该部分包含了大部分与比特币相关的术语。这些术语的使用贯穿于全书，所以对其进行标注以提供快速参考。

地址:

比特币地址（例如：1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV）由一串字符和数字组成。它其实是通过对160位二进制公钥哈希值进行base58check编码后的信息。就像别人向你的email地址发送电子邮件一样，他可以通过你的比特币地址向你发送比特币。

bip:

比特币改进提议 （Bitcoin Improvement Proposals的缩写），指比特币社区成员所提交的一系列改进比特币的提议。例如，BIP0021是一项改进比特币统一资源标识符（URI）计划的提议。

比特币:

“比特币”既可以指这种虚拟货币单位，也指比特币网络或者网络节点使用的比特币软件。

区块:

一个区块就是若干交易数据的集合，它会被标记上时间戳和之前一个区块的独特标记。区块头经过哈希运算后会生成一份工作量证明，从而验证区块中的交易。有效的区块经过全网络的共识后会被追加到主区块链中。

区块链:

区块链是一串通过验证的区块，当中的每一个区块都与上一个相连，一直连到创世区块。

拜占庭将军问题:

一个可靠的计算机系统必须能够处理一个或多个组件产生的失败。一个失败的组件可能表现出通常被忽略的行为类型，即发送矛盾的信息到系统的不同部分。处理这类失败类型的问题抽象地被表达为拜占庭将军问题。

coinbase:

一个用于为创币交易提供专门输入的特殊字段。coinbase允许声明区块奖励，并为任意数据提供多大100字节。不要与创币交易混淆。

Coinbase交易:

区块中的第一个交易。该交易是由矿工创建的，它包含单个coinbase。不要与Coinbase混淆

冷存储:

该术语指的是离线保存比特币。当比特币的私钥被创建，同时将该私钥存储在安全的离线环境时，就实现了冷存储。冷存储对于任何比特币持有者来说是重要的。在线计算机在黑客面前是脆弱的，不应该被用于存储大量的比特币。

染色币:

比特币2.0开源协议允许开发者在比特币区块链之上，利用它的超越货币的功能创建数字资产。

确认:

当一项交易被区块收录时，我们可以说它有一次确认。矿工们在此区块之后每再产生一个区块，此项交易的确认数就再加一。当确认数达到6及以上时，通常认为这笔交易比较安全并难以逆转。

共识:

当网络中的许多节点，通常是大部分节点，都拥有相同的本地验证的最长区块时，称为共识。不要与共识规则混淆。

共识规则:

全节点与其他节点保持共识的区块验证规则。不要与共识混淆。

难度:

整个网络会通过调整“难度”这个变量来控制生成工作量证明所需要的计算力。

难度重定:

全网中每新增2016个区块，全网难度将重新计算，该新难度值将依据前2016个区块的哈希算力而定。

难度目标:

使整个网络的计算力大致每10分钟产生一个区块所需要的难度数值即为难度目标。

双重支付:

双重支付是成功支付了1次以上的情况。比特币通过对添加到区块中的每笔交易进行验证来防止双重支付，确保交易的输入没有被支付过。

ECDSA:

椭圆曲线数字签名算法（ECDSA）是比特币使用的加密算法，以确保资金只能被其正确拥有者支付。

超额随机数:

随着难度增加，矿工通常在循环便利4亿次随机数值后仍未找到区块。因为coinbase脚本可以存储2到100字节的数据，矿工开始使用这个存储空间作为超额nonce空间，允许他们利用一个更大范围的区块头哈希值来寻找有效的区块。

矿工费:

交易的发起者通常会向网络缴纳一笔矿工费，用以处理这笔交易。大多数的交易需要0.5毫比特币的矿工费。

分叉:

分叉也被称为意外分叉，是在两个或多个区块拥有同一区块高度时发生的，此时使区块链产生了分叉。典型情况是两个或多个区块矿工几乎在同一时刻发现了区块。共识攻击的情况下也会出现分叉。

创世块:

创世区块指区块链上的第一个区块，用来初始化相应的加密货币。

硬分叉:

硬分叉，也叫硬分叉改变，是区块链中一个永久分歧。通常在已按照新的共识规则进行了版本升级的节点产生了新区块时，那些未升级节点无法验证这些新区块时产生硬分叉。不要与分叉、软分叉或者Git分叉混淆。

硬件钱包:

硬件钱包是一种特殊的比特币钱包，硬件钱包可以将用户的私钥存储在安全的硬件设备中。

哈希:

二进制输入数据的一种数字指纹。

哈希锁:

哈希锁是限制一个输出花费的限制对象，其作用一直持续到指定数据片段公开透露。哈希锁有一个有用的属性，那就是一旦任意一个哈希锁被公开打开，其他任何安全使用相同密钥的哈希锁也可以被打开。这使得可能创建多个被同意哈希锁限制的输出，这些支出将在同一时间被花费。

HD协议:

层级确定性（HD）密钥创建和传输协议（BIP32），该协议允许按层级方式从父密钥创建子密钥。

HD钱包:

使用创建层次确定的钥匙和BIP32传输协议的钱包。.

HD钱包种子:

HD钱包种子或根种子是一个用于为HD钱包生成主私钥和主链码所需种子的潜在简短数值。

哈希时间锁定合约:

哈希时间锁定合约（HTLC）是一类支付方式，其使用哈希锁和时间锁来锁定交易。解锁需要接收方提供通过加密支付证明承认在截止日期之前收到了支付，或者接收方丧失了认领支付的能力，此时支付金额将返回给支付方。

KYC:

充分了解你的账户（KYC，Know yourcustomer）是一个商业过程，用于认证和验证顾客的身份信息。也指银行对这些活动的监管。

LevelDB:

LevelDB是一个开源的硬盘键值对数据库。LevelDB是一个用于持久性绑定多个平台的轻量级、单用途的库。

闪电网络:

闪电网络是哈希时间锁定合约（HTLCs）的一种建议实现方式。闪电网络通过双向支付通道方式允许支付方通过多个点对点支付通道安全地完成支付。这将允许一种支付网络的构建，该网络中的一方可以支付给其他任何一方，即使在他们双方没有直接建立支付通道的情况。

锁定时间:

锁定时间（技术上来说是nLockTime）是交易的一部分，其表明该交易被添加至区块链中的最早时间或区块。

交易池:

比特币内存池是区块中所有交易数据的集合，这些交易已经被比特币节点验证，但为被确认。

默克尔根:

默克尔树的根是树的根节点，该节点为树中所有节点对的多次哈希计算结果。区块头必须包括区块中所有交易哈希计算得到的有效默克尔根。

默克尔树:

生成一棵完整的Merkle树需要递归地对哈希节点对进行哈希，并将新生成的哈希节点插入到Merkle 树中，直到只剩一个哈希节点，该节点就是Merkle 树的根。在比特币中，叶子节点来自于单个区块中的交易。

矿工:

一个为新区块通过重复哈希计算来寻找有效工作量证明的网络节点。

多重签名:

多重签名指的是需要多于一个密钥来验证一个比特币交易。

网络:

传播交易和区块至网络中每个比特币节点的点对点网络。

随机数:

随机数是比特币区块中一个32位（4字节）的字段，在设定了该值后，才能计算区块的哈希值，其哈希值是以多个0开头的。区块中的其他字段值是不变的，因为他们有确定的含义。

离线交易:

离线交易是区块链外的价值转移。当在链交易（通常简单来说就是一个交易）修改区块链并依赖区块来决定它的有效性时，离线交易则依赖其他方法来来记录和验证该交易。

操作码:

操作码来源于比特币脚本语言，通过操作码可以在公钥脚本或签名脚本中实现压入数据或执行函数的操作。

开放资产协议:

开放资产协议是一个建立在比特币区块链纸上简单有效的协议。它允许用户创建资产的发行和传输。开放资产协议是颜色币概念的一个进化。

OP_RETURN:

一个用在OP_RETURN交易中的一种输出操作码。不要与OP_RETURN交易混淆。

OP_RETURN交易:

OP_RETURN在比特币核心0.9.0中默认的一种被传播和挖出的交易类型，在随后的版本中添加任意数据至可证明的未花费公钥脚本中，全节点中无需将该脚本存储至他们的UTXO数据库中。不要与OP_RETURN操作码混淆。

孤块:

孤块由于父区块未被本地节点处理的区块，所以他们还不能被完全验证。

孤立交易:

孤立交易是指那些因为缺少一个或多个输入交易而无法进入交易池的交易。

交易输出:

交易输出（TxOut）是交易中的输出，交易输出中包含两个字段：1.输出值字段：用于传输0或更多聪；2.公钥脚本：用于确定这些聪需在满足什么条件的情况下才可花费。

P2PKH:

支付到比特币地址的交易包含支付公钥哈希脚本（P2PKH）。由P2PKH脚本锁定的交易输出可以通过给出由相应私钥创建的公钥和数字签名来解锁（消费）。

P2SH:

P2SH是一种强大的、新型的、且能大大简化复杂交易脚本的交易类型而引入。通过使用P2SH，详细描述花费输出条件的复杂脚本（赎回脚本）将不会出现在锁定脚本中。相反，只有赎回脚本哈希包含在锁定脚本中。

P2SH地址:

P2SH地址是基于Base58 编码的一个含有20 个字节哈希的脚本。P2SH地址采用“5”前缀。这导致基于Base58 编码的地址以“3”开头。P2SH 地址隐藏了所有的复杂性，因此，运用其进行支付的人将不会看到脚本。

P2WPKH:

P2WPKH签名包含了与P2PKH花费相同的信息。但是签名信息放置于见证字段，而不是签名脚本字段中。公钥脚本也被修改了。

P2WSH:

P2WSH与P2SH的不同之处在于加密证据存放位置从脚本签名字段转变至见证字段，公钥脚本字段也被改变。

纸钱包:

在大多数特定含义下，纸钱包是一个包含所有必要数据的文件，这些数据用于生成比特币私钥，形成密钥钱包。然而，人们通常使用该术语来表达以物理文件形式离线存储比特币的方式。第二个定义也包括纸密钥和可赎回编码。

支付通道:

微支付通道和支付通道是 设计用于允许用户生成多个比特币交易，且无需提交所有交易至比特币区块链中。在一个典型的支付通道中，只有两个交易被添加至区块链中，但参与双方可以生成无限制或接近无限制数量的支付。

矿池:

矿池一种挖矿方式，在矿池中多个客户端共同贡献算力来产生区块，然后根据贡献算力大小来分配区块奖励。

权益证明:

权益证明（POS）是一种方法，加密货币区块链网络获得分发共识。POS会让用户证明其拥有的资产总量(他们在数字货币中的权益)。

工作量证明:

工作量证明指通过有效计算得到的一小块数据。具体到比特币，矿工必须要在满足全网目标难度的情况下求解SHA256算法。

奖励:

每一个新区块中都有一定量新创造的比特币用来奖励算出工作量证明的矿工。现阶段每一区块有12.5比特币的奖励。

RIPEMD-160:

RIPEMD-160是一个160位的加密哈希函数。RIPEMD-160是RIPEMD的加强版，其哈希计算后的结果是160位哈希值。通过RIPEMD-160加密期望能实现在未来的10年或更长时间都是安全的。

中本聪:

中本聪有可能是一个人或一群人的名字。中本聪是比特币的设计者，同时也创建了比特币的最初实现，比特币核心。作为实现的一部分，他们还发明了第一个区块链数据库。在这个过程中，他们是第一个为数字货币解决了双花问题的人或组织。但他们的真实身份仍然未知。

脚本:

比特币使用脚本系统来处理交易。脚本有着类Forth语言、简单、基于堆栈以及从左向右处理的特点。脚本故意限定为非图灵完备的，没有循环计算功能。

ScriptPubKey (公钥脚本):

脚本公钥或者公钥脚本是包含在交易输出中的脚本。该脚本设置了比特币花费需满足的条件。满足条件的数据可以由签名脚本提供。

ScriptSig (签名脚本):

签名脚本是有支付端生成的数据，该数据几乎总是被用作满足公钥脚本的变量。

秘钥 (私钥):

用来解锁对应（钱包）地址的一串字符，例如5J76sF8L5jTtzE96r66Sf8cka9y44wdpJjMwCxR3tzLh3ibVPxh+。

隔离见证:

隔离见证是比特币协议的一个升级建议，该建议技术创新性地将签名数据从比特币交易中分离出来。隔离见证是一个推荐的软分叉方案；该变化将从技术上使得比特币协议规则更严谨。

SHA:

安全哈希是有NIST（国家标准技术研究所）发布的加密哈希函数族。

软分叉:

软分叉是区块链中的一个短暂分叉，通常是由于矿工在不知道新共识规则的情况下，未对其使用节点进行升级而产生的。不要与分叉、硬分叉、软分叉或者Git分叉混淆。

SPV (简化支付验证):

简化支付验证是在无需下载所有区块的情况对特定交易进行验证的方法。该方法被用在一些比特币轻量级客户端中。

旧块:

旧块是那些被成功挖出，但是没有包含在当前主链上的区块，很有可能是同一高度的其他区块优先扩展了区块链长度导致的。

时间锁:

时间锁是一种阻碍类型，用于严格控制一些比特币只能在将来某个特定时间和区块才能被支出。时间锁在很多比特币合约中起到了显著的作用，包括支付通道和哈希时间锁合约。

交易:

简单地说，交易指把比特币从一个地址转到另一个地址。更准确地说，一笔“交易”指一个经过签名运算的，表达价值转移的数据结构。每一笔“交易”都经过比特币网络传输，由矿工节点收集并打包至区块中，永久保存在区块链某处。

交易池:

一个无序的交易集合，该集合未在主链的区块中，但其有输入交易。

图灵完备:

在给定足够时间与内存的情况下，如果一个编程语言开发的程序能运行在图灵机上，该编程语言就被称为“图灵完备”的编程语言，

UTXO (未花费交易输出):

UTXO是未花费交易输出，UTXO可以作为新交易的输入。

钱包:

钱包指保存比特币地址和私钥的软件，可以用它来接受、发送、储存你的比特币。

WIF (钱包导入格式):

钱包导入格式是一个数据交换格式，设计用于允许导出和导入单个私钥，该私钥通过标志标明是否使用压缩公钥。