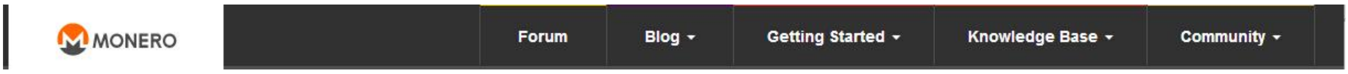
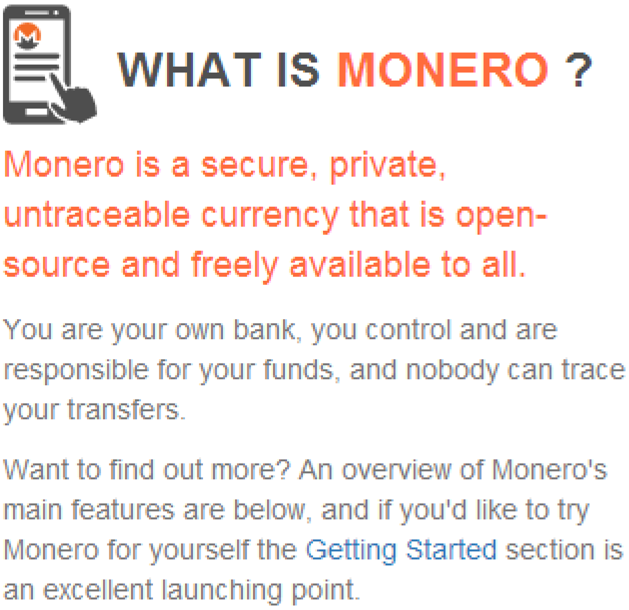
Section 1：Home page https://getmonero.org/home



门罗币　　　　　　　　　　　　　　　　　　　　　　　　论坛　博客　启用　知识库　社区



WHAT IS MONERO ?

Monero is a secure, private, untraceable currency that is open-source and freely available to all.

You are your own bank, you control and are responsible for your funds, and nobody can trace your transfers.

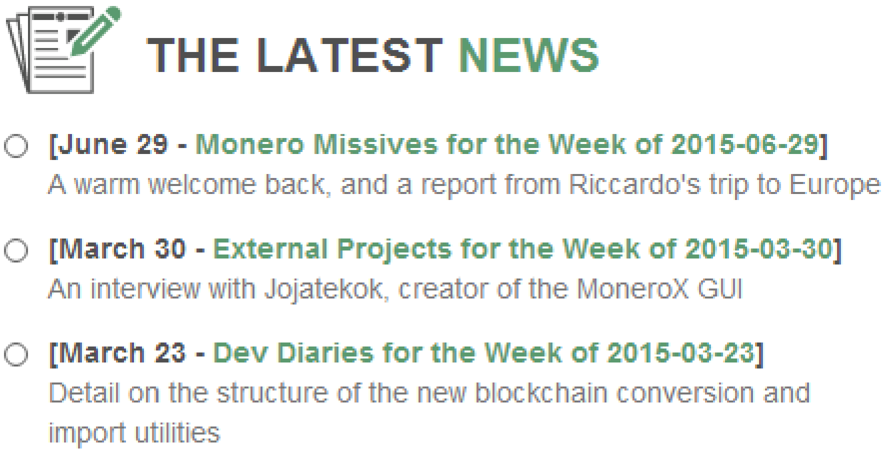
Want to find out more? An overview of Monero's main features are below, and if you'd like to try Monero for yourself the Getting Started section is an excellent launching point.

什么是门罗币（Monero）？

门罗币是一种安全性，隐私性极高的货币，同时具有开放性，适用人群广泛等特点。

使用门罗币时，您可以控制您的银行，操控并负责管理您的资金，其他人无法追踪您的任何货币转移行为。

想了解更多吗？请参考下文中门罗币的主要特点，如您有兴趣尝试门罗币，只需点击网页上方的启用标签，便可享受门罗币的卓越性。



THE LATEST NEWS

○ [June 29 - Monero Missives for the Week of 2015-06-29]
A warm welcome back, and a report from Riccardo's trip to Europe

○ [March 30 - External Projects for the Week of 2015-03-30]
An interview with Jojatekok, creator of the MoneroX GUI

○ [March 23 - Dev Diaries for the Week of 2015-03-23]
Detail on the structure of the new blockchain conversion and import utilities

最新消息

- 6 月 29 日-门罗简讯（2015 年 6 月 29 日）

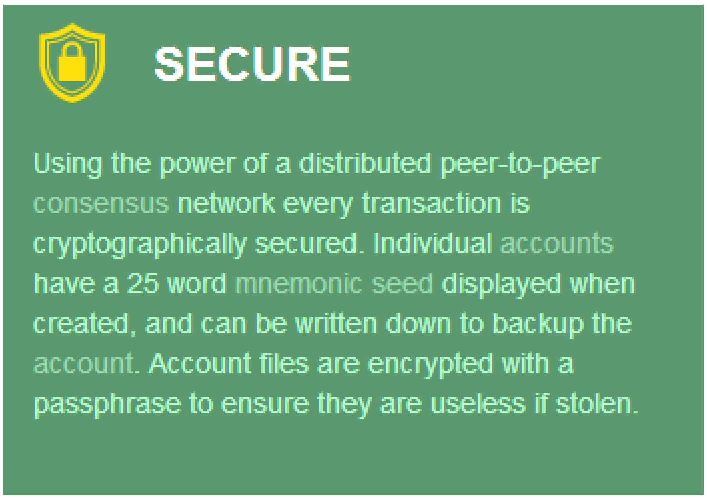
  欢迎回来，进来听 Riccardo 讲他的的欧洲之旅吧！

- 3 月 30 日-外聘项目（2015 年 3 月 30 日）

  采访 MoneroX 图形用户界面设计者 Jojatekok,

- 3 月 23 日-开发者札记 （2015 年 3 月 23 日）

  详细说明新的数据区块转换和导入实用程序

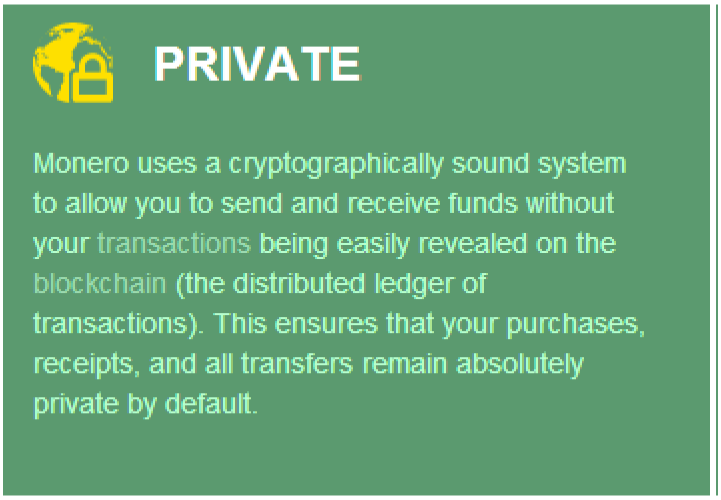


SECURE

Using the power of a distributed peer-to-peer consensus network every transaction is cryptographically secured. Individual accounts have a 25 word mnemonic seed displayed when created, and can be written down to backup the account. Account files are encrypted with a passphrase to ensure they are useless if stolen.

安全性

每笔交易都因受到点对点**共识**网络的保障而具有高度安全性。个人**账户**在创建时会显示 25 个**记忆种子**，并可被记录下来以作备份。**账户**文件可加密，因此，盗取这些文件也是无用功。

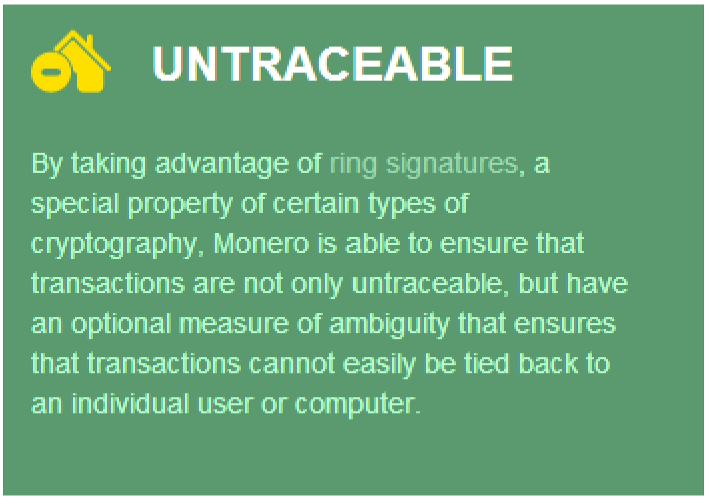


PRIVATE

Monero uses a cryptographically sound system to allow you to send and receive funds without your transactions being easily revealed on the blockchain (the distributed ledger of transactions). This ensures that your purchases, receipts, and all transfers remain absolutely private by default.

隐私性

门罗币采用加密安全系统，因此，无论是转入还是转出资金，**数据区块**（分布交易总账）都很难查出您的**交易**信息。这保障您的购买，接收，转账行为长期并自动处于隐秘状态。

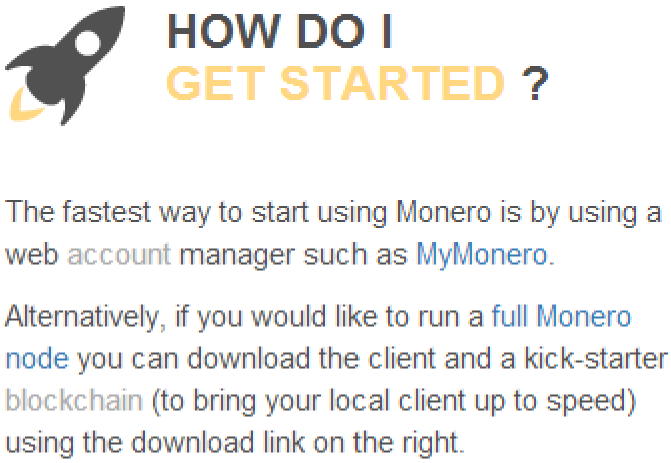


UNTRACEABLE

By taking advantage of ring signatures, a special property of certain types of cryptography, Monero is able to ensure that transactions are not only untraceable, but have an optional measure of ambiguity that ensures that transactions cannot easily be tied back to an individual user or computer.

无迹可寻

群签名是一种加密系统的特性。利用此特性，门罗币便可以保障交易不禁无迹可寻，而且用户也可选择模糊交易与计算机或用户间的联系。



HOW DO I GET STARTED ?

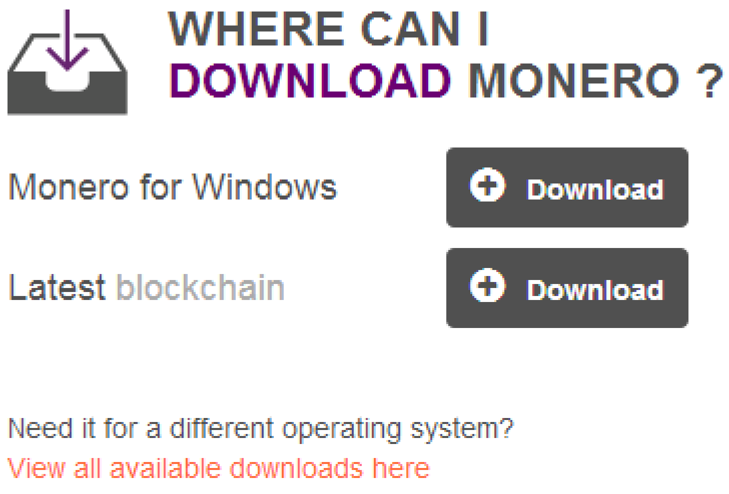
The fastest way to start using Monero is by using a web account manager such as MyMonero.

Alternatively, if you would like to run a full Monero node you can download the client and a kick-starter blockchain (to bring your local client up to speed) using the download link on the right.

我又如何开始呢？

最快的启用方式便是网络账户经理，如，“MyMonero”.

或者，如果您希望运行完整门罗币网络节点，请点击右侧下载链接，下载用户端及反冲启动数据区块（加速下载本地用户端）


WHERE CAN I DOWNLOAD MONERO ?

Monero for Windows

Latest blockchain

Need it for a different operating system?
View all available downloads here

在哪里下载门罗币 MONERO ?

Windows 用户　　　　　下载

最新数据区块　　　　　下载

您使用的是其他操作系统吗？

查看所有可用版本

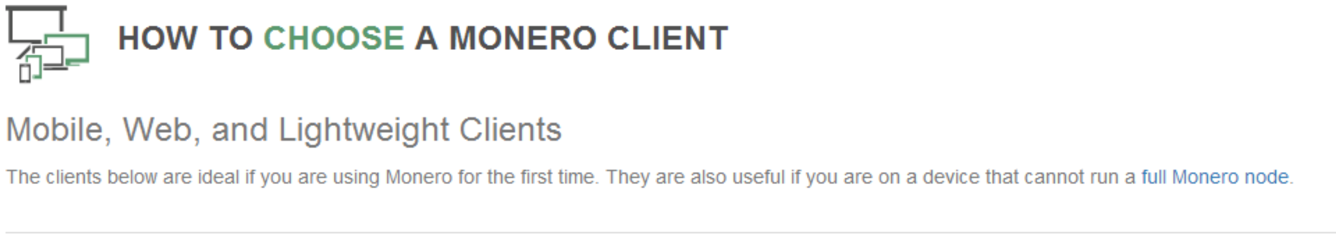
[Terms | Privacy | Copyright]

条款　　　隐私　　　版权

Section 2: Getting started—How to choose a Monero client.

https://getmonero.org/getting-started/choose

[Headers and footers can be found in Section 1: Homepage translation.]



HOW TO CHOOSE A MONERO CLIENT

Mobile, Web, and Lightweight Clients

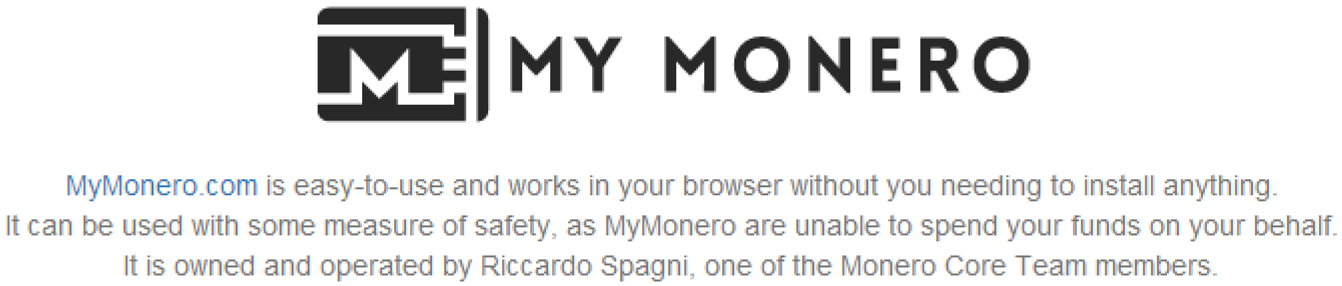
The clients below are ideal if you are using Monero for the first time. They are also useful if you are on a device that cannot run a full Monero node.

如何选择门罗币（Monero）客户端

手机版，网页版，和轻巧版客户端

如您是门罗币（Monero）的初次使用者，以下便介绍的客户端便是理想之选，同时适用于设备

性能有限，不能运行完整网络节点的用户

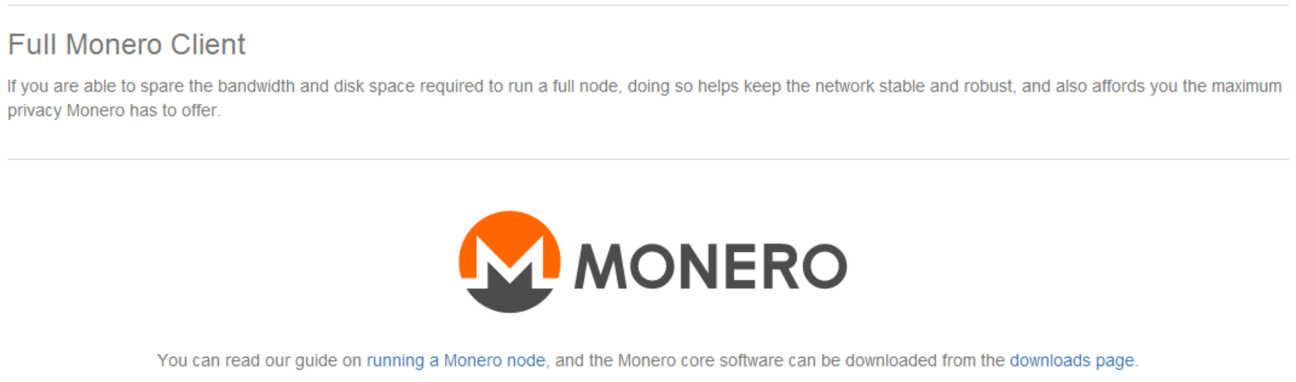


MyMonero.com is easy-to-use and works in your browser without you needing to install anything.
It can be used with some measure of safety, as MyMonero are unable to spend your funds on your behalf.
It is owned and operated by Riccardo Spagni, one of the Monero Core Team members.

MyMonero.com 使用方法简单，可直接在浏览器总打开，无需下载安装。

此网页无法代替您支配您的门罗币资金，因此安全度高。

网站由门罗币核心团队成员之一 Riccardo Spagni 负责操作运营。



Full Monero Client

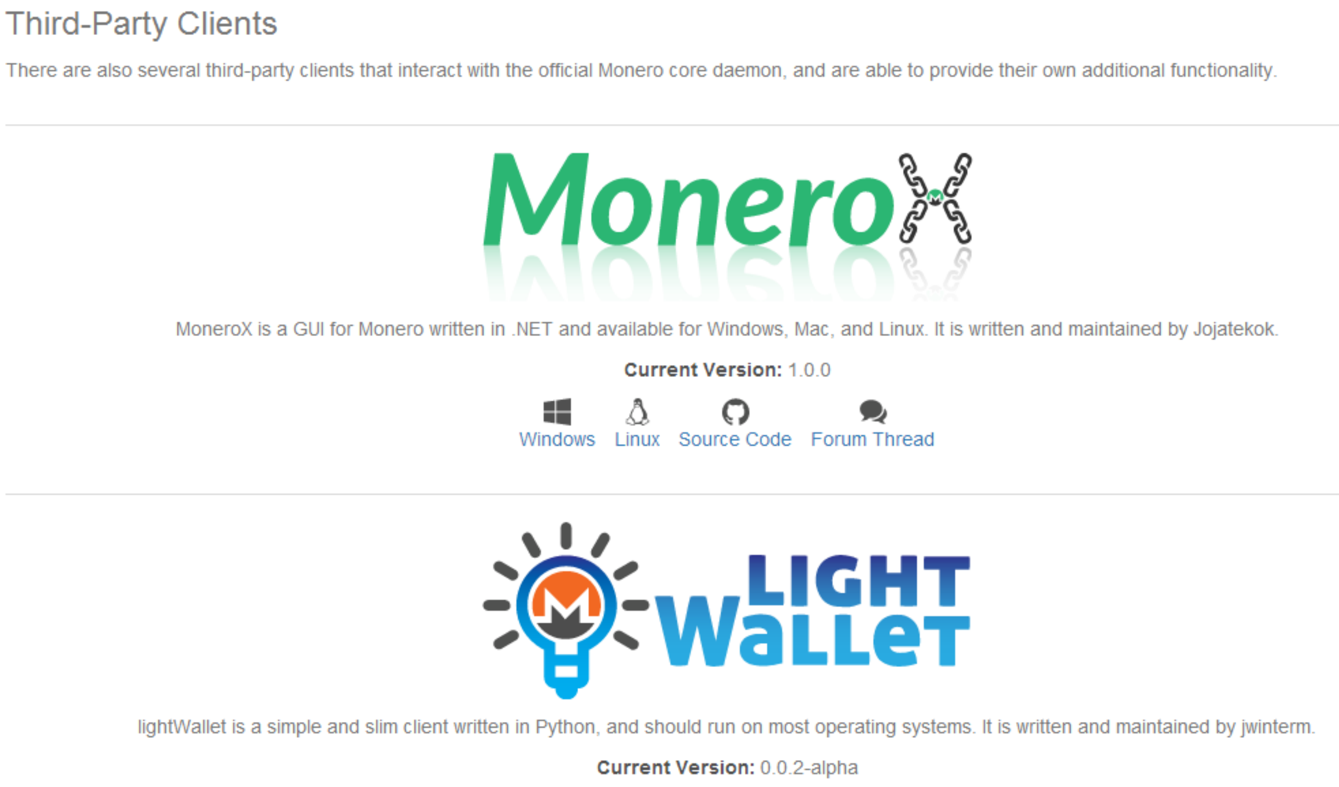
If you are able to spare the bandwidth and disk space required to run a full node, doing so helps keep the network stable and robust, and also affords you the maximum privacy Monero has to offer.

You can read our guide on running a Monero node, and the Monero core software can be downloaded from the downloads page.

完整门罗币客户端

如您可以扩展带宽及硬盘空间，并运行完整网络节点，您便可享受强大而稳定的网络，以及门罗币所提供的最高保密性。

请参考门罗币网络节点运行指南，也可以从下载页面下载安装门罗币核心软件。



Third-Party Clients

There are also several third-party clients that interact with the official Monero core daemon, and are able to provide their own additional functionality.

MoneroX is a GUI for Monero written in .NET and available for Windows, Mac, and Linux. It is written and maintained by Jojatekok.

Current Version: 1.0.0

lightWallet is a simple and slim client written in Python, and should run on most operating systems. It is written and maintained by jwinterm.

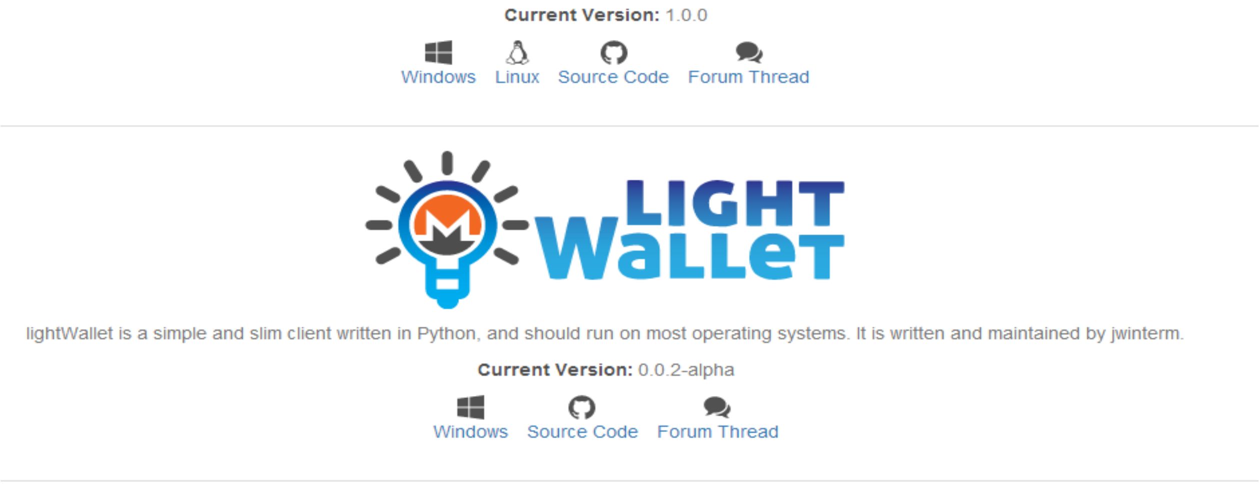
Current Version: 0.0.2-alpha

第三方客户端

其他与门罗币官方后台合作的第三方客户端会提供其他附加功能。

[Picture]

MoneroX 是.NET 版本的门罗币用户界面，此界面适用于 Windows,Mac 及 Linux.MoneroX 由 Jojatekok 编写并维护。



Current Version: 1.0.0

lightWallet is a simple and slim client written in Python, and should run on most operating systems. It is written and maintained by jwinterm.

Current Version: 0.0.2-alpha

最新版本：1.0.0

Windows Linux 源代码 论坛帖子

[Picture]

LightWallet 是一款轻便简单 Python 版的用户端。此用户端适用于多数操作系统。由 jwinterm 编写和维护。

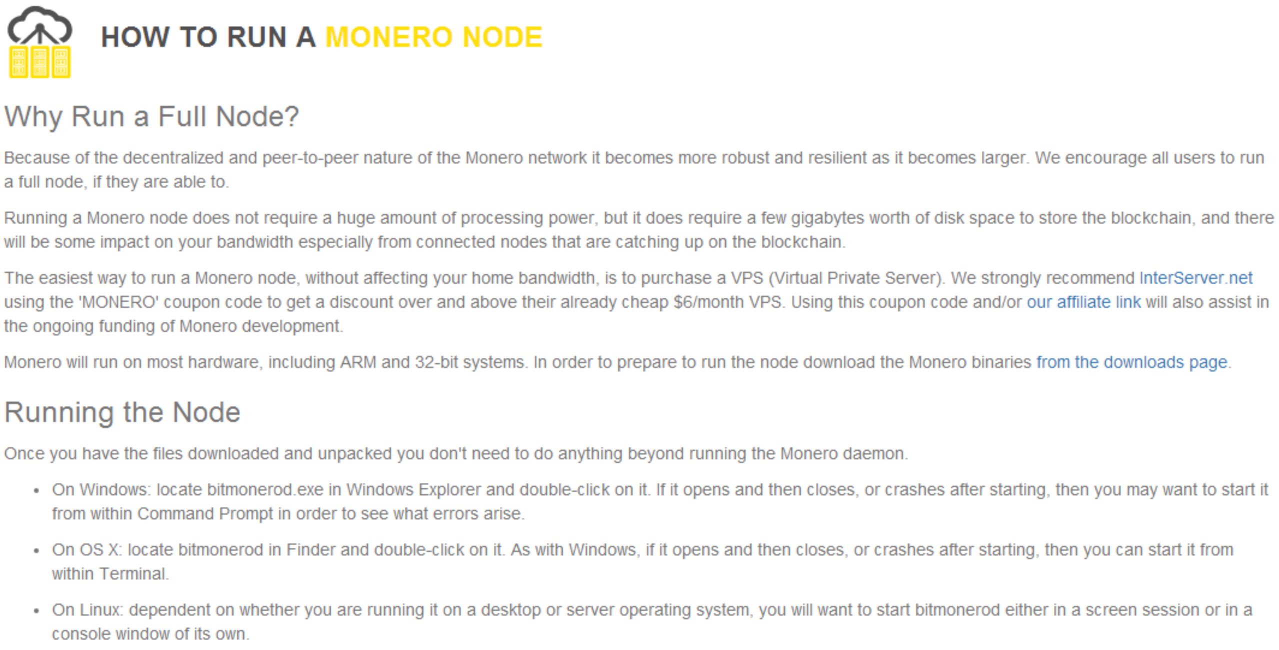
最新版本：0.0.2-alpha

Windows 源代码 论坛帖子

Section 3 Getting started—How to run a Monero node

https://getmonero.org/getting-started/running

[Headers and footers can be found in the translated main page.]



HOW TO RUN A MONERO NODE

Why Run a Full Node?

Because of the decentralized and peer-to-peer nature of the Monero network it becomes more robust and resilient as it becomes larger. We encourage all users to run a full node, if they are able to.

Running a Monero node does not require a huge amount of processing power, but it does require a few gigabytes worth of disk space to store the blockchain, and there will be some impact on your bandwidth especially from connected nodes that are catching up on the blockchain.

The easiest way to run a Monero node, without affecting your home bandwidth, is to purchase a VPS (Virtual Private Server). We strongly recommend InterServer.net using the 'MONERO' coupon code to get a discount over and above their already cheap $6/month VPS. Using this coupon code and/or our affiliate link will also assist in the ongoing funding of Monero development.

Monero will run on most hardware, including ARM and 32-bit systems. In order to prepare to run the node download the Monero binaries from the downloads page.

Running the Node

Once you have the files downloaded and unpacked you don't need to do anything beyond running the Monero daemon.

- On Windows: locate bitmonerod.exe in Windows Explorer and double-click on it. If it opens and then closes, or crashes after starting, then you may want to start it from within Command Prompt in order to see what errors arise.
- On OS X: locate bitmonerod in Finder and double-click on it. As with Windows, if it opens and then closes, or crashes after starting, then you can start it from within Terminal.
- On Linux: dependent on whether you are running it on a desktop or server operating system, you will want to start bitmonerod either in a screen session or in a console window of its own.

如何运行门罗币网络节点（Monero Node）

为什么要运转完整网络节点?

门罗币网络系统的分散性和对应性决定了它规模越大，功能越强大，灵活性也越高。我们鼓励所有有条件的用户使用完整网络节点。

运行门罗币网络节点并不需要强大的处理器，但您确实需要用几个 GB 的硬板空间来安置数据区块链，并且会对您的带宽有一定影响，特别是与数据区块链连接的网络节点。

运行门罗币网络节点，而不影响您家庭带宽最简单的方法，是购买 VPS（虚拟专用服务器）。我

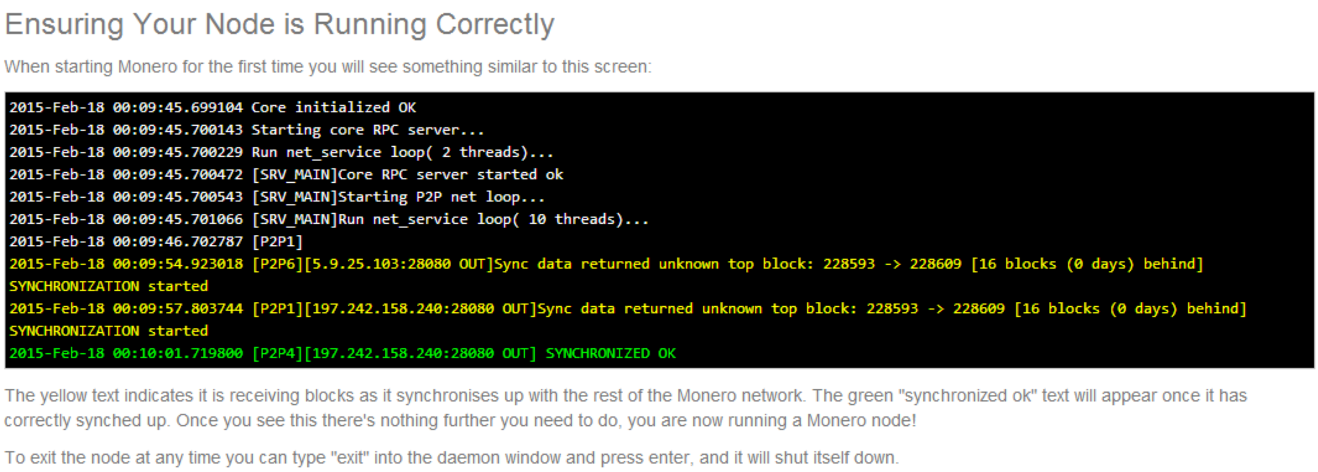
们强烈推荐 InterServer.net。使用“门罗币”优惠券代码可享受原价 $6/月基础上的折扣。使用此优惠券代码或友情链接也意味着您为门罗币的发展给予一臂之力。

门罗币可在多数硬件条件下运行，包括 ARM 及 32 位系统。运行网络节点之前，请在下载页面下载门罗币二进制文件。

运行网络节点

一旦文件下载及解压完成，您只需开始运行门罗币后台，无需任何其他操作。

- Windows 用户：在 Windows 资源管理器中找到 bitmonerod.exe 并双击。如程序开启后自动关闭或崩溃，您可以在命令提示符内启动，看是否依然出现同样问题。
- OS X 用户：在 Finder 中找到 bitmonerod 并双击。与 Windows 相同，如程序开启后自动关闭或崩溃，您可以尝试在 Terminal 中启动。
- Linux 用户：如您在桌面或服务器操作系统上运行它，与此对应您可在 Screen 作业中或其本身的控制台窗口启动 bitmonerod



Ensuring Your Node is Running Correctly

When starting Monero for the first time you will see something similar to this screen:

```
2015-Feb-18 00:09:45.699104 Core initialized OK
2015-Feb-18 00:09:45.700143 Starting core RPC server...
2015-Feb-18 00:09:45.700229 Run net_service loop( 2 threads)...
2015-Feb-18 00:09:45.700472 [SRV_MAIN]Core RPC server started ok
2015-Feb-18 00:09:45.700543 [SRV_MAIN]Starting P2P net loop...
2015-Feb-18 00:09:45.701066 [SRV_MAIN]Run net_service loop( 10 threads)...
2015-Feb-18 00:09:46.702787 [P2P1]
2015-Feb-18 00:09:54.923018 [P2P6][5.9.25.103:28080 OUT]Sync data returned unknown top block: 228593 -> 228609 [16 blocks (0 days) behind]
SYNCHRONIZATION started
2015-Feb-18 00:09:57.803744 [P2P1][197.242.158.240:28080 OUT]Sync data returned unknown top block: 228593 -> 228609 [16 blocks (0 days) behind]
SYNCHRONIZATION started
2015-Feb-18 00:10:01.719800 [P2P4][197.242.158.240:28080 OUT] SYNCHRONIZED OK
```

The yellow text indicates it is receiving blocks as it synchronises up with the rest of the Monero network. The green "synchronized ok" text will appear once it has correctly synched up. Once you see this there's nothing further you need to do, you are now running a Monero node!

To exit the node at any time you can type "exit" into the daemon window and press enter, and it will shut itself down.

确保您的节点运行正确

首次启动门罗网络节点时，你屏幕会显示如下图：

[The screenshot is not translated, since the program is not translated yet.]

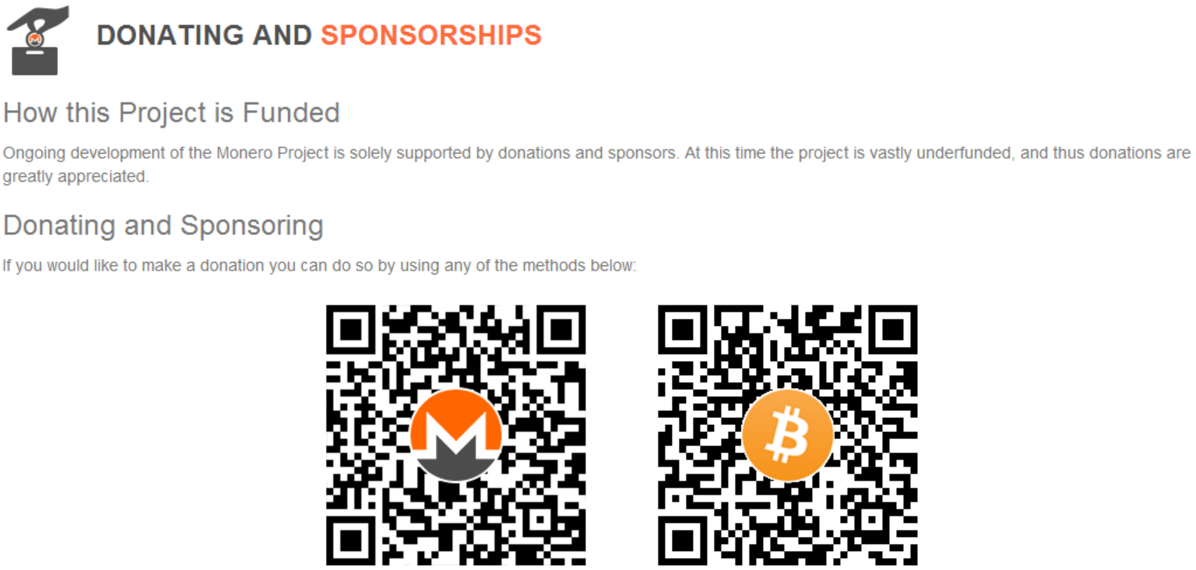
黄色文字表示在同步更新门罗网络的剩余部分同时，它也在接收的数据区块。一旦同步成功完成，屏幕会显示绿色的“synchronized OK”字样。至此，您的门罗网络节点顺利开始运行！

若要退出节点，您可在任何时候在后台键入“exit”，然后按回车键，程序便会自行关闭。

Section 4: Getting started—donating and sponsorships

https://getmonero.org/getting-started/donate/

[Headers and footers can be found in the translated main page.]



DONATING AND SPONSORSHIPS

How this Project is Funded

Ongoing development of the Monero Project is solely supported by donations and sponsors. At this time the project is vastly underfunded, and thus donations are greatly appreciated.

Donating and Sponsoring

If you would like to make a donation you can do so by using any of the methods below:

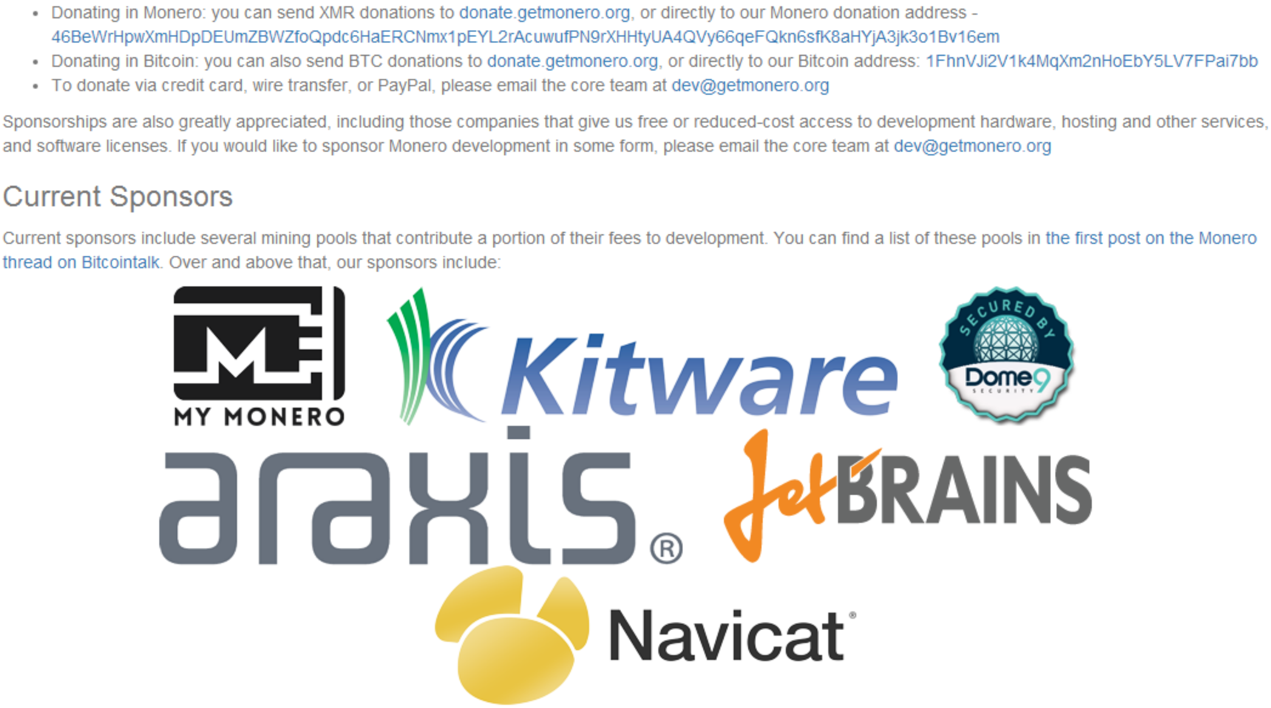
募捐及赞助

此项目是如何获得资助呢？

门罗币（Monero）项目的持续发展完全有赖于募捐和赞助商的支持。目前，该项目出于资金匮乏阶段，因此，门罗币团队将感激任何形式的捐赠。

捐赠和赞助

如果您愿意捐献一份力量，可以通过以下任何一种方式：



- Donating in Monero: you can send XMR donations to donate.getmonero.org, or directly to our Monero donation address - 46BeWrHpwXmHDpDEUmZBWZfoQpdc6HaERCNmx1pEYL2rAcuwufPN9rXHHtyUA4QVy66qeFQkn6sfK8aHYjA3jk3o1Bv16em
- Donating in Bitcoin: you can also send BTC donations to donate.getmonero.org, or directly to our Bitcoin address: 1FhnVJi2V1k4MqXm2nHoEbY5LV7FPai7bb
- To donate via credit card, wire transfer, or PayPal, please email the core team at dev@getmonero.org

Sponsorships are also greatly appreciated, including those companies that give us free or reduced-cost access to development hardware, hosting and other services, and software licenses. If you would like to sponsor Monero development in some form, please email the core team at dev@getmonero.org

Current Sponsors

Current sponsors include several mining pools that contribute a portion of their fees to development. You can find a list of these pools in the first post on the Monero thread on Bitcointalk. Over and above that, our sponsors include:

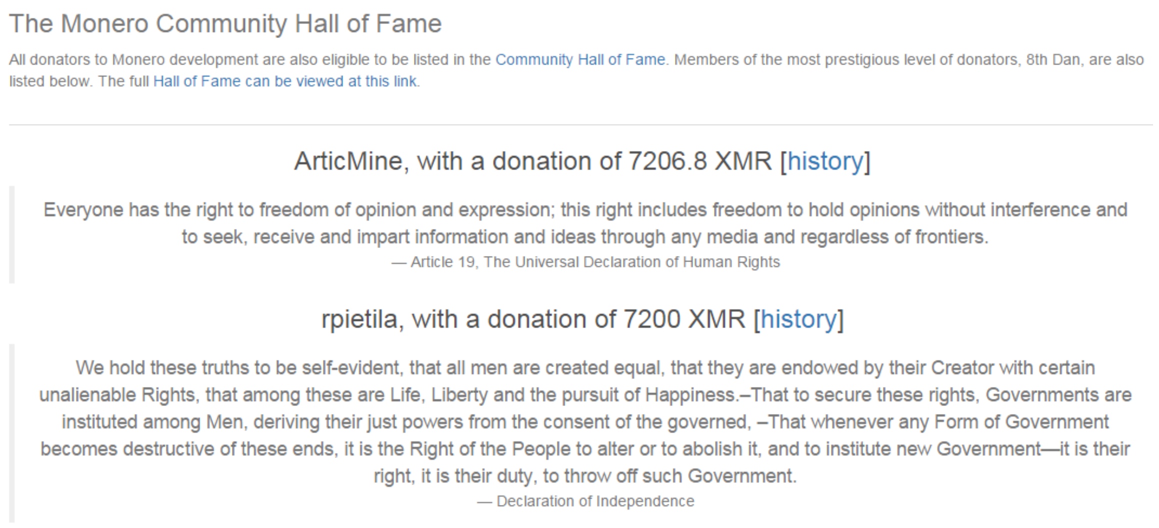
- 门罗币捐款：您可以向 donate.getmonero.org 捐赠 XMR，或直接向我们的门罗币地址捐款 46BeWrHpwXmHDpDEUmZBWZfoQpdc6HaERCNmx1pEYL2rAcuwufPN9rXHHtyUA4QVy66qeFQkn6sfK8aHYjA3jk3o1Bv16em；
- 比特币捐款：您可以想 donate.getmonero.org 捐赠 BTC，或直接向我们的比特币地址捐款 1FhnVJi2V1k4MqXm2nHoEbY5LV7FPai7bb；
- 信用卡，电汇，或支付宝捐款，请直接致邮件给核心团队 dev@getmonero.org ‘

同时，我们也非常感谢赞助商，包括向我们提供免费或折扣的开发硬件，网页寄存等服务，以及软件许可证。如您愿意以任何方式赞助门罗币的开发，请您致邮件给核心团队 dev@getmonero.org。

当前赞助商

目前有部分矿池向门罗币提供免费服务。矿池赞助商详细列表请 Bitcointalk 的 Monero 线程的

第一篇帖子。除此之外，我们的赞助商也包括：



The Monero Community Hall of Fame

All donators to Monero development are also eligible to be listed in the Community Hall of Fame. Members of the most prestigious level of donators, 8th Dan, are also listed below. The full Hall of Fame can be viewed at this link.

ArticMine, with a donation of 7206.8 XMR [history]

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
> — Article 19, The Universal Declaration of Human Rights

rpietila, with a donation of 7200 XMR [history]

> We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.–That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, –That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government—it is their right, it is their duty, to throw off such Government.
> — Declaration of Independence

门罗币社区之名人堂

所有捐赠者的名字会荣登社区名人堂。最富盛名的捐赠者 8th Dan 也在此列。查看完整的名人堂请点击此处。

ArticMine,捐款 7206.8 门罗币[历史]

每个人都有思想及言论自由，这项权利包括坚持自己的观点而不受外界干涉的自由，以及通过各种媒体，自由地追求，接受，传递信息与观点的权利。

--世界人权宣言 第 19 条

Rpietila，捐款 7200 门罗币[历史]

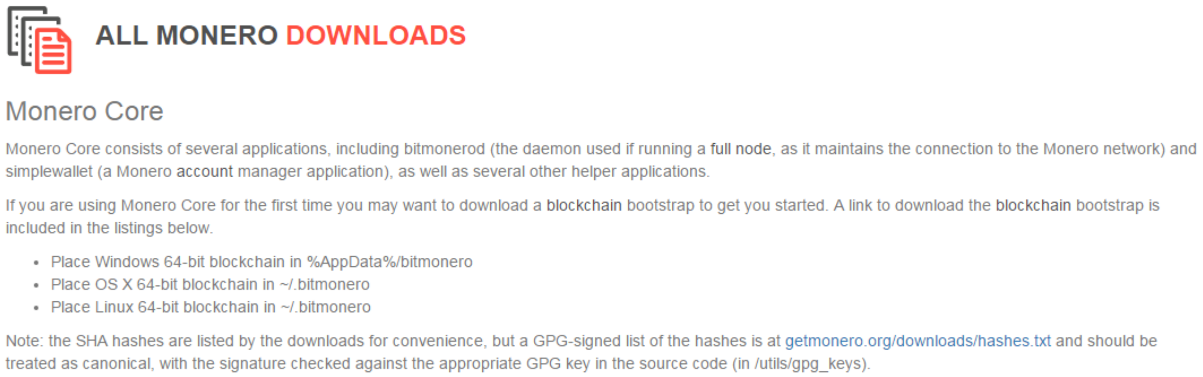
我们认为以下真理是不言而喻的：众生平等，造物主赋予他们某些不可剥夺的权利，其中包括生存，自由和追求幸福的权利。为了保障这些权利，人民建立了政府来制约和管理人民， - 因此，人民也有权改造或废除任何违背此初衷的政府，以建立一个新政府，这是人民的权利和义务。

--独立宣言

Section 5 Getting started—All monero downloads

https://getmonero.org/downloads/

[Headers and footers can be found in the translated main page.]



ALL MONERO DOWNLOADS

Monero Core

Monero Core consists of several applications, including bitmonerod (the daemon used if running a **full node**, as it maintains the connection to the Monero network) and simplewallet (a Monero **account** manager application), as well as several other helper applications.

If you are using Monero Core for the first time you may want to download a **blockchain** bootstrap to get you started. A link to download the **blockchain** bootstrap is included in the listings below.

- Place Windows 64-bit blockchain in %AppData%/bitmonero
- Place OS X 64-bit blockchain in ~/.bitmonero
- Place Linux 64-bit blockchain in ~/.bitmonero

Note: the SHA hashes are listed by the downloads for convenience, but a GPG-signed list of the hashes is at getmonero.org/downloads/hashes.txt and should be treated as canonical, with the signature checked against the appropriate GPG key in the source code (in /utils/gpg_keys).

门罗币下载大全

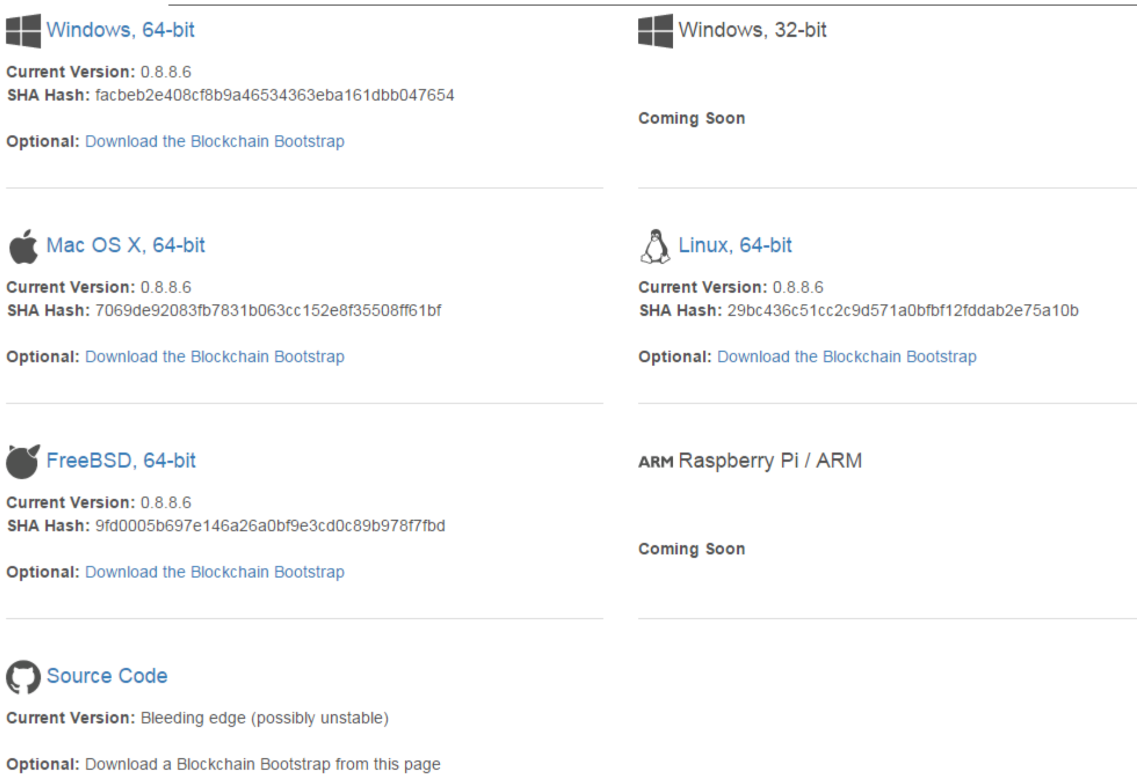
门罗币（Monero）核心由多个应用程序组成，包括 bitmonerod（如运行完整的网络结点，则需此后台程序进行与门罗币网络连接），和 simplewallet（门罗币帐户管理程序），以及若干其它辅助应用程序。

如果您是初次使用门罗币核心，你可以下载一个**数据区块**引导让你开始。**数据区块**引导下载链接请见以下列表。

- 将 Windows 64 位数据区块置于%APPDATA%/ bitmonero
- 将 OS X 64 位数据区块置于～/.bitmonero
- 将 Linux 64 位数据区块置于～/.bitmonero

注：SHA 散列也在列表中，以方便下载， GPG 认证的散列名单可在一下链接找到 getmonero.org/downloads/hashes.txt，此列表已与源代码（/ utils 的/ gpg_keys）中对应的

GPG 密钥核对，可作为规范。



Windows, 64-bit

Current Version: 0.8.8.6
SHA Hash: facbeb2e408cf8b9a46534363eba161dbb047654

Optional: Download the Blockchain Bootstrap

Windows, 32-bit

Coming Soon

Mac OS X, 64-bit

Current Version: 0.8.8.6
SHA Hash: 7069de92083fb7831b063cc152e8f35508ff61bf

Optional: Download the Blockchain Bootstrap

Linux, 64-bit

Current Version: 0.8.8.6
SHA Hash: 29bc436c51cc2c9d571a0bfbf12fddab2e75a10b

Optional: Download the Blockchain Bootstrap

FreeBSD, 64-bit

Current Version: 0.8.8.6
SHA Hash: 9fd0005b697e146a26a0bf9e3cd0c89b978f7fbd

Optional: Download the Blockchain Bootstrap

ARM Raspberry Pi / ARM

Coming Soon

Source Code

Current Version: Bleeding edge (possibly unstable)

Optional: Download a Blockchain Bootstrap from this page

Windows，64 位

当前版本：0.8.8.6

SHA 散列：facbeb2e408cf8b9a46534363eba161dbb047654

可选：下载数据区块引导

Windows, 32 位

即将推出

Mac OS X, 64 位

当前版本：0.8.8.6

SHA 散列：7069de92083fb7831b063cc152e8f35508ff61bf

可选：下载数据区块引导

Linux，64 位

当前版本：0.8.8.6

SHA 散列： 29bc436c51cc2c9d571a0bfbf12fddab2e75a10b

可选：下载数据区块引导

FreeBSD, 64 位

当前版本：0.8.8.6

SHA 散列：9fd0005b697e146a26a0bf9e3cd0c89b978f7fbd

可选：下载数据区块引导

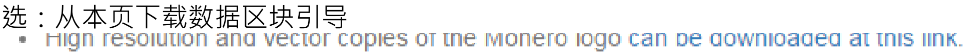
ARM Raspberry Pi/ARM

即将推出

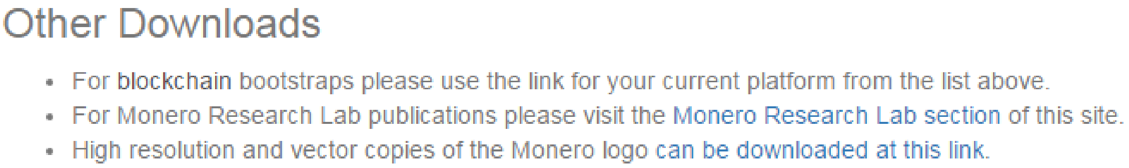
源代码

当前版本：Bleeding Edge （具有不稳定性）

可选：从本页下载数据区块引导



- High resolution and vector copies of the Monero logo can be downloaded at this link.



Other Downloads

- For blockchain bootstraps please use the link for your current platform from the list above.
- For Monero Research Lab publications please visit the Monero Research Lab section of this site.
- High resolution and vector copies of the Monero logo can be downloaded at this link.

其他下载资料

■ 下载数据区块连请参照上表。

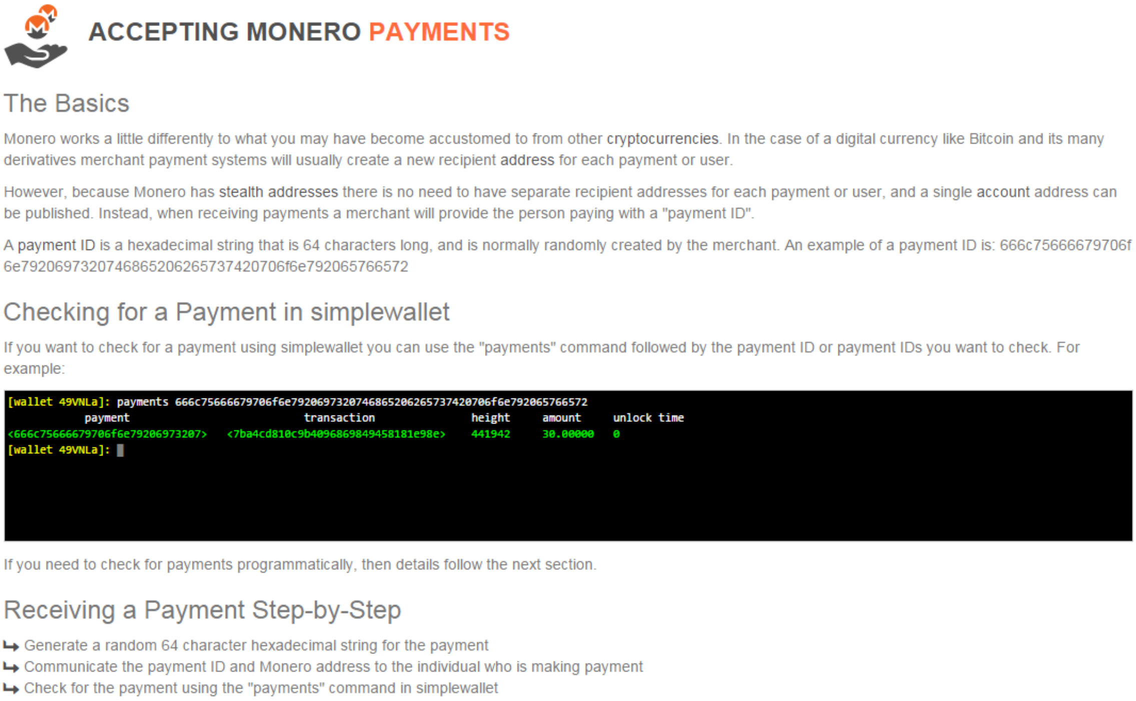
■ 查看门罗币研究室出版物，请您点击门罗币研究室区。

■ 高清版门罗币标志图请点此下载。

Section 6 Getting started—Accepting Monero Payments

https://getmonero.org/getting-started/accepting

[Headers and footers can be found in the translated main page.]



ACCEPTING MONERO PAYMENTS

The Basics

Monero works a little differently to what you may have become accustomed to from other cryptocurrencies. In the case of a digital currency like Bitcoin and its many derivatives merchant payment systems will usually create a new recipient address for each payment or user.

However, because Monero has stealth addresses there is no need to have separate recipient addresses for each payment or user, and a single account address can be published. Instead, when receiving payments a merchant will provide the person paying with a "payment ID".

A payment ID is a hexadecimal string that is 64 characters long, and is normally randomly created by the merchant. An example of a payment ID is: 666c75666679706f6e7920697320746865206265737420706f6e792065766572

Checking for a Payment in simplewallet

If you want to check for a payment using simplewallet you can use the "payments" command followed by the payment ID or payment IDs you want to check. For example:

```
[wallet 49VNLa]: payments 666c75666679706f6e7920697320746865206265737420706f6e792065766572
           payment                             transaction                height     amount     unlock time
<666c75666679706f6e79206973207>   <7ba4cd810c9b4096869849458181e98e>    441942     30.00000   0
[wallet 49VNLa]: 
```

If you need to check for payments programmatically, then details follow the next section.

Receiving a Payment Step-by-Step

↳ Generate a random 64 character hexadecimal string for the payment
↳ Communicate the payment ID and Monero address to the individual who is making payment
↳ Check for the payment using the "payments" command in simplewallet

接受门罗币（Monero）付款

基础

门罗币与您之前接触的加密货币略有不同。其他电子货币，如比特币及其多种衍生物，会为每笔交易或每个接收人创建一个新的地址。

然而门罗币的隐形地址免去了区分每笔交易的接受地址的麻烦，您只需将一个账户地址公开。取而代之的是，商家在接受付款时，为付款人提供一个“付款编号”。

“付款编号”为 64 个字符长的十六进制字符串，通常是由商机随机设置，例如：

666c75666679706f6e79206973207468652062657374206f6e792065766572

使用 simplewallet 查看交易记录

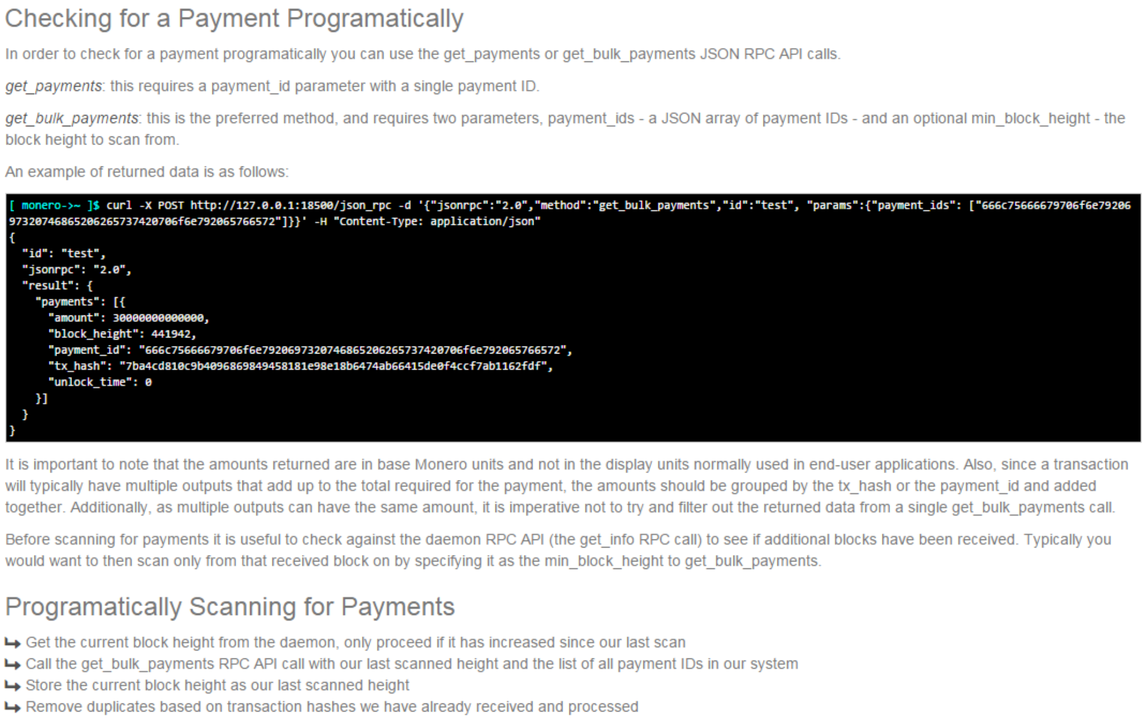
如使用 simplewallet 查看您交易记录，您可以使用“支付”命令查询对应的一个或多个付款编号。如下图：

[Screenshot]

如使用编程查看您的交易记录，请见本页后半部分。

收款步骤：

- 随机生成一个十六进制 64 个字符的字符串，以便付款使用；
- 与付款方交换付款编号和门罗币接受地址；
- 使用 simplewallet 的“付款”命令检查交易记录。



Checking for a Payment Programatically

In order to check for a payment programatically you can use the get_payments or get_bulk_payments JSON RPC API calls.

get_payments: this requires a payment_id parameter with a single payment ID.

get_bulk_payments: this is the preferred method, and requires two parameters, payment_ids - a JSON array of payment IDs - and an optional min_block_height - the block height to scan from.

An example of returned data is as follows:

```
[ monero->~ ]$ curl -X POST http://127.0.0.1:18500/json_rpc -d '{"jsonrpc":"2.0","method":"get_bulk_payments","id":"test", "params":{"payment_ids": ["666c75666679706f6e79206
973207468652062657374206f6e792065766572"]}}' -H "Content-Type: application/json"
{
  "id": "test",
  "jsonrpc": "2.0",
  "result": {
    "payments": [{
      "amount": 30000000000000,
      "block_height": 441942,
      "payment_id": "666c75666679706f6e79206973207468652062657374206f6e792065766572",
      "tx_hash": "7ba4cd810c9b4096869849458181e98e18b6474ab66415de0f4ccf7ab1162fdf",
      "unlock_time": 0
    }]
  }
}
```

It is important to note that the amounts returned are in base Monero units and not in the display units normally used in end-user applications. Also, since a transaction will typically have multiple outputs that add up to the total required for the payment, the amounts should be grouped by the tx_hash or the payment_id and added together. Additionally, as multiple outputs can have the same amount, it is imperative not to try and filter out the returned data from a single get_bulk_payments call.

Before scanning for payments it is useful to check against the daemon RPC API (the get_info RPC call) to see if additional blocks have been received. Typically you would want to then scan only from that received block on by specifying it as the min_block_height to get_bulk_payments.

Programatically Scanning for Payments

↳ Get the current block height from the daemon, only proceed if it has increased since our last scan
↳ Call the get_bulk_payments RPC API call with our last scanned height and the list of all payment IDs in our system
↳ Store the current block height as our last scanned height
↳ Remove duplicates based on transaction hashes we have already received and processed

使用编程查看交易记录

您可使用 get_payments 或 get_bulk_payments JSON RPC API 命令查看交易。

get_payments：需要一个 payment_id 参数，即付款编号。

get_bulk_payments（推荐选项）: 需要两个 payment_ids 参数，包括一个 JSON 数组的付款编号，和可选 min_block_height，从而以便进行扫描。

反馈数据如下图：

[Screenshot]

非常重要的一点是：反馈的金额是以门罗币为单位，而非以客户终端显示的单位为准。由于一笔交易的总金额往往会由多个输出数字的总和组成，因此，这些量应按照 tx_hash 或 payment_id 分组相加。此外，由于相同的总金额可以由不同输出量组成，应此要注意避免从单个 get_bulk_payments 滤出反馈数据。

扫描，它是非常有用的检查与守护 RPC API（中的 get_info RPC 调用），看看是否还有其他区块已收到。

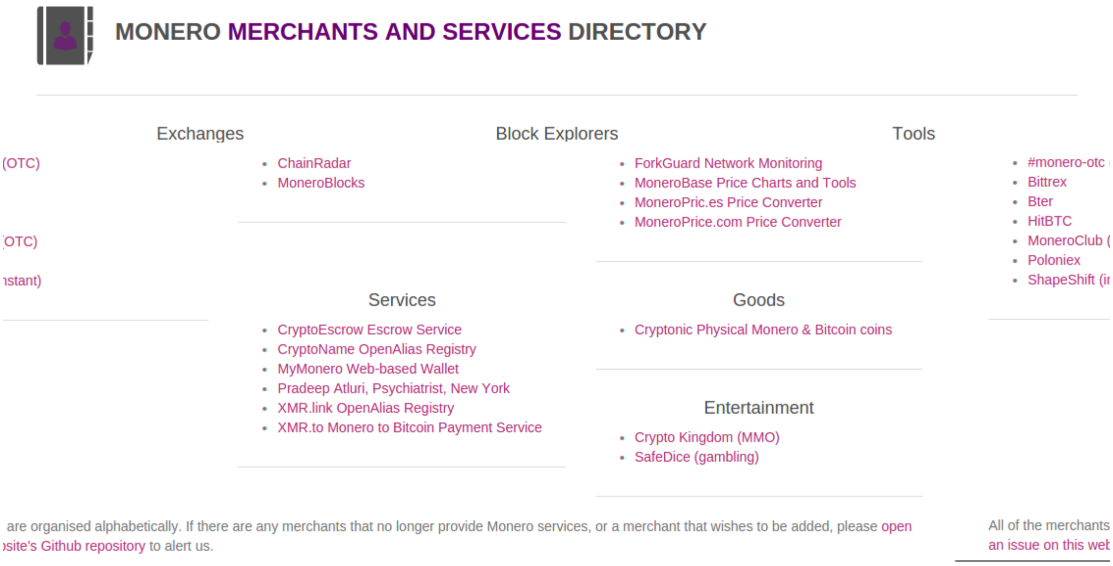
编程扫描付款

- 从后台获得当前区块的高度，确保此数值比上一次扫描增加后，再继续此程序；
- 使用最近一次扫描高度以及系统中所有付款编号列表运行 get_bulk_payments RPC API；命令；
- 存储当前块的高度；
- 删除已经接受并处理过的重复交易散列。

Section 7 Getting started--Merchants and services directory

https://getmonero.org/getting-started/merchants

[Headers and footers can be found in the translated main page.]



MONERO MERCHANTS AND SERVICES DIRECTORY

Exchanges

(OTC)

OTC)

ıstant)

- #monero-otc
- Bittrex
- Bter
- HitBTC
- MoneroClub (
- Poloniex
- ShapeShift (ir

Block Explorers

- ChainRadar
- MoneroBlocks

Tools

- ForkGuard Network Monitoring
- MoneroBase Price Charts and Tools
- MoneroPric.es Price Converter
- MoneroPrice.com Price Converter

Services

- CryptoEscrow Escrow Service
- CryptoName OpenAlias Registry
- MyMonero Web-based Wallet
- Pradeep Atluri, Psychiatrist, New York
- XMR.link OpenAlias Registry
- XMR.to Monero to Bitcoin Payment Service

Goods

- Cryptonic Physical Monero & Bitcoin coins

Entertainment

- Crypto Kingdom (MMO)
- SafeDice (gambling)

All of the merchants are organised alphabetically. If there are any merchants that no longer provide Monero services, or a merchant that wishes to be added, please open an issue on this website's Github repository to alert us.

门罗币（Monero）商家及服务目录

交易 区块浏览 工具

[links] [links] [links]

服务 商品

[links] [links]

娱乐

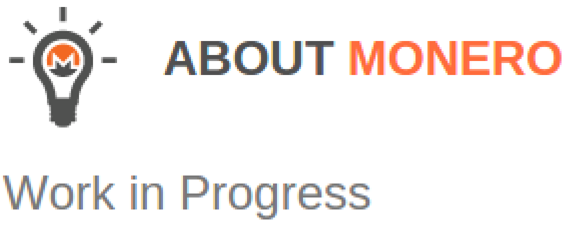
[links]

所有的商家按字母顺序排列。如果有任何商家不再提供门罗币服务或有意加盟，请在本网站资料库的 Github 上开始一个问题来提醒我们。

Section 8 Knowledge base--About Monero

https://getmonero.org/knowledge-base/about

[Headers and footers can be found in the translated main page.]



ABOUT MONERO

Work in Progress

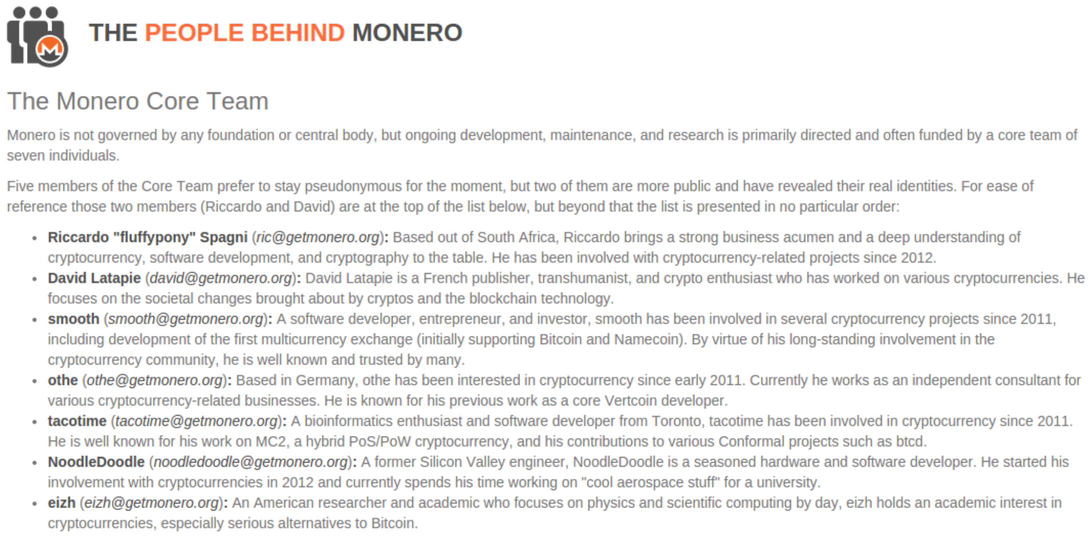
关于门罗币（Monero）

逐步完善中

Section 9 Knowledge base--The people behind Monero

https://getmonero.org/knowledge-base/people

[Headers and footers can be found in the translated main page.]



THE PEOPLE BEHIND MONERO

The Monero Core Team

Monero is not governed by any foundation or central body, but ongoing development, maintenance, and research is primarily directed and often funded by a core team of seven individuals.

Five members of the Core Team prefer to stay pseudonymous for the moment, but two of them are more public and have revealed their real identities. For ease of reference those two members (Riccardo and David) are at the top of the list below, but beyond that the list is presented in no particular order:

- **Riccardo "fluffypony" Spagni** (*ric@getmonero.org*)**:** Based out of South Africa, Riccardo brings a strong business acumen and a deep understanding of cryptocurrency, software development, and cryptography to the table. He has been involved with cryptocurrency-related projects since 2012.
- **David Latapie** (*david@getmonero.org*)**:** David Latapie is a French publisher, transhumanist, and crypto enthusiast who has worked on various cryptocurrencies. He focuses on the societal changes brought about by cryptos and the blockchain technology.
- **smooth** (*smooth@getmonero.org*)**:** A software developer, entrepreneur, and investor, smooth has been involved in several cryptocurrency projects since 2011, including development of the first multicurrency exchange (initially supporting Bitcoin and Namecoin). By virtue of his long-standing involvement in the cryptocurrency community, he is well known and trusted by many.
- **othe** (*othe@getmonero.org*)**:** Based in Germany, othe has been interested in cryptocurrency since early 2011. Currently he works as an independent consultant for various cryptocurrency-related businesses. He is known for his previous work as a core Vertcoin developer.
- **tacotime** (*tacotime@getmonero.org*)**:** A bioinformatics enthusiast and software developer from Toronto, tacotime has been involved in cryptocurrency since 2011. He is well known for his work on MC2, a hybrid PoS/PoW cryptocurrency, and his contributions to various Conformal projects such as btcd.
- **NoodleDoodle** (*noodledoodle@getmonero.org*)**:** A former Silicon Valley engineer, NoodleDoodle is a seasoned hardware and software developer. He started his involvement with cryptocurrencies in 2012 and currently spends his time working on "cool aerospace stuff" for a university.
- **eizh** (*eizh@getmonero.org*)**:** An American researcher and academic who focuses on physics and scientific computing by day, eizh holds an academic interest in cryptocurrencies, especially serious alternatives to Bitcoin.

门罗币（Monero）幕后团队

门罗币不受任何基金会或中央机构的控制，而是由七人核心成员带领的团队，不断研发及维护，七位核心成员同时也向本项目提供资金支持。

核心团队中的五名成员目前会使用昵称，但另外两位都公布了自己的真实身份。以下列表中将这两位（Riccardo 和 David）的名字至于顶部，以便参考。除此之外，该列表并无特定顺序：

- **Riccardo “fluffypony” Spagni**（ric@getmonero.org）: 现居南非，Riccardo 极具商业头脑，并对加密货币见解独到，善于软件及及加密货币的开发。 2012 年以来，他一直致力于与加密货币相关的项目。

- **David Latapie**（david@getmonero.org）: David Latapie 是一位法国出版商，超人类主义者。参与过多个加密货币开发项目的他，同时也对密码极具热忱，关注密码和区块链技术对社会的影响。

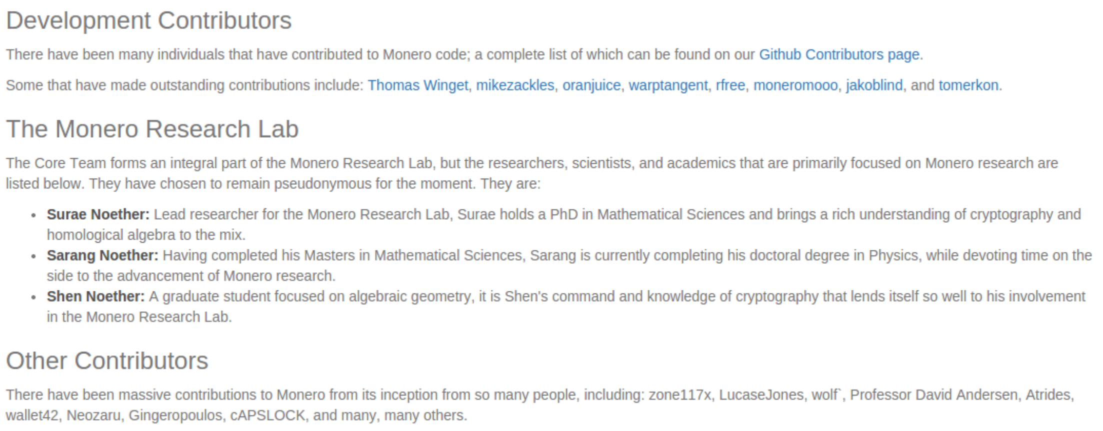
- **smooth**（smooth@getmonero.org）：软件开发者，企业家和投资家，2011 年以来 smooth 参与了多个加密货币项，其中包括最早期的多币种交易（比特币 Bitcoin 和域名币 Namecoin 的首要支持技术）。因其长期活跃于加密货币领域而众所周知，备受信赖。

- **othe**（othe@getmonero.org）：现居德国，自 2011 年年初，othe 就对加密货币产生了极大兴趣，目前为多种加密货币相关项目做独立顾问。作为前绿币（Vertcoin）开发商而闻名。

- **tacotime**（tacotime@getmonero.org）：来自多伦多的生物信息学爱好者，软件开发商，自 2011 年起，tacotime 便开始从事加密货币行业，因对 MC2，PoS /PoW 混合加密货币，Conformal 公司项目（如，btcd）作出的贡献而著名。

- **NoodleDoodle**（noodledoodle@getmonero.org）：前硅谷工程师。NoodleDoodle 是一位资深的硬件和软件开发员。于 2012 年开始涉入加密货币领域，目前致力于一所大学的“cool aerospace stuff”项目。

- **eizh**（eizh@getmonero.org）：美国研究者与学者，致力于物理和科学计算，eizh 对加密货币的学术意义有浓厚的兴趣，尤其侧重于比特币的替代品。



Development Contributors

There have been many individuals that have contributed to Monero code; a complete list of which can be found on our Github Contributors page.

Some that have made outstanding contributions include: Thomas Winget, mikezackles, oranjuice, warptangent, rfree, moneromooo, jakoblind, and tomerkon.

The Monero Research Lab

The Core Team forms an integral part of the Monero Research Lab, but the researchers, scientists, and academics that are primarily focused on Monero research are listed below. They have chosen to remain pseudonymous for the moment. They are:

- **Surae Noether:** Lead researcher for the Monero Research Lab, Surae holds a PhD in Mathematical Sciences and brings a rich understanding of cryptography and homological algebra to the mix.
- **Sarang Noether:** Having completed his Masters in Mathematical Sciences, Sarang is currently completing his doctoral degree in Physics, while devoting time on the side to the advancement of Monero research.
- **Shen Noether:** A graduate student focused on algebraic geometry, it is Shen's command and knowledge of cryptography that lends itself so well to his involvement in the Monero Research Lab.

Other Contributors

There have been massive contributions to Monero from its inception from so many people, including: zone117x, LucaseJones, wolf`, Professor David Andersen, Atrides, wallet42, Neozaru, Gingeropoulos, cAPSLOCK, and many, many others.

开发者

多为开发者曾为门罗币代码的编写作出了贡献；完整名单请见本网站 Github 贡献者页面。

突出贡献者包括：Thomas Winget, mikezackles, oranjuice, warptangent, rfree, moneromooo, jakoblind, and tomerkon.

门罗币研究室

门罗币核心团队固然是研究室的一个重要组成部分，但主要致力于门罗币研发的研究者，科学家以及学者目前希望以昵称的方式出现在以下列表中：

- Surae Noether：门罗币研究室的首席研究员，持有数学科学博士学位，并将对加密技术的丰富理解和同调代数的融会贯通。
- Sarang Noether：完成数学学士学位的 Sarang，目前正在修物理学博士学位，利用业余时间研究门罗币。
- Shen Noether：主修代数几何的博士生，Shen 对于密码学的全面理解使他成为门罗币研究室重要的组成部分。

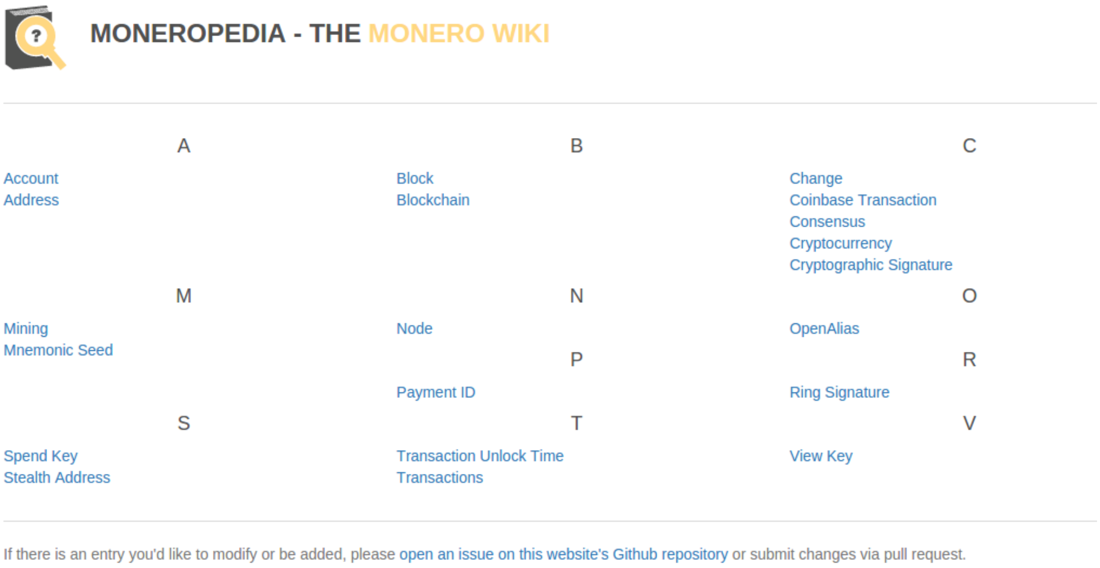
其他贡献者

门罗币自初始阶段以来有大量的贡献者参与其中，其中包括：zone117x, LucaseJones, wolf`, Professor David Andersen, Atrides, wallet42, Neozaru, Gingeropoulos, cAPSLOCK, 等诸多参与者。

Section 10 Knowledge base--Moneropedia

https://getmonero.org/knowledge-base/moneropedia/

[Headers and footers can be found in the translated main page.]



MONEROPEDIA - THE MONERO WIKI

A

Account
Address

B

Block
Blockchain

C

Change
Coinbase Transaction
Consensus
Cryptocurrency
Cryptographic Signature

M

Mining
Mnemonic Seed

N

Node

O

OpenAlias

P

Payment ID

R

Ring Signature

S

Spend Key
Stealth Address

T

Transaction Unlock Time
Transactions

V

View Key

If there is an entry you'd like to modify or be added, please open an issue on this website's Github repository or submit changes via pull request.

门罗百科

A	B	C
账户	区块	找零
地址	区块链	Coinbase 交易
		共识
M	N	加密货币

挖掘

助记种子

S

消费密钥

隐形地址

网络结点

P

付款编号

T

交易解锁时间

交易

加密签名

O

公开别名

R

群签名

V

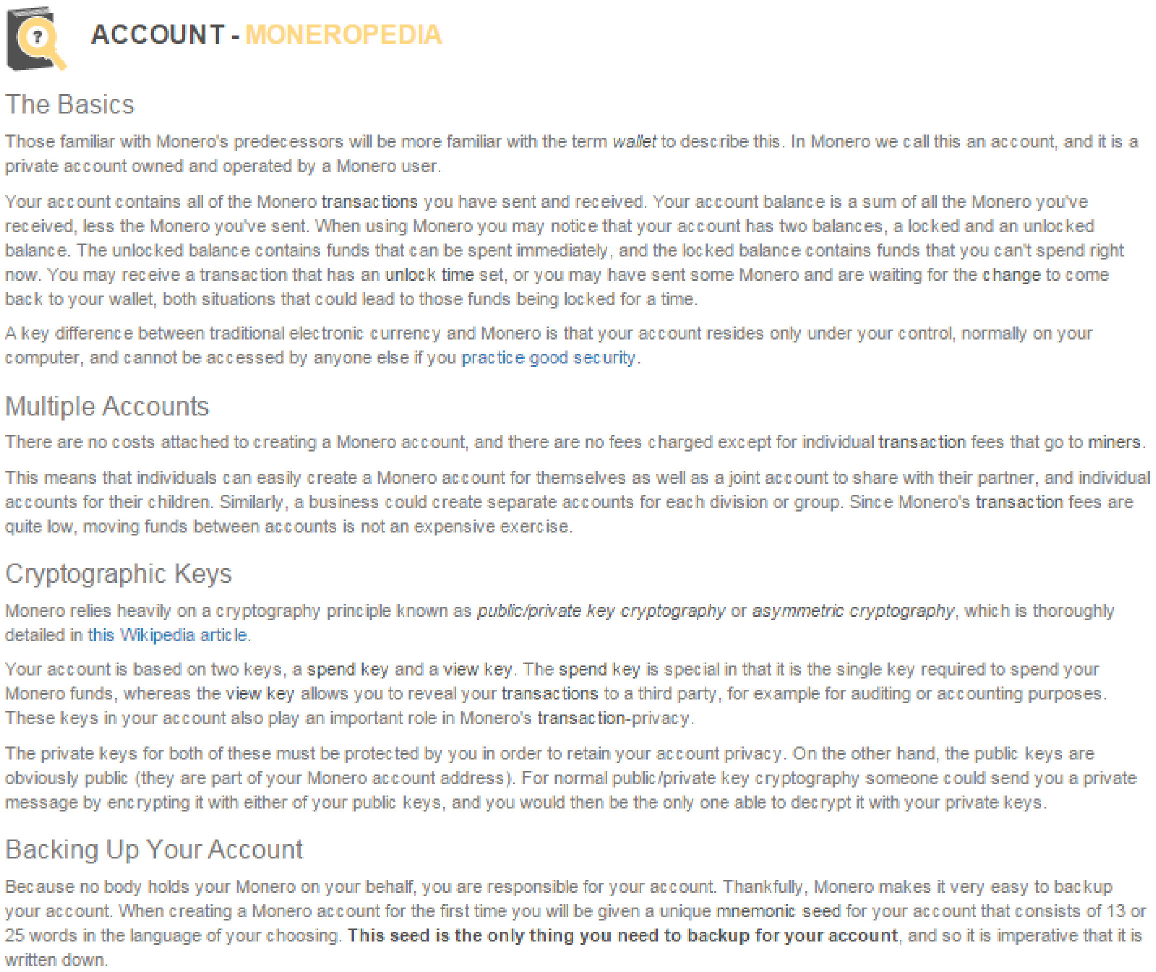
浏览密钥

如需添加或修改条目，请在本网站的资料库 Github 上打开一个问题，或者通过申请修改本页。

Section 10.1 Knowledge base—Moneropedia—Account

https://getmonero.org/knowledge-base/moneropedia/account

[Headers and footers can be found in the translated main page.]



ACCOUNT - MONEROPEDIA

The Basics

Those familiar with Monero's predecessors will be more familiar with the term *wallet* to describe this. In Monero we call this an account, and it is a private account owned and operated by a Monero user.

Your account contains all of the Monero **transactions** you have sent and received. Your account balance is a sum of all the Monero you've received, less the Monero you've sent. When using Monero you may notice that your account has two balances, a locked and an unlocked balance. The unlocked balance contains funds that can be spent immediately, and the locked balance contains funds that you can't spend right now. You may receive a transaction that has an **unlock time** set, or you may have sent some Monero and are waiting for the **change** to come back to your wallet, both situations that could lead to those funds being locked for a time.

A key difference between traditional electronic currency and Monero is that your account resides only under your control, normally on your computer, and cannot be accessed by anyone else if you practice good security.

Multiple Accounts

There are no costs attached to creating a Monero account, and there are no fees charged except for individual **transaction** fees that go to **miners**.

This means that individuals can easily create a Monero account for themselves as well as a joint account to share with their partner, and individual accounts for their children. Similarly, a business could create separate accounts for each division or group. Since Monero's **transaction** fees are quite low, moving funds between accounts is not an expensive exercise.

Cryptographic Keys

Monero relies heavily on a cryptography principle known as *public/private key cryptography* or *asymmetric cryptography*, which is thoroughly detailed in this Wikipedia article.

Your account is based on two keys, a **spend key** and a **view key**. The **spend key** is special in that it is the single key required to spend your Monero funds, whereas the **view key** allows you to reveal your **transactions** to a third party, for example for auditing or accounting purposes. These keys in your account also play an important role in Monero's **transaction-privacy**.

The private keys for both of these must be protected by you in order to retain your account privacy. On the other hand, the public keys are obviously public (they are part of your Monero account address). For normal public/private key cryptography someone could send you a private message by encrypting it with either of your public keys, and you would then be the only one able to decrypt it with your private keys.

Backing Up Your Account

Because no body holds your Monero on your behalf, you are responsible for your account. Thankfully, Monero makes it very easy to backup your account. When creating a Monero account for the first time you will be given a unique **mnemonic seed** for your account that consists of 13 or 25 words in the language of your choosing. **This seed is the only thing you need to backup for your account**, and so it is imperative that it is written down.

账户—门罗百科

基础

熟悉早期电子货币的用户会更加习惯用“钱包”命名此词条。在门罗币中，我们称其为帐户，门罗币具有高度隐私性，只有用户本人才可以管理帐户。

门罗币账户中会包含您所有的买卖交易，帐户余额则显示了您的门罗币收支差额。打开门罗币账户，您会注意到其中有两个分账户，锁定余额账户和非锁定余额账户。非锁定余额账户内的资金随时可以使用，而锁定余额账户则不然。您可能会遇到设置定时放款的交易，同时，您也可以在消费时设置，确认可以拿到找零后解锁付款。这两种交易类型在不同阶段均需临时锁定资金。

门罗币与传统电子货币的关键区别是：门罗币账户只允许用户本人操作，通常在用户的计算机上进行。只要用户有良好的安全意识，就可以防止其他任何人进入此账户。

多账户

出去交易中支付矿工们的少量手续费，门罗币账户的申请和使用完全免费。

如此以来，用户可以轻松地创建普通账户，夫妻联名帐户，甚至为孩子创建一个独立账户。同样，一个企业可以为每个部门创建单独的帐户。由于门罗币的交易费用低廉，账户之间资金转移十分方便。

加密密钥

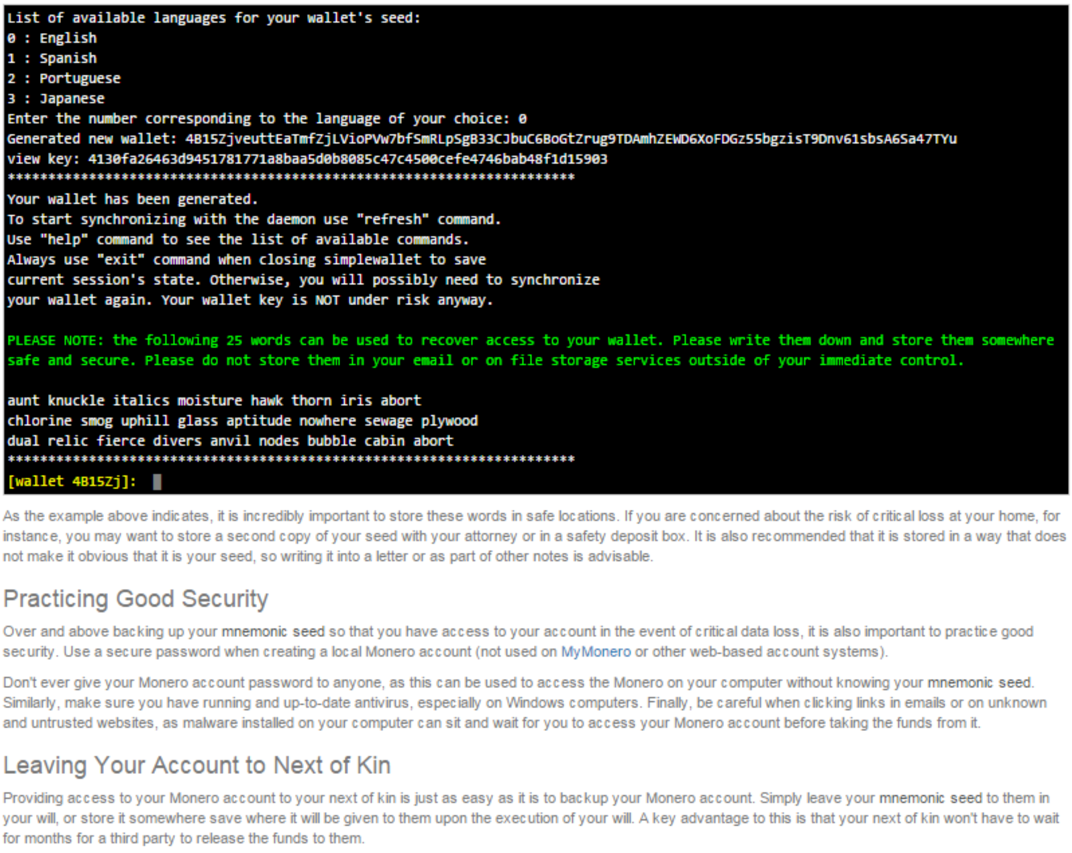
门罗币很大程度上依赖于一种加密系统，这个系统被称为公钥/私钥密码或非对称密码。具体加密原理请见此维基百科文章。

您的帐户是基于两个密钥，消费密钥和浏览密钥。消费密钥的特殊之处在于您只需着一个密钥便可以消费，而浏览密钥允许第三方由于特殊原因（例如审计或会计），浏览您的账户明细。这些密钥在保护您的交易隐私的重要作用。

用户要谨慎保存以上两个密钥以保证账户的隐秘性。另一方面，公共密钥作为您门罗帐户地址的一部分也具有公开性。一般情况下，如果有人想给您发送私信，他们就可以用您任何一个公共密钥给信息加密，之后，只有您在解密后才可以看得到。

账户备份

门罗币账户的安全性仅允许户主本人管理，因此，您需要完全为您的帐户负责。不过门罗币系统十分贴心，系统备份也是十分简单。当会员最初创建帐户时，门罗币会给您一个独一无二的助记种子，这个种子是由 13 个或 25 个字符组成，种子有多种语言供您选择。助记种子一旦产生，当务之急就是把它记下来，因为**门罗币系统备份需要的只是这个种子**。



```
List of available languages for your wallet's seed:
0 : English
1 : Spanish
2 : Portuguese
3 : Japanese
Enter the number corresponding to the language of your choice: 0
Generated new wallet: 4B15ZjveuttEaTmfZjLVioPVw7bfSmRLpSgB33CJbuC6BoGtZrug9TDAmhZEWD6XoFDGz55bgzisT9Dnv61sbsA6Sa47TYu
view key: 4130fa26463d9451781771a8baa5d0b8085c47c4500cefe4746bab48f1d15903
**********************************************************************
Your wallet has been generated.
To start synchronizing with the daemon use "refresh" command.
Use "help" command to see the list of available commands.
Always use "exit" command when closing simplewallet to save
current session's state. Otherwise, you will possibly need to synchronize
your wallet again. Your wallet key is NOT under risk anyway.

PLEASE NOTE: the following 25 words can be used to recover access to your wallet. Please write them down and store them somewhere
safe and secure. Please do not store them in your email or on file storage services outside of your immediate control.

aunt knuckle italics moisture hawk thorn iris abort
chlorine smog uphill glass aptitude nowhere sewage plywood
dual relic fierce divers anvil nodes bubble cabin abort
**********************************************************************
[wallet 4B15Zj]:
```

As the example above indicates, it is incredibly important to store these words in safe locations. If you are concerned about the risk of critical loss at your home, for instance, you may want to store a second copy of your seed with your attorney or in a safety deposit box. It is also recommended that it is stored in a way that does not make it obvious that it is your seed, so writing it into a letter or as part of other notes is advisable.

Practicing Good Security

Over and above backing up your **mnemonic seed** so that you have access to your account in the event of critical data loss, it is also important to practice good security. Use a secure password when creating a local Monero account (not used on MyMonero or other web-based account systems).

Don't ever give your Monero account password to anyone, as this can be used to access the Monero on your computer without knowing your **mnemonic seed**. Similarly, make sure you have running and up-to-date antivirus, especially on Windows computers. Finally, be careful when clicking links in emails or on unknown and untrusted websites, as malware installed on your computer can sit and wait for you to access your Monero account before taking the funds from it.

Leaving Your Account to Next of Kin

Providing access to your Monero account to your next of kin is just as easy as it is to backup your Monero account. Simply leave your **mnemonic seed** to them in your will, or store it somewhere save where it will be given to them upon the execution of your will. A key advantage to this is that your next of kin won't have to wait for months for a third party to release the funds to them.

[Screenshot]

正如上图，助记种子一定要保存在安全的地方。如果实在弄丢担心记忆种子，您可以让您的律师保存一份，或者把它存在保险箱中。同时还建议您将这串字符写入信件或笔记中，这样就不会过于明显。

提高安全意识

除了上述办法，提高安全意识对于账户管理同样重要。创建本地门罗币帐户时，要设置安全性高的密码。（尽量避免使用与 MyMonero 或其基于网页的系统相同的密码）

请勿在任何情况下向他人透漏门罗币密码，因为，即便没有你的助记种子，一旦拥有此密码，他人便会访问您的门罗币账户。同时，请确保开启并及时更新您的杀毒软件，尤其是在 Windows 系统上。最后一点，请慎重点击邮件中未知网站链接，恶意软件可以等您在访问门罗账户后，窃取您的账户信息，进而盗走您的资金。

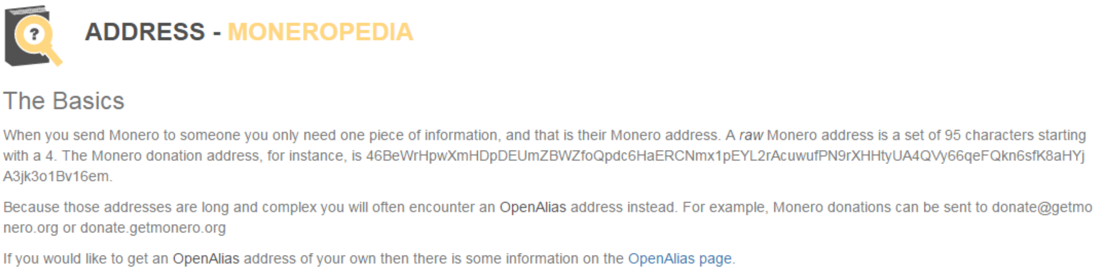
将账户转让给亲友

转让账户和系统备份一样容易。您只需要将助记种子留给他们即可。如此操作的关键优势在于：您的亲友无需再经过数月漫长等待后再得到第三方放款。

Section 10.2 Knowledge base—Moneropedia—Address

https://getmonero.org/knowledge-base/moneropedia/address

[Headers and footers can be found in the translated main page.]



ADDRESS - MONEROPEDIA

The Basics

When you send Monero to someone you only need one piece of information, and that is their Monero address. A *raw* Monero address is a set of 95 characters starting with a 4. The Monero donation address, for instance, is 46BeWrHpwXmHDpDEUmZBWZfoQpdc6HaERCNmx1pEYL2rAcuwufPN9rXHHtyUA4QVy66qeFQkn6sfK8aHYjA3jk3o1Bv16em.

Because those addresses are long and complex you will often encounter an OpenAlias address instead. For example, Monero donations can be sent to donate@getmonero.org or donate.getmonero.org

If you would like to get an OpenAlias address of your own then there is some information on the OpenAlias page.

地址—门罗百科

基础

发送门罗币的时候，您只需要确认一点，接受人的门罗地址。原始的门罗币地址是一串以 4 开头的 95 个字符。例，门罗币捐款地址：

46BeWrHpwXmHDpDEUmZBWZfoQpdc6HaERCNmx1pEYL2rAcuwufPN9rXHHtyUA4QVy66qeFQkn6sfK8aHYjA3jk3o1Bv16em.

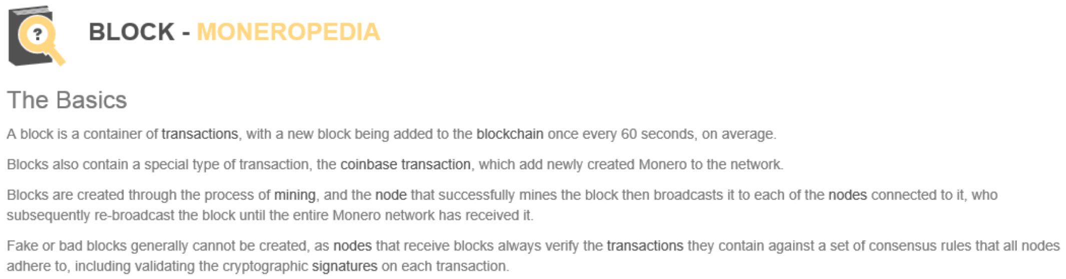
由于门罗币地址冗长而复杂，您会发现人们经常会使用公开别名代替。例如门罗币捐款也可以发送到 donate@getmonero.org 或 donate.getmonero.org。

如果您想获得您自己的公开别名地址，请参考公开别名页面。

Section 10.3 Knowledge base—Moneropedia—blocks

https://getmonero.org/knowledge-base/moneropedia/block

[Headers and footers can be found in the translated main page.]



BLOCK - MONEROPEDIA

The Basics

A block is a container of transactions, with a new block being added to the blockchain once every 60 seconds, on average.

Blocks also contain a special type of transaction, the coinbase transaction, which add newly created Monero to the network.

Blocks are created through the process of mining, and the node that successfully mines the block then broadcasts it to each of the nodes connected to it, who subsequently re-broadcast the block until the entire Monero network has received it.

Fake or bad blocks generally cannot be created, as nodes that receive blocks always verify the transactions they contain against a set of consensus rules that all nodes adhere to, including validating the cryptographic signatures on each transaction.

区块—门罗百科

基础

区块是包容着多个交易，平均来讲，每六十秒钟就有一个区块链就会有一个新的区块加入。

区块也包含了一种特种的交易，即 Coinbase 交易。这种交易可以将新生的门罗币。

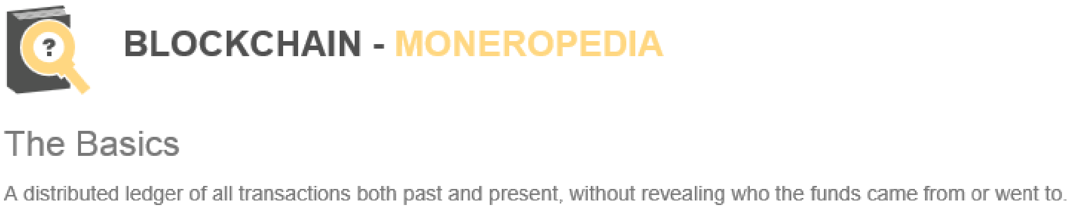
区块是伴随电子币的开采而产生的，而成功开采出货币的网络节点会将其传播给其它节点，其它节点继续传播，就这样一传十，十传百，直到遍布整个门罗币网络。

虚假或问题区块一般会在传播的过程中夭折。因为节点在接收区块时都会确认交易是否违反大家形成的共识，如，节点会验证每笔交易的加密签名。

Section 10.4 Knowledge base—Moneropedia—blockchain

https://getmonero.org/knowledge-base/moneropedia/blockchain

[Headers and footers can be found in the translated main page.]



BLOCKCHAIN - MONEROPEDIA

The Basics

A distributed ledger of all transactions both past and present, without revealing who the funds came from or went to.

区块链—门罗百科

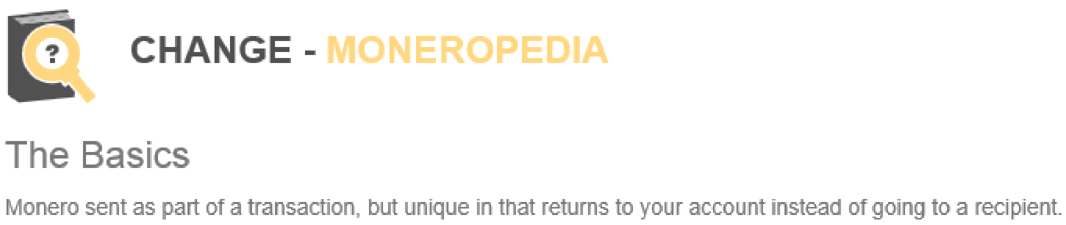
基础

历史交易和当前交易的总账，其中未显示每笔资金的来源与去路。

Section 10.5 Knowledge base—Moneropedia—change

https://getmonero.org/knowledge-base/moneropedia/change

[Headers and footers can be found in the translated main page.]



CHANGE - MONEROPEDIA

The Basics

Monero sent as part of a transaction, but unique in that returns to your account instead of going to a recipient.

找零—门罗百科

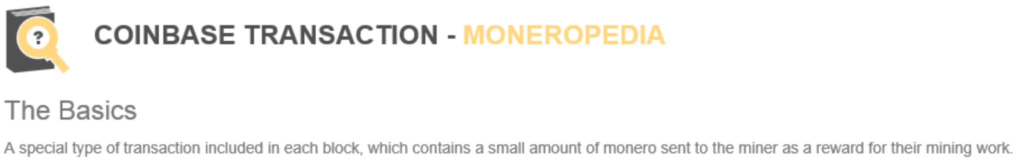
基础

交易的一部分门罗币，不同之处在于，这笔门罗币会回到付款人手中，而非收款人。

Section 10.6 Knowledge base—Moneropedia—coinbase transaction

https://getmonero.org/knowledge-base/moneropedia/coinbase

[Headers and footers can be found in the translated main page.]



COINBASE TRANSACTION - MONEROPEDIA

The Basics

A special type of transaction included in each block, which contains a small amount of monero sent to the miner as a reward for their mining work.

Coinbase 交易—门罗百科

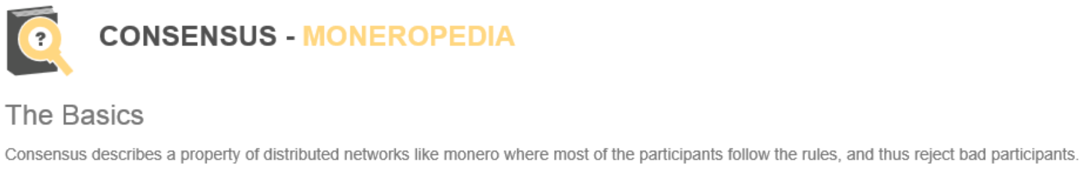
基础

存在于任何区块中的一种特殊交易，此种交易包括将少量门罗币发放给货币开采者，以作为报酬。

Section 10.7 Knowledge base—Moneropedia—consensus

https://getmonero.org/knowledge-base/moneropedia/consensus

[Headers and footers can be found in the translated main page.]



CONSENSUS - MONEROPEDIA

The Basics

Consensus describes a property of distributed networks like monero where most of the participants follow the rules, and thus reject bad participants.

共识—门罗百科

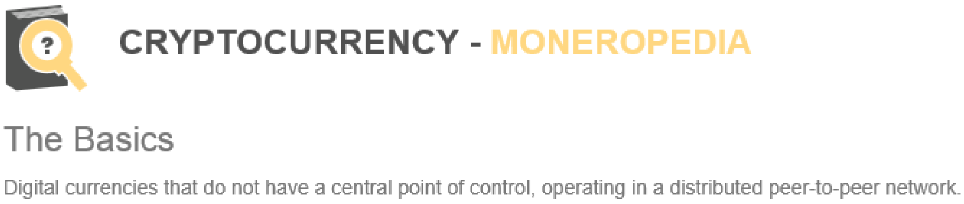
基础

共识体现了如门罗币形式分布式网络的一种属性，在分布式网络中，绝大多数参与者遵守规则，不良的参与者会被拒之门外。

Section 10.8 Knowledge base—Moneropedia—cryptocurrency

https://getmonero.org/knowledge-base/moneropedia/cryptocurrency

[Headers and footers can be found in the translated main page.]



CRYPTOCURRENCY - MONEROPEDIA

The Basics

Digital currencies that do not have a central point of control, operating in a distributed peer-to-peer network.

加密货币—门罗百科

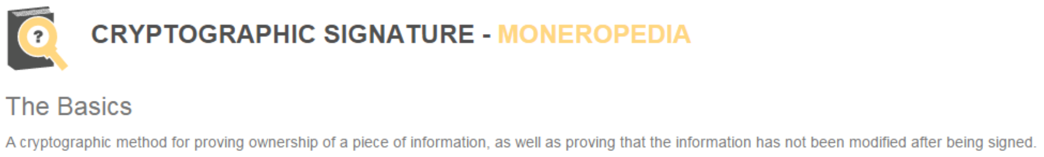
基础

不受集中控制的电子货币，此货币在点对点分布式网络中运行。

Section 10.9 Knowledge base—Moneropedia—Cryptocgraphic signature

https://getmonero.org/knowledge-base/moneropedia/signature

[Headers and footers can be found in the translated main page.]



CRYPTOGRAPHIC SIGNATURE - MONEROPEDIA

The Basics

A cryptographic method for proving ownership of a piece of information, as well as proving that the information has not been modified after being signed.

加密签名—门罗百科

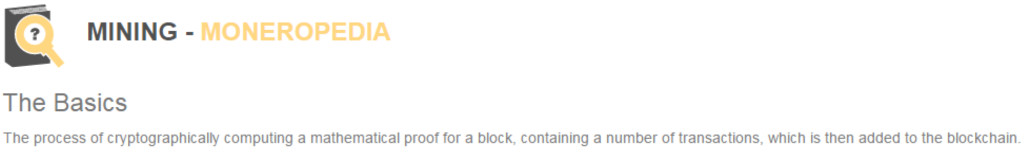
基础

一种用于证明对信息的所有权的加密方法，同时也说明信息在签署后未受修改。

Section 10.10 Knowledge base—Moneropedia—Mining

https://getmonero.org/knowledge-base/moneropedia/miners

[Headers and footers can be found in the translated main page.]



MINING - MONEROPEDIA

The Basics

The process of cryptographically computing a mathematical proof for a block, containing a number of transactions, which is then added to the blockchain.

挖掘—门罗百科

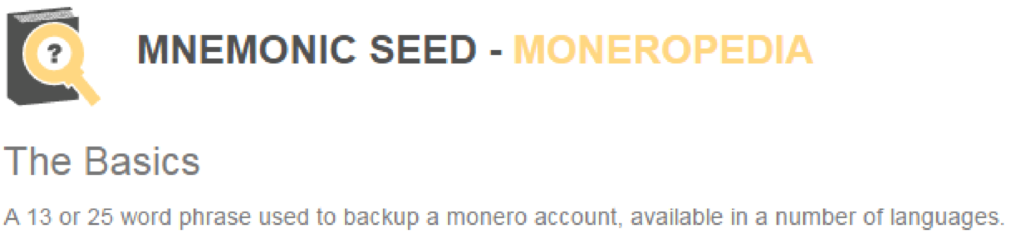
基础

为区块加密计算数学依据的过程，其中包括即将被加入区块链的数笔交易。

Section 10.11 Knowledge base—Moneropedia—Mnemonic seed

https://getmonero.org/knowledge-base/moneropedia/mnemonicseed

[Headers and footers can be found in the translated main page.]



MNEMONIC SEED - MONEROPEDIA

The Basics

A 13 or 25 word phrase used to backup a monero account, available in a number of languages.

助记种子—门罗百科

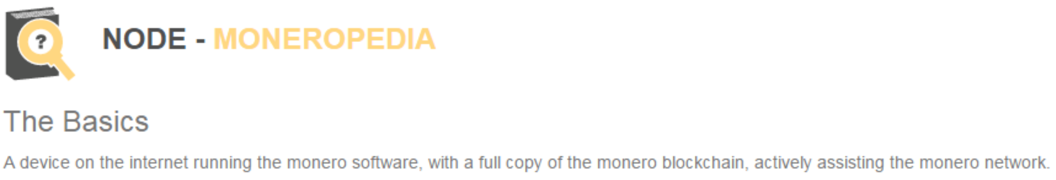
基础

用于备份门罗币账户的一个 13 到 25 个字的字符串，此字符现有多种语言可选。

Section 10.12 Knowledge base—Moneropedia—Node

https://getmonero.org/knowledge-base/moneropedia/node

[Headers and footers can be found in the translated main page.]



NODE - MONEROPEDIA

The Basics

A device on the internet running the monero software, with a full copy of the monero blockchain, actively assisting the monero network.

网络结点—门罗百科

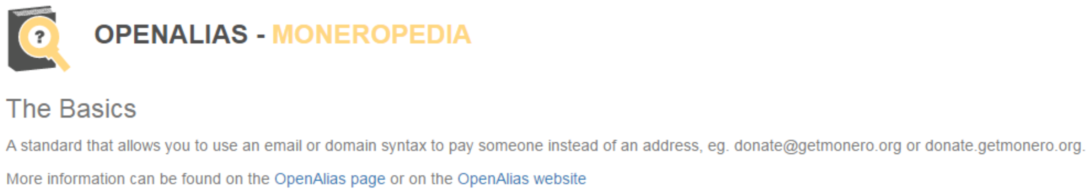
基础

互联网上可运行门罗币或门罗币区块链完整副本的设备，并积极协助门罗币网络。

Section 10.13 Knowledge base—Moneropedia—OpenAlias

https://getmonero.org/knowledge-base/moneropedia/openalias

[Headers and footers can be found in the translated main page.]



OPENALIAS - MONEROPEDIA

The Basics

A standard that allows you to use an email or domain syntax to pay someone instead of an address, eg. donate@getmonero.org or donate.getmonero.org.

More information can be found on the OpenAlias page or on the OpenAlias website

公开别名—门罗百科

基础

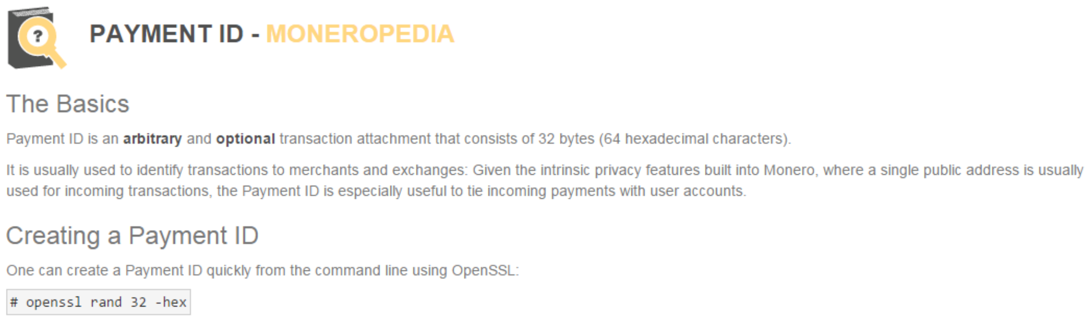
一个允许您使用邮箱地址或域名代替原始地址的标准，例如：donate@getmonero.org or donate.getmonero.org.

更多信息请见公开别名页面，或公开别名网站。

Section 10.14 Knowledge base—Moneropedia—Payment ID

https://getmonero.org/knowledge-base/moneropedia/paymentid

[Headers and footers can be found in the translated main page.]



PAYMENT ID - MONEROPEDIA

The Basics

Payment ID is an **arbitrary** and **optional** transaction attachment that consists of 32 bytes (64 hexadecimal characters).

It is usually used to identify transactions to merchants and exchanges: Given the intrinsic privacy features built into Monero, where a single public address is usually used for incoming transactions, the Payment ID is especially useful to tie incoming payments with user accounts.

Creating a Payment ID

One can create a Payment ID quickly from the command line using OpenSSL:

```
# openssl rand 32 -hex
```

付款编号—门罗百科

基础

付款编号是每笔交易产生的附属物。编号由 32 个字节（64 个十六进制字符）组成，具有任意性和可选性。

付款编号通常用于商家识别交易：鉴于门罗币自带的隐秘性，当卖家在交易中使用单一公共地址时，每笔交易对应的付款编号就显得尤为重要。

创建付款编号

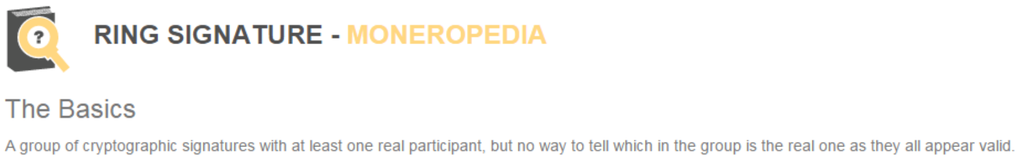
用户只需在命令行内使用 OpenSSL，即可简单快捷的建立起付款编号：

(Picture) # openssl rand 32 –hex

Section 10.15 Knowledge base—Moneropedia—Ring signature

https://getmonero.org/knowledge-base/moneropedia/ringsignatures

[Headers and footers can be found in the translated main page.]



RING SIGNATURE - MONEROPEDIA

The Basics

A group of cryptographic signatures with at least one real participant, but no way to tell which in the group is the real one as they all appear valid.

群签名-门罗百科

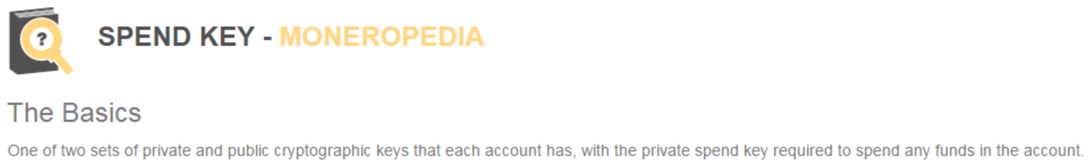
基础

一组加密签名至少需要一位真正的参与者，但所有组员的签名都会显示为有效签名，因此无法识别谁是真正的参与者。

Section 10.16 Knowledge base—Moneropedia—Spend key

https://getmonero.org/knowledge-base/moneropedia/spendkey

[Headers and footers can be found in the translated main page.]



SPEND KEY - MONEROPEDIA

The Basics

One of two sets of private and public cryptographic keys that each account has, with the private spend key required to spend any funds in the account.

消费密钥—门罗百科

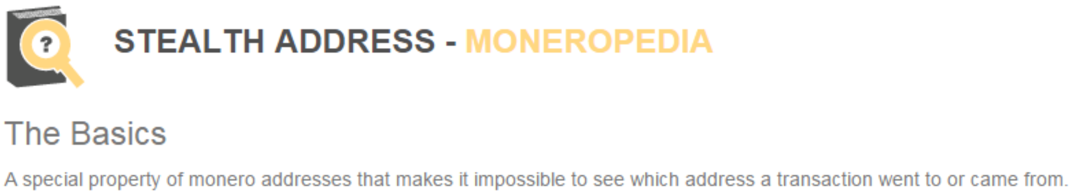
基础

公开与私人密钥中的私人密钥。此密钥为支配资金的必备密钥。

Section 10.17 Knowledge base—Moneropedia—Stealth address

https://getmonero.org/knowledge-base/moneropedia/stealthaddress

[Headers and footers can be found in the translated main page.]



STEALTH ADDRESS - MONEROPEDIA

The Basics

A special property of monero addresses that makes it impossible to see which address a transaction went to or came from.

隐形地址—门罗百科

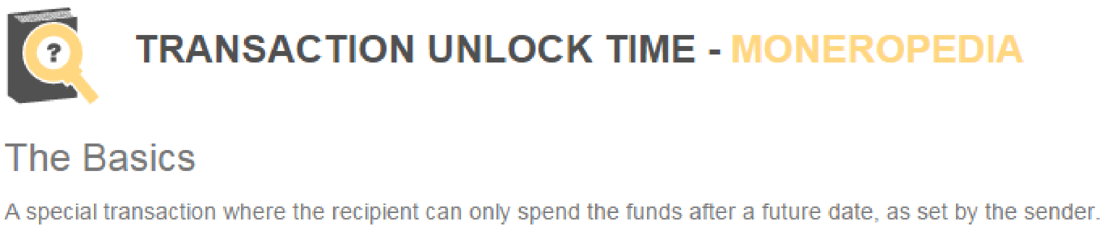
基础

门罗币的特性：隐藏交易的来龙去脉。

Section 10.18 Knowledge base—Moneropedia—Transaction unlock time

https://getmonero.org/knowledge-base/moneropedia/unlocktime

[Headers and footers can be found in the translated main page.]



TRANSACTION UNLOCK TIME - MONEROPEDIA

The Basics

A special transaction where the recipient can only spend the funds after a future date, as set by the sender.

交易解锁时间—门罗百科

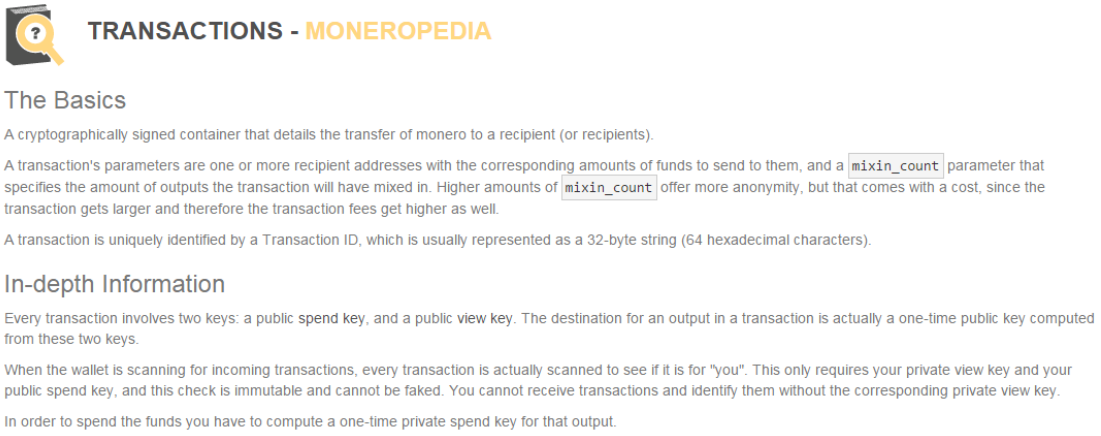
基础

一种特殊交易，此交易中接收人只能在发送人设定的时间内调动资金。

Section 10.19 Knowledge base—Moneropedia—Transaction

https://getmonero.org/knowledge-base/moneropedia/transaction

[Headers and footers can be found in the translated main page.]



TRANSACTIONS - MONEROPEDIA

The Basics

A cryptographically signed container that details the transfer of monero to a recipient (or recipients).

A transaction's parameters are one or more recipient addresses with the corresponding amounts of funds to send to them, and a `mixin_count` parameter that specifies the amount of outputs the transaction will have mixed in. Higher amounts of `mixin_count` offer more anonymity, but that comes with a cost, since the transaction gets larger and therefore the transaction fees get higher as well.

A transaction is uniquely identified by a Transaction ID, which is usually represented as a 32-byte string (64 hexadecimal characters).

In-depth Information

Every transaction involves two keys: a public spend key, and a public view key. The destination for an output in a transaction is actually a one-time public key computed from these two keys.

When the wallet is scanning for incoming transactions, every transaction is actually scanned to see if it is for "you". This only requires your private view key and your public spend key, and this check is immutable and cannot be faked. You cannot receive transactions and identify them without the corresponding private view key.

In order to spend the funds you have to compute a one-time private spend key for that output.

交易—门罗百科

基础

一种加密签名后的容器，详细包括了门罗币转移至一个或多个接收人的过程。

交易参数是一个或多个接收地址和所对应的自己，外加一个 mixin_count 参数。这个 mixin_count 参数会指定交易中混合了多少笔输出。mixin_count 参数越大，交易匿名度越高，但由于交易手续费会同时增加，因此成本也会变高。

不同的交易可以用对应的交易编号识别，交易编号通常为一个 32 字节（64 个十六进制字符）。的字符串

深入信息

每笔交易搜涉及到两个密钥：公开消费密钥和公开浏览密钥。交易中输出目的地其实是由此两密钥计算出的一个一次性的公共密钥。

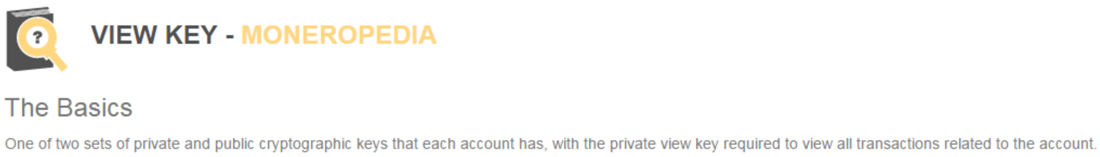
事实上，当您的电子钱包扫描传入事物时，它会检查每一笔交易是否属于您。这个过程需要您的私人浏览密钥和私人消费密钥，检查是不可改变和不可伪造的。您无法不提供对应的私人浏览密钥便接受并识别交易。

使用资金时，您需要针对此项输出，计算出一个一次性的私人消费密钥。

Section 10.20 Knowledge base—Moneropedia—View key

https://getmonero.org/knowledge-base/moneropedia/viewkey

[Headers and footers can be found in the translated main page.]



VIEW KEY - MONEROPEDIA

The Basics

One of two sets of private and public cryptographic keys that each account has, with the private view key required to view all transactions related to the account.

浏览密钥—门罗百科

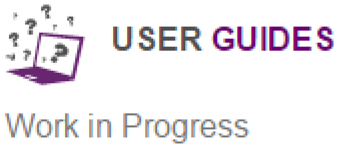
基础

每个账户都有的一组公私密钥之一：私人浏览密钥用于浏览此账户相关交易

Section 11 Knowledge base—User Guides

https://getmonero.org/knowledge-base/user-guides/

[Headers and footers can be found in the translated main page.]



USER GUIDES

Work in Progress

用户指南

正在完善中

Section 12 Knowledge base—Developer Guides

https://getmonero.org/knowledge-base/developer-guides/

[Headers and footers can be found in the translated main page.]

DEVELOPER GUIDES

Work in Progress

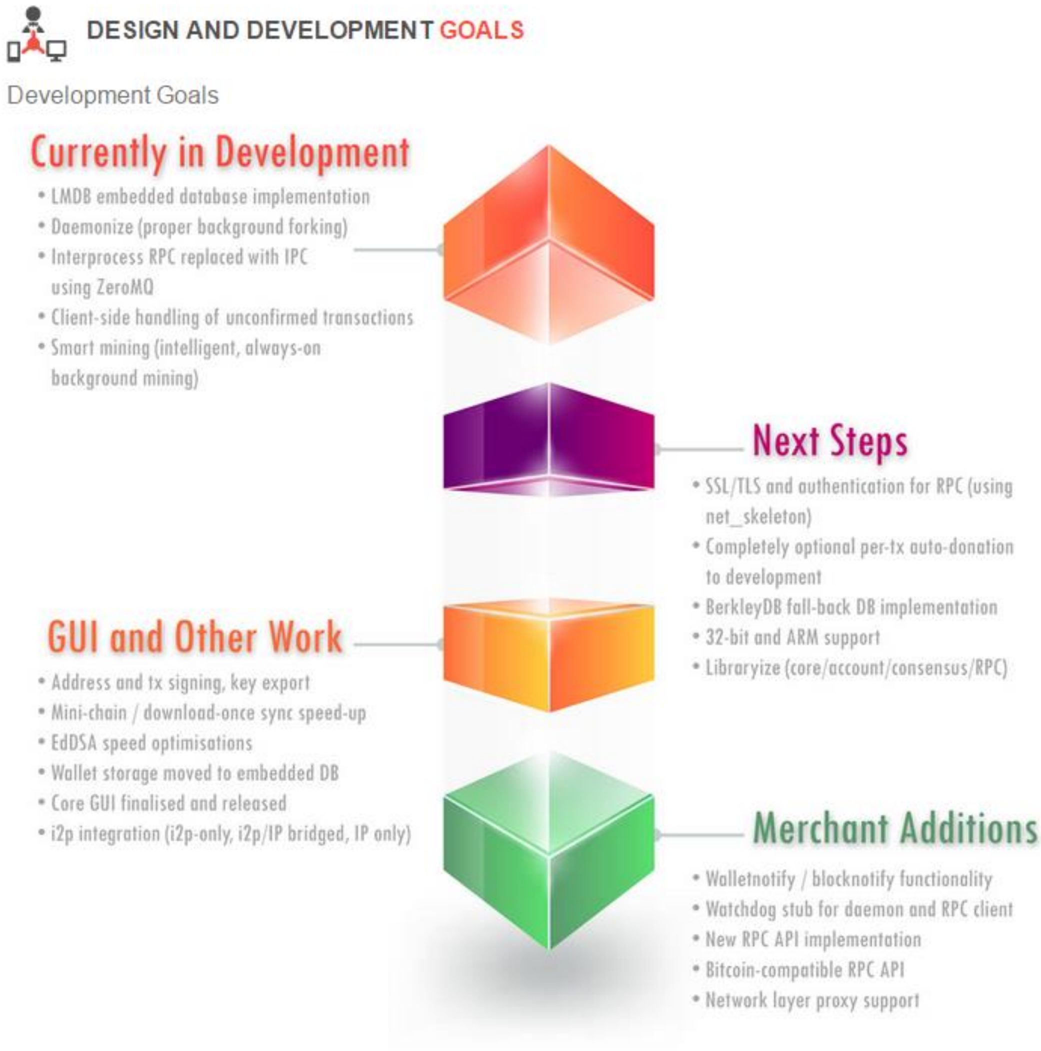
开发者指南

正在完善中

Section 13 Knowledge base—Design & Development goals

https://getmonero.org/design-goals/

[Headers and footers can be found in the translated main page.]



DESIGN AND DEVELOPMENT GOALS

Development Goals

Currently in Development

- LMDB embedded database implementation
- Daemonize (proper background forking)
- Interprocess RPC replaced with IPC using ZeroMQ
- Client-side handling of unconfirmed transactions
- Smart mining (intelligent, always-on background mining)

Next Steps

- SSL/TLS and authentication for RPC (using net_skeleton)
- Completely optional per-tx auto-donation to development
- BerkleyDB fall-back DB implementation
- 32-bit and ARM support
- Libraryize (core/account/consensus/RPC)

GUI and Other Work

- Address and tx signing, key export
- Mini-chain / download-once sync speed-up
- EdDSA speed optimisations
- Wallet storage moved to embedded DB
- Core GUI finalised and released
- i2p integration (i2p-only, i2p/IP bridged, IP only)

Merchant Additions

- Walletnotify / blocknotify functionality
- Watchdog stub for daemon and RPC client
- New RPC API implementation
- Bitcoin-compatible RPC API
- Network layer proxy support

设计及发展目标

发展目标

当前进程

- 完成 LMDB 嵌入数据库
- （根据背景程序派生）后台化
- 将 RPC 换位使用 ZeroMQ 的 IPC
- 未确认交易的客户端移交
- 智能开采（智能化，始终在线的后台开采）

即将进行

- SSL/TLS 和 RPC 身份验证（通过 net_skeleton）
- 每笔交易中的自动捐款将完全成为任选项
- 完成 BerkleyDB 数据库备份
- 32 位和 ARM 支持
- 软件库化（核心/账号/共识/RPC）

用户界面及其它

- 地址和交易签名，密钥输出
- 迷你链/加速一次下载同步

- 优化 EdDSA 速度
- 电子钱包储存转至嵌入的数据库
- 核心用户界面定稿并发布
- I2p 集成（仅有 i2p，i2p 与 IP 桥接，仅有 IP）

商户附加功能

- 电子钱包推送/区块推送功能
- 针对后台和 RPC 程序的 Watchdog stub
- 新的 RPC API 完成
- 与比特币兼容的 RPC API
- 网络层代理支持

研究目标

当前研究课题

- 更高难度的算法
- 多重交易，N 人组中 M 个人的交易
- 隐身付款编号，序列化到目的地址

侧链的基础

- 无 Coinbase 合并开采
- 多币种等价交换
- 子网络和结点交互功能和/或可支持的链
- 链上及传播前的双向认证（每笔交易都包含一个基于内部或外部服务的双向认证将为短信，谷歌验证, YubiKey 等奠定基础 ）

初始侧链

- 实验子链：Tippero (专为交易和一日多次的主链结算设计的超轻链)
- 门罗币编号（私有/自选/公开身份，也可以是不同个体或集团的组合，均可用于登陆）
- 门罗币 DNS (域名以.x 结尾，支持所有 DNS RDATA 类型，包括 DNSSEC，本地 DNS 服务器)
- MoneroTrust (网络身份之间的信任是交易的基础，评估会在 12 个月后进行)

研究方向

- 门罗币聊天工具（MoneroChat）（保存并转发加密信息，包括付款请求）
- 门罗币资产（MoneroAssets）（各个侧链交链交易中的资产市场）
- 门罗币交易（MoneroTrade）（去中心化的产品及服务类电子商务，满一个月后 huijinxing 修整，以保持市场秩序）

Section 14 Knowledge base— Monero research lab

https://getmonero.org/research-lab/

[Headers and footers can be found in the translated main page.]

THE MONERO RESEARCH LAB

Work in Progress

For current Monero Research Lab publications please visit: https://lab.getmonero.org/

门罗币研究室

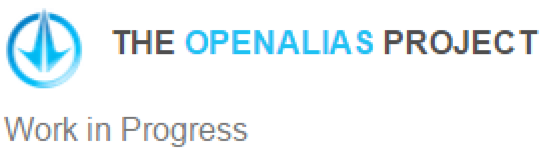
正在完善中

了解最新门罗币研究室刊物，请登录 https://lab.getmonero.org/

Section 15 Knowledge base— the OpenAlias project

https://getmonero.org/knowledge-base/openalias

[Headers and footers can be found in the translated main page.]



THE OPENALIAS PROJECT

Work in Progress

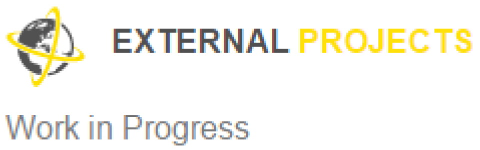
公开别名项目

正在完善中

Section 16 Knowledge base— external project

https://getmonero.org/knowledge-base/projects

[Headers and footers can be found in the translated main page.]



EXTERNAL PROJECTS

Work in Progress

对外项目

正在完善中