在上述概念的基础上，我们就可以介绍比特币的运行原理了。作为一种脱离了实物交接的货币形式，比特币需要解决如下几个基本问题：首先，谁来发行比特币并对其进行信用背书？其次，如何建立账户并进行管理？再次，比特币交易如何确认？

（1）发行和信用背书

与美元等国别信用货币不同，没有中央银行负责比特币的发行，也没有政府为其提供信用背书。比特币的发行是通过挖矿来完成的。每一次有效挖矿都将产生新的比特币，直至达到数量上限。比特币的信用，则源自所有参与比特币挖矿和交易的用户所付出的大量计算，以及由此消耗的时间和电力等成本。人们为此投入的劳动越多，就意味着对比特币的认可程度越高。比特币系统是一种互联网环境下的新型信用体系，它既不需要任何历史信用记录，也不需要任何机构或个人提供的信用担保。换言之，比特币主要依靠理论和技术的双重保障来保证其信用：一方面，人是理性的，在诚实劳动所能获得的报酬远高于欺骗时，没有人会花费力气进行欺骗；第二，比特币的特征决定了欺骗是极其困难的。要成功进行欺骗，不仅需要经受其他所有用户的检验，也需要具有高于全网总计算能力 51% 的计算设备。以目前比特币全网累积的计算能力来看，即便是全球最先进的大型计算机距离这一要求也相差甚远。随着越来越多的新增计算力加入，在比特币的世界里，欺骗的难度将变得越来越大。

（2）账户管理

账户管理涉及账户的建立、查询和安全保障，比特币也不例外。对比特币而言，建立账户就是生成一个地址。比特币的账户、地址和公钥等概念是基本重合的。账户就是一个地址（一串数字），相当于银行账户的户名，这当然是公开的。地址是由公钥通过一系列数学计算推导出来的，因此地址仅仅是公钥的另一种形式。有了地址，就可以查询比特币账户的余额。

虽然地址类似于银行账户名，但与银行账户不同，该地址的余额并没有特意记录在某个地方。如前所述，每一枚比特币自诞生之日起的所有交易路径都是可追溯的，都被记录在主区块链中。因此，每个账户的余额都可以通过对主区块链进行计算得到，而不需要单独记录。这种设计看似麻烦，但有着明显的优势：首先，每个使用者可以拥有的账户数量是没有限制的。随着比特币使用者的不断增多，账户数量也与日俱增，为每个账户单独保存余额是对存储空间的极大浪费；其次，对比特币而言，没有中央节点来保存并管理余额信息，想要保存余额信息，

就必须将其合并写入到区块中。否则，全网节点在对新生成区块的有效性进行检验时，就不仅需要对新的交易进行检验，还需要对全网所有账户的余额进行追溯检验，这无疑会显著增加工作量。在传统银行里，储户不能仅仅通过户名就对账户余额进行查询。然而，比特币世界允许上述操作，也即任何人都可以通过计算主区块链而查询任何账户的余额。比特币账号是完全匿名的，且每个人可以有多个账号，这就保证了比特币拥有者的个人信息不可能通过分析账号来获得。因此，即使将余额信息完全公开，也可以保证拥有者的个人隐私。

比特币账户的安全管理与传统银行系统完全不同。比特币的所有公开信息（例如交易与公钥）都保存在主区块链中，而主区块链在所有运行比特币软件的计算机上都有完整备份，因此其安全管理的关键在于用户私钥的管理。私钥与公钥一样，都是一长串无规律的数字，很难记忆。而且，私钥是独立存在的，不能被公钥或其他方式反推出来。由于私钥是用户对账户所有权的唯一证明，因此用户每次使用账户时都需要使用私钥。为方便起见，很多用户通常选择将私钥放在文件中或网络钱包中保存，这就使得私钥文件面临着被窃取的风险。而一旦私钥遗失或失窃，就意味着比特币账户的彻底丢失。为防范上述风险，“纸钱包”、“脑钱包”等方法正逐渐被接受。毕竟私钥只是一串数字，完全可以通过写在纸上或打印出来的方式进行保存。这种原始的办法在互联网时代反而是一种非常有效的方式。脑钱包的工作原理与纸钱包完全不同。用脑钱包生成私钥之时，我们可将一句话或一幅图片输入特定函数中，就可得到私钥，且这一过程可以反复进行。因此，脑钱包就把记忆私钥的负担转化为记忆一句话或一幅图片，从而显著降低了记忆的难度。即便这句话或这幅图片不慎被公开，他人也很难猜测其真实用途。

（3）交易确认

传统银行账户间的交易是由银行负责确认的，通常在几秒钟内就可以完成。但对挖矿过程中，每个节点在收到其他节点发过来的交易后都要进行验证，验证失败的交易被直接丢弃，而有效交易则会进入区块。由于全网在挖矿过程中可能在同一时间段生成很多有效区块，且由于网络时延的存在，不同地理位置的节点产生的有效区块可能包含不同的交易集合。因此最终哪个区块能够成为当前时间段的正式区块而进入主区块链，就成为一个问题。

如果一个节点收到了周边节点发来的两个不同的有效区块，它会将它们都挂在主区块链的最后，形成一个 Y 形分叉。后续收到的区块都会基于这两个区块产生，这使得分叉会继续向后延伸。最终，哪个分叉的长度最先达到要求，就会

正式变成主区块链的一部分，而另一条分叉则会被抛弃。由此可见，一个交易从发生到最终确认，需要等待一段时间。通常来讲，在包含这个交易的区块出现之后，还需要等待 5 至 6 个后续区块生成后，才能确认当前区块是否已经正式进入了主区块链。由于每个区块的生成时间大约为十分钟，这意味着一个交易在发生之后，需要等待较长时间才能够得到确认。这既是比特币自身的一大缺陷，也是 P2P 这种全民投票形式难以克服的弊端。