

3月27日，据巴基斯坦当地新闻刊物《黎明报》报道，拉哈尔警方破获了一起绑架案。在这起绑架案中，绑匪要求受害人家属用比特币支付赎金。

令人意想不到的是，在这起案件中，有两名绑匪竟然是警察，他们甚至曾经还担任过高级法院法官的警卫。另外还有两名绑匪是比特币交易员，据负责此案件的警察所言，这两名交易员在这起绑架案的赎金交付过程中起了关键作用。

利用身份便利，以比特币为工具来从事非法活动似乎已经变得轻而易举。比特币自问世以来就饱受争议，它在保护人们隐私，为全球汇款带来便利的同时，也在很大程度上降低了非法交易的成本和风险，提高了全球犯罪率。

2018年1月的一份研究报告称，近一半的比特币交易是非法交易。有数据显示，大约四分之一的比特币用户和近一半的比特币交易与非法活动有关。

除了此次巴基斯坦发生的这起绑架事件之外，以比特币为工具从事犯罪活动的例子数不胜数。2017年5月12日，一个名为“想哭”(WannaCry)的勒索软件，在短短数天，就让全球99个国家和地区超过7.5万台电脑遭遇病毒攻击。黑客利用一种锁死电脑的恶意软件“绑架”电脑用户的重要文档，要求用户用比特币支付赎金。黑客这一行为恰恰就是看中了比特币在支付转账时的全球化、去中心化和匿名性等优势。

还有一些暗网中的犯罪，像洗钱、走私、资产非法转移、逃避外汇管制等也都是利用了比特币在支付方面的强大功能。

据悉，这起案件是巴基斯坦国内发生的第一起此类案件，巴基斯坦当局十分担心这起案件的发生可能会成为一个先例，在以后的时间里诱发其他此类案件的发生。

但令拉哈尔警方疑惑不解的是，比特币使用的是一个完全公开的账簿，在Monero等加密软件中没有额外的隐私增强功能，因此犯罪分子选择用它来作为赎金的支付方式似乎是不智之举。

看似万能的比特币其设计原理究竟是什么呢？

比特币 (BitCoin) 的概念最初由中本聪在2009年提出，它是一种P2P形式的数字

货币。点对点的传输意味着它是一个去中心化的支付系统。

与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节的安全性。

P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。

比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。该货币系统曾在4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个。

比特币的设计原理注定它会存在弊端，但其优势却更明显

首先，比特币总量固定。这一点使得它在具有极强的稀缺性的同时也极大的降低了通货膨胀发生的可能性。另外用比特币交易降低了传统纸币发行、流通的高昂成本，提升经济交易活动的便利性和透明度，减少洗钱、逃漏税等犯罪，提升央行对货币供给和流通的控制力，可以更好地支持经济和社会的发展。

其次，任何可以访问互联网的人都可以免费拥有比特币账户。与现金一样，开设比特币账户不需要提交任何个人信息，因此无需担心私人信息泄露。

最后，比特币流通不受国界限制，用户转账的成本相对较低。这一点对于那些只能享受传统银行有限服务的个人来说非常重要。那些没有银行账户或享受到的银行服务不足的个人及家庭，可以通过比特币以及当前快速发展的全套去中心化金融体系去摆脱高成本的账单支付、信用卡费用、支票兑现服务和发薪日贷款。尤其是对于那些生活在高通胀国家的贫困人口而言，获得比特币这一抵抗本国货币政策的工具，这种好处可能会更大。

不可否认，近几年与比特币相关的犯罪事件发生的频率在逐渐提高，很多国家也在不断加强对数字货币的监管，但谁来监管、如何监管，成为考验各国政府的难题。由于缺乏有效的监管措施，不少国家政府开始对数字货币采取抵制措施。

但究其根本，我们会发现，技术本身并没有任何问题，比特币设计的初衷完全是为了造福人类。所以我们与其花尽心思去思考如何阻止比特币交易，还不如花时间去想想怎样完善监管体系，将人性放在法律的框架之中。因为在未来，数字货币广泛应用的大势一旦来临，它就会像当初的互联网时代一样，谁也无法阻挡。