国之重器出版工程

网络强国建设

国家网络空间安全能力提升系列

In-depth Exploration of Blockchain

深入探索区块链

李洪涛　曾宇　延志伟　南斗玄　编著

中国工信出版集团　人民邮电出版社 POSTS & TELECOM PRESS

国之重器出版工程

网络强国建设

国家网络空间安全能力提升系列

深入探索区块链

In-depth Exploration of Blockchain

李洪涛　曾宇　延志伟　南斗玄　编著

人民邮电出版社

北京

图书在版编目（CIP）数据

深入探索区块链 / 李洪涛等编著. -- 北京 : 人民邮电出版社有限公司, 2019.7
（国家网络空间安全能力提升系列）
国之重器出版工程
ISBN 978-7-115-50765-5

Ⅰ. ①深… Ⅱ. ①李… 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022830号

内 容 提 要

区块链作为多种网络与安全技术的融合创新，为信息和价值在不可信网络中对等体之间的传递提供了途径，其去中心化思想与机制正引领全球新一轮技术创新和产业革命。本书全面剖析区块链技术体系，不仅深入阐述区块链中的密码学技术、区块验证方法、分叉问题、安全保障及共识机制等核心要素，而且对当前区块链国内外标准化发展和应用态势进行了介绍。

本书适合科研机构、金融机构的人员以及高等院校相关专业的师生阅读。

◆ 编　　著　李洪涛　曾　宇　延志伟　南斗玄
责任编辑　邢建春
责任印制　杨林杰

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：710×1000　1/16
印张：18.75　　2019 年 7 月第 1 版
字数：347 千字　　2019 年 7 月河北第 1 次印刷

定价：138.00 元

读者服务热线：(010)81055493　印装质量热线：(010)81055316
反盗版热线：(010)81055315

《国之重器出版工程》
编辑委员会

专家委员会委员（按姓氏笔画排列）：

于　全　中国工程院院士

王少萍　“长江学者奖励计划”特聘教授

王建民　清华大学软件学院院长

王哲荣　中国工程院院士

王　越　中国科学院院士、中国工程院院士

尤肖虎　“长江学者奖励计划”特聘教授

邓宗全　中国工程院院士

甘晓华　中国工程院院士

叶培建　中国科学院院士

朱英富　中国工程院院士

朵英贤　中国工程院院士

邬贺铨　中国工程院院士

刘大响　中国工程院院士

刘怡昕　中国工程院院士

刘韵洁　中国工程院院士

孙逢春　中国工程院院士

苏彦庆　“长江学者奖励计划”特聘教授

苏哲子　中国工程院院士

李伯虎　中国工程院院士

李应红　中国科学院院士

李新亚　国家制造强国建设战略咨询委员会委员、中国机械工业联合会副会长

杨德森　中国工程院院士

张宏科　北京交通大学下一代互联网互联设备国家工程实验室主任

陆建勋　中国工程院院士

陆燕荪　国家制造强国建设战略咨询委员会委员、原机械工业部副部长

陈一坚　中国工程院院士

陈懋章　中国工程院院士

金东寒　中国工程院院士

周立伟　中国工程院院士

郑纬民　中国计算机学会原理事长

郑建华　中国科学院院士

屈贤明　国家制造强国建设战略咨询委员会委员、工业和信息化部智能制造专家咨询委员会副主任

项昌乐　“长江学者奖励计划”特聘教授，中国科协书记处书记，北京理工大学党委副书记、副校长

柳百成　中国工程院院士

闻雪友　中国工程院院士

徐德民　中国工程院院士

唐长红　中国工程院院士

黄卫东　“长江学者奖励计划”特聘教授

黄先祥　中国工程院院士

黄　维　中国科学院院士、西北工业大学常务副校长

董景辰　工业和信息化部智能制造专家咨询委员会委员

焦宗夏　“长江学者奖励计划”特聘教授

前　言

区块链技术作为密码学、P2P 网络、共识机制、分布式数据存储等多种技术的融合创新，为信息和价值在不可信网络中对等体之间的传递提供了途径，迅速成为近几年来各国及相关组织研究讨论的热点。业界在不断深度挖掘区块链技术的同时，推动与产业的纵深度结合，旨在将其转化为现实生产力。

习近平总书记多次强调“核心技术是国之重器”“要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破”。为此，中国区块链技术和产业发展论坛于 2016 年发布《中国区块链技术和应用发展白皮书（2016）》，工业和信息化部信息中心于 2018 年发布《2018 年中国区块链产业白皮书》，《“十三五”国家信息化规划》将区块链技术纳入重点前沿技术，国家互联网信息办公室于 2019 年 1 月发布《区块链信息服务管理规定》，这足以说明国家层面对区块链技术的重视程度。区块链技术去中心化的思想正在引领着全球新一轮技术创新和产业革命，目前已在征信、金融、供应链、产品溯源、版权保护等领域尝试应用，以期为社会管理和经济发展注入新活力。

本书首先从经典拜占庭问题入手，通过实际场景介绍如何在分布式对等条件下建立信任关系，这也是区块链技术的核心；其次详细介绍目前最广泛的区块链应用——比特币，包括比特币区块结构、交易结构和构建、交易脚本等；随后抽象到技术层面剖析区块链中的密码学知识、区块验证、分叉、区块链安全、共识机制等核心要素，对以太坊和超级账本等当前主流区块链项目进行介绍；最后概述当前区块链在国内外的标准化进程以及应用态势。

由于区块链仍然是一种年轻且正在成长的技术，其各方面的参考资料有限，本书在编写过程中借鉴了许多来自开源社区、公开“白皮书”和学术论文等的资料及案例，这里对提供区块链知识分享的前辈以及在此领域深耕的专家学者和创业者表示感谢。特别要声明的一点是，区块链技术体系仍不够成熟，且其发展演进快速，因此本书中阐述的技术细节可能存在瑕疵不足或纰漏错误，也因为笔者水平有限和参考资料不足使在某些方面的介绍深度和广度不够，笔者后续会持续深入地跟进区块链技术研究，进一步完善研究成果，欢迎读者提出宝贵的意见和建议。

作 者

2019 年 4 月 15 日

目 录

第1章
从拜占庭将军问题说起

拜占庭将军问题是描述分布式系统一致性问题的经典案例，由莱斯利·兰伯特（Leslie Lamport）等于 1982 年首次提出，其核心思想是多个军队在可能有叛徒发布虚假消息的情况下，如何保持进攻或撤退的一致性。由于其设置的场景与计算机领域的分布式系统协同关系具有一定关联，进而发展成一种分布式容错理论。本章主要通过对拜占庭将军问题的分析和解读，引出区块链技术作为分布式系统一致性问题的解决方案。

比特币自 2008 年由中本聪提出发展至今，已成为最具代表性的去中心化现金系统。去中心化是指在比特币系统中，各个用户权利对等，没有银行或者支付宝这种第三方权威的存在。然而，缺少了认证机构，货币面临的最大的两个问题是双花（Double Spending）问题和拜占庭问题。

“双花”很好理解，就是一笔现金被支付多次。而拜占庭问题又是什么？拜占庭问题实质上是一个分布式下的共识问题，在比特币系统没有第三方机构的情况下，演变成为大家如何认同同一个账本，并在这个账本上添加后续的交易。

拜占庭问题首先由 Leslie Lamport 等在 1982 年提出，被称为拜占庭将军问题（The Byzantine Generals Problem 或者 Byzantine Failure），其核心描述是多个军队在可能有叛徒发布虚假消息的情况下，如何保证进攻的一致性，由此引申到计算领域，发展成了一种容错理论。随着比特币的出现和兴起，这个著名问题重入大众视野。

1.1 拜占庭将军问题场景与实质

关于拜占庭将军问题，一个简易的非正式描述如下。

拜占庭帝国想要进攻一个强大的敌国，为此派出了十支军队去包围敌国。这个敌国虽不比拜占庭帝国强大，但也足以抵御五支常规拜占庭军队的同时袭

击。基于某些原因，这十支军队不能集合在一起进行单点突破，必须在分开的包围状态下同时攻击。他们任何一支军队单独进攻都毫无胜算，除非有至少六支军队同时袭击才能攻下敌国。他们分散在敌国的四周，依靠通信兵相互通信来协商进攻意向及进攻时间。困扰这些将军的问题是，他们不确定其中是否有叛徒，因为叛徒可能擅自变更进攻意向或者进攻时间。在这种状态下，拜占庭将军们能否找到一种分布式的协议让他们能够远程协商，从而赢取战斗？这就是著名的拜占庭将军问题。简单来说就是：n 个将军被分隔在不同的地方，忠诚的将军希望通过某种协议来达成某个命令的一致（如一起进攻或者一起后退），但其中一些背叛的将军会通过发送错误的消息阻挠忠诚的将军达成命令上的一致。

1.2　问题分析与证明

描述拜占庭问题的原始论文是通过口头和书面两种消息传递方式来分析的，将军也分为发令者和副官。

1.2.1　通过口头消息

只通过口头的方式传递消息，可以达成一致的前提为：如果有 m 个叛国将军，则将军的总数必须为 $3m+1$ 个以上。

下面是口头消息传递过程中默认的一些条件。

A1：每个被发送的消息都能够被正确地投递。

A2：信息接收者知道是谁发送的消息。

A3：能够知道缺少的消息。

A1 和 A2 假设两个将军之间通信没有干扰，即不会有背叛者阻碍消息的发送（截断），也不会有背叛者伪造他人消息的情况，每个将军都可以无误地将自己的消息发送给其他将军。

我们定义口头消息算法 OM(m)。对于所有的非负整数 m，每个发令者通过 OM(m) 算法发送命令给其他 $n-1$ 个副官。下面解释说明 OM(m)算法在最多有 m 个背叛者且总将军数至少为 $3m+1$ 的情况下，为何能解决拜占庭将军问题。

算法定义一个函数 majority(com1, com2,⋯,com$N$)，表示重复次数最多的命令。

OM(0)算法描述如下（初始设置）。

（1）发令者将他的命令发送给每个副官。

（2）每个副官执行他从发令者得到的命令，如果没有收到任何命令，则默认为撤退。

OM(m)算法描述如下（中间过程）。

（1）发令者将他的命令发送给每个副官。

（2）对于每个 i，vi 是每个副官 i 从发令者收到的命令，如果没有收到命令，则为撤退命令。副官 i 在 OM(m−1)中作为发令者将 vi 发送给另外 n−2 个副官。

（3）对于每个 j，并且 $j\neq i$，vj 是副官 j 从第（2）步中副官 i 发送来的命令（使用 OM(m−1)算法），如果没有收到第（2）步中副官 i 的命令，则默认为撤退命令。最后副官 j 使用 majority(v1,⋯,vN−1)得到最终指令。

可能算法在描述上比较复杂，但是结合图例大家就能很清晰明了地理解。我们来考虑一个 n=4，m=1 的情况。

1. 副官 D 是背叛者

第一步：发令者 A 执行算法 OM(1)将自己的命令发送给 3 个副官 B、C、D，3 个副官都正确地收到了命令，如图 1-1 所示。

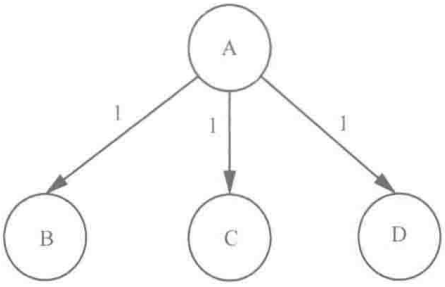

图 1-1　发令者发送命令（D 为背叛者）

第二步：每个收到命令的副官都作为发令者执行算法 OM(1)，将自己收到的命令转发给其余副官，因为副官 D 是背叛者，所以他给副官 B 和 C 传递的消息可能是假消息，如图 1-2 所示。副官 B 和 C 分别根据 majority 函数决定命令。

根据判定函数，B、C 最后得到的结果都是 1（与发令者相同）。因此，背叛的副官 D 无法干扰发令者的决定。那如果发令者是背叛者呢?

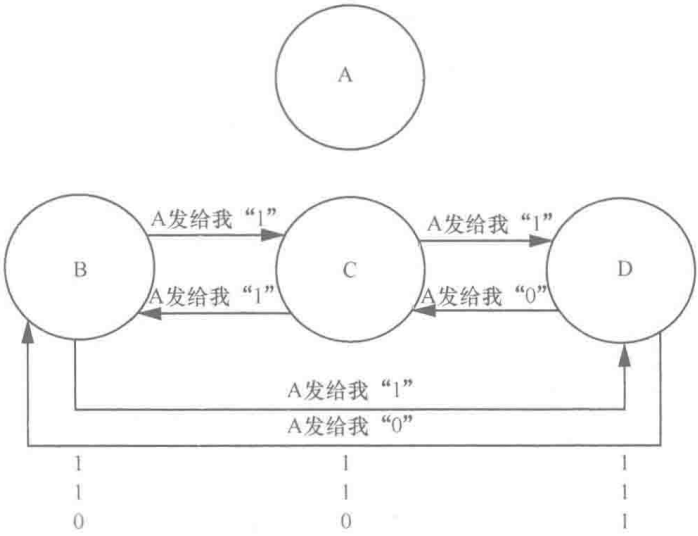

图 1-2　副官转发命令（D 为背叛者）

2. 发令者是背叛者，其余副官是忠诚的

第一步：发令者 A 向副官 B、C、D 发送不同的命令，如图 1-3 所示，这在实际情况中就是一个攻击者向不同方发送了不一致的值（如 0 或 1），企图扰乱副官做出一致决定。

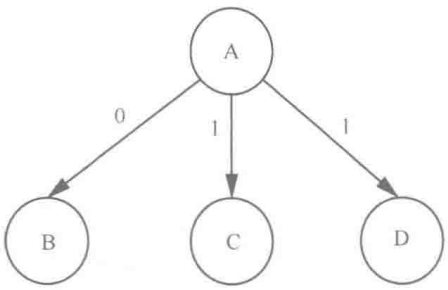

图 1-3　发送者发送命令（A 为背叛者）

第二步：副官收到命令后，变为发令者执行 OM(1)向所有的副官发送命令，如图 1-4 所示。通过多数表决算法，可以看到，副官最后仍可达成一致的命令。

这里没有提到多叛徒的形式，感兴趣的读者可以自己查阅原始文献。Lamport 证明了在采用口头协议的情况下，将军总数大于 $3m$、背叛者为 m 或者更少时，忠诚的将军可以达成命令上的一致。

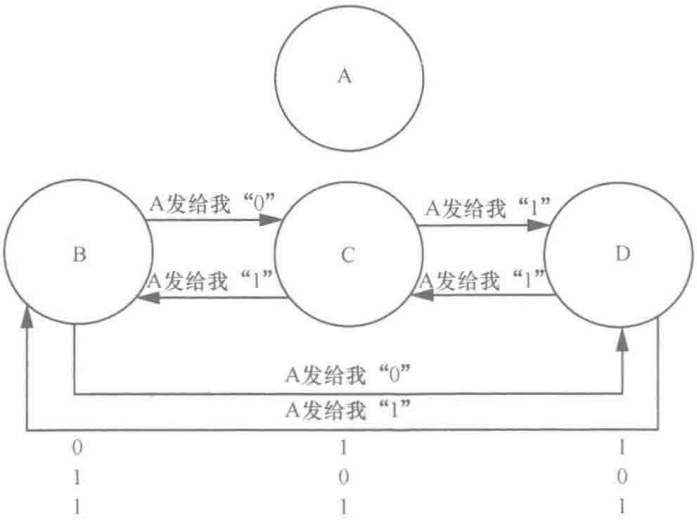

图 1-4　副官转发命令（A 为背叛者）

1.2.2　通过书面消息

通过以上描述可以看到：口头协议这种传递方式最大的缺点是消息不能溯源。那我们是否可以加入某些规则，让信息可以追本溯源，从而改变现状？这就是书面消息引入的灵感。

我们在口头消息 A1~A3 这 3 点要求的基础上，加入新的条件 A4，使之成为书面消息。

A4：① 签名不可被伪造，一旦被篡改即可发现；

② 任何人都可以验证将军签名的可靠性。

先说结论：对于任意 m，最多只有 m 个背叛者的情况下，算法 SM(m)能解决拜占庭将军问题。也就是说，SM(m)算法一定可以使忠诚的将军达成一致（但这个一致的结果并不一定正确）。

回顾下拜占庭将军问题的要求。

IC1：所有忠诚的副官都遵守一个命令，即一致性。

IC2：若发令者是忠诚的，每一个忠诚的副官遵守他发出的命令，即正确性。

我们要找到一个算法 SM(m)，使不管将军总数 n 和叛徒数量 m 是多少，只要采用该算法，忠诚的将军总能达成一致甚至正确（即上面的 IC1 和 IC2）。我们用集合 Vi 表示 i 副官收到的命令集，这是一个集合，也就满足互异性（没有重复的元素）