HZ BOOKS
华章IT

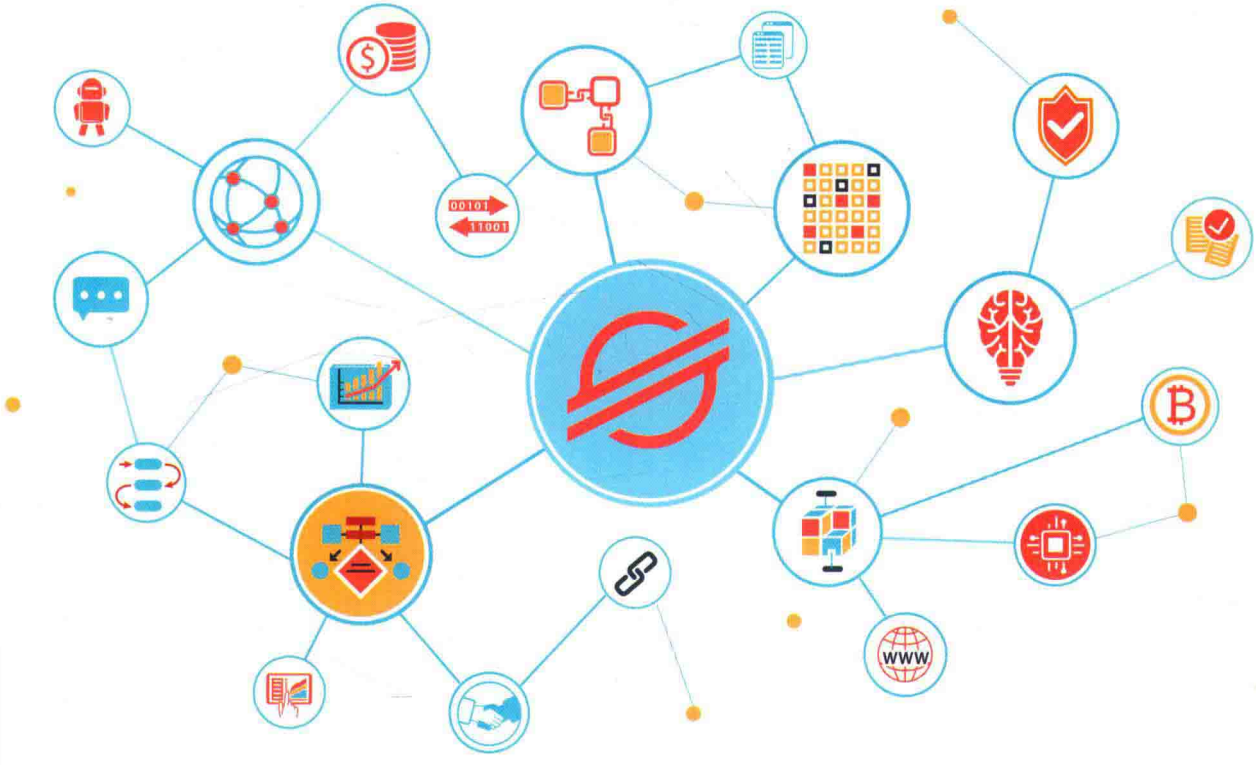
Stellar官方团队强烈推荐！
三位作者均是Stellar技术社区的资深技术专家和布道师，
Stellar创始人Jed McCaleb作序推荐

Stellar

区块链技术丛书

Stellar区块链
原理与实践

宋文鹏 梁然 韩丰 ◎ 著



PRINCIPLES AND PRACTICE OF STELLAR

从工作原理、架构设计、工程实践三个维度，全方位深入剖析Stellar区块链技术

机械工业出版社
China Machine Press

区块链
技术丛书

PRINCIPLES AND PRACTICE OF STELLAR

Stellar区块链
原理与实践

宋文鹏 梁然 韩丰 ◎ 著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Stellar 区块链：原理与实践 / 宋文鹏，梁然，韩丰著 . —北京：机械工业出版社，2019.4
（区块链技术丛书）

ISBN 978-7-111-62553-7

I. S… II. ①宋… ②梁… ③韩… 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 074698 号

Stellar 区块链：原理与实践

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：李 艺 责任校对：殷 虹
印 刷：北京市兆成印刷有限责任公司 版 次：2019 年 5 月第 1 版第 1 次印刷
开 本：186mm × 240mm 1/16 印 张：13
书 号：ISBN 978-7-111-62553-7 定 价：79.00 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

Preface 序

I co-founded Stellar Development Foundation（SDF）in early 2014 to build the Stellar network. From the very beginning and still today many of the most active contributors and supporters have been from the Chinese community. It took years of engineering effort by some of the most talented developers in the world to create and implement the Stellar network. But we got there and now Stellar is now growing rapidly and being used all over the world for a variety of things, cross border payments, tokenizing all kinds of assets, trading, etc. SDF is currently working on scalability. We are implementing things like payments channels and sub-networks to make the network scale way beyond its current capacity.

It is also no longer just SDF pushing things forward. There are now many companies built on top of Stellar and contributing to the ecosystem. It has been an amazing journey so far and although there is still a lot to do we are getting close to achieving our goal of creating an internet level protocol for payments and financial activity. This will level the playing field for everyone and increase not just financial inclusion but economic participation and lead to all kinds of interesting innovation and benefits for everyone.

Wenpeng Song, Ran Liang and Feng Han are all early participants in the Chinese technology community and Stellar community. I'm really excited that they are still involved and thank them for the books they brought to the Stellar technology community. Looking forward to the road ahead!

Jed McCaleb

前　言 Preface

当下，区块链技术受到越来越多的关注，区块链作为一种基础操作系统，是各种技术的黏合剂，是在不可信网络下实现可信交易（事务 / 业务）的一种手段，是在数据确权基础上的一种有效价值流通手段，是改变社会协作关系的一种有效途径。

区块链技术在当前处于发展早期阶段，各种区块链基础协议层出不穷，各种技术和思想百家争鸣，为了讨论方便，书中的图尽量采用 UML（统一建模语言）形式表达，同时，为达成共识，给出了以下统一基础术语：

- 区块链技术：一种分布式记账技术，各类与区块链相关技术的统称。
- 分布式记账技术：一种分布式技术，是区块链技术的超集和泛化。
- 账页：通常认为是区块链数据中的一个区块，包含了事务集合和额外区块头信息。
- 分布式账本：是账页的集合，区块链数据承载在分布式账本中。
- 区块链基础协议：通常含有 P2P、共识机制、密码学和智能合约等几部分的一种区块链技术完整实现。
- 区块链网络：区块链基础协议的实例化部署，一个区块链基础协议可以部署任意个区块链网络。

Stellar 区块链基础协议自 2014 年创建以来，其技术成熟度逐步得到业界认可，自身的技术社区逐步发展壮大。Stellar 自身的特征特点为开展区块链场景应用提供了很好的基础条件，为区块链基础协议开发提供了很好的实现参考依据。

本书结构

本书从逻辑上分为五部分：

第一部分（第 1 ～ 3 章）重点从工程实践的角度来审视区块链技术，介绍了区块链的基础

概念和 Stellar 区块链基础协议的概念。

第二部分（第 4、5 章）给出了两个典型的应用场景案例，一个是数据确权的应用场景，一个是基于数据确权的价值流通应用场景，展现了区块链的两层应用，引导读者结合区块链开展工程实践应用。

第三部分（第 6 章）给出了基于 Stellar 区块链技术的系统架构设计参考，从业务架构设计、逻辑架构设计、物理架构设计、数据架构设计和账户架构设计等几方面给出了关键架构设计要点。

第四部分（第 7、8 章）详细说明了如何将一个 stellar-core 区块链节点接入已有的 Stellar 区块链网络中，并搭建 horizon 实例以实现对外提供访问区块链网络的服务能力，同时，给出了搭建一个新的 Stellar 区块链网络的详细步骤，并介绍了对关键代码的定制化改造。

第五部分（第 9 章）介绍了 Stellar 技术社区已有的工具，以及将 Stellar 区块链技术和已有业务系统快速集成的方法。

本书读者对象

本书读者对象主要包括：

- 区块链技术开发者；
- 区块链应用产品经理；
- 技术架构师和业务架构师；
- 部分技术驱动型企业的中高层管理者。

致谢

本书的萌芽从 2016 年开始产生。笔者在进行基于 Stellar 的区块链系统开发过程中，基于 Stellar 官方文档，整理了大量的开发文档。为了方便区块链技术社区了解 Stellar 区块链技术，开阔思路，本书的三位作者，自 2017 年年底以来，经过一年多的讨论、收集社区反馈、对知识框架进行整理和重构，终于完成本书。

本书成书过程中得到了 Stellar 技术社区的早期参与者程宽、Ella、走路、老虎、陈斌等的鼓励和帮助，同时也得到 Stellar 区块链技术创始人 Jed McCaleb 先生的大力支持，Stellar 技术社区的小伙伴也提供了大量的反馈，在此一并谢过。

感谢机械工业出版的杨福川主编、李良编辑和李艺编辑细心指导和卓有成效的付出，同

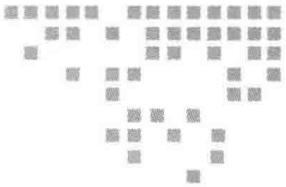
时，感谢爱人和父母的理解和支持，感谢所有在本书创作过程中以不同形式参与的同学和朋友。

区块链技术发展日新月异，各种区块链新技术不断提出，Stellar 区块链技术自身也在快速迭代，本书无法及时同步最新的技术变化，所以存在不足不可避免，欢迎各位读者朋友批评指正。

宋文鹏

2019 年于北京

Contents 目　录



第 1 章 Chapter 1

区块链基础

1.1 关键特征

区块链是一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理[⊖]的模式。

区块链通过 P2P 网络、共识机制、密码学和智能合约等四个基础功能模块，可以实现可信、匿名、可审计和成本低四大关键特征。其中智能合约不是区块链基础协议中必备的功能模块。

区块链中每条数据都经过签名和验签过程，明确数据归属，实现数据确权，确保数据来源的可信性。通过共识机制实现了数据防篡改，以技术手段保证了数据“只增不减”的可信性。通过数据可信实现价值交换可信。

注意 区块链的一个关键特点就是能实现数据确权，数据谁产生谁拥有。数据拥有者通过数据加密 / 解密的方式可以有效控制数据访问边界，但不可以删除。通常情况下区块链基础协议中不支持数据加密 / 解密，需要根据场景进行扩展。

区块链账户（尤其是当前的公有区块链网络）可以随意开立，与现实世界的人或者物未做到清晰映射，体现匿名性。但匿名性具有相对性，在进行有效的实名认证的基础上，明晰映射关系，基于区块链账本的确权数据，可以有效跟踪账户之间的操作关系，实施穿透式监管。

⊖ 事务处理包括但不限于可信数据的产生、存取和使用等。摘自中国区块链技术和产业发展论坛团体标准《区块链参考架构》。

区块链网络在业务逻辑层面表现为账户与账户之间各种关联关系的集合，同时由于分布式账本的数据可防篡改和透明可查，所以可以有效实现审计业务全过程。

通过区块链实现业务场景，可将不必要的中介去掉，用技术手段进行信任保证，对比传统的人为控制方式，可以有效降低价值交换成本。同时，在联盟链和专有链的实施过程中，可以有效降低 IT 实施成本和业务运营成本。

注意 区块链网络是一个虚拟世界，为了产生价值，不可避免地要与现实世界进行关联，需要有关键服务提供者为现实世界与区块链世界进行桥接，例如实名认证、确定事件源、资产和资金等，这类关键服务提供者本身就是传统的中心化可信机构，所以区块链只是将不必要的中介去掉了。

1.2 适合场景

区块链是目前解决“信任”问题最好的手段之一。

在参与方众多且跨领域明显的产业链条中，信息流转复杂性高，信息的真实性有待考证，导致业务运营效率低、风控成本高。同时，信任问题可能损害产业链中某一方的合法利益。

信息流转的任意一个环节都可能出现信息信任问题，无法有效确认问题的责任方，弱势一方的权益就会受到损害，造成不对等情况出现。当信息高度集中在产业链中的某一方时，如果做不到行业自律，将会对产业链的发展造成不良影响，严重者还可能导致产业动荡。

合理利用区块链技术可解决这些问题，可打破信息壁垒，确保信息的真实可靠、可查可追溯，出现问题可以迅速追溯审计，进行定责指正，使产业链条中所有参与方拥有平等的获取真实信息的权利，最大限度地保护自己的合法利益不受侵害。

区块链的应用场景包括两个层次。

- **首先是数据确权**。改变传统的人为控制，通过技术控制手段实现数据归属明确、数据防篡改和数据可访问等功能，在参与方众多、不同的利益体、跨越领域广泛等场景下，解决获取真实信息困难、审计成本高、不易存证、容易产生信息孤岛等问题。
- **其次是基于数据确权基础上的价值交换**。区块链技术是一种可信的记账技术，在可信的数据共享前提下，特别是在某个固定商圈，解决资金对账链条长、清结算复杂和运营效率低下等问题。

注意 区块链技术特别适用于涉及利益方多、混业经营的场景。通过解决涉众方的信任问题，实现混业创新场景应用。

1.3　关键组成

前面提过，区块链技术的基础协议主要由四个核心部分组成：P2P 网络、共识机制、密码学和智能合约。区块链基础协议的实例化形成区块链网络，基于区块链网络搭建各类应用。这些核心技术组成部分共同维护着整个区块链网络的安全可靠。

注意　智能合约并不是区块链基础协议的必备核心功能模块，当前并不是所有区块链基础协议都包含智能合约模块。

1.3.1　P2P 网络

P2P（Peer to Peer）网络又称对等网络，是由一个无须中心化的机构来做协调，用户（Peer）间平等通信的网络。网络中的资源和服务分散在所有网络节点上，无须中间网络节点介入，因此随着网络节点数量的逐步增多，在网络扩展性和健壮性方面会表现得更加优越。

在这样的网络中，每个用户（Peer）都可以直接对接其他用户（Peer），在特定的场景下，用户（Peer）间直接对接可以节省时间，提高效率，如图 1-1 所示。

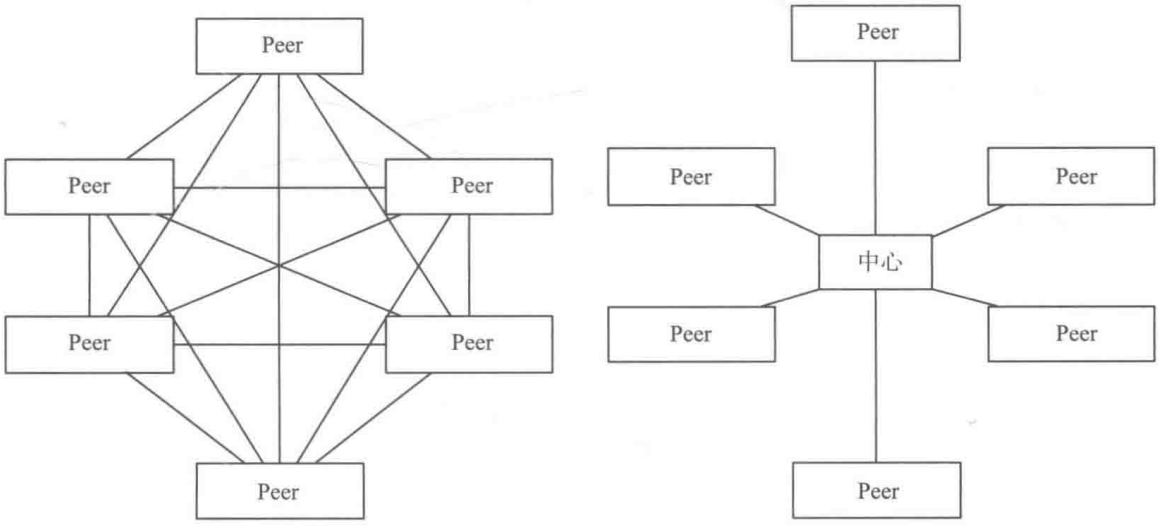


图 1-1　P2P 网络对比中心化网络

P2P 网络主要有以下 4 个特性。

1. 可扩展性

在 P2P 网络中，随着网络节点的加入，系统整体的服务能力也在同步扩充，理论上其可扩展性几乎是无限的。