区块链充斥着快速获得收益和轻松入场的承诺。所以在进入加密货币市场之前，有必要弄清你所持有的加密货币，是否精心策划的骗局一部分，目的在于骗取你的资金。

一般来说，在网上搜索相关资讯，常常会看见有安全专家建议——用户做自己的研究，但没有详细说明如何操作。

其实规避区块链常见的欺诈者和骗子，有8种简单但有效的分辨方法，可以帮助您确定加密货币是否值得，或者它是否具有诈骗的元素。

本文使用了以太坊网络作为例子，建立在其他链上的货币所使用的方法大同小异。

1、在 Etherscan 上验证校验码

访问 Etherscan 并检查加密货币项目的代码。

如果代码未经验证，您可能正遇上一个骗局。诈骗者之所以不透露他们的代码，往往因为该项目有问题或 BUG，甚至存在某些不可告人的目的。

2、 检查 Etherscan 评论区

如果有人留言称某一加密货币项目是骗局，那么有 99% 的可能是骗局。如果您也曾经受到某项目的欺骗，请不要犹豫发表评论，将信息分享给大众。

另外，移步 Etherscan 评论区，浏览他人对项目的看法，也是必不可少的步骤。

3、搜索加密货币项目的官网地址

如果您进行互联网搜索，但找不到明确的主页、“白皮书”或明显的加密货币用途，则可能是骗局。

4、查看 DappRadar 黑名单

DappRadar
罗列了许多加密货币骗局项目，如果其一项目在该列表中，就一定是骗局。

5、在加密浏览器中查看详情

如果您在 CoinGecko 或DappRadar
的加密浏览器（或类似的加密货币价格跟踪器）
上找不到该项目，那么该项目可能是一个骗局。

如果项目在加密浏览器上，而您又看到这样的警告通知，请谨慎操作：

而且出于验证目的，所有合法项目都与加密浏览器共享信息。

6、检查加密货币有多少交易所托管

如果加密货币项目只在几个分散的交易所（dex）交易，那么几乎可以肯定这是一个骗局。

7、检查加密货币余额池中的流动性数量

在 Uniswap V2 或其他 dex 等平台上检查加密货币的流动性非常容易。

流动性是指锁定在智能合约中的加密货币数量或代币数量，以使人们能够在去中心化交易所买卖资产。

如果流动性低于 100,000 美元或以显着速度下降，您可能正在碰上一个骗局。

使用 dex 时，请确保检查其它基本的链上活动：

- 交易量——被交换的代币数量，通常以美元为单位；
- 交易计数——代币交换的数量；
- 与智能合约交互的唯一活跃钱包——使用 Web3 钱包连接到 dex 的用户数量；

如果其中任何一个看起来不寻常，请进行更多挖掘。

8、检查第三方分析工具

以下是一些加密货币分析工具：

- 气味测试——这会对项目进行自动审计。其 100 分越低，该项目就越有可能是骗局。
- 这是蜜罐骗局吗？蜜罐是一种智能合约，其中故意插入了明显的编程缺陷。当攻击者试图利用该漏洞时，另一段隐藏代码被激活并从本质上攻击攻击者。无论您是否打算成为加密黑客，都应始终避免使用蜜罐。
- 学习 DEXtools 的基础知识。它记录实时加密货币价格，并将帮助您实时评估项目的真实价值。

诈骗者将永远存在，无论是在区块链上还是在现实世界中。遵循这些提示，您应该避免使用旨在骗取您钱财的虚假加密货币。

本文所阐述的观点仅供参考，不构成任何投资建议。每一个投资和交易动作都涉及风险，您应该在做出决定时进行自己的研究。

感谢您的支持与阅读，您的每一次点赞或转发，就是我继续前进的动力。同时也欢迎大家关注我的公众号——云图投研，进入社群与众多区块链爱好者一起学习进步！