**区块链那些事儿 (0.2.04222015)**

**第0章 说在前面的话**

0.1 本书风格

0.3 致敬互联网

**第1章 初识区块链**

* 1. 创世元灵——一切源自比特币

1.1.1 从比特币白皮书谈起

1.1.2 比特币核心程序——中本聪客户端

1.1.3 比特币的发行——挖矿

1.1.4 比特币钱包——标准钱包与轻钱包

1.1.5 比特币账本结构——区块链

1.1.6 比特币交易事务——UTXO

1.1.7动手编译比特币源码

* 1. 区块链的种类
  2. 区块链技术组成
  3. 区块链的技术意义
  4. 区块链结构图解
  5. 如何查看区块数据
  6. 知识点导图

**第2章 区块链应用发展**

2.1 比特币及其朋友圈——加密数字货币

2.1.1 莱特币

2.1.2 以太坊

2.1.3 零币

2.1.5 开发技术总结

2.2 区块链商业应用——智能合约

2.2.1 智能合约原理图

2.2.2 智能合约的应用设想

2.3 区块链基础设施——可编程社会

2.4 链内资产 vs 链外资产

2.5 知识点导图

**第3章 区块链骨骼**——**密码算法**

3.1 哈希算法

3.1.1 什么是哈希计算

3.1.2 哈希算法的种类

3.1.3 区块链中的哈希算法

3.2 公开密钥算法

3.2.1 两把钥匙——公开密钥算法

3.2.2 算法认识1——Elgamal算法

3.2.2 算法认识2——RSA算法

3.2.3 算法认识3——椭圆曲线密码算法

3.2.4 比特币中使用的算法——secp256k1

3.3 编码解码算法

3.3.1 Base64

3.3.2 Base58

3.4 比特币中的公钥、私钥与钱包地址

3.5 知识点导图

**第4章 区块链灵魂**——**共识算法**

4.1 分布式系统的一致性

4.1.1 一致性的问题

4.1.2 共识算法的目的

4.1.3 拜占庭将军问题

4.1.4 两个原理——FLP&CAP

4.2 Paxos算法

4.3 Raft算法

4.4 PBFT算法

4.5 工作量证明——PoW

4.6 权益证明——PoS

4.7 股份授权证明机制——DPoS

4.8 共识算法的社会学探讨

4.9 知识点导图

**第5章 区块链扩展**——**侧链&闪电网络**

5.1 比特币的扩容问题

5.2 侧链技术

5.3 闪电网络的设计

5.4 多链——区块链应用的扩展交互

**第6章 区块链开发平台**

6.1 以太坊项目

6.1.1 项目背景

6.1.2 以太坊的组成

6.1.3 以太坊的账户设计

6.1.3 关于两个以太的问题

6.2 以太坊编程

6.2.1 虚拟机设计

6.2.2 智能合约编程——Solidity

6.2.3 安装以太坊客户端

6.2.3 编写一个智能合约

6.3超级账本

6.3.1 项目背景

6.3.2 超级账本组成

6.3.3 Fabric的应用

**第7章 区块链应用集锦**

7.1 数字货币

7.2 公证防伪

7.3 资产交易

7.4 银行结算

7.4 物联网

7.5 区块链即服务

**第8章 动手做个体验**——微链

8.1 开发环境准备

8.2 设计一个简单的结构

8.3 源码解析

8.4 运行一下看看

**第9章 潜在的问题**

9.1 两个哭泣的婴儿——软分叉与硬分叉

9.2 达摩克利斯剑——51%攻击

9.3 简单的代价——轻钱包的易攻击性

9.4 忘了保险箱密码——私钥丢失

9.5重放攻击——交易延展性

9.5 说说The DAO事件

**第10章 未来应用场景**

10.1 虚拟社会——链上自治的世界

10.2 文明的波动——未来已来