

没有区块链，比特币就不可能存在。

这就是它的运作方式区块链技术通常与比特币和其他加密货币相关，但这只是冰山一角。一些人认为，区块链最终可能会改变许多重要行业，从医疗保健到政治。

无论你只是想投资比特币，交易一些以太坊，还是只是对真正的区块链感兴趣，你都来对地方了。

区块链不仅仅是比特币

当你深入研究细节时，区块链技术并不简单，但基本的思想并不难理解。。它实际上是一个由更广泛的社区验证的数据库，而不是一个中央机构。它是一群人监督和记录的记录集合，而不是依赖单个实体，如银行或政府，它们很可能在特定服务器上托管数据。当然，在纸面上保存的物理数据库永远无法由数以万计的对等方管理。这就是电脑和互联网的由来。

每个“块”表示多个事务性记录，而“链”组件将它们与哈希函数一起链接在一起。随着记录的创建，它们被分布式计算机网络所确认，并与链中的前一个条目配对，从而创建一个块的链，或者一个区块链。



整个区块链被保留在这个庞大的计算机网络上，这意味着没有人能够控制它的历史。这是一个重要的组成部分，因为它证明了以前链中发生的所有事情，这意味着没有人可以回头改变事情。它使得区块链成为一个无法轻易篡改的公共分类账，为其提供了一个内置的保护层，这在标准的集中式信息数据库中是不可能的。

虽然传统上我们需要这些中央机构互相信任并满足合同需求，区块链使我们的同行能够以自动化、安全的方式为我们提供担保。

这就是区块链的创新，这就是为什么你可能会听到它用来引用比特币和其他加密货币以外的东西。虽然通常还没有使用它，但区块链可以用来维护各种信息。一个名为Follow My Vote的组织正试图将其用于比现代版本更安全的电子投票系统，并且医疗保健提供商可能有一天会用它来处理患者记录。

区块链从哪里来？

尽管区块链技术在过去的十年中才得到有效利用，但其根源可以追溯到更远的地方。1976年一篇关于密码学新方向的论文讨论了相互分布式分类账的概念，这是区块链有效的作用。后来在20世纪90年代建立了一篇名为“如何给数字文件盖上时间戳”的论文。这需要几十年的时间和强大的现代计算机的组合，加上一个加密货币的巧妙实现，使这些想法变得可行。

数据安全失败，必须有一个更好的系统。区块链创造了一个安全的，不可改变的公共记录，并准备大大改善你周围的世界，从投票系统到租赁合同。

为了以与传统私人分类账相同的方式验证区块，区块链使用复杂的计算。反过来，这又需要功能强大的计算机，这些计算机拥有，运行并保持冷却成本很高。这是比特币充当区块链技术引入的一个很好的起点的原因之一，因为它可以奖励那些参与该过程的人，他们具有一定的财务价值。

比特币最终于2009年首次亮相，将分布式总账区块链的经典理念与完全数字化的货币汇集在一起，该货币不受任何个人或组织的控制。由匿名的“Satoshi Nakamoto”开发的加密货币允许使用交易方式进行交易，同时保护他们免受区块链使用的干扰。

加密货币如何使用区块链？

蓝鲸创服区块链公社认为尽管比特币和其它货币都采用区块链技术，但它们的做法各不相同。自从比特币首次发明以来，它已经在其核心开发者和更广泛的社区的要求下发生了一些变化，并且其他的alt-

coin已被创建用于改进比特币，以稍微不同的方式进行操作。

就比特币而言，其区块链中的新块大约每十分钟就创建一次。该块验证并记录或“证明”已发生的新交易。为了实现这一目标，“矿工”利用强大的计算硬件来提供工作证明 - 一种有效地创建验证块及其包含的交易的数字的计算。在比特币交易可以被视为有效完成之前，必须接受其中的几项确认，即使严格意义上说，比特币实际上是瞬间转移的。

这是近几个月比特币遇到问题的地方。随着比特币交易数量的增加，相对较难的10分钟创建时间意味着可能需要更长时间才能确认所有交易和积压事件的发生。

有一些alt-coins，这有点不同。对于莱特币来说，它更像是两分半钟，而在以太坊方面，阻塞时间只有10-20秒，所以确认的速度往往要快得多。这种变化有明显的好处，但是通过以更快的速率生成块，发生错误的可能性更大。如果在区块链上工作的计算机中有51%记录了错误，则它变得接近永久性，并且生成更快的块意味着处理它们的系统更少。

问题是什么？

区块链技术具有很多令人兴奋的潜力，但是在我们可以说它是未来的技术之前，还有一些严肃的考虑需要解决。

还记得验证交易所需的所有计算能力吗？这些电脑需要电力。比特币是一个巨大的区块链网络所要求的权力升级的典型代表。虽然关于比特币的功率要求的确切统计数据很难，但它在当前状态下经常与小国进行比较。鉴于今天对气候变化、发展中国家的电力供应和发达国家的电力可靠性的担忧，这并不吸引人。

交易速度也是一个问题。。如上文所述，链中的块必须由分布式网络进行验证，这可能需要时间，很多时间。更糟糕的是，比特币的平均交易时间超过了41个小时。以太坊的效率更高，但其平均时间约为15秒。用于加密货币以外目的的区块链可能遇到类似的问题。您可以想象，如果每次想要更改数据库条目时等待15秒会有多么令人沮丧。

随着区块链变得越来越流行，这些问题将需要解决。不过，考虑到我们距区块链的第一个实现还不到10年，我们似乎很可能只是看到了这个新想法的开始。