Gate Research

ZEC 重估之后，隐私赛道迎来全面复苏了吗？



Gate 研究院：ZEC 重估之后，隐私赛道迎来全面复苏了吗?

摘要

- ZEC 自身的价值重估，为其他隐私概念标的带来了久违的市场关注，并对其价格走势形成了较为普遍的短期催化。但短期跟涨不等于长期重新定价：多数标的仍未摆脱长期低价区间，也未形成持续的趋势反转。因此，本轮行情更应被理解为 ZEC 重估引发的关注度扩散与阶段性价格反应，而不是整个隐私赛道的共同牛市。
- ZEC 发生价值重估的主因并不来自隐私使用的增长，更与 Naval 的注意力催化及货币资产定位、合规与机构接入渠道改善、治理和安全冲击后的社区共识相关。NEAR 被市场视为 ZEC 强相关标的，因为 NEAR Intents 为外部资产与 ZEC 通过 Confidential Intents 提供隐私跨链通道，强化了 NEAR Intents 作为跨链产品的差异化竞争优势，但 NEAR 同时具有 AI、业务发展及传统资金接入等独立催化，不能把全部上涨归因于 ZEC。
- 隐私项目正从早期市场熟悉的单一混币工具定位走向私密 DeFi、应用网络和机密计算服务。TEE、零知识证明、FHE 和多方计算各有独特的优势，也各面临信任、效率与成熟度的约束，未来数年仍需看见更明显的技术突破，让成熟度与体验对齐主流公链，并进一步拓展与多区块链应用的交互。
- 隐私是长期需求，已经拥有了强货币定位与机构级采用的新叙事角度，但除 ZEC 外更多隐私相关标的的价值重估仍需时间检验。隐私相关的标的之间也会因为是否发生基本面变化，以及是否能够获得市场对新叙事的角度认可而出现越来越明显的表现分化。

前言

自 2025 年 9 月 ZEC 从长期低迷中启动以来，隐私赛道成为加密货币市场中突出的行情主线。以 9 月 22 日收盘为起始点，截至 2026 年 10 月 18 日，ZEC 上涨 2,253.36%，价格为起点的 23.53 倍；同期 BTC、ETH 分别下跌 27.11% 和 42.60%。

进入 2026 年下半年，ZEC 的突出表现又有了一条清晰的关联路线：NEAR 同期上涨 181.37%，与 ZEC 的 183.14% 接近，并明显超过 BTC 的 40.04% 和 ETH 的 53.33%。NEAR 原本并不是一个隐私概念标的，但 NEAR Intents 通过 Confidential Intents 等功能，为外部资产进入隐私交易环境提供了新的路径，从而强化了 NEAR 在跨链与隐私交互方面的产品叙事。通过 NEAR Intents，BTC、ETH、SOL、USDC 等资产能够直接兑换成隐私池中的 ZEC，相当于“为具有隐私需求的资金，提供了一条通往 ZEC 生态的隐私跨链通道”。

ZEC 和 NEAR 的强势，会给到市场一个下意识的想法，即“隐私赛道成为了本轮加密货币市场中突出的行情主线”。但具体的分析给出了反直觉的结论——无论是隐私货币，还是其他具体的隐私项目，大多数并没有同时像 ZEC 与 NEAR 一样形成相近的持续超额收益，也没有实现市值规模上的明显突破。ZEC 的巨大涨幅和权重容易造成“隐私赛道整体牛市”的印象，却不能据此期待流动性溢出并自然轮转到每一个具有隐私标签的标的上。

本文先比较隐私货币的长期价格结构，辨认行情是否形成板块轮动；随后解释 ZEC 两轮重估的催化，以及 ZEC 与 XMR 在使用需求和货币属性上的叙事偏重差异；再分别考察 NEAR Intents、隐私池、隐私网络与隐私计算，最后讨论隐私需求能否成为持续的投资主线。

一、行情边界：ZEC 重估不等于隐私赛道的全面牛市

1.1 资产分类：隐私货币与隐私应用的投资逻辑不同

隐私是一个很广泛的概念。如果非常广泛地定义加密货币市场中的隐私，不仅包括本轮最受关注的 ZEC，还包括诸多链上隐私应用。例如，以太坊创始人 Vitalik Buterin 曾多次使用的 RAILGUN，提供既有资产的屏蔽与私密交易功能；主打隐私的 AI 产品 Venice，则把隐私诉求延伸到用户与 AI 的交互。它们都讨论隐私，所保护的信息和对应的代币需求却不同。

对 ZEC 最准确的分类定义，是“隐私货币”。隐私货币的典型代表是 ZEC 与 XMR，核心是在协议层或账户层降低交易金额、地址关系或交易图谱的公开可见性，用户使用的价值载体本身

就是这项原生资产。具体的隐私应用及服务代币则依托应用、合约或计算服务提供隐私功能，代币可能承担治理、质押或其它效用，比如，使用 RAILGUN 不要求先持有 RAIL，质押 Venice 的 VVV 可取得 AI 推理容量，但这不意味着 RAIL、VVV 的链上转账本身被隐藏，这些代币本身也不作为一种原生的价值载体，不承担着“货币”属性。

因此，对于隐私的需求广泛存在，很多代币都能够被贴上“隐私”的概念标签，但实际的投资逻辑差别很大。首先要厘清的是，所谓加密货币市场的“隐私赛道行情”，其真正的核心到底是什么：隐私货币的重估、具体隐私应用需求的增长，还是所有能够被贴上“隐私”概念标签的资产共同上涨?

1.2 隐私货币的长期价格结构：反弹不等于趋势反转乃至价值重估

首先取 CoinGecko 上“隐私货币”分类按流通市值排名前 9 的币种，分析这 9 个币种自 ZEC 首轮起涨点（以 2025 年 9 月 22 日收盘为起始点）至 2026 年 10 月 18 日的表现。表格中额外列入了 DASH，从市场理解的角度而言，将 DASH 直接纳入隐私货币概念并放入表中并没有问题，但 DASH 有特殊的自身发展背景，且在本轮 ZEC 上涨行情中，其价格走势与 ZEC 高度相关，对于整体的分析讨论有重要意义，故将其列入下表内。

隐私货币板块在 ZEC 行情中的整体表现

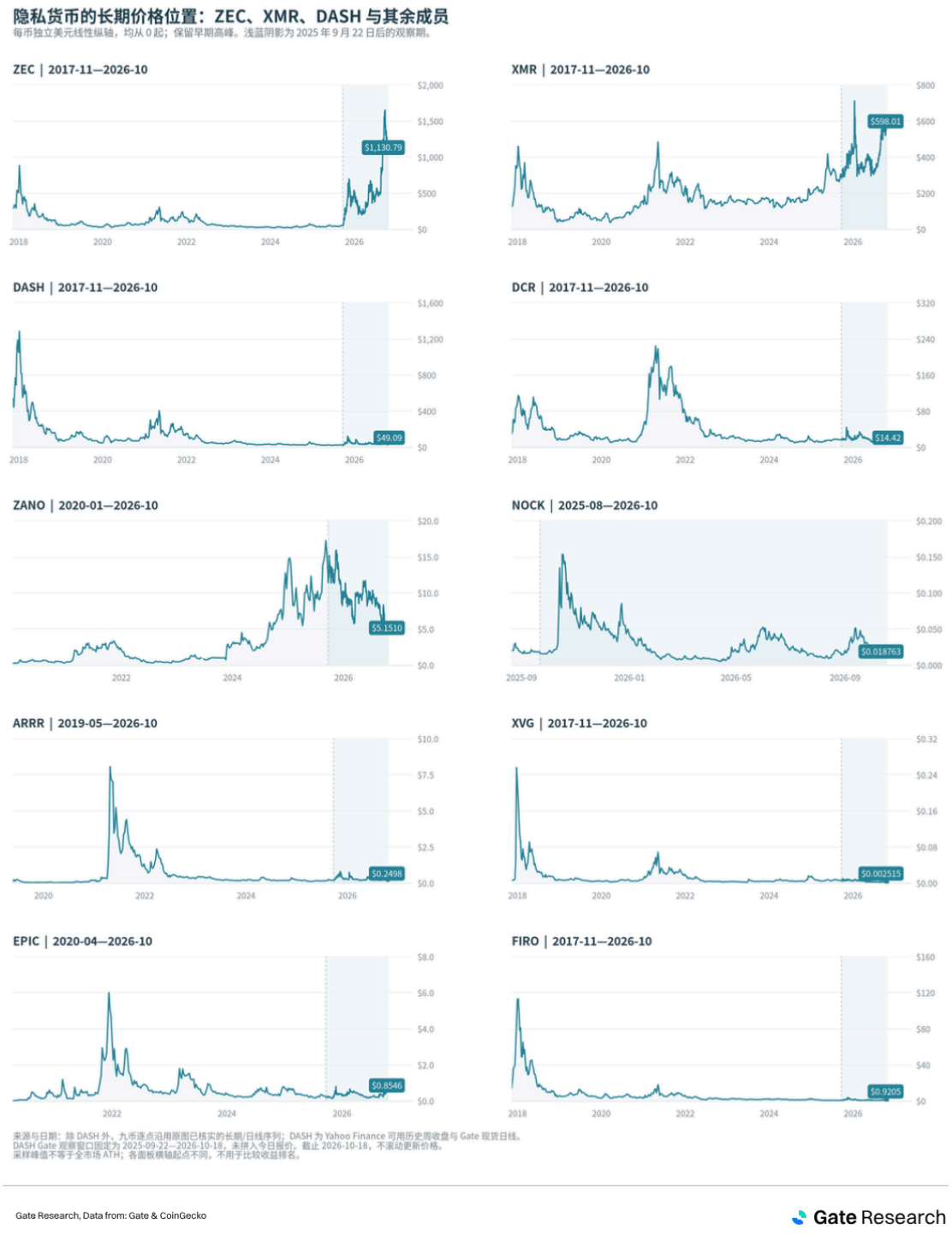
排名	资产	流通市值	完整周期收益	期末价格 / 起点
1	ZEC	206.05 亿美元	+2,253.36%	23.53 倍
2	XMR	115.94 亿美元	+107.61%	2.08 倍
3	DASH	6.50 亿美元	+131.88%	2.32 倍
4	DCR	2.60 亿美元	-12.11%	0.88 倍
5	ZANO	7,146 万美元	-55.00%	0.45 倍
6	NOCK	4,924 万美元	+16.47%	1.16 倍
7	ARRR	4,762 万美元	+29.70%	1.30 倍
8	XVG	4,334 万美元	-48.44%	0.52 倍
9	EPIC	1,718 万美元	+305.02%	4.05 倍
10	FIRO	1,686 万美元	+55.23%	1.55 倍
基准	BTC	—	-27.11%	0.73 倍
基准	ETH	—	-42.60%	0.57 倍

Gate Research, Data from: CoinGecko

Gate Research

流通市值排名前 9 的隐私货币，只有 ZEC 与 XMR 达到百亿美元级别，合计占隐私货币前 10 流通市值的约 96.54%；其余 8 个代币中，只有 DASH 和 DCR 的流通市值超过了 1 亿美元。在数据周期的起点，2025 年 9 月 22 日，ZEC 流通市值约为 7.94 亿美元，XMR 则约为 53.39 亿美元。仅通过隐私货币间的流通市值对比，就能够发现 ZEC 的大幅上涨并没有显著带动隐私货币板块整体的行情。同时，除 ZEC 与 XMR 外的币种，仅有一半录得完整周期收益正值。来看各币种具体的更长周期历史走势。DASH 和 NOCK 是唯一在数据周期内出现过剧烈上涨的代币。但从彼时至今，NOCK 为人关注的并不是隐私属性，而是 ZK 证明与 PoW 挖矿的混合属性，它在数据周期内的剧烈上涨并不由隐私概念引起。EPIC 与 FIRO，虽然在数据周期内录得较显著的涨幅，分别为 +305.02% 与 +55.23%，但价格仍然处于长期低位区间，并没有展现出明显的趋势反转。剩下的币种中，比较特殊的是 ZANO，它完全错开了 ZEC 的强势时间窗口，并且在周期内几乎呈现一路下行的趋势。

流通市值排名前 9 的隐私货币 + DASH 的长周期历史走势观察

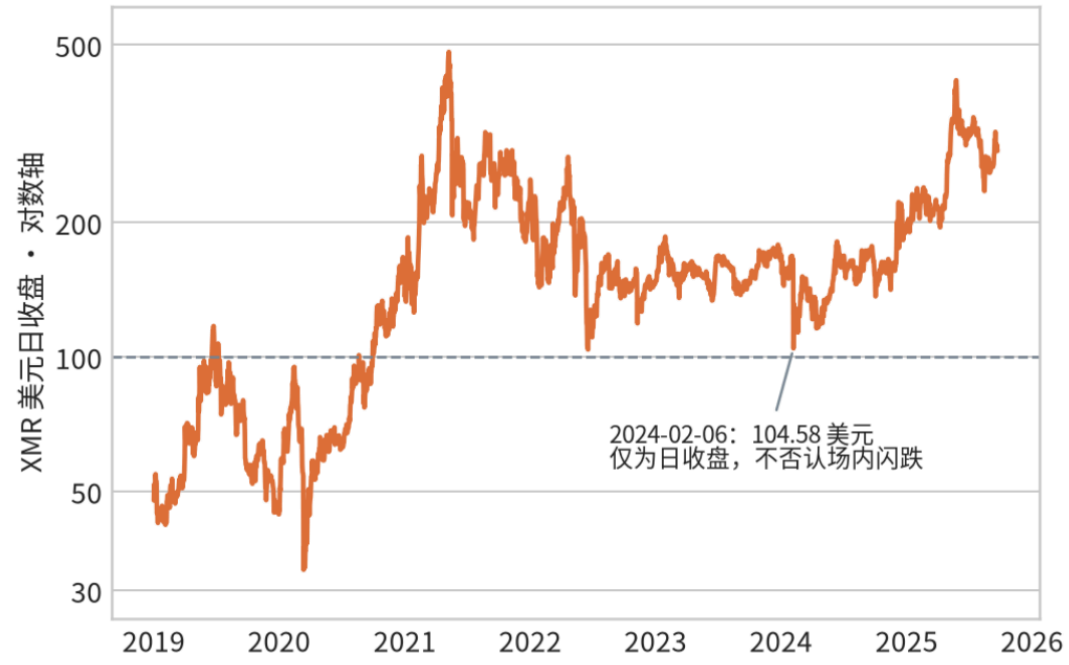


1.3 XMR：独立恢复周期早于 ZEC 的大幅上涨

XMR 的上涨也许不能排除 ZEC 的带动作用，但更应从被动跟涨的解释中分离。XMR 多年来的走势相当稳定，在 ZEC 大幅上涨前，它一直是隐私货币毫无疑问的龙头，其价格多年没有跌

破 100 美元，即便在 2024 年发生了重大的交易所下架冲击当天，其参考日收盘仍约为 104.58 美元。

XMR 的历史走势观察



Gate Research, Data from: CoinGecko

Gate Research

从 XMR 的长期走势来看，首先，它早在 2024 年 4 月开始就有明显恢复。2024 年 10 月至 2025 年 9 月 21 日（ZEC 启动前），XMR 由 153.10 升至 292.51 美元，上涨 91.06%，同期 ZEC 为 38.35%。

XMR 与 ZEC 的长期走势对比



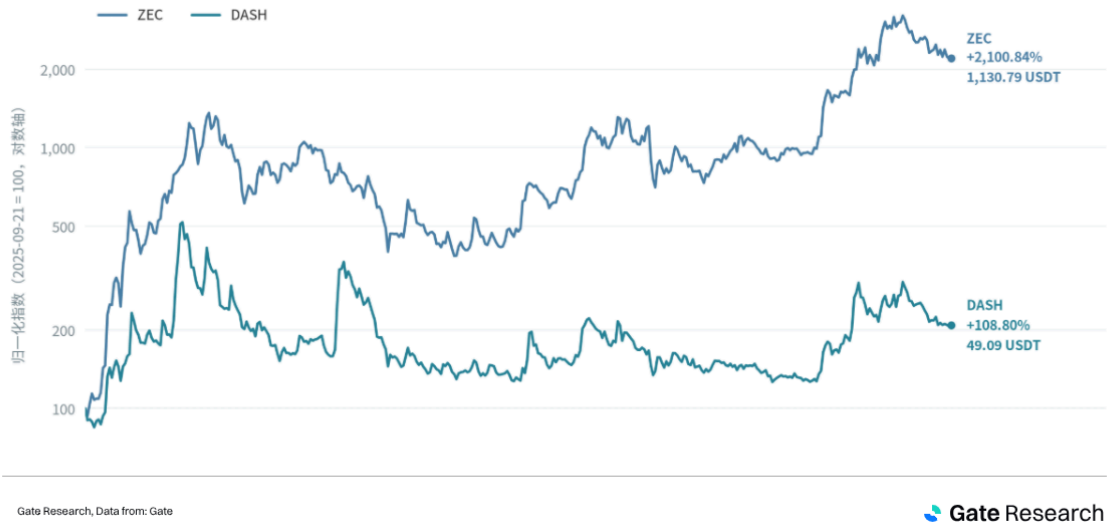
2025 年 8 月 - 9 月间，XMR 遭遇到一些较为严重的安全事件，但价格并未受到较大影响，体现了市场对其自身长期稳定的共识强度的认可。2025 年 8 月 11 日，Qubic 开始其最终阶段的自私挖矿行动，通过暂扣区块、随后发布竞争链来造成区块重组；次日它公开宣称取得了超过 51% 的算力或出块优势，引发市场对双花攻击的担忧。2025 年 9 月 14 日出现了更严重的 18 个区块重组，原链中的约 117—118 笔交易失效，Qubic 随后承认实施了此次重组，确实构成了潜在双花风险。

同期的价格表现，到 2025 年 8 月 18 日，XMR 已恢复至约 281.33 美元，比 8 月 10 日高 4.88%。而在 9 月 14 日的 18 区块重组发生时，价格从前一日约 286.07 美元升至 306.19 美元，日频涨幅为 7.03%，同期 BTC、ETH 分别下跌 0.49%、1.21%。

1.4 DASH：跟随 ZEC 最明显的标的，从支付定位回归重新强化隐私标签

DASH 自 2025 年 9 月下旬 ZEC 上涨以来，与 ZEC 的价格走势非常相像。

DASH 与 ZEC 的走势对比（自 2025 年 9 月下旬 ZEC 行情起点开始）



和 XMR 实际上与 ZEC 涨势的关联性弱不同，DASH 是那个非常符合跟涨 ZEC 定义的标的。在 ZEC 2025 年 9 月下旬开始的第一波上涨期间，查阅多家加密货币市场相关媒体的报道，往往会提到“ZEC 上涨带动隐私板块，DASH 上涨了 XX%”，但是 DASH 这个标的多年来专注发展的赛道并不是隐私，而是支付。

DASH 官网发表于 2019 年 10 月 24 日的一篇文章中，直接有着这样的一句，“严格来说，Dash 并非‘以隐私为中心的加密货币’，而是一种基于比特币的、专注于支付的数字货币。”彼时的背景是，2019 年 6 月 21 日，金融行动特别工作组（FATF）发布了《虚拟资产及虚拟资产服务提供商基于风险的方法指南》，其中包含一系列建议，旨在加强全球及各国加密货币行业的反洗钱（AML）/打击恐怖主义融资（CFT）工作。这些建议明确了指南的适用对象，并为虚拟资产服务提供商（VASP）提供了一系列建议，以降低通过其服务发生的非法金融活动的风险。其中许多建议涵盖了适用于传统金融行业的流程和最佳实践，但也有一些建议直接针对虚拟资产服务提供商所持有的虚拟资产（VA），包括匿名增强型货币（AEC）。在这篇文章中 DASH 还写道，“由于上述指导意见，一些交易所决定下架 DASH 以确保完全合规。然而，下架 DASH 的决定仅仅基于媒体将 DASH 描述为‘隐私币’，而非基于对 Dash 区块链本质的实际分析。”可见，为了加强自身合规性，DASH 官方甚至是抗拒媒体乃至市场将其定位为隐私币的。

2025 年 11 月 1 日，DASH 官方 X 账号还发表了一篇推文，解释 DASH 在 2025 年 10 月期间的价格上涨。推文中给出了 5 点原因，分别是提供折扣的消费功能 DashSpend 的钱包整合、对账单支付问题的优化、隐私支付功能的改进、首个支持 DASH 的跨链 AMM DEX 以及全新的 DASH Evolution 区块链。这 5 点原因，“隐私”只在隐私支付功能的改进中出现，不仅更多还是强调支付功能的进步，而且在这篇推文发表时，隐私支付功能的改进是正在做的事情，而不像其它 4 点是已经完成了的成果展示。

直到 2026 年 2 月初，DASH 才计划将基于Zcash 的 Orchard 技术的零知识隐私添加到其 Evolution 网络中，并且于 8 月 4 日在 Dash Evolution 主网上正式支持了屏蔽交易。

可以说，DASH 是在 ZEC 的上涨对其起到带动作用后，才选择跟随市场的旧有理解，重新强化自身的隐私标签。其后续的隐私功能更新，也非常参照 ZEC。它是隐私货币细分分类中，最能够说被 ZEC 直接带动的那个标的。

综上，通过在 ZEC 的最核心定位，隐私货币标的间的比较，分析结果并不支持“隐私货币板块存在整体行情”的结论，除了 DASH，ZEC 和其它隐私货币在 ZEC 自 2025 年 9 月下旬至今的走势间并没有持续的显著相关性。更严谨的说法是，ZEC 的上涨，确实为隐私货币板块带来了久违的关注度，但其自身的上涨没有让绝大部分隐私货币标的走出长期的低价区间，形成价格趋势的逆转。

那么，ZEC 为什么这么能涨，甚至从流通市值上超越了 XMR?

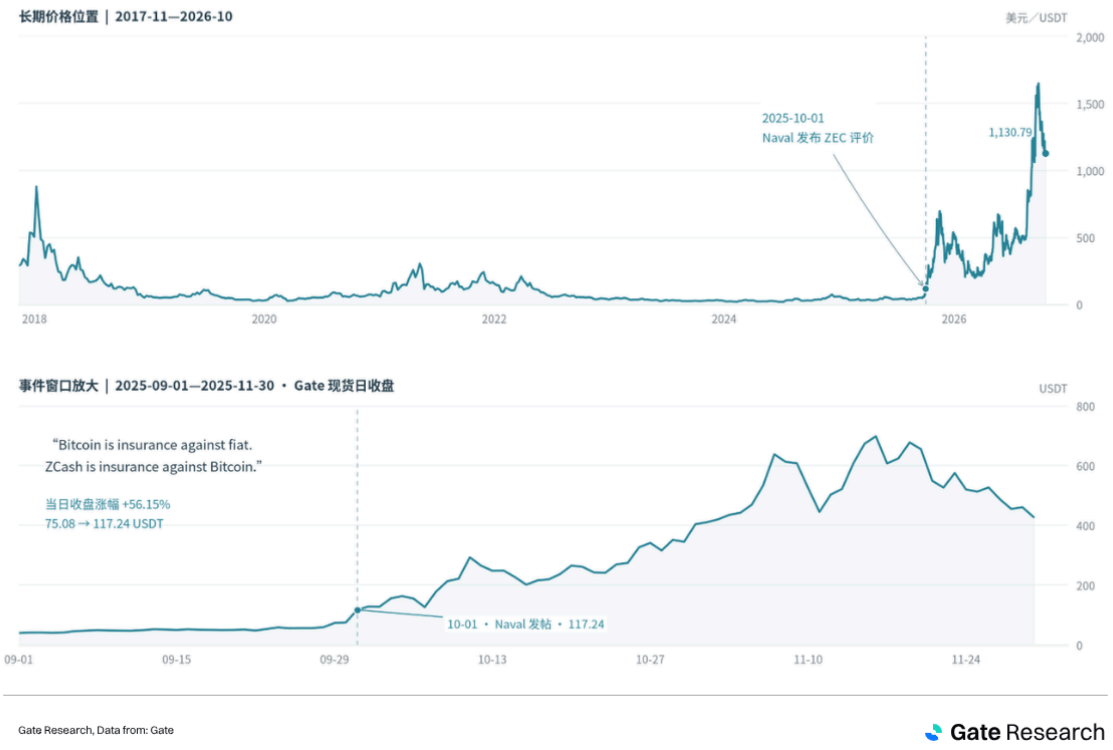
二、ZEC 的价值重估：注意力催化、合规通道与社区共识

2.1 注意力催化：Naval Ravikant 的“喊单”

2025 年 10 月 1 日，Naval Ravikant 发布了一条这样的推文：“Bitcoin is insurance against fiat. ZCash is insurance against Bitcoin.（比特币是对法币风险的保险，Zcash 是对比特币风险的保险。）”而就在这一天，根据 Gate 现货数据，ZEC 现货的日收盘涨幅为 56.15%。

单一注意力事件驱动无法解释 ZEC 的整段大幅上涨，甚至从流通市值上超越了 XMR 的行情，但 Naval 的推文，绝对是启动 ZEC 行情的标志性事件。

Naval 的推文直接催化了 ZEC 的第一波行情



在 ZEC 行情启动的最早期，市场并没有聚焦于“隐私叙事的回归”或“ZEC 基本面转变”等目前流行的原因或看法，而是非常简单直接地在追逐注意力效应。Naval Ravikant 作为知名的天使投资人，打造了估值 40 亿美元的创业融资平台 AngelList，其个人也参与了 Uber、Twitter 等 200 多家公司的早期投资。在加密领域，他同样有着知名度，在 2014 年联合创立了最早的加密对冲基金之一 MetaStable Capital。根据公开报道，MetaStable Capital 在 2017 年实现了 540% 的回报率。

这是非常有分量的“喊单”，但在当时也引来不少争议，因为 Naval 与 ZEC 存在利益关系。2015 年，Naval 参与了 ZEC 开发方 Electric Coin Company（2019 年改名，此前为 Zerocoin Electric Coin Company）合计 71.5 万美元的天使融资。他还曾担任 Zcash 基金会首届董事，有一定的治理决策上的影响力，但在 2018 年 6 月 28 日董事会会议前辞职。

在这里交代 Naval 的背景，只是为了说明其对 ZEC 上涨的催化作用为何如此巨大，而不是陷入一个“阴谋论”为主的上涨分析中。同时，这个短期的注意力催化事件，有着更深层的意义。因为 Naval 的推文内容本身透过其巨大的影响力向市场传递后，结合币价的上涨，加速了市场重新审视 ZEC 的进程。

Naval 的推文，为 ZEC 提供了不同于匿名转账工具的资产定位。如果主要把 Zcash 理解为隐藏交易记录的工具，其需求容易被局限在转账和支付场景，估值讨论也容易停留在使用频率上；“匿名交易”的标签同时伴随监管和合规疑虑。Naval 提供的角度则是：即使 Bitcoin 成功，持有人仍可能需要保护自己的财务信息，而 ZEC 可以作为这一需求的货币资产候选。Zcash 试图在类似的货币属性之上增加可选择的隐私：同样采用 PoW，并设置 2,100 万枚的供给上限，同时允许使用屏蔽路径。于是，ZEC 不再只能被问“有多少人需要匿名付款”，还可以被问“有多少资产持有人愿意长期持有一部分不公开暴露财务关系的货币”。这使潜在需求从交易流量扩展到资产保护和长期储值，为市场提供了一个重新评估 ZEC 的角度。

2.2 合规与机构通道：第二轮重估的资金入口

在过去的市场讨论中，隐私的第一印象往往是 Tornado Cash 这样的混币服务，或 XMR 这样对正常交易默认提供隐私保护的货币。它们与洗钱、被盗资金转移和暗网交易的关联报道，容易使市场把“隐私需求”理解为“规避监管”，而不是普通乃至机构用户保护财务信息的需求。

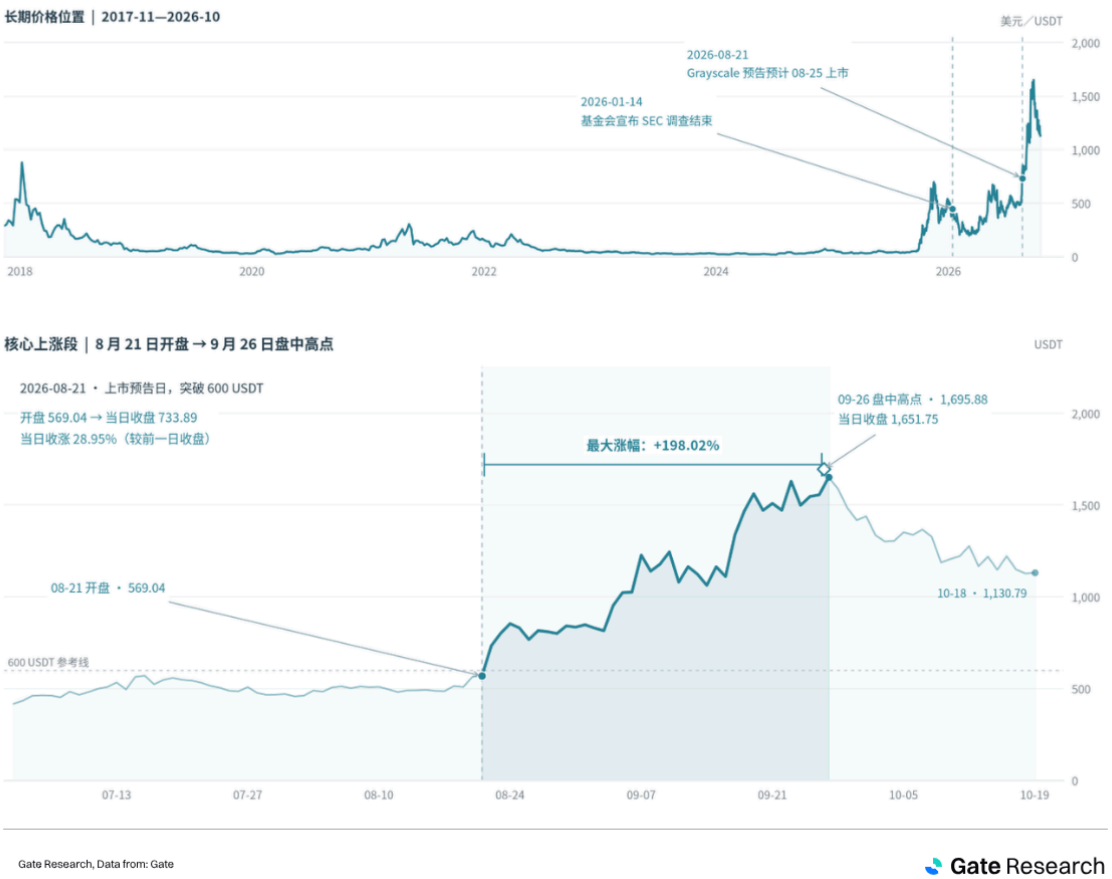
TORN 的历史负担最直接。2022 年 8 月 8 日，美国 OFAC 制裁 Tornado Cash，财政部公告将其描述为曾被用于清洗被盗虚拟资产的混币器。另一路法律风险发生在 2023 年 8 月 23 日：美国司法部起诉 Tornado Cash 开发者 Roman Storm 与 Roman Semenov，指控其合谋洗钱、违反制裁及经营无牌货币传输业务；2025 年 3 月 21 日，财政部撤除了对 Tornado Cash 的经济制裁，但不等于其所有相关行为获准：2025 年 8 月 6 日，开发者 Roman Storm 被陪审团裁定一项合谋经营无牌货币传输业务罪有罪，目前他仍在等待重审以撤销定罪。

监管层面的压力，让多家交易所不得不下架 TORN，同样的压力 XMR 和 ZEC 也同样面临，但根据目前仍上线对应标的的交易所数量，TORN 远少于 XMR，XMR 又远少于 ZEC。实际上，这 3 个币种所面临的压力并不相同。XMR 的压力比 TORN 小，因为不面临制裁、刑事起诉或调查，而是来自它本身的“强制隐私”。XMR 的链上转账强制采用隐私机制，会使交易所难以满足诸如 MiCA 第 76(3) 条：“交易平台不得准入具有内置匿名化功能的资产，除非平台能够识别持有人及其交易历史。”这样的合规要求。相比之下，对交易所来说，用户可自行选择是否对链上交易进行隐匿的 ZEC 要满足合规要求就容易得多，比如在充提方面，对 ZEC 的隐匿地址类型进行限制，接受透明地址的充提就可以满足。

ZEC 面临的是另外一个层面的合规困扰，它的压力来自于 SEC。Zcash 基金会在 2023 年 8 月 31 日收到 SEC 传票，调查名称为“某些加密资产发行事项”（In the Matter of Certain Crypto Asset Offerings）。2026 年 1 月 14 日，Zcash Foundation 宣布 SEC 已结束相关审查，不拟建议就该事项对基金会采取执法行动或其他变更，这为传统资金流入 ZEC 铺平了道路，也彻底让 ZEC 在合规层面遥遥领先 XMR。2025 年 11 月 26 日，Grayscale 提交将 Zcash Trust 私募信托转换为 Zcash 现货 ETF（交易代码 ZCSH），同时在申请中规划于 NYSE Arca 上市。2026 年 8 月 21 日，根据纽交所的 8-K 文件，ZCSH 预计于 2026 年 8 月 25 日在 NYSE Arca 开始交易。

从 SEC 结束相关审查到现货 ETF 上市，ZEC 合规基本面的巨大变化，是今年 8 月下旬开始的第二波大幅上涨行情的直接催化因素。

ZEC 现货 ETF 直接催化了 ZEC 的第二波行情



现在，对于“ZEC 为什么涨”这个问题，我们已经明确了两波大幅上涨行情启动的直接催化原因。第一波大幅上涨行情，来自 Naval 的“喊单”效应，以及为市场提供了理解 ZEC 隐私货

币属性的全新角度；第二波大幅上涨行情，来自于合规基本面的巨大改善，传统和机构资金的入场渠道被彻底打开。而在这两波大幅上涨行情之间，ZEC 还经历了一波下跌幅度一度达到 75% 的调整。对这段下跌调整行情的分析，我们还能为“ZEC 为什么涨”这个问题找出另一个层面的答案。

2.3 ECC 治理冲突：开发团队分离与钱包业务延续

第一波大幅上涨行情后，ZEC 迎来的第一个打击是 ECC 团队因治理冲突退出。2026 年 1 月 7 日，时任 ECC CEO Josh Swihart 公开宣布，原管理层及开发团队已集体离开 ECC。这里的 ECC 也就是前文 Naval 早期投资、法律名称为 Zerocoin Electric Coin Company 的同一家 Zcash 原始开发公司。它长期参与协议研发，并推出了 Zashi 钱包。

冲突的另一方是 Bootstrap Project，持有 ECC 的非营利母体。双方的核心分歧是 Zashi 钱包及相关知识产权如何从非营利母体控制的 ECC 转入营利结构，以及交易的估值、利益冲突和决策程序能否满足慈善组织要求。Swihart 认为董事会的治理方式使团队无法有效工作；Bootstrap 则强调，非营利组织的资产转移必须符合合理估值、公共利益及利益冲突控制要求。董事会当时并未完全反对营利化，而是反对其认为不合适的交易条件和程序。

离开 ECC 后，Swihart 与原团队另行成立 Zcash Open Development Lab（ZODL），在新的公司结构下继续开发 Zcash 协议和钱包。2026 年 2 月 16 日，团队公开说明了新公司的成立，并宣布 Zashi 钱包将更名为 Zodl。核心分歧后来通过分离协议得到解决，2026 年 2 月 27 日，Bootstrap 董事会公开确认，治理争议已经解决，并已授权转移 Zashi 钱包技术与相关知识产权；技术资产转移后，ECC 将有序结束运营，Bootstrap 则保留独立非营利组织及董事会结构。当天，Swihart 代表 ZODL 明确确认双方达成和解，资产转移安排使原开发团队可以在新公司继续创新。2026 年 3 月 4 日，Bootstrap 董事会进一步表示：“The deal is signed. The governance dispute is resolved.” 即协议已经签署、治理争议已经解决。在这一背景下，ZODL 于 3 月 9 日宣布超过 25,000,000 美元融资，既为原团队扩充开发资源，也让钱包业务能够在可接受外部投资的新公司结构中继续推进。

2.5 Orchard 漏洞：修复、历史风险与市场韧性

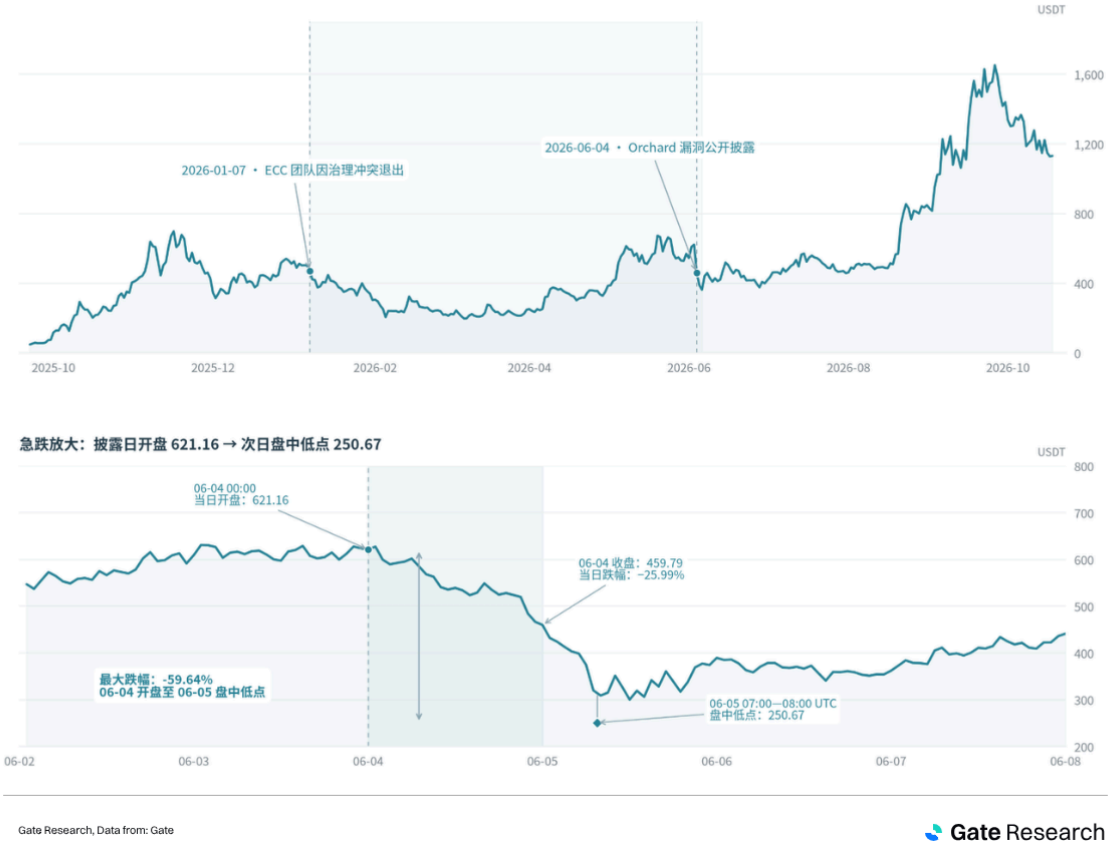
第二个打击相较于 ECC 退出更为致命。2026 年 5 月 29 日，Shielded Labs 的安全研究员 Taylor Hornby 借助 Anthropic Opus 4.8 模型进行定向审计时发现 Zcash Orchard 隐私池存

在严重漏洞，该漏洞自 2022 年 5 月以来一直未被察觉，理论上可能允许攻击者无限增发且无法被检测的假 ZEC。好在 Taylor Hornby 负责任地就此问题与 ZODL 进行了直接沟通，漏洞细节得到了严格保密。ZODL 的补救也很及时，首先在 6 月 2 日通过紧急软分叉阻断已知漏洞利用路径，让节点暂时拒绝所有含 Orchard Action 的交易和区块，直到 NU 6.2 激活。6 月 3 日，NU 6.2 硬分叉网络升级成功激活，Orchard 服务也通过修正后的电路重新启用。

但这个漏洞最致命的地方在于无法追溯。6 月 4 日，Shielded Labs 进一步公开解释了伪造增发机制，并明确指出，无法用密码学证明漏洞在修复前是否曾被利用。也就是说，漏洞的补救虽然很及时，但只是阻断了漏洞在未来被利用的可能性，至于从 2022 年 5 月以来，过去是否通过该漏洞发生过伪造、伪造了多少，以及哪些旧 Orchard 池余额源于伪造，通通无法确定。简单来说，如果过去曾经有人利用该漏洞从旧 Orchard 池中伪造了余额并且退出了 Orchard 池，就会挤占真实资产持有者的退出额度，导致真实资产持有者无法从池内取出余额。

因为这种未知的财产风险，该漏洞披露后 ZEC 受到的价格冲击非常明显。6 月 3 日 ZEC 收盘为 621.28 USDT，6 月 4 日降至 459.79 USDT，当日下跌 25.99%；6 月 6 日收盘进一步降至 362.10 USDT，较 6 月 3 日低 41.72%。6 月 5 日的盘中最低价则为 250.67 USDT。

ECC 治理冲突与 Orchard 漏洞对 ZEC 价格的影响

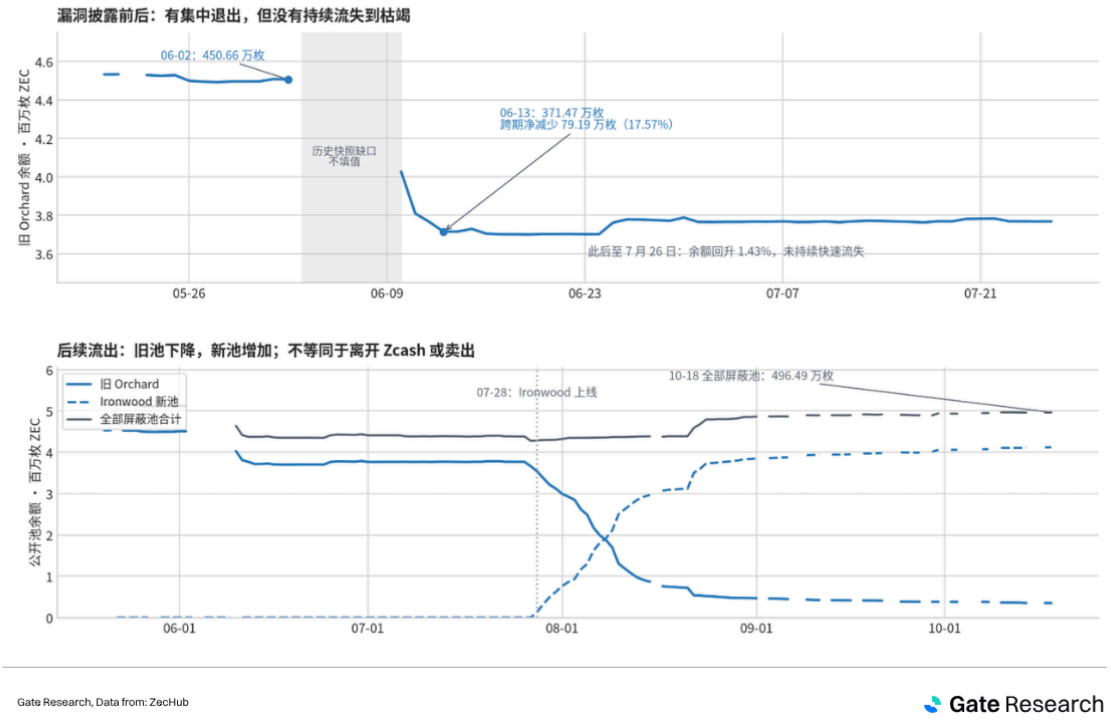


Gate Research, Data from: Gate

Gate Research

最后，7 月 28 日 NU 6.3 引入 Ironwood 新池。旧 Orchard 池不再允许价值净流入，池内余额也不能继续正常跨地址支付，这个漏洞造成的问题算是最终告一段落，旧 Orchard 池的资金开始逐渐流出并向 Ironwood 池流入。但到这里，我们的问题是，一个甚至无法被评估是否曾经受到利用且可能造成重大资金损失的恶性漏洞，为什么最终被市场消化了呢？原因是没有漏洞披露后，并没有出现超额资金尝试退出 Orchard 池的情况，而潜在的漏洞利用者通常有抢先迁出、兑现价值的动机。这让市场能够从漏洞披露最开始时面对未知风险的恐慌中恢复过来，并倾向于认为漏洞未曾被利用。

Orchard 漏洞公开披露前后，Orchard 池的资金变化情况



Gate Research, Data from: ZecHub

Gate Research

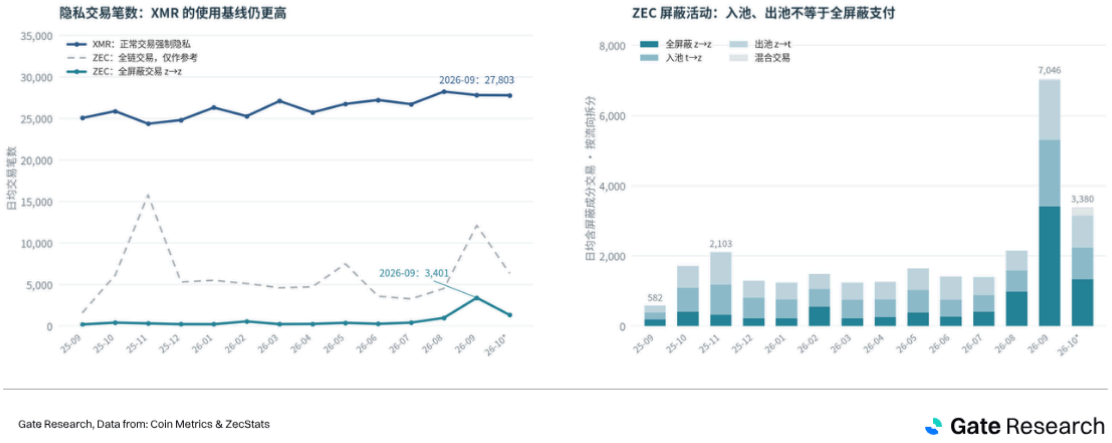
当 ZEC 的叙事重点从“隐私”转向“货币”，其社区共识强度的重要性就会与实际隐私使用需求站在一个层面上，甚至会高于后者。经历了这两起利空事件后，ZEC 所展现出来的韧性，也是对 Naval 给出的隐私货币新角度的直接检验。

三、ZEC 与 XMR：隐私实际使用与货币属性的竞争

3.1 交易活动：XMR 隐私使用规模更高，ZEC 增长并非单向

常见到的看空 ZEC 的观点之一是，ZEC 的实际隐私使用增长情况完全跟不上币价的涨幅，也远远不如 XMR，这是事实。在日均隐私交易笔数乃至全链交易笔数上，从 2025 年 9 月下旬 ZEC 起涨至今，XMR 都大幅领先 ZEC。

ZEC 与 XMR 的隐私使用活动对比



Gate Research, Data from: Coin Metrics & ZecStats

Gate Research

2025 年 9 月，XMR 日均交易笔数约 25,047 笔，ZEC 全链日均交易笔数约 1,584 笔，但其中按 ZecStats 分类的全屏蔽交易日均只有 189.5 笔，XMR 约为后者的 132.18 倍。到 2026 年 9 月，ZEC 全屏蔽日均升至约 3,401 笔，差距有所收窄；但 XMR 同期约 27,803 笔，仍是前者的 8.18 倍。10 月 1—18 日，ZEC 全屏蔽日均回落至约 1,324 笔，XMR 日均约 27,782 笔，比值又扩大到约 20.98 倍。

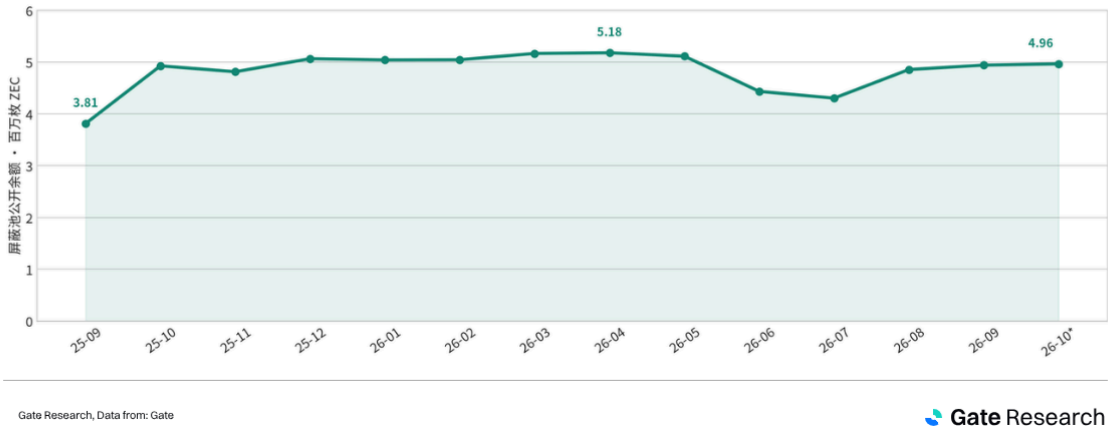
2025 年 11 月，ZEC 全链共录得 473,530 笔交易，但 ZecStats 的含屏蔽成分交易为 63,100 笔，其中全屏蔽交易为 9,401 笔。全屏蔽只占含屏蔽成分交易的约 14.90%，其余主要是入池、出池及混合活动。实际上，2025 年 11 月的全屏蔽日均笔数还比 10 月下降约 22.75%。

ZEC 的全屏蔽活动后来确实扩张，但仍不是一路增加。2026 年 9 月的日均全屏蔽笔数较 2025 年 9 月增长约 1,694.58%，显著快于 XMR 同期约 11.00% 的增长。不过，Ironwood 池上线后的从旧 Orchard 池的迁移可能贡献了其中一部分，所以也不能把它全部归于新增隐私支付；到 10 月 1—18 日，ZEC 全屏蔽日均又较 9 月下降约 61.07%。

3.2 屏蔽余额：留存规模与交易频率是两类指标

交易笔数反映活动频率，屏蔽余额则反映有多少 ZEC 留在屏蔽体系内。两者回答的是不同问题。ZEC 屏蔽池公开余额从 2025 年 9 月末的 3,813,217 枚增至 2026 年 10 月 18 日的 4,964,917 枚，增加约 30.20%；但仍比 2026 年 4 月末的 5,180,071 枚低约 4.15%。

ZEC 屏蔽池公开余额变化情况



Gate Research, Data from: Gate

Gate Research

3.3 供给与资金接入：使用领先为何没有换来同等重估

但正如前文我们反复提到的，发生在 ZEC 上的是叙事重点从隐私转向货币以及合规基本面上的巨大变化。ZEC 的巨幅上涨所表现出来的，是“价值重估”。相比之下，XMR 的叙事重点仍然是“隐私”，合规基本面上无显著变化。它的实际隐私使用情况还是领先 ZEC，很好也很稳定，但引发不了 ZEC 那样的市场重定价。

ZEC 与 XMR 的对比，恍惚让人看到了当年比特币“大小区块之争”的现在进行时版本。要注意到供求关系上的细微差别：ZEC 像比特币一样保持了上限 2,100 万枚，约四年减半的供给规则，而 XMR 的供应上限只存在于 2014 年的初始发行公式中，2015 年 3 月就加入了尾部发行机制，目前固定为每区块奖励 0.6 XMR，使发行不再最终降至零，供应也不再有上限。这个差别在如今展示出了 ZEC 更重货币属性，XMR 更重隐私使用属性的倾向。为了更广泛的采用和发展，ZEC 的隐私交易是可选的，而 XMR 是强制的。前者终于在多年后打开了机构乃至传统资金入场的大门，后者则在实际隐私使用上保持稳定领先。这同时意味着，在隐私货币这个细分赛道里，几乎不会再有能够与 ZEC 和 XMR 的竞争者出现了，“隐私”和“货币”两个层面的挑战门槛被它们高高立起，且难以撼动。

而 ZEC 和 XMR 之间的“路线”竞争，也并不能在现在就给出论断，认为 ZEC 的可选隐私以及合规路径已经是隐私货币龙头之争的最后赢家，仍然需要更多的时间来进行检验。

四、隐私应用与基础设施：业务联系与行情分化

4.1 广义隐私资产：两轮 ZEC 大幅上涨行情中的表现对照

隐私货币之外的项目并不共享同一业务逻辑。本章先比较广义隐私资产在两轮 ZEC 大幅上涨行情中的表现，再按隐私跨链入口、隐私池、隐私网络和隐私计算分别展开，考察各项目的功能、信任边界、实际使用与独立催化。

广义隐私资产在 ZEC 行情中的整体表现

资产	分类	流通市值	ZEC 第一波大幅上涨行情内表现（2025 年 10 月 1 日 - 2025 年 11 月 16 日）	ZEC 第二波大幅上涨行情内表现（2026 年 8 月 21 日 - 2026 年 9 月 26 日）
NEAR	ZEC 强相关 / Near Intents	68.17 亿美元	-19.17%	+156.08%
NIGHT	隐私智能合约网络	6.71 亿美元	起始时间点未发币	+17.87%
DASH	隐私支付 / Orchard	6.57 亿美元	+174.82%	+85.75%
ZAMA	FHE 保密计算	1.94 亿美元	起始时间点未发币	+75.00%
RAIL	隐私池	1.46 亿美元	+217.19%	+28.79%
AZTEC	隐私智能合约 L2	5,783 万美元	起始时间点未发币	+17.39%
TORN	隐私池	3,382 万美元	-1.90%	+2.39%
FOLD	多方机密计算	1,631 万美元	起始时间点未发币	-24.32%

Gate Research, Data from: Gate & CoinGecko

Gate Research

4.2 隐私跨链入口：NEAR Intents

NEAR 原来并不被归到隐私赛道中，它之前的定位是一条 Layer 1 公链，市场对 Near 链的认知主要停留在分片、高 TPS 和低 Gas 费。其产品 NEAR Intents 最初定位也不是隐私，而是跨链交易与意图执行基础设施，让用户指定想要的结果，由执行方完成兑换和结算。

截至 10 月 14 日，根据 NEAR 官方 Dune 数据，NEAR Intents 总累计成交额约为 349.24 亿美元，ZEC 累计成交额约为 26.58 亿美元，占比约 7.61%，仅次于 USDT、USDC 和 BTC，是 ZEC 换出外部资产，或外部资产换入 ZEC 的重要链上通道。

2026 年 2 月 25 日，NEAR Intents 的隐私功能 Confidential Intents 首次上线，并于 7 月 7 日宣布向所有开发者正式开放。该功能解决了传统链上交易会提前暴露订单信息的问题，通过 NEAR Intents，BTC、ETH、SOL、USDC 等资产能够直接兑换成隐私池中的 ZEC，这让这条

本就重要的、出入 ZEC 的链上通道在叙事层面再度进化，成为“为具有隐私需求的资金，提供了一条通往 ZEC 生态的隐私跨链通道”。

对比 ZEC 和 NEAR 的价格走势，可以非常明显地发现，在 ZEC 第一波大幅上涨行情内（2025 年 10 月 1 日 - 2025 年 11 月 16 日），NEAR 与 ZEC 呈现相反的走势，不具有关联性。而从 Confidential Intents 首次上线开始，NEAR 的走势与 ZEC 高度相似，并且自 2 月 25 日以来的涨幅也是相近的。

NEAR 与 ZEC 的走势对比（自 2025 年 9 月下旬 ZEC 行情起点开始）

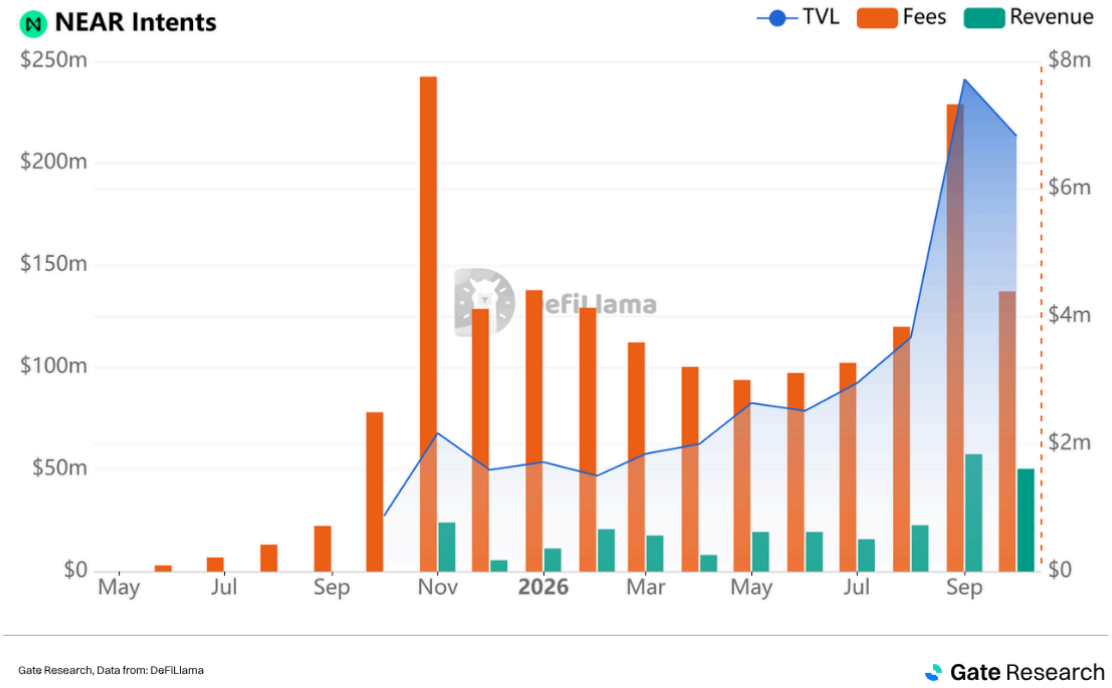


Gate Research, Data from: Gate

Gate Research

再看 DeFiLlama 给出的 NEAR Intents 历史 TVL、手续费以及实际收入数据。2025 年 6 月至 2025 年 11 月，NEAR Intents 的这 3 项数据快速增长，但增长并没有反映在 NEAR 的价格表现上，反而同期的 NEAR 价格是下跌的。而从 2026 年 3 月到 8 月，这个周期内 NEAR Intents 的 3 项数据趋于稳定并且在周期内经过了先下滑后回升的过程，同期 NEAR 的价格却跟随 ZEC 上涨。

NEAR Intents 历史 TVL、手续费以及实际收入数据变化情况



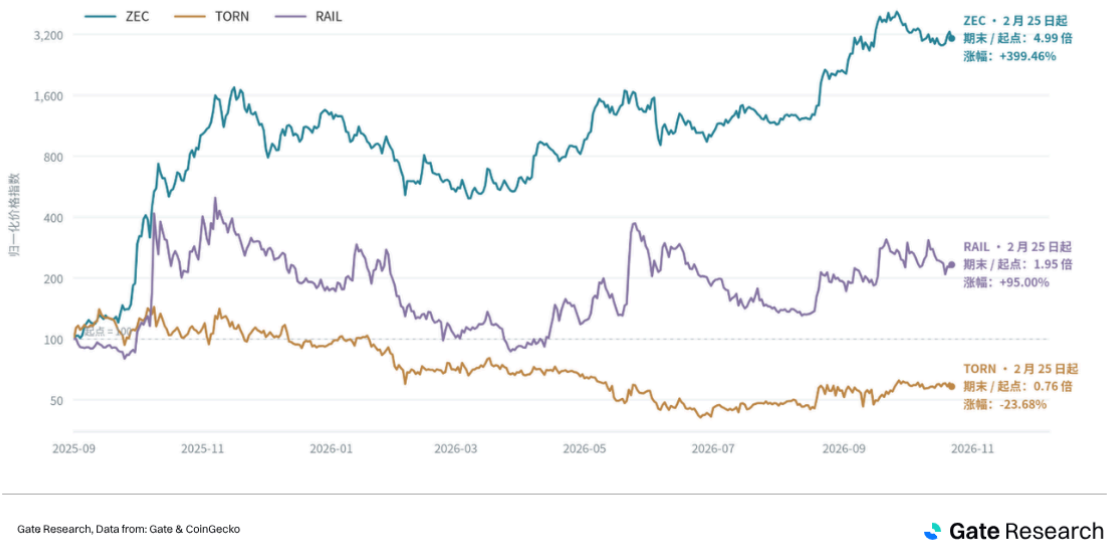
当然，也不能据此完全说 NEAR 的上涨完全由 ZEC 带动，其自身在 NEAR Intents 外还有其它利好。3 月 20 日，Venice 与 NEAR AI 宣布集成，用户可以选择由 NEAR AI 提供的可验证隐私推理服务，NEAR AI 成为 Venice 的底层隐私计算能力提供商之一。9 月 29 日，美国首支 NEAR 现货 ETF Bitwise NEAR ETF（交易代码：NRR）在 NYSE Arca 正式上市。更为准确的结论是，NEAR 正在摆脱原有的 Layer 1 标签，在隐私、AI 以及传统资金进入方面都有了巨大的基本面改善，其叙事与市场定位或将引起价值重估。而在隐私层面与 ZEC 的强相关，以及 NEAR Intents 的隐私功能 Confidential Intents，让 NEAR 在隐私概念中拥有了一个独特的生态位，即“资金出入隐私生态的隐私跨链通道”，这让 NEAR Intents 突破了原有的跨链产品定位，拥有了差异化竞争优势。

4.3 隐私池：从混币工具走向私密 DeFi

4.3.1 功能边界与合规差异

隐私池是大家都比较熟悉的一个隐私细分赛道，核心基本功能就是切断存款与提款之间的公开关联，代表项目是Tornado Cash 与 RAILGUN。来看看 ZEC 本轮行情中，这两个项目与 ZEC 的走势对比。

TORN 和 RAIL 与 ZEC 的走势对比（自 2025 年 9 月下旬 ZEC 行情起点开始）



Gate Research, Data from: Gate & CoinGecko

Gate Research

Tornado Cash 的面临的监管压力较大的问题前文有提及，虽然美国财政部 OFAC 的制裁已被法院认定无效，但开发者 Roman Storm 仍在等待重审以撤销定罪 。因此，其价格走势完全没有享受到 ZEC 上涨为隐私概念整体带来的注意力效应不会太让人感到意外。

4.3.2 RAILGUN：独立催化、隐私池规模与交易活动

要重点分析的是 RAILGUN。RAILGUN 和 Tornado Cash 比较起来，首先在产品层面，它不只是一个“混币器”，还具有连接隐私合约与外部应用的适配模块 Adapt Module。它可以在同一笔原子交易中组织一组操作，先从屏蔽余额中取出相应资产，由共享模块调用外部 DeFi 合约，再将获得的资产重新 shield 回用户的屏蔽余额。例如，用户用私密余额中的 DAI 兑换 WETH。模块先处理 DAI 的支出，再经 0x 路由执行兑换，最后把 WETH 和剩余 DAI 写回屏蔽 note。资产不必先经过用户自己的公开钱包地址，便能完成兑换并回到私密余额。

RAILGUN 也更好地配合了监管需求，有一个去中心化的恶意交易预防系统“Private Proofs of Innocence 私密无罪证明”，该系统使用公开的来自链上的恶意地址集，可以在不影响用户隐私的前提下证明资金来源的安全性，避免用户接受到非法资金。同时，RAILGUN 支持用户通

过只读查看密钥，自愿向审计方披露其钱包余额与交易历史，并提供隐私保护的资金来源筛查证明。

对于 RAILGUN 与 ZEC 之间的价格关联性，在 ZEC 第一波大幅上涨行情内（2025 年 10 月 1 日 - 2025 年 11 月 16 日），RAILGUN 也出现过大幅上涨。但当时 RAILGUN 自身有着同样强劲的注意力因素催化，其背景主要是自 2025 年开始，以太坊创始人 Vitalik Buterin 就越来越多提到以太坊的隐私。

2025 年 9 月 14 日，以太坊基金会发布端到端隐私路线图，旨在为全球第二大区块链构建全面的隐私保护。原“隐私与扩展探索团队”已更名为“以太坊隐私管家（PSE）”，其工作重心从推测性探索转向解决实际问题和优化生态成果。2025 年 10 月 9 日，以太坊基金会宣布成立隐私集群（Privacy Cluster），由 47 位区块链顶尖研究人员、工程师、协调员和密码学专家组成，旨在推动以太坊网络的隐私保护功能。该集群由 Igor Barinov 协调，将整合基金会现有的隐私研发项目，并推动新的隐私相关计划。同日，Vitalik 转发了 Kohaku 路线图，表示全栈隐私和安全是以太坊的首要任务。Kohaku 是一个旨在增强链上隐私和安全性的开源项目。它提供了一个模块化的基础框架，使开发者能够构建安全、注重隐私的钱包，而无需依赖中心化的第三方机构。在 Kohaku 的官方 Github 页面中，文档提到了 3 个保护隐私的资金池协议，RAILGUN 位列其中。

隐私池类型项目的网络效应较强。隐私池的 TVL 规模能够展现其被使用程度，但独立用户数和交易笔数更为重要，难以关联的真实活动越多，隐私池的隐匿效果才越强。将 RAILGUN 的 TVL 与月度进出池数据与其价格走势进行对比，在 ZEC 第二波大幅上涨行情内（2026 年 8 月 21 日 - 2026 年 9 月 26 日），TVL 与月度进出池数据有所上升，但不是突破性增长。

RAIL 价格走势与月度进出池活动以及隐私池 TVL 变化情况的对比



Gate Research, Data from: DeFiLlama & Dune

Gate Research

综上，ZEC 的第二波大幅上涨行情为隐私概念整体带来的市场关注度，对于隐私池赛道的代表项目有所提振。但 TORN 的疲软，说明这种提振作用有限定条件，首先必须更符合监管需求，其次隐私池项目在如今不再局限于传统的混币器功能，它需要承担更多与外部 DeFi 乃至其它区块链技术应用形成交互，承担支付等更多应用，比如通过 RAILGUN 在 Polymarket 上进行匿名预测交易就是一个比较有趣的用例。

4.4 隐私网络：技术路径与信任边界的分化

比较隐私网络，关键不是它们能否通过其隐私实现实现什么具体化的支付、投票或拍卖用例，而是 4 个问题：明文在哪里，谁需要被信任，谁能看到哪些交易信息，以及为此付出了怎样的性能和成熟度代价。TEE 在硬件隔离区内处理明文；Aztec、Midnight 依靠客户端的私有执行与证明，使验证节点不必取得私有输入；Canton 将加密交易视图只分发给有权方；后文的 FHE／MPC 项目则进一步分工密文计算、密钥与解密、证明验证。它们可服务部分相似业务，但保护范围、信任条件和成熟度不等价，所用技术也不是互斥组件。

4.4.1 Oasis 与 Secret：TEE 保护合约执行，应用需求决定采用

这类型的项目包括 Oasis、Secret 等。它们不是将全链改造成可选或强制匿名账本，而是让合约处理敏感内容而不在链上公开，实现的基本流程都是“用户先加密敏感输入 → 节点在 SGX 隔离区内解密并执行合约 → 将需要保密的结果和合约状态重新加密后保存”。

Oasis 和 Secret 实现这种隐私合约执行的技术路线都差不多，都是通过英特尔 SGX 硬件来建立 TEE（可信执行环境）。SGX 在处理器中提供 enclave（安全隔离区），让合约在连操作系统和服务器管理员也不能直接读取内部数据的隔离区中运行。用户对敏感数据进行加密输入后，节点在 SGX 硬件的安全隔离区内解密并执行合约。但只有硬件支持还不够，一台服务器即使支持 SGX，普通程序也不会自动获得保护。开发者需要将合约执行程序、解密逻辑和密钥处理放入 enclave，配好运行这些程序所需的软件环境。网络收发、磁盘读写等工作可以留在外部，但跨过隔离边界的数据必须受到保护。例如，外部软件收到加密报价后，把密文送入 enclave；区内程序解密、比较报价，再将应保密的状态加密后交出去。硬件负责阻止外部直接读取或篡改，区内软件负责决定怎么算、保存什么、公开什么。只有都做好了，才能算通过 SGX 硬件建立起了合格的 TEE。

因此这种类型的项目，潜在缺陷也很明显，那就是得保证这个 TEE 不被攻破，必须信任 SGX 硬件及其配套软件的隔离机制没有被攻破。否则，隔离区里的密钥和明文就可能暴露。

由于提供的是针对合约计算执行层面的隐私，该类型项目就很看生态内是否有能够带来实际使用需求的项目。从目前的情况看，隐私计算公链这个方向遇到了很大的发展瓶颈。截至 2026 年 10 月 18 日，Oasis 的 TVL 只有不到 50 万美元，Secret 则遭遇了很大的内部混乱，SCRT Labs 想要将链迁移到 Arbitrum，已经于 9 月 1 日停止对 Layer 1 级别的开发和支持。

Oasis 与 Secret 的 TVL 变化情况

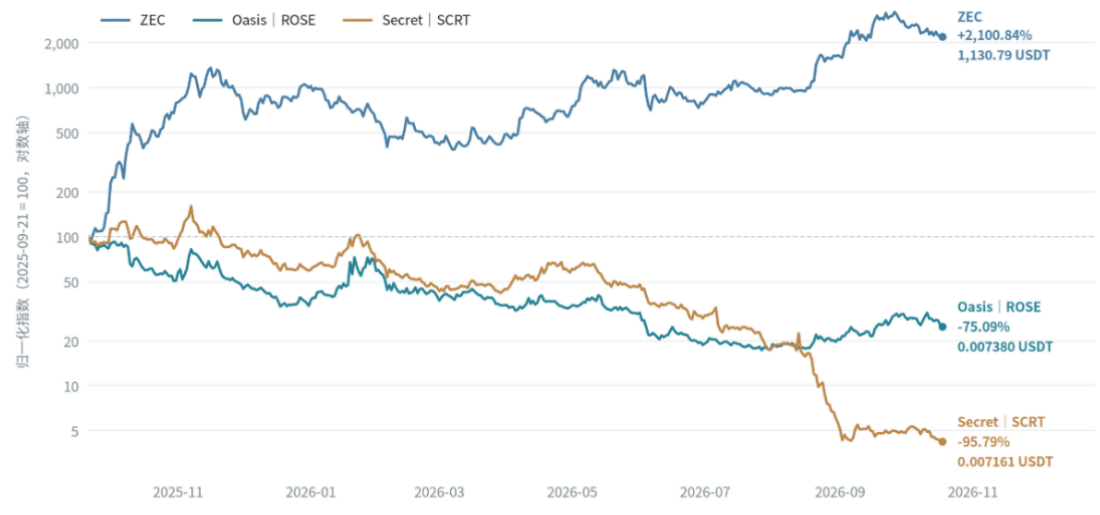


Gate Research, Data from: DeFiLlama

Gate Research

将这两个项目的代币价格走势和 ZEC 进行对比，可以非常明显地看出，它们像是在隐私概念中被遗忘了。但仍然正常运行的 Oasis，在 ZEC 第二波大幅上涨行情内（2026 年 8 月 21 日 - 2026 年 9 月 26 日），还是在价格表现上有些许回暖。

ROSE 和 SCRT 与 ZEC 的走势对比（自 2025 年 9 月下旬 ZEC 行情起点开始）



Gate Research, Data from: Gate & CoinGecko

Gate Research

4.4.2 Aztec：零知识证明驱动的隐私 L2

这类型的代表项目是 Aztec 和 Midnight。Aztec 是以太坊上的隐私优先 Layer 2，主要依靠零知识证明（ZKP），而不是 SGX + TEE 来保护私密计算。

Aztec 所实现的基本流程是“用户在本地执行私有合约并生成证明 → 网络验证证明、更新状态并完成必要的公开执行 → 将批量状态转换证明提交以太坊验证和结算”。从发挥的隐私作用来说，Aztec 能做的，大体上 TEE 路线公链也能做。而 Aztec 相比于 TEE 路线公链的优势在于减少了验证节点对隐私内容的接触。在执行隐私计算时，Aztec 不需要用户将明文交给执行节点，例如用户可以证明自己有足够余额、转账符合规则，而不公开完整余额和私有输入。零知识证明让节点在不知道秘密内容的情况下，仍能检查计算是否符合规则，因此即使攻击者读取了验证节点的内存，也拿不到隐私内容。

为了这个优势，Aztec 要面临的困难是工程复杂度远高于 TEE 路线公链，开发周期实在太长。该项目在 2022 年就获得了 a16z crypto 领投的 1 亿美元 B 轮融资，但到今年 3 月才上线首个提供完整执行环境的 Alpha Network 版本。7 月激活 Alpha V5 后，又在 7 月 27 日发现 V5 证明系统存在严重漏洞。

但 Aztec 也已经足够优秀。证明时间方面， Alpha V5 在 M2 MacBook（12 核限至 8 核）上完全私有代币转账的原生客户端证明时间约为 2.5 秒，JavaScript / V8 环境约为 6.8 秒。需要继续提升的是出块间隔时间、用户感知交易延迟时间以及 TPS。出块间隔时间方面，2026 年 7 月 21 日官方发布的 Alpha V5 说明称，平均出块间隔时间从 14 秒降至 6 秒。但通过调用 Aztec 主网公开 RPC，取连续 50 个区块（区块编号 136,108 至 136,157）所计算出来的平均值为 73.47 秒。用户感知交易延迟时间与 TPS 方面，Aztec 现在给出的发展目标是中位数 12 秒 / 10 TPS。整体来看，Aztec 当前的成熟度与速度仍和主流公链存在差距。

将 AZTEC 的价格走势和 ZEC 进行对比，在 ZEC 第一波大幅上涨行情内（2025 年 10 月 1 日 - 2025 年 11 月 16 日），Aztec 还未 TGE，无法进行对比分析。而在 ZEC 第二波大幅上涨行情内（2026 年 8 月 21 日 - 2026 年 9 月 26 日），AZTEC 的价格展现出了跟涨回暖的态势。考虑到 Aztec 的实际开发进展日久且艰，认为 ZEC 对 AZTEC 的价格表现起到了一定的带动作用有着合理性。

AZTEC 与 ZEC 的走势对比（自 2025 年 9 月下旬 ZEC 行情起点开始）



Gate Research, Data from: Gate & CoinGecko

Gate Research

4.4.3 Midnight：零知识证明驱动的合作公链

Midnight 也是走零知识证明路线的隐私链，但它是作为一条 Cardano 的隐私增强型“合作公链（partner chain）”出现的。Midnight 是拥有自己账本和共识的公链，不把交易 roll up 回 Cardano。它通过 Compact 将合约交互拆成本地私有数据、证明规则和公开账本更新。尽管有这样的区别，但技术实现呈现出来的效果没有太大差异，Midnight 也是让私有状态和相关数据在用户设备或钱包本地加密保存，客户端产出证明，网络据此验证规则满足而不提交见证。

将 NIGHT 的价格走势和 ZEC 进行对比，在 ZEC 第一波大幅上涨行情内（2025 年 10 月 1 日 - 2025 年 11 月 16 日），Midnight 还未 TGE，无法进行对比分析。TGE 后一段时间的价格上涨后，NIGHT 进入了长达半年左右的价格下行调整。最近的价格上涨与 ZEC 第二波大幅上涨行情（2026 年 8 月 21 日 - 2026 年 9 月 26 日）是错开的，并且有其自身的利好催化，即 9 月 28 日 Midnight 主网正式上线了无需许可的智能合约部署。

NIGHT 与 ZEC 的走势对比（自 2025 年 9 月下旬 ZEC 行情起点开始）



Gate Research, Data from: Gate & CoinGecko

Gate Research

4.4.4 Canton：按需知悉架构下的机构结算网络

这是最为特别的一个隐私网络细分分类，因为它可以被列入到广义的隐私网络范畴，但实际上更像服务于机构的 RWA 基础设施。

这类型的代表项目是 Canton。Canton 对隐私功能的实现主要靠架构设计，通过“按需知悉”的交易视图分区和定向分发实现隐私，只有有权方能读取内容。例如，一笔原子交易包含“A 向 B 付款、B 再向 C 付款”。Canton 可以让 A 只看到第一段，C 只看到第二段，B 看到两段；每方验证自己相关的部分，再由协议协调确认。这种隐私的实现是从架构上就不让所有节点拥有完整交易，限制数据分发范围并进行局部验证。

机构间结算可以使无关节点看不到成交金额、价格和对手方业务内容，同时让获授权的审计者读取必要信息。Canton 实际上更接近金融业务的数据权限控制，而不是加密货币典型的隐私技术实现，这就是为什么说虽然它可以被列入到广义的隐私网络范畴，但实际上更像服务于机构的 RWA 基础设施。

综上，Canton 的代币走势几乎不与 ZEC 代币价格走势呈现相关性的结果是显而易见的，通过走势对比图也可以非常明显地看出。

CC 与 ZEC 的走势对比（自 2025 年 9 月下旬 ZEC 行情起点开始）



Gate Research, Data from: Gate & CoinGecko

Gate Research

4.5 隐私计算：为既有区块链提供机密执行能力

隐私计算类项目为既有区块链应用提供机密执行能力。它们与前文隐私网络在支付、投票、拍卖等业务目标上存在重叠，但不能仅凭场景名称认定能力或成熟度等价。本章讨论的 Zama 与 The Interfold 不另建一条新的公链或 Layer 2，而是依托已有区块链组织机密计算服务；区别首先在部署与执行方式，而非哪一类独占某种隐私用例。

在这里主要的分析对象是 Zama 与 The Interfold，原因是他们所采用的技术路径与前面在分析隐私网络时所提到的 TEE、零知识证明以及机构按需知悉都不相同。

4.5.1 Zama：全同态加密与隐私 DeFi 应用

代表项目是 Zama。Zama 为 Ethereum 等现有链提供机密合约能力。开发者通过 fhEVM 在 Solidity 合约中使用加密数值及对应运算，选择哪些内容公开、哪些内容保持加密。

Zama 采用的技术路线是全同态加密（FHE）。和零知识证明相比，全同态加密的优势在于“计算者不看明文输入，也能执行运算”，而单纯的零知识证明主要解决“验证者不看私有输入，也能确认计算符合规则”。举例来说明这种优势的话，假设有一个拍卖需要确定最高出价者，但所有买方既不愿公开出价，也不愿让拍卖运营者看到出价。甲只知道自己的报价，乙只知道自己的报价，其他买方也是如此。运营者收到的是加密报价。

这里有两个不同任务：一是检查每份报价是否合法，二是把所有报价放在一起比较，算出赢家。验证各份输入合法，并不等于已经知道它们之间谁最高。因此，单独使用零知识证明，可以完成前一个任务，却不会自动完成后一个任务。而全同态加密则提供了直接处理这些隐私输入的办法。买方按协议将报价加密，运营者不取得解密密钥，也能在密文上执行比较和条件选择，产生加密的赢家结果；最后只由获授权的机制解密必要结果，不必先公开全部报价。

全同态加密的劣势则在于成本。全同态加密密文中存在密码学噪声，运算会消耗可用的噪声预算。自举（bootstrapping）可以在不公开明文的情况下刷新密文，让计算继续进行，但这个步骤非常耗费算力，对硬件要求很高。2026 年 7 月 27 日，Zama 宣布在配备 8 块 NVIDIA H100 (SXM5) GPU 的单节点上达到了 1,040 TPS，场景是 ERC-7984 隐私转账。虽然这一目标比预期提前了一年实现，而且是在通用 GPU 而非定制硬件上完成的，但想要支撑机构级的大规模采用，仍然远远不够。

将 ZAMA 的价格走势和 ZEC 进行对比，在 ZEC 第一波大幅上涨行情内（2025 年 10 月 1 日 - 2025 年 11 月 16 日），ZAMA 还未 TGE，无法进行对比分析。最近的价格上涨与 ZEC 第二波大幅上涨行情（2026 年 8 月 21 日 - 2026 年 9 月 26 日）有一定重叠，但更多源于 Zama 自身的基本面变化。9 月 17 日至 10 月 5 日，Zama 的屏蔽池 TVL 从 超 6,500 万美元快速增长至超 1 亿美元。9 月 15 日，Zama 宣布“隐私 DeFi（Confidential DeFi）”进入规模化阶段，这是 Zama 对自身的新定义，同时一次性上线 16 个隐私金库并推出隐私 Swap 协议；9 月 17 日又与 Merkl 打通，让隐私代币接入激励分发。更早一些的时候，它与 Steakhouse、Morpho 合作的首个隐私金库 TVL 在 2 个多月的时间里达到 4,000 万美元，跻身 Morpho 上 USDC 金库前 10。全同态加密这个技术标签正在逐渐被 Zama 淡化，市场正在以隐私 DeFi 生态的角度对 Zama 重新定价。

ZAMA 与 ZEC 的走势对比（自 2025 年 9 月下旬 ZEC 行情起点开始）



Gate Research, Data from: Gate & CoinGecko

Gate Research

4.5.2 The Interfold：多方协作与门限解密

代表项目是 The Interfold。The Interfold 让应用可以请求一个临时的加密执行环境（E3），让多个参与者提交私密输入，按事先约定的程序计算共同结果。

The Interfold 并非单纯的多方计算系统，而是将同态加密、分布式门限密码学和零知识证明组合使用。同态加密负责处理密文，多方计算／门限机制主要负责分散解密权，零知识证明则检查计算和密钥操作是否正确。理解这项分工，再看其私密投票用例，就不会把“多个节点参与”误解为每个节点都能读取选票。

多方计算（MPC）的核心思路，是让多个参与方在不向彼此公开秘密输入的情况下共同完成计算。举例来说明这种能力，假设一个组织需要投票决定是否通过提案，但成员既不愿公开自己的选择，也不愿让计票运营者看到选票。Fold 为这次投票选出一个节点委员会，由成员协同生成加密公钥，各自持有解密密钥份额，单个节点没有完整解密能力。投票者用公钥加密选票，计算提供者直接在密文上计票，并提交计算正确性的证明；最后，委员会共同提供足够的解密份额，只公布总结果，不公开个人选票。

当然，The Interfold 能实现上面这个举例，是因为它不是一个单纯的多方计算系统，而是将同态加密、分布式门限密码学和零知识证明组合使用。同态加密负责处理密文，多方计算／门限机制主要负责分散解密权，零知识证明则检查计算和密钥操作是否正确。

这套技术方案的劣势在于协调成本与安全门限。节点需要交换信息、生成密钥份额并验证证明，结果解密也依赖足够成员在线配合。The Interfold 的 Alpha 上线公告披露，当时一次分布式密钥生成仍需数小时。同时，“单个节点无法解密”不等于“任何情况下都无法泄露”，达到解密门限的成员如果串谋，仍可能解密同一公钥下的私密输入。

FOLD 在今年 8 月 19 日才完成 TGE，可观察周期过短。并且由于存在新币上新交易所，以及以太坊创始人 Vitalik Buterin 在 The Interfold 的第一轮 CCA 公开拍卖中投入了 16 ETH 等新币种特有的利好，其近期价格走势独立性较强，难以说明 ZEC 的上涨对其价格走势发挥了直接作用。

五、市场研判与总结：隐私需求与投资主线仍需区分

5.1 隐私货币：价值重估与长期共识

原生隐私货币可能被重估，关键不只是隐私交易需求增长，而是市场是否将其理解为需要长期持有或用于结算的价值载体。ZEC 在长期隐私定位的基础上，以货币属性提供了新的叙事角度，合规基本面及资金接入渠道的改善则为重估提供了条件；这与单纯将其视为匿名转账工具不同。XMR 则有早于 ZEC 的独立恢复周期，并保持较高的隐私交易规模；ZEC 与 XMR 分别体现可选隐私、货币定位与资金接入，以及强制隐私与实际使用的不同取舍，不能仅以某一阶段的涨幅判断哪条路线已成为最终胜者。

5.2 隐私应用：生态扩展与效率、成熟度约束

隐私应用或服务项目不能因具备隐私标签，便与原生货币采用同一估值逻辑。其代币是否受益，取决于费用、质押、治理或其他机制能否把真实使用传导为持有需求；不同项目还应分别考察隐私机制与信任边界、效率及用户体验、合规接入方式和产品成熟度。业务扩张与技术进步是观察采用的线索，不能以阶段性价格同步替代对自身价值捕获机制的检验。

5.3 总体结论

综合全文，本轮 ZEC 的资产重估为较广泛的隐私概念标的带来了短期关注与价格催化，但多数标的未持续摆脱长期低价结构，也未形成可确认的长期趋势反转；因此，它不是所有隐私项

目共同进入新估值区间的共同牛市。XMR 有自身更早开始的独立恢复周期，DASH 的部分行情共振和隐私功能强化也不足以证明流动性已向整个赛道持续扩散。

判断能否由阶段性关注走向持续重估，需先区分谁需要持有资产：对于原生隐私货币，应检验持有或结算需求是否扩大；对于应用或服务代币，则须检验费用、质押、治理等机制是否使使用转化为资产持有人的经济价值。技术和业务使用本身并不自动实现代币价值捕获；ZEC 的强势走势也不能证明 Orchard 历史漏洞未曾被利用，安全历史风险仍需继续面对。

Canton 的按需知悉架构服务于机构结算与 RWA 的独立业务路径，应与 NEAR 的跨链入口、RAILGUN 和 Zama 的私密 DeFi、其他网络及计算服务分别观察，不能用 ZEC 主题行情概括。业务联系、技术借用和阶段性价格同步可以构成研究线索，却不能替代对各项目自身需求与价值捕获路径的检验。

若在行情冷却后，相关项目仍能持续呈现真实使用，且原生货币的持有或结算需求、应用或服务代币的价值捕获能够由资产持有人承接，并同时经受安全边界、合规接入与用户体验的检验，则应重新评估其是否已形成稳定且更广泛的投资主线。在此之前，研究重点仍应从是否带有隐私标签转向解决了什么需求、谁因此需要持有资产、风险由谁承担。

参考链接：

- CoinGecko, https://www.coingecko.com/en/categories/privacy-coins
- CoinGecko, https://www.coingecko.com/en/categories/privacy
- Dash, https://www.dash.org/news/dash-complies-with-the-financial-action-task-force/
- X, https://x.com/Dashpay/status/1984644020560413099
- X, https://x.com/naval/status/1973254136394293708
- Wired, https://www.wired.com/2015/11/zerocoin-startup-revives-the-dream-of-truly-anonymous-money
- Github, https://github.com/ZcashFoundation/ZcashFoundation/blob/master/board-documents/minutes/2018-06-28.md

- Zama, https://www.zama.org/post/1000-tps-confidential-transfers-gpu-zama-protocol
- Midnight, https://midnight.network/blog/state-of-the-network-september-2026
- Secret, https://forum.scrt.network/t/community-continuance-of-secret-network-l1/8011
- Aztec, https://docs.aztec.network/participate/alpha
- Dune, https://dune.com/railgun_project/railgun
- DeFiLlama, https://defillama.com/protocol/near-intents
- Nansen, https://nansen.ai/post/near-q3-2026-report

Gate 研究院是一个全面的区块链和加密货币研究平台，为读者提供深度内容，包括技术分析、热点洞察、市场回顾、行业研究、趋势预测和宏观经济政策分析。

免责声明

加密货币市场投资涉及高风险，建议用户在做出任何投资决定之前进行独立研究并充分了解所购买资产和产品的性质。 Gate 不对此类投资决策造成的任何损失或损害承担责任。

相关链接

Gate研究院社媒

往期研究报告

关于 Gate 研究院

Gate 研究院是专注于区块链产业研究的专业机构，长期致力于深入研究区块链产业发展趋势 ， 为从业人员和广大区块链爱好者提供专业、前瞻性的产业洞察。我们始终秉持着普及区块 链知识的初心，力求将复杂的技术概念转化为通俗易懂的语言，透过对海量数据的分析和对市 场趋势的敏锐捕捉，为读者呈现区块链行业的全貌，让更多人了解区块链技术，并参与这个充 满活力的产业。

免责声明:本报告仅用于提供研究和参考之用，不构成任何形式的投资建议。在做出任何投资决策前，建议投资者根据自身的财务状况、风险承受 能力以及投资目标，独立做出判断或咨询专业顾问。投资涉及风险，市场价格可能会有波动。过往的市场表现不应作为未来收益的保证。我们不对 任何因使用本报告内容而产生的直接或间接损失承担责任。

本报告中包含的信息和意见来自 Gate 研究院认为可靠的专有和非专有来源，Gate 研究院不对信息的准确性和完整性作出任何保证，也不对因错误 和遗漏(包括因过失导致的对任何人的责任)而产生的任何其他问题承担责任。本报告所表达的观点仅代表撰写报告时的分析和判断，可能会随着 市场条件的变化而有所调整。