

基于区块链理念带来了一场风暴，人们开始思考如何彻底改变权力集中化的结构，将控制和管理信息的权力迁移到一个无人掌控的去中心化系统中。

相对于中心化的系统，比特币具有去中心化的、发行总量固定、不可伪造、账户匿名、全球流通等特点。

去中心化运作，无央行存在

比特币是一种分散的货币，采用端到端（P2P）的技术实现。去中心网络的架构非常简洁，本身需要的基础设施很少，与比特币有关的所有事宜，包括发行、交易处理和验证都是通过网络进行的，不存在一个专门的机构来监控整个资金流动的过程。

比特币使用P2P技术，且不受中央机构的管辖。这就意味着，从人类社会现今至未来对于互联网的依赖性来看，只要互联网和人类不毁灭，比特币就会一直存在下去，并一直被人们所拥有、使用、流通。

相比之下，传统的货币是由各国央行发行的，是国家货币政策的一部分。这种传统货币发行机制是完全依托于人民对于国家、政府、经济体系的信任存在的，一旦政策变更、政府变动、国家颠覆或经济危机，法币的价值、流通等诸多方面将会受到严重的打击。

总量固定，不会通货膨胀，但可无限分割

比特币的发行上限为2100万枚，大约在2140年其新增量将降至无限接近于0。从这个角度看，无论单位币值如何变化，由于其整体总量的严格限定，比特币只能是通缩的货币，而不可能形成通胀。

相对应的传统货币的发行没有上限。各国央行可以根据政府需要、当前经济总量变化、黄金储备等方面的因素，不断地增发货币，这就是传统货币所不可避免的通货膨胀现象。

虽然有些批评者认为比特币发行量不够大，但支持者认为一枚比特币的价值可以切分到小数点后八位，即比特币的最高价值可以达到 21×10^{14} ，足以满足将来各种可能的需求。

货币不可伪造，无法多重支付，交易不可逆转

工作量证明(PoW共识)是区块链账本的安全机制，这一共识机制保证了区块链上的数据记录的可靠性。

如果有人修改了算法，那么其生产出来的区块中所记录的数据就会有所改变，系统中所有节点在进行正确性判定时会第一时间发现差异，将会不承认它，那么修改算法后的运算就是无效的，这样就保证了其货币的不可伪造特性。

比特币系统中的交易是拥有严格的信用机制的，其主要表现在交易过程中不可出现透支与空头支付。同时，比特币在交易中也是不能够进行多重交易的，所谓多重交易是指将同一笔钱消费两次以上。

账户匿名，且任何人均无法冻结，无法收税

比特币存在于某一个或多个存款地址中，这些地址都是不记名的，没有人知道一个长达32位的比特币地址是谁的。尽管这个地址的各种交易又被全网的节点所验证和记录。账户没有署名，自然也就无法针对该账户的收入与交易收税，因为比特币系统中是不提供发票的。

比特币账户无法被司法冻结，因为网络是去中心化的，就算也知道某个地址中有大量的比特币，政府或司法机构得到了这个地址，但不知道被多重加密的私钥，因此无法将地址中的比特币转出，亦无法对账户进行限制。

全球无障碍流通，快速支付且成本极低

目前全球各地有数十万个比特币节点，我们不仅可以通过渠道从这些节点中购买到比特币，也同样可以通过互联网很方便地将比特币兑换成许多国家的法定货币。我们只要有一个比特币钱包，加上一个可以随时随地上网的手机或笔记本电脑，就可以在那里畅行无阻，随时随地上网换钱或通过支付比特币购买到想要的商品和服务。

比特币的兑换与交易速度很快，可在几秒内完成交易，10分钟之内得到全网确认并记录，实现交易完成。这比用一种法币兑换另一种法币来得容易且成本低很多。

区块链技术的应用

取代金融领域现有设施是比特币的设计目标之一，而在金融领域，银行家们开始正视区块链技术用于替代银行间证券和资金转移、清算、结算这类复杂流程的可能性。

利用比特币技术，我们可以鼓励此前无法存在的新型协作方式的出现，革新一系列产业，转变组织的设置方式。确实，区块链技术具有广泛潜力。下面列举了一些潜在的例子，但并没有覆盖所有的可能性：

- 不可侵犯的产权记录，人们可以证明对自家房产、汽车或其他资产的所有权；
- 银行和银行间实时、直接进行的证券交易结算，这可能会开启一个万亿美元的银行间市场，替代涉及数十个特定机构并需2-7天才能完成的模式；自我主权身份识别机制，无须依赖某个政府或公司去建立个人身份；
- 去中心化计算，能够通过普通用户的计算机硬盘和运算能力代替各种公司的云计算和网站存放业务；
- 去中心化的物联网交易，在其中设备能够直接进行安全对话和交易，移除了中介机构带来的摩擦，为运输产业和去中心化能源网络带来很大的发展潜力；
- 基于区块链的供应链，其中各家供应商在某种特定商品的生产流程中，可以使用一个共同的数据平台去分享其业务流程，最大限度地提高可追责性、效率及融资机会；
- 去中心化的媒体和内容平台，这将为音乐家和艺术家赋能，此外，在理论上，任何人在网络上发布有价值的信息后都可以管控和追踪这种“数字资产”。

比特币将信任的管理分发给一个由共同协议引导的去中心化网络，而非依赖某个可信的中介机构，再引入全新的、数字化的货币、代币和资产，我们可以改变组织的根本性质。这种方式可以拓展成一个社会性的技术，构建起如何治理社区的蓝图，若要让区块链技术走向正确的方向，需要社会各个方面的共同努力。

声明：国内禁止ICO融资和虚拟货币的交易、炒作；本人未持有比特币等虚拟货币及进行相关行业投资；本文是个人出于兴趣而做的记录，不构成投资建议。