在这篇文章中我们探一探区块链技术背后的历史，从上世纪80年代的拜占庭将军问题到今天的复杂的智慧契约，区块链是如何一步步走到今天的呢？

区块链基础

区块链是随着比特币等数字加密货币的日益普及而逐渐兴起的一种全新技术，它提供了一种去中心化的、无需信任积累的信用建立范式，目前已经引起金融行业、科研机构、政府部门和投资公司的高度重视与广泛关注。

区块链技术通过建立一个共同维护且不可被篡改的数据库来记录过去的所有交易记录和历史数据，所有的数据都是分布式存储且公开透明的。在这种技术下，任何互不相识的网络用户都可以通过合约、点对点记账、数字加密等方式达成信用共识，而不需要任何的中央信任机构。在这种技术下，我们可以建立数字货币、数字资产、智能财产以及智能合约等。

通过上一章的介绍，相信大家已经对区块链和比特币有了初步的认识，在本章中，我们将继续探讨区块链的技术细节。

本章将首先介绍区块链的相关基本概念及其运作原理，然后介绍区块链上可以进行的操作和相关细节，最后再讨论区块链上的交易流程和它的验证过程。

区块链技术

区块链本质上是一个对等网络（peer-to-peer）的分布式账本数据库。比特币的底层就采用了区块链的技术架构。

区块链本身其实是一串链接的数据区块，其链接指针是采用密码学哈希算法对区块头进行处理所产生的区块头哈希值。每一个数据块中记录了一组采用哈希算法组成的树状交易状态信息，这样保证了每个区块内的交易数据不可篡改，区块链里链接的区块也不可篡改。

1.基本概念

一个完整的区块链系统包含了很多技术，其中有存储数据的数据区块及其之上的数字签名、时间戳等技术，有作为支撑的P2P网络和维护系统的共识算法，有挖矿和工作量证明机制，有匿名交易机制和比特币钱包，还有链龄、UTXO、Merkle树、双花等相关技术概念。

正是这些技术，使得区块链在无中心的网络上形成了运转不息的引擎，为区块链的

交易、验证、链接等功能提供了源源不断的动力。

2.数据区块

比特币的交易记录会保存在数据区块之中，比特币系统中大约每10分钟会产生一个区块，每个数据区块一般包含区块头（Header）和区块体（Body）两部分

区块头封装了当前的版本号（Version）、前一区块地址（Prev-block）、时间戳（Timestamp）、随机数（Nonce）、当前区块的目标哈希值（Bits）、Merkle树的根值（Merkle-root）等信息。

区块体中则主要包含交易计数和交易详
情。
交易详情就是比特币系统中的记账本，每一笔交易都会被永久地记入数据区块中，而且任何人都可以查询。

区块体中的Merkle树将会对每一笔交易进行数字签名，如此可以确保每一笔交易都不可伪造且没有重复交易。所有的交易将通过Merkle树的Hash过程产生一个唯一Merkle根值记入区块头。关于Merkle树本章后面将详细介绍。

如果你使用的是比特币核心钱包（Bitcoin core），那么每当你打开客户端时，区块数据文件都会被同步到电脑硬盘中，可以在blocks文件夹下找到它们。

我们还可以使用hexdump指令在终端上将数据区块以十六进制的方式显示出来。我们可以通过解析这些数据得出交易记录、区块大小等基本信息，
因此我们说区块链中的数据是完全公开透明的。 我们使用指令hexdump -n 10000 -C
blk00000.dat打开了编号为00000的创世区块（比特币中的第一块区块链）。

3.挖矿与分叉问题

区块在挖矿过程中产生。所谓挖矿，实际上是穷举随机数算法，把上个区块的哈希值加上10分钟内的全部交易单打包，再加上一个随机数，算出一个256位的字符串哈希值，输入的随机数Nonce使哈希值满足一定条件就获得这个区块的交易记账权。

新产生的区块需要快速广播出去，以便其他节点进行对其验证，以防造假。每个区块存着上一个区块的哈希值，可以溯源到源头，只有经过验证后才最终获得区块的交易记账权。比特币系统会让挖矿的矿工竞争记账权（在主链上链接区块的权利）

，这个竞争机制就是工作量证明机制。

挖矿需要付出大量的能源和时间，谁付出的工作量多就能以更大的概率获得一个区块的记账权。获取记账权的矿工会将当前区块链接到前一区块，形成最新的区块主链，该矿工也会得到系统奖励的一定数量（2009～2013年每10钟产生50个比特币，2014年至今每10分钟产生的比特币将减半成25个）的比特币。所有的区块链接在一起形成了区块链的主链，从创世区块到当前区块，在区块链之上的所有数据历史都可以被追溯和查询。

需要说明的是，可能会出现不同地区的两个矿工同时“挖出”两个新区块加以链接的情况，这时主链上就会出现“分叉”。系统并不会马上确认哪个区块不合理，而是约定后续矿工总是选择累计工作量证明最大的区块链。因此，当主链分叉以后，后续区块的矿工将通过计算和比较，将其区块链接到当前累计工作量证明最大化的备选链上，形成更长的新主链，并自动抛弃分叉处的短链，从而解决分叉问题。

4.时间戳和不可篡改性

时间戳是指从格林威治时间1970年01月01日00时00分00秒（北京时间1970年01月01日08时00分00秒）起至现在的总秒数，通常是一个字符序列，唯一地标识某一刻的时间。在比特币系统中，获得记账权的节点在链接区块时需要在区块头中加盖时间戳，用于记录当前区块数据的写入时间。

每一个随后区块中的时间戳都会对前一个时间戳进行增强，形成一个时间递增的链条。时间戳技术本身并没有多复杂，但在区块链技术中应用时间戳却是一个重大创新，时间戳为未来基于区块链的互联网和大数据增加了一个时间维度，使得数据更容易追溯，重现历史也成为可能。

同时，时间戳可以作为存在性证明（Proof of Existence）的重要参数，它能够证实特定数据必然在某特定时刻是的确存在的，
这保证了区块链数据库是不可篡改和不可伪造的，这也为区块链技术应用于公证、知识产权注册等时间敏感领域提供了可能。

5.分布式数据库

比特币系统中的区块就像一个记账本一样，记录了所有比特币的交易信息，每一个比特币用户的比特币收支情况都被永久地嵌入了数据区块中以供别人查询。这些数据区块中的交易数据存放在每一个比特币用户的客户端节点中，所有的这些节点则组成了比特币及其坚韧的分布式数据库系统。
任何一个节点的数据被破坏都不会影响整个数据库的正常运转，因为其他的健康节

点中都保存了完整的数据库。

6.UTXO交易模式

UTXO（Unspent Transaction Outputs）是未花费的交易输出，它是比特币交易过程中的基本单位。除创世区块以外，所有区块中的交易（Tx）会存在若干个输入（Tx_in，也称资金来源）和若干个输出（Tx_out，也称资金去向），创世区块和后来挖矿产生的区块中给矿工奖励的交易没有输入，除此之外，在比特币系统中，某笔交易的输入必须是另一笔交易未被使用的输出，同时这笔输入也需要上一笔输出地址所对应的私钥进行签名。

当前整个区块链网络中的UTXO会被储存在每个节点中，只有满足了来源于UTXO和数字签名条件的交易才是合法的。
所以区块链系统中的新交易并不需要追溯整个交易历史，就可以确认当前交易是否合法。

7.哈希函数

哈希函数在比特币系统中也有着重要的应用，区块链中的数据并不只是原始数据或者交易记录，还包括它们的哈希函数值，即将原始数据编码为特定长度的、由数字和字母组成的字符串后，记入区块链。哈希函数有着很多适合存储区块链数据的

优点：

1）哈希函数处理过的数据是单向性的，通过处理过的输出值几乎不可能计算出原始的输入值；

2）哈希函数处理不同长度的数据所耗费的时间是一致的，输出值也是定长的；

3）哈
希函数的输入
值即使只相差一个字节，输
出值的结果也会迥然不同。
比特币系统中最常采用的哈希函数是双SHA256哈希函数，通俗来说就是将不同长度的原始数据用两次SHA256哈希函数进行处理，再输出长度为256的二进制数字来进行统一的识别和存储。

总之，哈希函数是比特币系统中的关键技术，为比特币系统提供了很多便利。本书后面的章节将会对哈希函数做详细介绍，此处不赘述。

8.Merkle树

Merkle树是数据结构中的一种树，可以是二叉树，也可以是多叉树，它具有树结构的所有特点。如图2-4所示，比特币区块链系统中的采用的是Merkle二叉树，它的作用主要是快速归纳和校验区块数据的完整性，它会将区块链中的数据分组进行哈希运算，向上不断递归运算产生新的哈希节点，最终只剩下一个Merkle根存入区块头中，每个哈希节点总是包含两个相邻的数据块或其哈希值。

在比特币系统中使用Merkle树有诸多优点：
首先是极大地提高了区块链的运行效率和可扩展性，使得区块头只需包含根哈希值而不必封装所有底层数据，
这使得哈希运算可
以高效地运行在智能手机甚至物联网
设备上；
其次是Merkle树可支持
“简化支付验证协议”（SPV），
即
在不
运行完整
区块链网络节点的
情况下，也能够对交易数据进行检验
。所以，
在区块链中使用Merkle树这种数据结构是非常具有意义的。本书后面的章节将会对Merkle树做详细介绍。

9.双重支付

双重支付问题又称为“双花”问题，即利用货币的数字特性用“同一笔钱”完成两次或者多次支付。在传统的金融和货币体系中，由于金钱货币是物理实体，具有客观唯一存在的属性，所以可以避免双重支付的情况。但在其他的电子货币系统中，则需要可信的第三方管理机构提供保证。

区块链技术则在去中心化的系统中不借助任何第三方机构而只通过分布式节点之间的相互验证和共识机制，有效地解决了双重支付问题，在信息传输的同时完成了价值转移。
区块链技术通过区块链接形成的时间戳技术加上验证比特币是否满足UTXO（未花费交易）和数字签名，有效避
免了双重支付的问题。
如果有人用同一笔UTXO构造了两笔付给不同交易方的交易，则比特币客户端只会

转发最先被侦听到的那个。矿工会选择将那笔交易包入未来区块，当其中一笔交易所在的区块后有5个链接的区块，这笔交易已经得到了6次确认。在比特币区块链上，6次确认后可以基本上保证比特币不被双花。

10.P2P网络

P2P网络（peer-to-peer network，对等网络）是一种在对等者（peer）之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。
因此，从字面上，P2P可以理解为对等计算或对等网络，P2P网络示意图如图2-5所示。国内的迅雷软件采用的就是P2P技术。

区块链系统是建立在IP通信协议和分布式网络的基础上的，它不依靠传统的电路交换，而是建立于网络通信之上，完全通过互联网去交换信息。网络中所有的节点具有同等的地位，不存在任何特殊化的中心节点和层级结构，每个节点均会承担网络路由、验证数据区块等功能。网络的节点根据存储数据量的不同可以分为全节点和轻量级节点，全节点存储了从创世区块以来的所有区块链数据（比特币网络现在大约有几十GB，且还在不断增长中）。

全节点的优点是进行数据校验时不需要依靠别的节点，仅依靠自身就可以完成校验更新等操作，缺点是硬件成本较高。
轻量级节点只需要存储部分数据信息，当需要别的数据时可以通过简易支付验证方式（Simplif?ied Payment
Verif?ication，SPV）向邻近节点请求所需数据来完成验证更新。

11.加密算法

除了哈希算法以外，比特币中还存在一种为交易加密的非对称加密算法（椭圆曲线加密算法）。非对称加密算法指的就是存在一对数学相关的密钥，使用其中一个密钥进行加密的数据信息，只有使用另一个密钥才能对该信息进行解密。这对密钥中，对外公开的密钥叫作公钥，不公开的密钥就叫作私钥。打个比方来说，公钥就像银行的账户，私钥就像是该账户的密码或者账户所有者的签名。

区块链之上的有效交易有一个用于交易发起方私钥签名有效的数字签名，而该交易的签名可以通过使用交易发起方
的公钥进行验证。
公钥可以通过算法从私钥中计算得出，但私钥却不能从公钥中推出。比特币系统中使用的就是一种非常典型的非对称加密算法——椭圆曲线加密算法（ECC）。

比特币系统一般从操作系统底层的一个密码学安全的随机源中取出一个256位随机数作为私钥，私钥总数为2256个，所以很难通过遍历所有可能的私钥得出与公钥的对应的私钥。用户使用的私钥还会通过SHA256和Base58转换成易书写和识别的50位长度的私钥，公钥则首先由私钥和Secp256k1椭圆曲线算法生成65字节长度的随机数。

一般情况下，比特币钱包的地址也由公钥所生成，其生成过程为首先将公钥进行SHA256和RIPEMD160双哈希运算，并生成20字节长度的摘要结果（即Hash160结果），这个将作为比特币地址的主体（body）信息，再在前面加上版本前缀0x00，在后面添加4个字节的地址校验码。
地址校验码通过对摘要结果进行两次SHA256运算，取哈希值的前4位产生。最后通过Base58处理把连在一起的版本前缀、主体信息和校验码转换成可以容易让人识别的比特币字符地址。

12.数字签名

数字签名就是在信息后面加上另一段内容，作为发送者的证明并且证明信息没有被篡改。一般是发送者将信息用哈希算法处理得出一个哈希值，然后用私钥对该哈希值进行加密，得出一个签名。然后发送者再将信息和签名一起发送给接收者。接收者使用发送者的公钥对签名进行解密，还原出哈希值，再通过哈希算法来验证信息的哈希值和解密签名还原出来的哈希值是否一致，从而可以鉴定信息是否来自发送者或验证信息是否被篡改。

13.比特币的隐私模型

传统隐私模型为交易的参与者提供了一定程度的隐私保护，第三方不会交出交易者的个人身份信息，公众所得知的只是某个人将一定数量的货币发给了另外一个人，但是难以将该交易与某个特定身份的人联系起来，公众无法知道这人到底是谁。这同股票交易所发布的信息是类似的，每一手股票买卖发生的时间、交易量是记录在案且可供查询的，但是交易双方的身份信息却不予透露。但实际上，交易双方的个人信息是存放在第三方机构，所以一定程度上交易参与者的隐私信息还是会有泄露的风险。

在比特币的隐私模型中，所有的交易不需要第三方的操控，也不需要提供任何身份信息，只需要提供比特币的地址就可以跟任何人完成一次准匿名的交易。在一定程度上，交易不可追溯到交易者本身，因此比特币上的交易可以在一定程度上摆脱监管。但通过对区块链上交易的地址以及交易额做关联分析，也可以获得有关交易者的蛛丝马迹。因此，比特币的交易还不是纯粹的匿名交易机制，而是准匿名（pseudo-anonymous）交易机制。

框架与特点

1.框架简介

目前大多数区块链技术的应用与比特币类似，大部分是在比特币架构基础上的扩展。目前，区块链技术在金融行业得到广泛关注，被认为可以用来从最底层重构传统金融业现有的IT基础架构。我们将区块链的基础架构分为三层来进行讲解。

首先，在网络层之上，区块链是建立在IP通信协议和对等网络的基础上的一个分布式系统，和传统带中心的分布式系统不一样，它不依靠中心化的服务器节点来转发消息，而是每一个节点都参与消息的转
发。
因此P2P网络比传统网络具有更高的安全性，任何一个节点被攻击都不会影响整个网络，所有的节点都保存着整个系统的状态信息。

其次，在数据层面上，区块链就是一个只可追加、不可更改的分布式数据库系统，是一个分布式账本。
如果是公开的区块链，也就是公有链，那么这个账本可以被任何人在任何地方进行查询，完全公开透明。在区块链网络中，节点通过使用共识算法来维持网络中账本数据库的一致性。

同时采用密码学的签名和哈希算法来确保这个数据库不可篡改，不能作伪，并且可追溯。
例如，在比特币系统中，只有在控制了51%的网络算力时才有可能对区块链进行重组以修改账本信息。由于比特币系统的设计者中本聪在系统设计中巧妙地加入了带有经济激励的挖矿工作量证明（PoW）机制，使得即使拥有网络51%以上算力的人也不会损害其自身利益而发起对网络的攻击。因此，比特币系统自上线7年多来一直持续不断地正常运行，没有出现过因为比特币系统本身缺陷而造成的安全故障。

再次，在应用
层面，我们可以用区块链代
替传统的登记、清算系统。
2016年6月22日，波士顿咨询公司指出，到2030年，全球支付业务收入预计将会达到8070亿美元。基于区块链技术的汇兑和支付属于区块链的1.0应用版，其安全性、交易时间、成本都会对传统支付业务进行颠覆式改进。花旗银行也明确指出，到2020年，如果各大金融机构都使用区块链技术，每年能够节省超过200亿美元的成本。

国信证券分析报告指出，通过区块链的点对点分布式的时间戳服务器来生成依照时

间前后排列并加以记录的电子交易证明，可以解决双重支付问题，从而带来结算成本趋零的可能性。
根据德国银行的一份引用波士顿咨询的研究报告，欧洲银行的IT成本支出平均占据银行整体运行成本的16%[5]。一个重要原因就是传统银行在账本的维护、支付交易的结算和清算方面的架构过于复杂，维护成本过高。

在应用方面，区
块链平台能够提供编程环境让用
户编写智能合约。
通过智能合约，可以把业务规则转化成在区块链平台自动执行的合约，该合约的执行不依赖可信任的第三方，也不受人为的干预。

理论上只要一旦部
署，一旦符合合约执行的条件就会自
动执行。
执行结果也可以在区块链上供公开检查，提供了合约的公正性和透明性。因此，智能合约可以降低合约建立、执行和仲裁中所涉及的中间机构成本。区块链的智能合约奠定了未来建立可编程货币、可编程金融，甚至是可编程社会的基础。

2.架构特点

区块链具有去中心化、可靠数据库、开源可编程、集体维护、安全可信、交易准匿名性等特点。如果一个系统不具有以上特征，将不能被视为基于区块链技术的应用。

（1）去中心化

区块链数据的存储、传输、验证等过程均基于分布式的系统结构，整个网络中不依赖一个没有中心化的硬件或管理机构。作为区块链一种部署模式，公共链网络中所有参与的节点都可以具有同等的权利和义务。

（2）可靠数据库

区块链系统的数据库采用分布式存储，任一参与节点都可以拥有一份完整的数据库拷贝。除非能控制系统中超过一半以上的算力，否则在节点上对数据库的修改都将是无效的。

参与系统的节点越多，数据库的安全性就越高。并且区块链数据的存储还带有时间戳，从而为数据添加了时间维度，具有极高的可追溯性。

（3）开源可编程

区块链系统通常是开源的，代码高度透明公共链的数据和程序对所有人公开，任何人都可以通过接口查询系统中的数据。并且区块链平台还提供灵活的脚本代码系统，支持用户创建高级的智能合约、货币和去中心化应用。

例如，以太坊（Ethereum）平台即提供了图灵完备的脚本语言，供用户来构建任何可以精确定义的智能合约或交易类型。关于以太坊的更多内容请参考2.2节。

（4）集体维护

系统中的数据块由整个系统中所有具有记账功能的节点来共同维护，任一节点的损坏或失去都不会影响整个系统的运作。

（5）安全可信

区块链技术采用非对称密码学原理对交易进行签名，使得交易不能被伪造；同时利用哈希算法保证交易数据不能被轻易篡改，最后借助分布式系统各节点的工作量证明等共识算法形成强大的算力来抵御破坏者的攻击，保证区块链中的区块以及区块内的交易数据不可篡改和不可伪造，因此具有极高的安全性。

（6）准匿名性

区块链系统采用与用户公钥挂钩的地址来做用户标识，不需要传统的基于PKI（Public Key Infrastructure）的第三方认证中心（Certif?icate Authority，CA）颁发数字证书来确认身份。通过在全网节点运行共识算法，建立网络中诚实节点对全网状态的共识，间接地建立了节点间的信任。

用户只需要公开地址，不需要公开真实身份，而且同一个用户可以不断变换地址。因此，在区块链上的交易不和用户真实身份挂钩，只是和用户的地址挂钩，具有交易的准匿名性。。

区块链技术的核心优势是去中心化，能够通过运用哈希算法、数字签名、时间戳、分布式共识和经济激励等手段，在节点无需互相信任的分布式系统中建立信用，实现点对点交易和协作，从而为中心化机构普遍存在的高成本、低效率和数据存储不安全等问题提供了解决方案。

近年来，伴随着国内外研究机构对区块链技术的研究与应用，区块链的应用前景受到各行各业的高度重视，被认为是继大型机、个人电脑、互联网、移动/社交网络之

后计算范式的第5次颠覆式创新，是人类信用进化史上继血亲信用、贵金属信用、央行纸币信用之后的第4个里程碑。它被视为下一代云计算的雏形，有望彻底重塑人类社会活动形态，并实现从现在的信息互联网到价值互联网的转变。

区块链运作的核心技术

1.区块链的链接

顾名思义，区块链即由一个个区块组成的链。每个区块分为区块头和区块体（含交易数据）两个部分。区块头包括用来实现区块链接的前一区块的哈希（PrevHash）值（又称散列值）和用于计算挖矿难度的随机数（nonce）。前一区块的哈希值实际是上一个区块头部的哈希值，而计算随机数规则决定了哪个矿工可以获得记录区块的权力。

2.共识机制

区块链是伴随比特币诞生的，是比特币的基础技术架构。可以将区块链理解为一个基于互联网的去中心化记账系统。类似比特币这样的去中心化数字货币系统，要求在没有中心节点的情况下保证各个诚实节点记账的一致性，就需要区块链来完成。所以区块链技术的核心是在没有中心控制的情况下，在互相没有信任基础的个体之间就交易的合法性等达成共识的共识机制。

区块链的共识机制目前主要有4类：PoW、PoS、DPoS、分布式一致性算法。

（1）PoW

PoW（工作量证明），也就是像比特币的挖矿机制，矿工通过把网络尚未记录的现有交易打包到一个区块，然后不断遍历尝试来寻找一个随机数，使得新区块加上随机数的哈希值满足一定的难度条件，例如前面10位是零。找到满足条件的随机数，就相当于确定了区块链最新的一个区块，也相当于获得了区块链的本轮记账权。

矿工把满足挖矿难度条件的区块在网络中广播出去，全网其他节点在验证该区块满足挖矿难度条件，同时区块里的交易数据符合协议规范后，将各自把该区块链接到自己版本的区块链上，从而在全网形成对当前网络状态的共识。

优点：完全去中心化，节点自由进出，避免了建立和维护中心化信用机构的成本。只要网络破坏者的算力不超过网络总算力的50%，网络的交易状态就能达成一致。

缺点：目前比特币挖矿造成大量的资源浪费；另外挖矿的激励机制也造成矿池算力

的高度集中，背离了当初去中心化设计的初衷。更大的问题是PoW机制的共识达成的周期较长，每秒只能最多做7笔交易，不适合商业应用。

（2）PoS

PoS权益证明，要求节点提供拥有一定数量的代币证明来获取竞争区块链记账权的一种分布式共识机制。如果单纯依靠代币余额来决定记账者必然使得富有者胜出，导致记账权的中心化，降低共识的公正性，因此不同的PoS机制在权益证明的基础上，采用不同方式来增加记账权的随机性来避免中心化。

例如点点币（PeerCoin）PoS机制中，拥有最多链龄长的比特币获得记账权的几率就越大。NXT和Blackcoin则采用一个公式来预测下一个记账的节点。拥有多的代币被选为记账节点的概率就会大。未来以太坊也会从目前的PoW机制转换到PoS机制，从目前看到的资料看，以太坊的PoS机制将采用节点下赌注来赌下一个区块，赌中者有额外以太币奖，赌不中者会被扣以太币的方式来达成下一区块的共识。

优点： 在一定程度上缩短了共识达成的时间，降低了PoW机制的资源浪费。

缺点：破坏者对网络攻击的成本低，网络的安全性有待验证。另外拥有代币数量大的节点获得记账权的几率更大，会使得网络的共识受少数富裕账户支配，从而失去公正性。

（3）DPoS

DPoS（股份授权证明）机制，类似于董事会投票。比特股（bitshares）采用的PoS机制是持股者投票选出一定数量的见证人，每个见证人按序有两秒的权限时间生成区块，若见证人在给定的时间片不能生成区块，区块生成权限交给下一个时间片对应的见证人。持股人可以随时通过投票更换这些见证人。DPoS的这种设计使得区块的生成更为快速，也更加节能。

优点：大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。

缺点：选举固定数量的见证人作为记账候选人有可能不适合于完全去中心化的场景。另外在网络节点数少的场景，选举的见证人的代表性也不强。

（4）分布式一致性算法

分布式一致性算法是基于传统的分布式一致性技术。其中有分为解决拜占庭将军问题的拜占庭容错算法，如PBFT。另外解决非拜占庭问题的分布式一致性算法（Pas

ox、Raft），详细见本书第5章的共识算法。该类算法目前是联盟链和私有链链场景中常用的共识机制。

优点：实现秒级的快速共识机制，保证一致性。

缺点：去中心化程度不如公有链上的共识机制；更适合多方参与的多中心商业模式。

3.解锁脚本

脚本是区块链上实现自
动验证、自动执行合约的重要技术。
每一笔交易的每一项输出严格意义上并不是指向一个地址，而是指向一个脚本。脚本类似一套规则，它约束着接收方怎样才能花掉这个输出上锁定的资产。

交易的合法性验证也依赖于脚本。
目前它依赖于两类脚本：锁定脚本与解锁脚本。锁定脚本是在输出交易上加上的条件，通过一段脚本语言来实现，位于交易的输出。解锁脚本与锁定脚本相对应，只有满足锁定脚本要求的条件，才能花掉这个脚本上对应的资产，位于交易的输入。通过脚本语言可以表达很多灵活的条件。解释脚本是通过类似我们编程领域里的“虚拟机”，它分布式运行在区块链网络里的每一个节点。

比特币的脚本目前常用的主要分为两种， 一种是普通的P2PKH（Pay-to-Public-Key-Hash），
即支付给公钥的哈希地址，接收方只需要使用地址对应的私钥对该输出进行签名，即可花掉该输出。
另一种是P2SH（Pay-to-Script-
Hash），
即支付脚本的哈希。以多重签名来举例，它要求该输出要有N把私钥中的M把私钥（M≤N）同时签名才能花掉该资产，它类似于现实生活中需要多把钥匙才能同时打开的保险柜，或是多人签名才能使条约生效一样，只是它是自动执行。

比如在比特币中，P2PKH的脚本规则如下：

Pubkey script: OP_DUP OP_HASH160 OP_EQUALVERIFY OP_CHECKSIG

Signature script:

P2SH的脚本规则如下：

Pubkey script: OP_HASH160

Signature script: [sig] [sig...]

在上述的两种脚本规则里，Pubkey script代表锁定脚本，Signature script代表解锁脚本。OP_开头的单词是相关的脚本命令，也是“虚拟机”所能解析的指令。这些命令规则根据Pubkey script的不同来进行划分，它也决定解锁脚本的规则。

比特币中的脚本机制相对简单，只是一个基于堆栈式的、解释相关OP指令的引擎，能够解析的脚本规则并不是太多，不能实现很复杂的逻辑。
但它为区块链可编程提供了一个原型，后续一些可编程区块链项目其实是基于脚本的原理发展起来的，
比如以太坊就是深入增强了脚本机制，脚本机制里不再单单是简单的OP指令，而是支持脚本的一套图灵完备语言，该脚本语言可以通过“虚拟机”去执行。以太坊实现了一个支持图灵完备脚本语言的区块链平台。

脚本的机制对于区块链来说非常重要，它类似于区块链技术提供的一个扩展接口，任何人都可以基于这个接口开发基于区块链技术的应用，比如智能合约的功能。脚本机制也让区块链技术作为一项底层协议成为可能。未来很多基于区块链的颠覆性应用，都有可能通过区块链的脚本语言来完成。

4.交易规则

区块链的交易就是构成区块的基本单位，也是区块链负责记录的实际有效内容。一个区块链交易可以是一次转账，也可以是智能合约的部署等其他事务。

就比特币而言，交易即指一次支付转账。其交易规则如下：

1）交易的输入和输出不能为空。

2）对交易的每个输入，如果其对应的UTXO输出能在当前交易池中找到，则拒绝该交易。
因为当前交易池是未被记录在区块链中的交易，而交易的每个输入，应该来自确认的UTXO。如果在当前交易池中找到，那就是双花交易。

3）交易中的每个输入，其对应的输出必须是UTXO。

4）每个输入的解锁脚本（unlocking
script）必须和相应输出的锁定脚本（locking script）共同验证交易的合规性。

对于以太坊来说，交易还可能是智能合约的部署。交易规则就确定了符合一定语法规则的合约才能被部署在区块链上。

5.交易优先级

区块链交易的优先级由区块链协议规则决定。对于比特币而言，交易被区块包含的优先次序由交易广播到网络上的时间和交易额的大小决定。随着交易广播到网络上的时间的增长，交易的链龄增加，交易的优先级就被提高，最终会被区块包含。对于以太坊而言，交易的优先级还与交易的发布者愿意支付的交易费用有关，发布者愿意支付的交易费用越高，交易被包含进区块的优先级就越高。

6.Merkle证明

Merkle证明的原始应用是比特币系统（Bitcoin），它是由中本聪（Satoshi Nakamoto）在2009年描述并且创造的。比特币区块链使用了Merkle证明，为的是将交易存储在每一个区块中。使得交易不能被篡改，同时也容易验证交易是否包含在一个特定区块中，Merkle树说明详见4.2节。

Merkle树的一个重要使用场景就是快速支付验证，也就是中本聪描述的“简化支付验证”（SPV）的概念：轻量级节点（light client）不用下载每一笔交易以及每一个区块，可以仅下载链的区块头，每个区块中仅包含下述5项内容，数据块大小为80字节。

（1）上一区块头的哈希值

（2）时间戳

（3）挖矿难度值

（4）工作量证明随机数（nonce）

（5）包含该区块交易的Merkle树的根哈希

如果一个轻客户端希望确定一笔交易的状态，它可以简单地要求一个Merkle证明，显示出一个在Merkle树特定的交易，其根是在主链（main chain，非分叉链）上的区块头。

Merkle证明可以让区块链得到更广阔的应用，但比特币的轻客户有其局限性。虽然可以证明包含的交易，但无法证明任何当前的状态（例如：数字资产的持有，名称

注册，金融合约的状态等）。一笔交易影响的确切性质（precise nature）可以取决于此前的几笔交易，而这些交易本身则依赖于更为前面的交易，所以最终你需要验证整个链上的每一笔交易。为了解决这个问题，以太坊进行了更进一步的创新。

以太坊的每一个区块头中并非只包含一棵Merkle树，而是包含了3棵Merkle树），分别对应了以下3种对象：

（1）交易（Transactions）

（2）收据（Receipts，基本上，它是展示每一笔交易影响的数据条）

（3）状态（State）

这三棵树允许轻客户端轻松地进行并核实以下类型的查询答案：

（1）这笔交易被包含在特定的区块中了吗？

（2）告诉我这个地址在过去30天中，发出X类型事件的所有实例（例如，一个众筹合约完成了它的目标）。

（3）目前我的账户余额是多少？

（4）这个账户是否存在？

（5）假装在这个合约中运行这笔交易，它的输出会是什么？

第一种是由交易树（transaction
tree）来处理的；第3和第4种则是由状态树（state
tree）负责处理，第2种则由收据树（receipt tree）处理。计算前4个查询任务是相当简单的。在服务器简单地找到对象，获取梅克尔分支，并通过分支来回复轻客户端。第5种查询任务同样也是由状态树处理。

7.RLP

RLP（Recursive Length Pref?ix，递归长度前缀编码）是Ethereum中对象序列化的一个主要编码方式，其目的是对任意嵌套的二进制数据的序列进行编码。

以太坊中的所有数据都以“递归长度前缀编码”（Recursive Length Pref?ix encoding，RLP）形式存储，这种编码格式将任意长度和维度的字符串构成的数组串连

接成字符串。例如，['dog', 'cat']被串接（以字节数组格式）为[130，67，100，111，103，67，99，97，116]；其基本的思想是把数据类型和长度编码成一个单独的字节放在实际数据的前面（例如‘dog’的字节数组编码为[100，111，103]，于是串接后就成了[67，100，111，103]）。

注意RLP编码正如其名字表示的一样，是递归的；当RLP编码一个数组时，实际上是在对每一个元素的RLP编码级联成的字符串编码。需要进一步提请注意的是，以太坊中所有数据都是整数；所以，如果有任何的以一个或多个0字节开头的哈希或者地址，这些0字节应该在计算出现问题的时候去除。以太坊中没有串接数据结构包含任何以0开头的数值。整数以大端基础（Big
Endian）256格式存储（例如32767字节数组格式为[127，255]）。

区块链交易流程

以比特币的交易为例，区块链的交易并不是通常意义上的一手交钱一手交货的交易，而是转账。如果每一笔转账都需要构造一笔交易数据会比较笨拙，为了使得价值易于组合与分割，比特币的交易被设计为可以纳入多个输入和输出，即一笔交易可以转账给多个人。从生成到在网络中传播，再到通过工作量证明、整个网络节点验证，最终记录到区块链，就是区块链交易的整个生命周期。

交易的生成。
所有者A利用他的私钥对前一次交易和下一位所有者B签署一个数字签名，并将这个签名附加在这枚货币的末尾，制作成交易单。

交易的传播。
A将交易单广播至全网，每个节点都将收到的交易信息纳入一个区块中。

工作量证明。
每个节点通过相当于解一道数学题的工作量证明机制，从而获得创建新区块的权力，并争取得到数字货币的奖励。

整个网络节点验证。
当一个节点找到解时，它就向全网广播该区块记录的所有盖时间戳交易，并由全网其他节点核对。

记录到区块链。
全网其他节点核对该区块记账的正确性，没有错误后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块链。

来源： 火球财经

转载请注明“来源：FinPlus
FinTech投资基金旗下自媒体FinTech猫观察（微信号：FinTechCat）”

FinTech 猫观察

每只猫需要花8分钟吃掉一条鱼，FinTech猫让你每天只需8分钟，就可以吃掉一篇行业动态或者标的研究或者深度解读又或者……

FinTech猫观察，国内首个专注于FinTech投资和加速的天使基金FinPlus旗下自媒体，以猫的态度玩转FinTech，敏捷快速的精华资讯、观察透彻的行业研究、角度全面的深度解读、沉稳深邃的冷静分析、硬派Geek的新潮科技，每天给你带来不同的啃食体验。

FinPlus，利用自身产业积累的资源发起FinPlus Wormhole 加速计划。FinPlus Wormhole 加速计划是FinPlus组织业内专家导师而设计的针对于所投的FinTech Startups
的加速课程，内容涵盖金融产品设计、运营规划、经营合规等十多个领域。
有正在FinTech领域创业的团队，可以将商业计划书投递到 BP@FinPlus.me。

FinPlus，旨在以FinPlus Fund + FinPlus Accelerator
的形式搭建行业生态系统FinTech Eco-System，与FinTech
产业链上下游的伙伴们一起，推动中国FinTech发展。

www.FinPlus.vc

本文来自FinTech猫观察，创业家系授权发布，略经编辑修改，版权归作者所有，内容仅代表作者独立观点。[下载创业家APP，读懂中国最赚钱的7000种生意]