摘要： 比特币的隐私保护做得足够好吗？

作者 | 李火华出品 | 白话区块链

近年来，随着网络技术的发展，个人隐私数据被泄漏的事件层出不穷。

比特币因为其匿名性
，受到了一部分重视隐私的用户的喜爱；
但在另一部分人眼里，比特币的
匿名性仍然很弱，
因为比特币的所有交易人人可查询、追踪，通过数据挖掘，标记“污染地址”，仍有可能找出某个比特币地址背后对应的所有者。

事实上，美国FBI就锁定了很多与非法活动有关联的比特币地址，通过数据挖掘逮捕了不少犯罪份子。著名的“门头沟事件”发生之后，门头沟用户之一、软件工程师Nilsson就通过追踪被盗的比特币流向，最后成功锁定了隐匿数年的案犯。

为了进一步增强加密货币的匿名性，保护使用者的隐私，一种新类别的Token诞生了——匿名币。

目前，比较有名的、经过市场较长时期检验的匿名币有Monero（XMR，门罗币）、DASH（达世币）以及ZCash（ZEC，大零币）。

下面，简单介绍下它们是如何做到自身的匿名性强于比特币的匿名性。

一、Monero（XMR，门罗币）

从市值上看，门罗币是目前最受欢迎的匿名币。门罗币保护用户隐私的手段主要有：1、通过环交易，保护发送者；2、通过隐藏地址，保护接受者；3、使用环签名算法，隐藏交易金额。

也就是说，
在区块链浏览器上，门罗币的交易数据是不公开的，没有人能知道在这之前，你的门罗币经历过哪些交易，也无法查询到此刻你的门罗币转给了谁。

值得一提的是，普通电脑也能参与门罗币挖矿。
门罗币使用的是CryptoNight算法，用CPU挖矿比用GPU挖矿效率还高，因此不需要专门的专业矿机，普通的电脑也可以进行门罗币挖矿。

二、DASH（达世币）

达世币使用了一种名为“混币”的技术来增强匿名性。“混币”技术，简单来说，就是将来自不同发币地址的币混合起来，然后再发送出去。这样就切断了发送人地址与接受人地址的一一对应关系，从而更好地保护隐私；缺陷是相比于门罗币，达世币的交易金额可以查询到。

三、ZCash（ZEC，大零币）

大零币使用了Zk-SNARKs，或者说零知识证明
，一种可以在不知道交易本身的情况下验证交易的证明系统。零知识证明被《麻省理工科技评论》评为“2018年10大全球突破性科技技术”之一，白话区块链专门写过《价格炒到4万多的匿名币，如何实现匿名交易？》进行介绍，这里不再赘述。

著名的匿名币，除了上文介绍的Monero（XMR，门罗币）、DASH（达世币）以及ZCash（ZEC，大零币）外，还有后起之秀、前段时间很火的Grin和Beam。

莱特币创始人李启威说：“可互换性是比特币和莱特币唯一缺少的健全货币属性。既然规模的争论已经过去了，
下一个战场将是可替换性和隐私
”。也就是说，作为比特币新技术的先行者，莱特币接下去也将会增强用户的隐私保护。

你认为
比特币还需要
进一步加强用户的隐私保护，增强匿名性吗？为什么？欢迎在文末留言。

本文为旧文重发，内容略作调整

——End——

『声明：本系列内容仅供区块链科普入门学习，不构成任何投资意见或建议。如有任何错漏，敬请留言指出。』

作者：白话区块链；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
凡“得得号”文章，原创性和内容的真实性由投稿人保证，如果稿件因抄袭、作假等行为导致的法律后果，由投稿人本人

负责
得得号平台发布文章，如有侵权、违规及其他不当言论内容，请广大读者监督，一经证实，平台会立即下线。如遇文章内容问题，请发送至邮箱：linggeqi@chaindd.com