**目 录**

[前言 10](#_Toc54968562)

[内容简介 12](#_Toc54968563)

[作者简介 14](#_Toc54968564)

[1 第一章区块链概述 15](#_Toc54968565)

[1.1 什么是区块链？ 15](#_Toc54968566)

[1.2 区块链历史 16](#_Toc54968567)

[1.3 区块链的分类 19](#_Toc54968568)

[1.4 区块链解决的问题 22](#_Toc54968569)

[1.5 区块链技术概述 26](#_Toc54968570)

[1.6 区块链技术的应用 27](#_Toc54968571)

[1.7 区块链面临的挑战 29](#_Toc54968572)

[1.7.1 安全性挑战 30](#_Toc54968573)

[1.7.2 效率挑战 35](#_Toc54968574)

[1.7.3 落地应用的有效性 37](#_Toc54968575)

[1.7.4 区块链发展的政策法规监管 37](#_Toc54968576)

[1.8 习题 38](#_Toc54968577)

[2 第二章 区块链技术 39](#_Toc54968578)

[2.1 区块链的一般架构 39](#_Toc54968579)

[2.2 哈希函数 41](#_Toc54968580)

[2.3 密码学算法 42](#_Toc54968581)

[2.3.1 对称加密体系 43](#_Toc54968582)

[2.3.2 不对称加密体系 45](#_Toc54968583)

[2.3.3 国密 47](#_Toc54968584)

[2.3.4 RSA 48](#_Toc54968585)

[2.3.5 魏尔斯特拉斯曲线 51](#_Toc54968586)

[2.3.6 蒙哥马利曲线（ ECSD25519 ） 53](#_Toc54968587)

[2.3.7 爱德华兹曲线 53](#_Toc54968588)

[2.4 共识算法 54](#_Toc54968589)

[2.4.1 两个定理 55](#_Toc54968590)

[2.4.2 共识算法的目的 56](#_Toc54968591)

[2.4.3 工作量证明 57](#_Toc54968592)

[2.4.4 权益证明 58](#_Toc54968593)

[2.4.5 委托权益证明 59](#_Toc54968594)

[2.5 博弈论 60](#_Toc54968595)

[2.5.1 纳什均衡 60](#_Toc54968596)

[2.5.2 公地悲剧问题 60](#_Toc54968597)

[2.5.3 囚徒困境 60](#_Toc54968598)

[2.5.4 博弈理论在区块链里的应用 61](#_Toc54968599)

[2.6 P2P算法 63](#_Toc54968600)

[2.6.1 Gossip 63](#_Toc54968601)

[2.6.2 Kademlia 67](#_Toc54968602)

[2.7 数据结构 74](#_Toc54968603)

[2.7.1 默克尔树 74](#_Toc54968604)

[2.7.2 布隆过滤器（Bloom Filter） 76](#_Toc54968605)

[2.8 习题 80](#_Toc54968606)

[3 第三章 以太坊与智能合约 82](#_Toc54968607)

[3.1 以太坊介绍 82](#_Toc54968608)

[3.1.1 燃料 83](#_Toc54968609)

[3.1.2 以太坊虚拟机(Ethereum Virtual Machine， EVM) 85](#_Toc54968610)

[3.1.3 账户 86](#_Toc54968611)

[3.2 以太坊关键数据结构 87](#_Toc54968612)

[3.2.1 递归长度前缀编码RLP 87](#_Toc54968613)

[3.2.2 梅克尔帕特里夏树 88](#_Toc54968614)

[3.3 智能合约介绍 94](#_Toc54968615)

[3.3.1 虚拟机 94](#_Toc54968616)

[3.3.2 容器（Docker） 95](#_Toc54968617)

[3.3.3 优势 95](#_Toc54968618)

[3.4 现有智能合约框架介绍 96](#_Toc54968619)

[3.5 习题 97](#_Toc54968620)

[4 第四章 SOLIDITY编程 100](#_Toc54968621)

[4.1 sol文件结构 100](#_Toc54968622)

[4.2 合约文件结构 103](#_Toc54968623)

[4.3 变量类型 104](#_Toc54968624)

[4.3.1 值类型 104](#_Toc54968625)

[4.3.2 引用类型 106](#_Toc54968626)

[4.3.3 字典/映射 108](#_Toc54968627)

[4.3.4 特殊情况 108](#_Toc54968628)

[4.4 操作符 110](#_Toc54968629)

[4.5 语句 110](#_Toc54968630)

[4.5.1 条件语句 110](#_Toc54968631)

[4.5.2 循环语句 111](#_Toc54968632)

[4.5.3 其他 111](#_Toc54968633)

[4.6 修饰符 111](#_Toc54968634)

[4.6.1 修饰符说明 112](#_Toc54968635)

[4.6.2 修饰符区别 114](#_Toc54968636)

[4.6.3 自定义修饰符 116](#_Toc54968637)

[4.7 数据位置 118](#_Toc54968638)

[4.8 事件 120](#_Toc54968639)

[4.9 继承 124](#_Toc54968640)

[4.9.1 单继承 124](#_Toc54968641)

[4.9.2 多重继承 124](#_Toc54968642)

[4.10 其他 125](#_Toc54968643)

[4.10.1 类型转换及推断 125](#_Toc54968644)

[4.10.2 异常 127](#_Toc54968645)

[4.10.3 汇编 127](#_Toc54968646)

[4.10.4 This关键字 129](#_Toc54968647)

[4.11 习题 130](#_Toc54968648)

[5 第五章 智能合约开发 132](#_Toc54968649)

[5.1 智能合约开发的不同点 132](#_Toc54968650)

[5.2 智能合约的生命周期 134](#_Toc54968651)

[5.3 开发智能合约的周期 135](#_Toc54968652)

[5.4 设计模式 136](#_Toc54968653)

[5.4.1 工厂合约模式 136](#_Toc54968654)

[5.4.2 映射迭代 137](#_Toc54968655)

[5.4.3 名字登录 138](#_Toc54968656)

[5.4.4 撤出模式 139](#_Toc54968657)

[5.4.5 合约自毁 140](#_Toc54968658)

[5.4.6 访问限制 141](#_Toc54968659)

[5.4.7 断路器 143](#_Toc54968660)

[5.4.8 状态机 144](#_Toc54968661)

[5.5 基础算法 147](#_Toc54968662)

[5.6 安全 150](#_Toc54968663)

[5.6.1 智能合约安全问题分类 150](#_Toc54968664)

[5.6.2 智能合约 最佳安全开发指南 175](#_Toc54968665)

[5.6.3 代码审计 184](#_Toc54968666)

[5.7 总结 184](#_Toc54968667)

[5.8 习题 184](#_Toc54968668)

[6 第六章Solidity智能合约高级话题 186](#_Toc54968669)

[6.1 可升级 186](#_Toc54968670)

[6.1.1 升级要考虑的问题 186](#_Toc54968671)

[6.1.2 方法 187](#_Toc54968672)

[6.1.3 通用的代理模式 191](#_Toc54968673)

[6.1.4 存储升级 195](#_Toc54968674)

[6.2 省Gas 204](#_Toc54968675)

[6.3 汇编代码 214](#_Toc54968676)

[6.3.1 栈 214](#_Toc54968677)

[6.3.2 调用数据 214](#_Toc54968678)

[6.3.3 内存 216](#_Toc54968679)

[6.3.4 存储 217](#_Toc54968680)

[6.4 合约间调用 218](#_Toc54968681)

[6.4.1 函数调用 219](#_Toc54968682)

[6.4.2 依赖注入 220](#_Toc54968683)

[6.4.3 消息调用 222](#_Toc54968684)

[6.4.4 获取合约间调用的返回值 226](#_Toc54968685)

[6.5 ABI 编程 228](#_Toc54968686)

[6.5.1 内存结构 228](#_Toc54968687)

[6.5.2 函数选择子 229](#_Toc54968688)

[6.5.3 类型的定义 229](#_Toc54968689)

[6.5.4 EVM里的数据表示 230](#_Toc54968690)

[6.5.5 编码 238](#_Toc54968691)

[6.6 运行原理 248](#_Toc54968692)

[6.6.1 合约导入代码 253](#_Toc54968693)

[6.6.2 合约本体通用部分 254](#_Toc54968694)

[6.6.3 合约本体特定代码 256](#_Toc54968695)

[6.6.4 合约运行全视图 256](#_Toc54968696)

[6.7 习题 257](#_Toc54968697)

[7 第七章基于Solidity智能合约的去中心化应用（DApp） 259](#_Toc54968698)

[7.1 DApp的特点 259](#_Toc54968699)

[7.2 DApp架构 263](#_Toc54968700)

[7.2.1 客户端 264](#_Toc54968701)

[7.2.2 服务器端 265](#_Toc54968702)

[7.2.3 流程详解 267](#_Toc54968703)

[7.3 去中心化数据存储 271](#_Toc54968704)

[7.3.1 Swarm 272](#_Toc54968705)

[7.3.2 星际文件系统（IPFS/Filecoin） 275](#_Toc54968706)

[7.4 消息通信 277](#_Toc54968707)

[7.4.1 通信加密 277](#_Toc54968708)

[7.4.2 Envelope(信封) 277](#_Toc54968709)

[7.4.3 Topic(主题) 278](#_Toc54968710)

[7.4.4 Filter(过滤器) 278](#_Toc54968711)

[7.5 名字解析 278](#_Toc54968712)

[7.6 习题 280](#_Toc54968713)

[8 第八章 超级账本 281](#_Toc54968714)

[8.1 Fabric 284](#_Toc54968715)

[8.1.1 组件（Component） 284](#_Toc54968716)

[8.1.2 技术架构 292](#_Toc54968717)

[8.1.3 网络架构 294](#_Toc54968718)

[8.2 Fabric智能合约—链码（Chaincode） 296](#_Toc54968719)

[8.2.1 链码的分类 296](#_Toc54968720)

[8.2.2 链码的生命周期 297](#_Toc54968721)

[8.3 Chaincode智能合约交互 299](#_Toc54968722)

[8.4 习题 300](#_Toc54968723)

[9 第九章Web Assembly（WASM） 309](#_Toc54968724)

[9.1 为什么需要WASM 309](#_Toc54968725)

[9.1.1 EVM的缺陷 309](#_Toc54968726)

[9.1.2 WASM的优越性 314](#_Toc54968727)

[9.2 Web Assembly 315](#_Toc54968728)

[9.2.1 特点 315](#_Toc54968729)

[9.2.2 WebAssembly 动态运行库 317](#_Toc54968730)

[9.3 如何前后端交互（以golang为例） 319](#_Toc54968731)

[9.3.1 从后端（Golang）到前端Javascript 319](#_Toc54968732)

[9.3.2 从前端Javascript到后端（Golang） 321](#_Toc54968733)

[9.4 如何从Solidity迁移到WASM 322](#_Toc54968734)

[9.5 习题 322](#_Toc54968735)

[10 附录A SOLIDITY常用函数 324](#_Toc54968736)

[10.1.1 特殊变量 324](#_Toc54968737)

[10.1.2 数学和加密函数 324](#_Toc54968738)

[10.1.3 地址相关 325](#_Toc54968739)

[10.1.4 合约相关 325](#_Toc54968740)

[10.1.5 特殊单位 325](#_Toc54968741)

[11 附录B 区块链大事记 327](#_Toc54968742)

[12 附录C 区块链术语 328](#_Toc54968743)

[12.1 节点(Node) 328](#_Toc54968744)

[12.2 矿工(Miner) 328](#_Toc54968745)

[12.3 Ether (ETH) 328](#_Toc54968746)

[12.4 交易 329](#_Toc54968747)

[12.5 对称点对点网络(P2P)  329](#_Toc54968748)

[12.6 分叉 330](#_Toc54968749)

[12.7 通证 332](#_Toc54968750)

[12.8 环签名技术 333](#_Toc54968751)

[12.9 零知识证明 333](#_Toc54968752)

[13 附录D以太坊内置合约 334](#_Toc54968753)

[13.1 Address 0x01: ecrecover(hash, v, r, s) 334](#_Toc54968754)

[13.2 Address 0x02: sha256(data) 334](#_Toc54968755)

[13.3 Address 0x03: ripemd160(data) 334](#_Toc54968756)

[13.4 Address 0x04: datacopy(data) 334](#_Toc54968757)

[13.5 Address 0x05: bigModExp(base, exp, mod) 335](#_Toc54968758)

[13.6 Address 0x06: bn256Add(ax, ay, bx, by) 335](#_Toc54968759)

[13.7 Address 0x07: bn256ScalarMul(x, y, scalar) 336](#_Toc54968760)

[13.8 Address 0x08: bn256Pairing(a1, b1, a2, b2, a3, b3, ..., ak, bk) 336](#_Toc54968761)

[14 参考文献 338](#_Toc54968762)