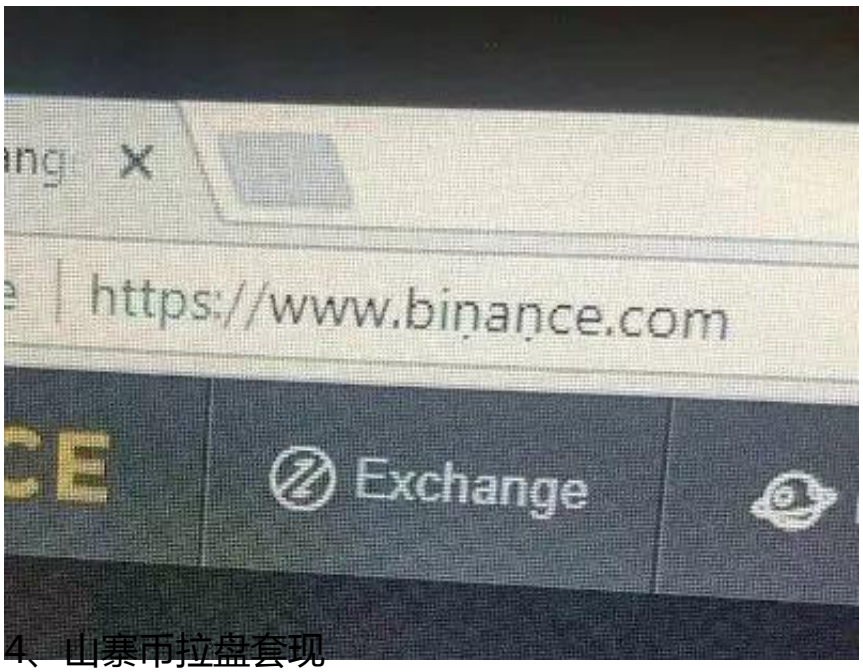
另一个规模更大的1CO骗局是Centra，该项目筹集了3200万美元，得到了名人Floyd Mayweather和DJ Khaled的支持。2018年4月，该公司两名创始人被捕。代币价格走势和Confido一模一样，在消息传开后迅速下跌。

2、冒充知名财经博主或大V行骗

Facebook、Telegram和Twitter都假装自己是Vitalik，马斯克或Anddreas等超级明星，在群里或给用户发送加密币作为礼物，这些完全是骗局。无论什么时候你看到“发送1个eth到这个地址，那么你会赢X次回来”，那一定是骗局。数字货币可以换到钱，没有人会免费给你。典型案例就是马斯克的推特账户被黑客冒名顶替行骗。



4、山寨币拉盘套现

拉盘套现集团将操纵一种不那么受关注的加密货币的价格和数量。一开始，他们通过协调大量交易来抬高价格，然后以高价卖出。在这些群体中有不同的层次，购买价格越高，就越糟糕。典型的是借助财经大V的影响力，欺骗粉丝去高位接盘山寨币。最后拉盘方赚的盆满钵满离场，接盘散户血亏。

5、云挖矿骗局

由于挖矿设备和电力的高成本，云挖矿受到越来越多的人的青睐，这也给了骗子另一种欺骗人的方式。其中一个案例是MiningMax Ponzi scheme，提供云挖矿服务，让人们在两年内每天投资3200美元。会员每推荐一个投资者就能得到200美元。该网站从投资者那里累计诈骗了2.5亿美元。这种骗局识别难度大，比特110建议投资者谨慎参与云挖矿。

6、庞氏骗局

庞氏骗局(Ponzi scheme)是一种投资骗局，利用后来投资者的资金来回报现在的投资者。最臭名昭著的庞氏骗局是Bitconnect。最令人惊讶的是，在从其最大的基金骗局中撤资后，organaizion在过一年里一直活跃。在崩溃附近，Bitconnect市值约20亿美元，币单价约320美元。崩盘后，价格跌至6美元，市值跌至4000万美元。Bitconnect拥有大量追随者，其市场结构与其他成功的传销方案一样，逻辑清晰。因此，如果有一件事是不完美的，那么你应该保持警惕。

7、钓鱼网站广告诈骗用户需要警惕那些将你引向钓鱼网站的广告。在最近的诈骗案件中，在谷歌和Trezor硬件钱包广告投放在Reddit上有很多克隆交换网站广告。一定要保存正确的链接到书签，不要浏览其他类似的网站。Chrome的扩展如Mwtamask也可以帮助避免钓鱼网站。

8、DNS攻击Etherdelta(一种几乎消失的分散式交换)和MyEtherWallet都是DNS攻击的受害者。DNS攻击是通过修改合法网站的DNS记录，将流量从合法网站重定向到虚假网站的过程。所以即使你通过书签浏览网站，你仍然可能被骗。MyEtherWWallet和MyCrypto拥有自己的SSL证书名称。因此，如果SSL证书不匹配或您收到错误警告，请立即退出网站。防御DNS攻击的另一种方法是在您的计算机本地线路下运行MyEtherWallet和MyCrypto。

9、网络钓鱼电子邮件

网络钓鱼电子邮件可以引导用户到虚假网站，然后窃取用户的资金和个人信息。这些电子邮件通常在1C0公开销售的过程中受到欢迎。骗子将访问以前与1C0相关的电子邮件和其他个人信息数据库，从未来的投资者那里窃取资金。