幣圈入門指南丨什麼是隱私幣？

原文：
https://www.btcc.com/zh-TW/academy/crypto-basics/what-is-privacy-coin

加密貨幣通常是匿名的，但不一定是私有的。比特幣（BTC）和其他資產在區塊鏈上運行，每筆交易都在網上公開發布。在兩方或多方的交易過程中，資產會轉移到不同的錢包中，每個錢包由一串字符代表。而加密市場中存在一種被稱為隱私幣、私人幣或匿名幣的加密資產，它們試圖隱藏交易信息，給予用戶更多的隱私。

什麼是隱私幣？

隱私幣是為將隱私元素放在首位和中心而創建的加密貨幣。許多隱私幣支持者認為，金融隱私是穩健貨幣的基本且不可協商的屬性。

隱私幣在大多數國家和地區都是合法的，但它也存在被禁止的風險。像韓國和日本這樣的地方已經開始禁止它。

三種流行的隱私幣

隱私幣使用不同的方式進行工作，目前熱門的隱私幣有三種。

1. 門羅幣（XMR）

門羅幣（XMR）是加密領域最早的隱私幣項目之一。隱形地址、環簽名、零知識證明（zk-proofs）和 RingCT 構成了門羅幣的專有隱私協議。

當在門羅幣上發起交易時，協議會為交易創建一個隨機的、一次性使用的目標地址，稱為隱形地址。隱形地址不能鏈接回收件人，以確保他們的隱私。為了保護髮送者的匿名性，門羅幣使用環簽名來簽署交易。環簽名由發送者的公鑰和許多其他公鑰組成。這有助於混淆實際發件人的身份。

而為了保護髮送者的匿名性，使用環簽名來簽署交易。環簽名由發送者的公鑰和許多其他公鑰組成。這有助於混淆實際發件人的身份。 最後，Ring CT混淆了實際的交易價值。Monero 還會在每筆交易中廣播誘餌錢包地址。這樣做可以確保交易線索上的任何人都可以愉快地篩選所有交易，無論是真實的還是其他的。

門羅幣團隊的大部分成員今天仍然是匿名的。到目前為止，該團隊已設法每 6 個月推出一次更新。門羅幣開發者社區並不是單一的。相反，它根據各自的專業知識組織成工作組。

2.Zcash

Zcash使用比特幣算法，但具有 zk-proofs 和屏蔽地址。屏蔽地址類似於 Monero 的隱形地址，不同的是它可以同時對發件人和收件人啟用。

與門羅幣類似，Zcash 也使用非交互式zk-proof的一個版本，稱為“ zk-SNARK ”（零知識簡潔非交互式知識論證）。此外，Zcash 發送者還可以在隱蔽交易中包含私人備忘錄。

Zcash 是獨一無二的，因為它提供完全私密和完全公開的交易，允許用戶公開某些交易細節，同時混淆其他細節。實際上，Zcash 的絕大多數交易都是公開的。這引起了第三方可以通過消除過程識別私人交易的擔憂。

3.Dash

Dash 是一種將用戶效用放在首位的硬幣，隱私是它為用戶提供的一項可選功能，該功能會產生更高的交易費用。

Dash 使用一種混合方法（稱為 CoinJoin）來執行 PrivateSend 交易。使用 CoinJoin，每個 PrivateSend 交易都被分割成許多小金額，並且錢包地址與其他 PrivateSend 用戶的地址打亂。然後 Dash 將合併所有交易，並將其作為單個統一交易發布。這種方法使得解讀交易並確定哪些金額屬於誰是不可行的。

隱私幣的風險

隱私幣的風險直接源於其能夠混淆所有交易的核心吸引力。這提高了隱私幣被不良行為者用於非法活動和金融交易的可能性，而且執法機構將很難識別資金踪跡。

由於大多數政府對隱私幣的不認同，許多加密貨幣交易所對上市隱私幣時通常也採取謹慎態度。這很大程度上會降低隱私幣對普通加密貨幣用戶的吸引力。