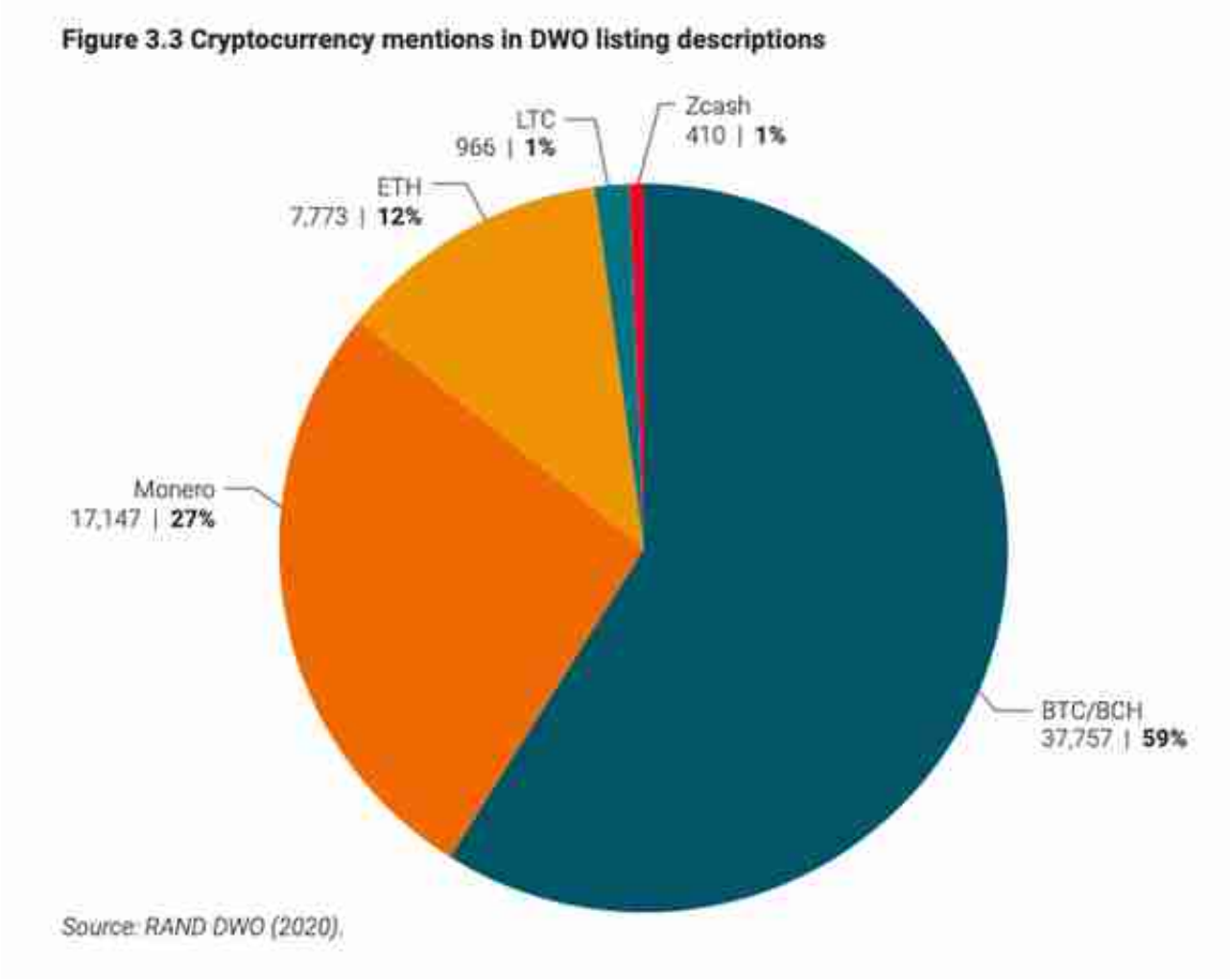


资料来源：Rand Corporation

在现有的 Zcash Token 中，只有不到 10% 的 Token
是受保护或私有的。与智能合约平台相比，用户和交易量并没有太大的增长。

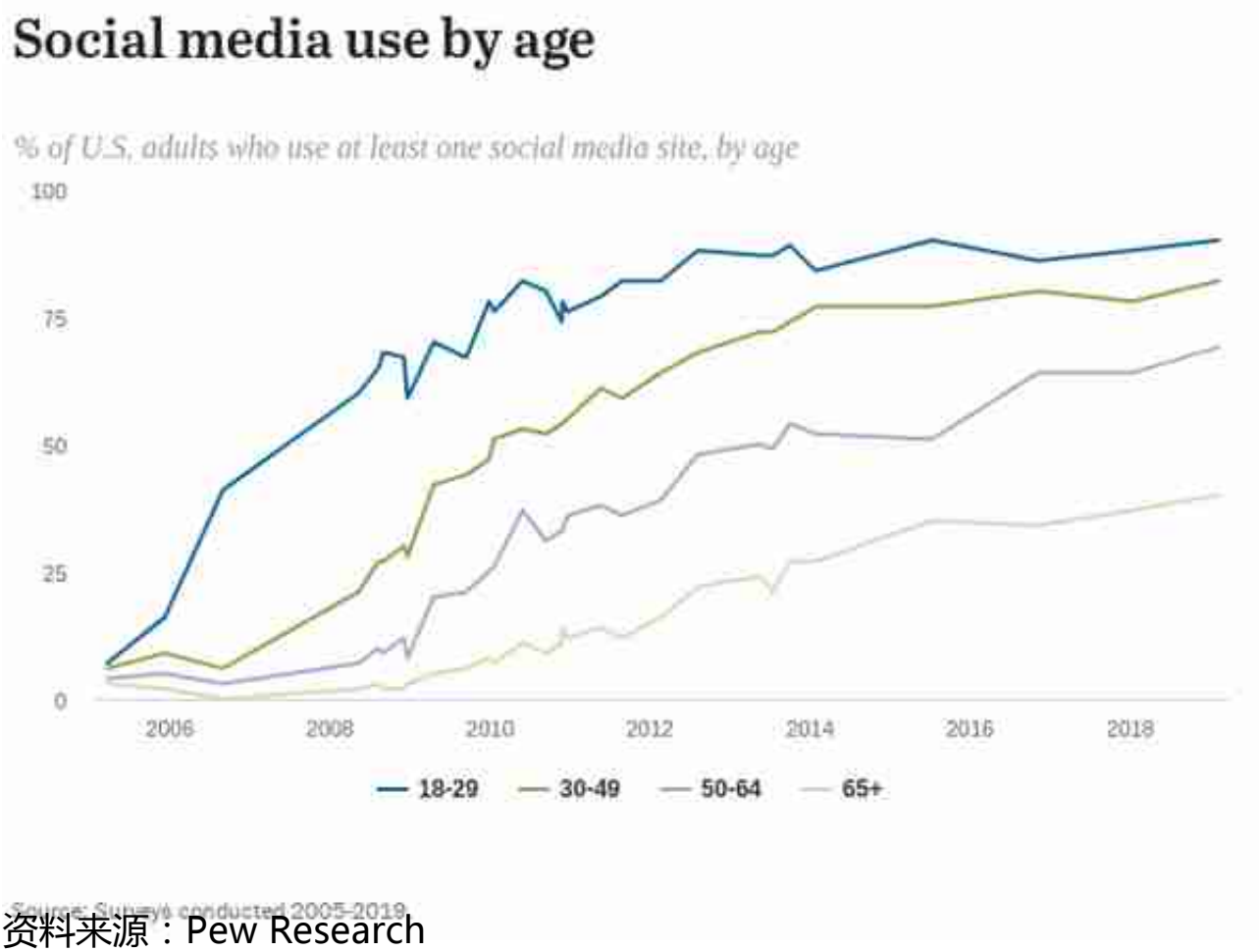
隐私币的发展一直不尽如人意，这是由什么原因导致的呢？

在我看来，主要有以下四个原因。

1. 没有人愿意用隐私币进行交易

人们可能希望自己的钱是私人财产，但并不一定想用隐私币来进行支付。当大多数
人想到「隐私 Crypto」时，他们想到的往往是隐私 BTC 或
ETH，或者是隐私稳定币，基本没人会仅仅因为一种 Token
可以保护隐私就使用这种 Token 进行交易。

这也就是为什么基于 Ethereum 的隐私系统Tornado Cash，会有如此大的吸引力。Tornado 只在人们实际所处的地方，比如在智能合约链上进行隐私保护，并使用用户真正喜爱的 Token，如 ETH、USDC 或 DAI。相比之下，Monero 币的钱包、出金功能和流动性都不够完善，所以最终大多数用户都不再使用该币。



资料来源：Pew Research

隐私是一项公共利益。经济学中的一条铁律是，在自由市场之下，公共利益常常面临缺失。如果只有少数用户使用隐私保护技术的话，那么使用这些技术将成为一种耻辱。我们可以比较一下 WhatsApp 和 Monero 在隐私方面的建设，前者的 E2E 加密早就成为了一项普及的技术，而同样是隐私保护，后者的行为就被即刻认定为可疑操作。

互联网用户基本可以分成两大类，一类是根本不关心隐私问题，只希望他们的近邻、配偶和朋友不知道他们所作所为的人（使用像 Bitcoin 或 Ethereum 这样的区块链就可以很好的做到这一点，这样他们的邻居就无法追踪他们的活动了）；另一类是有隐私意识，并希望通过强大的隐私管控技术来保护其不被第三方所侵害的人。如果 Monero 应用得当的话，它便可以有效地阻止公司、政府和黑客获取用户的隐

私。然而，所有这些都需要付出高昂的代价。

与少部分在意隐私问题的群体相比，很少有人愿意为隐私支付额外的费用。在隐私保护的成本大幅下降之前，Crypto 领域不会出现类似于 HTTPS 这样的颠覆性技术。

接下来我想谈谈监管问题。

4. 要想在棕熊袭击中幸存下来，你不用跑过熊，只需要跑过你身后的人就足够了

隐私币一直是监管部门调查的首要目标，因为每当有人要求监管机构有所作为时，那么最容易挑出问题的一定是神秘莫测的隐私币了。

在监管的影响下，韩国、日本、英国和美国一系列隐私币都选择了退市。各国政府正不断收紧对隐私币的管控（具体可以参见这三则消息：1. 法国财政委员会建议禁止使用隐私币；2.澳大利亚 Crypto 交易所被迫将隐私币退市，否则将被除名；3.特勤局警告 Monero 和 Zcash 隐私币采取法律行动）。

虽然 Crypto 游说团队的规模在不断增长，许多零售企业和机构也都有了 BTC 和 ETH，但它们之中很少有人愿意为隐私币辩护。因为在这些人看来，与其让整个行业受到玷污，他们宁愿让隐私币成为牺牲品。

我很欣赏 Coin Center 和电子前沿基金会为保护美国公民的自由，使用隐私保护技术所作出的各项努力。但与此同时我也担心，如果这之中涉及到私人 Crypto 的话，那么这些努力注定会以失败告终。

在此之前，我估计监管机构还将继续把隐私币作为替罪羊，而且其接受度和流动性也将因此受到影响。如果让我来猜测一下的话，我预计将来在隐私领域，与去中心化金融和稳定币整合的简易隐私解决方案将成为该领域最大的增长点。