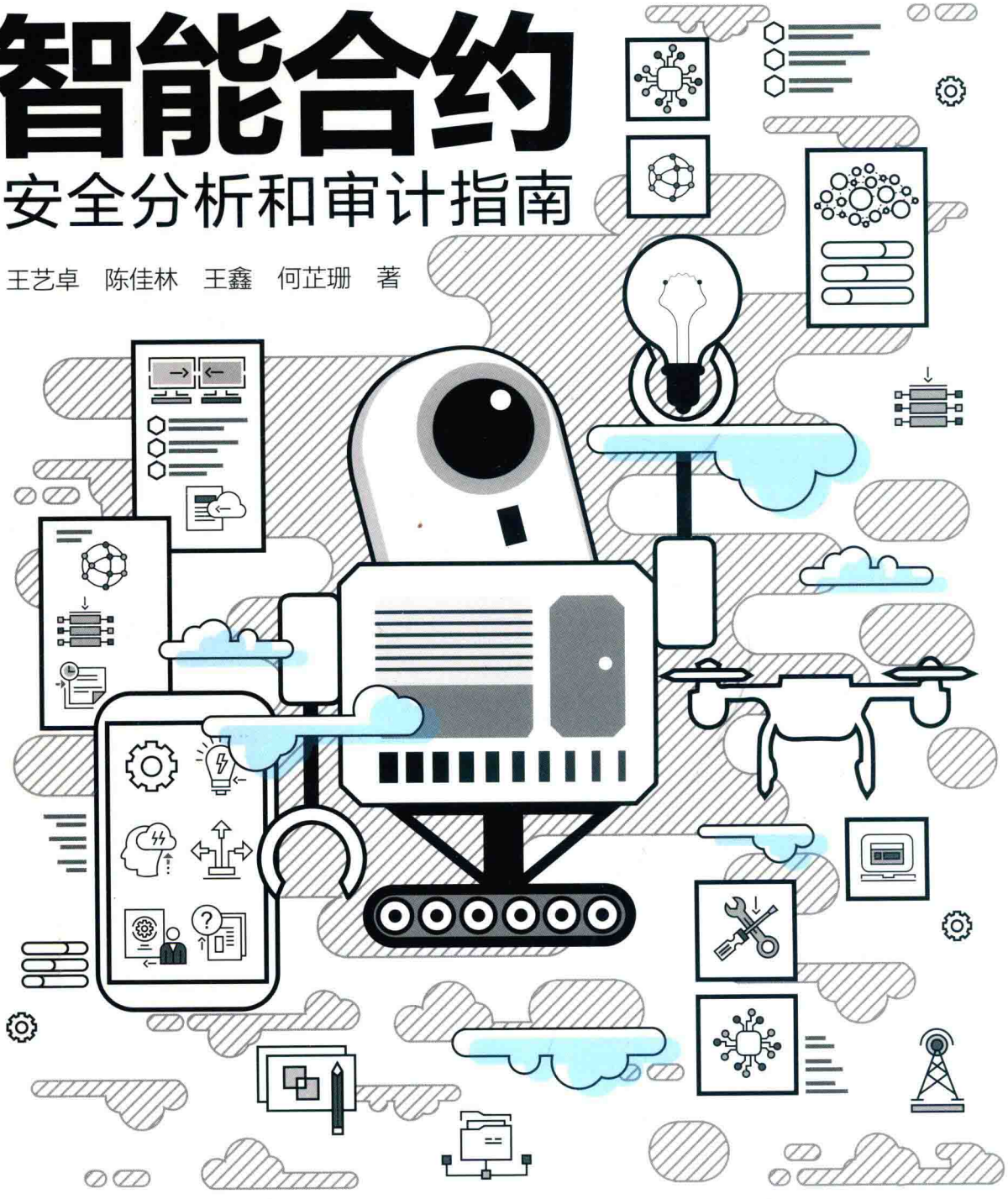
Broadview®
www.broadview.com.cn

看雪 安全技术大系

智能合约

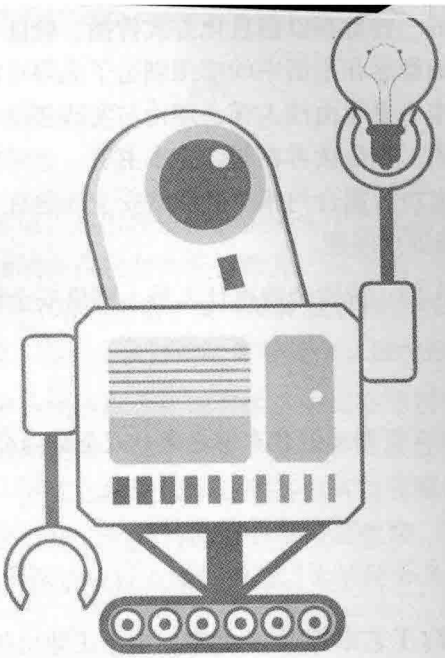
安全分析和审计指南

王艺卓 陈佳林 王鑫 何芷珊 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

安全技术大系



智能合约

安全分析和审计指南

王艺卓　陈佳林　王鑫　何芷珊　著

电子工业出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

智能合约是近年来出现的一种旨在以信息化方式传播、验证、执行合同的计算机协议。尽管可编程的区块链为去中心化的概念在生活中的应用创造了无限可能，但区块链项目的大规模落地与推广仍面临一系列挑战。本书秉承由浅入深、理论与实践相结合的思想，在阐述理论的同时，也对相关操作进行了详细说明。相信读者在阅读完本书后，会对以太坊智能合约有比较完整的了解，更重要的是，会对与以太坊智能合约相关的网络安全问题有充分的认识，并能够在开发和审计过程中积极应对常见的网络安全问题。

本书适合智能合约开发人员、智能合约审计人员、网络安全研究人员，以及对区块链、智能合约感兴趣的读者阅读。

图书在版编目（CIP）数据

智能合约安全分析和审计指南 / 王艺卓等著. —北京：电子工业出版社，2019.8
（安全技术大系）
ISBN 978-7-121-36784-7

Ⅰ. ①智… Ⅱ. ①王… Ⅲ. ①计算机网络—网络安全—研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2019）第 109060 号

责任编辑：潘　昕
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
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：20　　字数：532 千字
版　　次：2019 年 8 月第 1 版
印　　次：2019 年 8 月第 1 次印刷
定　　价：79.00 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至 dbqq@phei.com.cn。

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

序

比特币作为一种新型加密货币，其出现使得区块链去中心化的概念成为密码学研究的热点方向。去中心化本身，则是金融领域现有机制的有益补充，甚至是一大突破。以以太坊为代表的区块链 2.0，作为可编程的区块链去中心化平台，其 EVM 及智能合约的创举，为去中心化在金融、日常生活等领域创造了无限可能。在一个良好的生态环境中，区块链正在茁壮成长。

尽管可编程的区块链为去中心化的概念在现实生活中的应用创造了无限可能，但区块链项目的大规模落地与推广仍面临一系列挑战。除了容量、延迟、拓展性等性能方面的问题，一大制约因素就是区块链的安全问题。一方面，区块链本身的共识机制需要从安全性的角度加以证明；另一方面，自区块链 2.0 出现以来，由于区块链部署的不可更改性，智能合约本身的安全受到了密切关注，DAO 等由于智能合约漏洞造成巨大损失乃至以太坊硬分叉的安全事件，更是将智能合约的安全问题提到了新的高度。

区块链作为当下的热点领域，应用日趋广泛，未来的发展需要安全人才保驾护航。看雪学院（kanxue.com）专注安全领域 20 年，一直致力于培养安全人才、促进产业发展。对于区块链领域，看雪学院也为众多研究者提供了交流、研讨的平台。本书针对区块链 2.0——以太坊，着眼于智能合约安全，进行了深入的分析与探讨，相信对于区块链设计、开发人员，以及未来有志从事区块链领域工作的人士，都会有很大的帮助。

段　钢

看雪学院创始人

2019 年 5 月 9 日

前　言

区块链作为一种去中心化的分布式数据存储结构，以数字加密货币为源头发展至今，在商业、金融、信息等多个领域发挥着重要的作用并受到了普遍的认可，在学术界和产业界掀起了潮流。据相关报道，2019 年 5 月，区块链的总市值达到 2300 亿美元。

以太坊是仅次于比特币的第二大区块链系统。以太坊智能合约的链上编程语言使其不仅仅是一种加密货币，还是一个基于智能合约的去中心化应用程序（DApp）平台。2018 年年底，以太坊已经托管了超过 100 万份智能合约。截至 2019 年 5 月，在全球范围内 2667 个成熟且活跃的分布式应用中，约有 92% 来自以太坊平台。

与比特币的脚本相比，以太坊智能合约作为图灵完备的语言，在拥有功能更为强大、更具拓展性等优势的同时，也因其复杂性产生了诸多安全问题。一方面，由于智能合约编程语言 Solidity 本身缺乏大整数等特性，需要开发人员在编写过程中注重代码的安全性、完整性；另一方面，由于区块链本身的不可更改性，存在漏洞的合约一旦部署上链，就会造成不可逆的损失。以著名的 DAO 攻击事件为例，黑客利用智能合约中的重入漏洞转移了价值约 6000 万美元的以太币，导致以太币的市值一度下跌了 40%。因此，如何保障智能合约的安全性成了区块链落地的关键。

在本书的写作过程中，我们秉承由浅入深、理论与实践相结合的思想，在阐述理论的同时，对实际操作进行了详细说明。

- 第 1 章对区块链的发展历程进行了由浅入深的介绍。借助一个故事，结合经典的《比特币白皮书》，梳理了区块链 1.0 ~ 区块链 3.0 的框架，并对以太坊及其智能合约进行了简单的探讨。
- 第 2 章旨在将区块链和以太坊的概念与实现对应起来。结合实践，对常用的以太坊客户端 geth、钱包、浏览器等应用的操作进行讲解，既提供了命令行环境，也展示了图形界面。
- 第 3 章将智能合约的语法、操作、应用融为一体，不仅介绍了智能合约的语法特性，还详细讲解了如何利用 Truffle 实现代币合约和众筹合约。
- 第 4 章对智能合约的常见漏洞及其原理进行了分析，在 Remix IDE 中对漏洞的代码进行了调试，并针对每一个漏洞给出了相应的防范建议。
- 第 5 章介绍了常见的智能合约蜜罐，结合原理讲解和复现操作，提供了相应的安全建议。
- 第 6 章对现有智能合约分析与审计工具的使用进行了说明。
- 第 7 章介绍了智能合约的审计流程，并提供了审计案例。
- 第 8 章深入以太坊虚拟机的运行机制，介绍了智能合约是如何部署和执行的。

相信读者在阅读完本书后，会对以太坊智能合约有较为完整的了解，更重要的是，会对以太坊智能合约的安全问题有更加充分的认识，能够在开发和审计过程中发现并识别常见的漏洞和蜜罐。本书覆盖面虽广，但内容由浅入深、通俗易懂，同时不乏深度的思考。例如，智能合约审计工具的研发是研究的热点，智能合约字节码的解构能力是在以太坊上进行开发的敲门砖。

在本书的编写过程中，我们得到了来自家人、同事、朋友及看雪区块链研究社区的支持和鼓励，在此表示感谢！

最后，希望本书能为推动区块链的落地和技术的进步作出微薄的贡献。

作　者

2019 年 6 月于上海

目　录

第 1 章　由浅入深理解区块链

第 2 章　智能合约开发实战

第 3 章　智能合约语法实战

第 4 章 智能合约常见漏洞

第 5 章 智能合约蜜罐

第 6 章　常见智能合约分析与审计工具

第 7 章　智能合约审计实战

第 8 章　智能合约字节码解构

第1章　由浅入深理解区块链

1.1　区块链简介

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。所谓“共识机制”，是指区块链系统中负责在不同节点之间建立信任、获取权益的数学算法，它从根本上避免了引入可信任第三方的问题。

在最初，区块链是比特币（BTC）的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术使用。区块链是一个使用密码学方法，通过关联而产生的数据块，每一个数据块中都包含一笔比特币网络交易的信息，用于验证信息的有效性（防伪）和生成下一个区块。

随着以太坊、DApp 等的诞生与发展，区块链的技术也得到了更新和拓展。打个比方，区块链就好比机动车的发动机，1.2 节将要介绍的区块链 1.0 就好比摩托车（比特币）的发动机，1.3 节将要介绍的区块链 2.0 就好比小轿车（以太坊）的发动机，1.4 节将要介绍的区块链 3.0 就好比大巴车（DApp）的发动机——作为发动机的区块链技术是不断发展、进步的。

接下来，我们就来回顾和梳理区块链的发展历程。

1.2　区块链 1.0——比特币，一种点对点的现金支付系统

1.2.1　比特币的产生

为了理解比特币，我们不妨通过一个故事来了解一下比特币及其作为一种支付系统的特别之处。我们通过虚构一个村庄“比特村”，看看这个村庄所使用的货币的发展历程。

1. 以物易物

比特村与世隔绝、自给自足，村民们一直过着以物易物的生活，交易的形式基本上就是老王用一袋面粉换老何的一头羊。

2. 实物货币

由于以物易物存在诸多不便，比特村便召开村民大会，讨论如何解决这个问题。有人提议：以便于分割且稀有的东西作为一般等价物，用其作为交易的衡量物。于是，村民们选定了黄金，并确定了每种物品相对于黄金的价值，例如一克黄金换一头羊。

3. 符号货币

由于开采金矿费时费力且成本很高，加上黄金容易磨损或丢失，有人提议：在交易时并不一定要使用实物黄金，可以在一张纸上写“一克黄金”来代表一克黄金。但是，黄金的价值源于其开采和冶炼的成本及稀有性，因此，如果想用“纸”来代替黄金，就需要由第三方来控制“纸”、确定什么样的“纸”是有效的及“纸”的发行量。于是，村民们推举德高望重的老村长担任这个第三方角色，由老村长在纸上写字作为纸币，按各家拥有的黄金的数量将纸币发给各家，即：老村长收回黄金并将相应数量的纸币发给村民。从此，村民们就可以用黄金和老村长兑换相应价值的纸币，或者用磨损的纸币换取新的纸币了。老村长严格遵守销毁多少纸币就新写多少纸币的规则，从而控制纸币的数量，防止出现通货膨胀。

从此，比特村进入了符号货币时代。

4. 中央系统虚拟货币

过了几年，老村长由于终日忙于核对新旧纸币、记录账目，过于辛劳而去世，比特村的村民们再次开会商讨。老村长的儿子小村长自告奋勇接下父亲的任务。他发现，不用写那么多纸币，只要把村民手中的纸币收回并销毁，同时在账簿上记录每位村民交来的纸币的数量（对应于该村民拥有多少黄金），以后村民需要支付时，给自己打个电话，自己在账簿上记录这个村民的名下应该扣掉多少黄金，就算支付成功了。

比特村进入了中央系统虚拟货币时代，不再使用实物货币（纸币）支付，支付过程变成了小村长账簿上数字的变更。

5. 分布式虚拟货币——主角登场

某日，小村长头脑一热，心想：账簿在我手上，我岂不可以私自划分？于是，他私自从老张账下划了 10 克黄金给自己。后来，事情败露，小村长被赶下了台。比特村再次召开大会，商讨如何进行支付，并指出了货币体系完全交由第三方集中管理的安全隐患。这时，一个自称“中本聪”的“宅男”科学家登场，提出了一套新的货币体系。

（1）对现有账簿进行改造

账簿上不再记录每个村民的余额，改为记录每一笔交易，包括付款人、收款人、交易金额。那么，只要账簿初始状态确定、每笔交易可靠并按时间排序，就可以推算出每个人持有的金额。

账簿由私有改为公开，只要村民需要，就能获得当前完整的账簿。那么，接下来需要解决的就是由账簿公开带来的隐私问题。

（2）引入身份与签名机制（公钥加密系统）

中本聪提出：在交易中，每个人不使用真名，而采用唯一的代号。另外，他发给每位村民一个保密印章和一个印章扫描器。保密印章是唯一的且包含一串肉眼不可见的字符，用于在纸上盖章，他人无法通过观察来仿制这个印章。印章扫描器用于扫描印章中隐含的那串字符，从而获得保密印章所有人的信息。这样，村民们就可以在不暴露身份的情况下进行交易了。

（3）成立虚拟矿工组织（挖矿群体）

中本聪面向全村招募虚拟矿工。矿工以小组为单位，每天要花一定的时间进行比特币挖矿活动（不同于挖金矿，虚拟矿工只要在家中就可以完成任务），有一定的可能性获得报酬，且挖矿付出的努力越多，报酬就越高。新矿工可以随时加入，老矿工可以随时退出。

（4）建立初始账簿

中本聪将小村长的那本账簿中记录的黄金余额还给村民，并销毁了那本账簿，然后拿出了一本新的账簿，在第一页记录了初始信息。在初始信息中，付款人均为“系统”，收款人为每个保密印章所对应的隐含字符，代表初始时刻系统为每位用户默认分配的比特币。不过，在初始时刻大家的比特币数量都很少，只有几个，一些“不幸”的村民甚至没有分配到比特币。当然，中本聪也表示，自己没有权力让所有村民都接受这个体系，然而，随着比特币的流通与矿工工作量的积累，比特币会越来越多、越来越普及。

（5）交易与支付

交易与支付的步骤，具体如下。

①付款人签署交易单。

以老王付给老何 10 个比特币为例。为了支付 10 个比特币，老王需要老何的标识字符串，例如“ABCDEFG”。同时，老王也有一个标识字符串，例如“HIJKLMN”。老王写了一张单子，内容为“HILKLMN 支付 10 个比特币给 ABCDEFG”，用自己的保密印章盖一个章，然后将这张单子交给老何。为了便于追溯，还要在单子里注明这笔钱原本记录在账簿的哪一页。在这张单子上，老王的 10 个比特币来自建立账簿时系统的赠送，记录在账簿的第一页。

②收款人确认单据签署人。

老何拿到这张单子后，需要确认这张单子是由“HIJKLMN”这个人（也就是老王）签署的。于是，老何拿出印章扫描器来扫描印章。如果扫描器显示的字符和付款人的字符一致，就可以确认这张单子是由付款人签署的了。这是因为，根据保密印章机制，没有人可以伪造印章，任何人只要扫描印章，都可以确认单子的付款人和盖章人是否一致。

③收款人确认付款人的余额。

通过保密印章，收款人虽然可以确认付款人签署了这张单子，但无法自行确认付款人是否有足够的金额用于支付。从前，小村长负责检查付款人的余额并通知收款人交易是否有效，而现在，村民们把小村长“开除”了，谁来负责记账和确认每笔交易的有效性呢？

中本聪设计的这个系统是一个分布式货币系统，不依赖任何中央人物，所以不会由一个或少数几个人来承担任务，最终承担任务的是矿工组织。

（6）矿工的工作

矿工使用的工具，列举如下。

- 每个矿工小组先要自己复制一份初始账簿和若干张空白账簿纸。初始账簿中只有一页，记录了系统在初始时刻赠送比特币的情况。空白的账簿纸上只有账簿结构，大致包括“交易单”“本账单编号”“上一张账单编号”“幸运数字”四个字段，但没有内容（内容的书写规则将在后面讲解）。
- 编码生成器（散列函数）。中本聪向矿工组织中的每个小组分发若干个编码生成器，将一张填好内容的账簿纸放入这个机器，机器就会在账簿纸的“本账单编号”栏中自动打印一串由 0 和 1 组成的编号（共 256 位）。编码生成器的功能包括：生成的编号仅与账簿纸上填写的内容有关，与填写人、字体、填写时间等均无关；内容相同的账簿纸生成的编号总是相同的，但是，哪怕只修改了账簿纸上的一个字符，编号都会变得不同；编码生成器在打印编码时需要读取所有填在账簿纸上的交易单，机器会核对该交易单与填入的交易单的一致性，尤其是保密印章，如果发现保密印章和付款人不一致，将拒绝打印编号；将一张打印完成的账簿纸放入机器，机器会判定这张账簿纸是否是由有效的机器打印的，并判定其编号和内容是否一致（这个编号是无法伪造的）。
- 交易单收件箱与公告板。每个矿工小组都要在门口挂一个箱子来收集交易单。另外，需要一个公告板来公示一些信息。

矿工的工作流程如下。

①收集交易单。

中本聪规定，每笔交易的发起人，不仅要将交易单发给收款人，还要同时复制若干份一模一样的交易单并将其投递到每个矿工小组的收件箱里。矿工小组的成员要定期到自己的收件箱里把收集到的交易单取出来。

②填写账簿。

矿工小组的成员拿出一张空白账簿纸，把这些交易填到“交易单”栏中，同时找到当前账簿的最后一页，将该页的编号抄写到“上一张账单编号”栏中。还有一个“幸运数字”栏，在这里可以随便填写一个数字，例如 12345。然后，将写好的账簿纸放入编码生成器，打印编号。这样，一张账簿纸就写完了。

体现工作量的时候到了。中本聪有个“变态”的规定：只有编号的前 10 位数字均为 0，这张账簿纸才算有效。

根据之前对编码生成器的描述，要想修改编号，只能修改账簿纸上的内容，而“交易单”和“上一张账单编号”两栏中的内容是不能随便修改的，那么，只能修改“幸运数字”栏的内容了。为了生成有效的账簿纸，矿工需要不断抄写账簿纸（每张账簿纸上的“幸运数字”都不同），然后将账簿纸放入编码生成器，如果生成的编号不符合规定，这张账簿纸就作废了——重复这个过程，直到生成一串有效的编号。如果编号中的每个数字都是随机的，那么平均要写大约 1000 张“幸运数字”不同的账簿纸，才能获得一个有效的编号。

还记得之前说过，矿工是有报酬吧？这就是矿工工作的动力。中本聪规定：每一张账簿纸上的交易单的第一条交易为“系统给这个小组支付 50 个比特币”。也就是说，如果一位矿工生成了一张有意义的账簿纸，且这张账簿纸被所有的矿工小组接受了，就意味着这条交易被接受了，这位矿工所在的小组将获得 50 个比特币。

这就是矿工被称作“矿工”的原因，也是之前说的“随着比特币的流通与矿工工作量的积累，比特币会越来越多、越来越普及”的原因。

③确认账簿。

当某矿工小组幸运地生成了一张有意义的账簿纸的时候，为了得到奖励，必须立刻请其他小组确认自己的工作。所以，这个矿工小组必须将有效的账簿纸誊抄很多份，快马加鞭送到其他小组的交易单收件箱中请求确认。

中本聪规定，当某个矿工小组收到其他小组送来的账簿纸时，必须立即停下手里的挖矿工作，进行账簿纸的确认。需要确认的信息有三个：账簿纸的编号有效；账簿纸的前一页账簿纸有效；交易单有效。

对收到账簿纸的矿工小组来说，如果完成了上述所有验证且全部通过，就表示确认上述账簿纸有效。然后，将这张账簿纸并入自己的主账簿，舍弃目前正在进行的工作，后面的挖矿工作会基于更新后的主账簿来进行。

④账簿确认反馈。

对一个矿工小组来说，把账簿纸送出后，如果收到了其他小组送来的账簿纸，其“上一张账单编号”为自己之前送出的账簿纸的编号，就表示他们的工作成果被其他小组认可了（因为已经有矿工小组基于他们的账簿纸继续工作了）。此时，基本可以认为该矿工小组已经得到了 50 个比特币。

另外，当任何一个矿工小组生成了一张新的有效账簿纸或者确认了其他矿工小组的账簿纸时，都要将最新被承认的交易写到公告牌上。收款人只要发现相关交易被各矿工小组认可了，基本上就可以认为这笔钱已经到了自己的账上，此后就可以在付款时将钱的来源指向这笔交易了。

1.2.2　深入分析比特币的工作机制

基于 1.2.1 节中的故事，我们继续分析比特币这种分布式虚拟货币的运行机制。

1. 情况一：同时收到两张合法的账簿纸

在前面介绍的运行机制中，各个矿工小组是并行工作的，因此完全有可能出现这样的情况：某矿工小组收到两张不一样的账簿纸，它们都基于当前这个小组的主账簿的最后一页，内容也都完全合法。这时该如何操作？

中本聪认为：矿工小组不应该以线性结构来组织账簿，而应该以树状结构来组织账簿，在任何时刻，都要以当前最长分支为主账簿，但要保留其他分支。

举个例子，某矿工小组同时收到 A、B 两张账簿纸，经核算，它们都是合法的。此时，该小组应该将这两张账簿纸以分支的形式组织起来，如图 1.1 所示，黑色的结构表示当前账簿的主干。

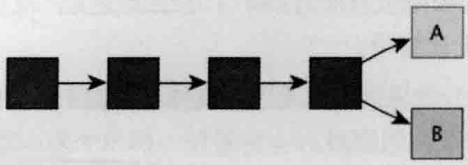


图 1.1

任意选择一张账簿纸作为当前的主分支，例如 A，如图 1.2 所示。

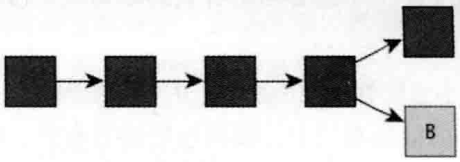


图 1.2

如果有一张新的账簿纸是基于 A 的，那么主分支就可以延续下去，如图 1.3 所示。如果主分支一直这么延续下去，就表示大家基本都以它为主干，另一个分支就会被遗忘。

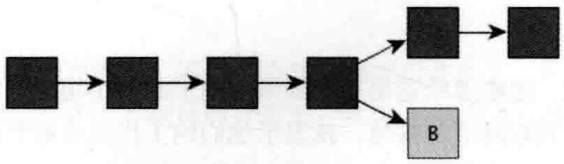


图 1.3

当然，也有一种可能，就是 B 所在的分支变得更长，如图 1.4 所示。

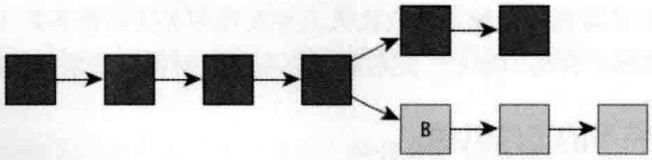


图 1.4

此时，就要以 B 所在的分支为主干，基于这个分支进行后续的工作，如图 1.5 所示。

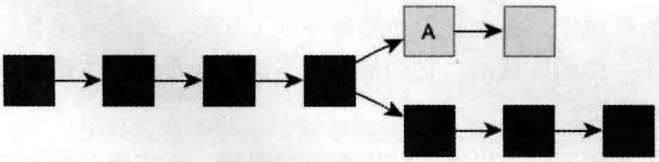


图 1.5

从局部来看，虽然在某一时刻各个小组的账簿主干可能不一致，但大方向是一致的，那些偶尔由于不同步而产生的分支将很快被遗忘。

2. 情况二：矿工小组中有人试图伪造账簿

中本聪认为：只要大多数矿工是诚实的，这个系统就是可靠的。这句话也可以理解为：只要大多数 CPU 的计算能力都没有联合起来对全网进行攻击，那么那些诚实的节点将会生成超过攻击者链条长度的最长链条。

基于保密印章机制，编码生成器在打印编号时会核对所有交易单的保密印章，如果保密印章和实际付款人不一致，就会拒绝打印，所以，没有人能伪造他人的身份来付款。同时，诚实的矿工也不会承认不合法的交易（例如，在某笔交易中，付款方的余额不够）。因此，只有一种可能存在的攻击行为：当收款人确认收款后，在另一条分支上建立另外一张交易单，然后取消之前的付款，将同一笔钱付给另一个人（Double-Spending 问题）。下面用一个例子来说明这个问题。

假设攻击者拥有 10 个比特币，他准备将这笔钱同时付给受害者 A 和受害者 B，并得到两位受害者的承认。

①攻击者准备从受害者 A 手里购买价值 10 个比特币的黄金。攻击者与受害者 A 签署了交易单，然后将 10 个比特币转给受害者 A。

②这笔交易在最新的账簿纸中被确认，这一消息由各个矿工小组通过公告发布。受害者 A 看到公告，确认比特币到账，将与 10 个比特币等值的黄金交给攻击者。

③攻击者找到账簿，在包含刚才那笔交易的账簿纸的前一页上建立一个分支，生成了更多的账簿纸，使这个分支的长度超过了之前分支的长度。因为此时由攻击者制造的分支变成了主干分支，所以矿工组织不再承认刚才的转账，受害者 A 得到 10 个比特币的交易单被取消了。

④攻击者与受害者 B 签署交易单，将从受害者 A 那里拿回的 10 个比特币付给受害者 B。受害者 B 确认比特币到账后，将等值的黄金支交给攻击者。

至此，攻击者两次花费手里的 10 个比特币，分别从两名受害者那里购买了等值的黄金。攻击者还可以如法炮制，取消对受害者 B 的转账，将这 10 个比特币支付给其他人。

整个过程，如图 1.6 ~ 图 1.9 所示。

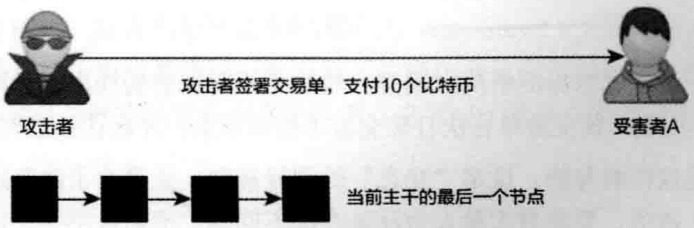


图 1.6