2022年8月8日，美国财政部的海外资产控制办公室（The Office of Foreign Assets Control of the US Department of the Treasury，简称OFAC）的官网显示，将部分与Tornado Cash协议或与之相关的以太坊地址进行交互的地址，放入SDN List(美国特别制定国民名单）。

据悉，如果被加到了这个名单，名单中的人员会根据OFAC管理的各种制裁计划，个人或者相关实体的财产和财产权益会被冻结。

Tornado Cash到底是什么，本次制裁将对Web3.0的匿名战争造成什么影响，今天我们就来讨论一下。

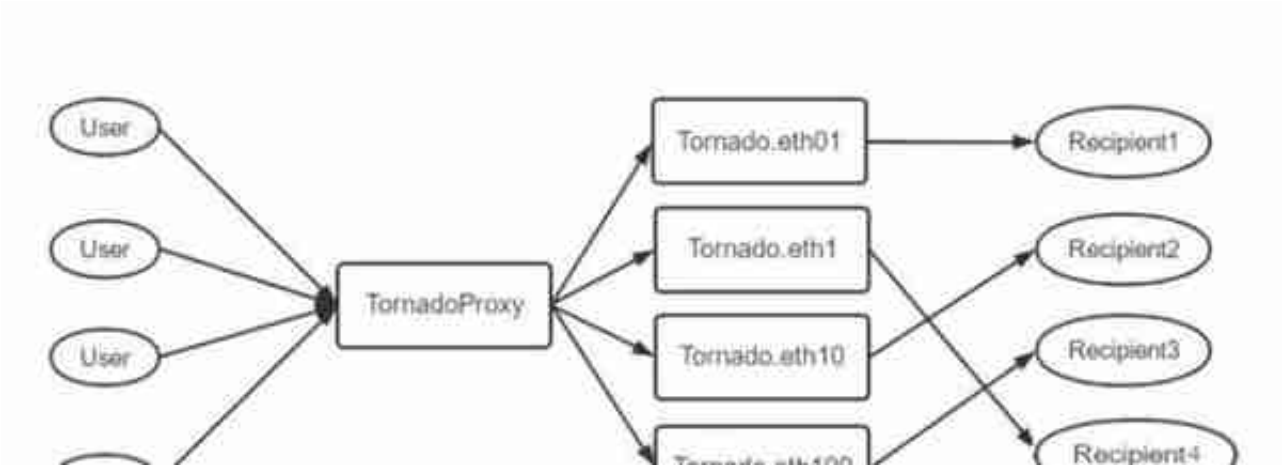
1 加密货币的匿名战争，什么是混币服务和洗钱？

在回答这些问题之前，我们先来了解下混币服务和洗钱。

虚拟货币的交易信息在链上是公开可查的，只要知道一个人的虚拟货币地址，他在链上的所有操作都是清晰可视且可追踪的，在这种情况下，为了解决隐私性和匿名性问题，混币技术诞生了。

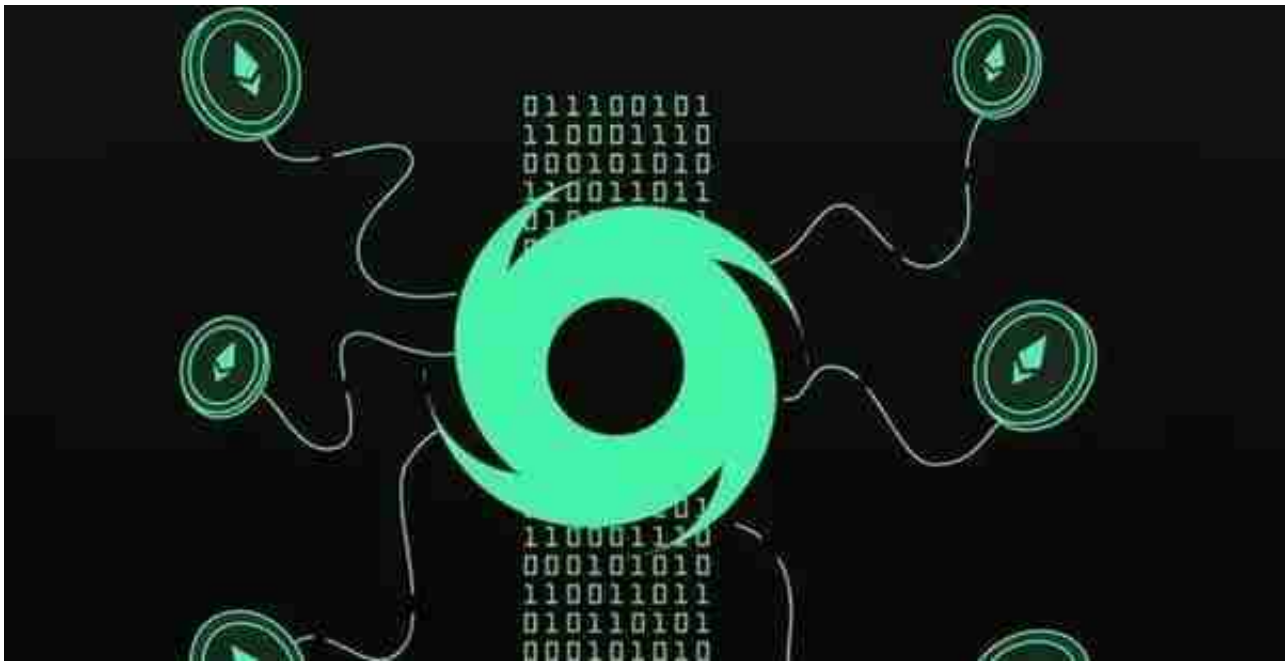
混币（Coin Shuffle） 是一个去中心化的隐私功能，它可以让用户快速高效地与其

他用户的资金进行混合，在现有的用户账户和混币后的新账户之间创建随机的映射关系，从而实现完全匿名。



Tornado Cash
使用智能合约从一个地址接受代币存款，然后用一个全新的地址将资金提取出来。

Tornado
Cash的用户想要将一笔资产进行匿名转移或者混币，先需要将资产转移至Tornado Cash的智能合约上，Tornado Cash给用户一个随机生成的密钥作为凭据，此凭据可以证明你已经执行了存款，但未透露原始地址；取出时只需向Tornado Cash提交之前系统给予的随机密钥，同时用户提交一个新地址后，智能合约会将资产转到新地址中并完成资产的“混币”，这样就无法追溯到该笔交易了。这也是大多数黑客选择Tornado Cash的原因。



2021 年 8 月，比特币混合器 Helix的首席执行官拉里·哈蒙 (Larry Harmon)对涉嫌洗钱 345,468 比特币（当时相当于 3 亿美元）的洗钱指控认罪。同时，经营 Coin Ninja 混合服务的 Harmon 被罚款 6000 万美元。

今年 4 月，美国司法部（DOJ）与德国当局合作，没收了俄罗斯暗网网站 Hydra的服务器， 并对该网站进行了制裁。

可见，美国财政部一直致力于揭露虚拟货币生态系统的犯罪组成部分，例如 Tornado Cash 和 http://Blender.io，网络犯罪分子使用这些工具来进行非法网络活动和犯罪，他们通过混合器、点对点交换器、暗网市场和交易所逃避法律制裁。

4 Web3.0的匿名战争结束了吗？使用混币后资金如何追踪？

虽然该禁令影响 Tornado Cash 的使用，但目前仅限于美国及其公民，使用地址隐藏的用户也可以正常使用 Tornado Cash。

最后要提的是，区块链领域还处于一个探索发展的阶段，当和主权国家政策监管发生碰撞时，必然会受到政策监管
层面的诸多影响。
而借助区块链技术引发的诈骗、洗钱、盗窃、挖矿犯罪等案件频发，对全球的监管系统的风险预判能力提出了更高的要求。

作为一家致力于区块链
安全生态建设的公司，成都链安同时
致力于全链条打击虚拟货币犯罪能力建设体系，提供全链条打击虚拟货币犯罪的服务+产品。

依托协助执法部门破获数百起区块链犯罪案件的经验积累（包括数起进入Tornado的案件），
以案件研判过程为场景
切入打造的契合执法机构办案流程的
虚拟货币案件智能研判平台——链必追。
能为执法机构提供链上线索发现、链上行为刻画、资金追踪溯源、混币穿透、调查取证、判例库等一站式虚拟货币犯罪分析研判技战术能力，解决执法机构面对新型虚拟货币犯罪案件侦破难的痛点问题。如果您在案件侦办过程中，遇到资金追踪、洗钱活动技术协助需求，可直接联系我们（仅限执法人员）。