区块链技术丛书

主编◎孙 溢 / 副主编◎张 引 余恪平

区块链安全技术

Blockchain Security Technology

本书作者及顾问团队是国内区块链技术和应用领域的深度实践者

北京邮电大学出版社
www.buptpress.com

区块链技术丛书

区块链安全技术

主　编　孙　溢
副主编　张　引　余恪平

北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书首先简要介绍了区块链，从其本质、特性到其发展，力求通俗易懂，力求带给读者一个清晰的形象化的理解；接着将区块链所涉及的基础知识、相关协议以及算法进行梳理；随后从区块链基础架构出发，逐层分析其脆弱性，对区块链安全问题进行系统解析；然后将作者及其团队一直致力于攻关的也是国内外研究热点问题——区块链信任问题及解决信任问题的核心技术进行分析介绍，希望能够为广大读者提供一个新视角；再然后结合区块链应用实例，介绍区块链应用中所涉及的安全问题及其解决方案和应用实例；最后介绍区块链相关的政策和法律法规，以便读者全方位了解并能在法律法规的指导下正确应用区块链技术。

图书在版编目(CIP)数据

区块链安全技术 / 孙溢主编. -- 北京 ：北京邮电大学出版社，2021.7

ISBN 978-7-5635-6404-0

Ⅰ. ①区… Ⅱ. ①孙… Ⅲ. ①区块链技术—安全技术 Ⅳ. ①TP311.135.9

中国版本图书馆 CIP 数据核字(2021)第 131665 号

策划编辑：姚 顺 刘纳新 **责任编辑**：刘 颖 **封面设计**：七星博纳

出版发行：北京邮电大学出版社

社 址：北京市海淀区西土城路 10 号

邮政编码：100876

发 行 部：电话：010-62282185 传真：010-62283578

E-mail：publish@bupt.edu.cn

经 销：各地新华书店

印 刷：唐山玺诚印务有限公司

开 本：720 mm×1 000 mm 1/16

印 张：18.75

字 数：296 千字

版 次：2021 年 7 月第 1 版

印 次：2021 年 7 月第 1 次印刷

ISBN 978-7-5635-6404-0 定价：48.00 元

// 孙溢

博士，毕业于北京邮电大学，长期从事信息安全及应用方面的研究，作为团队学术科研负责人带领和指导团队博士生、硕士生致力于解决区块链安全问题，主要研究方向包括网络安全、保护隐私的数据共享、区块链安全等，主持和参与了包括国家自然科学基金青年科学基金、国家重点研发计划-子课题、国家高技术研究发展计划（863计划）等多个科研项目，并在多个高水平国际期刊发表科研论文，获得“国防科研优秀教师”荣誉称号。

区块链技术丛书

《揭秘区块链》

陈晓华　刘　彬 ◎编著

《区块链性能提升技术》

杨耀东　周　期　杜　挺 ◎编著

《区块链技术的应用实践》

姜景锋　李　军 ◎编著

《区块链思维》

高泽龙　吕　艳 ◎著

《区块链安全技术》

主编 ◎孙　溢

区块链技术专业交流群
群号：801165674

前 言

作为一项近年来备受关注的技术，区块链的快速发展及广泛普及为其在金融、医疗、物联网等诸多领域的应用提供了坚实基础。正因其去中心化、公开透明、不可篡改等特性，区块链在多方场景中具有显著优势和巨大潜能，成为构建多方信任基础的重要技术。

区块链是按时间顺序以哈希值连接的数据区块的链式结构，其本质是通过去中心化方式利用密码学技术实现安全可信防篡改的分布式数据库。作为区块链技术的第一个也是迄今为止最成功的应用，比特币是一个无需可信第三方的抗双重支付的电子货币支付系统。在比特币系统中，信任的来源不是中央权威机构的授权，而是网络中不同节点共同承认的某种计算范式。因此，区块链技术构建多方信任基础的原理是，通过分布式共识机制，在多方间就网络中事务的合法性判断达成一致认识，对合法行为记录上链，从而构建信任基础。

然而，区块链应用于现实生活中还存在很多安全隐患，就区块链可信安全方面，存在诸多挑战与困难：

一是，隐私数据可信共享问题。部分数据提供者希望共享的数据只向受

限用户可见，而不是对所有用户可见。区块链上的交易都以明文存储，所有节点均可接触到链上存储的信息，这将导致敏感隐私数据会暴露于所有网络参与者。但是，出于缺乏信任以及担心隐私泄露的缘故，数据提供者并不愿意共享隐私数据。

二是，链下数据可信上链问题。区块链所构建的共识是对链上行为的共识，用户对其他用户的信任仅限于网络中发生的行为。作为一个封闭的确定性环境，区块链只能获取链上数据，不能获取链下真实世界的信息。然而，在区块链与实际场景的结合中，要将区块链内的去信任环境推广到链外，智能合约的触发和执行不可避免地要从链下获取数据，但智能合约本身又无法获取链外信息。因此，如何实现链下数据的可信上链成为推动区块链技术落地的关键问题。

三是，链下计算可信扩展问题。比特币系统的设计理论吞吐量为每秒 7 笔交易，但在实际中，由于区块未达到容量上限、块内包含复杂输入输出的交易等问题，比特币的实际吞吐量仅为每秒 3 笔。即使在 2017 年通过软分叉引入了隔离见证协议，比特币的吞吐量也仅为每秒 4～5 笔。以太坊最初每秒能处理 15 笔交易。随着矿工群体逐步提高区块的 gas 上限，实际吞吐量能提升至每秒 36 笔交易，但带来的影响是交易方需要付出相比以往 2.5 倍的手续费。相比每秒处理数千笔交易的 Visa 等主流支付平台，区块链的低吞吐量一直是备受诟病的问题，极大地限制了区块链在实际场景中的应用。而极具潜力能够提升区块链吞吐量链下扩容成为区块链研究的重点方向。链下扩容通过在主链之外建立二层网络，将链上大部分计算转移到链下完成，将计算结果提交至主链。但如何证明二层网络提交至主链数据的真实性，实现链下计算可信扩展成为链下扩容方案的核心问题。

基于此，本书关注于区块链安全问题，一共分为 8 章，分别是：绪论、区块链安全相关基础知识、区块链协议、区块链安全算法、区块链安全分析、区块链信任安全、区块链安全应用以及区块链安全相关政策与规范。首先，

全书从区块链的起源、本质、特性到发展历史带给读者一个清晰形象化的理解，不仅可为初学者入门学习，也适合专业人士用于知识结构梳理；其次，区块链安全的相关基础知识、协议、安全算法以及安全分析和信任安全部分，分别从不同层面进行分析，可为研究者提供区块链安全方面的参考；最后，区块链的应用以及相关政策规范部分，结合与其他学科领域的交叉以及各行各业的应用，分门别类地列举区块链在实际生活中的应用案例，让广大读者切身感受区块链在现实生活的应用。

由于作者水平有限，书中难免存在不当之处，欢迎读者批评指正，来函请发至作者邮箱：sybupt@bupt.edu.cn，不胜感激！如果遇到技术疑难问题，也欢迎探讨和交流，希望我们一起共同成长！

作　者

目　录

CONTENTS

第1章 绪 论

1.1 区块链是什么

1.1.1 由货币发展史看区块链

1. 我国古代货币的发展史

货币是人类文明发展的产物，是实现价值交换的媒介。中国是世界上最早使用货币的国家之一，有五千年的货币使用历史。从最初使用贝壳到使用金银，再到后来使用纸币。人类的货币史大致可分为3个阶段。第一阶段是实物货币，从最早的贝壳到黄金，于1816年形成金本位制。第二阶段是政府信用，即1944年确立的以美元为核心的布雷顿森林体系。前两个阶段都有一个显著的特点，即有形态、有实物、可呈现。随着科技的进步，货币的第三个阶段必将是数字货币，这也是互联网时代的大势所趋。

中国最早的货币是商朝时的贝币(如图1-1所示)。贝币能够成为货币的原

因有 4 个：一是形状好看；二是以个为单位，便于计数；三是它很坚固且容易携带；四是它不易得到，比较珍贵。商品数量的日益增多和商品交换的日益广泛使得货币的需求量增大，海贝已满足不了当时的货币需求，于是聪明的人们改用易得到的铜来仿制贝币，贝币逐渐演变为商朝铜币（如图 1-2 所示）。随着人工仿制铸造货币的大量使用，贝币这种自然货币慢慢消失，铜币的出现，是我国古代货币史上自然货币向人工货币的一次重大演变。

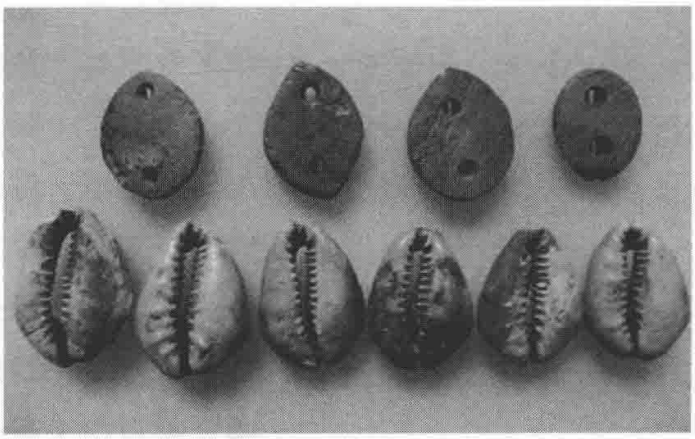

图 1-1　贝币

图 1-2　铜币

到了战国时期，受诸侯称雄割据的影响，货币分为四大体系：铲币（如图 1-3 所示）、刀币（如图 1-4 所示）、环钱、楚币（爰金、蚁鼻钱）。

秦始皇统一中国后，于公元前 210 年颁布货币法，规定在全国范围内通行秦国圆形方孔半两钱，结束了我国古代货币形状各异、重量悬殊的杂乱状态，是我国古代货币史上货币由杂乱形状向规范形状的一次重大演变。

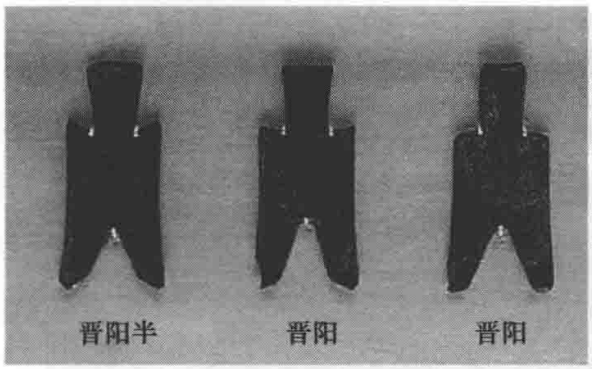

图 1-3 铲币

图 1-4 刀币

刘邦建汉后，允许私铸钱币。很多富商和地方势力乘机大铸钱币获取利润，于是在元鼎四年(前 115 年)，汉武帝收回郡国铸币权，改为中央统一铸造和发行五铢钱。这是中国古代货币史上地方铸币向中央铸币的一次重大演变，此后历代铸币都由中央直接管理。

秦汉以来，钱文中普遍明确标明重量，武德四年(621 年)，唐高祖李渊废掉轻重不一的钱币，统一铸造“开元通宝”，钱文不书重量。这是我国古代货币由文书重量向通宝、元宝的演变，开源通宝是我国最早使用的通宝钱，此后我国铜钱都以通宝、元宝相称(如图 1-5 所示)，一直沿用到辛亥革命后的“民国通宝”。

图 1-5 圆形方孔通宝和元宝

北宋时，铸钱铜料紧缺，政府为弥补铜钱的不足大量铸造铁钱，后来由于铁钱笨重且不便携带，在现在四川所在地区出现了中国乃至世界最早的纸币——交子(如图 1-6 所示)。交子的出现，是我国古代货币史上金属货币向纸币的一

次重要演变。

到了清朝后期，国外先进科学技术逐渐传入，光绪年间开始在国外购买造币机器，用于制造银圆、铜圆。清末机制货币的出现，是我国古代货币史上手工铸币向机制货币的一次重要演变。

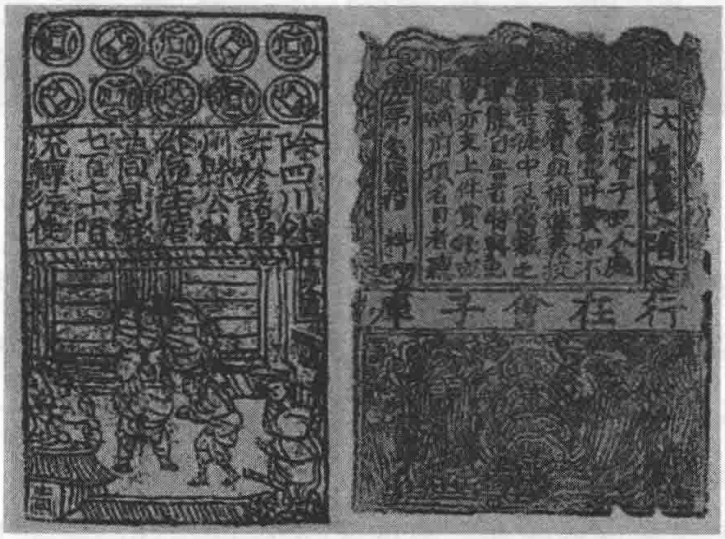

图 1-6　交子

2. 新中国货币发展史

1948 年 12 月 1 日，中国人民银行成立，首次发行人民币纸币（如图 1-7 所示），共 12 种面额，62 种版别。人民币的统一发行清除了国民党政府发行的各种货币，解决了通货膨胀问题，结束了中国近百年外币、金银币在市场流通买卖的历史，对人民解放战争的胜利起了促进作用，对建国初期经济恢复也起了激励作用。

第二、第三、第四、第五套人民币（如图 1-8 所示）分别于 1995 年、1962 年、1987 年和 1999 年开始发行。其中，第二套人民币共 11 种面额；第三套人民币共 7 种面额，13 种券别；第四套人民币共 9 种面额，14 种券别；第五套人民币增加了 20 元的面额，同时取消了 2 元的面额，人民币面额在一次次的发展和演变中变得更加合理，中国的货币制度也随着人民币的演变逐渐健全起来。现在除第五套人民币外，之前的都已经退出市场流通，进入了收藏领域，中国钱币的演化，一步步地完善改进，每一套人民币的发行，都记载着一段历史。

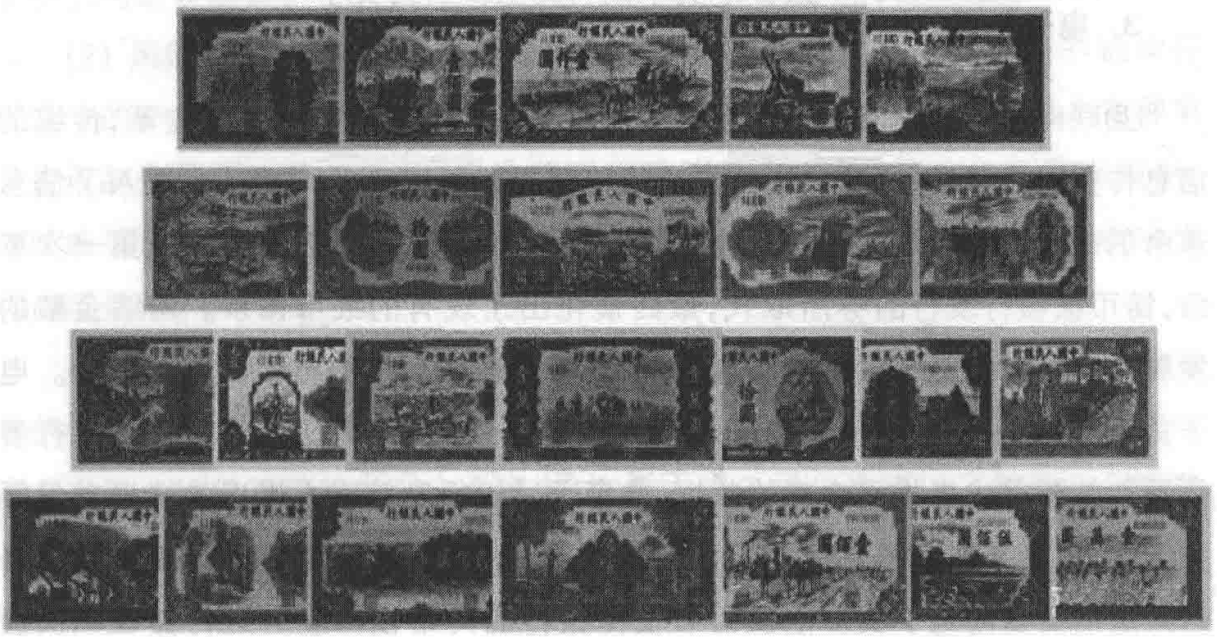

图 1-7 第一套人民币

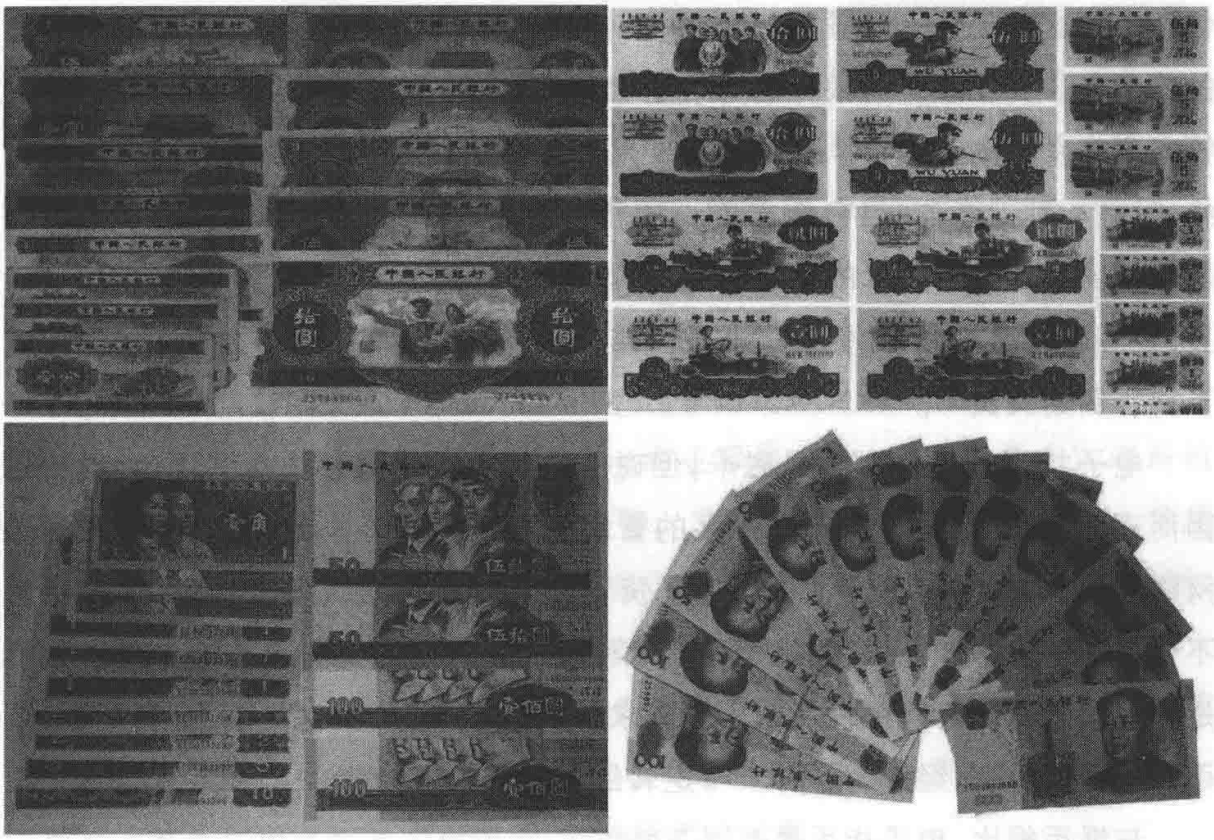

图 1-8 第二、三、四、五套人民币