

门罗币历史价格走势走势图

XMR/USD 价格走势走势图



什么是门罗币 (XMR) ?

门罗币，也被称为 XMR，是一种加密货币，在其协议中编码了隐私增强功能。大多数流行的加密货币，如比特币和以太坊，在透明、不可变的分类账上运行，使任何人都可以查看和跟踪交易。Monero 也是一个开源区块链，但其功能旨在减少可追溯性并保护用户匿名性。

门罗币的隐私增强功能

门罗币的主要目的是提供一个去中心化的网络，增强交易隐私性和匿名性。正如 Monero Space 工作组的组织者 Justin Ehrenhofer 所解释的那样，“我们希望提供隐私，只是堵住大多数加密货币协议中存在的一些基本漏洞.....因此，门罗币确实是唯一一种隐藏发送方、接收方和金额的货币。”

门罗币区块链采用了多种以隐私为中心的方法来掩盖用户的交易历史：

- 环签名 (Ring signatures) 将多个用户连接在一个 “环” 中，以隐藏他们的个人身份，从而使确定哪个用户生成给定签名变得更加困难。
- 2017年，Ring Confidential Transactions (RingCT) 被添加到门罗币中，并隐藏了交易金额。
- 通过使用隐身地址，所有门罗币发送者每次发起新交易时都会自动生成新地址，从而模糊了资金的来源和目的地。隐身地址与实际接收付款的公共地址加密绑定，但只有发送方和接收方知道两者之间的关联。相关方有一个私有视图密钥（用于显示传入的交易）和一个私有支出密钥（用于发送支付）。
- 交易可以通过 Tor/I2P 发起，它利用匿名网络保护交易源的隐私。这个功能是最近才开始的，仍然被认为是实验性的。
- dandelion++ 隐藏与节点关联的 IP 地址，以减少使用敏感信息暴露地址身份的风险。



门罗币挖矿奖励

与比特币区块链类似，门罗币采用了工作量证明共识机制。它的 PoW 算法 RandomX 旨在维持去中心化的挖矿，并抵制专用硬件（如 ASICs）。XMR 的发行是无限的，以确保持续地挖矿激励，门罗币大约每两分钟生成一个新的区块。矿工可以决定是单独挖矿还是在池中挖矿，尽管门罗币项目鼓励单独挖矿，因为这有助于提高网络安全性。

在 2020 年 3 月至 2023 年 1 月期间，Chainanalysis 确定了门罗币挖矿奖励接受者的代表性样本。在我们的样本中，三个主要矿池开采了超过 80% 的 XMR。

门罗币历史价格走势走势图以及它的一些基础知识分享到这里就结束了，希望能帮助到各位投资者！