本书从区块链的基础知识开始讲起，以HyperLedger Fabric为主线，清晰讲解区块链的原理、源码、搭建与应用，可帮助读者轻松上手区块链。

Broadview
www.broadview.com.cn

区块链轻松上手

原理、源码、搭建与应用

Leader-us 李艳军 赵锴 编著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

区块链轻松上手
原理、源码、搭建与应用

Leader-us 李艳军 赵锴 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书首先从以比特币为代表的数字货币的历史与现状开始，讲解区块链的概念、生态、底层技术与架构；然后讲解 Fabric 的开发环境与调试方法，并细致解析配置文件及命令行的用法；其次以 Fabric Java SDK 为主介绍如何使用 Java 代码开发 Fabric 应用，包括客户端管理、通道配置、事件监听、智能合约开发等；再次深入解析 Fabric 源码，解析客户端交易、智能合约初始化及背书流程；最后深入讲解 Fabric 的安全机制，以及 Fabric CA 的使用与管理等内容。

本书兼顾原理与实战，主要面向想快速上手区块链及了解其原理与架构的学生、爱好者、开发人员、架构师与技术管理人员。

图书在版编目（CIP）数据

区块链轻松上手：原理、源码、搭建与应用 / Leader-us 等编著. —北京：电子工业出版社，2018.10
ISBN 978-7-121-34878-5

Ⅰ. ①区… Ⅱ. ①L… Ⅲ. ①程序设计 Ⅳ. ①TP311.1

中国版本图书馆 CIP 数据核字（2018）第 184611 号

策划编辑：张国霞
责任编辑：孙学瑛
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：15.75　字数：350 千字
版　　次：2018 年 10 月第 1 版
印　　次：2018 年 10 月第 1 次印刷
印　　数：3000 册　　定价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：010-51260888-819，faq@phei.com.cn。

前　言

在说什么是区块链之前，先说一个小故事。

看过《三国演义》的人都知道，刘备自称刘皇叔，是中山靖王之后，以匡扶汉室之名，拉拢一批人建立了蜀国，形成三国鼎立之势。但回过头来看，大家为什么相信他真的是“刘皇叔”呢？其实在《三国演义》里有这么一段描述：

帝宣上殿，问曰：“卿祖何人？”玄德奏曰：“臣乃中山靖王之后，孝景皇帝阁下玄孙，刘雄之孙，刘弘之子也。”帝教取宗族世谱检看，令宗正卿宣读曰：“孝景皇帝生十四子。第七子乃中山靖王刘胜。胜生陆城亭侯刘贞。贞生沛侯刘昂。昂生漳侯刘禄。禄生沂水侯刘恋。恋生钦阳侯刘英。英生安国侯刘建。建生广陵侯刘哀。哀生胶水侯刘宪。宪生祖邑侯刘舒。舒生祁阳侯刘谊。谊生原泽侯刘必。必生颍川侯刘达。达生丰灵侯刘不疑。不疑生济川侯刘惠。惠生东郡范令刘雄。雄生刘弘。弘不仕。刘备乃刘弘之子也。”帝排世谱，则玄德乃帝之叔也。帝大喜，请入偏殿叙叔侄之礼……

原来就是翻出族谱，追溯整整十八代，才相信刘备为汉室之后。事实上，社会因为“信任”问题需要付出极大的代价，而解决该问题的方法之一就是从可以追溯且不能修改的记录中找到信任的依据。这种信任的实现方式就是讨论区块链的基础。

区块链到底是什么？比特币为什么这么值钱？那些看不见也摸不着的数字货币到底是不是传销？毫无疑问，作为区块链技术的应用之一——比特币已经大获成功，区块链所涉及的账本、分布式与去中心化、共识算法、智能合约、数字密钥、隐私保护、可信计算等技术也变得非常热门，基于这些技术的大量项目涌现。而区块链的发展价值就在于试图通过技术手段降低社会信任成本，并提高社会生产效率。

当然，区块链现在还有不足之处：除了比特币，还没有特别成功的典型应用。究其原因，一方面是区块链在高并发、低延迟的交易场景下还有许多技术问题需要解决；另一方

面是只能保证线上数据可信的特性限制了其应用场景。在大规模应用区块链时，社会的接受成本也是我们必须考虑的要素。在商业利益的驱动下，即使区块链能够提供各种各样的好处，选择应用区块链也只是一种纳什均衡而非最优策略。无论如何，区块链并不是“包治百病的灵丹妙药”，它还只是一个崭新的领域，正在蓬勃发展。

本书总计 6 章：第 1 章从以比特币为代表的数字货币的历史与现状开始，讲解区块链的概念，并通过一个简单示例让读者与 Fabric 有一次“亲密接触”；第 2 章阐述区块链的生态、底层技术与架构；第 3 章讲解 Fabric 的开发环境与调试方法，介绍更复杂的 Fabric 网络，并细致解析配置文件及命令行的用法；第 4 章以 Fabric Java SDK 为主介绍如何使用 Java 开发 Fabric 应用，包括客户端管理、通道配置、事件监听、智能合约开发等；第 5 章从创世区块开始，逐步深入解析 Fabric 源码，解析客户端交易、智能合约初始化及背书流程；第 6 章深入讲解 Fabric 的安全机制，以及 Fabric CA 的使用与管理。本书提供了部分示例代码(参见 GitHub 网站的 MyCATApache/SuperLedger 项目),希望对读者有所帮助，也希望读者能及时反馈并与我们沟通，指出书中的错漏之处，帮助我们完善内容。

最后，感谢家人的理解与支持，感谢张国霞编辑的耐心指导，感谢 Mycat 社区的帮助与鼓励！

目 录

第 1 章
全面理解区块链

1.1 从比特币开始

1.1.1 颠覆性的比特币

比特币（BTC）于 2008 年被中本聪首次提出，其价格在三年后首次突破 1 美元，此后一路飞涨并引发全球投资者的关注。2017 年 2 月 8 日，一枚比特币的价格超过 1 盎司（约 28.35 克）黄金的价格；2017 年 8 月，比特币之父中本聪“高位套现”3000 枚比特币；2017 年 11 月至 12 月初，一枚比特币的价格达到迄今为止的最高点，接近两万美元。

比特币并不是真实的货币，而是一种数字化的货币（简称数字货币）。与黄金一样，比特币的发行方式、发行总量及发行速度并不是由某个国家的央行以不透明方式控制的。可一句话概括：比特币是一种发行透明的、去中心化的、自动控制的数字货币。

首先，比特币的发行规则是完全透明的。比特币不像任一国家的纸币，每年印多少钞票完全由这个国家的央行人为决定。比特币的设计者为了避免比特币的发行数量过多，导致类似纸币“通货膨胀”现象的发生，在设计之初就确定了比特币总量有限的规则：比特币的总量为 2100 万个，在 2009 年生成第一批 50 枚比特币，此时的货币总量就是 50，之后新币以约每 10 分钟 50 个的速度发行；当未发行的比特币数量减少到总量的 50%

即 1050 万时，新币的发行速度就开始减半，约每 10 分钟产生 25 个新币，依此类推。当未发行的比特币数量减少到总量的 25%即 525 万时，新币的发行速度继续减半，并基本上保持新币发行量每 4 年减半的节奏，预计在 2140 年以后不再产生新币。因此，比特币基本能保持零通胀的趋势，不像大部分纸币，随着时间的流逝，其购买力和价值不断缩水。

其次，比特币是一种去中心化的货币。比特币平台基本上是“零门槛”入门的，门槛低到什么程度？只要有一台可以连接互联网的计算机，再加入比特币的 P2P 分布式网络中，就能参与比特币的发行和交易等核心业务了。在比特币平台上，任何个人或者机构都可以自由参与，不需要任何机构的审批，在比特币网络中也不存在任何中心控制节点，每个加入比特币网络中的运算节点都是平等的，它们之间的差别仅仅是算力的多少，每个节点都“努力工作”，用算力来证明自己，这或多或少地影响着比特币的发行、交易、记账等核心业务。

最后，比特币是一种自动控制的数字货币。比特币是一套自动化的软件代码，新币的发行、身份的验证、交易的确认、账本的记录等流程都是由比特币网络中的计算机节点（矿工，或称 Miner）自动执行的，全程没有任何人工参与，需要终端用户（User）参与的只有比特币的买卖操作。每个用户都拥有一个比特币账号，这个账号由一对密钥及比特币的钱包地址（Bitcoin Addr）组成，比特币的买卖操作就是一个用户把比特币转到另一个用户的钱包地址中，如果一个用户把自己所有的比特币都转卖出去，就可以认为是清仓套现。

1. 深入理解“挖矿”及其原理、机制

中本聪在设计比特币之初就限定了比特币的总量，可以想象这些比特币就好像黄金一样被埋在地下，等待着无数玩家（又称矿工）去挖掘（又称挖矿）。一枚比特币的诞生源自比特币矿工的辛劳挖矿，当然，这里的“挖矿”并非指真实的挖矿山的行为，而是矿工通过专有的机器（又称矿机）计算和挖掘出一个很难得到的随机数，谁先计算出来，谁就得到相应的比特币。如果看过斯皮尔伯格的《头号玩家》这部电影，你就能很快弄明白挖矿是怎么回事了。而无数矿机夜以继日地挖矿，挖掘出一枚枚新币的过程，就是比特币的发行过程。

如果想成为比特币网络中的一名矿工，就得先购买一套不错的装备——矿机。一开始，人们都用自己的计算机去做矿机，因为僧少粥多，所以最早的矿工们还能轻松挖到比特币，但随着比特币市值的一路飙升，大批淘金者蜂拥而入，同时，新币的数量在不断减少，基本上每 4 年就减少一半，这时人们基本上都得拼装备了，谁的装备越强，谁的挖矿速度就越快，矿工们不得不购买算力更强的装备。后来，很多矿工自发形成各种挖矿组织——矿

池，最后，比特币的“矿山”成为一个完全数字化的战场，遍布全球的散户与各种“矿池巨兽”一起角逐，其场面像极了《头号玩家》里的“绿洲”。更有趣的是，《头号玩家》里的 101 组织是一个大玩家，不仅靠售卖游戏装备获利，还派人参与争夺游戏中的彩蛋；在比特币世界中也有这样的大玩家，也就是制造、出售矿机和拥有自己的矿池的玩家，其中的头号玩家是我国的比特币大陆（Bitmain）公司，比特币大陆公司 2017 年赚的钱在同期甚至超过知名的英伟达公司！有分析师认为：比特币大陆公司在 2017 年的运营利润为 30 亿～40 亿美元，而英伟达同期的运营利润为 30 亿美元，比特币大陆公司在短短 4 年内取得的成绩，英伟达却用了 24 年，这就是新经济的速度吧。

现在，我们不太可能靠挖矿致富了，但可以尽力理解挖矿背后的原理。在前面已经了解到，挖矿就是各个矿机去计算和挖掘一个很难得到的随机数，实际上，这是一个纯粹的、拼蛮力、拼算力的竞赛。挖矿算法也被称为工作量证明（Proof of Work，PoW）算法，即矿机不断地重复一些简单的 SHA256 哈希运算，直到找到符合条件的目标哈希值。举个例子，给出以下游戏规则：

> 给定一个基本的字符串"Hello, world!"，可以在这个字符串后面添加一个叫作 Nonce 的整数值，然后对新的字符串执行 SHA256 哈希运算，如果得到的哈希结果（以 16 进制的形式表示）是以“0000”开头的，就找到了符合要求的一个哈希值，谁先找到这个哈希值并上报对应的 Nonce 值，谁就是赢家，谁就能赢取奖品。

按照游戏规则，假设 Nonce 值是从零开始的，则我们不停地递增 Nonce 值，然后对新拼接的字符串执行 SHA256 哈希计算，所以需要经过 4251 次计算才能找到前 4 位恰好为 0 的哈希散列，部分计算的输出结果如下：

```
   "Hello, world!0" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
   "Hello, world!1" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
   ...
   "Hello, world!4250" =>
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

上述例子中的 Nonce 就是我们挖矿所要找的那个随机数！我们通过 SHA256 算法得到的是一个长度为 256 位（bit）的数值，可以把计算这个哈希值的过程类比为一次次“抛硬币”的过程。好比有 256 枚硬币，对每个硬币给定依次为 1、2、3 直到 256 的编号，每进行一次哈希运算，就像抛一次硬币，256 枚硬币要同时抛出，要求编号 1 到 N（$0<N<256$）的所有硬币在落地后全部正面向上！试想一下，如果 N 是 128，则要活到几千岁才有可能

抛出一个符合条件的结果，别无他法。所以，矿机只能进行一次次的重复运算，同时比拼速度，谁能更早地计算出这个 Nonce，谁就是赢家，这就是所谓的工作量证明（PoW）。PoW 的流程如图 1-1 所示。

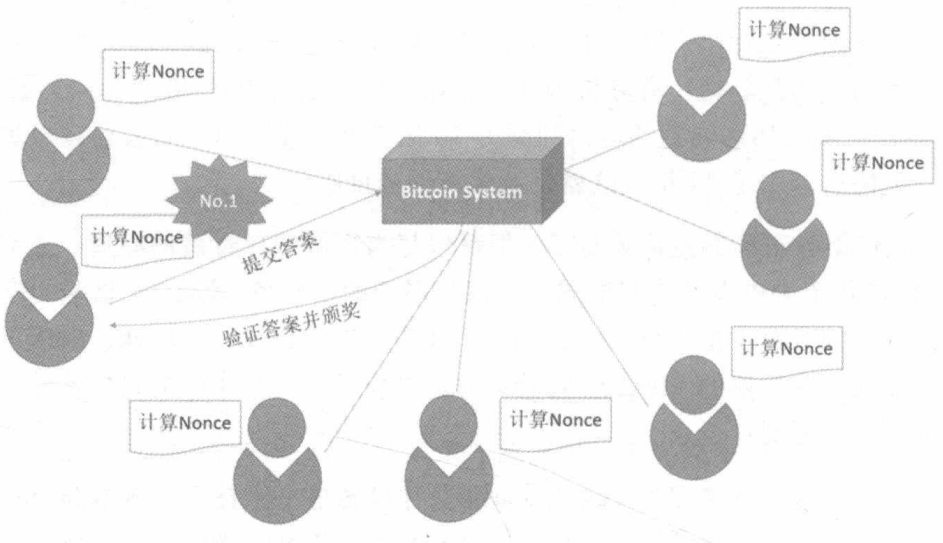

图1-1

在 SHA256 计算中，N 每增大一次，计算目标 Nonce 的工作量就增加很多，矿机不得不花费更多的时间去完成计算，这就减慢了比特币的“造币”速度，因此在挖矿算法中，N 对应的就是 Difficulty（难度值）这个关键参数。Difficulty 会根据全网算力的变化进行自适应调整，以保持造币的速度。中本聪规定每生成 2016 页账本（Block），挖矿的难度就自动增加一级，这就是前面所说的，比特币的新币发行量基本上保持每 4 年减半的节奏的真正原因。虽然寻找这个随机数需要大量的重复运算，但由于这个工作是矿工交给自己的矿机全天 24 小时自动执行的，因此只要装备好，矿工还是有机会“勤劳致富”的。其结果就是全球各地的无数矿工们乐此不疲地“挖矿”，然后在比特币交易市场中出售、变现，再购买更高级的矿机继续挖矿。

由于比特币的总量有限，所以比特币终有一天会被挖完，若要长久地鼓励矿工们为比特币网络“打工”，就需要挖矿以外的激励制度，这就是交易手续费（Transaction Fees），类似于银行转账业务中的手续费。在通常情况下，比特币的转账交易的确是免费的，但在某些情况下必须支付手续费才能完成转账，这是为了激发矿工们的热情，因为矿工打包、转账、交易需要耗费资源（带宽、存储、验证），对矿工们的这些付出进行付费是合理的，同时，针对小额比特币交易则强制收费，这样可以防止黑客用大量的小额比特币交易来冲

击整个 P2P 网络，但收取的费用通常很少，比如 0.000 1 枚比特币。这就带来了另一个值得我们思考的问题，即比特币的总数虽然有限，只有 2600 万枚，但一枚比特币并不是一枚“硬币”，它是可以继续分割的，一枚比特币可以被分割到小数点后 8 位的程度，所以比特币的最小单位是 0.000 000 01BTC，因此，有些人认为比特币仍然是一种可以膨胀的数字货币。

2. 比特币的交易机制

在挖到比特币以后，最重要的就是兑现真实的货币了，毕竟矿工挖矿也是有成本的，特别是电力消耗及矿机长期高负荷运行所带来的损耗。此外，在比特币世界中充斥着大量的比特币投资者，对于这些投资者来说，最重要的就是能够像炒股票一样方便地买入和卖出比特币，以获取差价了。这就涉及比特币交易的问题。我们知道，每个比特币用户都有一个比特币钱包（Bitcoin Wallet），这个钱包有一个接收比特币转账的地址——Bitcoin Address（又称比特币地址），类似于支付宝账号或者银行卡账号，对比特币的交易（Bitcoin Transaction）就是将比特币从一个比特币地址提出，转到另一个比特币地址，在这个过程中不必将比特币转换成人民币等货币，但比特币的受让方必须支付等值资金给比特币的出让方，这就是比特币的场外交易，即一方通过支付宝、微信或银行转账将资金打给另一方。由于这种私下的场外交易存在很高的风险，因此需要一个第三方的交易市场来完成比特币的交易活动。在很长一段时间内，我国拥有全世界最大的交易市场，掌控着世界八成以上的交易量，但从 2017 年下半年起，比特币中国、火币网、OKCoin 币行等几个国内知名的交易市场陆续关停，在我国境内不再存在合法的比特币交易市场。2018 年，国外比较知名的数字货币交易市场有币安、Bittrex、Poloniex 等。

如果认真阅读了上面这段关于比特币交易的说明，你就可能发现一个“疑点”，即在比特币钱包里有一个用来收取比特币的“比特币地址”，却没有账户余额的信息，这完全违背了我们对支付系统的理解！在我们的理解中，所有支付系统都是以账户余额为核心进行设计的，银行也好，证券交易系统也好，互联网第三方支付系统也好，都基于账户余额的设计思想，在数据库里每个账号都有一个余额属性，保存当前账户的资产金额。举例来说，鸣人的钱包里有 100 元，路飞的宝箱里有 50 元，当鸣人要购买路飞捕捞的一只澳洲龙虾交给 Mycat 总部的厨神做定制拉面时，鸣人需要支付 30 元给路飞，其转账交易过程如下。

（1）平台检查鸣人的账户余额是否充足，如果不足 30 元就终止交易，转账失败。

（2）若鸣人的账户余额充足，则在鸣人的账户里减去 30 元（不考虑手续费）。

（3）在路飞的账户里增加 30 元。

（4）交易成功，保存交易流水记录。

但是，在这个看似简单、直观的流程背后，有很多的约束条件及实现代价。

（1）首先，我们需要一个高度可靠的关系型数据库，并且这个数据库严格遵循 ACID 规范。

（2）其次，我们需要编程来确保上述 1 到 3 的过程是在一个数据库事务中执行的，中间任何一步失败，则都需要回滚。

由于事务的约束和限制，我们需要一个中心化的账户系统来保存所有参与交易的账号信息，并且随着交易量的增加，系统中的交易流水记录也会迅速膨胀。试想一下，若全球有超过 100 亿个用户使用比特币，则这个中心化的账户系统的数据库会有多大？因此传统的、中心化的、基于关系数据库的账户余额的设计思路根本无法满足比特币的交易需求，于是中本聪丢弃了中心化的账户数据库的设计思路，独创了以 UTXO 为核心的交易系统，彻底规避了传统交易系统的局限性。UTXO（Unspent Transaction Output，交易输出）的设计受到了业界的高度评价，斯坦福大学密码学与计算机安全教授 Dan Boneh 对 UTXO 的设计给予了很高的评价。

要深入理解 UTXO，最简单的办法就是把一枚比特币从诞生到在市场上流通的整个环节再理解一遍。还是以鸣人买龙虾为例，假设回到故事的起点，鸣人得到蛤蟆仙人的指点，要打败最终的 Boss，需要组织史上最强打怪军团，这需要很多经费，而现在赚取经费的最好方式是挖矿；当然，鸣人天赋异禀，拥有火影多重影分身禁术，天生就是一名挖矿好手！按照当前的市值，鸣人只要挖 100 枚比特币就可以组建一只华丽的打怪军团。于是鸣人一路狂奔去挖矿，路上遇到赶赴好莱坞的黄飞鸿，鸣人看他轻功了得，于是说服他加入打怪军团，一路上又收了远方表弟路飞，三人很快抵达最大的比特币挖矿场地——比特币绿洲，有路飞与黄飞鸿保驾，鸣人施展火影多重影分身禁术，开启并行挖矿，不到 1 小时就挖出了 120 枚比特币，这 120 枚比特币的收入会在比特币的账本里被记录为一笔交易，每笔交易都有若干笔资金来源，即交易输入或者转账人，也都有若干笔资金去向，即交易输出或者收款人，这个交易输出对于收款人来说，就是未花费过的交易输出，即 UTXO。如下所示为鸣人挖矿获取 120 枚比特币的交易记录，这个记录被称为生产交易或者 CoinBase 交易，经常是每个区块的第 1 个交易。

CoinBase 交易

交易编号：#1001

交易输入（Transaction Input）	交易输出（Unspent Transaction Output）		
资金来源	条目编号	金额	收款人地址
挖矿所得	1	120	鸣人

由于打怪军团只需要 100 枚比特币的经费，所以，接下来鸣人分给路飞和黄飞鸿各 10 枚比特币，于是分别产生了两笔交易，这两笔交易的内容分别如下。

普通交易

交易编号：#2001

交易输入（Transaction Input）	交易输出（Unspent Transaction Output）		
资金来源	条目编号	金额	收款人地址
#1001-1	1	10	路飞
#1001-1	2	110	鸣人

普通交易

交易编号：#3001

交易输入（Transaction Input）	交易输出（Unspent Transaction Output）		
资金来源	条目编号	金额	收款人地址
#2001-2	1	10	黄飞鸿
#2001-2	2	100	鸣人

每笔交易都需要做到交易输入与交易输出平衡，因此，在编号为#2001 的鸣人给路飞转账的交易中虽然只有一次转账，但也产生了两条记录。实际上，我们可以将 UTXO 理解为转账流水记录+余额的复式结构，每笔交易的 UTXO 必然是下一笔交易的输入项，在一系列交易后，在鸣人的账号上（比特币地址）最终登记了 100 枚未花费的比特币，路飞与黄飞鸿则各有 10 枚，此外，以区块链方式记录的账本数据有不可篡改的特点，这样我们

就可以很方便、很准确地追踪每一笔资金的来龙去脉，如图 1-2 所示。

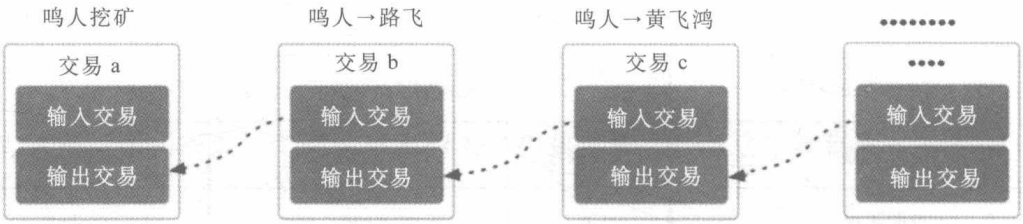

图1-2

UTXO 还具有隐私性，因为一个用户可以拥有很多个比特币地址来充当“收款人地址”，因此很难追查一个用户究竟有多少比特币。UTXO 中的收款地址其实是比特币用户的公钥哈希值，用对应的私钥才能“解锁”。因此，只有拥有这个收款地址的用户才能用自己的私钥来解锁对应地址的钱包，然后将在这个地址中记录的“输出交易”转到另一个用户的收款地址，在这个过程中涉及复杂的数字证书与加解密问题，后面会深入讲解。中本聪考虑到比特币系统在几十年甚至数百年以后可能会产生更多的目前无法预见的交易类型，而不是简单的转账交易，因此在交易模块中引入了脚本系统以增强系统的适用性，我们可以将这视为数字货币系统中最早的“智能合约”，其之后在以太坊（Ethereum）及超级账本中被进一步发扬光大。

3. 小结

在比特币平台中，当前的每时每刻都存在造币（挖矿）与交易（Transaction）两种行为，比特币平台中的交易与银行转账及支付宝转账在本质上没有什么不同，都是用户 A 转账给用户 B，但比特币平台有以下几个明显特征。

- 交易使用的货币是比特币。
- 交易数据采用了高强度的数字加密技术，杜绝伪造与欺诈问题。
- 比特币网络是一个 P2P 对等网络，交易过程完全去中心化，不存在第三方的中介机构。
- 交易的手续费由确认该交易合法的矿工获取，人人都有机会参与赚钱。
- 交易的账本数据分布在每个矿工（节点）的矿机上，加入系统的每个节点都可以拉取并在本地保存一份完整的交易记录数据。
- 比特币系统具有很高的容错性，即使大部分节点崩溃，整个比特币平台仍然可以正常运行。