什么是加密货币混币器？

用户可以向混币器合约确认他们已经存入了存款，而不需要在提现交易中使用诸如环签名和zk-SNARKs等几种可访问的加密技术之一来暴露他们所发放的存款交易。

加密货币混币器的运作原理是什么？

加密货币混币器的设计思路是通过一个隐藏数字签名的“黑匣子”来运行交易的数字签名。

加密货币混币器是一种程序，它在将特定数量的加密货币转移到指定的接收者之前，在私人池中混合。例如，一个跟踪所有比特币交易的比特币浏览器会显示，A将比特币转移到混币器，B从混币器接收比特币。这样，就没有人知道是谁发送了BTC，发送给了谁。因此，“脏比特币”在加密货币混币过程中被洗白。

加密货币混币器的功能是，将你的加密货币与一大堆其他加密货币混合，然后将较小的加密货币单位返回到你选择的地址，比你存入的总金额为减少1-3%。混币公司通常获得1-3%的利润，这是他们谋生的方式。

混币与洗钱这种犯罪行为类似。然而，仅仅因为有人参与了混币，并不意味着他们是在犯罪。相反，这只是意味着他们想要增加加密货币交易的隐私。

使用加密货币混币器犯法吗？

使用混币服务是否违法由你所居住的司法管辖区决定。此外，比特币混币器是必要的吗？或者，加密货币混币合法吗？这取决于你使用这些服务的目的。

美国前助理司法部长布莱恩·本茨科夫斯基(Brian Benczkowski)表示，使用混币器来伪装加密货币交易是犯罪行为。例如，比特币的关键功能是隐私而不是匿名，这意味着你的身份并不总是被披露，但你的交易可以被审计，以调查任何不当行为。那么，比特币混币行为是非法的吗?

比特币混币器被美国金融犯罪执法网络(FinCEN)归类为货币传送器。因此，它们必须在FinCEN注册，并申请州对州之间的经营许可证。2021年，一名俄亥俄州公民因涉嫌洗钱被捕，原因是他在暗网上运营比特币混币服务。FinCEN有强制性的许可规定，而该公民并未注册货币交易服务，在没有许可的情况下进行了货币交易。

你能追踪加密货币混币器或比特币混币器吗?

由于加密货币混币服务，很难跟踪特定的加密货币，因为所有的币都汇集在一起，然后随机间隔分布。

通过使用各种数字货币构建自定义区块链，加密货币混币器可以让零售商重写他们的加密历史。他们通过其他虚拟交易所组成的复杂半随机网络进行交易，这使得用户很难将货币与特定交易所联系起来。因此，如果通过混币服务转移，加密货币无法被追踪。

比特币混币器（tumbler和mixer），是可以混淆比特币转移踪迹的替代技术。尽管它们都实现了同样的作用，比特币tumbler服务的是那些希望相信第三方的人，而比特币mixer服务的是那些不相信任何人的人。

BitMix是一个比特币tumbler和mixer应用程序，它通过自己的系统提供匿名交易，利用BTC固有的匿名功能，使比特币难以追踪。

另一方面，许多工具通过将公开的区块链数据与威胁行动者的已知地址结合起来，来追踪该加密货币的使用情况，并对这些信息进行评估，以确定洗钱交易以及货币互换和混币器的使用情况。