新人必读：区块链实用型技能树

原创 张开翔 FISCO BCOS开源社区 2019-12-12

张开翔

FISCO BCOS 首席架构师

联盟链老司机

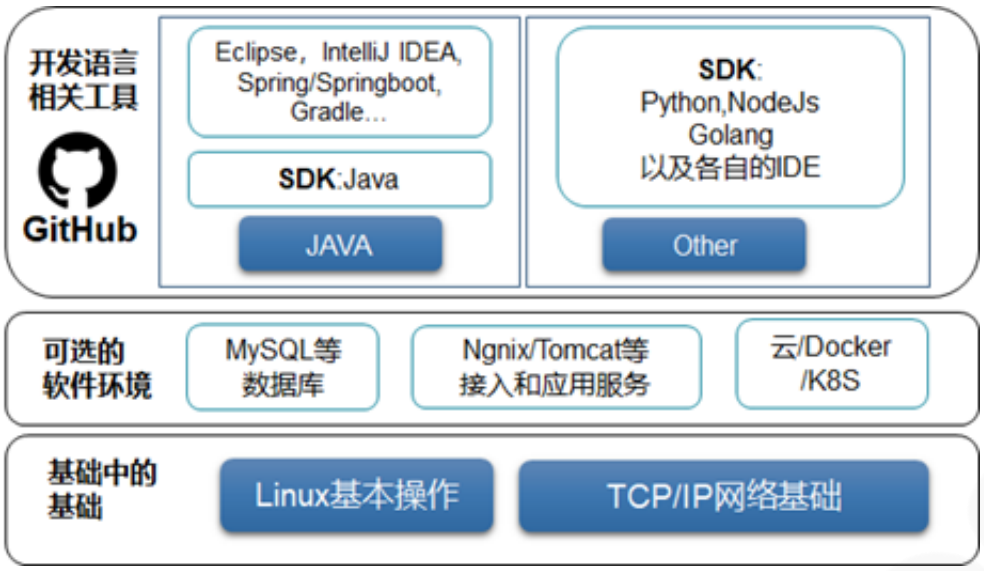
AUTHOR | 作者

随着新一波的区块链热潮，许多同学怀着巨大的热情进入了这个领域，同时也会遇到不少疑惑，区块链开发需要哪些知识？怎么学习？从哪里学习？遇到问题怎么办？本文将试图给区块链领域新人一个快速实用的指引。

FISCO BCOS

一、基本IT技能

区块链堪称“黑科技”，本身具有大量的技术元素，有志于从技术角度切入区块链的人，应该具备或掌握基本的IT技能，达到至少是常规级别“程序员”或“系统管理员”的技能水平。



首先需要熟练的Linux操作系统知识。

大多数区块链系统是可以跑在Linux上的，包括CentOS和Ubuntu等，你至少要会一些基本的Linux操作指令，比如ls查看目录、ps或top查看进程、find查找文件、netstat查看网络、ulimit检查系统参数限制、df/du查看磁盘空间、用apt/yum安装软件等等，如果这些基本命令都不掌握，在Linux上操作肯定是举步维艰的。

这方面的书和资料都很多，相信一星期就能上手。另外，善于Linux的man指令，可以获得每个命令的详细帮助。如果学会写shell脚本，那更如虎添翼，可以把大量的繁琐操作给自动化了。

要有清晰的网络概念。

区块链本来是分布式系统，节点之间一定是通过网络相连的，只是跑起来的话，不需要多高深的网络知识，只需要了解什么是TCP/IP；公网、内网、本地地址的区别；端口如何配置；节点和节点、SDK和节点之间的互联是否会被防火墙和网络策略挡住；采用ifconfig、telnet、ping、netstat等命令检查网络信息和进行探测、定位网络问题。一般来说，Linux书籍也都会介绍这部分内容。

区块链周边的支持，如浏览器、中间件、业务应用，会依赖一些第三方基础软件，如MySQL/MariaDB数据库、Nginx服务、Tomcat服务等，至少懂得怎么去安装指定版本的软件，掌握修改这些软件的配置文件并使之生效的基本操作，了解各款软件的密码、权限配置和网络安全策略，以保护自身安全。

如果是基于云、docker或者k8s等容器环境构建，需要了解使用的服务商或容器的功能、性能、配置方式，包括对资源的分配：CPU、内存、带宽、存储等，以及安全和权限的配置、网络策略

配置、运维方式，达到轻松分发构建的同时，还能保持其稳定性和可用性。

各种云服务商和容器解决方案都有周全的文档和客服服务渠道，可以帮助用户顺畅地使用。

到编程语言阶段，可以根据自己的学习路径，选择不同的语言。

如果是使用Java语言，那就应该熟练掌握Eclipse、IntelliJ IDEA等集成IDE，熟悉Gradle为主的工程管理软件，熟悉Spring、Springboot等java的基础开发组件，熟悉在IDE或命令行下对资源路径如ApplicationContext等路径的定义，或许还有myBatis等流行的组件，这些都可以在java相关的社区和网站找到资料和书籍。

在熟练使用Java语言的情况下，采用Java SDK接入到区块链，跑起一个Demo Sample，将是非常轻松写意的事情。

如果是采用其他语言，我们也提供了Python、Node.js、Golang等语言的区块链SDK。

不同的语言，其安装包有不同的稳定版本，会采用不同的环境和依赖安装配置方法，会有不同的IDE和调试方法，就不在本文一一罗列，相信学习和使用语言这件事本身，于程序员已经是最基本的技能了。

最后，作为在开源世界里冲浪的玩家，“全球最大同性交友网站”——github一定是要上的了。

注册github账号，掌握git版本管理工具的基本操作，clone和pull开源软件代码，提交issue，commit自己的修改，给开源项目提交pull request，再顺手点个star，激情而有范儿，在开源世界里留下你的姓名。

二、区块链领域的基础知识栈

以下部分的知识和区块链或区块链某一个平台更加相关，从底到上依次是：

HASH（哈希算法）、签名、证书

严格来说，这并不是区块链领域的专有知识，只是必须具备的基础知识，包括SHA3/SHA256/RIPEMD160等摘要算法，以及这些算法和“区块链地址”的关系，基于公私钥的数字签名和验证方法，数字证书的概念和格式，比如X.509证书，以及保存证书/公私钥的文件格式，如PEM文件、keystore文件等。

基础应用密码学

基础应用密码学其实范围很广，作为入门者，至少要了解对称和非对称加密的常见算法，如AES对称加密，RSA、ECDSA椭圆曲线等非对称加密算法，以及这些算法在签名验签、数据加密、通信协商和保护方面的作用。如果要使用国密，那么需要了解SM2~SM9一系列算法的概念和使用。

分布式网络结构

区块链是先天的“分布式网络系统”，节点和节点通过网络的P2P端口互连，客户端、SDK通过RPC/Channel端口互连，首先要保证网络之间是互通的，监听的地址和端口是对的，端口是开放的，防火墙和网络策略是正确的，用于安全连接的证书已经到位，才能保证区块链的“通则不痛”。

这也要求使用者具备基本的网络知识、网络工具，同时了解区块链特有的节点类型（共识节点、观察节点、轻节点等）、互连方式（点对点双向连接、JSON RPC的HTTP短连接、Channel长连接等）。详情点击参考《FISCO BCOS网络端口讲解》。

智能合约

智能合约可说是应用开发者直面区块链的一道大门，入得此门，精彩无穷。流行的智能合约语言是Solidity语言，这门源自以太坊，从诞生开始就是为区块链而来的。

Solidity语言更新活跃、文档完备，具有良好的一致性和事务性，功能足够实现中型的商业应用。

当然，它在实时调试、第三库支持、运行速度等方面还比不上成熟的语言，如果开发者想要用C++等语言编写智能合约，那就要对区块链上的计算范式进行深入了解，避免写出无法共识的智能合约来，一般是建议有深入的了解后再采用Solidity之外的其他语言编写合约。

要掌握Solidity合约，当然是通读文档，并动手尝试。具体参考以下文档：
https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/manual/smart_contract.html

ABI接口原理

在采用EVM作为虚拟机的区块链上，EVM执行的是Solidity语言的合约。合约编译会生成后缀名为ABI的文件，其实里面就是该合约接口定义的JSON文本，可以用文本查看器查阅，了解你写的合约如何翻译成ABI里的接口，接口返回类型，参数列表，参数类型等，只要有合约的ABI文件，就可以调用区块链SDK的接口，解析这个合约相关的交易、返回值、回执等。

区块数据结构

区块（Block）有区块头和区块体。区块体有交易列表，交易列表里的每个交易（Transaction或Tx）有发起方、目标地址、调用方法和参数，以及发送者签名。交易的结果会生成一个“回执（Receipt）”，回执里包含被调用方法的返回值、运行过程生成的EventLog等……

了解这些，基本上就掌握了区块链数据的脉络，还可以继续深究数据结构里的merkle root以及对应的merkle tree是如何生成的，有什么作用（如用于SPV：Simplified PaymentVerification）。具体参考以下文档：

https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/design/protocol_description.html

RPC接口

这里把区块链节点暴露的功能接口统称为“RPC接口”。查看链上数据，包括区块、交易、回执、系统信息、配置信息，向链上发起交易，以调用智能合约、修改系统配置等，或者通过AMOP协议发送消息、监听事件，都是通过RPC接口。

几十个RPC接口建议一一走读，或善用搜索，以发现自己想要的接口。

接口通信采用的协议可能是JSON RPC，或者是FISCO BCOS独创的Channel协议，SDK基本上已经对接口和协议进行了良好的包装，也可以在深入理解ABI和RLP等编码模式前提下自行开发接口客户端。具体参考以下文档：
https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/api.html

准入和权限模型

联盟链强调安全可控，节点准入是第一步，在链初始化后，其他节点或者SDK配置了相应的证书，才能接入到既有的联盟链上。

链上的角色用权限模型控制，包括管理员权限、发布合约的权限、创建表的权限、参数配置权限等，以避免角色之间操作混淆，某些角色既当运动员又当裁判员。

初学者需要仔细阅读区块链平台提供的技术文档了解原理，遵循操作手册的步骤进行操作。具体参考以下文档：
https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/manual/permission_control.html

数据存储模型

区块链节点会采用文件数据库（LevelDB或RocksDB），或者关系型数据库如MySQL保存数据，所以，链上是真的有“数据库”的。

写入数据库的数据包括区块、交易、回执、合约产生的状态数据等，是否写入“调用合约产生的历史数据”根据不同的平台而定，FISCO BCOS默认只保存最新的状态值，可以选择性地将修改记录

写入“回执”或“历史表”里进行追踪。

FISCO BCOS还提供方案，将历史数据导出到链下数据库进行关联分析。具体参考以下文档：
https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/design/storage/index.html

共识机制原理

联盟链通常采用插件化共识机制实现，FISCO BCOS提供PBFT和RAFT两种高效共识算法，而不会采用“挖矿”这些高耗能低效率的共识。

共识机制是区块链的灵魂，对共识机制进行深入学习，才可以深入理解区块链通过多方协作、达成高度一致性、支持交易事务性、防篡改防作恶的功效。具体参考以下文档：
https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/design/consensus/index.html

区块链的知识包罗万象，更深层次的知识还有分布式系统理论、博弈论、前沿密码学、经济学、社会学等，掌握以上的基础知识，再深入学习，举一反三，用场景去验证和探索创新式应用，方可发挥技术的潜力，感受分布式商业的魅力。

三、做一个怎样的学习者

在这个过程中，希望学习者做到：

读文档的耐心

我们的开源项目文档足有20万字以上的篇幅，公众号里还有大量的技术解析和科普文章，这都是程序员们在coding之外，用尽自己仅有的语文储备，码出的海量文字，是一笔巨大的技术财富，涵盖了相关开源项目的方方面面。如果能通读，或者记住文档结构和标题，需要时快速打开，足以解惑且深入。

搜资料的能力

文档、公众号都有搜索功能，当想起和开源社区有关的问题时，可以随手用关键字搜索，一般都

能找到答案。如果有语言不详之处，可以向开源项目团队提出，或者根据自己的理解进行补充。通用的知识点，如操作系统、网络等，通过公网搜索引擎，一般都能找到答案。

排查环境和依赖问题的能力

开源软件牵涉的系统环境、第三方软件、软件的版本等常常有错综复杂的依赖关系，太高或太低的版本都可能会有一些问题，请注意阅读项目文档对软硬件环境和依赖的描述，保证自己的环境符合要求，并善用配置管理工具、软件安装工具获取和设置合适的版本。

调试能力

如上所述，Solidity语言的调试工具完善程度尚未达到完美，但可以善用合约的返回值、EventLog等方式，通过WeBASE、控制台等趁手的工具进行调试，并查阅Solidity文档，了解问题可能出在哪里。

区块链节点的日志开启debug级别后，也会打印详细的信息，可以查阅运行日志，获取运行信息和可能的错误信息，将这些信息与自己所做的操作比如发交易的流程结合起来进行分析，提高调试效率。

同时，目前的开源软件通常会在屏幕上打印错误原因和解决问题的提示，仔细查看操作反馈，大概率能了解错误原因和解决方案。

代码阅读能力

开源软件的最大效能是把代码毫无遗漏的摊到了开发者和学习者面前，了解代码结构，查阅代码里的关键流程，用关键字去搜索代码里的对应实现，都可以深入系统细节，挖掘设计思想，定位问题，寻找优化方法。一个好学且硬核的程序员，足可通过代码，和世界对话。

问问题的方式方法

“一个好问题，比答案还重要”。我们的社区非常活跃，大家都很热情地答复和解决问题。我们鼓励在社区里公开提出问题，一方面使大家都可以分享问题，找到解决方案，另一方面提问者也可以得到更多人的帮助。同时，希望提问者提出问题时，一次性描述详尽，把相关的操作步骤、系统环境、软件版本、出错提示以及希望得到的解决方案都提出来。

如果是通用性的问题，可以先搜索再提问，有利于培养独立解决问题的能力。希望提问者能向社

区反馈更深层次的问题，以帮助社区快速优化。对很多典型问题，社区也积累了一些行之有效的解决方案，我们会整理和公布出来，以便查阅。

从新人到老鸟的路也许漫漫，如果能参考这篇小文的一些方法，可以少踩许多坑，多写一些应用。Enjoy blockchain，社区与你共同进步。

FISCO BCOS

资源链接：

各项开源组件索引：
https://fintech.webank.com/

FISCO BCOS开源文档：
https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/

新人请注重阅读：

关键概念：
https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/tutorial/key_concepts.html

以及使用手册：
https://fisco-bcos-documentation.readthedocs.io/zh_CN/latest/docs/manual/index.html

FISCO BCOS公众号的开发教程仓库：
http://mp.weixin.qq.com/mp/homepage?__biz=MzU5NTg0MjA4MA==&hid=9&sn=7edf9a62a2f45494671c91f0608db903&scene=18#wechat_redirect

《麻雀虽小五脏俱全 | 从Python-SDK谈谈FISCO BCOS多语言SDK》，此文详细讲解了从客户端的应用出发，去理解区块链接口的方法。

Solidity智能合约（中文）：

https://solidity-cn.readthedocs.io/（注意选择对应版本）

Solidity智能合约（英文）：

https://solidity.readthedocs.io/（注意选择对应版本）

《如何优雅地写智能合约》

《WeBASE数据导出：助力区块链大数据场景快速落地》，区块链数据导出到链外，采用海量数据存储。

图形化的区块链，WeBase文档：

https://webasedoc.readthedocs.io/zh_CN/latest/index.html

推荐书目：

《鸟哥的linux私房菜》（系列）

https://book.douban.com/subject/2208530/

《UNIX网络编程》（系列）

https://book.douban.com/subject/1500149/

《java核心技术》（系列）

https://book.douban.com/subject/26880667/

《Springboot实战》

https://book.douban.com/subject/26857423/

《Spring实战》

https://book.douban.com/subject/26767354/

FISCO BCOS的代码完全开源且免费

下载地址↓↓↓

https://github.com/FISCO-BCOS/FISCO-BCOS