知，理解什么是区块链，了解区块链的原理架构和典型应用，以及区块链能用来做什么。

本章学习目标

- 了解区块链的基本概念和几个重要的发展阶段。
- 理解区块链的原理和架构设计。
- 熟悉区块链的典型应用。
- 掌握区块链的现状和发展方向。

1.1 什么是区块链

区块链是近年来社会上的一个热门词汇，经常在各种新闻媒体上可以看到区块链的相关报道。但在区块链被广泛谈论的过程中，人们对区块链这个新鲜事物在认知上还存在不少的误区的。这里将常见的认知误区整理如下。

- 区块链是比特币，比特币也就是区块链。
- 区块链很值钱。
- 区块链可以运用在任何领域。
- 区块链是免费的。
- 区块链是非常安全的。

下面，分别对以上的误区进行分析和澄清。

比特币和区块链是有很深的渊源（在区块链发展历程中会有详细介绍），但比特币和区块链两者不能等同。实际上，区块链是比特币的底层技术，好比用面粉可以做包子，但不能说面粉等于包子，包子等于面粉。这里的区块链相当于面粉，而比特币相当于包子。除了比特币外，还有很多其他的基于区块链技术的应用。

区块链的确是一种很神奇的技术，很有可能就像当初互联网技术改变世界一样再次重构整个世界，但区块链本身只是一种技术，真正产生价值的是应用区块链技术产生的落地服务。

区块链不是万能的，当前区块链只会对某些领域，如金融、供应链等区块链适用的行业产生重大影响，区块链在其他行业的使用场景还有待研究。

区块链是有成本的，区块链中的每一个“区块”通常都需要用大量的运算来解决，为支持区块链服务的所有设备的耗电量成本相当不菲。

和传统的互联网相比，区块链在安全性方面有着天然的优势。非对称加密保证了交易数据的安全性；分布式存储和记账显著降低了数据被篡改、网络受攻击以及网络瘫痪的可能性。但区块链现在还处在初步发展阶段，其技术本身可能还存在一些漏洞，这些漏洞会被那些恶意的黑客利用去实施一些破坏行为，所以说区块链的安全是相对的，并不是绝对安全。

实际上应该还会有一些其他的思维误区，这里就不再一一讨论了。澄清了这么多误区，那么，回过头来看，究竟什么是区块链呢？

1.1.1 区块链的概念

“区块链”这个概念是一个网名为中本聪的人在 2008 年发表的《比特币：一种点对点的电子现金系统》中提出的。其描述如下。

时间戳服务器对以区块（Block）形式存在的一组数据实施随机散列并加上时间戳，然后将该随机散列进行广播，就像在新闻或世界性新闻组网络（Usenet）的发帖一样。显然，该时间戳能够证实特定数据于某特定时间是的确存在的，因为只有在该时刻存在了才能获取相应的随机散列值。每个时间戳应当将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前的一个时间戳进行增强（Reinforcing），这样就形成了一个链条（Chain），即区块链，如图 1-1 所示。

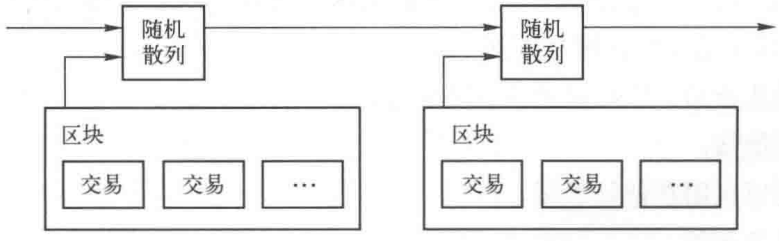

图 1-1　区块链的链条结构

构成区块链的区块是基于密码学生成的，每一个区块包含了前一个区块的哈希值（由加

密算法生成的）、对应的时间戳记录以及交易数据等信息（对区块结构的详细介绍参见下一节相应内容）。本质上，区块链是包含这些交易记录的分布式系统，类似于一个账本。所以，区块链也被称为分布式账本系统。

这个分布式账本系统是由分布式系统中的诸多结点共同创建和维护的一个链表。链表由基于密码学原理生成的一个个区块组成。其中每个区块包含了交易者的公钥、金额、时间等交易信息，区块链的链表结构如图 1-2 所示。

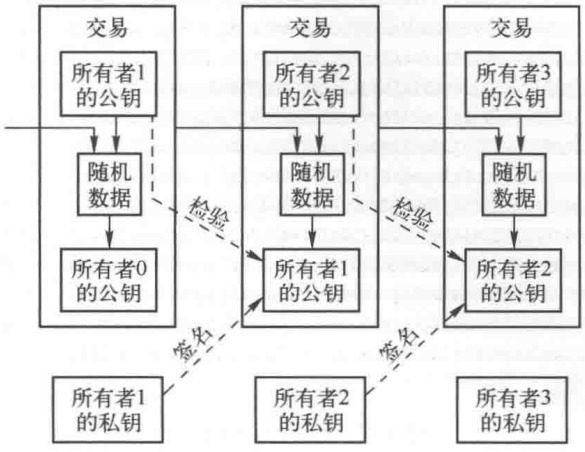

图 1-2　区块链的链表结构

不过，分布式账本系统是区块链狭义上的含义。广义上来说，区块链是一个统称，除了基于区块链结构的分布式账本系统，它还包括共识机制、智能合约、点对点网络、自治社区等一系列和分布式账本相关的功能。可以将区块链看作是很多个技术的组合。

了解了区块链的概念后，接下来认识一下构成区块链的区块到底是什么。

1.1.2　区块的概念

区块是区块链的组成单元，就像金字塔是由一块块石头组成的一样，区块链就是由一个个区块组成的。

1．区块

从本质上说，区块链中的区块是由一系列特征值和一段时间内的交易记录组成的一个数据结构。这里以比特币区块为例进行说明。

登录比特币区块查询网站：https://webbtc.com/可以看到最新生成的比特币区块信息。本节截取了 2016 年 12 月 17 日生成的十几个区块的列表信息，如图 1-3 所示。

图中的 3 列信息依次为区块的高度（Height）、区块的哈希值（Hash）和区块的生成时间（Time）。单击第一个区块可以查看这个区块的详情，如图 1-4 所示。详情信息包括区块的哈希值（Block）、高度（Height）、父区块哈希值（Prev Block）和一系列交易信息（Transactions）。详情信息中，前一个 Transactions 后面跟的数字是这个区块包含的交易总量，下面的 Transactions 则显示了一个个具体的交易数据）。

Bitcoin - Recent Blocks

Height	Hash	Time	Tx	Si
443888	000000000000000000cdc0d2a9b33c2d4b34b4d4fa8920f074338d0dc1164dc	2016-12-17 20:29	444	2
443887	0000000000000000001806a922d4d35a37ad9324c690f72d556c6445cb7a9c214	2016-12-17 20:26	20	6.
443886	000000000000000000f061205567dc79c4e718209a568879d66132e016968ac6	2016-12-17 20:26	351	2
443885	0000000000000000002b1502dc9a00036e66790c4cde07df425c6cbae3e0d8eca	2016-12-17 20:24	1,945	8
443884	0000000000000000000b27456bcb96b255d98cdac8c10df9be5d8859a9c279ef3	2016-12-17 20:13	93	9
443883	0000000000000000001a1f18b82dcb6696db3136a601c1ac53b59db13201b18b7	2016-12-17 20:13	1,062	4
443882	000000000000000000015c4fe93fa30dd7e497f140f4879959733a1e00b8b404fc	2016-12-17 20:07	727	3
443881	000000000000000000126c8dab37f7146baaa88a3d68cdfca996e824a0f8a0d04	2016-12-17 20:04	2,529	9
443880	0000000000000000000d30b003adcdfcc843c0dc5f46ed26d136294d110158c21	2016-12-17 19:48	1,130	9
443879	000000000000000000368ca004e61fa5ff9502b1cd5721f03318c968cdc941531	2016-12-17 19:42	514	9
443878	000000000000000001b267c75f6b97ff58d1367d16ddc9b6ddcead31041f8058	2016-12-17 19:40	1,052	9
443877	000000000000000000b57d57fc57e022fbebc6fbdee108095dcf1bfcdd68b4d5	2016-12-17 19:35	366	1
443876	0000000000000000034f2855c116b426305d82a54b29cceb32641da639aeef82	2016-12-17 19:33	891	3
443875	000000000000000009b58ed9b94ca8a88f838d69669d64547caf5a01dfaebcc	2016-12-17 19:28	1,330	9
443874	000000000000000001db9e3f4108bc27f6bb6616d7d12b5d71f099e3ac8034ab	2016-12-17 19:21	1,480	6
443873	00000000000000000060793d4a146c9256431a743a858d6428c584fc6a3a92ed	2016-12-17 19:12	298	1
443872	0000000000000000013938072daf1a1e10d723ec884297e19032489ee68a8ad	2016-12-17 19:10	441	2
443871	00000000000000000529329de4b85211e63d10e6aaebablad2fe90167a12f7f	2016-12-17 19:09	1,086	4
443870	0000000000000000002775ff227222f47a46cad46b0f634db53c1a8737d7ecd41	2016-12-17 19:07	9	
443869	0000000000000000002424db0163641940c9fd999ec897b412ce64e36d6ab7650	2016-12-17 19:03	1,836	9

图 1-3　比特币区块信息

Bitcoin - Block Details

Block	000000000000000000b27456bcb96b255d98cdac8c10df9be5d8859a9c279ef3
Height	443884
Prev Block	0000000000000000001a1f18b82dcb6696db3136a601c1ac53b59db13201b18b7
Next Block	0000000000000000002b1502dc9a00036e66790c4cde07df425c6cbae3e0d8eca
Merkle Root	6d942f012235491abda7e22dfaeb039747599899884310 4c6bb1d5d4887f6915
Time	2016-12-17 20:13:40 UTC
Transactions	93
Size	975 KB
Total Value	41.42625996
Block Work	1,332,120,993,527,795,410,415
Chain Work	62,382,847,179,298,513,585,592,988
Formats	[json] [hex] [binary]

Transactions

Hash	Inputs	Outputs
e16a6e66f75d7...	coinbase	1DTh7XPb42PgCFnuMHSitMPWxCfNNFej8n(1
c0b336d773fla...	1Mms6aqBQWuKg9uEC2UAJQdpiFTp4BDMnM(0.01743654)	1E5h1P2ZbcEQFk2hDBFFTBvvzQtLu5g41g (13AxDGGDiBatZzXMsNej8a8H9EooQ8TBnD (
d2c698f7dcd9f...	38ENmTr2AD1avJrmmi9iM7PfS6nZVmuMKf(0.45419291)	38ENmTr2AD1avJrmmi9iM7PfS6nZVmuMKf (14fW6wd2WoCR1jjeTf3yp7bBsPvnj8cekz (1GiWKErSNyMH1wSx4XZhpDRgnR2r57NzZV (
42493dc9bc193...	1FTRy3PyYJa6CRxiNuPZGR8y1dPngZybHz(1.70149888)	1HJ19wdgK5c2ab86Parkvkqtw9nT8JbFCJ (1EcqYTQJW65REiWJ1QkMxn7cnBLTDEhSrM (
68196d967d0e7...	1FU5wJ6xvayyZrvwersc7TzUQThM9vwbMr(0.01672497) 19wpXy4EBzeraDfRkeAmCFw8YYW2RpqFyd(0.01404025)	1AfBPa4nVJDAQyCEEEdaMUN4F8691VreFq (33pQU4bfFyx6rfvwzb1HapdhQpE2p72Naq (
ec68378c698d5...	1FZyCjVkxYfEEMg76xmSTkAKoaPxsbWY4Q(0.11000000)	1B3g9P3bX1BQPDtu1grnpZ57S7GPuoxUNg (

图 1-4　比特币区块详情

单击 Formats 中的“json”项可以以 Json 格式显示这个区块的信息，如图 1-5 所示。


```
{
  "hash": "000000000000000000b27456bcb96b255d98cdac8c10df9be5d8859a9c279ef3",
  "ver": 536870912,
  "prev_block": "0000000000000000001a1f18b82dcb6696db3136a601c1ac53b59db13201b18b7",
  "mrkl_root": "6d942f012235491abda7e22dfaeb039747599899884310 4c6bb1d5d4887f6915",
  "time": 1482005620,
  "bits": 402885509,
  "nonce": 1171280212,
  "n_tx": 93,
  "size": 998142,
  "tx": [
    {
      "hash": "e16a6e66f75d70043f13cf484ef9ab20679bc8d96a59d09795c36341521f759e",
      "ver": 1,
      "vin_sz": 1,
      "vout_sz": 1,
      "lock_time": 0,
      "size": 129,
      "in": [
        {
          "prev_out": {
            "hash": "0000000000000000000000000000000000000000000000000000000000000000",
            "n": 4294967295
          },
          "coinbase": "03ecc5061f4d696e656420627920416e74506f6f6c20757361312025aa35152058559c747627000(
        }
      ],
      "out": [
        {
          "value": "12.55820396",
          "scriptPubKey": "OP_DUP OP_HASH160 88adcf0215d5fcbca5c6532aaecffb48128cf1a6 OP_EQUALVERIFY OI
          "address": "1DTh7XPb42PgCFnuMHSitMPWxCfNNFej8n"
        }
      ],
      "nid": "ea55af54f76d94a3dc42082e00cda31d907e69e0afe810859445c05db02b28fe"
    },
    {
```


图 1-5　比特币区块的详情以 Json 格式显示

这个区块的数据结构看上去有点复杂，但没关系，通过接下来的详细解释后就很容易理解了。

2．区块的结构

区块的数据结构由区块头和区块体组成。区块头包含了当前区块的特征值，区块体中包含的是实际的交易记录数据。

（1）区块头

区块头由 80 个字节组成，主要由版本号、前一个区块的哈希值、Merkle 根、时间戳、bits、Nonce 这几项区块的特征值组成，如图 1-6 所示。


```
"ver": 536870912,
"prev_block": "0000000000000000001a1f18b82dcb6696db3136a601c1ac53b59db13201b18b7",
"mrkl_root": "6d942f012235491abda7e22dfaeb039747599899884310 4c6bb1d5d4887f6915",
"time": 1482005620,
"bits": 402885509,
"nonce": 1171280212,
```


图 1-6　区块头

其中 ver（版本号）表示本区块遵守的验证规则；prev_block（父区块哈希值）就是这个区块连接的上一个区块的哈希值，mrkl_root 根是该区块链交易的 Merkle 树根的哈希值（Merkle 是一种哈希树的数据结构，在第 2 章中会详细讲解），时间戳是区块生成的时间，bits 是区块的难度值 Nonce 是一个随机数，其中各个字段的长度和详细说明如图 1-7 所示。

区块头组成

	长度（字节）	说明
版本	4	区块版本号
父区块哈希值	32	前一区块的哈希值
Merkle根	32	该区块中交易的Merkle树根的哈希值
时间戳	4	该区块产生的近似时间，精确到秒的UNIX时间戳，必须严格大于前11个区块时间的中值，同时全节点也会拒绝那些超出自己两个小时时间戳的区块
目标难度	4	该区块工作量证明算法的难度目标，已经使用特定算法编码
Nonce	4	为了找到满足难度目标所设定的随机数，为了解决32位随机数在算力飞升的情况下不够用的问题，规定时间戳和coinbase交易信息均可更改，以此扩展nonce的位数

图 1-7　区块头组成

（2）区块体

区块头下面的部分是区块体，如图 1-8 所示。


```
"n_tx": 93,
"size": 998142,
"tx": [
  {
    "hash": "e16a6e66f75d70043f13cf484ef9ab20679bc8d96a59d09795c36341521f759e",
    "ver": 1,
    "vin_sz": 1,
    "vout_sz": 1,
    "lock_time": 0,
    "size": 129,
    "in": [
      {
        "prev_out": {
          "hash": "0000000000000000000000000000000000000000000000000000000000000000",
          "n": 4294967295
        },
        "coinbase": "03ecc5061f4d696e656420627920416e74506f6f6c20757361312025aa35152058559c7476270000
      }
    ],
    "out": [
      {
        "value": "12.55820396",
        "scriptPubKey": "OP_DUP OP_HASH160 88adcf0215d5fcbca5c6532aaecffb48128cf1a6 OP_EQUALVERIFY OP_
        "address": "1DTh7XPb42PgCFnuMHSitMPWxCfNNFej8n"
      }
    ],
    "nid": "ea55af54f76d94a3dc42082e00cda31d907e69e0afe810859445c05db02b28fe"
  },
  {
    "hash": "c0b336d773f1a5ea7be25013e0fd293a30ef2e6a193f10bd4774041189188dfc",
    "ver": 1,
    "vin_sz": 1,
    "vout_sz": 2,
    "lock_time": 443872,
    "size": 226,
    "in": [
      {
```


图 1-8　区块体

区块体主要包括交易数量（n_tx）、区块大小（size）和长度不定的交易记录（tx 字段包含的交易列表）等信息。但这只是比特币中的区块体结构，实际上区块体中可以包括任何内容，比如以太坊中的区块体中除了交易数据还包含智能合约。

了解了区块结构，再来看看区块的特点。

3．区块的特点

区块的一个特点是，它是由计算机通过加密算法生成的。如果成功地生成一个有效的区块，该计算机（或者说结点）就能获得一定的奖励，这个奖励就是加密数字货币。这一过程就像是在开采有价值的矿产，故而被形象地称为“挖矿”，执行操作的计算机被称为“矿机”，用矿机挖矿的人也就被称之为“矿工”了。

除此之外，区块还有一个特点，若区块是有效的，则该区块的哈希值必须满足一定的条件。这个条件就是能够使得区块头中特征值相加生成的哈希值符合一定格式，比如以 000 开始。由于哈希值随着输入的不同而不同，故计算机要不断尝试改变区块头的 Nonce 值直至最终生成的哈希值满足条件才算生成了一个有效的区块，如图 1-9 所示。

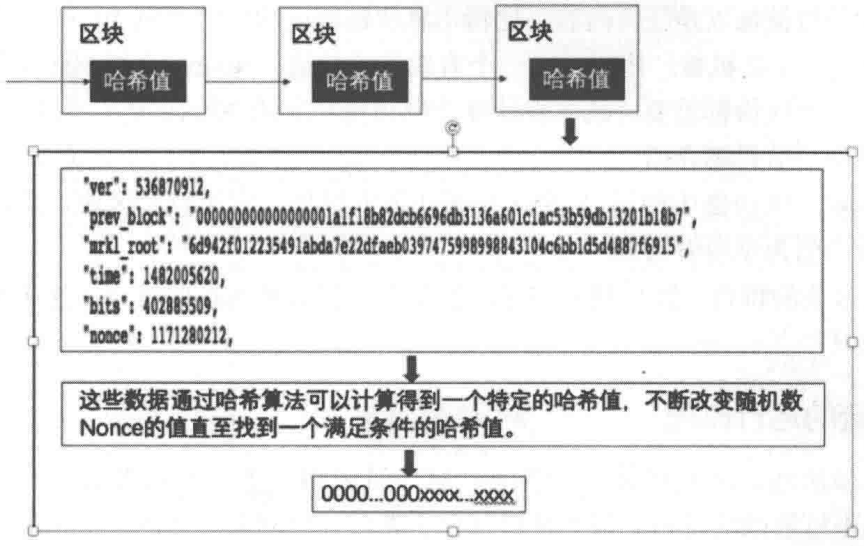

图 1-9　生成有效区块

寻找特定 Nonce 值生成有效区块的机制叫作工作量证明。工作量证明是常见的共识机制之一，关于共识机制的内容将在第 3 章中详细讲解。

在区块结构中各个字段也有其各自的特点和作用，如图 1-10 所示。

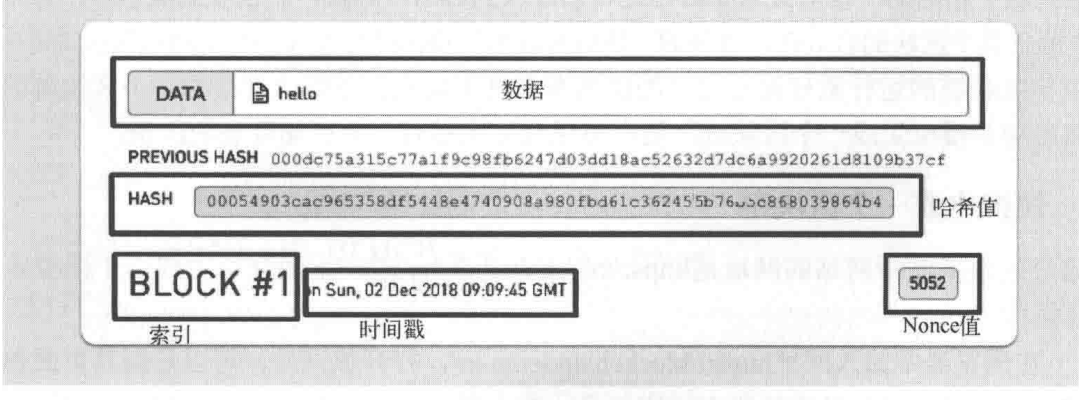

图 1-10　区块中的字段

区块结构中字段的说明如下。

- 索引标示了区块在区块链中的位置，其中第 1 个区块——创世区块的索引为 0，第 2 个区块的索引为 1，第 3 个区块的索引为 2，依次累加。
- 时间戳表示的是该区块生成的时间，根据时间戳可以判断区块链中各个区块生成的先后顺序。
- 哈希值是每个区块的唯一标示，也可称为区块的“数字指纹”。哈希值的长度是固定的，而且和区块内容紧密关联，一旦区块内容发生改变，该区块的哈希值也会发生改变。而且，区块中的哈希值还有有效和无效之分，满足特定条件的哈希值是有效的，否则就是无效，这个特定条件一般称之为困难度（Difficulty）。父区块哈希值就是区块链中特定区块前一个区块的哈希值。
- 区块中的数据可以是任何内容，比特币区块链的区块中的数据为一串串交易记录。
- Nonce 是一个随机数，用来生成一个有效的哈希值。Nonce 会根据区块数据的不同而不同，每个区块都需要经过大量计算才能找到对应的 Nonce 值。关于 Nonce 值的概念会在下一节详细介绍。
- 创世区块。区块链中的第 1 个区块叫作创世区块，它没有父区块，故创世区块的父区块哈希值为空或者为 0。

以上就是区块的特点，区块链的很多特性都是基于区块的这些特点。接下来介绍区块链的运行原理。

1.1.3 区块链的运行原理

如 1.1.1 节所述，区块链是一个链表，这个链表由一个个区块组成，这些区块依次连接，形成一个不可篡改的链条。每个区块包含了索引、时间戳、父区块哈希值、交易数据、Nonce 值、本区块的哈希值等信息。那么这个链表具体是怎么生成和维护的？

首先是构成区块链的去中心化网络中的第 1 个结点初始化，并生成区块链中的创世区块；然后通过“挖矿”生成的新区块被添加到区块链中；新的结点加入到去中心化网络后会先同步一份最新的区块链数据；随后每个结点生成的区块都会向网络中的其他结点进行广播；其他结点接收到这个结点的广播后会判断自己是否已经收到过这个区块，若已收到就忽略，若未收到过则先验证这个区块的有效性，有效的区块会被收到广播的结点添加到自身结点的区块链中。

对于区块链的运行原理通过文字的描述有点过于抽象，下面读者结合一个区块链的演示网站自己动手模拟生成一个区块链，这样可以对区块链有一个更加直观的认识。

1.1.4 模拟生成一个区块链

这个区块链演示网站的网址是https://blockchaindemo.io/，下面介绍生成一个模拟区块链的具体操作。

1）在浏览器中输入网址https://blockchaindemo.io/，打开该网站，可以看到其页面包括 4 个区域，左上角是区块链中的所有结点信息，右上角有一个“Add Peer”按钮可以往区块链