基本概念

莱特币 (Litecoin, LTC) 是受比特币(BitCoin, BTC)
的启发而推出的改进版数字货币，由一名曾任职于谷歌的程序员（李启威Charlie Lee）设计并编程实现，2011年11月9日发布运行。莱特币与比特币在技术上具有相同的实现原理，但莱特币的创造和转让基于一种开源的加密协议，不受到任何中央机构的管理。

莱特爸爸

李启威是一名亚裔美国人，1999年毕业于麻省理工学院（MIT），拥有学士和硕士学位，主攻专业电气工程和计算机科学。毕业后他成为了谷歌的一个默默无名的程序员。

李启威在谷歌工作期间受到比特币的启发，基于同样的去中心化数字货币原理开发了莱特币。他的聪明之处，就是承认莱特币是比特币山寨币，以“比特金，莱特银”的口号，让莱特币的市值一直稳居数字货币前十。莱特币曾一度霸占数字货币市值的第二名，仅次于比特币。

李启威，不但在运营数字货币项目上是一把好手，在预测行情上也精准到出人意料。17年12月20日莱特币到顶后，李启威在Reddit发帖称在过去的几天中抛出了手上全部的莱特币，可谓成功逃顶。

减半变化

今年8月，莱特币即将迎来第二次减半(每840,000个块)，相比于上次2015年8月28减半，行情5月22发动，提前84天，结束于7月9号，持续58日。从9元到55元，35以上的价格只维持了3天，然后迅速暴跌到25。走了明显的五浪结构，五浪暴涨。冲顶只用5天。2019年8月5日减半，按照这个规律，5月初之前需要提前做好布局，然后跟踪行情变化。

VS比特币

共同点

1、同为虚拟货币：

莱特币和比特币一样，都是虚拟货币，没有实体形态。开发和支付过程都是一连串复杂的求解代码，通过挖矿来获得币而不是印刷，根本上杜绝了普通货币的假币泛滥问题。在支付过程中都使用地址和私钥来交易，这好比密码和钥匙，这些地址和私匙的组合排列有上亿种可能，很难破解，提高了安全性。不过即使是去中心化的支付系统，莱特币和比特币系统仍然受到“51%Attack”的威胁，即使用全网的51%以上的算力进行运算构建一个区域链与全网赛跑，一旦成功将能掌控币，这将造成严重的后果。它们采用区块链技术，所有历史记录按照时间先后顺序，打包成一个个单独的区块，再把这些单独的区块链接在一起形成一个总账本。这些区块内除了包含交易记录外，还包含新发行的莱特币和交易的手续费，这两笔钱支付给挖矿的矿工作为酬劳。无论谁挖到该区块，那么该区块内含有的新发行的莱特币和交易的手续费这两笔钱都归挖到者，以鼓励矿工积极参与结算。

区块链技术容易产生51%攻击的问题：无论任何组织甚至个人，只要掌控某一种基于区块链原理的虚拟货币的全部运算能力的51%，这个人或组织就能够任意操纵该虚拟货币的所有交易。如果区块链只认运算能力最大者，谁的运算能力最大，谁就能抢到下一个区块，如果某个个人或组织掌控了全部运算能力的51%，那就意味着没人比他运算能力更强，故而他就可以随意操纵。所以，对于基于区块链原理的虚拟货币，参与挖矿的越多就越健壮，运算能力越分散就越健壮；挖坑者越少越脆弱，运算能力越集中就越脆弱，矿池越集中也就越脆弱。虽然“51%Attack”发生的概率很小，但是对于一个公共虚拟货币系统来说，这样的漏洞是不应该被忽视的。

2、去中心化架构：

莱特币和比特币一样，都是去中心化的架构，无任何中心机构控制，新币发行和交易支付、转让不需要中央银行、也不需要商业银行。

不同点，改进之处

1、工作量证明机制算法：

比特币使用SHA-256算法，而莱特币工作量证明机制算法采用了scrypt算法，使运算能力难以集中，难以形成像比特币那样的大型矿池，挖矿的矿工比比特币更分散，这也就更有利于防止51%攻击。如果某个山寨币的算法跟比特币相同，那么矿工就可以直接将为比特币定制的芯片矿机拿来挖这些山寨币，或者实施51%攻击；这就会让这些与比特币算法相同的山寨币迅速失去价值。所以，正是因为莱特币的scrypt算法跟比特币的算法不同，比特币芯片矿机无法拿来挖莱特币，这就让莱特币免于攻击，保持了正常发展。同时，相比于比特币，在普通计算机上进行莱特币挖掘更为容易。每一个莱特币被分成100,000,000个更小的单位，通过八位小数来界定。

2、总量上限

莱特币总量上限是8400万个，比特币总量上限是2100万个，莱特币总量上限是比特币的四倍。

3、区块生成速度快

莱特币是2.5分钟，比特币是10分钟。比特币的一个缺点就是交易的确认比较慢，区块打包需要10分钟，打包之后还要全网节点验证，验证的时间更长，两个时间加起来总共需要大约40至50分钟左右。莱特币的区块打包速度是比特币的四倍，加上交易确认的时间，总共大约20分钟之内即可完成。

4、安全节点多

2013年5月，比特币的全网算力是全球排名前500名超级计算机的总和的8倍，达158THash/s。而莱特币因GPU挖矿的性能限制，全网算力仅为15GHas/s。莱特币每2.5 min处理一个区块，比特币是10min，对区块链发起一次双重支付攻击的进度服从泊松分布，其攻击成功的概率随区块数的增长而呈指数级下降。当区块数大于6个时，攻击成功的概率将下降到忽略不计的程度，这也正是比特币建议6个确认数方可保障交易安全的依据。当区块的处理速度提高至比特币的4倍时，攻击者制造出一个假节点的成功概率也急剧上升，通过计算泊松分布的概率密度，避免双重支付攻击所需要的节点确认数也将上升至比特币的4倍，即菜特币需要24个节点确认才能达到比特币6个节点确认的安全性。

总结

虽然莱特币没有白皮书，没有长期的路线图，但它的定位是明确的——做一个“轻量级的比特币”，通过更快的交易速度、更低廉的交易，专注于日常小额支付的加密货币，正如其“比特金，莱特银”的口号一样。

加密货币的分散化、解除管制、交易透明度和匿名性以及去中心化支付的安全性，收到了越来越多的追捧。未来的市值到底会有多少？一切都有待时间给我们答案。