门罗币 概要

门罗币是一种安全的、私有的、任何人都可以拥有的、不可追踪的电子货币。

用户花得放心，没有人可以看到他们的余额或追踪到他们的交易。

Revised 7/26/2018 - **Printer Friendly Version**
Created for the community by Monero Outreach

getmonero.org

核心原则

作为个开源性的项目，门罗币是一群去中心化的开发者和社区成员开发的，它具有不可篡改性。大多数贡献者是志愿者，参与者遍布全球。

安全

作为去中心化加密货币，门罗币因全球用户众多而更安全。交易被分布式共识确认后，将会被记录在区块链中，无法被篡改。

可扩展性

为了提供更低的交易费用和更快的交易速度，门罗币动态区块尺寸可以根据交易量进行调整。高交易量会形成更大区块尺寸限制，而低交易量又会形成更小的区块尺寸限制。门罗币动态块根据交易量来变化，这样交易费用会更低，交易会更快。高交易量会带来更大的动态块限制，反之亦然。

核心原则

在门罗币上的交易不会显示用户真实身份，因此用户不受监察和资本控制。

审查阻力

门罗币使用一种基于环签名的复杂加密方式，环保密交易，和隐秘的地址来混淆交易的原点，数额，以及交易的所有目的地。

隐私权益

因为默认加密，门罗币有可互换性。换言之，每一枚门罗币都是对等的。门罗币不会因为产生的源点和历史而受到交易者或者交易所的歧视。

可互换性

门罗币的历史

门罗币始发于 2014 年 4 月。门罗币的 Cryptonote 参考代码，发起公平且有提前声明。门罗币没有任何预挖现象，开发者也没有私自挖取，并且研发团队也没有享受区块奖励。门罗币有了几次大的改进。您应该可以看到 Bitcointalk 原文这里。

发起后门罗币进行了几次大改进。几乎所有的改进都是以改善隐私、增强安全为首要，或更便于使用。门罗币继续以保密性和安全性为首要开发目的，应用的便捷性和高效性次之。

门罗币是什么意思?

‘门罗币’这个词是来自世界语。门罗币的创造者借 用 这个世界语的单词，因为它是个‘去中心 化’的语 言，代表着打破人群和范围的限制。
在世界语中，Monero 由三个自由组成的语素构成，每个语素都有各自的意义。

mon-	：	钱
-er-	：	最小部分
-o	：	一件事物（从语法上说指一个名词）

也就是说，门罗币的含义可以被看作是“一个描述钱的最小部分的名词”，或者说 —— 币。

关键的差异化特质

- **门罗币使用‘CryptoNote’代码基库：** 这从根本上不同于比特币、以太坊、和大部分相互衍生出的加密货币。门罗币以大幅度改善用户隐私而著称。

- **它默认保护用户隐私，用户可以自行选择交易是否透明：** 门罗币最前沿的密码学模糊了每 一 层交易 : 信息发送者、接收者、以及交易本 身。如果用户想要透明交易的话，他们可以建 立 并分享 一 个能够显 示 已输 入 并且只供可读访问的钱包 。

- **日常的网络升级：** 门罗币社区的开发者经常进行网络升级（硬分叉）来确保所有用户均可享有当下最好的安全，隐私和其他特色。这样有助于门罗币通过网络升级，适应任何可能出现的机会和挑战来维持系统安全。 为什么人们总是讨论硬分叉?

- **门罗币区块奖励的轨道计算：** 区块奖励将要渐渐地出现，最后一个阶段的区块奖励在 2022 年五月开始，那时奖励将会定为 0.6 XMR 每区块。最后一个阶段提供持续的，无限期的矿工奖励。此外，或许更重要的是，最后一个阶段会提供门罗币一种内置的、 稳定且可预见的的通货膨胀率。这对健全货币来说必不可少。

- **门罗币的研究实验室：** 门罗币不仅致力于开发可替代数字货币，也同样持续关注包括加密货币在内的金融隐私领域。至此，数学和计算物理学的研究人员发表了白皮书，并且正努力实现更多的研究目标。

- **挖矿是易操作的：** 任何有一台连接网络的设备或网页浏览器都可以参加。

现实世界的应用场景

因为门罗币安全，交易费用低且无国界限制，人们可以轻易的汇款，无需担心政府腐败或者银行破产。 这为个人提供了应对身处受压制国家以及经济萎靡的经济支撑。这帮助了个人加强经济安全。私人的金融历史保护消费者和公司免受价格操控，供应链剥削以及经济歧视或者类似情况。

门罗币是唯一一种可以完全对等的、去中心化的电子加密货币。

技术基础

（如 *7/26/2018*）

活动节点总数：	1,233（来源：https://monerohash.com/nodes-distribution.html）
网络哈希率：	430.7 MH/s
每小时平均交易数：	168（平均 30 日）
CPU 核心保护网络数：	14,357,070
在流通中的门罗币：	16,260,440 XMR（近似）
市场资本总值：	$2,308,736,565 USD（~0.77% 数字货币市场的总值）
目前的区块奖励：	4.169 XMR
平均区块区间：	2 Minutes

奖励率将会稳定降低直到 *2022* 年 *5* 月末，到那时一共将有一千八百一十三万两千 *XMR* 在流通中，*0.6 XMR* 的区块奖励将会无限持续。
通过最终阶段的 *0.6 XMR*/ 每区块奖励，到 *2040* 年，门罗币的总数将会和比特币持平（大约在 *2100* 万左右）

在开发中的功能

虽然门罗币在全球范围内使用中，开发者们还是有很多令人兴奋的目标，包括继续加强隐私性，安全，和可使用性等，以及普通加密货币的问题。有一些功能即将面向公众：

Bulletproofs: 更有效保存区块链，交易速度更快。

Kovri: 这是一个重要的私密性上的升级，给门罗币交易加上四重私密性。Kovri 使用 garlic-encryption （想一想 Tor X10） 来掩盖发送方和接收方的 IP 地址。每一重门罗币交易，从发送方，接收方，交易数额以及（用 Kovri) 交易本身，都将会是私密的，安全的。

硬件钱包： 有名的 Ledger 和 Trezor 硬件钱包在努力加上门罗币。门罗币社区目前资助一个团队基于门罗币理念来建立一个硬件钱包。这些硬件钱包都预期在 2018 年底开始运行使用。

Kasisto: 针对商人和商业简化销售 (POS solution) 行为而设计。

额外资源

getmonero.org（官方网站）
monero.how
reddit.com/r/monero
门罗币指南 *(post)*
门罗币深入的技术分析
门罗币入门导论 *Zero to Monero*

避免诈骗
门罗币 *FAQ*
门罗币 *SWOT* 分析
跟门罗币社区联系
掌握门罗币 -（即将推出）

Monero Quick Facts - 修订 7/26/2018 为门罗币社区，由门罗币 Outreach 社区创建

门罗币 Outreach 社区以教育和公共关系为致力日益普及 —— 您的捐款成为可能

47oKHkoaQdBdFpTJNKaetUS6UsCGHVbJbGxPGaaHFQPqXSCLbqXYsBo6x7abwtfdXTeiBhtZLnYF5bRRAhYsUVb5Sd1aqiD