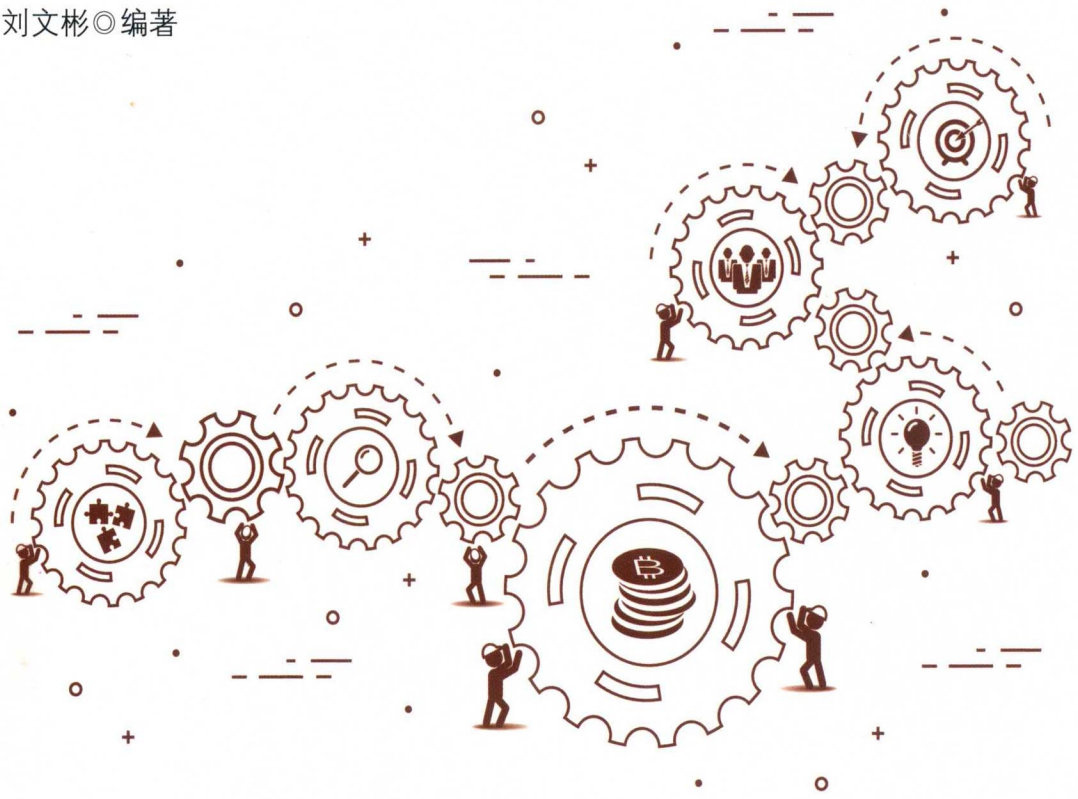
Broadview®
www.broadview.com.cn

EOS
实战与源码分析

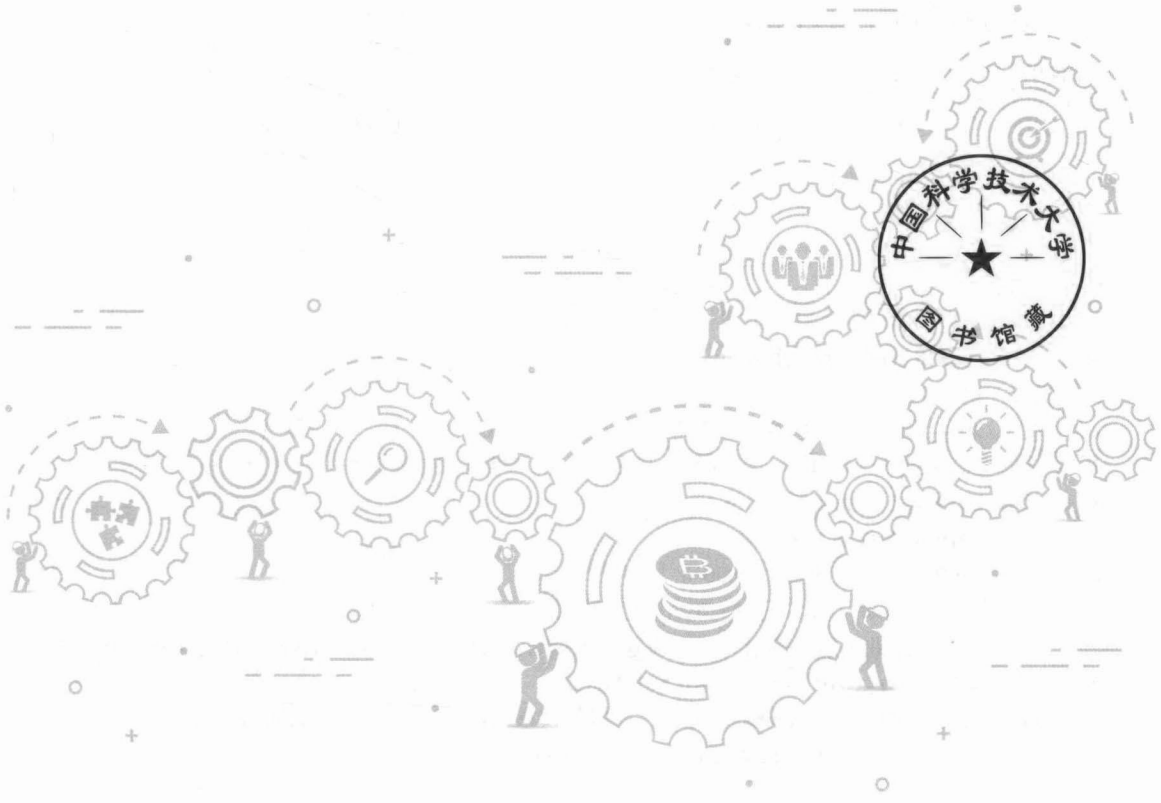
刘文彬◎编著



中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

EOS
实战与源码分析

刘文彬◎编著



電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

在区块链世界，区块链 1.0 时代是比特币，区块链 2.0 时代是以太坊，区块链 3.0 时代是 EOS。EOS 如同一个完整的操作系统，用户或者机构可基于它构建各种应用程序。

本书共有 8 章，可分为使用手册与源码分析两部分。使用手册部分主要介绍如何快速启动单节点 EOS 链、终端交互命令 cleos 的使用，并模拟公链的配置与启动。源码分析部分主要介绍源代码调试、EOS 数据持久化机制、系统智能合约架构以及插件系统。

无论是正在使用 EOS 的软件工程师、测试工程师、运维工程师、架构师，还是热衷新技术的产品经理、管理人员，本书都具备很强的辅导和参考价值。

图书在版编目（CIP）数据

EOS 实战与源码分析 / 刘文彬编著. —北京：电子工业出版社，2019.7

ISBN 978-7-121-36928-5

Ⅰ. ①E… Ⅱ. ①刘… Ⅲ. ①电子商务－支付方式－研究 Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字（2019）第 122735 号

责任编辑：安　娜　　特约编辑：田学清
印　　刷：三河市君旺印务有限公司
装　　订：三河市君旺印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×980　1/16　　印张：17.25　　字数：331.2 千字
版　　次：2019 年 7 月第 1 版
印　　次：2019 年 7 月第 1 次印刷
印　　数：2500 册　　定价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件到 dbqq@phei.com.cn。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

前　言

2017 年，区块链、加密货币、ICO（公募）的声音吵闹了整个夏天，截至 9 月，声音才渐渐消失。许多技术人员借此了解了区块链技术，并且被区块链的技术蓝图所震撼，激发了强大的兴趣，为自己能够置身于一个技术蓬勃发展的时代而感到荣幸。

笔者正是其中之一。在同样的时间，一头扎进区块链的世界，从区块链 1.0 时代的比特币到 2.0 时代的以太坊，再到 3.0 时代的 EOS。呈现在眼前的区块链世界就像一个技术万花筒，深深地吸引笔者不断向前探索。

目前，EOS 是区块链炙手可热的技术之一。它如同一个完整的操作系统，用户或者机构可基于它构建各种应用程序。下一代区块链不是 ICO，而是大规模的各行各业的 DApp 的兴起，所以能够做好大型商业应用基建工作的公链将成为未来区块链的宠儿。目前，呼喊着百万级 TPS、手续费为 0、快速部署 DApp 的 EOS 无疑切中了所有的要点。

笔者作为 EOS 开源项目的贡献者，在超级节点的运维工作过程中，系统地研究了区块链的底层技术。后来笔者深入区块链的应用领域，总结了很多心得体会。本书共有 8 章，可分为使用手册与源码分析两部分。使用手册部分主要介绍如何快速启动单节点 EOS 链、终端交互命令 cleos 的使用，并模拟公链的配置与启动。源码分析部分主要介绍源代码调试、EOS 数据持久化机制、系统智能合约架构以及插件系统。

无论是正在使用 EOS 的软件工程师、测试工程师、运维工程师、架构师，还是热衷新技术的产品经理、管理人员，本书都具备很强的辅导和参考价值。

EOSIO 是构建 EOS 的开源项目，是一个由 block.one 公司开发的、基于区块链结构

设计的、能够支持水平和垂直扩展的、去中心化的应用平台，提供了账户、认证、数据库、异步通信和跨平台、跨集群的定时应用。同时，有望支持每秒百万级事务，完全零费率，并可以快速且容易地部署去中心化应用。

希望能与热爱区块链技术的朋友共同研究EOS技术，笔者的博客地址是http://www.cnblogs.com/Evsward，欢迎各位朋友前来留言讨论。

EOS 中的易混淆名词

- EOS，目前指的是基于 ERC20 在以太坊上发行的代币体系，用于 block.one 公司开发软件与社区运营。
- EOSIO，由 block.one 开发的可构建公链的软件源代码。
- EOS platform，采用 EOSIO 软件构建的公链平台。
- DApp，此处指的是未来在 EOS 公链平台上基于 EOSIO 软件开发部署的去中心化应用，通常是由智能合约实现的，但在 EOS 中也可以通过插件的方式实现。

名词解释

EOS 中有很多专用名词，下面通过表格列举展示。

EOS专用名词解释

序　号	名　词	解　释
1	Account	账户，由用户自定义创建，可包含语义的账户名字。这比区块链只有一个加密长串地址作为账户要方便很多
2	Authority	权力，要与 Permission 做好区分。Permission 是权限的意思，相比权力更加具体，而 Authority 通常用于校验某账户是否有做某件事的权力
3	Block	缩写为 Blk，每个区块可包含 0 个或者多个事务
4	DAC	分权自治集体或者分权自治公司
5	DAO	分权自治组织

续表

序　号	名　词	解　释
6	Deferred Transaction	缩写为 defTx，延期事务。该事务是由智能合约创建的，会在未来的某个时间被执行。这个事务也能够创建另一个在其之后的事务。因此，延期事务可以创建无限循环的顺序事务。用户授权一个延期事务必须指定到执行的时刻应拥有足够的带宽，存储执行预期事务
7	DLT	分布式账本技术。分布式账本也被称作共享式账本，是一个基于复制、共享及同步数字化资产的跨站点、跨国家、跨机构的数据库
8	DPoS	授权权益证明。此外，也可以代表民主即权益证明。DPoS 是共识算法的一种，即区块生产者能够针对事务或者区块的真实性、可验证性、不可逆性等特性达成共识的一种方法
9	Key pair	缩写为 keys，一个密钥对，包括公钥和其对应的私钥
10	Larimer	一种 EOS 的计量单位，等于 0.000 1 EOS，如同以太坊中的 Wei
11	Master Password	用于解锁或者解密一个钱包文件的密码
12	Action	一个对区块链的改变动作。一个或者多个动作可组成一个事务
13	Non-Producing Node	非生产节点，也可以理解为普通节点。这是一个完整的区块链节点，能够智能观察和验证区块，只能维护本地区块链的拷贝。一个普通节点可以在一个“备用池”中，通过投票流程成为生产节点，即具备出块权的超级节点；也会被投票出局，成为一个普通节点进入“备用池”。但值得注意的是，大多数普通节点并不在“备用池”中
14	Oracle	在区块链和智能合约的上下文中是一个代理，被智能合约用于找到和验证外部世界中实际发生的真实数据并提交到区块链上
15	Peer-to-Peer	简称 P2P，即对等计算机网络，是一种在对等者之间分配任务和工作负载的分布式应用构架
16	Permission	加权安全机制，通过评估其签名确定一个信息是否被正确授权
17	Private key	用于签名事务的私钥
18	Public key	缩写为 pub key，公钥，在事务间传输
19	Scope	作用域，智能合约的作用域，账号可写入同一个作用域的（自己的）合约，但对于其他作用域的合约，该账号不能写入数据，只能读取
20	Smart Contract	缩写为 SC，智能合约，一个计算机协议，旨在促进、验证或者执行谈判
21	Standby Pool	100 个全节点的集合，渴望被选中为 21 个超级节点之一。实际上已经拥有超级节点的能力。当区块链需要替换一个超级节点时，就会从备用池中选择它
22	Transaction	缩写为 Tx，一般称作事务，是一个完整的原子的区块链的变化，一个或者多个消息的组合。在 EOS 中通常是由一个智能合约执行的

续表

序　号	名　词	解　释
23	Wallet	钱包，会生成一个加密钱包文件或者是通过客户端进行管理，如 cleos 管理私钥以及用一个安全的方式促进事务的签名。钱包可以被锁定或者解锁
24	Block Producer	缩写为 bp，21 个超级节点之一，正在出块轮次的超级节点

读者服务

轻松注册成为博文视点社区用户（www.broadview.com.cn），扫码直达本书页面。

- **提交勘误**：您对书中内容的修改意见可在【提交勘误】处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。
- **与读者交流**：在页面下方【读者评论】处留下您的疑问或观点，与其他读者一同学习交流。

页面入口：http://www.broadview.com.cn/36928

目　录

第1章 加密算法

1.1 单向哈希函数

单向哈希函数，又称单向散列函数，可以把任何数据变为一段无现实意义的定长数据串。因此，单向哈希函数有两个重要功能：一是将不同长度结构的数据因子转化为等长数据；二是在不传输明文数据的前提下，只是对比加密数据串就可以确定明文数据是否一致，常用于网络文件防篡改、文件完整性校验等场景。

单向哈希函数的特点是正向容易逆向困难，目标是生成速度越快越好，而反推明文数据则越困难、越慢越好。除以上标准，评判一种哈希函数是否优秀的关键是碰撞率要足够低。不同的明文数据生成相同的加密数据串，这种情况被称为哈希函数发生了碰撞。碰撞的出现会造成数据危险，因此一个哈希函数的碰撞率足够低是至关重要的。常见的算法有 MD4（已淘汰）、MD5、SHA-224、SHA-256、SHA-384 和 SHA-512。从速度和碰撞率来讲，目前较常用的是 SHA-256。

在互联网中，单向哈希函数是常见的解决方案。在登录过程中，服务器端及网络传输中只保存登录密码的加密数据串而不保存明文。用户登录时输入的明文密码，会先在客户端通过单向哈希函数处理，得到的加密数据串再经由网络传输到服务器端，与数据

库中的加密数据串进行比对，如果一致则密码正确，如果不一致则密码错误。这种方法避免了明文密码传输泄露的风险。

然而，黑客专门制作了一个字典表，保存了一批明文数据与加密数据串的映射关系。例如，将 123456 使用 SHA-256 算法得到加密数据串，与 123456 相对应，以此类推，最终获得一个容量很大的字典表。接着，黑客通过截取网络传输数据或者盗取公司数据库，得到加密数据串，然后在字典表中遍历查找，如成功找到即可破解明文密码。

字典表越来越大，遍历查找会越来越慢。为了加快速度，黑客把具有相同特征的加密数据串统一分组，然后创建一个彩虹表保存特征与一组加密串的映射关系。例如，字典表中所有以 0 开头的加密串都将被归纳到彩虹表索引为 0 的那一项中。当黑客截取到的加密数据串以 0 为开头时，则只需要通过彩虹表查询到对应的那一组加密串，然后在组内遍历即可，可参照桶排序的原理。彩虹表技术大大提升了字典查找速度。

黑客破译了明文密码，并从字典表攻击升级到效率更高的彩虹表攻击。针对这些攻击手段，防御方可采用加盐的方式，将一段新字符串（盐）与明文数据拼接组成新的源数据，即可避免通用的字典表攻击。除非黑客盗取了盐或者采用笨方法愿意专门制作一个针对某加盐网站的字典表，那么就需要不断地尝试明文与密文的映射。随着防御方不断地更换盐，黑客也需要重新生成字符串，并刷新自己的数据库，这就是黑客机会成本的提高。

1.2 对称加密

或许受到“加盐”的提示，从对称加密开始，有了密钥的概念。密钥用于加密和解密，掌握在数据使用的双方手里，不对外透露。如果密钥泄露，则数据无安全可言。对称加密算法有 DES、3DES、AES、IDEA，推荐使用 AES 和 IDEA。

黑客可以通过选择密文/明文攻击或者唯密文/明文攻击。其原理是要先掌握一定的明文片段、密文信息、加密算法，通过攻击解密服务，可在不知道密钥的情况下解密完整明文。所以，防御者要注意保护明文信息、加密算法类型及密文信息。在网络传输之前，对明文数据使用单向哈希函数做一步数据混淆是不错的选择。

1.3　非对称加密

密钥分为公钥和私钥。解密者先使用随机数算法随机生成一个数据串作为私钥，然后利用私钥通过截取、重组、哈希等操作生成公钥。公钥生成后会被发布出去，加密者拿到公钥加密明文数据，解密者通过自己的私钥解密，外人无法通过公钥解密。非对称加密算法包括 RSA、椭圆曲线加密（ECC）、SM2，区块链普遍使用的是 ECC。非对称加密算法包含随机数算法及公钥生成算法。ECC 的随机数算法从概念上很容易理解，但伪随机的种子发生器是核心，目前使用的是美国国家标准协会（NIST）和美国国家安全局（NSA）发布的标准。公钥生成算法是通过数学模型生成的，特点是正向快速、逆向困难，包括 secp256k1 和 secp256r1[①]两种。secp256k1 是比特币率先使用的；虽然 secp256r1 更有优势，但其也有潜在的漏洞，由于比特币没有使用 secp256r1，因此还有“比特币躲过 secp256r1 子弹”的说法。目前这两种算法 EOS 均支持。

1.4　本章小结

区块链的基础是加密算法。加密算法随着计算机网络场景的不断丰富而发展，最初的加密形态源自单向哈希函数，通过比对密文判断数据准确性，可保护敏感信息不泄露。接着演进出密钥的方式，利用同一把钥匙进行加解密，这就是对称加密算法，也称作单密钥加密算法。后来，密钥又分为公钥和私钥，公钥公开，私钥私有，这就是非对称加密算法。非对称加密算法衍生出很多对区块链非常重要的实用场景，如公钥加密、私钥解密，以及私钥签名、公钥验证。

本章提到了一些区块链相关的名词概念，下文将对这些概念展开讨论并研究其原理。通过这些概念的引导，可以大致描述出一个 EOS 的生态范围。EOS 是第三代区块链产品，值得技术人员深入研究。加密货币是比特币时期区块链最大的应用场景，以太坊为区块链增加了智能合约，EOS 站在巨人的肩膀上，通过更多的创新点，区块链将更加贴近商业和社会，也会有更多的应用场景。

① secp256k1 和 secp256r1 是两种椭圆曲线数学模型，均属于公钥生成算法。