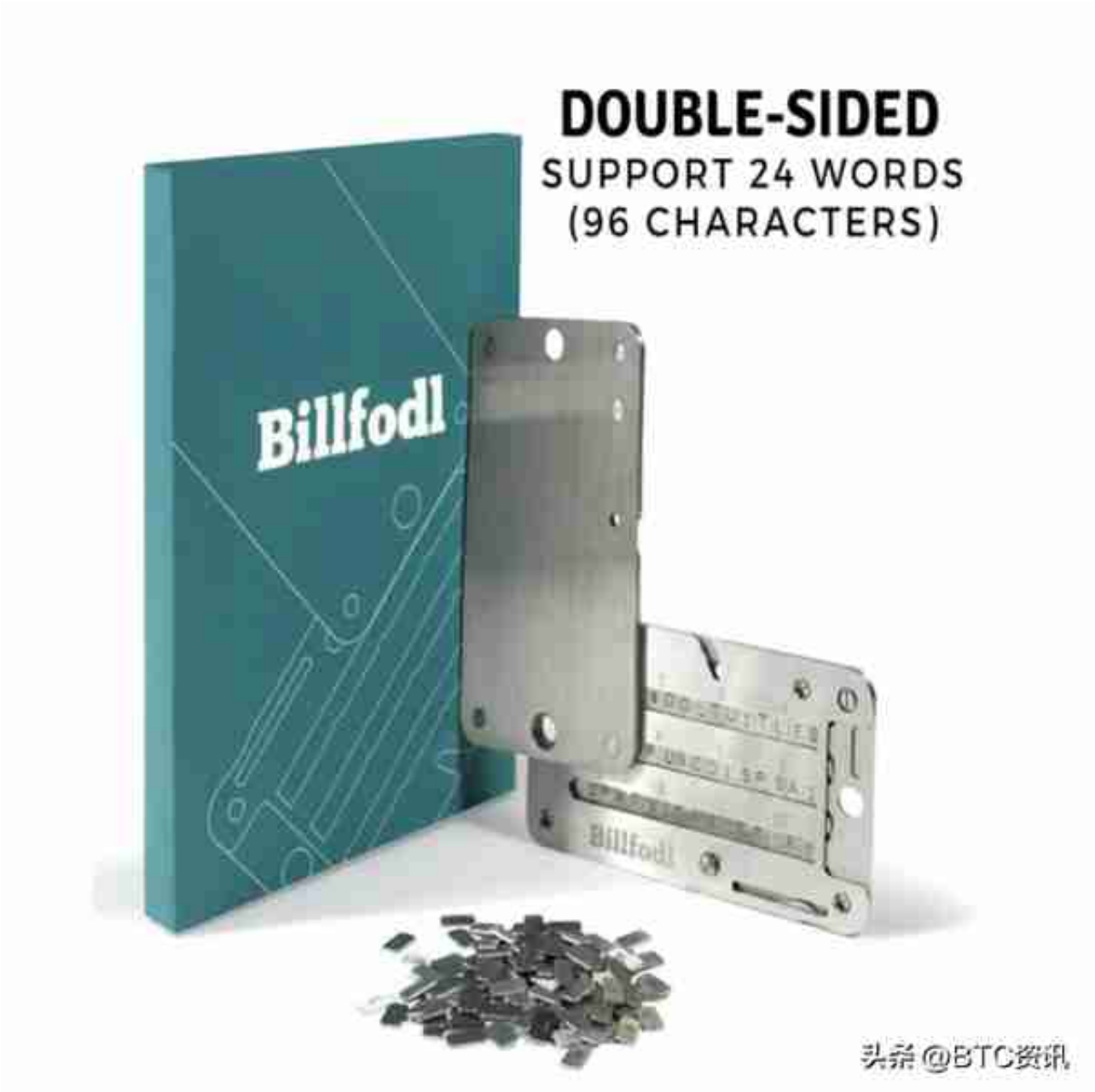
比特币钱包可以是硬件产品，也可以是在移动设备、网络或应用程序上运行的软件。一些最流行的比特币硬件钱包包括Trezor 和
Ledger设备，而其他流行的比特币钱包包括移动应用程序Blue
Wallet和桌面应用程序Wasabi Wallet。

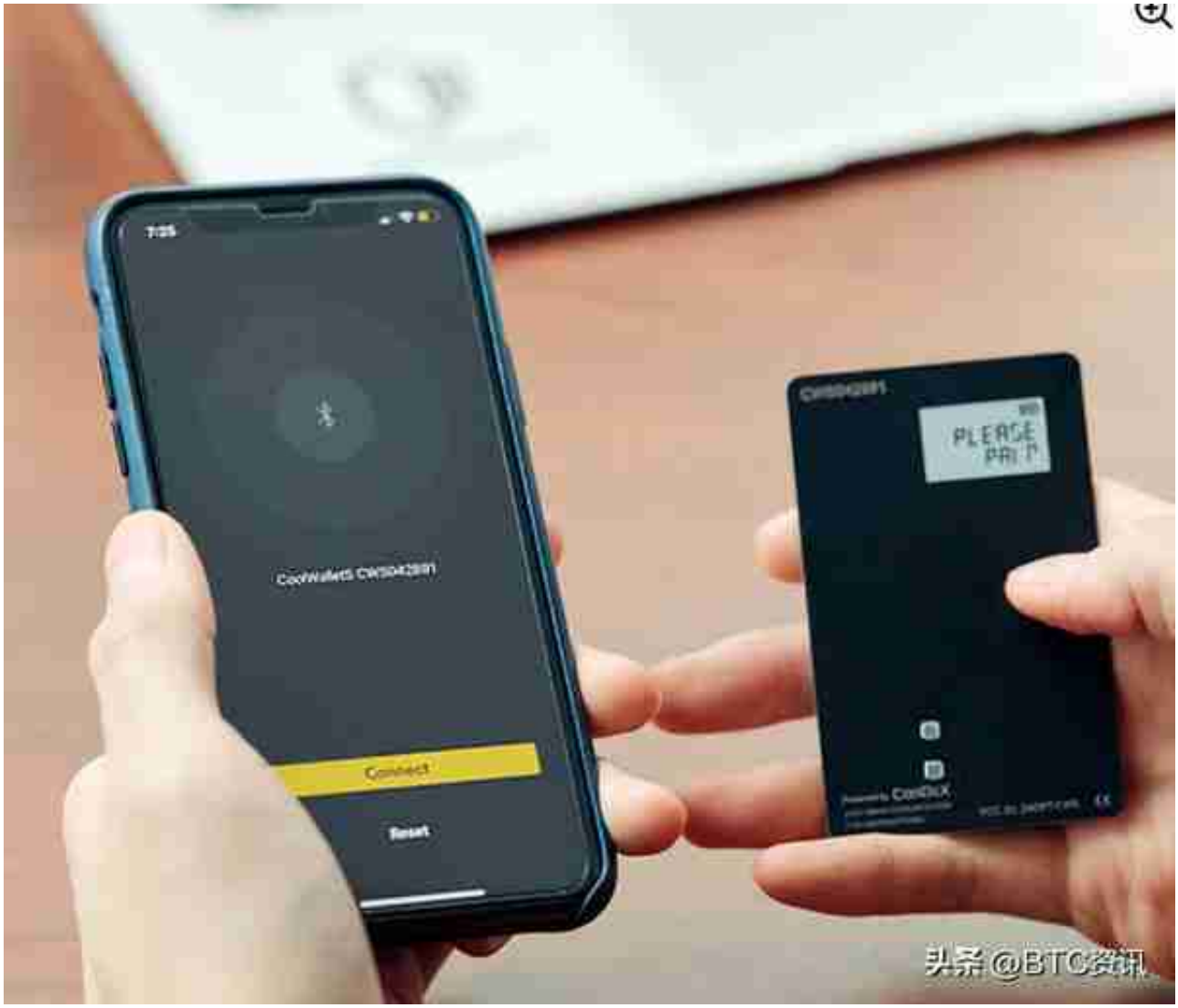


Billfodl
产品可以使加密私钥或恢复种子比写在纸上更安全，因为纸很容易被火或水损坏。

每个比特币地址都有两个密钥：“公钥”和“私钥”。比特币地址来源于公钥，这些比特币地址是共享的。将其想象成与某人共享您的电子邮件地址：他们可以向您

发送电子邮件，但无法进入您的收件箱阅读您的邮件。同样，没有人可以使用公钥进入钱包并从中取出比特币；它只能用于发送比特币。因此，分享是安全的。

另一方面，私钥代表访问属于特定比特币地址的比特币的能力。这是需要放在安全地方的钥匙。



CoolWallet S 硬件钱包通过蓝牙连接到 CoolBit X Crypto 应用程序 (iOS/Android)。

许多人认为硬件钱包（包括我们硬件商店出售的各种产品）是保护比特币所有权的最安全方式。顾名思义，这些钱包采用物理设备的形式，通过加密所有信息来保护用户的密钥，并通过密码或助记词授予用户访问权限。

硬件钱包最重要的品质是对您私钥的物理保护，而不是在计算机上保护它们。这就是使它们比其他任何类型的钱包都更安全的原因。

通过从连接互联网的计算机中删除这些密钥，黑客或恶意程序极不可能窃取您的私钥。所有优秀的硬件钱包都会在钱包内生成密钥以避免此类风险。

如果您在计算机和一张纸上都有您的私钥副本，那么与该密钥相关联的比特币的安全性取决于最薄弱的环节；如果私钥从一个位置被盗，则与该密钥关联的比特币在其他所有实例中都将消失。如果您在计算机和一张纸上都有私钥的副本，则与密钥的安全取决于最薄弱的环节；如果私钥从一个位置被盗，那么在其他所有情况下，与该密钥相关联的比特币的访问权限都会消失。

顾名思义，这种纸钱包是印在纸上的副本。具体来说，这些类型的钱包有一个私钥、一个比特币地址和一个代表每一个的二维码，打印在纸上以便于查看。由于安全生成密钥的挑战，通常不建议使用这种保护比特币安全的方法。例如，如果用户想要创建一个纸钱包，他们需要采取额外的预防措施，以确保生成密钥的计算机没有感染任何病毒。

软件钱包