如何检查代币是否存在诈骗并增加实现盈利的机会？

作者：GeekTop，Web3见闻

现代区块链充满了快速赚钱和轻松赚钱的承诺。然而，了解你持有的代币是否是精心策划的骗局的一部分至关重要，该骗局旨在骗取你辛苦赚来的钱。随着成千上万种不同的 meme 币定期发行，确定代币是否安全且不受诈骗变得越来越困难。

在本文中，我们将探讨检查代币和项目是否存在欺诈的有效方法。这些方法可以帮助您避免欺诈并增加实现盈利增长的机会！

要检查代币的合法性，您始终可以从最容易获得的方法开始，例如在 Google 和 Twitter 上搜索。这包括研究代币及其团队、检查危险信号或警告信号，以及寻找可靠的信息来源，例如官方网站、新闻文章和经过验证的社交媒体帐户。

### 在 Twitter 和 Telegram 上查看代币

经过验证的 Twitter 帐户通常可以帮助证明项目的合法性。此外，您可以参与代币讨论，以了解社区的观点和意见。

谨慎对待社交媒体关注者众多但活动很少的项目。垃圾账户的自动评论也应引起关注。如果所有评论都是“这是一个很棒的项目”和“月球即将到来”，就要小心了。

要在 Twitter 上查看代币信息，请在搜索栏中输入：$TICKER。

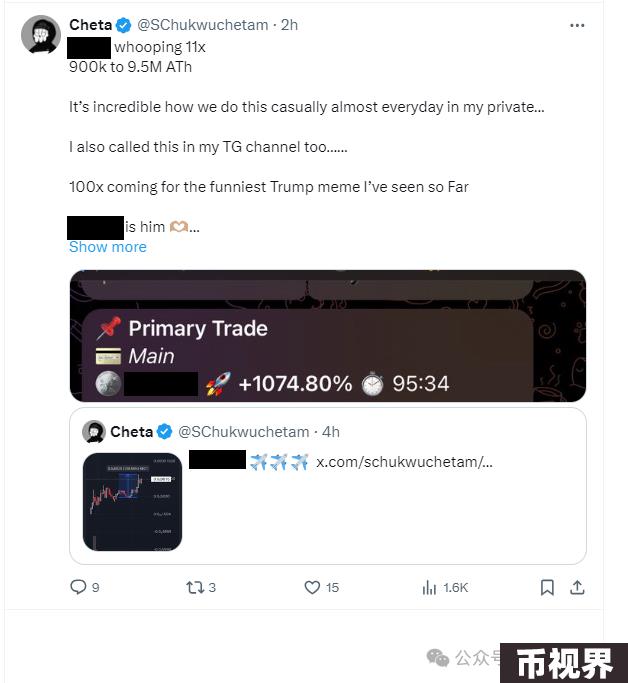


或者使用#TOKEN\_NAME 查找有关该项目的更多信息：



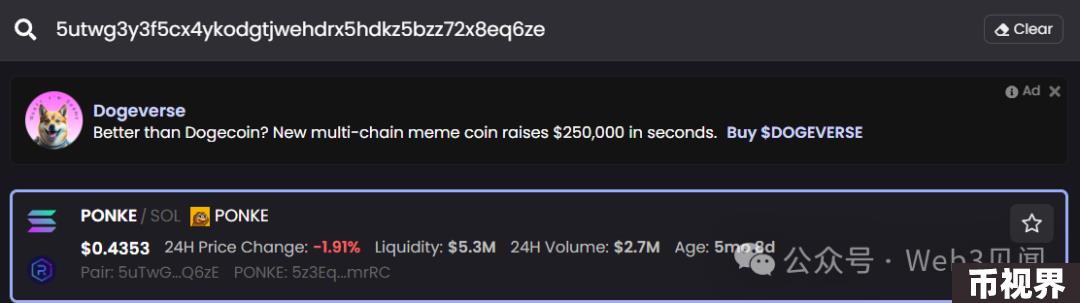
如果代币是最近推出的，请先检查有关代币的第一条新闻。为此，请在搜索栏中输入 $TICKER 并滚动到提要底部。

通常，有关代币的第一个新闻来自新闻机器人或有影响力的人，例如以下情况：

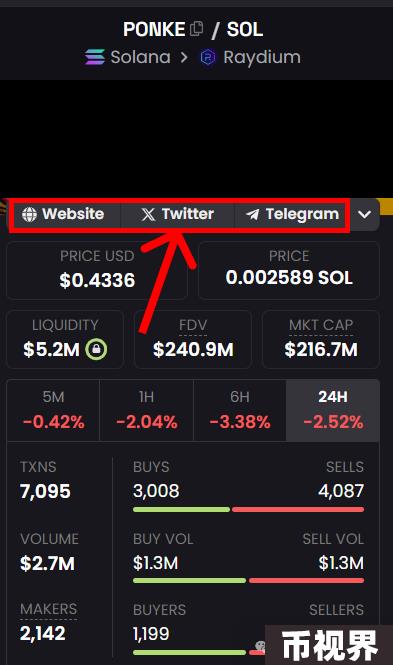


一个重要的因素是研究该项目在 Twitter 上的简介。如果它发布重复的新闻和统一的购买呼吁，那么骗局的可能性就会增加。

要在 Twitter 上查找代币项目，请转到 DexScreener 并插入代币的合约（例如，Ponke - 非财务建议）：



在右上角，您将看到该项目的网站、Twitter 和 Telegram。通过访问这些链接，您可以研究该项目：



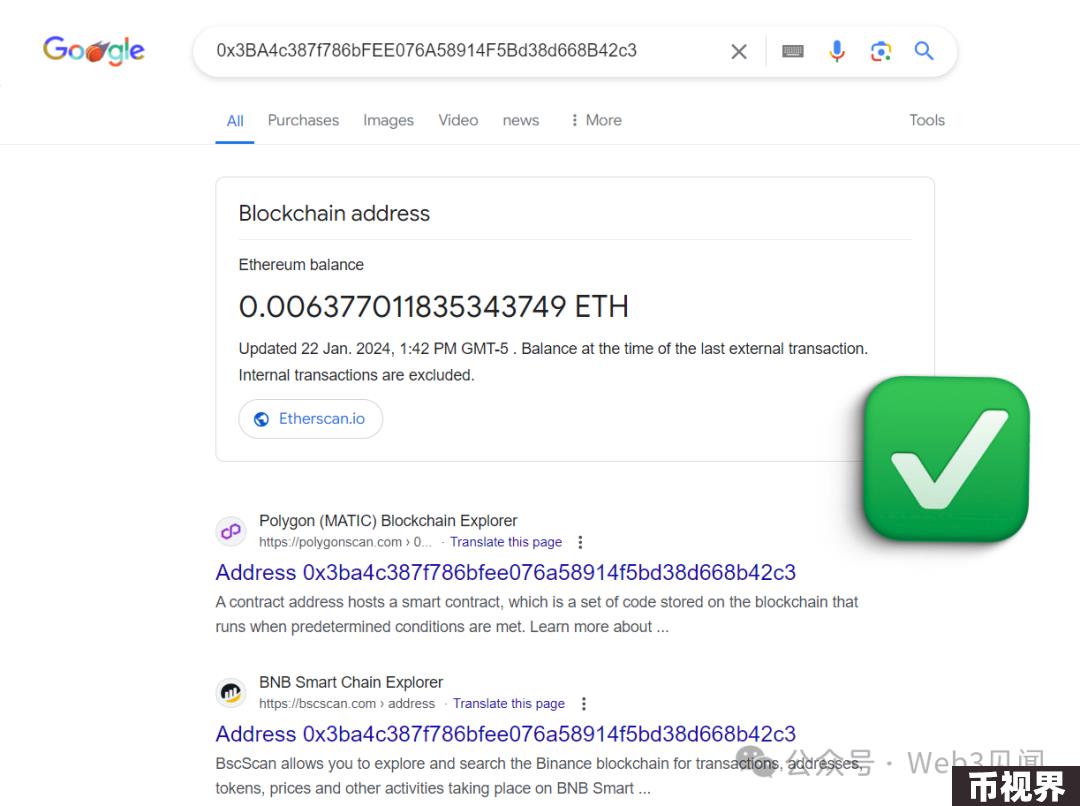
如果您找不到任何项目链接（没有网站、Twitter 或 Telegram），这是一个明显的危险信号，表明诈骗的可能性较高。

在分析项目的 Telegram 时，要注意社区对项目的态度。如果社区强烈相信并支持该项目，那么这对潜在的短期增长来说是一个积极的信号。

### 在 Google 搜索中检查令牌地址

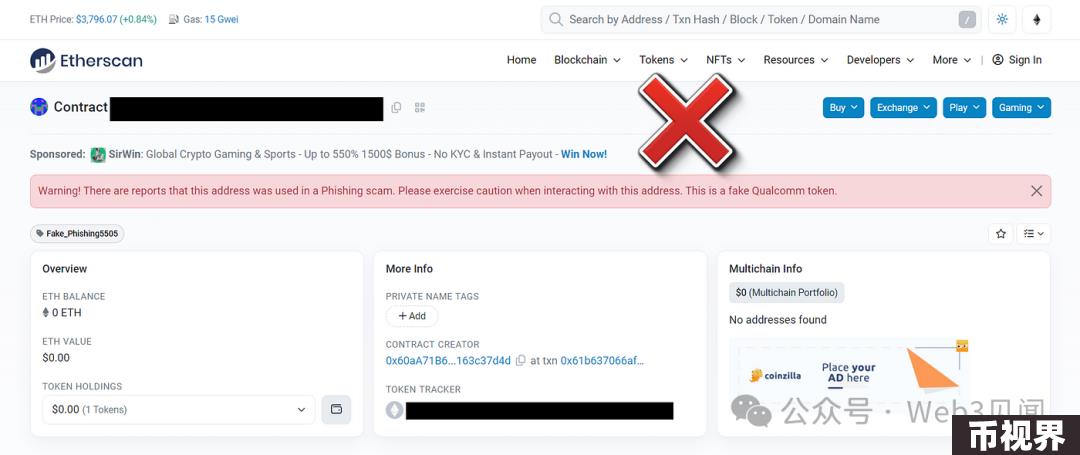
如果您在互联网上搜索，却找不到明确的主页、“白皮书”或代币的明显用途，那么这很可能是一个骗局。当您搜索代币地址时，您应该很容易找到区块浏览器、官方网站和白皮书的链接。如果没有，请将其视为危险信号。

另外，请注意，Google 广告通常是欺诈网站的免费区域。切勿点击 Google 搜索结果顶部的广告。务必确保您访问的是官方网站，以避免点击钱包清理器或其他黑客软件。



### 在 Explorer 中检查

访问所选链的区块浏览器，查看源代码是否已验证。例如，在以太坊的区块浏览器Etherscan上，它看起来像这样。下面显示的代码未经验证，这应该是一个明显的警告信号。如果代码未经验证，您可能正在处理骗局。



如果您想检查部署在另一个网络上的令牌，请使用以下浏览器：

基地 —https://basescan.org/

Solana——https://solscan.io/

Ton —https://tonscan.org/

BSC —https://bscscan.com/

为什么诈骗者不验证他们的代码？

因为一旦合约的源代码公开，每个人都可以理解合约背后的意图。然后他们会看到一个荒谬的税收制度或开发人员窃取你所有代币的方法。

### 查看评论部分

这很简单，但各种区块浏览器通常都有评论部分。在大多数情况下，没有评论，但如果该项目是一个骗局，你很可能会在评论部分发现一群愤怒的暴徒。所以一定要检查一下。如果有人称其为骗局，99% 的情况下，它就是骗局。如果你已成为这种活动的受害者，也不要犹豫留下评论。

分析代币时，可以在此行找到注释部分（Etherscan上的示例），但对于大多数代币来说，它是隐藏的。



### 检查 DappRadar 黑名单

DappRadar 允许社区帮助识别诈骗代币。一旦发现，你可以将其添加到GitHub 上的代币黑名单中。

另外，如果你正在研究代币，你可以检查一下黑名单，看看你的代币是否在名单上。如果代币地址在名单上，那么这个代币肯定是一个骗局。

### 检查代币在多少家交易所上市

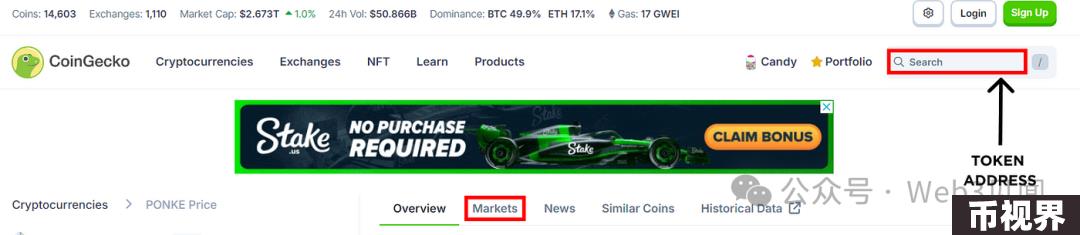
如果代币仅在少数几个去中心化交易所(DEX)上交易，那么几乎可以肯定是骗局。在中心化交易所上市需要 KYC 和额外的信任，交易所越大，上市代币的声誉就越好。

这是否意味着仅在去中心化交易所上市的代币就一定是骗局？不。有些项目不需要大量的交易量，其他项目可能只向 Web3 用户提供代币，而不向代币交易者提供。

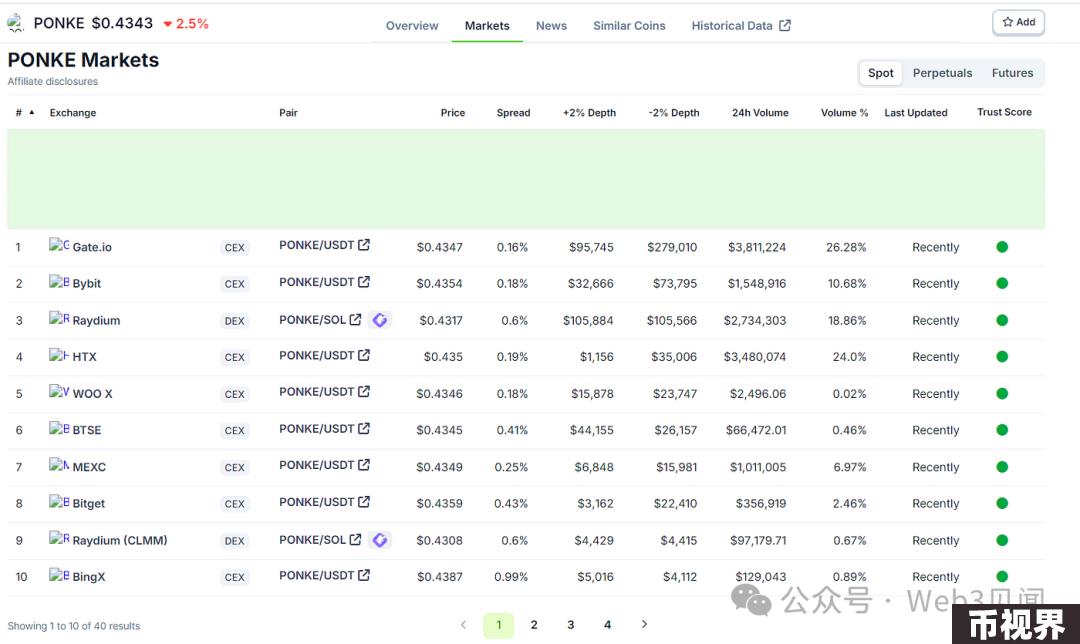
由于大多数 meme 币在出现在 CEX 之前都显示出显着的涨幅，因此在 CEX 上拥有代币并不是代币分析的严格标准。

然而，仅在去中心化交易所上市的加密货币代表着更高风险的投资。

要查找哪些交易所列出该代币，请转到Coingecko，在“搜索”栏中输入代币地址，然后选择“市场”：



如果代币至少在一家 CEX 上，则为绿色信号。在这种情况下，代币在 CEX 上列出：Bybit、BingX、Bitget、Gate.io：

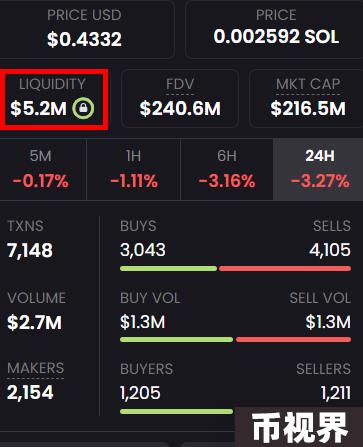


### 检查代币的流动性量

在投资代币之前，您可以检查总体需求和可用流动性。在Uniswap V2或其他去中心化交易所等平台上检查代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或代币数量，这些合约允许人们通过（去中心化）交易所买卖资产。如果流动性低于 100,000 美元或大幅下降，则您很可能正在遭遇骗局。

您可以在知名的DexScreener上查看流动性量，进入代币合约后，在右侧中间部分可以看到流动性量：



如果流动性量旁边出现绿色圆圈内的锁定符号，则表示流动性已被锁定——这是该项目的另一个绿色标志。

此外，考虑完全稀释估值 (FDV) 或市值也很重要。这些数字越大，代币价格上涨所需的购买量就越大。

此类代币的良好指标是流动性量从 100 万美元起、代币年龄超过 2 天，以及流动性/FDV 比率约为 1:10。

### 检查第三方分析工具

以下是一些 token 分析工具：

嗅觉测试——对代币的自动审核。其得分（满分 100 分）越低，代币是骗局的可能性就越大。

检查蜜罐上的代币。蜜罐是故意制造明显软件缺陷的智能合约。当攻击者试图利用该漏洞时，会触发另一段隐藏代码，本质上就是攻击攻击者。无论您是否打算成为加密黑客，都应始终避免使用蜜罐。

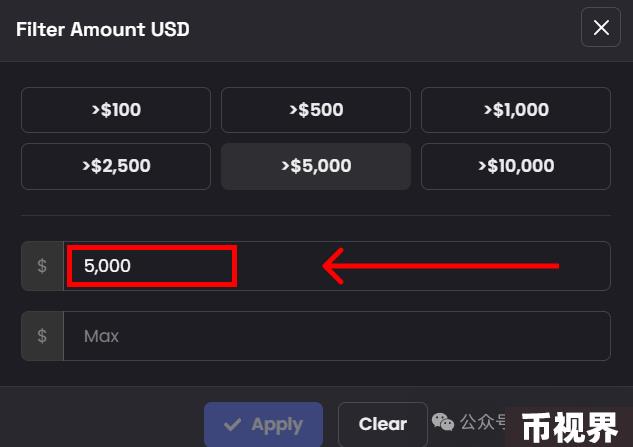
### 了解DEXScreener的基础知识

它记录当前的代币价格并帮助您实时评估代币的真实价值以及识别主要持有者。

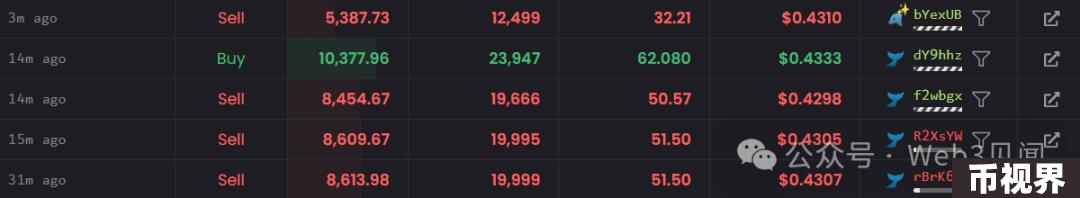
例如，要识别最近以 5,000 美元以上购买代币的用户，请单击 DEXScreener 底部的“美元”：



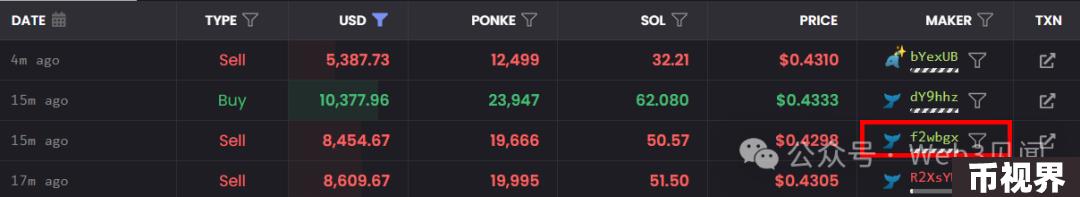
输入金额 5,000 美元（可选，您可以指定最高代币购买金额）并按“Enter”或“Apply”：



此后，所有最近以 5,000 美元或以上价格购买代币的买家都将显示：



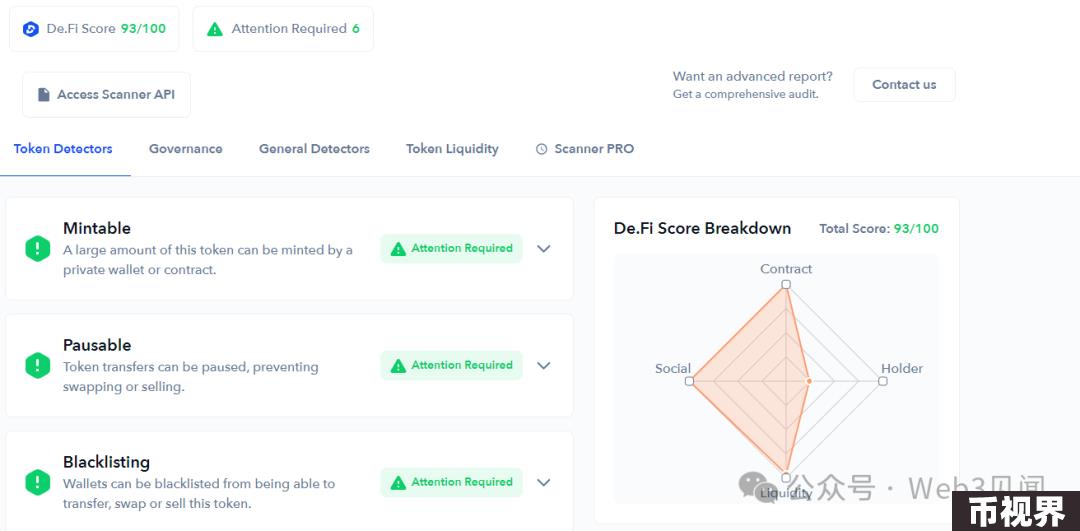
您还可以查看某些钱包的购买区域。为此，请单击所需钱包旁边的杯子图标，然后在钱包图表上查看所有购买区域和代币购买级别：





### 使用 De.Fi 防病毒软件分析代币

De.Fi是一个最近向其社区分发空投的项目，它通过根据各种参数评估代币合约并为代币提供估计的安全余额来充当防病毒软件：

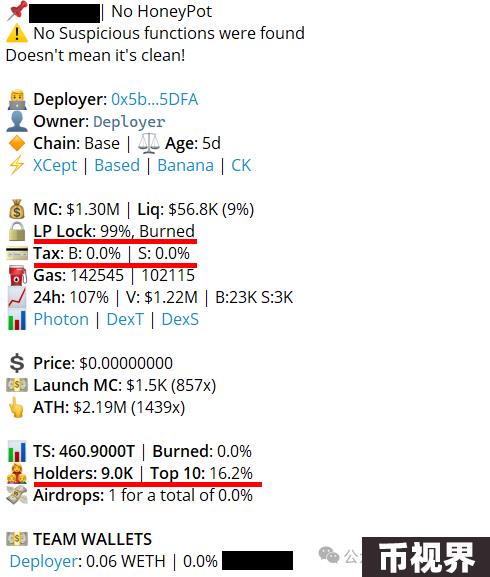


### 使用TTF Bot

这款多功能机器人可以快速自动分析代币，这对代币猎人来说非常方便。特别注意锁定或销毁的流动性数量。如果流动性被销毁，则是一个绿色信号。

此外，请注意代币的税收规模。如果税收为零，则这是肯定的事实。

另外，还需关注持有者的数量及其所占的供应量：



如果前 10 名持有者持有超过 30-50％ 的代币供应量，则遭遇骗局的可能性更高。

### 结论

通过使用上述分析工具，您可以学会如何避免诈骗代币并从合法代币中获利。但是，请务必记住进行自己的研究 (DYOR)。