门罗贡献者Diego Salazar表示：

> 门罗非常重视去中心化和草根结构，这意味着我们没有预挖，我们不收取区块奖励，没有ICO。

Salazar估计有100到200名志愿者参与门罗项目的开发。

此外，根据Salazar的说法，该项目本身不仅仅只是构建区块链协议，更是关于重新定义和支持以数字隐私为核心的全球性运动。

> 我们不仅仅是想创造全球互联网货币。我们正试图告诉人们隐私等事物的重要性，这是一个非常强大的工具，我认为在我们这个时代，这是一个非常必要的工具。

为此，意大利开发者和门罗贡献者“SerHack”发布了免费的PDF读物《精通门罗币》以纪念其诞生五周年。该书最早于2018年末出版，完全由门罗社区资助，并向

非加密圈的用户传递了“隐私和抗审查交易”的重要性。此外，该项目的在线社区还通过各种活动进一步纪念了这个重要日子。

虽然门罗并不是唯一一种致力于链上隐私交易的区块链，但它是同类币种中市值最高的，据QKL123，门罗的市值超过了80亿人民币。

在这五年的时间里，该项目进行了一系列重大升级，包括增强可互换性（fungibility）和交易隐私的升级。

从自选隐私到默认隐私

门罗贡献者Justin Ehrenhofer说：

> 对于门罗的可互换性来说，保密资金来源是至关重要的。这样一来，你就不知道自己接收的资金之前的用途。

从一开始，门罗就试图通过“环签名”（ring signatures）来混淆资金来源。通过环签名，交易由一组参与者中的某一位成员签署（每个参与者都有私钥），但其目的是让人们很难知道这组参与者中究竟是谁提供了特定的数字签名。

Ehrenhofer解释道：

> 在门罗网络中，你所花费的每一个输入，都会从区块链中提取其他的输入，即其他人的随机输入……这会使所有这些输入看起来都被花费了。从数学上看，这些（输入）中的任何一个都可能是（交易）签名者。

然而，在启动时，提取随机用户的交易输入（即环签名）并不是强制性的。加密货币交易所、公开的矿池和其他不在乎交易隐私的用户可以选择将“ringsize”（环的大小）设为零。

门罗的研究人员意识到，如果有过多用户选择不混淆他们的交易来源，那么其他用户的隐私可能会受到损害。

Ehrenhofer说：

> 如果我发送了一个显示我实际支出的交易，那么这意味着，如果其他人再用我的支出进行伪装，所有人都会知道这是假支出，因为在我的交易中，

> 我显然已经花费出去了。

因此，在2016年3月22日，门罗执行了一个硬分叉来强制所有用户至少将ringsize设置为3来混淆他们的交易源。这意味着用户在进行自己的交易时，需要从网络中至少其他三个随机交易输入中提取数据，从而共同参与增强整个区块链的隐私。

> 门罗一开始就需要克服的一个重大挑战是改善现有的基础设施。这基本上意味着迫使人们使用最佳实践，并强制启用环签名。

环签名+保密交易形成的强大隐私保护网

门罗历史上第二大重要的改进也和环签名有关。

即环“保密交易”（CT）。此升级于2017年1月5日通过硬分叉执行。它通过混淆门罗的交易金额，有效地为环签名增加了一层额外的隐私。

RingCT的激活意味着，除了无法识别交易来源或地址外，Monero现在已经彻底隐藏了交易金额。

Ehrenhofer表示：

> 这些输出已经与地址断开了连接。RingCT更进一步地展示出，当这些输出被处理时，我们也不知道其具体金额。

事实上，当用户在区块链浏览器上查找门罗地址时，其将收到一个“警告”：

> 啊哦，好像想偷看这个门罗交易的地址……看起来你真的像是，想看看这个家伙的余额。但是门罗说不可以！

RingCT来源于Blockstream首席技术官Gregory Maxwell提出的一项名为“保密交易”（Confidential Transactions）的比特币提案。之后由门罗开发者进行重新设计并用于环签名。

然而，在提高门罗区块链的隐私的同时，RingCT实际上在可扩展性方面做出了重大牺牲。

Ehrenhofer透露：

> 在RingCT添加之前，交易大小约为3kb，大约是比特币交易的10倍。RingCT让这一些数字增加到了13kb，也就是增加了4到5倍。

门罗网络的“防弹”保护

在这一点上，“Bulletproofs”（防弹）——虽然没有对隐私做出直接的改善——但仍然被认为是对该网络的重大改进。

Ehrenhofer称，Bulletproofs技术让门罗的交易规模和验证时间减少了约80%，实现了从13kb到1.5kb的惊人改变，门罗的交易大小已经大幅下降——尽管目前仍然比比特币交易更大，也更难验证。

这项技术在2017年底发布，被誉为隐私方面的重大突破，最初由伦敦大学学院的Jonathan Bootle和斯坦福大学的Benedikt Bunz为比特币设计。最终，在2018年10月18日，门罗成为第一个通过硬分叉使用该技术的主流加密货币。

尽管如此，Ehrenhofer指出，网络上的验证时间仍然是“目前门罗最大的阻碍”。

> 在门罗网络中最难实现扩容的并非交易大小，而是验证时间。我们今天可以让门罗的环签名变得十分强大……但交易验证时间依然难以突破。即使它不会占用你电脑上那么多的空间，你也要花很长时间才能搞清楚它。

因此，展望未来，Ehrenhofer希望即将到来的协议改进能够找到一种方法，增加环签名的大小，以便在某一天能够承载超过1000个匿名集。

在Salazar看来，门罗另一个即将到来的改进是对网络用户界面和体验的升级。

> 很多东西都是从头开始重新设计的，比如个人页面、交易历史页面、发送和接收页面。