资深区块链专家撰写，ChinaLedger技术委员会主任白硕和多个区块链公司的CTO、科学家联袂推荐

零基础掌握以太坊的关键技术、工作原理和DApp开发方法，多个案例实战并附实战项目源代码

区块链技术丛书

BLOCKCHAIN IN ACTION

Key Technology and Case Analysis for Ethereum

区块链开发实战

以太坊关键技术与案例分析

吴寿鹤　冯翔　刘涛　周广益◎著

机械工业出版社
China Machine Press

区块链技术丛书

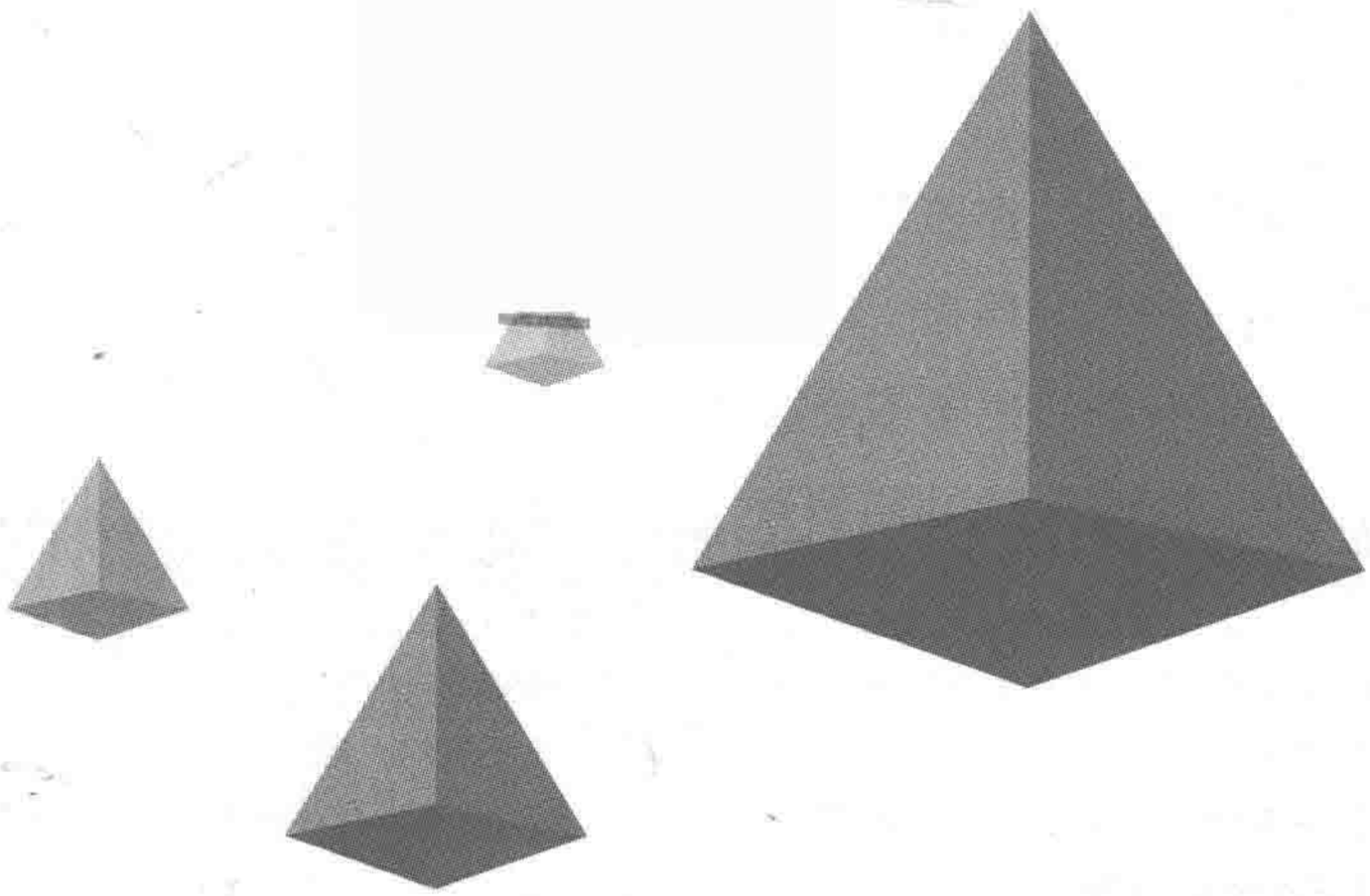
BLOCKCHAIN IN ACTION

Key Technology and Case Analysis for Ethereum

区块链开发实战

以太坊关键技术与案例分析

吴寿鹤 冯翔 刘涛 周广益◎著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

区块链开发实战：以太坊关键技术与案例分析 / 吴寿鹤等著 . —北京：机械工业出版社，2018.5
（区块链技术丛书）

ISBN 978-7-111-59956-2

I. 区… II. 吴… III. 电子商务 – 支付方式 – 案例 IV. F713.361.3

中国版本图书馆 CIP 数据核字（2018）第 095174 号

区块链开发实战：以太坊关键技术与案例分析

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：张锡鹏　　责任校对：殷　虹
印　　刷：北京市兆成印刷有限责任公司　　版　　次：2018 年 6 月第 1 版第 1 次印刷
开　　本：186mm × 240mm　1/16　　印　　张：15
书　　号：ISBN 978-7-111-59956-2　　定　　价：69.00 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　88379649　68995259　　读者信箱：hzit@hzbook.com

Preface 前　言

为何写作本书

近年来区块链技术逐步占据各大技术类网站的头条，各种基于区块链特性的想法和创新层出不穷。这些繁荣是区块链技术在幕后默默支撑的，可是人们经常忽略区块链的技术而把投资、融资、保值等金融属性和区块链画上了等号。其实区块链本质上还是一门技术。区块链技术源于比特币，经过近几年的发展，已经超越比特币逐步形成一门单独的技术体系。目前区块链技术已经渗透到各行各业中，比如区块链技术同大数据、人工智能等技术产生了让人意想不到的化学反应。我们有理由相信区块链技术在未来一定会成为 IT 基础技术之一，成为每个 IT 技术人员必备的基础技能。

同时我们也可以看到区块链技术在国内外的发展非常迅速。在国外，IBM 发起了超级账本项目，并把超级账本项目的源码捐献给了 Linux 基金，借助社区的力量来发展。全球已经有将近 200 多个公司和组织加入了超级账本，成为超级账本项目的会员。当然其他巨头也随之跟进，微软早就和以太坊达成了战略合作协议。互联网巨头 Google、社交媒体行业的龙头 Facebook 等在区块链领域均有所布局。

但是在繁荣的背后我们也应该看到危机，目前区块链技术在实际项目中的应用还存在不少问题。我们认为出现这种情况是因为目前区块链技术的实用化还存在以下障碍：

- 技术新，学习资料匮乏。区块链技术是最近几年刚刚兴起的一门综合技术，目前资料特别是中文资料还是比较缺乏的。
- 技术种类多，有一定的学习成本。区块链是一门综合型的技术，如果把每个单项技术列出来学习并不难，但是当把这些技术组合起来之后学习难度就大大增加了。
- 可借鉴的成功案例少。由于区块链技术是一门比较新的技术，因此目前缺少比较成功的案例。即使诸如 IBM 等巨头开发了一些成功案例，但是由于各种各样的原因，目

前并没有公开，这些都给广大技术人员学习区块链技术特别是把区块链技术应用到具体项目中造成了一定的障碍。

这些问题的存在是我们编写“区块链开发实战”系列图书的目的，第一批有两本书同时面世，分别是基于 Hyperledger Fabric 和以太坊进行区块链开发实战。我们希望读者通过这两本书，在了解区块链的基本概念和核心技术的同时，能够将区块链技术更多应用到具体的项目中，解决现有技术无法解决的一些行业痛点。

读者对象

这两本书都非常适合区块链开发工程师、区块链架构师、区块链技术爱好者阅读。

其中：

- Hyperledger Fabric 部分更适合对 Hyperledger Fabric 和比特币技术感兴趣的相关技术人员；
- 以太坊部分更适合以太坊爱好者、以太坊 DAPP 开发者、比特币开发者等。

主要内容

《区块链开发实战：Hyperledger Fabric 关键技术与案例分析》

这本书以 Hyperledger Fabric 和比特币这两个典型区块链技术平台的核心技术、开发方法和相关的项目案例为核心内容，此外，还提供了大量的命令脚本和代码示例供读者参考，力图使读者在最短的时间内掌握这两个平台的使用方法。

全书分为三个部分：

- 第一部分（第 1 ～ 2 章）：首先从基本认识的角度对区块链进行了宏观上的介绍，包括区块链技术的起源和演进过程、区块链核心技术及其特性、区块链技术的缺点和常见错误认识，以及区块链技术的应用领域和常见的技术框架；然后介绍了进行区块链开发需要掌握的技术和使用的工具。
- 第二部分（第 3 ～ 13 章）：主要讲解了 Hyperledger Fabric 的核心技术、原理、开发方法，以及多个项目案例。包括 Hyperledger 的全面介绍、Fabric 的技术特性和快速入门、Fabric 的核心模块和账号体系、Fabric 的智能合约和编程接口、Fabric 的系统架构与设计、Fabric 项目案例的开发流程和方法，以及几个综合性的案例，如区块链浏览器、供应链金融、食品溯源等。
- 第三部分（附录）：主要讲解了比特币的原理、运行方式、重要模块和编程接口，同时还讲解了一个比特币客户端的案例。

《区块链开发实战：以太坊关键技术与案例分析》

本书详细讲解了以太坊和比特币这两个典型的区块链技术平台的技术特性、原理、开发方法，同时也配有多个综合性的项目实例。

全书分为三个部分：

- 第一部分（第 1 ～ 2 章）：首先从基本认识的角度对区块链进行了宏观上的介绍，包括区块链技术的起源和演进过程、区块链核心技术及其特性、区块链技术的缺点和常见错误认识，以及区块链技术的应用领域和常见的技术框架；然后介绍了进行区块链开发需要掌握的技术和使用的工具。
- 第二部分（第 3 ～ 11 章）：主要讲解了以太坊的基本使用、技术特性、工作原理、开发方法和项目案例。首先介绍了以太坊的各种核心概念——编译、安装、运行，以及私有链的搭建和运行等基础内容；其次详细讲解了 Solidity 语法、Solidity IDE、Solidity 智能合约的编译部署，以及 Solidity 的智能合约框架 Truffle；最后讲解了 DApps 开发的方法和流程。
- 第三部分（附录及后记）：主要讲解了比特币的原理、运行方式、重要模块和编程接口，同时还讲解了一个比特币客户端的案例。

为什么两本书有重复内容

大家可能注意到，两本书有部分内容是重复的，这么安排并不是为了凑篇幅，而是经过精心考虑的。主要原因如下：

- 以太坊和 Hyperledger Fabric 是两个不同的技术平台，涉及的技术都非常多，读者一般不会同时学习并在这两个平台上进行开发，于是我们没有将这两个主题的内容放到一本书中，这样便于读者按需选择。
- 两本书的前两章是相同的，因为这两章的内容对两个平台的用户来说是通用的，而且是都需要了解和学习的。
- 两本书关于比特币的内容是相同的，因为比特币系统是出现最早、运行最稳定的区块链技术平台，它的很多概念和核心技术对其他区块链平台有非常好的借鉴意义，值得所有区块链开发者学习。

主要特色

这两本书是作者在参与众多区块链项目之后提炼而成，具有以下特点：

- 既没有高深的理论也没有晦涩难懂的公式，力求通过最简单通俗的语言和大量的图表让读者能够了解区块链技术的精髓。

- 提供大量的命令脚本和相关程序的源代码文件，这些命令脚本和源代码文件都来自实际的项目，我们整理后展现给读者，通过这些命令和源代码读者可以了解到相关区块链技术平台的操作细节。
- 提供了大量的项目案例，这些项目案例能够帮助读者更好地理解区块链技术和业务场景的结合。
- 与国内专业的区块链技术社区——“区块链兄弟”深度合作，社区中有两本书的专题页面，读者可以到社区中与作者和其他读者进行深入交流。

本书相关源代码下载地址：https://github.com/blockchain-technical-practice。

致谢

这本书能够完成首先要感谢机械工业出版社华章公司的杨福川先生为本书的顺利出版付出的努力。同时我们要感谢区块链技术社区的全体“兄弟”，你们对区块链的探索和执着是我们创作的动力，你们对区块链的付出和努力给我们提供了创作的素材。在编写这本书的过程中无论是提问题的“兄弟”，还是回答问题的专家“兄弟”，感谢你们。最后我们还要感谢所有加入的区块链技术讨论组，在和你们的交流中我们发现了本书的价值。

本书编写小组

2018 年 2 月于上海

Contents 目　录

第1章 Chapter 1

全面认识区块链

人类自诞生以来，一直对物质移动的速度有着孜孜不倦的追求和探索。在人类探索和改造世界的过程中，绝大多数具有颠覆性的技术创新都与物质传递的速度有着非常密切的联系。比如轮子改变人和物体传递的方式，铁轨改变人和物体传递的效率，电力的出现改变了能量的传递方式，互联网的诞生则是彻底颠覆了信息传递的方式和效率。

区块链技术被认为是轮子、铁轨、电力、互联网之后，又一个具备颠覆性的核心技术。作为一种构建价值互联网的底层技术，区块链改变的将是价值传递的方式。区块链的出现将解决人类社会诞生以来一直在思考的问题——如何获取未知的信任。区块链技术到底是怎样一种技术？本章将从宏观角度介绍这个问题。

1.1 区块链技术的起源和解释

提到区块链技术，比特币是无法回避的一个重要部分，因为比特币是迄今为止出现最早、规模最大、运行最稳定、技术最成熟的基于区块链技术的应用。2008 年一个网名叫“中本聪”的人发表了一篇名为《比特币：一个点对点的电子现金系统》的论文。在该论文中，“中本聪”描绘了一个完全去中心化的电子现金系统，在这个系统中每一个参与者都是独立并且对等的，这些参与者不依赖于通货保障或者结算交易验证保障的中央权威。

为了实现这套系统，相关的技术社区利用密码学中的椭圆曲线数字签名算法（ECDSA）来实现数据的加密，基于 P2P 网络来实现数据的分布式存储，从而实现了一个去中心化的，不可逆、不可篡改的特殊数据存储系统。这套系统就是目前被称为区块链技术的雏形。比特

币就是构建在区块链技术之上典型的成功应用。比特币系统这些年来稳定而且高效的运行，证明了这些技术理论的正确性和可靠性。

随着业界对比特币系统技术架构的深入了解，人们发现这些技术除了应用在比特币上面之外，还能应用在其他领域。于是相关技术社区将这些技术抽象之后给它们起了一个统一的名字：区块链。从此区块链脱离比特币成为一门单独的技术。

目前区块链已经成为一个独立的技术名词，而不是依赖于某个具体产品的附属技术。区块链这个技术名词，从不同的角度看会有不同的解释。

- 从网络的角度看：区块链的底层网络模型提供了分布式数据存储的完美实现，比特币系统从诞生至今没有发生过一次宕机事件，这有利地证明了该网络模型的稳定和高效。
- 从底层技术的角度看：区块链更像是一个数据结构，用区块存储数据，把区块按照顺序链接起来组成区块链，从而达到防止数据被篡改的目的。
- 从密码学的角度看：区块链利用椭圆曲线数字签名算法来保证数据的完整性和真实性。
- 从数据存储的角度看：区块链更像是一个分布式数据库，不但数据的存储是分布式的（以共享账本为例，所有的数据可以对等地存储在所有参与数据记录的节点中，而非集中存储于中心化的机构节点中），而且数据的产生也是分布式的（账本所有的节点集体维护，而非一个单独的中心机构来维护）。

区块链技术源于比特币但是高于比特币，发展至今，已经形成一个非常完整的技术栈。区块链技术栈中的每个单项技术并不是新发明的技术，如果将这些单项技术单独提取出来，都是比较普通的，但正是这些普通的技术通过精巧地组合之后诞生了一项足以颠覆世界的新技术。这和鸡尾酒非常相识，组成鸡尾酒的每个单独的原料都非常普通，但是组合之后就产生了非常神奇的化学反应，从而诞生了一个让人痴迷的新事物。

套用一句网络流行的话，重要的事情要说三遍：区块链不是一个单独的技术，而是由多种技术组成的技术栈，在学习区块链技术的时候一定要注意区块链技术的这个特性。所以如果想学会区块链技术首先需要对组成区块链技术栈的各个单项技术有所了解，然后再开始学习相关的区块链技术框架，这一点在基于区块链技术的项目实施中尤其重要。

1.2 区块链的核心技术及其特性

通过前面章节的介绍我们知道区块链技术是一个技术栈，由多种相关技术组成。那么区块链技术栈到底是由哪些具体技术组成的呢？在回答这个问题之前，我们先要了解一下区块链具有哪些特点。

1.2.1　区块链技术的特性

区块链技术有什么特点？这个问题很多人从不同的角度定义过。在这里，我们引用维基百科上面的说明：“区块链技术是基于去中心化的对等网络，用开源软件把密码学原理、时序数据和共识机制相结合，来保障分布式数据库中各节点的连贯和持续，使信息能即时验证、可追溯，但难以篡改和无法屏蔽，从而创造了一套隐私、高效、安全的共享价值体系。”通过这段描述我们可以把区块链技术的特点归纳为以下几点：

- 区块链没有一个统一的中心，数据分布式存储，并且每个节点是对等的。
- 数据存储按照特定的时序组织并且采用密码学原理加密，这样使得数据不可篡改（密码学加密）并且可以追溯（时序组织）。
- 数据的创建和维护由所有参与方共同参与，任何一方都不能在不经过其他参与方允许的情况下独立对数据进行维护。

这些特性是绝大多数区块链技术的基本特性，但是随着对区块链技术的深入研究，人们发现这些特性已经不能满足业务的需求，因此在区块链技术中增加了一些新的特性，这些新增的特性中最重要的就是智能合约。区块链的智能合约是条款以计算机语言而非法律语言记录的智能合同。智能合约让我们可以通过区块链与真实世界的资产进行交互。当一个预先编好的条件被触发时，智能合约执行相应的合同条款。

通过上面的描述我们可以发现区块链技术具有分布式数据库、密码学、P2P 网络等技术特点。区块链的这些技术特点，使得通过区块链技术可以构建一个去中心化的、安全的、对等的、不可更改的价值传播网络。这些技术通过精巧的组合之后，形成了一种全新的数据记录、传递、存储与展现的方式。以前数据的存储和维护都是由一个统一的中心机构来完成，而区块链技术可以让所有数据的参与方都有机会成为数据维护者。区块链技术在没有中央控制点的分布式对等网络下，使用分布式集体运作的方法，构建了一个 P2P 的自组织网络。通过复杂的校验机制，区块链数据库能够保持完整性、连续性和一致性，即使部分参与者作假也无法改变整个区块链的完整性，更无法篡改区块链中的数据。

现在我们可以对区块链的技术特点进行一下总结。区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链技术栈包含了以下技术特性：

- 分布式数据库的技术特性
- 密码学特性
- 共识机制
- 智能合约

1.2.2　区块链的分布式存储技术特性

从技术的特性上看，区块链具有分布式数据库技术的特点。传统的关系性数据库都必

须满足 ACID 原则，ACID 原则本质上是对事务而言的。在传统的关系型数据库中，事务是一个不能分割的操作单元。因此对于传统的关系数据库而言，事务必须具备以下四个特性：

- 原子性（Atomicity）：事务中的所有操作要么全部执行，要么全部拒绝，没有任何中间状态；
- 一致性（Consistency）：数据库的完整性约束不会被任何事务破坏；
- 隔离性（Isolation）：多个事务完全隔离开来，一个事务的执行不会被其他事务所影响；
- 持久性（Durability）：一个事务完成之后，该事务对数据库的变更会被永久地存在数据库中。

从 ACID 四个属性我们看出，区块链可以满足上面的部分特性。

- 原子性，区块链的数据存储在区块中，一个区块链中的数据要么全部进入区块链，要么全部被丢弃。
- 一致性，区块加入区块链之后原有的区块链保持不变。
- 隔离性，所有节点可以同时生成区块，但是最终只有一个区块可以加入区块链中。
- 持久性，一旦区块加入区块链中，就会被永久保存并复制到其他节点。

移动互联网对数据的存储数量以及数据的读写速度都提出了更高的要求，因此基于 ACID 的关系数据已经不能满足于业务的需求。相关技术社区在原有的 ACID 数据库的基础上面创建了分布式数据库系统。分布式数据库系统有这样一些特点，我们称之为 BASE。BASE 是一组单词的首字母缩写，它们是：

- 基本上可用（basically available）：主要的需求是可用性，即使出现划分的情况下，也应该允许更新，哪怕以牺牲一致性为代价；
- 软状态（soft state）：网络划分可能导致数据库每个副本都有一定程度不同的状态，从而导致整体状态不明；
- 最终一致性（eventually consistent）：当解决完划分后，要求最终所有副本形成一致。

和 ACID 的强一致性概念比较，BASE 面向的是可扩展的分布式系统。BASE 在牺牲强一致性的基础上换取了可用性，允许在某个时间段内不同节点之间存在数据的不一致性，但是最终所有节点的数据都是一致的。而区块链的节点是分布在全世界各个地方的，在一定的时间段内，不同节点的区块数存在不一致的情况，但是最终都是一致的。所以我们认为区块链是符合分布式数据库 BASE 规则的。通过上面的对比我们发现，区块链符合传统的关系数据库和互联网时代的分布式数据库特性。

1.2.3 区块链的密码学技术特性

为了保证数据的不可逆、不可篡改和可追溯，区块链采用了一些密码学相关的技术。主要使用的是哈希算法、Merkle 树、非对称加密算法这三种密码学中常用的技术。

1. 哈希算法

哈希算法将任意长度的二进制值映射为较短的固定长度的二进制值，这个小的二进制值称为哈希值。哈希值是一段数据唯一且极其紧凑的数值表示形式。如果哈希一段明文而且哪怕只更改该段落的一个字母，随后的哈希值都会发生变化。要找到哈希值相同而输入值不同的字符串，在计算上是不可能的。所以数据的哈希值可以检验数据的完整性。在哈希算法中如果输入数据有变化，则哈希也会发生变化。哈希算法可用于许多操作，包括身份验证和数字签名（也称为“消息摘要”），不过一般用于快速查找和加密算法。

区块链的数据是存储在区块中的，每个区块都有一个区块头，区块头存储区块中所有数据经过哈希算法获取的一个哈希值，同时每个区块中存储前面一个区块的哈希值，这样每个区块都会通过所存储的前一个区块的哈希值串联起来，这样就形成了区块链。如果有人试图篡改其中的一笔交易，势必会导致该交易所在区块的哈希值发生变化，为了使得被篡改的交易得到所有节点的认可，篡改者需要以被篡改的节点为起点，重新计算后面的所有区块，但是如果要让所有的节点都承认和接受这些篡改，那基本上是不可能完成的事情了。从这里我们可以发现哈希算法的应用使得篡改的成本已经远远超过收益了。

区块链系统常用的哈希算法是 SHA256 和 RIPEMD160。SHA256 是 SHA 算法的一个变体。SHA（安全散列算法）是由美国国家安全局（NSA）设计，美国国家标准与技术研究院（NIST）发布的一系列密码散列函数，包括 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512 等变体。这些算法主要适用于数字签名标准（Digital Signature Standard DSS）里面定义的数字签名算法（Digital Signature Algorithm DSA）。SHA256 算法在抗碰撞性和效率之间做了一个平衡处理，在很多区块链系统中均支持 SHA256 哈希算法。

对于哈希算法来说，抗碰撞性越高，相对需要的计算资源越大，对系统性能也会有一定的影响。因此很多区块链系统可以通过配置参数修改算法，使用者可以根据业务需求选择合适的哈希算法。

---

2. Merkle 树

通过前面的描述我们知道区块中的数据是存储在区块中的，一个区块中会存储若干数据，那么这些数据是以什么样的方式组织才能够做到不可篡改呢？ Merkle 树解决了这个问题。

（1）什么是 Merkle 树

Merkle 树是一种树（数据结构中所说的树），通常称为 Merkle Hash Tree。组成 Merkle 树的所有节点都是哈希值。Merkle 树具有以下特点：

- Merkle 树是一种树型数据结构，可以是二叉树也可以是多叉树，具有树型结构的所有特点；

- Merkle 树的叶子节点上的 value 可以任意指定，比如可以将数据的哈希值作为叶子节点的值；
- 非叶子节点的 value 是根据它下面所有的叶子节点值，然后按照一定的算法计算得出的。如 Merkle 树的非叶子节点 value 是将该节点的所有子节点进行组合，然后对组合结果进行哈希计算所得出的哈希值。

（2）Merkle 树的应用领域

目前，在计算机领域 Merkle 树多用来进行比对以及验证处理。比特币钱包服务用 Merkle 树的机制来做“百分百准备金证明”。在处理比对或验证的应用场景中，特别是在分布式环境下进行比对或验证时，Merkle 树可以大大减少数据的传输量以及计算的复杂度。

（3）Merkle 树的优点

Merkle 树明显的一个好处是可以单独拿出一个分支（作为一个小树）来对部分数据进行校验，这个特性在很多使用场合可以带来哈希列表所不能比拟的方便和高效。

（4）Merkle 树在区块链中的应用

在区块链中，区块中的交易是按照 Merkle 的形式存储在区块上面的。每笔交易都有一个哈希值，然后不同的哈希值向上继续做哈希运算，最终形成了唯一的 Merkle 根。这个 Merkle 根将会被存放到区块的区块头中。利用 Merkle 树的特性可以确保每一笔交易都不可伪造。

3. 非对称加密算法

加密算法一般分为对称加密和非对称加密，非对称加密是指为满足安全性需求和所有权验证需求而集成到区块链中的加密技术。非对称加密通常在加密和解密过程中使用两个非对称的密码，分别称为公钥和私钥。非对称密钥对具有两个特点：一是用其中一个密钥（公钥或私钥）加密信息后，只有另一个对应的密钥才能解开；二是公钥可向其他人公开，私钥则保密，其他人无法通过该公钥推算出相应的私钥。

非对称加密一般划分为三类主要方式：大整数分解问题类、离散对数问题类、椭圆曲线类。大整数分解问题类指用两个较大的质数的乘积作为加密数，由于质数的出现具有不规律性，想要破解只能通过不断试算。离散对数问题类指的是基于离散对数的难解性，利用强的单向散列函数的一种非对称分布式加密算法。椭圆曲线类指利用平面椭圆曲线来计算成组非对称特殊值，比特币就使用此类加密算法。

非对称加密技术在区块链的应用场景主要包括信息加密、数字签名和登录认证等。其中信息加密场景主要是由信息发送者（记为 A）使用接受者（记为 B）的公钥对信息加密后再发送给 B，B 利用自己的私钥对信息解密。比特币交易的加密即属于此场景。数字签名场景则是由发送者 A 采用自己的私钥加密信息后发送给 B，再由 B 使用 A 的公钥对信息解密，