人生最悲哀的事莫过于：人死了，钱还没有花完，更悲哀的是人还活着，钱已经花完了。

有一群人的经历比上面还要悲哀：钱存得好好的，管钱的人却死了，存的钱将永远无法取出。

私钥丢失的悲剧

加拿大加密货币交易平台QuadrgaCX的创始人Gerald COtten，在去印度旅行时因意外去世，这个交易平台的私钥只有创始人自己知道，钱包里价值上亿美元的加密货币，随着创始人的逝去将彻底被“上锁”，永远也拿不出来。

类似这样的悲剧还有很多，高晓松曾在自己的微博上发布过这样一段话，在网上流传甚广。

虽然不知道真假，但类似的因为忘记密码而损失财产的事是确实存在的。有一个用户提到，他的姐夫在早期就收购了大量比特币，然而随着他的自杀，妻子和6个月大的孩子急需用钱，家人在他的电脑上能找到他的账户，但没有找回私钥的方法，可以说比高晓松微博那个故事还要悲惨了。

这样的悲剧是否可以避免呢？

在区块链里，只认私钥不认人

去中心化的比特币交易机制中，核心就是通过不对称加密，将公钥和私钥分别分配给付款人和接受比特币的人。正因为如此，系统才能够在没有中央银行的情况下处理大笔交易，因为每次交易都通过使用公钥和私钥实现从一个钱包到另一个钱包进行身份验证。然而私钥只掌握在用户自己手中，如果你没有私钥，谁也无法访问你的比特币。

私钥丢失问题，其实有解

我们常见的钱包是一把私钥对应一个钱包地址，适用于公司的HD钱包是一把主私钥对应N个地址，知名微博@比特派钱包曾发文称大额资产丢失其实可以通过“多重签名”的功能来解决。

多重签名技术可以根据需求定制其所需的密钥组合，比如2/3,3/5,4/7等等。最常见的是2/3的多重签名，即通过3把不同的私钥生成一个多重签名地址，需要其中的2把钥匙才能动用这个地址里的币。

多重签名的好处不言而喻，即便其中一把私钥丢失或是被黑客盗取了，地址里的币也还是安全的且还可以转出来，多重签名还可以三人签名，也可以设置资产转移需要几人同时签名等，来实现对资产的个性化控制。

然而Quadrigacx创始人并没有这么做，绝大多数交易的财产都在冷钱包存储着，只有少部分在热钱包中。现在，这家交易所得用户们只能眼睁睁的看着自己的数字加密货币就在交易所里存着，但是这辈子都拿不到属于自己的加密货币资产了。

虽然某些主流的钱包软件已经支持多重签名，但还是有一定的操作门槛。对于普通人而言，他们大多数认为把比特币存在交易平台是最安全的场所，但并不为然，交易平台也有可能会被黑客入侵，导致资产丢失。只有在钱包中才是存放比特币最佳安全的场所。

（作者：曲速未来安全区，内容来自链得得内容开放平台“得得号”；本文仅代表作者观点，不代表链得得官方立场）