

BLOCKCHAIN
PRACTICAL DECODING 730 QUESTIONS

区块链实用解码

730问

上册 基础与核心

王骥 编著



实用 全面 系统

—— 百科全书 ——



法律出版社
LAW PRESS · CHINA

BLOCKCHAIN

PRACTICAL DECODING 730 QUESTIONS

区块链实用解码

730问

上册 基础与核心

王骥 编著



法律出版社
LAW PRESS · CHINA

编写说明

本书分为上下两部分,上部分包括区块链的构架、共识机制与算法以及加密机制与算法;下部分包括区块链 1.0:从比特币到数字货币、区块链 2.0:智能合约与可编程金融、区块链 3.0:可编程的经济与社会。

本书较同类图书更为详细,仅区块链的核心机制与技术——共识算法与加密算法,就以 10 章篇幅进行了论述。本书以问答方式的体例,730 个问题既普及知识,又答疑解惑,更易为读者所接受。

之前的互联网是“信息互联网”;今后,区块链将促使互联网华丽换体,嬗变成“价值互联网”,前景不可估量。

王 骥

2018 年 8 月 15 日

总 目 录

上 册

第一部分 框架解密与颠覆

第 1 章	区块链及其背后的神秘组织	(3)
第 2 章	深度解密:区块链的本质、核心与价值颠覆	(22)
第 3 章	区块链的系统构架、数据结构及运行机制	(38)
第 4 章	分布式网络(P2P)与分布式账本	(61)
第 5 章	区块链的分类与应用等问题详解	(78)

第二部分 共识机制与算法

第 6 章	分布式系统的一致性问题	(89)
第 7 章	拜占庭将军问题与共识算法的引入	(97)
第 8 章	工作量证明(PoW)算法	(104)
第 9 章	权益证明(PoS)算法	(113)
第 10 章	委托权益证明机制(DPoS 算法)	(121)

第三部分 加密机制与算法

第 11 章	区块链密码算法:概述与哈希算法	(139)
第 12 章	梅克尔哈希算法	(159)
第 13 章	区块链密码算法:公开密钥算法	(172)
第 14 章	区块链加密算法:椭圆曲线算法	(184)

第 15 章	区块链密码算法:编码和解码算法	(194)
--------	-----------------------	-------

下 册

第四部分 区块链 1.0:从比特币到数字货币

第 16 章	区块链 1.0 数字货币概述、安全与监管	(205)
第 17 章	比特币的内涵、运行机制与原理	(218)
第 18 章	比特币的功用安全、误解攻击、炒作违法与监管等	(242)
第 19 章	比特币扩容,隔离见证与闪电网络	(261)
第 20 章	百花齐放的“山寨币”	(274)

第五部分 区块链 2.0:智能合约与可编程金融

第 21 章	区块链 2.0 的基石:智能合约	(297)
第 22 章	区块链 2.0 与可编程金融	(309)
第 23 章	以太坊的内涵框架、机制运行及其与比特币的比较	(318)
第 24 章	以太坊代币、雷电网络、应用及其典型项目	(336)
第 25 章	超级账本的构架特色、价值功用与开发应用	(349)
第 26 章	以太坊、超级账本与比特币的比较	(359)
第 27 章	B3i、R3 及国内外著名的区块链组织	(366)

第六部分 区块链 3.0:可编程的经济与社会

第 28 章	区块链 3.0 的概述	(385)
第 29 章	EOS 及 IPFS:区块链 3.0 的实力先行者	(395)
第 30 章	迅雷链:区块链 3.0 的实力竞争者	(405)
第 31 章	九大区块链 3.0 公链的性能、应用及其比较	(414)
第 32 章	区块链 3.0 与自主主权身份革命	(428)

目 录

上 册

第一部分 框架解密与颠覆

第 1 章 区块链及其背后的神秘组织	(3)
1.1 区块链背后的神秘组织及其运动	(3)
1.1.1 产生、背景与过程	(3)
1.1.2 宣言与使命	(6)
1.1.3 区块链颠覆与价值	(9)
1.2 “神”一样的“朋克大牛”	(10)
1.2.1 向“大牛”致敬	(10)
1.2.2 贡献与推动	(11)
1.3 解密中本聪	(13)
1.3.1 身份与注册解密	(13)
1.3.2 隐匿大法与“圈”中影响	(15)
1.4 客观评价中本聪	(18)
1.4.1 极端与客观	(18)
1.4.2 坐拥 700 亿元人民币与“义侠”价值	(20)
第 2 章 深度解密:区块链的本质、核心与价值颠覆	(22)
2.1 11 大视角解密:区块链的内涵与误解	(22)
2.1.1 区块链的突破、颠覆与诞生	(22)
2.1.2 万物账本与数据库	(25)
2.1.3 三大核心问题与演进	(28)
2.1.4 多技术融合与互联网协议	(29)

2.2 深度解密区块链特征	(30)
2.2.1 一般性特征	(30)
2.2.2 去中心化偏差与争议	(30)
2.2.3 信任改写与共识颠覆	(32)
2.2.4 开放匿名、不可篡改与万物平台	(33)
2.3 区块链与网络本质、核心问题的解决	(34)
2.3.1 重塑交易与万物互信	(34)
2.3.2 信息互联网转变为价值互联网	(35)
2.3.3 代码即法律的颠覆	(35)
2.3.4 网络本质的填实与桥梁	(36)
第3章 区块链的系统构架、数据结构及运行机制	(38)
3.1 区块链的系统框架	(38)
3.1.1 区块链的系统构架、运行与讲解思路	(38)
3.1.2 数据层、网络层与共识层	(40)
3.1.3 激励层、合约层与应用层	(41)
3.2 区块的概念及识别	(42)
3.2.1 区块与区块头	(42)
3.2.2 区块的识别	(43)
3.3 创世区块与区块的连接	(44)
3.3.1 创世区块及其数据	(44)
3.3.2 区块的连接	(46)
3.4 区块链的数据结构	(48)
3.4.1 区块链的结构基础及其讲解思路	(48)
3.4.2 哈希值、梅克尔根等数据及作用	(49)
3.4.3 难度确认、运行及其作用	(50)
3.4.4 时间戳、随机数及其作用	(52)
3.5 区块链的工作流程与机制	(53)
3.5.1 步骤与防止分叉	(53)
3.5.2 安全、透明与不可篡改的系统机制	(54)
3.6 从 1.0 到 3.0 的演化升级	(56)
3.6.1 区块链的进化	(56)

3.6.2 区块链 1.0	(57)
3.6.3 区块链 2.0	(57)
3.6.4 区块链 3.0	(58)
第 4 章 分布式网络(P2P)与分布式账本	(61)
4.1 P2P 的概念、问题及事物	(61)
4.1.1 类型与概念	(61)
4.1.2 分散化、负载均衡与隐私	(63)
4.1.3 高效、健壮与可扩展	(64)
4.2 常见问题与分布式事物	(65)
4.3 P2P 的两种架构	(66)
4.3.1 分类及性能	(66)
4.3.2 非结构化的 P2P 网络	(67)
4.3.3 结构化的 P2P 网络	(68)
4.4 广播机制	(69)
4.5 验证机制	(70)
4.5.1 概念与验证	(70)
4.5.2 步骤与唯一性	(71)
4.6 分布式账本	(72)
4.6.1 概念与特点	(72)
4.6.2 分布式账本与商业账本的比较	(73)
4.6.3 应用价值与操作	(75)
第 5 章 区块链的分类与应用等问题详解	(78)
5.1 分类标准与解密思路	(78)
5.2 公有链、私有链与联盟链	(79)
5.2.1 公有链的概念、优势与不足	(79)
5.2.2 私有链的特点、界定与争议	(80)
5.2.3 联盟链的特点、关系与运用	(82)
5.2.4 三大链的选择、落地与现实问题	(83)
5.3 主链与测试链	(84)
5.4 单链、侧链与互联链	(85)

第二部分 共识机制与算法

第 6 章 分布式系统的一致性问题	(89)
6.1 分布式系统一致性概述	(89)
6.1.1 分布式系统一致性的概念与模型	(89)
6.1.2 难度、要求与解决	(90)
6.2 三个重要定理	(92)
6.2.1 FLP 定理及意义	(92)
6.2.2 CAP 定理及应用	(92)
6.2.3 BASE 定理	(94)
第 7 章 拜占庭将军问题与共识算法的引入	(97)
7.1 拜占庭将军问题	(97)
7.1.1 概念、实质与条件	(97)
7.1.2 两军问题	(98)
7.1.3 拜占庭将军问题的解决与意义	(100)
7.2 共识算法的引入与目的	(101)
7.2.1 思维与激励机制	(101)
7.2.2 随机性与属性	(101)
7.2.3 适用范围	(102)
第 8 章 工作量证明 (PoW) 算法	(104)
8.1 PoW 的概念与要求	(104)
8.2 PoW 的原理	(105)
8.2.1 原理解析	(105)
8.2.2 例证解析	(107)
8.3 比特币的 PoW 算法	(108)
8.3.1 PoW 函数与区块	(108)
8.3.2 难度值、过程与步骤	(110)
8.4 PoW 算法的优缺点	(111)
第 9 章 权益证明 (PoS) 算法	(113)
9.1 概念、产生与原理	(113)

9.2 造币、主链与 PoS	(114)
9.2.1 币龄与区块的生成	(114)
9.2.2 造币与主链协议	(116)
9.3 校验签名与防止震荡通膨	(116)
9.3.1 校验、签名与节能	(116)
9.3.2 震荡、通膨与马太效应	(118)
9.4 PoS、PoW 的对照与混合	(119)
9.4.1 PoS 的优缺点	(119)
9.4.2 PoS 和 PoW 比较与混合	(119)
第 10 章 委托权益证明机制(DPoS 算法)	(121)
10.1 DPoS 算法概述	(121)
10.1.1 概念、背景与原理	(121)
10.1.2 DPoS 算法的逻辑与解决的问题	(123)
10.2 DPoS 算法运行机制	(123)
10.2.1 委托人代表	(123)
10.2.2 修改、重组与费率	(125)
10.3 DPoS 算法的操作	(126)
10.3.1 准备、正常与分叉	(126)
10.3.2 双重生产、碎片化与不可逆	(127)
10.3.3 出块人、PoS 与混洗	(130)
10.3.4 安全性能与优缺点	(131)
10.4 PoW、PoS 与 DPoS 的对比	(133)
10.4.1 PoW、DPoS 在能耗、攻击与治理的对比	(133)
10.4.2 PoW 与 DPoS 的共识、去中心化等的对比	(134)
10.4.3 PoW、PoS 与 DPoS 的对比	(135)

第三部分 加密机制与算法

第 11 章 区块链密码算法:概述与哈希算法	(139)
11.1 密码算法概述及本部分思路	(139)
11.1.1 密码算法及其相关概念	(139)

11.1.2 密码算法区块链应用概述	(140)
11.2 区块链中的哈希算法	(141)
11.3 哈希算法的概念、种类与挑战	(142)
11.3.1 哈希算法的概念与特点	(142)
11.3.2 哈希算法概念的碰撞与安全	(144)
11.3.3 哈希算法的常用语流行种类	(145)
11.3.4 主要哈希算法的对比与挑战	(146)
11.4 哈希算法的常规应用	(148)
11.4.1 密码学上哈希算法的安全条件与优势	(148)
11.4.2 数字签名与文件校验	(149)
11.4.3 数据结构管理中的哈希算法	(151)
11.4.4 P2P、DHT 网络的哈希算法	(152)
11.5 SHA-256 算法	(152)
11.5.1 SHA-256 算法概念与哈希运算步骤	(152)
11.5.2 SHA-256 算法的预处理	(154)
11.5.3 SHA-256 算法的哈希过程	(155)
11.6 哈希指针与区块链的防篡改	(157)
11.6.1 哈希指针与区块的链接	(157)
11.6.2 哈希指针的防篡改	(158)
第 12 章 梅克尔哈希算法	(159)
12.1 梅克尔树概述	(159)
12.1.1 梅克尔树的概念、特点和形式	(159)
12.1.2 梅克尔树的提出与研究	(161)
12.2 梅克尔树与哈希列表的关系	(162)
12.3 梅克尔树在区块链中作用	(163)
12.4 梅克尔的证明、运用与局限性	(165)
12.4.1 梅克尔的证明	(165)
12.4.2 梅克尔的服务机制与局限	(167)
12.5 梅克尔树的升级与梅克尔·帕特里夏树	(169)
12.5.1 梅克尔树的升级	(169)
12.5.2 梅克尔·帕特里夏树	(170)

第 13 章 区块链密码算法:公开密钥算法	(172)
13.1 公开密钥算法	(172)
13.1.1 对称与非对称两种算法及关系	(172)
13.1.2 公开密钥算法体系	(174)
13.1.3 公开密钥算法原理	(175)
13.2 RSA 算法	(175)
13.2.1 RSA 算法概述	(175)
13.2.2 RSA 算法必备的数学知识	(177)
13.2.3 RSA 算法操作的主要环节	(179)
13.2.4 RSA 算法的编程实现	(182)
第 14 章 区块链加密算法:椭圆曲线算法	(184)
14.1 椭圆曲线加密算法概念与级别比较	(184)
14.2 椭圆曲线加密算法的特点、优势与运用	(185)
14.3 椭圆曲线加密算法的数学原理	(187)
14.3.1 椭圆曲线加密算法的加法	(187)
14.3.2 椭圆曲线加密算法离散对数问题	(189)
14.4 密码学中的椭圆曲线加密算法	(190)
14.5 椭圆曲线加密算法的简单加密和解密	(192)
第 15 章 区块链密码算法:编码和解码算法	(194)
15.1 编码和解码算法的概念与美国标准信息交换代码对照表	(194)
15.2 Base64 编码	(196)
15.2.1 Base64 编码的概念与原理	(196)
15.2.2 Base64 操作与实现	(198)
15.3 Base58 编码	(199)
15.3.1 Base58 的概念与编码表	(199)
15.3.2 Base58 的编码与解码表	(200)
15.4 Base58Check	(201)

问答目录

001	区块链背后的神秘组织是什么,是如何产生的?	(3)
002	“密码朋克”运动的历史背景与重大过程是什么?	(4)
003	“密码朋克”发布过哪些重要文件,对比特币、区块链的诞生有何 重大指引?	(6)
004	“密码朋克”宣言的使命、目标和思想是什么,有何重大影响?	(8)
005	区块链、“密码朋克”产生的现实价值及其颠覆性作用是什么?	(9)
006	“密码朋克”有哪些“大牛”,人们是如何向他们致敬的?	(10)
007	“密码朋克”的“大牛”们,都为区块链做了什么贡献?	(11)
008	戴伟的 B-money 与比特币最大的区别是什么?	(12)
009	中本聪特殊的注册生日,如何解密?	(13)
010	中本聪到底是什么身份,如何揭秘?	(14)
011	中本聪“神龙不见首尾”的藏匿大法到底怎样?	(15)
012	中本聪在“密码朋克”中的影响度到底如何?	(17)
013	如何客观评价中本聪的成就?	(18)
014	坐拥近 700 亿元人民币财富却不认领,中本聪的“义侠”意义?	(20)
015	中本聪“销声匿迹”背后的伟大价值是什么?	(21)
016	“人类金融史上的最大突破”,区块链概念是如何诞生的?	(22)
017	从区块链创新的角度看区块链如何诞生?	(23)
018	如何从一个古老问题上来看区块链概念的诞生?	(24)
019	如何从比特币底层技术角度来看区块链的诞生?	(24)
020	如何从总账副本的角度来理解区块链的一般性概念?	(25)
021	如何从账本“记账”的动态角度来理解区块链?	(26)
022	如何从数据库的构造角度来理解区块链?	(27)
023	如何从解决三大核心问题的角度来理解区块链?	(28)

024	如何从升级换代的历史演进角度来理解区块链?	(28)
025	如何从多种技术组合的角度来理解区块链?	(29)
026	如何从互联网应用协议的角度来理解区块链?	(29)
027	区块链有哪些重要特点?	(30)
028	如何深度理解区块链点对点与去中心化特点?	(30)
029	对区块链的去中心化有什么争议?	(31)
030	如何深度理解区块链的去信任与共识机制?	(32)
031	如何理解区块链的时间戳与不可篡改性?	(33)
032	如何理解区块链的开放性与匿名性?	(33)
033	如何理解区块链的跨平台与万物性?	(34)
034	以颠覆性的模式解决了万物交换的互信问题,如何理解?	(34)
035	信息互联网转变为价值互联网,区块链改写了什么?	(35)
036	未来社会,“代码即法律”的颠覆,区块链有何作用?	(35)
037	颠覆性地弥补了传统互联网的不足,如何理解?	(36)
038	搭建虚拟世界与现实世界的桥梁,区块链做了些什么?	(36)
039	区块链的系统构架与各层级的讲解思路是什么?	(38)
040	区块链系统构架是如何互动与运行的?	(39)
041	如何简要理解区块链的数据层?	(40)
042	如何简要理解区块链的网络层?	(40)
043	如何简要理解区块链的共识层?	(41)
044	如何简要理解区块链的激励层?	(41)
045	如何简要理解区块链的合约层?	(41)
046	如何简要理解区块链的应用层?	(41)
047	什么是区块,其数据结构是怎样的?	(42)
048	什么是区块头,其数据结构是怎样的?	(42)
049	区块如何识别,区块哈希值是什么?	(43)
050	什么是区块高度,它是如何识别区块的?	(43)
051	创世区块是如何诞生的?	(44)
052	创世区块的数据与信息是什么?	(44)
053	区块是如何连接的?	(46)
054	区块链的构造示意图即过程是怎样的?	(48)

055	区块链的数据结构基础及本节思路是什么?	(48)
056	什么是哈希值,怎样构成区块链的数据结构?	(49)
057	什么是梅克尔根,如何构成区块链的数据结构?	(50)
058	区块链数据结构中的难度目标与什么有关,作用是什么?	(50)
059	区块链数据结构中的难度值是什么,作用是什么?	(51)
060	难度目标与新难度值是如何计算的?	(51)
061	什么是时间戳,与区块链数据结构的关系是什么?	(52)
062	什么是随机数,与挖矿的关系是什么?	(52)
063	区块链的工作步骤有哪些?	(53)
064	如何理解全网广播与杜绝分叉问题?	(54)
065	时间戳在区块链中的重要作用是什么?	(54)
066	区块链网络是如何成为诚实可信系统的?	(54)
067	区块链网络是如何做到安全、透明与不可篡改的?	(55)
068	区块链是如何进化的?	(56)
069	区块链 1.0 的特点主要是什么?	(57)
070	区块链 1.0 的实质与运用是什么?	(57)
071	区块链 2.0 的特点主要是什么?	(57)
072	区块链 2.0 的另一种划分观点是什么?	(58)
073	区块链 2.0 作为可编程的智能合约,其应用主要包括什么?	(58)
074	区块链 3.0 的概念是什么?	(58)
075	区块链 3.0 的特点主要是什么?	(59)
076	区块链 3.0 的应用主要有哪些?	(59)
077	举例说明区块链 3.0 的一些应用是怎样的?	(59)
078	有哪三种网络模式?	(61)
079	什么是分布式?	(61)
080	什么是分布式网络(P2P 网络)?	(62)
081	如何理解 P2P 网络的分散化与负载均衡的特点?	(63)
082	如何理解 P2P 网络的隐私性特点?	(64)
083	如何理解 P2P 网络的可扩展性特点?	(64)
084	如何理解 P2P 网络的高性能特点?	(65)
085	如何理解 P2P 网络的健壮性特点?	(65)

086	P2P 网络中常见的问题有哪些?	(65)
087	什么是 P2P 网络的分布式事物?	(66)
088	分布式(P2P)网络的两种架构是什么?	(66)
089	分布式(P2P)网络两种架构的性能如何?	(67)
090	什么是非结构化的 P2P 网络?	(67)
091	非结构化的 P2P 网络数据索引效率为何很低?	(68)
092	什么是结构化 P2P 网络?	(68)
093	结构化的 P2P 网络的优缺点是什么?	(69)
094	广播与验证机制有何意义?	(69)
095	交易广播的概念及其作用是什么?	(69)
096	区块构造广播的概念及其意义是什么?	(70)
097	区块链 P2P 网络的验证机制是什么?	(70)
098	交易信息的验证机制是怎样的?	(70)
099	区块构造的验证机制是什么?	(71)
100	区块构造验证的具体步骤是什么?	(71)
101	验证如何保证区块链的唯一性?	(72)
102	什么是账本?	(72)
103	什么是分布式账本?	(72)
104	区块链分布式账本系统的特点是什么?	(73)
105	传统的商业记账方式是什么?	(73)
106	传统商业账本存在的问题有哪些?	(74)
107	分布式账本记账的方式是什么?	(74)
108	区块链分布式账本的优势是什么?	(74)
109	分布式账本存在的问题和解决思路是什么?	(75)
110	分布式账本的产品应用价值是什么?	(75)
111	比特币如何采用分布式账本?	(76)
112	在分布式模式下,交易如何进行?	(76)
113	区块链有哪些分类?	(78)
114	什么是区块链的公有链?	(79)
115	公有链主要有哪些特点?	(79)
116	公有链的不足之处有哪些?	(80)

117	什么是区块链的私有链?	(80)
118	对私有链概念、内涵的界定,业界有哪些争议?	(81)
119	私有链主要有哪些特点?	(81)
120	怎样理解区块链的联盟链?	(82)
121	联盟链与公有链、私有链有何关系?	(82)
122	联盟链如何在金融集团之间运用?	(83)
123	三种链的落地趋势如何?	(83)
124	引入不同区块链主要面临哪些现实问题?	(84)
125	什么是区块链的主链?	(84)
126	什么是区块链的测试链?	(85)
127	什么是单链,需要注意什么?	(85)
128	什么是侧链,对照比特币如何理解其关键内涵?	(85)
129	什么是互链?	(86)
130	什么是分布式系统的一致性问题?	(89)
131	一致性有哪些模型?	(89)
132	最终一致性模型的变种是什么?	(90)
133	分布式系统一致性问题为何很难解决?	(90)
134	分布式系统,一般希望它具备哪些能力?	(91)
135	如何技术性地理解或处理分布式系统的一致性?	(91)
136	什么是 FLP 定理,有何重大意义?	(92)
137	FLP 定理的发现者林奇有何其他贡献?	(92)
138	什么是 CAP 定理?	(92)
139	CAP 定理是如何应用的?	(93)
140	CAP 定理实际应用有什么技巧?	(93)
141	什么是 BASE 定理?	(94)
142	BASE 定理中的“基本可用”须注意什么?	(94)
143	BASE 定理中“最终一致性”的其他观点是什么?	(95)
144	BASE 定理和 ACID 的区别与联系是什么?	(95)
145	什么是拜占庭将军问题?	(97)
146	拜占庭将军问题的实质是什么?	(98)
147	拜占庭将军问题隐含的条件和结论是什么?	(98)