



MONERO

Monero 是安全、保護隱私且完全匿蹤
人人皆可使用的加密貨幣。

三分鐘懶人包

使用者可以安全地支付，沒有人能夠窺探
他們的帳戶餘額或是追蹤其帳戶活動。



去中心化

這個開源專案是由一個去中心化團隊所創立與帶領的。這團隊由一群開發者與社群成員所組成，因此無法對其進行政治審查，絕大多數的開發者都是自發性的貢獻，開發社群成員遍布全球各地。

安全性

作為一個去中心化的加密貨幣，Monero 是由世界各地眾多的使用者所構築的大型網路。交易是由分散式共識所確認並記錄於無法竄改的區塊鏈中。

可擴容性

Monero 的動態區塊容量會隨著交易量調整以提供較低的手續費與更快的交易速度。較高的交易量將會提高區塊容量上限，反之將會帶來較小的區塊容量。防彈協定也大幅度縮減交易所需的容量，使得其在加密貨幣世界中更加的具有優勢。



核心原則

在 Monero 區塊鏈上的交易並不會揭露特定使用者的資訊，或其在真實世界中的身分，因此使用者不須擔心受到資本審查或管控。

防止審查

Monero 使用成熟的密碼學技術如環狀簽名、保密交易與隱匿性地址以混淆所有交易中的付款來源、交易金額以及收款者的資訊。

保護隱私

Monero 具有可替代性，因為它是預設保護隱私，這代表著一個 Monero 的價值永遠與另一個 Monero 相等，你將不用擔心你的加密貨幣會因為上游的交易黑歷史而被商家或交易所拒收。

可替代性

MONERO 的歷史

Monero 專案在 2014 年四月開始發行。是一次公平並預先公開的發行，使用了 [CryptoNote](#) 協定原始碼。專案不存在著預挖或瞬挖，也沒有從區塊獎勵中抽成。

在[這裡](#)可以看到發行時的公告討論串。

在 Monero 發行後經過了數次的升級改版，幾乎所有的改進都是為了提供更安全及更好的隱私保護，或是讓它變得更加容易使用。Monero 會持續不斷地朝著開發目標前進，也就是隱私與安全優先，接著是容易使用與效率。

MONERO 這字背後的意涵是什麼？

Monero 一詞是取自世界語 (Esperanto)。之所以選擇使用世界語是因為它是一個去中心化的語言，並代表著打破世界上人與人的藩籬。在世界語中，Monero 一詞是由三個部分所組成的一個單字：mon + er + o。每個部分都有其意義。

mon-：金錢

-er-：最小單位

-o：一個事物（代表一個名詞）

這說明了 monero 一詞代表著：

一個代表最小單位的金錢，或是錢幣。

MONERO 的關鍵特別之處

- Monero 使用 CryptoNote 程式碼：這和比特幣或乙太幣或許多從他們衍生出來的貨幣相比，有著截然不同的程式碼架構，這是為了做到更好的保護隱私功能。

- 隱私是預設必要的；而透明性是可以自行選擇的。Monero 的設計可以混淆交易資訊的每一個層面：付款者、收款者、還有交易本身。如果使用者需要透明性，他們可以選擇公開他們的唯讀錢包以揭露該錢包的收款資訊。

- 例行性網路協定升級：Monero 的社群開發者定期地進行網路協定升級（硬分叉）以確保所有使用者都能享受到最佳的安全、隱私保護及其他功能。這樣做法讓 Monero 能夠更安全也更靈活地去應對任何可能興起的安全性威脅。[那些我曾聽說的許多分叉幣是什麼？](#)

- Monero 區塊獎勵策略：區塊獎勵會緩慢地下降直到 2022 年的五月底會固定在尾發行的速率，約為 0.6 XMR / 每區塊。尾發行將會持續提供永久的挖礦動機。此外，更重要的是，尾發行也提供了 Monero 一個內建穩定且可預測的通膨，這是一個真正的貨幣所需要的特性。

- Monero 研究室：Monero 不僅僅是要打造一款有替代性的貨幣，更是要持續探索加密貨幣的金融隱私領域。為了達到這點，Monero 社群中的一些數學與計算物理學家們發表了[白皮書](#)，揭露數個正在進行中的[研究目標](#)。

- 低門檻的挖礦：人人只要有一台連上網路的電腦或是網頁瀏覽器就能參與挖礦。

真實世界中的應用

由於 Monero 是安全、低手續費、無疆界的貨幣，人們可以自由發送交易，不受到貪腐、破產的政府或銀行的影響。這提供了身處於[苛政的國家](#)或經濟蕭條的人民一個獨立的金融管道。

完全隱匿保護的金融歷史記錄保護消費者與公司不受到價格操控、原物料鏈暴露、經濟歧視等等的傷害。[Monero 是目前唯一在加密貨幣中](#)可以提供完全的可替代性、去中心化的電子現金。

技術性基本資料

(資料截至 11/14/2018)

活躍節點數量： 1,756 (來源：<https://monerohash.com/nodes-distribution.html>)
交易網路算力： 435.17 MH/s
平均每小時交易數： 178 (30 天平均)
全網挖礦 CPU 核心數： 14,499,178
貨幣流通量： 16,570,126 XMR (估計值)
貨幣市值： \$1,503,928,296 USD (約佔 0.77% 加密貨幣總市值)
目前區塊獎勵： 3.5984 XMR
平均區塊區間： 2 分鐘

Monero 的區塊獎勵會緩慢下降直到 2022 年五月，屆時將有 一千八百多萬的 XMR 總發行量，伴隨永遠的 0.6 XMR 固定發行速率。

以尾發行的速率 (0.6 XMR / 區塊) 來說，2040 年時將會達到相當於比特幣的總發行量，約為兩千一百萬 XMR。

正在開發中的功能

雖然 Monero 已經可以在全世界使用，社群開發者仍然還有一些令人興奮的目標，都是為了讓 Monero 更加安全、更好的隱私保護與更容易使用的功能。有些目標預計很快就能完成：

防彈協定：[這項開發](#)可以讓交易在區塊鏈上儲存的效率提升，並帶來更快的交易速度。

Kovri：這會是一個隱私保護功能的升級，為 Monero 交易加上第四層保護。Kovri 使用 [garlic-encryption](#) (就像是 Tor on steroids) 用來遮蔽發送者與接收者在網路上的 IP 位址。如此一來，在 Monero 上的交易每一層面包括發送者、接收者、交易金額和交易本身 (使用 Kovri) 將都會得更隱私且更加安全。

硬體錢包：Trezor Model T 硬體錢包已經將 Monero 列入[支援清單](#)，而 [Ledger 硬體錢包](#)已可以在 Monero 的官方 GUI 錢包中使用。而另外 Monero 社群更成功募資支持了一個團隊以打造 [Kastelo 開源硬體錢包](#)，系統將基於 Monero ethos 上開發。這些硬體錢包都完全支援 Monero 的交易。

Kasisto：這是 [銷售點終端 \(POS\) 的方案](#)，設計用來讓商業行號可以更輕鬆的接受 Monero 支付。

更多資訊

[getmonero.org \(官方網站 \)](https://getmonero.org)
monero.how
reddit.com/r/monero
[Guide to Monero \(post\)](#)
[Monero In-Depth Technical Intro](#)
[Zero to Monero](#)

[避免詐騙](#)
[Monero FAQ](#)
[Monero SWOT Analysis](#)
[Connect w/ Monero Community](#)
[Mastering Monero - \(即將完成 \)](#)



Monero Quick Facts - 修訂於 11/14/2018
由 Monero Outreach 團隊製作提供 Monero 社群使用

Monero Outreach 致力於提供教育與公關資訊以推廣
Monero 的 使用與提高接受度。你的捐獻讓這一切成為可能。