HZ BOOKS
华章IT

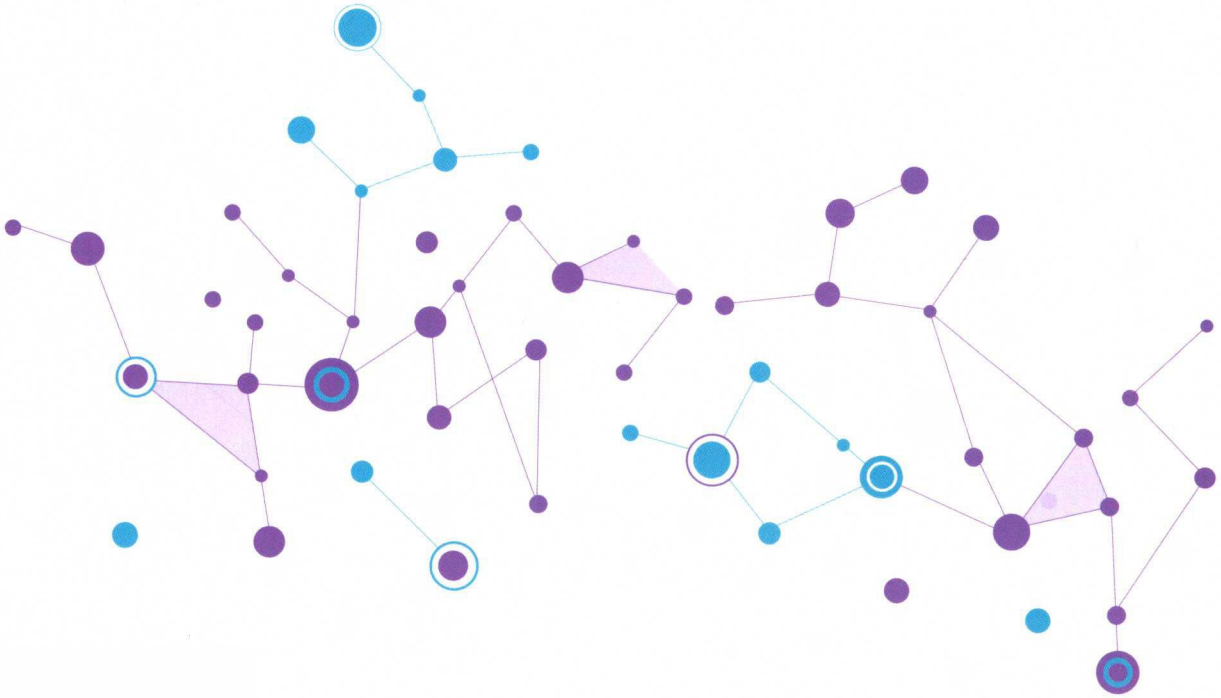
比原链CTO朗豫鼎力推荐。

从基础架构到代码实践，深度解析公链技术原理和功能设计，包括应用层、内核层、网络层，层层抽丝剥茧，揭开区块链底层技术实现的神秘面纱。

区块链技术丛书

GO语言公链开发实战

郑东旭 杨明珠 潘盈瑜 翟萌 ◎编著

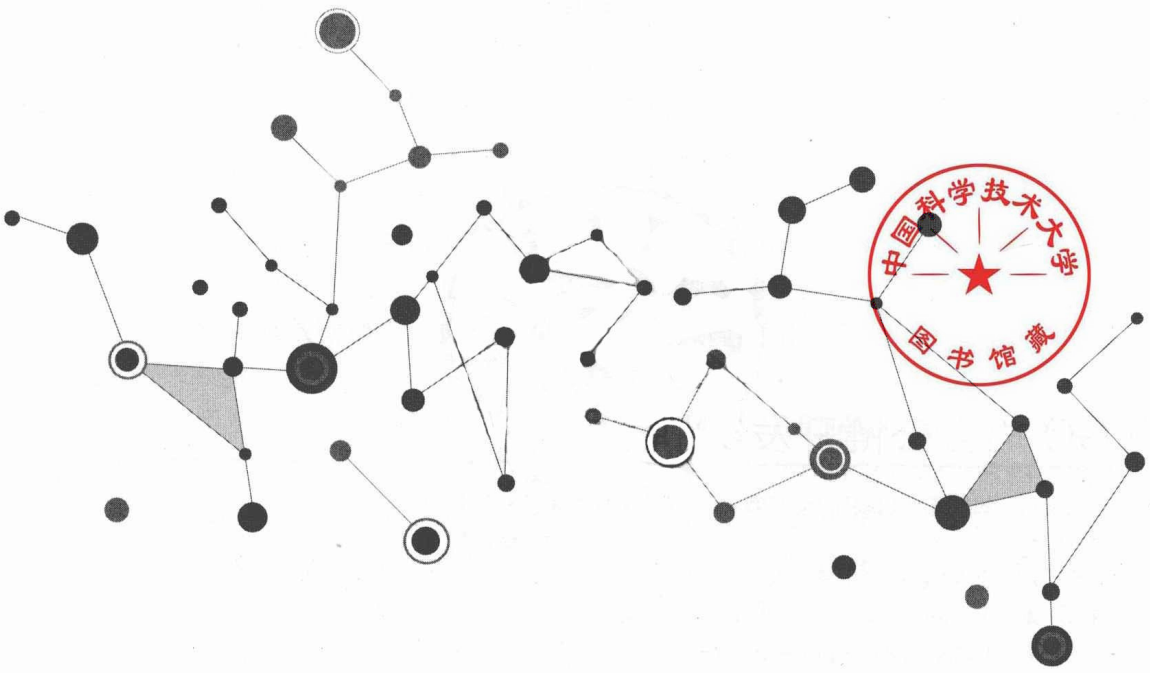


机械工业出版社
China Machine Press

区块链技术丛书

GO语言公链开发实战

郑东旭 杨明珠 潘盈瑜 翟萌 ◎编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

GO 语言公链开发实战 / 郑东旭等编著 . —北京：机械工业出版社，2019.6
（区块链技术丛书）

ISBN 978-7-111-62987-0

I. G… II. 郑… III. 电子商务 - 支付方式 - 研究 IV. F713.361.3

中国版本图书馆 CIP 数据核字（2019）第 116596 号

GO 语言公链开发实战

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：吴　怡　　责任校对：殷　虹
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2019 年 7 月第 1 版第 1 次印刷
开　　本：186mm×240mm　1/16　　印　　张：19.25
书　　号：ISBN 978-7-111-62987-0　　定　　价：89.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88379426　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　　读者信箱：hzit@hzbook.com

Foreword 推荐序一

我与本书作者同在中国较早的一个公有区块链开源技术社区，同样学习和研究区块链，书中的区块链实例也来源于此，我想我可以简单说几句。

区块链最早源于极客社区点对点电子现金论文，时至今日已有十年。早年的开发应用及技术著作均围绕电子现金类的应用展开。即便有链以及应用，也多是介绍联盟链的应用，较少涉及公链类应用。想要深入学习比较困难，当时业界开发类书籍仅有一本《Mastering Bitcoin》为指路明灯。我早年也曾应《程序员》杂志约稿写过一篇文章《区块链产品三定律》，其中罗列了当时市面流行的六七种应用案例，但总体而言，大环境不完善，产业并不繁荣，产品及技术方面的学习颇为不便，国内从事开发、研究的人员也相当稀少，仅二三十人，中文技术类图书也极度短缺。

技术的可贵之处在于，不仅展现了人类的精湛设计，而且提供了解决问题后所带来的改变。区块链之所以备受瞩目，是因为它创造了一种新的范式，能连接资产服务所涉及的各参与方，能够打破数据孤岛，提高安全性，增强风险控制能力，保护隐私，降低交易成本的同时带来收益。

在资本和产业的热捧中，已出现了各种区块链应用。我们很高兴看到本书作者团队以比原链为实例，完成了这本 GO 语言开发实战类书籍。本书是我见过的为数不多的剖析区块链技术面面俱到，并兼具深度的专业著作，从公链的整体架构开始，到接口，再到内核，从外及里一步步揭示公链的技术原理。在揭示这些技术原理的过程中，作者不满足于浅尝辄止，而是深入到参数解析，使本书除了供知识学习之外，更成为一本实操的参考书籍。最为难能可贵的是，在解析区块链技术的同时，本书对公链构建过程中使用的一些其他技术也有涉及，将区块链的来龙去脉都说得非常清楚，而不是仅仅关注区块链本身。本书虽然以比原链为蓝本，但实际上所用技术在区块链中也都大致通用。

希望本书能帮助更多对区块链感兴趣的读者、开发者、技术人员进入这片新天地。

段新星，比原链创始人

2019 年元旦

推荐序二 *Forword*

2017年，我带领团队创办北京邮电大学平行汇区块链实验室。两年来，实验室一直致力区块链技术研究，积极参与行业内交流与技术分享，与政府、企业齐心合力推进区块链技术更好更快落地。目前，区块链的发展也更加理性，已广泛用于产品溯源、版权验证、数据共享、IOT控制等众多领域。借助区块链技术去中心化、不可篡改的特点，未来大数据流通和广泛数字应用场景的安全性、可靠性、便利性都将得到显著改善。

区块链作为一种新兴的技术，目前仍有很多可供人们施展才能的方向。其中的公链技术，是去中心化思想的集大成者。且不谈比特币（一种虚拟货币）的发展是以公链为载体，目前所熟知的以太坊平台等也是基于公链技术。公有链技术重在强调如何通过严谨的密码学算法，为无先验的节点提供可信的服务，恰似聚散沙为磐石。虽然公链技术始终是区块链技术爱好者的一片热土，但是对新入门的开发人员而言，并无体系成熟、翔实可靠的开发指导，初学者往往淹没在各种问答式的经验帖中，无助于形成完备的技术体系。

本书是市面上不多见的体系完备之作，在兼顾将公链核心技术讲通透的同时，不囿于细节，致力于呈现给读者区块链的全局脉络。

北京邮电大学副教授，硕士生导师

陈萍

2019年春节

Preface 前　言

2008 年由中本聪第一次提出了区块链的概念，在随后的几年中，区块链成为了电子货币比特币的核心组成部分：作为所有交易的公共账簿。2017 年笔者的很多朋友已经在关注区块链技术领域，笔者也在各种技术峰会上分享过多次区块链技术实现细节，在线上也组织了几个区块链技术群。笔者发现有相当多的朋友询问如何深入学习区块链实现技术，但目前市面上很多的资料都仅介绍区块链上的某部分技术，比如加密货币交易、智能合约开发等，并没有完整介绍公链的技术实现。在一次技术峰会演讲后与北京邮电大学区块链实验室的老师交流，受到陈萍老师的鼓励，想到编写一本系统性介绍公链开发的书籍，对学习区块链的初学者会有帮助，于是便开始组织本书的写作。

本书的目标是引导读者全面了解区块链技术实现原理，笔者也一直坚信，了解某一系统最直接的方式就是研读它的源码，所以本书并不是只介绍区块链技术，而是深入分析其背后的实现原理。通过阅读本书，读者可以全面地了解一条公链的技术实现。本书基于比原链的源代码进行分析，比原链是一个开源的有智能合约功能的公共区块链平台，是国内优秀的公链，目前比原链的代码量不多，而且源码结构清晰，特别适合初学者学习。

本书主要内容包括：

第 1 章介绍公链设计架构，使读者能够宏观地了解区块链技术架构。

第 2 章介绍比原链相关的交互工具，包括交互工具的操作及代码实现。

第 3 章介绍比原链的核心进程 bytomd，包括启动过程中的初始化等操作。

第 4 章介绍 API Server 实现及原理。详解 HTTP 请求的完整生命周期，并介绍区块链相关的 API 接口设计。

第 5 章和第 6 章详细介绍区块链核心部分，包括区块、区块链、交易的核心数据结构，以及 UTXO 模型、隔离见证、交易脚本、验证等概念的实现。

第 7 章和第 8 章详细讲解比原链智能合约以及智能合约在 BVM 虚拟机上运行的过程。

第 9 章介绍区块链钱包的基本概念，包括密钥、账户、资产管理、交易管理等，以及钱包的备份和恢复方式。

第 10 章详解区块链 P2P 分布式网络实现原理，以及 Kademlia 结构化网络算法的实现。

第 11 章介绍数据持久化存储，以及区块与交易的缓存和存储过程。

第 12 章和第 13 章详解 PoW 与 PoS 共识机制以及挖矿相关的概念和流程。

第 14 章介绍区块链技术未来的发展趋势，我们相信区块链能够为人类做出重大贡献。

本书适合区块链开发者、Go 语言开发者阅读。由于时间与水平比较有限，我们在编写本书时也难免会出现一些纰漏和错误。读者可以随时通过邮箱 weilandeshanhuhai@126.com 与我们联系，希望和大家一起学习与讨论区块链技术。

本书在写作过程中得到很多人的帮助，特别是郜策宇、陆志亚、王庆华、朱益祺、阳胜、林浩宇，在此深表感谢。尤其感谢比原链技术团队设计了这样一个优秀的公链，给区块链社区做出了贡献。

郑东旭

2019 年 3 月 14 日

Contents 目　录

第 1 章 Chapter 1

公链设计架构

1.1 概述

区块链技术起源于 2008 年中本聪的论文《比特币：一种点对点电子现金系统》，区块链诞生自中本聪的比特币。

区块链是一个分布式账本，一种通过去中心化、去信任的方式集体维护一个可靠数据库分布式账本是一种在网络成员之间共享、复制和同步的数据库，记录网络参与者之间的交易，比如资产或数据的交换。

区块链分类如下。

- 公链：无官方组织及管理机构，无中心服务器。参与的节点按照系统规则自由地接入网络，节点间基于共识机制开展工作。
- 私链：建立在某个企业内部，系统运作规则根据企业要求进行设定，读写权限仅限于少数节点，但仍保留着区块链的真实性和部分去中心化特性。
- 联盟链：若干个机构联合发起，介于公链和私链之间，兼容部分去中心化的特性。

本书基于国内优秀项目比原链（Bytom），为读者展开公链技术的完整实现。如果说比特币代表区块链 1.0 时代，以太坊拥有图灵完备性代表的是区块链 2.0 时代的话，比原链则基于 UTXO 模型支持了更丰富的功能（图灵完备的智能合约、多资产管理、Tensority 新型的 PoW 共识算法等），其代表的是区块链 2.5 时代。比原链是一个开源项目，整个项目基于 GO 语言开发，代码托管于 GitHub 上（https://github.com/Bytom/bytom）。

本书基于比原链的 1.0.5 版本源码进行分析。读者不用纠结本书为何不使用比特币或以太坊作为示例，所谓“有道无术，术尚可求也，有术无道，止于术”，作者认为大部分区块

链技术实现都是相似的。目前主要在共识算法（PoW、PoS）和模型（UTXO 或 Account 模型）方面有所不同。比原链作为国内优秀的公链，代码量并不多，而且清晰的源码结构使得程序员和链圈爱好者的学习成本也不高。我们从中可以学到很多东西，如 GO 语言程序设计及应用、公链设计架构、公链运行原理等。

本章主要内容包括：

- 比原链的总体架构。
- 比原链架构内部各模块功能。
- 比原链编译部署及应用。

1.2 公链总体架构

比原链（Bytom Blockchain 或者 Bytom）是一个开源的有智能合约功能的公共区块链平台。比原链公链设计架构如图 1-1 所示。

1.3 比原链各模块功能

我们将从图 1-1 所示的比原链总架构图中抽离出各个模块，逐一分析及阐述。

1.3.1 用户交互层

比原链的用户交互层如图 1-2 所示。

1. bytomcli 客户端

bytomcli 是用户与 bytomd 进程在命令行下建立通信的 RPC 客户端。在已经部署比原链的机器上，用户能够使用 bytomcli 可执行文件发起对比原链的多个管理请求。

bytomcli 发送相应的请求，请求由 bytomd 进程接收并处理。bytomcli 的一次完整生命周期结束。

2. bytom-dashboard

bytom-dashboard 与 bytomcli 功能类似，都是发送请求与 bytomd 进程建立通信。用户可通过 Web 页面与 bytomd 进程进行更为友好的交互通信。

在已经部署比原链机器上，会默认开启 bytom-dashboard 功能，无须再手动部署 bytom-dashboard。实际上通过传入的参数用户可以决定是否开启或关闭 bytom-dashboard 功能。如传入 --web.closed，则可以关闭该功能。项目源码地址：https://github.com/Bytom/bytom-dashboard。

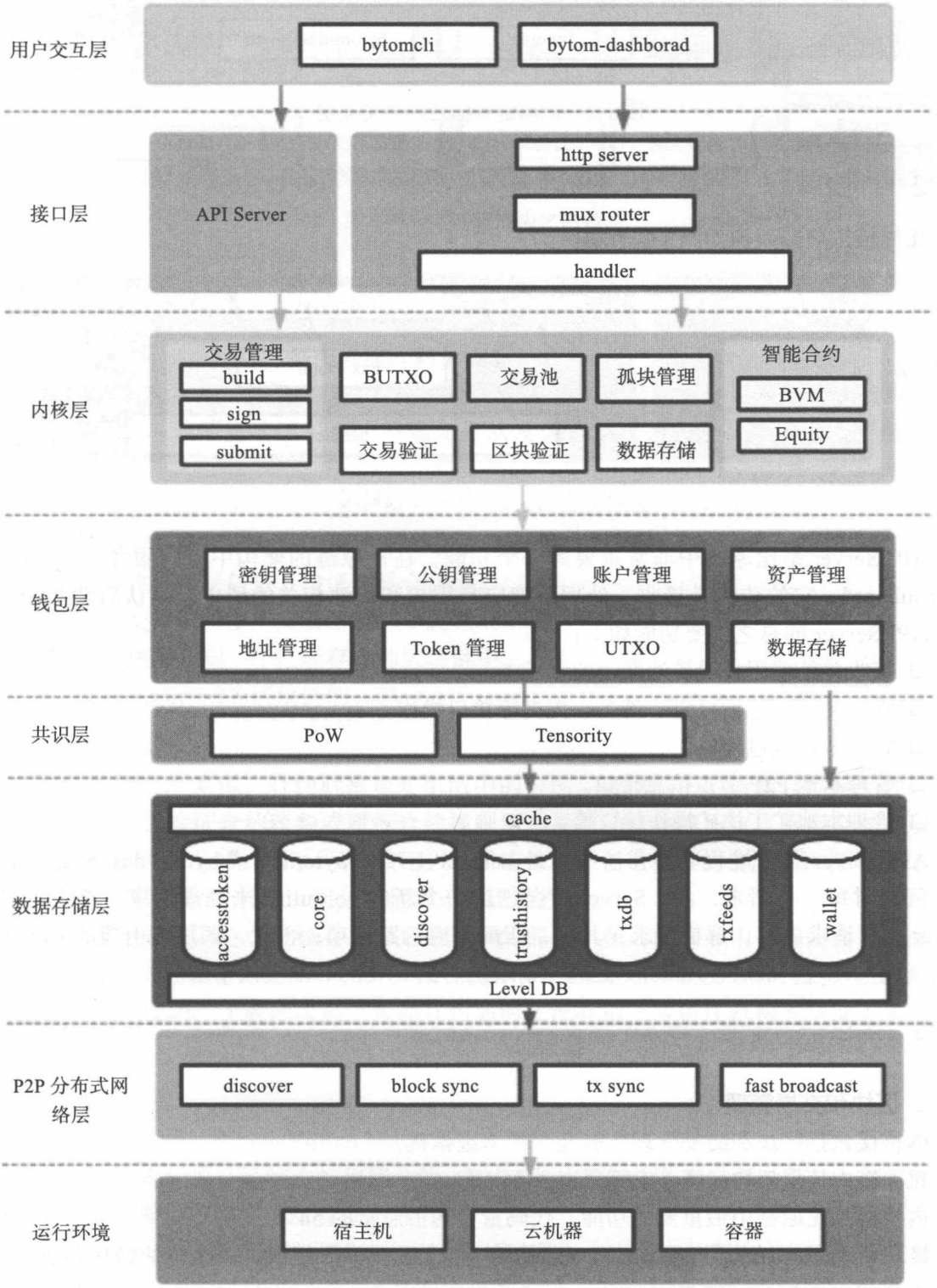

用户交互层
bytomcli
bytom-dashborad
接口层
API Server
http server
mux router
handler
内核层
交易管理
build
sign
submit
BUTXO
交易池
孤块管理
智能合约
BVM
Equity
交易验证
区块验证
数据存储
钱包层
密钥管理
公钥管理
账户管理
资产管理
地址管理
Token 管理
UTXO
数据存储
共识层
PoW
Tensority
数据存储层
cache
accesstoken
core
discover
trusthistory
txdb
txfeeds
wallet
Level DB
P2P 分布式网络层
discover
block sync
tx sync
fast broadcast
运行环境
宿主机
云机器
容器

图 1-1　比原链架构

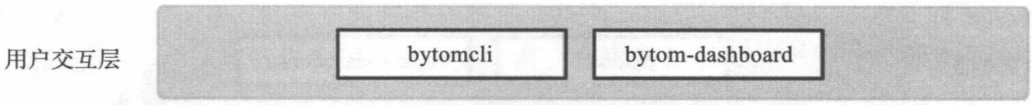


图 1-2 比原链架构之用户交互层

1.3.2 接口层

比原链接口层架构如图 1-3 所示。

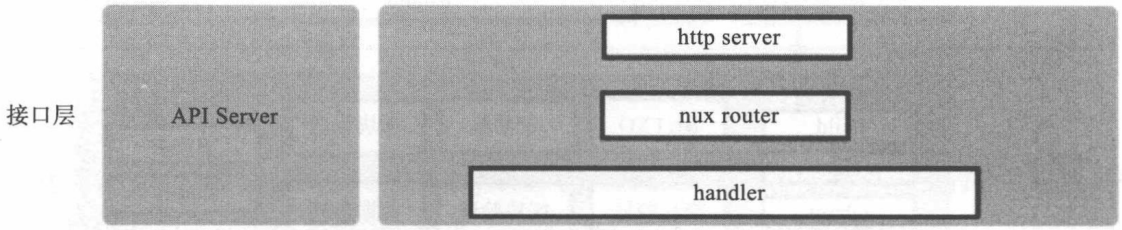


图 1-3 比原链架构之接口层

API Server 是比原链中非常重要的一个功能，在比原链的架构中专门服务于 bytomcli 和 dashboard，它的功能是接收、处理并响应与用户和矿池相关的请求。默认启动 9888 端口。API Server 的总之主要功能如下：

- 接收并处理用户或矿池发送的请求。
- 管理交易，包括打包、签名、提交等接口操作。
- 管理本地钱包接口。
- 管理本地 P2P 节点信息接口。
- 管理本地矿工挖矿操作接口等。

API Server 服务过程中，在监听地址 listener 上接收 bytomcli 或 bytom-dashboard 的请求访问，对每一个请求，API Server 均会创建一个新的 goroutine 来处理请求。首先，API Server 读取请求内容，解析请求；其次，匹配相应的路由项；再次，调用路由项的 Handler 回调函数来处理；最后，Handler 处理完请求之后给 bytomcli 响应该请求。

1.3.3 内核层

1. 区块和交易管理

内核层包括区块和交易管理、智能合约、虚拟机。

比原链内核层架构如图 1-4 所示。

内核层是比原链中最重要的功能，代码量大约占总量的 54%。

区块链的基本结构是一个链表。链表由一个个区块串联组成。一个区块链中包含成千上万个区块，而一个区块内又包含一个或多个交易。在比原链内核层有一个重要的功能是对区块和交易进行管理。

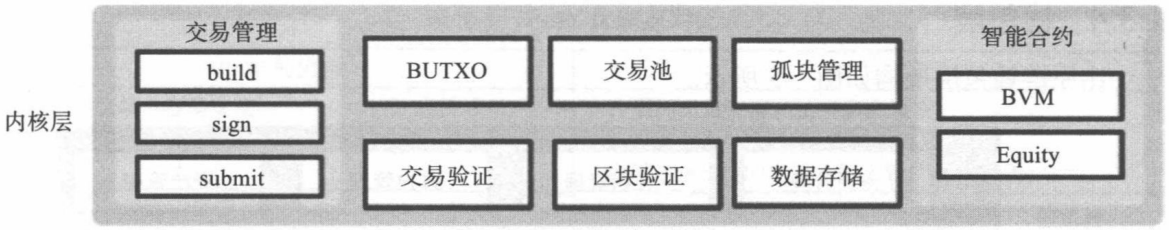


图 1-4　比原链架构之内核层

当网络中的某个节点接收到一个新的有效区块时，节点会验证新区块。当新的区块并未在现有的主链中找到它的父区块，这个新区块会进入孤块管理中等待父区块。如果从现有的主链中找到了父区块，则将其加入到主链。

当网络中的某个节点接收到一笔交易时，节点会验证交易的合法性。验证成功后，该笔交易放入交易池等待矿工打包。一笔交易从发送到完成的整个生命周期需要经过如下过程：

1）A 通过钱包向 B 发出一笔交易，交易金额为 100 比原币（BTM）。

2）该笔交易被广播到 P2P 网络中。

3）矿工收到交易信息，验证交易合法性。

4）打包交易，将多个交易组成一个新区块。

5）新区块加入到一个已经存在的区块链中。

6）交易完成，成为区块链的一部分。

2. 智能合约

从传统意义上来说，合约就是现实生活中的合同。区块链中的智能合约是一种旨在以数字化的方式让验证合约谈判或履行合约规则更加便捷的计算机协议。智能合约本质上是一段运行在虚拟机上的“程序代码”，可以在没有第三方信任机构的情况下执行可信交易。

智能合约具有两个特性：可追踪性和不可逆转性。

智能合约是比原链中最核心、也是最重要的部分。在后面章节中，我们会详细介绍智能合约模型（主流模型：UTXO 模型、账户模型）、运行原理，以及 BVM 虚拟机工作机制。我们还将深入代码，了解区块链上智能合约如何在没有第三方信任机构的情况下进行可信交易。

3. 虚拟机

比原链虚拟机（Bytom Virtual Machine，BVM）是建立在区块链上的代码运行环境，其主要作用是处理比原链系统内的智能合约。BVM 是比原链中非常重要的部分，在智能合约存储、执行和验证过程中担当着重要角色。

BVM 用 Equity 语言来编写智能合约。比原链是一个点对点的网络，每一个节点都运行着 BVM，并执行相同的指令。BVM 是在沙盒中运行，和区块链主链完全分开。

1.3.4 钱包层

比原链钱包层架构如图 1-5 所示。

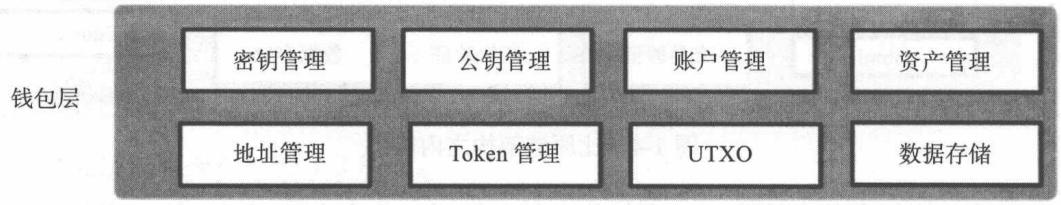


图 1-5 比原链架构之钱包层

钱包可以类比于我们日常生活中的保险箱，我们关心保险箱的开门方式（密钥）和其中保存的财产（UTXO）。比原链钱包层主要负责保存密钥、管理地址、维护 UTXO 信息，并处理交易的生成、签名，对外提供钱包、交易相关的接口。

比原链的交易发送分为三步：

1）Build：根据交易的输入和输出，构造交易数据。

2）Sign：使用私钥对每个交易输入进行签名。

3）Submit：将交易提交到网络进行广播，等待打包。

1.3.5 共识层

比原链共识层架构如图 1-6 所示。

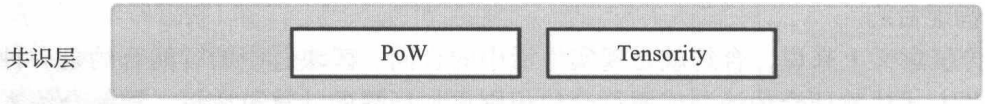


图 1-6 比原链架构之共识层

共识层用于实现全网数据的一致性，区块链是去中心化账本，需要全网对账本达成共识。共识层通过验证区块和交易，保证新的区块在所有节点上以相同的方式产生。简单说，共识机制就是通过某种方式竞争“记账权”，得到记账权的节点可以将自己生成的区块追加到现有区块链的尾部，其他节点可以根据相同的规则，验证并接受这些区块，丢弃那些无法通过验证的区块。

常见的共识机制有工作量证明（Proof-of-Work，PoW）、股权证明（Proof-of-Stake，PoS）等。

PoW 共识机制利用复杂的数学难题作为共识机制，目前一般使用“hash 函数的计算结果小于特定的值”。由于 hash 函数的特性，不可能通过函数值来反向计算自变量，所以必须用枚举的方式进行计算，直到找出符合要求的 hash 值。这一过程需要进行大量运算。PoW 的复杂性保证了任何人都需要付出大量的运算来产生新的块，如果要篡改已有的区块，则需要付出的算力比网络上其他节点的总和都大。PoW 优缺点对比如表 1-1 所示。