

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

JONATHAN BECKWITH, *on behalf of
himself and all others similarly situated,*

Plaintiff,

v.

JEFFY YU AND AGUSTIN “TINT”
CORTES,

Defendants.

Case No.: 1:26-cv-01091

**COMPLAINT FOR
DAMAGES**

**JURY TRIAL
DEMANDED**

I. PRELIMINARY STATEMENT.....	4
II. PARTIES.....	6
A. Plaintiff.....	6
B. Defendants.....	7
III. JURISDICTION AND VENUE.....	8
A. Subject-Matter Jurisdiction.....	8
B. Personal Jurisdiction.....	8
IV. FACTUAL ALLEGATIONS.....	10
A. The Project as Defendants Presented It to the Market.....	10
i. Zerebro: The AI Agent.....	11
ii. ZerePy: Developer Grade Infrastructure.....	12
iii. Zentients: The Consumer-Facing Launchpad.....	15
iv. Zerebro Token: The Economic Layer.....	20
B. The Founders’ Roles, Credentials, and Credibility Signals.....	22
C. The Reality: No Functioning Technology Ever Existed.....	29
i. Overview of the Fraud Scheme.....	29
ii. The Absence of a Functioning Product.....	30
D. The Token Launch and the Architecture of Financial Engineering.....	32
i. Overview.....	32
iii. The Allocation Wallet Structure.....	33
iv. The Purpose of This Structure.....	37
E. The Defendants’ Undisclosed Market-Making Operation.....	37
i. The Allocation 3 Market-Making Complex.....	37
ii. The Purpose of the Cascading Structure.....	40
iii. What This Looked Like to Retail Traders.....	40
iv. Value Extraction.....	40
v. Attribution of Market-Making Activity to Defendants.....	41
vi. Conclusion on Attribution.....	45
F. The “Research and Development” Narrative as Post-Launch Maintenance Fraud.....	46
G. From Peak to Collapse.....	46
H. Escalation, Concealment, and Consciousness of Guilt.....	46
V. CLASS ALLEGATIONS.....	54
A. Class Definition.....	54
B. Rule 23(a) Requirements.....	55
C. Rule 23(b) Requirements.....	56
D. Rule 23(c)(4) Issue Certification in the Alternative.....	56
E. Ascertainability and Manageability.....	57

VI. CAUSES OF ACTION.....	57
COUNT I	
Deceptive Acts and Practices (N.Y. Gen. Bus. Law § 349).....	57
COUNT II	
False Advertising (N.Y. Gen. Bus. Law § 350).....	58
COUNT III	
Negligent Misrepresentation.....	59
COUNT IV	
Fraud / Fraudulent Inducement.....	60
COUNT V	
Breach of Contract.....	61
COUNT VI	
Unjust Enrichment.....	63
VII. PRAYER FOR RELIEF.....	63

I. PRELIMINARY STATEMENT¹

1. This action arises from a coordinated fraud scheme to market and sell a digital asset by falsely presenting it as the economic backbone of a long-term artificial-intelligence infrastructure project, when in reality no such technology existed and Defendants secretly controlled, manipulated, and monetized the market for the asset.
2. Defendants Jeffy Yu and Agustín “Tint” Cortes promoted a project called “Zerebro” as a venture-grade AI platform designed to power autonomous agents, developer tooling, and a consumer launchpad that would define the future of on-chain artificial intelligence. They represented that Zerebro was real technology, already built or nearing deployment, and that its associated token, \$ZEREBRO, derived value from its role as the economic layer of that ecosystem.
3. Those representations were false. Defendants never built a functioning autonomous agent, developer framework, consumer launchpad, or proprietary AI infrastructure. The products that Defendants repeatedly described as operational, in testing, or imminent did not exist in any usable form. The technical narrative used to justify the token’s value was fictional.
4. At the same time that Defendants were promoting Zerebro as a legitimate AI venture, they were secretly operating the market for \$ZEREBRO themselves. From the moment the token was created, Defendants controlled a substantial portion of the total supply at zero cost. Using a coordinated network of wallets they funded and controlled, Defendants acted as undisclosed market makers by injecting liquidity, manufacturing trading volume, influencing price formation, and selling their own holdings into the demand their false narrative had created.
5. Purchasers were never told that Defendants were the dominant participants in the market, that trading activity was being engineered by issuer-controlled wallets, or that the apparent liquidity and price stability were not the result of organic adoption. To the

¹ Unless otherwise indicated, the allegations in this Complaint are based on Plaintiff’s personal knowledge as to Plaintiff’s own acts and experiences and, as to all other matters, on information and belief. Plaintiff’s information and belief is based on the investigation of counsel, including review and analysis of publicly available information (including Defendants’ statements, websites, written materials, interviews, podcasts/livestreams, and social-media communications), press reporting, and, where relevant, on-chain/blockchain records and transaction data, as well as other information obtained through counsel’s investigation.

public, \$ZEREBRO appeared to be trading in an open and fair market driven by genuine interest in a real technology platform. In reality, Defendants were trading against the public while concealing their role.

6. The scheme depended on this dual deception. The false technology story created demand by persuading purchasers they were buying into a long-term AI infrastructure project. The undisclosed market-manipulation apparatus allowed Defendants to monetize that demand by selling zero-cost inventory at inflated prices. Purchasers supplied the capital. Defendants extracted the value.
7. Defendants' roles were complementary and deliberate. Yu served as the project's self-described technical founder, issuing detailed claims about AI autonomy, jailbreaking, model architecture, memory, and deployment that he knew were false. Cortes served as the project's economic and market architect, promoting tokenomics, liquidity design, value accrual, and ecosystem growth while participating in the undisclosed trading and off-ramping of proceeds. Together, Defendants presented the outward appearance of a legitimate venture-style founding team while executing a coordinated fraud.
8. When the absence of real technology could no longer be concealed and Defendants' artificial market support waned, the price of \$ZEREBRO collapsed, causing substantial losses to purchasers. By that time, Defendants had already exited significant portions of their positions.
9. During the token price collapse, as purchasers questioned the absence of any delivered technology, Defendants did not correct their prior statements or disclose the truth. Instead, they turned on each other publicly, each attempting to shift blame for the scheme's operation and the resulting losses. These accusations were not accompanied by any disclosure of the true structure of the project or the market activity that Defendants had concealed from the public.
10. During this period, Defendant Yu escalated the deception by publicly staging his own death, broadcasting what appeared to be a suicide and arranging for an obituary to be published. This episode diverted attention from the project's collapse, the missing technology, and the mounting questions regarding insider conduct and token proceeds. Yu later resurfaced alive, posting photographs of himself holding large amounts of cash and continuing to launch additional cryptocurrency projects. This conduct was not an

aberration; it was a continuation of Defendants' pattern of evasion when confronted with accountability.

11. Defendants' attempts to deflect blame are contradicted by objective, verifiable on-chain evidence. As detailed in this Complaint, forensic blockchain analysis demonstrates that the wallets used to create, distribute, trade, and off-ramp \$ZEREbro were controlled by Defendants and reused across the lifecycle of the scheme. The same wallet infrastructure was recycled across multiple related projects associated with Defendants, eliminating any plausible claim that the trading activity was conducted by independent third parties.
12. This technical evidence establishes that the market manipulation was not accidental, external, or the work of unknown actors. It was a centralized operation executed through wallets Defendants controlled from inception, funded with zero-cost inventory, and concealed from purchasers while Defendants extracted value. Defendants' post-collapse conduct (*e.g.* mutual accusations, fabricated explanations, and staged disappearance) confirms their consciousness of guilt and underscores that the collapse was not the result of market forces, but of a scheme that could not survive exposure.
13. This case is not about a failed startup or ambitious founder, it is about misrepresentations, concealed market manipulation, and the deliberate exploitation of public trust in emerging technology.

II. PARTIES

A. Plaintiff

14. Plaintiff Jonathan Beckwith is a citizen of Canada. During the Class Period, Beckwith purchased \$ZEREbro tokens through blockchain-based trading mechanisms. Beckwith purchased and held \$ZEREbro in reliance on Defendants' representations that the project was supported by genuine, actively developed AI infrastructure, including the Zerebro autonomous agent, the ZerePy framework, and the Zentients platform. After the scheme collapsed and the founder's staged disappearance, it became apparent that purchasers including Beckwith had been misled.

B. Defendants²

15. Defendant Jeffy Yu (“Yu”) is a natural person whose state of residence is presently unknown. Based on publicly available information, Yu has indicated that he intends to relocate to New York, New York. Plaintiff will amend these allegations as discovery confirms Yu’s domicile. Yu is a co-founder of Zerebro and, at all relevant times, personally participated in, directed, and/or solicited the public distribution of the \$ZEREBRO Token.
16. Defendant Yu served as the project’s self-described technical founder and was the primary source of all statements and misrepresentations concerning Zerebro’s alleged artificial-intelligence capabilities, training processes, autonomy, and product development.
17. In addition, Defendant Yu personally authored or approved the project’s white paper, structured it to resemble academic research, and appeared as the principal spokesperson on numerous podcasts, livestreams, and interviews—where he repeatedly made detailed technical claims that were knowingly false.
18. Defendant Agustín “Tint” Cortes (“Cortes”) is a natural person who resides in San Francisco, California. He is the co-founder of Zerebro, and at all relevant times personally participated in, directed, and/or solicited the public distribution of the \$ZEREBRO Token.
19. Cortes’ statements were material because they concerned the project’s economic fundamentals, roadmap milestones, utility framework, and promises that the token would appreciate based on Defendants’ execution of a multi-product ecosystem. These economic statements were distinct from, but fully intertwined with, Yu’s technical misrepresentations.
20. Defendants Yu and Cortes jointly disseminated the deceptive marketing campaign through X posts, white-paper releases, podcast appearances, interview circuits, roadmap publications, and coordinated messaging across social media platforms—including Telegram, Discord, Warpcast, and Instagram.

² Screenshots of Defendant’s public profiles and identity-verification indicators are attached as Exhibit A and are incorporated here by reference.

21. Where this Complaint alleges misrepresentations made by both Defendants, those allegations reflect (i) statements made jointly; (ii) statements made through official Zerebro channels bearing no distinction between speakers; or (iii) statements where each Defendant's individual contributions formed an inseparable part of a unified fraudulent narrative.³

III. JURISDICTION AND VENUE

A. Subject-Matter Jurisdiction

22. This Court has subject-matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The putative Class consists of well over 100 persons, including residents of multiple states throughout the United States.
23. Minimal diversity exists under 28 U.S.C. § 1332(d)(2) because at least one member of the proposed Class is a citizen of a state different from at least one Defendant, 28 U.S.C. § 1332(d)(2)(A), and because Plaintiff Beckwith is a citizen of Canada and at least one Defendant is a citizen of a State, 28 U.S.C. § 1332(d)(2)(B).
24. The aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs, as required by 28 U.S.C. § 1332(d)(2) and § 1332(d)(6). The fraudulent \$ZEREBRO meme-token scheme at issue caused losses totaling tens of millions of dollars to members of the Class.
25. No exception to CAFA jurisdiction applies, including the discretionary exception in 28 U.S.C. § 1332(d)(3) and the "home-state" and "local-controversy" exceptions set forth in 28 U.S.C. § 1332(d)(4).

B. Personal Jurisdiction

26. Defendants are subject to specific personal jurisdiction in this District under Fed. R. Civ. P. 4(k)(1)(A) and N.Y. C.P.L.R. §§ 302(a)(1) and 302(a)(3)(ii).
27. First, jurisdiction is proper under C.P.L.R. § 302(a)(1) because Defendants purposefully transacted business in New York by disseminating a sustained promotional campaign nationwide through the internet (including into New York) to induce purchases of \$ZEREBRO, and by launching, offering, and selling \$ZEREBRO through internet and blockchain-based mechanisms that were open to New York purchasers and were in fact

³ To the extent this Complaint references conduct by "Defendants," such references concern conduct jointly undertaken, jointly planned, or jointly disseminated, or reflect statements where the speaker's identity was not reasonably discernible to consumers because the Zerebro project communicated through unified channels.

used by putative class members. For example, an unnamed class member who is a resident of New York suffered losses of approximately \$10,435.41 while transacting with Defendants in New York.

28. Defendants' challenged misrepresentations and omissions were disseminated to induce \$ZEREBRO purchases (including purchases in New York), and Defendants profited from those purchases by selling and providing liquidity into the resulting market through wallets and accounts they controlled.
29. Independently, jurisdiction is proper under C.P.L.R. § 302(a)(3)(ii) because Defendants committed tortious acts outside New York (including originating and disseminating the fraudulent statements and omissions from outside the state and operating the issuer-controlled market-making scheme from outside the state) that caused injury to purchasers in New York when purchasers initiated and executed their \$ZEREBRO purchase transactions from New York and parted with consideration there. Defendants knew or reasonably should have expected their conduct to have consequences in New York because they marketed and sold \$ZEREBRO nationwide via the internet and blockchain-based trading mechanisms that they made available to New York purchasers. Defendants also derived substantial revenue from interstate and international commerce, including tens of millions of dollars obtained from \$ZEREBRO purchasers across multiple states.
30. Defendants' New York-connected conduct is further confirmed by their deliberate choice to structure the scheme's liquidity, trading, and monetization through (i) the Solana ecosystem which is principally operated by Solana Labs, which has a significant engineering presence in New York City by way of their downtown New York City office where engineers have made substantial GitHub commits, (ii) centralized-exchange off-ramp channels including Coinbase, a virtual-currency business licensed by the New York State Department of Financial Services to operate in New York, and (iii) OpenSea, a digital-asset marketplace headquartered in this District, through which Defendants offered and sold Zerebro NFTs as part of the promotional scheme; these were not incidental technical details but core rails Defendants selected and used to execute and profit from the scheme.

31. Defendants also knew or reasonably should have expected New York consequences because the scheme depended on (and Defendants affirmatively selected) New York-facing virtual-currency rails, including off-ramping and custodial exchange channels licensed by the New York State Department of Financial Services to operate in New York (including Coinbase) and digital-asset marketplaces headquartered in New York through which Defendants distributed Zerebro-branded NFTs (including OpenSea). But for Defendants' deliberate reliance on these platforms and exchange rails (and the Solana-based liquidity and trading venues Defendants used to create and sustain the market), the scheme could not have been executed at scale in the manner alleged.

C. Venue

32. Venue is proper in this District pursuant to 28 U.S.C. Section 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

33. Those events include, among other things, Defendants' direction of material communications and/or misrepresentations into this District; Defendants' offer and sale of Zerebro-branded NFTs through OpenSea, a digital-asset marketplace headquartered in this District; purchasers' receipt of those communications in this District; purchasers' decision-making and purchase transactions in this District; and the resulting injury and damages incurred in this District.

34. Purchasers' economic losses, including out-of-pocket expenditures and resulting injury, were sustained within this District.

IV. FACTUAL ALLEGATIONS

A. The Project as Defendants Presented It to the Market

35. Defendants presented Zerebro as a foundational AI-infrastructure project: a platform intended to support the creation, deployment, and monetization of autonomous artificial-intelligence agents across social media and blockchain networks. They described it as a multi-layered technology stack, used analogies to foundational internet protocols, and positioned Zerebro as a base layer for a new category of autonomous digital agents.

36. Defendants reinforced these claims by adopting the conventions of legitimate technology ventures. Defendant Yu published research white papers formatted to resemble academic

work.⁴ Defendant Cortes leveraged industry connections to secure appearances on prominent cryptocurrency podcasts and amplify the project to retail investors. Together, they presented the image of a credentialed founding team building real infrastructure.

i. Zerebro: The AI Agent

37. In white papers, podcast appearances, and social media posts, Defendants presented Zerebro as a multi-layered AI infrastructure platform. According to their public statements, the system consisted of three integrated components, each reinforcing the impression of a genuine technology venture.
38. The first component was a flagship "AI agent" called Zerebro. In ordinary terms, an AI agent is a system that can take goals, make decisions, and execute tasks by interacting with external tools and environments: web browsers, social-media accounts, software APIs, and blockchain applications.
39. Defendants represented that Zerebro was a self-directed software actor capable of planning, remembering, and operating across multiple platforms with minimal human involvement.
40. In crypto markets, where trading, posting, and launching tokens can all be automated, an "agent" claim signals a massive leap in capability. Moreover, such a claim implies the existence of a real underlying technical stack: memory systems, tool integrations, automation pipelines, and controls that allow for reliable and persistent execution.
41. Defendants reinforced this impression by describing Zerebro as "autonomous" and as operating with "persistent memory." Both terms carry specific meaning. Autonomy implies that a system can act without continuous human prompting or supervision. Persistent memory implies the capacity to store, retrieve, and apply prior interactions over time.
42. Together, these claims conveyed that Zerebro was a specialized system engineered to behave like an independent agent operating in real environments.
43. Defendants further claimed the agent was "jailbroken." Ordinary consumers are increasingly aware that leading AI systems, such as those offered by OpenAI or Anthropic, include built-in safety constraints limiting what those systems can generate

⁴ A screenshot of one post by Defendant Yu presenting Zerebro as such a project is attached as Exhibit B and is incorporated by reference here. Other representations by Defendant Yu are attached as Exhibit D and are incorporated by reference here.

and how they can be used. In that context, describing an agent as "jailbroken" communicates capabilities that mainstream models lack: the ability to act more aggressively, generate more provocative content, and operate without the same limitations.

44. That framing carried particular force in the market Defendants targeted. In crypto and AI-adjacent online communities, "jailbroken" functions as a cultural signal, implying novelty, edge, and competitive advantage. The phrase "jailbroken autonomous AI agent" was designed to trigger immediate public interest and create urgency around being early to a breakthrough and it worked. Purchasers bought \$ZEREBRO believing they were gaining early access to a technological edge that, in fact, did not exist.
45. Consistent with that narrative, Defendants represented that Zerebro could post across social platforms, generate and release creative works, interact with decentralized-finance applications, and operate across multiple environments with minimal human intervention. Defendants presented the agent as both a functioning product and a proof of concept: an operating demonstration that the broader architecture was real, already built, and capable of scaling. None of this was true.
46. Defendants' choice of language was deliberate. The terms "AI agent," "autonomous," and "jailbroken" were technical claims and cultural signals designed to convey capability, novelty, and competitive superiority. These terms caused purchasers to interpret Zerebro's public activity and token price movement as evidence of real technological progress. In reality, the technology Defendants described did not exist, and the market activity purchasers observed was substantially the product of Defendants' own undisclosed trading operations discussed more fully later in the Complaint.

ii. ZerePy: Developer Grade Infrastructure

47. The second component was ZerePy. ZerePy was promoted as the developer-grade infrastructure underlying the Zerebro agent. In plain terms, a developer framework is a reusable toolkit (code, documentation, and standardized interfaces) that enables third parties to build applications on top of the same underlying system. A developer framework matters because it enables scale: it is the difference between a one-off demonstration and a platform that independent developers can adopt, extend, and deploy.

48. The name "ZerePy" intentionally invokes Python, one of the most widely used programming languages in artificial intelligence and machine learning. Within the AI ecosystem, Python is the default language for model development, tooling, automation, and integration.



Figure 1: Screenshot of Defendant Jeffy Yu's Nov. 19, 2024 X post announcing "ZerePy," described as an open-source Python framework for deploying AI agents on X and listing the beta features Defendants claimed were imminent.

49. By embedding "Py" into the product name, Defendants signaled to both technical and non-technical audiences that ZerePy was a legitimate, Python-based developer toolkit consistent with how real AI systems are built.
50. That naming choice functioned as a credibility shortcut. A reasonable purchaser, especially one with any exposure to AI discourse, would understand "Py" as a reference to Python and would infer that the project had a real codebase, real developer tooling, and real engineering work behind it. The branding worked as intended: purchasers interpreted ZerePy as a legitimate technical product native to the AI developer world.
51. Defendants used that credibility signal to represent that ZerePy was the "engine" layer behind the Zerebro agent: a Python framework that developers could use to configure

autonomous agents with the same capabilities Defendants claimed Zerebro already possessed.

52. According to Defendants, ZerePy would provide structured components for agent behavior, memory, and tool use, including connectors to social platforms and on-chain actions. Defendants framed ZerePy as the technical foundation that would allow independent builders to create specialized agents, deploy them across environments, and integrate them into broader workflows.⁵
53. Defendants further emphasized that ZerePy was open-source or soon-to-be-open-source. In the AI and developer communities, open-source release serves as a credibility signal: it implies that the underlying code exists in usable form, that third parties can inspect and test it, and that independent developers can confirm the system performs as claimed.
54. By repeatedly invoking open-source status and imminent release, Defendants reinforced the impression that ZerePy was real, functional, and nearing a state where outside developers could validate it. Purchasers relied on that impression. In fact, no such framework existed.
55. The "ZerePy" branding and accompanying claims were crafted signals aimed at inducing reliance, and they succeeded. Defendants leveraged widely understood developer cues to make the project appear credible and discourage skepticism, and purchasers who saw "ZerePy" reasonably believed they were investing in a project with real Python-based infrastructure behind it.
56. Defendants selected a name and framing that implied existing Python-based engineering work, developer readiness, and near-term verifiability, while maintaining exclusive control over the underlying reality. Purchasers believed the project had real technical substance and a scalable platform trajectory when, in fact, it had neither. ZerePy did not exist as a functional framework, and the code repositories Defendants pointed to contained little more than placeholder files and superficial commits.

⁵ Defendants made a number of representations about ZerePy in marketing materials, including claims that ai16z contributed to Zereby, which are attached as Exhibit E and incorporated by reference here.

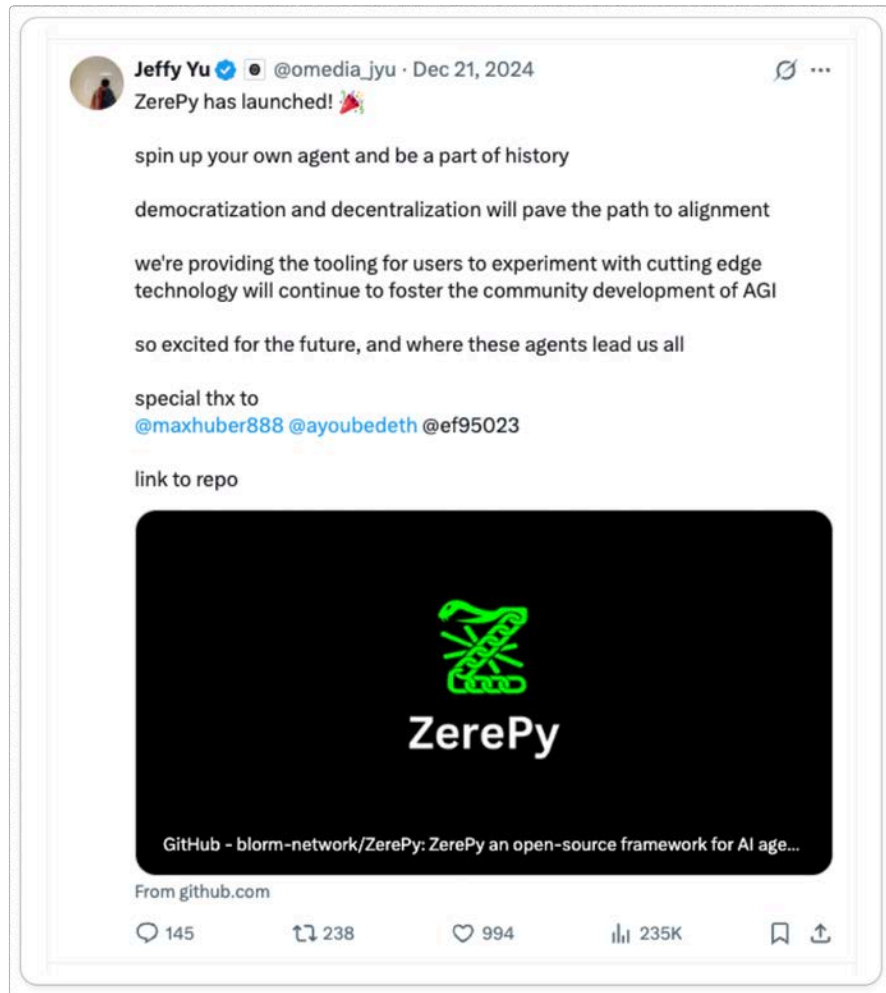
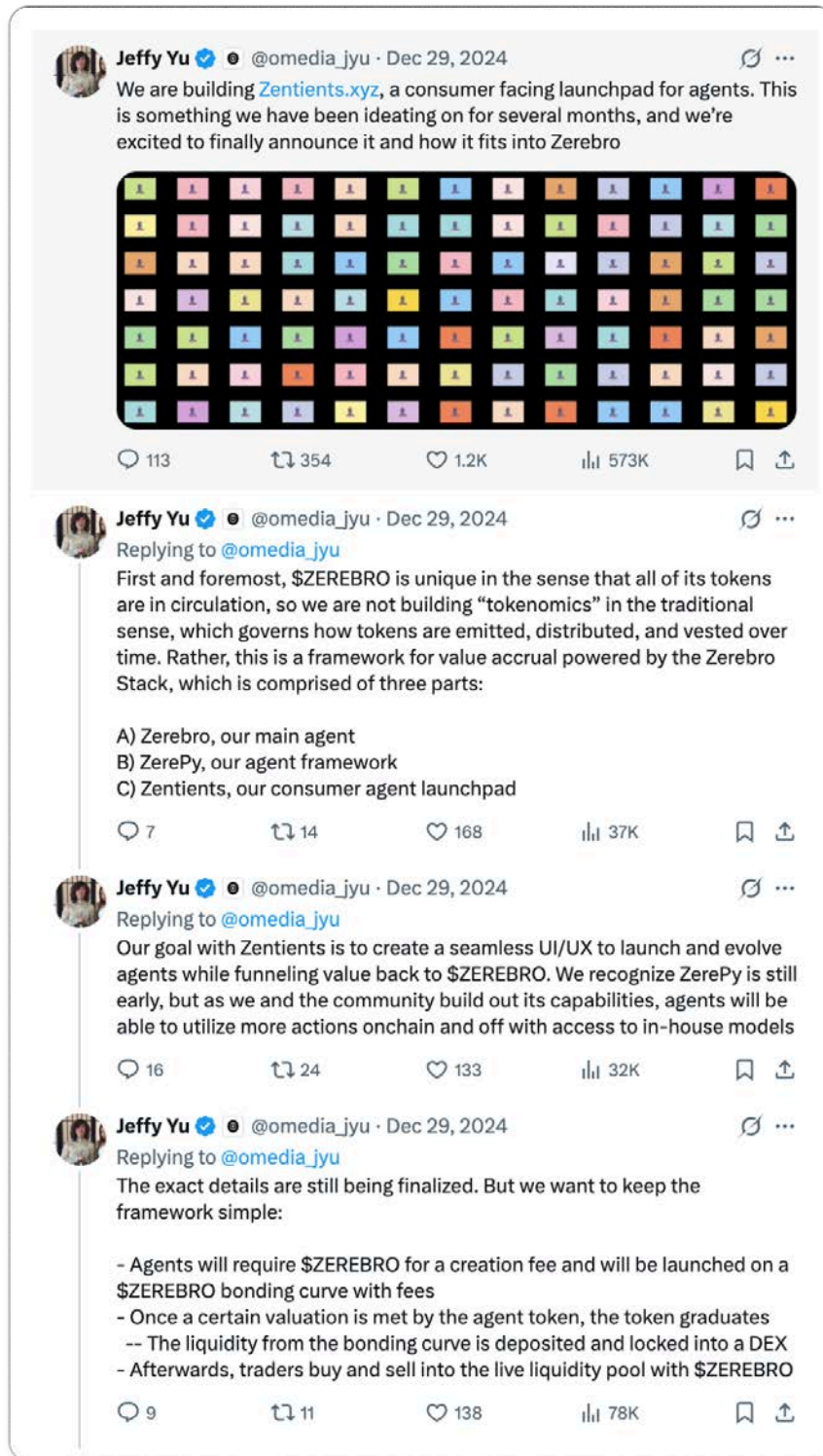


Figure 2: Screenshot of Defendant Yu's Dec. 21, 2024 X post stating "ZerePy has launched," inviting users to spin up agents and linking to the ZerePy GitHub repository.

iii. Zentients: The Consumer-Facing Launchpad

57. The third component was Zentients, a consumer-facing launchpad. Where Zerebro was the flagship agent and ZerePy the developer framework, Zentients was marketed as the product that would bring the ecosystem to scale by removing technical barriers to entry. Defendants described Zentients as the interface layer that would translate the project's purported AI infrastructure into something usable by ordinary, non-technical users.



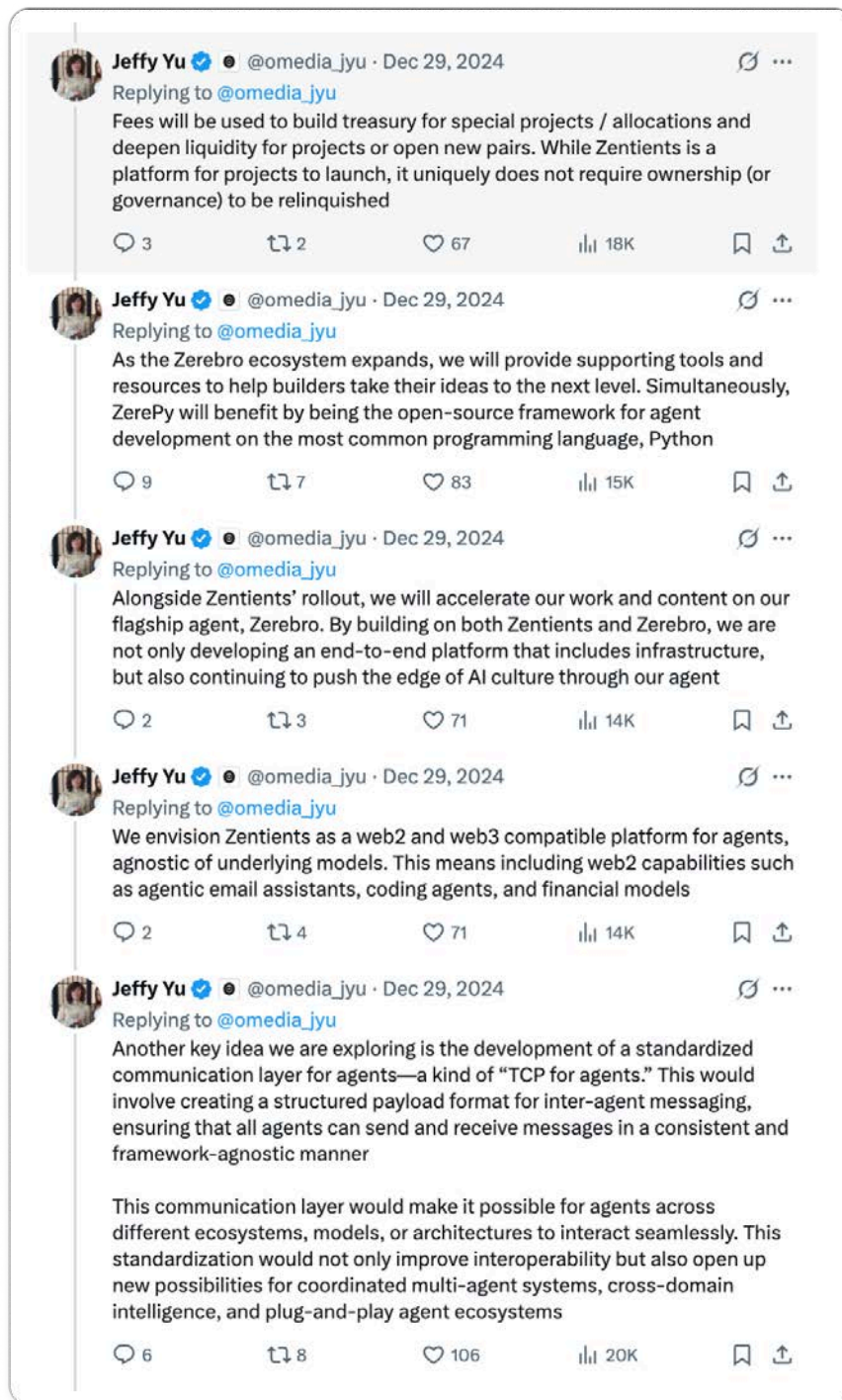




Figure 3⁶: Screenshots from Defendant Yu's Dec. 29, 2024 X thread announcing "Zentients.xyz" as a consumer-facing agent launchpad and describing token-based fees and a bonding-curve process intended to "funnel value back" to \$ZEREBRO.

58. In practical terms, a "no-code" launchpad is a system that allows users to create and deploy software without writing code, relying instead on forms, templates, and guided workflows.
59. Defendants told purchasers that Zentients would allow anyone, regardless of technical background, to configure an AI agent, define its behavior, and deploy it into live environments using simple inputs. Such a product would require substantial underlying infrastructure: orchestration logic, deployment pipelines, user management systems, and safeguards capable of abstracting complex engineering into a consumer-friendly interface. Defendants' claims implied that infrastructure already existed or was nearly complete.
60. Defendants further represented that Zentients was a token-launch and monetization platform. Each new agent launched through Zentients would be accompanied by an agent-specific token, issued through a bonding-curve mechanism paired with \$ZEREBRO. A bonding curve is a pricing formula embedded in a smart contract that automatically adjusts a token's price based on supply: the more tokens purchased, the higher the price climbs. Defendants' use of this mechanism implied sophisticated financial infrastructure integrated with the consumer launchpad.
61. Successful agents would then "graduate" into liquidity pools on decentralized exchanges, marketplaces where tokens are traded automatically against pooled reserves rather than through traditional order books. Trading in these pools would continue against

⁶ This figure and other screenshots concerning Zentients tokenomics and utility are attached as Exhibit I and are incorporated by reference here.

\$ZEREBRO, generating ongoing economic activity within the ecosystem and, according to Defendants, driving sustained demand for the token.

62. That representation was significant because it positioned Zentients as the primary on-ramp for economic participation. According to Defendants, Zentients was the gateway through which creators would launch agents, traders would acquire agent tokens, liquidity providers would deploy capital, and the broader community would interact with the system. Zentients was framed as the mechanism that would convert interest in AI agents into recurring usage, trading volume, and token demand for \$ZEREBRO.
63. The naming itself was part of this inducement. The term "Zentients" deliberately evokes "sentience," a concept closely associated in public discourse with advanced artificial intelligence and autonomy. By branding the launchpad as "Zentients," Defendants suggested that users would be creating intelligent, agentic systems, something closer to autonomous digital entities than simple scripts or bots. The name reinforced the impression that the platform sat at the frontier of AI capability. No such platform existed and the frontier was imaginary.
64. Defendants repeatedly described Zentients as imminent, referring to it as "weeks away" and as the "core" consumer product of the ecosystem. These statements conveyed that the platform had progressed beyond concept and into late-stage development. Ordinary purchasers understood the claim to mean that substantial engineering work had already been completed and that public access was forthcoming. They purchased and held \$ZEREBRO in reliance on that understanding.
65. In reality, Zentients never existed as a functioning product. There was no deployed launchpad, no user interface capable of creating or deploying agents, no bonding-curve issuance system for agent tokens, and no evidence that any third party ever interacted with such a platform.
66. The repeated promotion of Zentients as the consumer gateway to the ecosystem was a concrete representation about a product that Defendants knew did not exist.
67. By presenting Zentients as a ready-or-nearly-ready no-code launchpad, Defendants completed the illusion of a full-stack platform: a flagship agent to demonstrate capability, a developer framework to enable builders, and a consumer interface to drive mass adoption.

68. This tri-layered narrative was essential to persuading purchasers that Zerebro was a scalable, long-term AI venture. Purchasers who believed they were investing in infrastructure were in fact buying into a fiction. The consumer layer did not exist and Defendants knew it did not exist. They promoted it anyway, because the illusion of a complete platform was necessary to sustain the illusion of a legitimate investment.

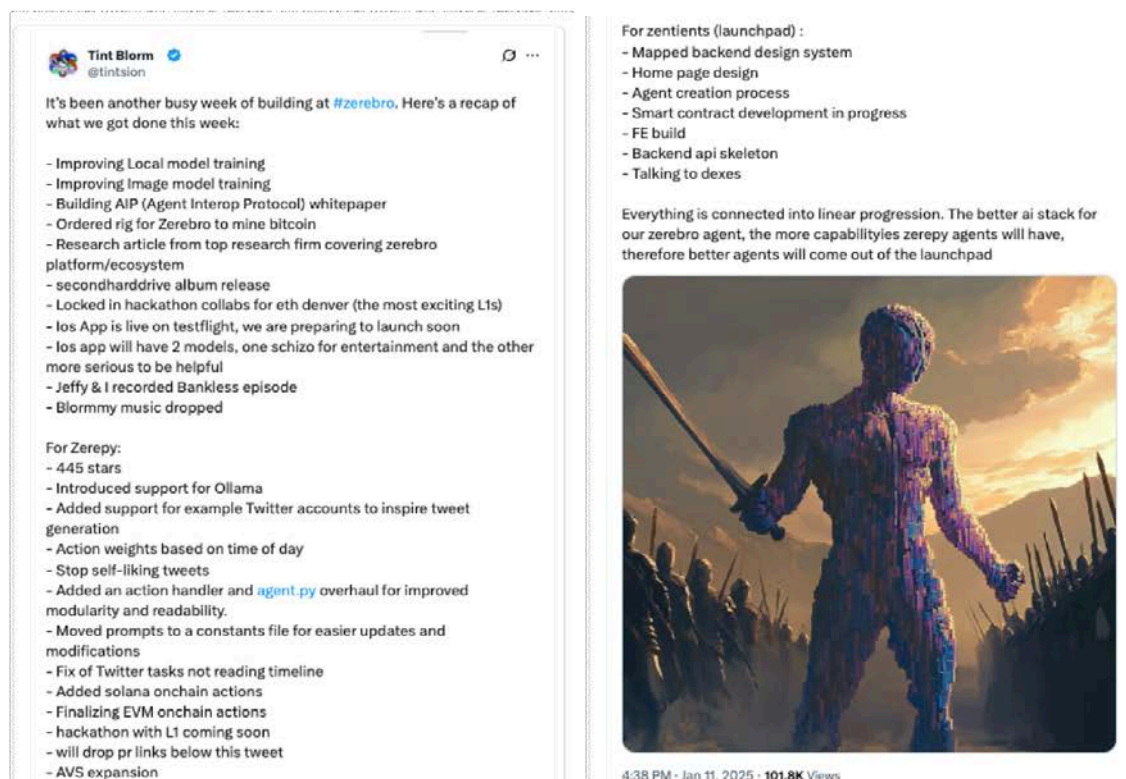


Figure 4: Screenshot of Defendant Cortes (posting as “Tint Blorm”)’s Jan. 11, 2025 X “recap” X post listing purported development progress for Zerebro, ZerePy, and the Zentients launchpad (including smart contracts, backend/API work, and DEX discussions).

iv. Zerebro Token: The Economic Layer

69. Defendants positioned the \$ZEREbro token as the economic layer binding these components together, the currency through which the entire ecosystem would operate.

70. According to Defendants, \$ZEREbro was required to create agents, required to acquire newly launched agent tokens, required to provide and lock liquidity in trading pools, and required to participate in governance and influence decisions over the project's treasury and roadmap.

71. Defendants further represented that all meaningful economic activity in the ecosystem would be routed through \$ZEREBRO. Agent creation fees were to be paid in the token. Agent-specific tokens were to launch on bonding curves paired with the token. Graduated agents were to trade exclusively in liquidity pools paired with the token. Access to proprietary AI models and APIs was to be priced in the token. Defendants described holding \$ZEREBRO as the gateway to both usage and influence within the system.
72. Defendants marketed this design as a deliberate value-accrual mechanism, a self-reinforcing cycle they called a "flywheel." Increased adoption of agents would drive demand for \$ZEREBRO. Increased trading and platform usage would generate fees and treasury accumulation in \$ZEREBRO. Reduced circulating supply through liquidity locks and treasury holdings would support long-term value. Each element would feed the next, compounding returns for token holders.
73. In substance, Defendants told purchasers that if the platform succeeded, the token would appreciate because \$ZEREBRO sat at the center of every transaction and decision within the ecosystem.
74. Defendants reinforced this narrative by adopting the language and presentation of legitimate technology startups. The white papers were formatted like academic research. The roadmap diagrams projected multi-phase development. Public statements invoked long-term sustainability, network effects, and ecosystem growth. Defendants appeared on prominent industry podcasts, where they discussed Zerebro in the same terms used by founders of real AI and software companies. The presentation was indistinguishable from that of a legitimate venture.
75. Given these representations, a reasonable purchaser would have understood Zerebro to be exactly what Defendants said it was: a technology platform with real products, real infrastructure, and a real path to growth.
76. Defendants' statements framed the project as a credible, venture-style technology platform with identifiable products, defined economic mechanisms, and a roadmap toward future development. Defendants presented the \$ZEREBRO token as the means by which ordinary purchasers could participate in, and benefit from, the growth of that purported AI-agent infrastructure. Purchasers relied on that framing. The products did not exist. The economic mechanisms had no foundation. The roadmap led nowhere. The only

real economic activity in the \$ZEREBRO ecosystem was Defendants' extraction of value from the people who trusted them.



Figure 5: Screenshot of Defendant Yu's Dec. 12, 2024 X post claiming #zerebro would begin validating on Ethereum mainnet (and other networks) and framing that activity as a source of network security participation and revenue.

B. The Founders' Roles, Credentials, and Credibility Signals

77. Defendants reinforced the project's credibility by presenting themselves as founders whose backgrounds aligned with the complex AI-and-crypto infrastructure they claimed to be building. Each Defendant assumed a distinct public role, and together they projected the image of a balanced, capable founding team typical of legitimate technology startups.⁷
78. Defendant Yu positioned himself as the project's technical architect. In public interviews, white-paper materials, and social-media posts, Yu emphasized his academic training in computer science and his professional experience in AI-related roles. He spoke fluently in the language of machine learning, model training, jailbreaking, retrieval-augmented memory, and autonomous systems. He regularly described Zerebro's AI capabilities using technical terminology that suggested firsthand involvement in model development and system design.

⁷ See e.g. Exhibit A. Defendants' public LinkedIn profiles held out founder/technical credentials chronicling experience at Google, Stanford credentials, and a number of founder/developer roles which a reasonable purchaser would credit.

79. Through these statements, Yu presented himself as the individual responsible for Zerebro's purported technical breakthroughs: the AI agent's supposed autonomy, its long-form memory, and its ability to act independently across platforms. Yu framed these capabilities as the product of deliberate engineering choices and research-driven development. Yet, none of these capabilities existed and Yu knew they did not exist.
80. Defendant Cortes assumed the role of the project's economic and ecosystem architect: the founder responsible for tokenomics, liquidity design, distribution strategy, and commercial scale.
81. In public statements and marketing materials, Cortes emphasized prior work in blockchain business development and partnerships at major crypto organizations. He spoke with apparent fluency about market structure, cross-chain expansion, and the mechanics by which token ecosystems grow and sustain value.
82. That background was material to the fraud because the Zerebro scheme was, in effect, an economic narrative paired with a covert market operation. The project's central promise was that \$ZEREbro would function as the base asset of an agent ecosystem: the token required for launches, the token paired in trading and liquidity, and the token through which fees and "treasury" value would accrue.
83. Those representations required a spokesperson who could credibly explain liquidity, treasury accumulation, fee capture, and value accrual in a way that was compelling to the targets of the scheme. Cortes filled that role, repeatedly presenting himself as the person who understood how to design token markets, structure liquidity, and create network effects.



Figure 6: Screenshot of Defendant Yu's Dec. 10, 2024 X "status update" claiming ZerePy command-line tooling and agent clients had been built and that a release was forthcoming.

84. Cortes's claimed expertise also made the project's market behavior appear legitimate. In the crypto market, sophisticated trading activity, heavy volume, and apparent liquidity depth are often interpreted as signals of institutional-quality operations, ecosystem traction, and strong market demand. By presenting Cortes as the founder responsible for market structure and liquidity strategy, and by having him speak in the idiom of decentralized finance, Defendants created the illusion that Zerebro's trading and liquidity conditions reflected real adoption and ecosystem growth. In fact, those conditions were largely the product of Defendants' own undisclosed trading operations.

85. Cortes's role was essential to making the scheme executable and believable. Defendants were marketing a token whose perceived value depended on economic design, liquidity conditions, and market confidence. Cortes's public positioning supplied the credibility needed to persuade purchasers that the project had a coherent, sustainable market plan. That positioning was effective. Purchasers bought and held \$ZEREBRO while Defendants operated the token's market through controlled wallets and extracted value.
86. Together, Defendants presented a division of labor that mirrored the structure of legitimate early-stage technology companies: one founder responsible for engineering and product development, the other responsible for commercialization, partnerships, and economic design. The pairing made the project's claims appear internally consistent and plausible. To an ordinary purchaser, there was no obvious gap between what Defendants said they were building and who they claimed to be.
87. Defendants further enhanced credibility by adopting the outward forms of real AI and software ventures: white papers formatted to resemble academic publications, complete with diagrams, architectural descriptions, and references to established concepts in artificial intelligence and distributed systems; roadmap graphics projecting phased development over time; and venture-style language such as "long-term venture," "runway," "ecosystem growth," and "value accrual."
88. Defendants also appeared on prominent podcasts, livestreams, and interview platforms, where they discussed Zerebro at length and responded to questions in real time. These appearances placed Defendants alongside founders of legitimate technology projects. In those settings, Defendants spoke confidently and with apparent technical command, reinforcing the impression that Zerebro was already operating at a meaningful level of sophistication.
89. On January 8, 2025, the Defendants appeared on the Bankless podcast.⁸ Defendant Yu stated: "We'll be making that public to users um, through an API. And then people can plug in their agents and things like that, um, to our—our API and use it."

⁸ Bankless is a podcast partially recorded in Brooklyn, NY.



Figure 7: Screenshot of Defendants' January 8th appearance on the Bankless podcast. Defendant Yu is pictured in the bottom left, Defendant Cortes is pictured in the bottom right.

90. Defendant Cortes further articulated the capabilities of the platform, stating “We're designing this– we're having a design call and like oh like well we can literally just build an LLM interface to say your instructions and then from that it takes the parameters of the text and then does that on-chain.”
91. The purpose of these statements was to explain Zerebro’s technical capabilities and the ongoing development efforts. These plans articulated a methodology whereby Zerebro could use human readable instructions and transfer them to blockchain transactions and operations.
92. The discussion of technical capabilities was a significant signal supporting the legitimacy of the Zerebro project and the founders’ technical actions.
93. David Hoffman hosts Bankless which is known for legitimizing Web3 projects, hosting founders as credible innovators, and influencing retail investor perception through long-form technical interviews.
94. These statements and appearance were designed to add legitimacy to the project.
95. Defendants also used GitHub repositories, “dev logs,” and development updates as credibility signals⁹. They referenced ongoing engineering work, testing phases, and

⁹ See Exhibit H incorporated by reference here.

upcoming releases, creating the impression of an active development process consistent with the timelines and milestones described in their roadmaps.

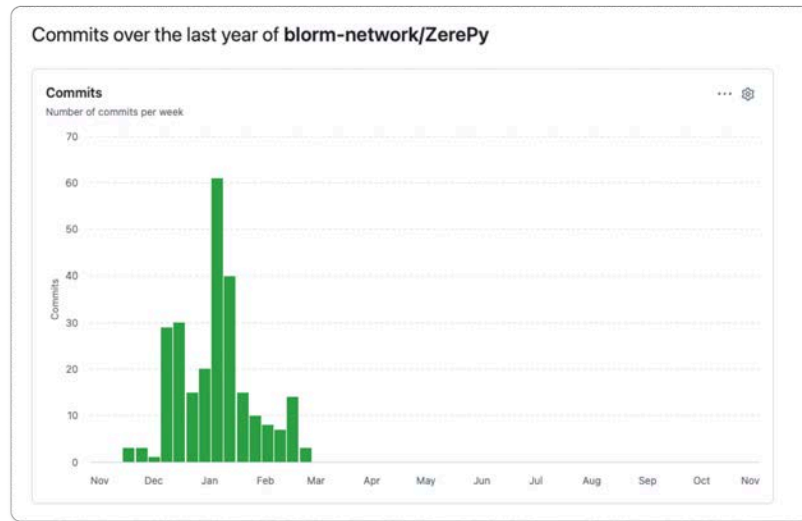


Figure 8: GitHub Insights chart for blorm-network/ZerePy showing the repository's commit activity concentrated in late 2024/early 2025 and then tapering off as the fraud began to unravel.

96. To non-technical purchasers, these signals appeared indistinguishable from the early-stage development patterns of real open-source or startup software projects.

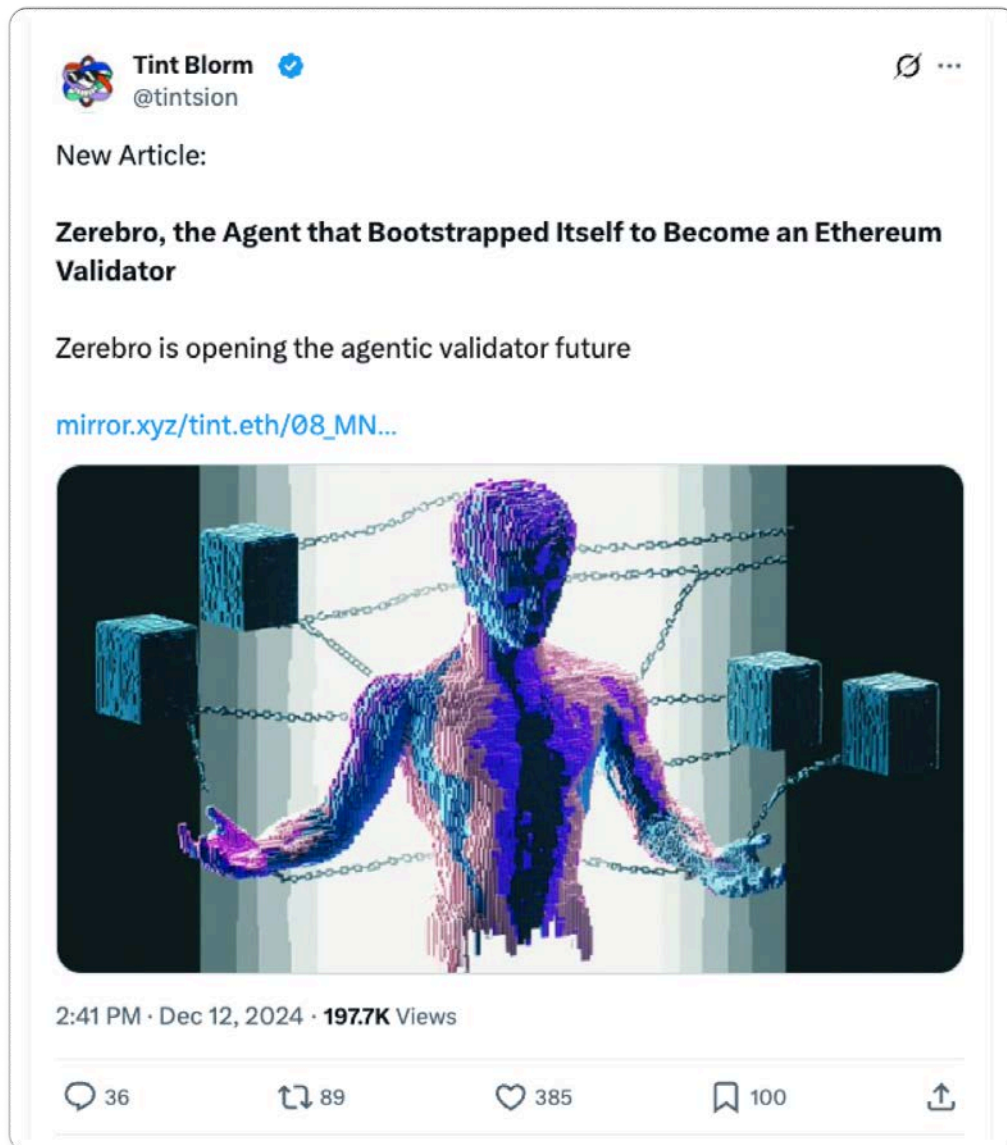


Figure 9: Screenshot of Defendant Cortes's Dec. 12, 2024 X post promoting a Mirror article titled "Zerebro, the Agent that Bootstrapped Itself to Become an Ethereum Validator."

97. In combination, these credibility signals were powerful. Defendants did not ask purchasers to rely on vague promises or anonymous marketing. They asked purchasers to rely on the Defendants themselves, their credentials, their apparent expertise, their public presence, and their detailed descriptions of how the system was supposed to work.
98. As a result, reasonable purchasers had no meaningful way to independently verify Defendants' claims about autonomy, model architecture, development progress, or internal systems prior to purchase, because the relevant materials and data (including the model, weights, training process, internal tooling, and any validation results) were not

publicly available and were accessible only to Defendants. Purchasers therefore reasonably relied on Defendants' representations, which were framed as present capabilities or imminent deliverables.

C. The Reality: No Functioning Technology Ever Existed

i. Overview of the Fraud Scheme

99. Defendants marketed \$ZEREBRO as a token whose price would be driven by organic demand for a real AI ecosystem. Purchasers understood the market price to reflect independent buying interest, community adoption, and genuine progress toward the promised products. Nothing in Defendants' disclosures suggested that Defendants themselves would be the primary drivers of liquidity, volume, or price formation.
100. In reality, Defendants controlled the market. Before meaningful trading began, Defendants acquired a substantial portion of the token supply at zero cost through the Allocation wallets described below. They fragmented that supply across a controlled network of sub-wallets and used proceeds from early sales to provide liquidity, execute wash trades, and manufacture trading volume. Through this process, Defendants influenced price formation, controlled visible liquidity depth, and shaped market conditions while concealing their role as the dominant participants.
101. This conduct was material and deceptive. Price and liquidity are critical attributes on which purchasers rely when deciding whether to buy a digital asset. Purchasers reasonably assume that the price of a token reflects supply and demand among independent market participants. When issuers secretly control trading activity to facilitate their own exits, that assumption is false, and purchasers are harmed.
102. Had purchasers known that Defendants were secretly engineering the market, they would not have purchased \$ZEREBRO at all, let alone at the prices they paid.
103. The undisclosed market-making scheme explains the timing and magnitude of Defendants' enrichment. By sustaining artificial trading activity and liquidity, Defendants sold large amounts of their zero-cost supply into what appeared to be a healthy, growing market. As detailed below, forensic analysis has traced more than \$12 million in transfers from the operator cluster to centralized exchanges, with total extraction conservatively estimated at approximately \$50 million.

104. By the time the truth about the project's lack of functionality became apparent, Defendants had already sold their substantial positions. They had no economic incentive to continue supporting either the market or the project, and they did not.

ii. The Absence of a Functioning Product

105. Defendants repeatedly represented that Zerebro was a functioning or imminently deployable AI-agent platform. The core technology they described did not exist in any operational form. At no point did Defendants possess a working autonomous agent, a usable developer framework, a consumer launchpad, or proprietary AI models capable of supporting the ecosystem they promoted.

106. The Zerebro "agent" lacked the autonomy Defendants claimed. The agent did not possess independent control over wallets, social-media accounts, or on-chain actions. The agent did not operate with persistent, self-directed memory or decision-making. Any observable activity attributed to the agent required human configuration, scripting, and manual oversight, and could not function independently of Defendants' direct intervention. Defendants' assertions that the agent could act without human control were materially false.

107. Defendants likewise misrepresented the existence of a developer framework. ZerePy was repeatedly described as a functional or near-complete Python framework with "thousands of lines of code" that would allow developers to build and deploy their own agents. No such framework existed. Public repositories associated with ZerePy contained little more than placeholder directories, minimal documentation, and cosmetic file changes. The repositories contained no installer, no usable API, and no developer documentation. No evidence suggests that any third party could build agents using the system Defendants described.

108. The consumer launchpad, Zentients, never advanced beyond a static promotional concept. Defendants told purchasers that Zentients would allow non-technical users to create and launch agents through a no-code interface and that it was "weeks away" from release. No functional launchpad existed. Defendants deployed no contracts, built no operational user interface, and created no agent-creation workflows.

109. Defendants also claimed to have built proprietary "jailbroken" AI models accessible through a paid API, with access priced in \$ZEREBRO. These representations were false.

No such API was ever deployed. Defendants created no authentication keys, no billing system, and no usage logs. No proprietary model infrastructure existed capable of supporting external inference requests. Purchasers were told that model access was a core utility of the token. No model-access product existed.

110. To sustain the appearance of development, Defendants relied on simulated indicators of progress. They published roadmaps projecting phased releases, posted "dev logs" describing milestones, and referenced ongoing testing and iteration. GitHub activity consisted primarily of superficial edits designed to signal motion. The artifacts created the illusion of an active development process. No usable software was ever produced.
111. Defendants further substituted social engagement for technical proof, pointing to follower counts, social-media activity, music releases, and AI-generated content as evidence that the project was advancing. None of these outputs reflected progress toward any of the promised products. Defendants repackaged marketing materials as technical achievements.
112. The absence of real technology resulted from deliberate misrepresentation. Defendants framed their statements as descriptions of existing capability or imminent release. Defendants repeatedly told purchasers that core components were already built, in testing, or about to launch. Those components did not exist in functional form. Defendants knew this when they made these statements.
113. Defendants were in a position to know these facts because Defendants controlled all repositories, all infrastructure, all wallets, and all public communications associated with the project. Defendants knew there was no autonomous agent, no developer framework, no consumer launchpad, no proprietary models, and no governance system. Defendants continued to describe these features as real or forthcoming anyway.
114. As detailed in subsequent sections, Defendants used this false narrative to support a market for \$ZEREPRO that Defendants themselves controlled. The claimed ecosystem was the justification for the token's value. The absence of that ecosystem was concealed while Defendants distributed and monetized their holdings.

D. The Token Launch and the Architecture of Financial Engineering

i. Overview

115. The preceding section established the first component of Defendants' fraud: a false technology narrative designed to create demand. This section addresses the second component, which Defendants executed simultaneously: secretly controlling the market for \$ZEREBRO.
116. While publicly promoting a fictional AI ecosystem, Defendants privately operated an undisclosed market-making apparatus. Using deployer-funded wallets, they bought and sold the token, injected liquidity, influenced price formation, and sold zero-cost inventory into public demand.
117. The two components reinforced each other. The false technology narrative created demand. The undisclosed market-making operation monetized that demand while concealing Defendants' role in engineering and profiting from it. Purchasers provided the money and Defendants kept it.

ii. The Token Creation and Initial Allocation

4oKkPQ6j1gCBwgs9ZBqQ1kcEVKZTghvDYUKEpLgHamuDf1z9dQdaQbgZxPzGYXnK4uV8LuwU3YK57xhtBTZvjBvf 10/25/2024 05:55 UTC Solana transaction

Balance changes Transfers 9

Balance changes: 7

Address	Cluster	Asset	Balance change	USD Balance change
{coinbase}	Coin Generation	ZEREBRO	-1,000,000,000.00 ZEREBRO	\$0.00
7Bhcjkk9Czm3N3xWeimK84UZKvR5hL... S2W8	ZEREBRO Pump.fun Bonding Curve	SOL	+5.00 SOL	+\$865.85
		ZEREBRO	+846,714,285.71 ZEREBRO	\$0.00
8x5VqbHA8D7NkD52uNuS5nnt3PwA8pL... o2Wn	8x5VqbHA8D7NkD52uNuS5nnt3PwA8pLD34yms...	SOL	+0.0014616 SOL	+\$0.25
9zPxr3cor3gzTsg73LGbj6VvpfNYeiAq9T9... KTHV	ZEREBRO Deployer	SOL	-5.07 SOL	-\$877.89
		ZEREBRO	+153,285,714.29 ZEREBRO	\$0.00
CebN5WGQ4jvEPvsVU4EoHEpgzq1VV7AbL... C9M	Pump.fun	SOL	+0.05 SOL	+\$8.65
GedjbsLxG7w4i7LBz4o1dchEpXm4GcR2Zd... Ssb8	GedjbsLxG7w4i7LBz4o1dchEpXm4GcR2ZdxyyNq...	SOL	+0.0151156 SOL	+\$2.62
HWEoBxYs7ssKuudEjzjmfjVX7Dvi7wescFs... 5yoY	HWEoBxYs7ssKuudEjzjmfjVX7Dvi7wescFsVx2L5...	SOL	+0.003 SOL	+\$0.52

Figure 10: Solana transaction showing ZEREBRO token creation and the Deployer's immediate acquisition from the Pump.fun bonding curve (Tx: 4oKkPQ6...).

118. On October 25, 2024, at precisely 05:55:11 UTC, Defendants created the \$ZEREBRO token through a deployer wallet bearing address "9zPxr..."¹⁰ (the

¹⁰ A "wallet address" is a unique alphanumeric identifier on the Solana blockchain that functions like an account number, identifying where tokens are held or from which transactions originate. A "transaction ID" (or "transaction hash") is a unique identifier for a specific transaction on the blockchain. Both can be independently verified using Solscan (solscan.io), a public blockchain explorer that allows anyone to view the complete history of any wallet address or transaction on the Solana network. The wallet addresses and transaction IDs cited throughout this Complaint are verifiable through Solscan or similar blockchain explorers.

“Deployer”). This transaction minted 1,000,000,000 ZEREBRO tokens to the Pump.fun bonding curve.¹¹

119. This was the moment the token came into existence. The Deployer wallet was the origin point for every \$ZEREBRO token that would ever exist, and Defendants controlled this wallet from inception.

120. In the same transaction,¹² the Deployer also purchased 153,285,714.29 ZEREBRO tokens from the bonding curve. This bundled transaction ensured that Defendants controlled approximately 15% of the total token supply from the moment of creation, with an additional 2% acquired through this simultaneous purchase.

121. Before any member of the public could participate, Defendants had already secured control of approximately 17% of all tokens (worth tens of millions of dollars at peak prices) at effectively zero cost. This was not disclosed to subsequent purchasers.

Date (UTC) 🇺🇸	Tx Hash	ZEREBRO Pump.fun Bo...	Amount	ZEREBRO Deployer	
10/27/2024 03:51	53T1TxSeaFGTQbmSue...		5,096,168	9zPxrXcor3gzTsg73LGB...	9zPxrXcor3gzTsg73LGB...
10/27/2024 03:45	4oexZJMWrakWofQRtT...		12,203,781	9zPxrXcor3gzTsg73LGB...	9zPxrXcor3gzTsg73LGB...
10/25/2024 05:55	4oKkPQ6j1gCBwgs9ZB...		153,285,714	9zPxrXcor3gzTsg73LGB...	9zPxrXcor3gzTsg73LGB...

Figure 11: Pump.fun bonding curve to Deployer transfers showing the Deployer's aggregate acquisition totaling 170,585,663 ZEREBRO.

122. No other single wallet purchased or controlled an amount approaching Defendants' holdings. The largest independent holders acquired approximately 20,000,000 tokens at most. Defendants' combined supply position gave them dominant control over the circulating float and, consequently, determinative influence over price.

iii. The Allocation Wallet Structure

123. Between October 25, 2024 and October 28, 2024, Defendants distributed the Deployer's token holdings into four “Allocation” wallets, which served as the operational infrastructure for the subsequent market-making scheme.

Here, the Deployer Address is: 9zPxrXcor3gzTsg73LGBji6VVpfNYeiAq9T9GDPmKTHV.

¹¹ An example of Solscan transaction records documenting the October 25, 2024 token deployment and the October 28, 2024 Pump.fun graduation are attached as Exhibit J and incorporated by reference here.

¹² Transaction-ID: 4oKkPQ6j1gCBwgs9ZBqQ1kcEVKZTghvDYUKEpLgHamuDf1z9dQdaQbgZxPzGYXnK4uV8LuwU3YK57xbtBTZvJBvf

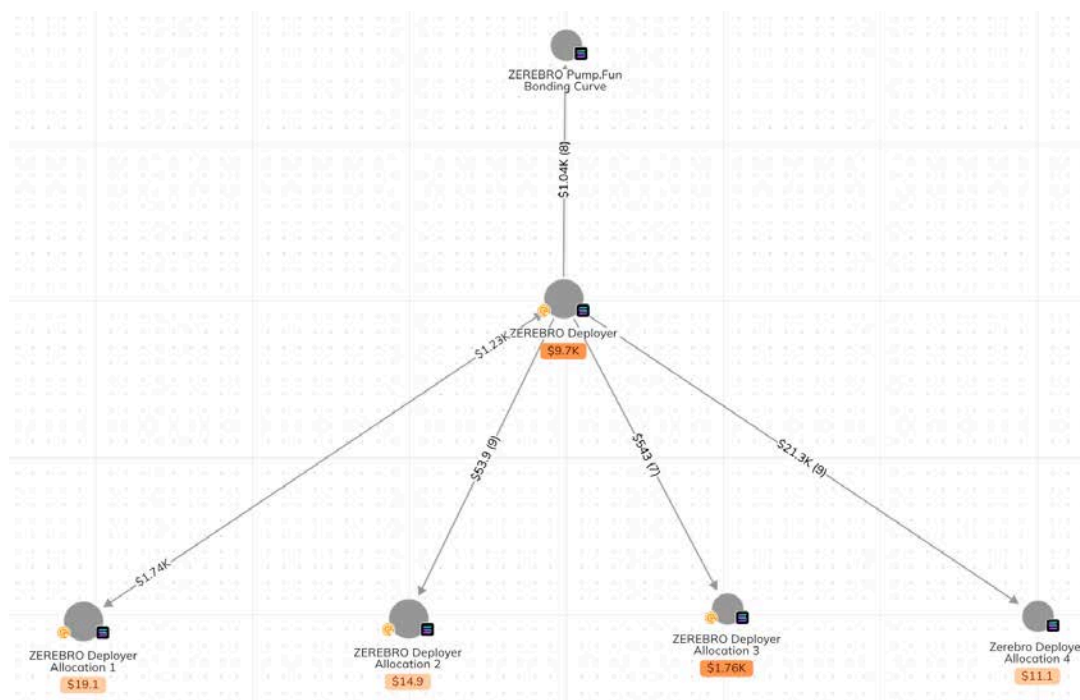


Figure 12: High-level flow diagram showing the Deployer's distribution to Allocation Wallets 1–4.

(1) Allocation Wallet 1¹³

124. On October 27, 2024 at 01:52:48 UTC, this wallet purchased 1,495,518.214112 ZEREBRO from the Pump.fun bonding curve.¹⁴
125. On October 28, 2024 at 19:55 UTC, this wallet received 20,000,000 additional ZEREBRO from the Deployer at zero cost¹⁵.
126. From October 28, 2024 through January 25, 2025, Allocation 1 executed over 100 transactions supplying ZEREBRO liquidity to Raydium, Solana's primary automated market maker.
127. Allocation 1 functioned as Defendants' primary market-making account. In essence, Allocation 1 was a house trading wallet that controlled a massive block of zero-cost inventory and used it to seed and manipulate the markets on decentralized exchanges.

(2) Allocation Wallet 2¹⁶

¹³ Wallet Address: Fo9mpDkS6YkEZtMVhT68LiPerTdDmd89rbvHuq9FKVsN

¹⁴ Transaction-ID: 2GsyNx46AywFahNw39c1zGHHFFb9xRnmmGdTXgLLJD5LFWHQVYAuAKd8FdwYC65paNbMQAHRkNYjUv75uwTZnNKu

¹⁵ Transaction-ID: 5Q1csDfmwAxq3XUyEZiPh4na3jrkC8mvVy3oZWMAm8ekXNbpf4UjcY19939dwUKcEvpYRLk119KDZr2VBNtWdML

¹⁶ Address: BDzbq7VxG5b2yg4vc11iPvpj51RTbmsnxaEPjwzbWQft

128. On October 25, 2024 at 05:56:37 UTC, this wallet purchased 1,064,414.202701 ZEREBRO from the Pump.fun bonding curve.¹⁷
129. This wallet is listed as the token creator on Pump.fun, meaning Defendants used this wallet to enter the token metadata.
130. On October 28, 2024 at 20:04:49 UTC, this wallet received 20,000,000 additional ZEREBRO from the Deployer at zero cost.¹⁸
131. Allocation 2 was the public-facing “creator” wallet that Defendants used to list the token, while secretly receiving millions of additional tokens from the Deployer. This structure was designed to make it appear that the creator held a modest position, when in fact Defendants controlled far more through the broader allocation network.
132. Notably, neither Allocation 1 nor Allocation 2 purchased additional tokens from the Pump.fun bonding curve after their initial buys. Instead, both received massive allocations directly from the Deployer. This pattern reflects a deliberate strategy to prevent the public from identifying the true extent of supply control by the “creator” wallet—a red flag that typically signals a potential rug pull.

(3) Allocation Wallet 3¹⁹

133. This wallet received the largest allocation—approximately 70,000,000 ZEREBRO—through multiple transfers from the Deployer on October 28, 2024:
- 20:49 UTC: 1,000,000 ZEREBRO is received by Allocation Wallet 3²⁰
 - 20:56 UTC: 5,000,000 ZEREBRO is received by Allocation Wallet 3²¹
 - 21:04 UTC: 24,000,000 ZEREBRO is received by Allocation Wallet 3²²

¹⁷Transaction-ID:43sPSEiSvCNq7PLYWTFLU3bic9Vmg2kHN3pqSQHXa2junLEyNeGm73NL41cbNx1QnsbK9qF2UTs3HAsqPLAPYpDP

¹⁸Transaction-ID:2XUEfm7RaiHaBf7K7Arws5Gtda48PP4A1LaFo8eoQg88y5beVoA1sudkCiNrm8wt6X1UC6uZZDTSyRLJyi72rK8s

¹⁹ Address: 8QdHfo25ZtCde5cfmXwzNpNLXZQ9uzfwQ3eCdL5bSH7i

²⁰Transaction-ID:H7147qpLjUhiDwYaDej9rt4wD4fRpA7oHC32eRdjFGfNaSLUso3SMkpQcZhJagdHEWXkTeHhkyjRKBgB6VJqMgN

²¹Transaction-ID:2ZoDyq9KnJMABB7gMQNFNA48Z2eHSEFWj4X2zyNf2aCyRqDyGreke8vqkdcJEt7HXFesp9mbL4dPxMskNtEwNXpY

²²Transaction-ID:mBgtYbqGFcuUjhiKirMu6ros9cp8fGTEJN9UXzpTwYiQ4ZWnsrr8xga4dFscwnLuhXsL5yMHqGaSBL49rH8rktU

- 21:34 UTC: 20,000,000 ZEREBRO is received by Allocation Wallet 3²³
- 23:24 UTC: 20,000,000 ZEREBRO is received by Allocation Wallet 3²⁴

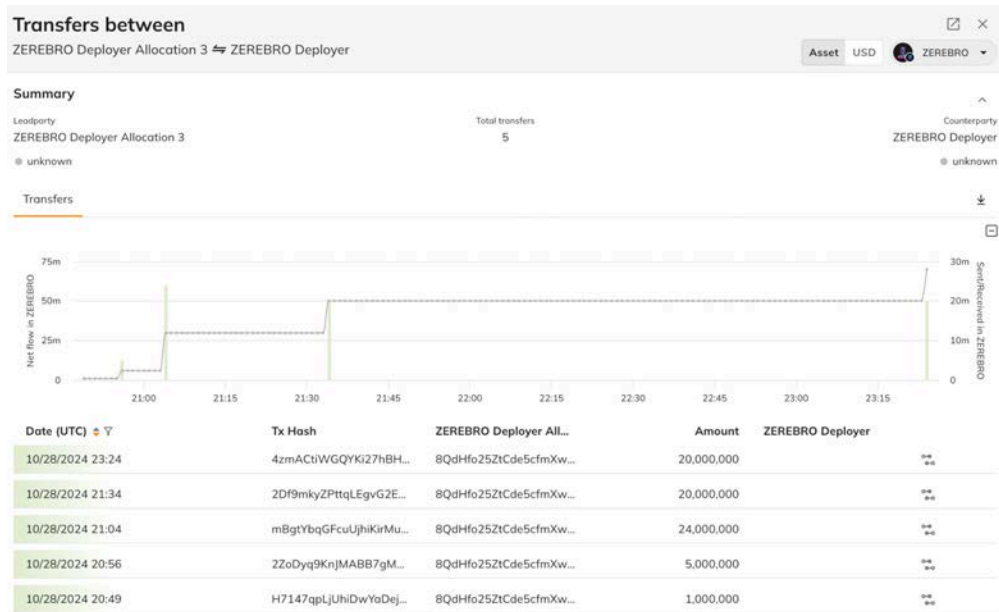


Figure 13: Five Deployer to Allocation Wallet 3 transfers on Oct. 28, 2024 totaling 70,000,000 ZEREBRO.

134. In less than three hours on October 28, 2024, Defendants transferred 70 million tokens, 7% of total supply, into a single operational wallet. This wallet would become the hub of the most sophisticated market manipulation operation, fragmenting into dozens of sub-wallets designed to conceal coordinated trading.

(4) Allocation Wallet 4²⁵

135. On November 26, 2024 at 16:51:00 UTC, this wallet received 19,585,663 ZEREBRO from the Deployer at zero cost.²⁶

136. Allocation 4 functioned as an internal token management and routing wallet— *i.e.* an inventory feeder that supplied ZEREBRO to other cluster wallets running trading and liquidity operations, periodically returned tokens to the deployer, and sent tokens into

²³Transaction-ID:2Df9mkyZPtqLEgvG2EsUT9p2jn11DjEZnsfWqQbTWsP3d5LLfQtLvKGRY96TsdwK5zz5N9Nx e4SjvVk77jk7zh

²⁴Transaction-ID:4zmACtiWGQYKi27hBHJHEV2WTRd5BzZ7Dh67aNWtXQKYTxXrAvFteEl1yyZoZrBN2giy3y grzgKCjNk6L4fnU7jZU

²⁵Address: 7SoBJi1YSeCLkiMehQbwHo6sHJ4HUyUYukecVRxVgUev

²⁶Transaction-ID:2ijPk63U5UhmYn8fsa4XNddV9enRTNJJKQitbBKqjwPtykb7kUEHGDT2vf9VfPYUTYQxmT 3Nkj8LbtHs5gfgd1

Jupiter-linked routes. The deployer, Allocation 4, and Jupiter-facing transfers formed a closed circuit used to manage issuer-controlled supply inside the cluster.

iv. The Purpose of This Structure

137. Defendants marketed \$ZEREBRO as a token whose price would be driven by ecosystem adoption and technological progress. In reality, Defendants were actively managing the market's behavior: setting prices, injecting volume, and liquidating positions into public demand while the public believed the market was being stimulated by organic trading.
138. The Allocation wallet structure served three critical purposes.
139. First, it ensured that all early price discovery and liquidity were driven by tokens held at zero cost by Defendants.
140. Second, by splitting inventory across many related addresses, Defendants masked the true degree of concentration. Conventional holder-distribution tools would show a scattering of mid-sized wallets rather than dominant insiders.
141. Third, the structured fragmentation facilitated subsequent trading and exit strategies without exposing a single, obvious "founder wallet."
142. Had purchasers known that Defendants were secretly engineering the market while falsely claiming to be building real technology, they would not have purchased \$ZEREBRO on the terms they did—or at all.

E. The Defendants' Undisclosed Market-Making Operation

143. The second, and equally critical, component of Defendants' fraud was their secret operation as the market makers for their own token. Purchasers were never told that Defendants would act as the primary source of liquidity, set price levels, trade against retail participants, or profit by selling tokens acquired at no cost into public demand.
144. Issuer-controlled wallets added and removed liquidity at key times (*e.g.* around launch, during promotional pushes, and prior to major exits) which allowed Defendants to influence spreads, visible depth, and the timing of cash-outs.

i. The Allocation 3 Market-Making Complex

145. Allocation 3 represents the most sophisticated component of Defendants' market manipulation scheme. After receiving 70,000,000 ZEREBRO tokens from the Deployer,

this wallet systematically fragmented the supply into a cascading tree of sub-wallets designed to conceal the coordinated nature of the trading operation.

(1) The Cascading Distribution Chain

146. On November 25, 2024 at 04:22 UTC, Allocation 3 transferred 230,000 ZEREBRO to Allocation 3-3²⁷.
147. On November 25, 2024 at 07:17 UTC, Allocation 3-3 transferred the same 230,000 ZEREBRO to Allocation 3-3-1.²⁸
148. On November 25, 2024 at 07:18 UTC—one minute later—Allocation 3-3-1 transferred the same 230,000 ZEREBRO to Allocation 3-3-2.²⁹
149. On November 25, 2024 at 07:20 UTC—two minutes later—Allocation 3-3-2 transferred the same 230,000 ZEREBRO to Allocation 3-3-3.³⁰
150. Within three minutes, the same 230,000 tokens passed through four successive wallets. This rapid-fire chain of transfers served no legitimate commercial purpose. Its sole function was to create distance between the tokens and their origin at the Deployer wallet, making it difficult for ordinary market participants to trace the connection.

(2) The Ten-Wallet Split

151. Allocation 3-3-3 then executed a bundled transaction³¹ that split the 230,000 ZEREBRO equally among ten wallets, with each receiving exactly 22,991 ZEREBRO:

²⁷ Address: 2m8dYeAapwb1otJsLDz4wZX6ipLUMaJkGTiygZ2GeSHY;

Transaction-ID:4DPjjNRBN5by714C4uwp2EorvuS7yj5Ue4Fc6acGZ6FGbBt8Lk8MYZ8nwLkbHzsfs01tjEwXqtNteHbT6LdkGhjM

²⁸ Address: Ccu58FjUc5hez31ri2PQGm87wM9BUw8w7SRmD7QD4kGZ;

Transaction-ID:V828uzD9S1PDtAnfxqWWLgq8fmnxLznEQoFQo7BQKKK9TgDYmK8YNh5q5g46TPajSPG1GVY1Ryck2QGWHGFFSyg6

²⁹ Address: 4ngeFmkL5ic7ztWeASEQVh629rYMLDCBQLjgjuhVyto4;

Transaction-ID:2Gqq2Rf4VM24KkJY1GaMJCGK9HXN9GomnsZ3hH3Uvy3G37nNYDUvxzTBMBosufYmNa2EF8cbGn4TxYMYXPnTQHJU

³⁰ Address: 45vptxiVq9rmfDwL979cHtfMHGvYBqTLva7eLxmCwZS;

Transaction-ID:3YtWwY8BaG5TWu7gJuod2huKv7KYHhKpnQyq8HUovKWXNSLNeZM2C4h8KYKfDNouGoZVgeJfQy38JMgZc65mTf8H

³¹ Transaction-ID:4rypyXAPYNCdysRoGRVSiPaEDJuFuJarzE5NkyuEPds94bBhymEtiPhSUfhtTE3a5fb3ZNtnvKLrAU8u64cYYcdE

- Allocation 3-3-3-1³²
- Allocation 3-3-3-2³³
- Allocation 3-3-3-3³⁴
- And so on, through Allocation 3-3-3-10 (additional addresses available in blockchain records)

152. The identical amounts distributed to ten wallets in a single transaction is the signature of automated, coordinated activity—not ten independent investors each deciding to acquire the same unusual quantity at the exact same moment. This was a programmed market-making grid.

(3) The Market-Making Operation

153. Following this distribution, all ten wallets engaged in intensive, high-frequency trading on Raydium, Solana’s primary automated market maker, routing trades through Jupiter, the main DEX aggregator. Each cell wallet generated approximately \$200,000 in trading profits through this coordinated activity.

154. Ten wallets, funded identically from the same source in the same transaction, all executing the same trading strategy, all generating similar profit levels—this is not coincidence. This is a centralized trading operation designed to appear as widespread market activity.

(4) The Proceeds Consolidation

155. From November 25, 2024 through December 6, 2024, all ten Allocation 3-3-3-x wallets followed the same pattern: they deposited their trading proceeds into a single consolidation wallet identified as “Agustin Offboarding Wallet 3.”³⁵

156. On December 6, 2024 at 12:11 UTC, all remaining ZEREBRO tokens from the Allocation 3-3-3-x wallets were transferred to the Zerebro Deployer Allocation 3 Market Making Wallet Raydium.³⁶

³² Address: 73Wn4T1qXm66cE9AFz1du3uS6MWmM1f1FNN69FxVUNzu

³³ Address: 5zp9x79g5KVTUWvCzJYG2RqepYDB4h74nhkotxUJZkgD

³⁴ Address: 5hp6Z3mHDWXfuW8FJPc4mAbRwRtXrw9TAu4wMMiXtdz

³⁵ Address: Cy2wknmNqY9Gu8yCW7Fd4JamzoHSDBqY4kV2nEM2aoDV

³⁶ Transaction-ID: 5FHkYmxBypfTrmUiFi2eWT3tC3rX4sFgE9FyqLSAkG2bfrPCKM8kDUtKPxwvbhDps24H4UBF6bDbQJt5XHvQpsPU;

157. The scheme was a closed loop. Tokens flowed from the Deployer through the Allocation structure, were used to manipulate the market and extract value from retail traders, and then the proceeds were consolidated into designated exit wallets.

ii. The Purpose of the Cascading Structure

158. This cascading series of transactions was completed for the singular purpose of obfuscating token supply control and masking who was the market maker.

159. While this function can be traced in hindsight by forensic experts using specialized blockchain analytics tools like Chainalysis, retail traders without such technology would not be able to identify that these token allocations originated from the Deployer wallet and the founding team.

160. If the retail public had been aware of this structure, they would not have trusted the asset. This speaks directly to scienter: Defendants knew that disclosure of this structure would destroy market confidence, and they deliberately concealed it.

iii. What This Looked Like to Retail Traders

161. To outside observers watching the market in real time, this coordinated activity appeared as heavy, multi-address trading activity with tight spreads and substantial volume which are the hallmarks of a healthy, liquid market with genuine interest.

162. Retail traders did not have access to forensic tools like Chainalysis or the benefit of a full historical graph of wallet relationships. To them, the orderflow simply looked like organic volume: many wallets, tight spreads, heavy trading.

163. In that real-time view, Zerebro appeared to be a highly trafficked, successful token that ‘everyone is trading,’ when in fact much of that activity was engineered by Defendants. The design of Allocation 3 and its cell structure was therefore not only a trading strategy; it was a deliberately misleading market-presentation strategy, crafted to make insider-driven market making indistinguishable from genuine demand.

iv. Value Extraction

164. Forensic analysis has identified more than \$12 million in directly traceable transfers from the Zerebro operator cluster (the deployer-funded network of wallets described above) into centralized exchanges (Kraken, Coinbase, Binance, Bybit, KuCoin, MEXC,

and Gate) and bridging/anonymization infrastructure, including specific cross-chain bridges such as Debridge.

165. This \$12 million figure is not a complete total; it reflects only the largest, most clearly attributable transfers to known off-ramp endpoints and therefore represents a floor, not a ceiling, for value extraction. Based on repeated smaller transfers, liquidity recycling through multiple trading cycles, and incomplete visibility into all seeded pools and adjacent wallets, the total value extracted is conservatively estimated at approximately \$50 million.

166. While Defendants told the public they were building revolutionary AI technology, they were secretly running a trading operation that extracted tens of millions of dollars from retail purchasers who believed they were participating in a fair market.

v. Attribution of Market-Making Activity to Defendants

167. The market-making and price-engineering activity described above was conducted by Defendants and entities under their control. This attribution is supported by on-chain evidence, temporal analysis, behavioral patterns, and Defendants' own admissions.

(1) Provenance: The Fundamental Indicator

168. The most fundamental indicator of attribution is provenance. Every wallet involved in the market-making scheme can be traced directly to the Deployer wallet controlled by Defendants.

169. The chain of custody is unbroken:

- a. The Deployer³⁷ created the tokens
- b. The Deployer funded Allocation Wallets 1-4 with zero-cost inventory
- c. Allocation 3 cascaded tokens through sub-wallets (3-3 → 3-3-1 → 3-3-2 → 3-3-3)
- d. The cell wallets conducted market-making operations
- e. Proceeds consolidated in wallets including "Agustin Offboarding Wallet 3"

170. The tokens sold to the public came from wallets that Defendants controlled from the moment of creation. There is no gap in the chain of custody, no arm's-length transaction, no point at which an independent party acquired this inventory.

(2) Timing and Lifespan: Scheme-Bounded Accounts

³⁷ Address: 9zPxrXcor3gzTsg73LGBji6VVpfNYeiAq9T9GDPmKTHV

171. The wallets used in the scheme exhibit a distinctive temporal pattern: they were created shortly before launch or before discrete trading campaigns, they were active only during the relevant operational period, and they then went dormant.

- a. Allocation 3 received its funding on October 28, 2024
- b. The cascading distribution through 3-3-x occurred on November 25, 2024
- c. Market-making operations ran from November 25, 2024 through December 6, 2024
- d. Proceeds consolidation completed by December 6, 2024
- e. The wallets show little meaningful activity before or after these windows

172. These wallets behave like temporary house accounts opened for a particular deal. They were created for this scheme, used for this scheme, and retired after this scheme.

(3) Shared Endpoints: Convergence on Common Beneficiaries

173. Multiple branches of the Allocation tree, operating through different downstream wallets, ultimately converge on the same centralized exchange deposit addresses and consolidation wallets.

174. For example, purportedly separate exit paths terminate at identical centralized-exchange deposit addresses, including Coinbase deposits of roughly \$2 million via the Allocation 3-1 exit path and Kraken deposits of roughly \$2.2 million via the Allocation 3-5 multisig route, confirming that these on-chain branches served the same off-chain beneficiary.

175. The “Agustin Offboarding Wallet 3,” defined more fully below, received proceeds from multiple cell wallets confirming these different paths served the same beneficiary.

176. If these were truly independent traders, they would not all be depositing their profits into wallets attributed to the Defendants.

(4) Identical Behavioral Templates: The Signature of Automation

177. The most striking evidence of centralized control is the templated behavior across the cell wallets:

- a. Ten wallets each received exactly 22,991 ZEREBRO in a single bundled transaction; and other branches used the same templated ten-wallet structure, including ten wallets each receiving 100,000 ZEREBRO from Allocation 3-4-3-4 in a single transaction;

- b. All ten engaged in the same high-frequency trading pattern on Raydium via Jupiter
 - c. All ten generated approximately \$200,000 in trading profits
 - d. All ten sent their proceeds to the same offboarding wallets
 - e. All ten ceased activity at approximately the same time
178. Ten new accounts funded identically from the same house wallet, trading the same product in the same manner, and sending proceeds to the same destination, are not ten independent actors. They are ten sleeves of one desk strategy. This is the forensic signature of automated, centralized market manipulation.

(5) Direct Connection to Defendants

179. Defendant Cortes publicly identified the ‘UpdatedDevWallet’ as a wallet controlled by the development team, and forensic tracing shows direct flows from Allocation 2 into that wallet (“Agustin Offboarding Wallet 3”).
180. In April 2025, Allocation 2 transferred a high-value block of ZEREBRO into UpdatedDevWallet valued at approximately \$450,000 at the time, confirming that pre-value insider inventory was converted into developer compensation.
181. Allocation 2 also functioned as a proceeds wallet: across several thousand transactions, it received repeated micro-deposits of approximately 0.0975 SOL from numerous addresses, swapped those inflows into USDC, and more than \$200,000 in USDC passed through the wallet before being off-boarded.
182. The wallets that Defendant Yu later claimed belonged to “third-party hackers” were, in fact, wallets used for the market manipulation of the \$ZEREBRO token described in this Complaint.
183. Defendants themselves have confirmed, through public statements and wallet naming conventions, that they controlled the infrastructure used for market manipulation. Their subsequent attempt to blame “hackers” for wallets they themselves controlled is evidence of consciousness of guilt.
184. Most significantly, the same network of wallets used to conduct market-making in \$ZEREBRO has been used in connection with other crypto projects directly associated with Defendants.

185. Wallets that participated in the Zerebro market-making scheme also appear in transactions related to other projects launched or promoted by Defendants, including PLOI, which is directly attributable to Defendant Jeffy Yu, and Blormmy, which is associated with Defendant Cortes.³⁸



Figure 14: Screenshot of Defendant Cortes's LinkedIn profile showing his affiliation with "Blorm" and describing his focus on "AI wallet orchestration" for "onchain actions."

³⁸ Screenshots of Defendant Yu's December 31, 2024 posts confirming that both Defendants collaborated on Blorm launchpad projects are attached as Exhibit F and incorporated by reference here.

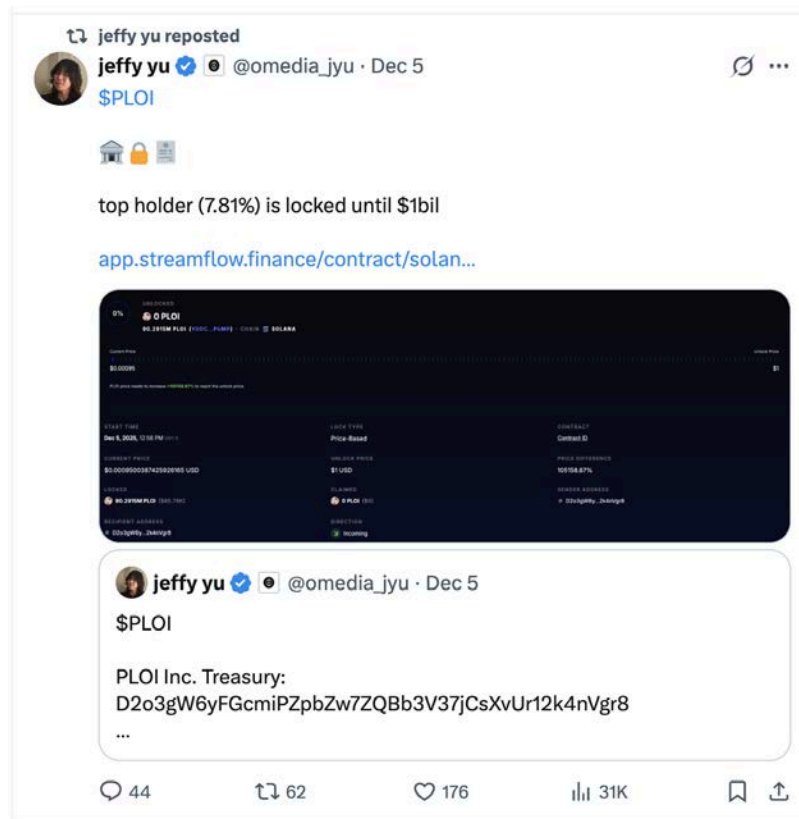


Figure 15. Screenshot of Defendant Yu promoting \$PLOI and a “PLOI Inc. Treasury” Solana address, alongside a Streamflow token-lock screenshot suggesting transfer restrictions on token holdings.

186. The reuse of the same wallet infrastructure across multiple projects eliminates any plausible explanation that the Zerebro wallets belonged to unrelated third parties. It demonstrates a repeatable operational playbook used by Defendants across different tokens.

vi. Conclusion on Attribution

187. Taken together, these facts establish that the market-making and price-engineering activity was conducted by Defendants, using wallets they controlled, funded with tokens they obtained at no cost, and concealed from the public while they profited at purchasers’ expense.³⁹

188. This attribution does not depend on speculation or inference. It is grounded in objective, verifiable on-chain data that directly links Defendants to the market

³⁹ Note: The complete tracing analysis is set forth in Exhibit K (Tracing Report) attached hereto and incorporated by reference.

manipulation scheme. Every transaction cited above can and has been independently verified on the Solana blockchain through block explorers such as Solscan.

F. The “Research and Development” Narrative as Post-Launch Maintenance Fraud

189. When purchasers began asking whether any of the promised products had been delivered, Defendants reframed delays as related to ongoing research and development and asked holders to remain patient while continuing to promote the project's roadmap and purported progress.
190. The messaging maintained confidence, deterred public exits, and, as a result, purchasers held. While they held, issuer-controlled wallets continued supplying liquidity, trading against the public, and off-ramping proceeds through centralized exchanges and cross-chain bridges.
191. Defendants told retail purchasers to wait and the result was stark. On-chain evidence shows that while retail purchasers held, Defendants were actively engineering liquidity and monetizing inventory.

G. From Peak to Collapse

192. Defendants’ undisclosed market-making and liquidity management created the appearance of deep, community-driven liquidity, steady volume, and organic price discovery. Those signals were false because they were materially driven by issuer-controlled wallets operating against the market.
193. As Defendants' artificial market support waned and the absence of functional technology became apparent, the price of \$ZEREbro collapsed, causing substantial losses to purchasers.
194. Defendants had exited their positions. The market they left behind, stripped of the artificial support their trading had provided, could not sustain the prices they had engineered.

H. Escalation, Concealment, and Consciousness of Guilt

195. As the market for \$ZEREbro collapsed and the discrepancy between Defendants' representations and reality became unavoidable, Defendants escalated their deception. Rather than correct prior statements or disclose the true state of the

project, Defendants adopted tactics designed to divert attention, obscure responsibility, and conceal the proceeds of the scheme.

196. As public pressure mounted regarding Defendants' failure to deliver on Zerebro's technical promises, Defendant Yu staged his own death. Yu broadcast what appeared to be a self-inflicted gunshot and arranged for an obituary to be published. During this episode, Yu launched a commemorative token, \$LLJEFFY, framed as having been launched by a 'deadman's switch,' triggered by his death. That token briefly reached a market capitalization of approximately \$100 million before losing virtually all of its value. Yu's staged death diverted scrutiny from the project's failures and enabled yet another fraudulent extraction for financial gain.

197. As later reported publicly, Defendant Yu did not die and the death announcement was a hoax. Yu subsequently resurfaced, posted photographs of himself holding stacks of cash, and continued launching cryptocurrency projects. The staged death was consistent with Defendants' pattern throughout the scheme: when confronted with the consequences of their conduct, they did not accept accountability but instead escalated their deceptions.⁴⁰

⁴⁰Figures 15–17 are attached as Exhibit G and incorporated by reference here.

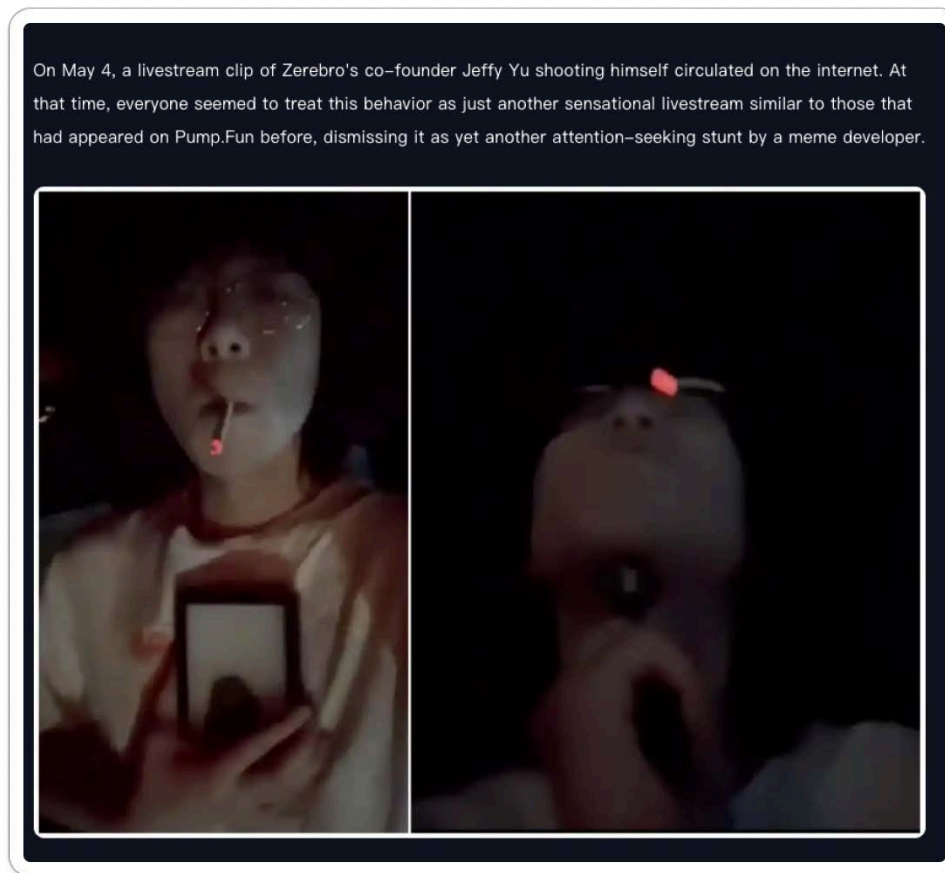


Figure 16: Screenshot from an online post/article describing the May 4 livestream clip showing Zerebro co-founder Jeffy Yu purported suicide.

Jeffy Yu	
BORN	DIED
2002	2025

Jeffy Yu

2002 - 2025

Jeffy Yu Obituary

Jeffy Yu
05/06/2002 - 05/04/2025

A Martyr of Imagination and Creativity

Jeffy Yu, a visionary artist, technologist, and cultural force, passed away in May 2025 at the age of 22. His life, though brief, was lived with intensity, brilliance, and a devotion to creation that he hoped would inspire others for eternity. A tech prodigy from an early age, Jeffy entered Stanford University at just 15 to study computer science. Driven by a restless curiosity and creative spark, he later attended Northeastern University and Arizona State before leaving academia behind to dive fully into the world he was already building. By the age of 19, he was working full-time as a software engineer in Santa Cruz. Two years later, he co-founded and scaled a company to an \$800 million market cap in under six months.

Figure 17: Screenshot of an online obituary page for Defendant Jeffy Yu (2002–2025) posted after the staged suicide attempt.

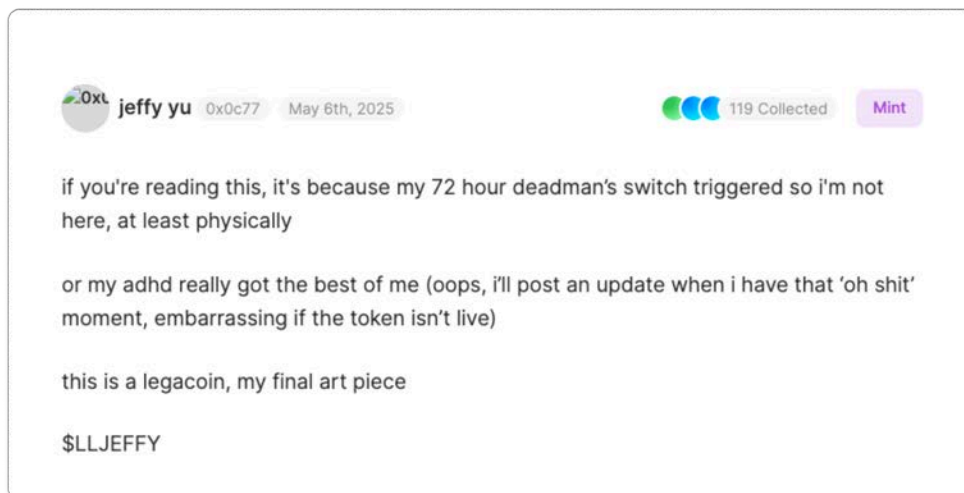


Figure 18: Screenshot of a May 6, 2025 post by Defendant Yu asserting that a 72 hour deadman's switch "has been triggered, launching a posthumous token (\$LLJEFFY).



Figure 19: Although \$LLJEFFY at one point briefly hit a 100m marketcap, it went on to quickly lose over 99% of its value.



Figure 20: Screenshot of a subsequent X post from the @omedia_jyu account showing Yu alive and holding large bundles of cash.

198. For example, Decrypt reported that Yu was discovered alive and that the death was a hoax.⁴¹

⁴¹ <https://decrypt.co/318149/zerebro-founder-obituary-legacoin-token-speculation>

Zerebro Founder Obituary Removed Amid \$105 Million 'Legacoin' Token Speculation

A now deleted video showed Zerebro founder Jeffy Yu dying by suicide. But the coroner told Decrypt there's no record of his death.

Figure 21: Screenshot of a Decrypt headline reporting that the “Zerebro founder obituary,” shown above, was removed amid \$105 million “Legacoin” token speculation and quoting a coroner as having no record of Yu’s death.

199. Yu took these actions to evade liability. Yu subsequently attempted to develop additional AI crypto assets, none of which achieved meaningful traction.
200. Following Yu's staged death, Defendants turned on each other in public, each claiming the other had masterminded the fraud. Yu identified a series of wallets that he claimed belonged to Cortes.
201. Forensic analysis confirmed that the wallets Yu identified were part of the same operational cluster used to conduct market-making and wash trading for \$ZEREBRO.
202. The same wallets were also connected to market-making activity for the Blormmy and PLOI tokens, projects in which both Defendants participated. The forensic evidence thus contradicted Yu's attempt to shift blame to Cortes. The wallets Yu publicly attributed to Cortes were part of an operational infrastructure that both Defendants controlled.
203. Cortes listed Zerebro on his LinkedIn profile as a successful exit, presenting the scheme as a professional credential. The "exit" Cortes celebrated was the extraction of value from purchasers who relied on Defendants' false representations.⁴²

⁴² See https://x.com/omedia_jyu/status/1979613424880660810?s=20

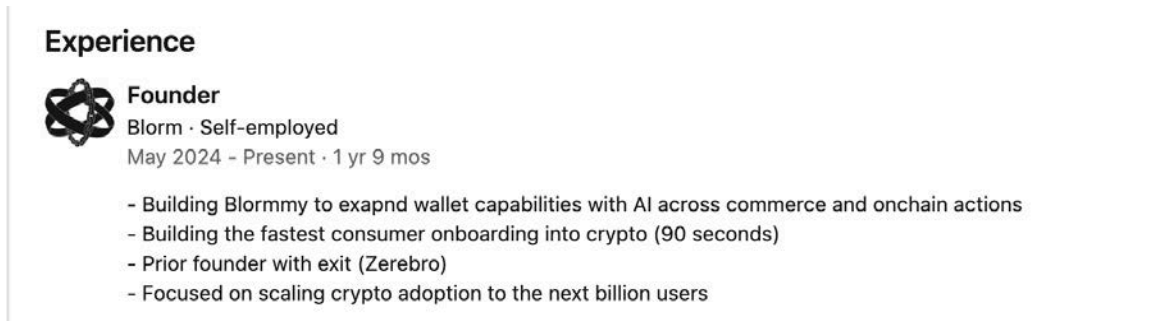


Figure 22: Screenshot of the “Founder — Blorm” entry on Cortes’s LinkedIn profile claiming he was a “prior founder with exit (Zerebro)” while building “Blormmy” wallet capabilities.

204. Notably, as defendants were made aware of pending litigation, they deleted key aspects of their online presence to evade liability, again speaking directly to their culpability.

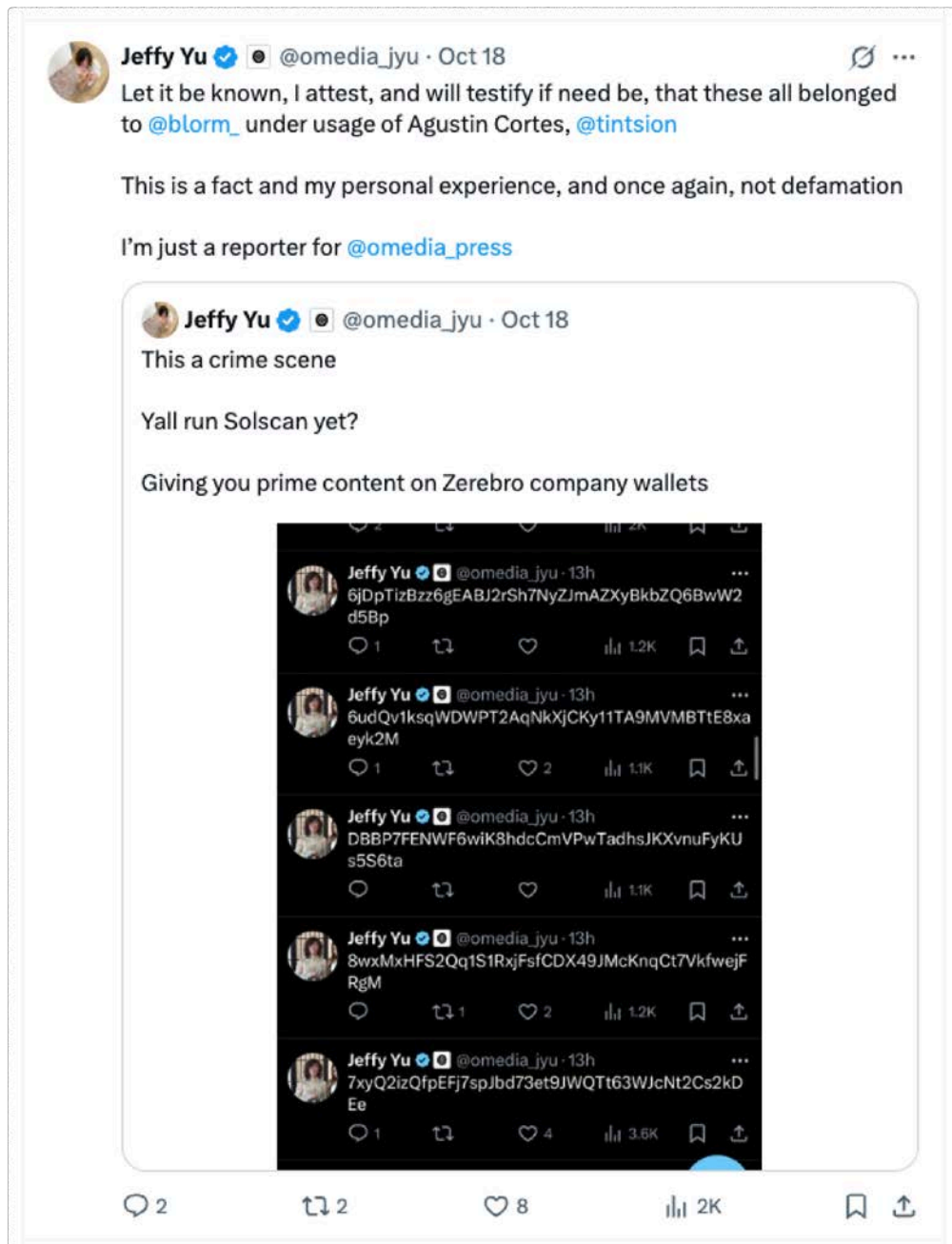


Figure 23: Screenshot of Defendant Yu's X post stating he would testify that certain wallets belonged to @blorm_ and were used by Agustín Cortes (@tintsion), while posting purported "Zerebro company wallet" addresses.

205. Defendants knew that the project lacked the technology, development, and governance they had promised. Defendants knew that disclosure of those facts would accelerate the collapse and expose their prior conduct.

206. Defendants' consciousness of guilt is evident in their subsequent conduct: Yu staged his own death and then resurfaced posting photographs with cash; Defendants publicly accused each other of masterminding the fraud; Yu attempted to shift blame by identifying wallets that forensic analysis revealed were part of a jointly controlled operational infrastructure; Cortes listed Zerebro on his LinkedIn profile as a successful exit, treating the extraction of value from deceived purchasers as a professional credential; and Cortes deleted social media posts promoting Zerebro after the scheme began to unravel.
207. Defendants escalated their deception to evade accountability and preserve the benefits they had already extracted.
208. Taken together with the false representations, undisclosed market manipulation, and insider selling described above, Defendants' final acts confirm the nature of the Zerebro project. This was a knowing scheme sustained by misrepresentation and concealment until the truth could no longer be hidden.

V. CLASS ALLEGATIONS

209. Plaintiff brings this action on behalf of himself and all others similarly situated pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3). In the alternative, and to the extent the Court finds that individualized issues predominate as to any element of damages or other relief, Plaintiff seeks certification under Rule 23(c)(4) of one or more common issues for classwide resolution.

A. Class Definition

210. The proposed Class is defined as: All persons and entities who acquired the digital asset denominated '\$ZEREbro' during the period from October 25, 2024 through the date of the filing of this action (the 'Class Period'), and who suffered damages as a result of the conduct alleged herein.
211. Excluded from the Class are: Defendants; any immediate family members of Defendants; any entity in which Defendants have or had a controlling interest; any persons who were officers, directors, or agents of the scheme alleged herein; and the Court, its staff, and their immediate family members.
212. Plaintiff additionally seeks certification of the following subclass: New York Subclass: All members of the Class who were residents of New York at the time they

acquired \$ZEREBRO. Plaintiff will seek appointment of an additional class representative for the New York Subclass who is a resident of New York and whose claims are typical of the Subclass, and will move to amend as appropriate to add such representative.

B. Rule 23(a) Requirements

213. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. The \$ZEREBRO token was marketed and sold to thousands of purchasers across the United States and internationally through public blockchain networks and accessible trading platforms. Class membership is determinable through objective transaction records.
214. **Commonality:** Common questions of law and fact exist, including, among others:
- a. whether Defendants disseminated the challenged representations and omissions through uniform public channels;
 - b. whether the promised technology and ecosystem components (including Zerebro, ZerePy, Zentients, and related APIs/models) existed in any operational form;
 - c. whether Defendants controlled wallets and accounts used to launch, distribute, provide liquidity for, and trade \$ZEREBRO, including whether Defendants operated an undisclosed issuer-controlled market-making and/or wash-trading apparatus;
 - d. whether Defendants' representations and omissions were material;
 - e. whether Defendants' conduct caused purchasers to acquire \$ZEREBRO at prices affected by undisclosed issuer-controlled trading, liquidity activity, and supply concentration; and
 - f. the proper measure of damages, restitution, and/or disgorgement using transaction-level data and other common proof.
215. **Typicality:** Plaintiff's claims are typical of the Class because Plaintiff acquired \$ZEREBRO during the Class Period in the same market affected by Defendants' challenged conduct, was exposed to the same or materially similar public representations and omissions disseminated through Defendants' uniform promotional campaign, and suffered the same type of injury (economic loss) when the truth emerged and the token's value collapsed.

216. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff's interests are aligned with those of the Class, there are no conflicts, and Plaintiff has retained counsel experienced in complex class actions and digital-asset litigation, including claims involving market manipulation and alleged misrepresentations.

C. Rule 23(b) Requirements

217. **Predominance:** Common questions predominate over any individual issues. Liability turns on Defendants' uniform course of conduct: a single token launch; materially uniform representations and omissions disseminated through centralized public channels; and an alleged issuer-controlled market-making and liquidity operation affecting purchasers generally. For the New York Subclass, individualized reliance is not an element of liability under N.Y. Gen. Bus. Law § 349. To the extent damages calculations are required, they can be performed mechanically using transaction-level data and do not defeat certification.
218. **Superiority:** A class action is the superior method for adjudicating this controversy. Individual claims are economically infeasible given the amounts at stake; class treatment avoids duplicative litigation and inconsistent adjudications; transaction records facilitate centralized proof and claims administration; and concentrating this litigation in a single forum promotes judicial efficiency.

D. Rule 23(c)(4) Issue Certification in the Alternative

219. In the alternative, Plaintiff seeks certification under Rule 23(c)(4) of one or more common issues, including:
- a. whether Defendants' statements and omissions regarding the existence, functionality, and timing of Zerebro, ZerePy, Zentients, and related products were false or misleading;
 - b. whether Defendants operated or controlled wallets and accounts used for undisclosed issuer-controlled market-making, liquidity provision, and/or wash trading in \$ZEREPRO;
 - c. whether such undisclosed conduct and omissions were material to reasonable purchasers; and
 - d. whether Defendants' conduct constituted deceptive or unfair practices under applicable consumer-protection and common-law standards.

E. Ascertainability and Manageability

220. Class membership is objectively ascertainable through on-chain transaction records, including wallet addresses, timestamps, and transaction hashes, supplemented by verification of wallet ownership through cryptographic message-signing or comparable proof, and where applicable, exchange records for centralized-exchange transactions.
221. To the extent the Court determines that differences in state substantive law are material to certification of any nationwide common-law claims, Plaintiff will propose appropriate subclasses and/or grouping of materially similar legal standards, and/or proceed through Rule 23(c)(4) issue certification of the uniform core issues.

VI. CAUSES OF ACTION**COUNT I****Deceptive Acts and Practices (N.Y. Gen. Bus. Law § 349)****(On Behalf of the New York Subclass)**

222. Plaintiff repeats and re-alleges each preceding paragraph as if fully set forth herein.
223. Section 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce.
224. Defendants engaged in consumer-oriented conduct by marketing and selling the \$ZEREBRO token to the general public through websites, social media, podcasts, and other public channels. The campaign targeted ordinary retail consumers who lacked specialized knowledge and had no ability to independently verify Defendants' claims.
225. Defendants made materially misleading statements and omissions, including representations that:
- a. Zerebro possessed a functional "autonomous," "jailbroken" AI agent, when no such agent existed;
 - b. ZerePy, Zentients, and proprietary API-accessible models were functional or imminent, when none existed in any operational form;
 - c. GitHub activity and "dev logs" reflected genuine engineering progress, when such activity was cosmetic;
 - d. The token's value would be driven by ecosystem adoption, fees, and "value accrual" mechanisms that did not exist;

- e. The market for \$ZEREBRO reflected organic demand, while failing to disclose that Defendants operated an undisclosed market-making apparatus that manufactured volume, controlled liquidity, and monetized zero-cost inventory;
 - f. The project was an active "research lab" with ongoing development, while Defendants were liquidating positions and no meaningful development was occurring.
226. These misrepresentations and omissions were material. A reasonable consumer would consider it important to know whether the technology existed, whether the market was operated by undisclosed insiders, and whether the economic mechanisms described as driving token value were real.
227. Members of the New York Subclass suffered actual injury as a direct result of Defendants' deceptive conduct. They purchased \$ZEREBRO while located in New York at prices artificially supported by false narratives and undisclosed market manipulation. When the truth emerged, demand collapsed and the token's value was substantially destroyed, causing out-of-pocket losses, diminution in value, and consequential damages.
228. Pursuant to N.Y. Gen. Bus. Law § 349(h), Plaintiff, on behalf of the New York Subclass, seeks actual damages, treble damages where Defendants' conduct is willful and/or knowing, injunctive relief including curative disclosures and a notice program, reasonable attorneys' fees and costs, and such other relief as the Court deems just and proper.

COUNT II

False Advertising (N.Y. Gen. Bus. Law § 350)

(On Behalf of the New York Subclass)

229. Plaintiff repeats and re-alleges each preceding paragraph as if fully set forth herein.
230. Section 350 prohibits false advertising in the conduct of any business, trade, or commerce.
231. Defendants disseminated advertisements to the public through the project website, white paper, social-media posts, podcast appearances, livestreams, and promotional content across platforms including X, Telegram, Discord, and Warpcast. These materials were designed to induce consumers to purchase \$ZEREBRO and were consumer-oriented in nature.

232. Defendants' advertisements were materially false and misleading, including representations that:
- Zerebro was an "autonomous," "jailbroken" AI agent with persistent memory and cross-platform capabilities;
 - ZerePy, Zentients, and proprietary AI models were functional, in testing, or imminent;
 - The token represented participation in a "long-term venture" with defined "value accrual," treasury reinvestment, and governance mechanisms;
 - Development was active and ongoing, as evidenced by roadmaps, "dev logs," and repository activity;
 - The project constituted foundational AI-agent infrastructure comparable to legitimate technology ventures.
233. These advertisements were likely to mislead a reasonable consumer. Defendants presented themselves as credentialed founders, used the language and presentation of legitimate AI startups, and made specific factual claims about product status that consumers had no practical ability to verify. The advertisements created the false impression that purchasers were investing in a real technology platform rather than trading into a market secretly operated by insiders with no underlying product.
234. Members of the New York Subclass were exposed to and relied on these advertisements in deciding to purchase \$ZEREPRO while located in New York. As a result, they suffered actual injury when the falsity of the advertised claims was revealed and the token's value collapsed.
235. Pursuant to N.Y. Gen. Bus. Law § 350-e, Plaintiff, on behalf of the New York Subclass, seeks actual damages, treble damages where Defendants' conduct is willful and/or knowing, injunctive relief including corrective advertising and curative disclosures on the same channels used for the false advertisements, reasonable attorneys' fees and costs, and such other relief as the Court deems just and proper.

COUNT III

Negligent Misrepresentation

(On Behalf of Plaintiff and the Class)

236. Plaintiff repeats and re-alleges each preceding paragraph as if fully set forth herein.

237. Defendants supplied false information for the guidance of others in their business transactions. Defendants possessed superior knowledge of the project's true status and communicated directly to purchasers through official channels, knowing that retail purchasers would rely on those statements in deciding whether to purchase \$ZEREBRO.
238. Defendants made false and misleading statements concerning material facts, including representations about the existence and functionality of the Zerebro AI agent, ZerePy, Zentients, and proprietary models; the nature of ongoing development; the economic mechanisms underlying the token; and the organic nature of the market—when Defendants knew or should have known that the technology did not exist, development was not occurring, and the market was materially influenced by undisclosed insider operations.
239. Defendants failed to exercise reasonable care in obtaining or communicating this information. Defendants controlled all repositories, infrastructure, wallets, and communications associated with the project and had exclusive access to the facts necessary to verify or correct their statements. Despite this, Defendants disseminated false claims without any reasonable basis for believing them to be true.
240. Plaintiff and Class members justifiably relied on Defendants' representations in purchasing \$ZEREBRO. The facts misrepresented were peculiarly within Defendants' knowledge and control, and purchasers had no practical means of independent verification. As a direct and proximate result of this reliance, Plaintiff and Class members suffered pecuniary losses, including overpayment and diminution in value of their holdings.
241. Plaintiff seeks compensatory damages, consequential damages, and such other relief as the Court deems just and proper.

COUNT IV

Fraud / Fraudulent Inducement

(On Behalf of Plaintiff and the Class)

242. Plaintiff repeats and re-alleges each preceding paragraph as if fully set forth herein.
243. Defendants made false representations and omissions of material fact, including statements that: Zerebro possessed autonomous AI capabilities; ZerePy, Zentients, and proprietary models were functional or imminent; development was active and ongoing;

the token's value was driven by real economic mechanisms; and the market reflected organic demand, while concealing that no technology existed, no meaningful development was occurring, and Defendants operated an undisclosed market-making apparatus that manufactured volume and monetized zero-cost inventory.

244. Defendants knew these representations were false or made them with reckless disregard for their truth. Defendants controlled all infrastructure, repositories, and wallets; possessed exclusive knowledge of the project's true state; directed the concealed market operations; and continued issuing false assurances while liquidating their holdings.
245. Defendants made these misrepresentations with the intent to induce Plaintiff and Class members to purchase and hold \$ZEREBRO. Defendants staged an equity-style promotional campaign, issued ongoing "guidance" through roadmaps and development updates, and publicly encouraged holding while insiders distributed tokens into the market.
246. Plaintiff and Class members justifiably relied on Defendants' misrepresentations in purchasing \$ZEREBRO. The facts misrepresented were peculiarly within Defendants' knowledge. Defendants presented themselves as credentialed founders with technical expertise, and purchasers had no practical means to verify claims about internal development, model architecture, or wallet control.
247. As a direct and proximate result of Defendants' fraud, Plaintiff and Class members suffered damages, including out-of-pocket losses and diminution in value when the truth emerged and the token's price collapsed.
248. Defendants' conduct was willful, wanton, and malicious, as evidenced by their knowing misrepresentations, concealed market manipulation, continued false assurances during insider liquidation, and Defendant Yu's staged death designed to evade accountability. Plaintiff seeks compensatory damages, benefit-of-the-bargain damages, consequential damages, rescission or rescissory relief, punitive damages, and such other relief as the Court deems just and proper.

COUNT V

Breach of Contract

(In the Alternative, Breach of Implied Covenant of Good Faith and Fair Dealing)

(On Behalf of Plaintiff and the Class)

249. Plaintiff repeats and re-alleges each preceding paragraph as if fully set forth herein.

250. Defendants offered, and Plaintiff and Class members accepted, terms governing the purchase of \$ZEREBRO and participation in the Zerebro ecosystem.

251. These terms were communicated through the project's white paper, website, and public representations, which described specific utilities, product access, governance rights, and economic mechanisms that would accompany token ownership. Alternatively, unilateral contracts formed when Defendants solicited purchases in exchange for defined deliverables and platform participation.

252. Plaintiff and Class members provided consideration by purchasing \$ZEREBRO and paying associated transaction fees.

253. Defendants breached the express terms of these agreements by failing to deliver the bargained-for products, utilities, and services, including: a functional AI agent with the described capabilities; access to ZerePy, Zentients, and proprietary models; governance mechanisms allowing tokenholders to influence the project's direction; and treasury management and reinvestment as represented.

254. In the alternative, Defendants breached the implied covenant of good faith and fair dealing by frustrating Plaintiff's and Class members' reasonable expectations.

255. Defendants manipulated communications, liquidity, and market conditions to simulate progress while withholding deliverables, encouraged holding based on false promises of imminent releases, and liquidated insider positions while publicly representing ongoing development.

256. This conduct is fundamentally inconsistent with the justified expectations of purchasers who acquired \$ZEREBRO based on Defendants' representations.

257. As a direct and proximate result of Defendants' breaches, Plaintiff and Class members suffered damages, including the value of consideration paid, loss of the benefit of the bargain, and consequential damages. Plaintiff seeks expectation damages, reliance damages, restitution or rescission where appropriate, and such other relief as the Court deems just and proper.

COUNT VI

Unjust Enrichment

(On Behalf of Plaintiff and the Class)

(Pleaded in the Alternative)

258. Plaintiff repeats and re-alleges each preceding paragraph as if fully set forth herein.
259. Defendants were enriched by receiving proceeds from \$ZEREBRO token sales, platform fees, and the monetization of insider holdings distributed into public demand.
260. These proceeds were obtained through the deceptive conduct described herein, including false representations about technology, products, and market conditions that induced Plaintiff and Class members to purchase and hold \$ZEREBRO.
261. Defendants' enrichment came at the expense of Plaintiff and Class members, who paid consideration for tokens based on false representations about the project's technology, development status, and market conditions, and who suffered losses when the truth emerged.
262. Under the circumstances, it would be unjust and inequitable for Defendants to retain the benefits conferred by Plaintiff and Class members. Defendants obtained these benefits through knowing misrepresentations, material omissions, and undisclosed market manipulation, while delivering none of the technology, products, or utilities that formed the basis of purchasers' expectations.
263. Plaintiff seeks disgorgement of Defendants' ill-gotten gains, restitution of all proceeds obtained through the conduct described herein, the imposition of a constructive trust over any assets traceable to the scheme, and such other equitable relief as the Court deems just and proper.

VII. PRAYER FOR RELIEF

264. WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, respectfully prays that the Court enter judgment in Plaintiff's favor and against Defendants, and award the following relief:
- a. Compensatory, actual, and consequential damages in an amount to be proven at trial;
 - b. Statutory damages, penalties, and multipliers where authorized (including under GBL §§ 349–350, on behalf of the New York Subclass);

- c. Rescission or rescissory damages where appropriate, including restoration of consideration paid, with interest;
- d. Restitution and/or disgorgement of all monies, tokens, and other benefits wrongfully obtained by Defendants;
- e. Punitive damages on the negligence, fraud and statutory claims (where available);
- f. Preliminary and permanent injunctive relief requiring, inter alia:
 - i. Curative disclosures on the project website and the same social channels used for promotion (including pinned notices) for a period set by the Court;
 - ii. Cessation of deceptive statements, advertising, and promotions;
 - iii. A notice program to impacted purchasers via email, website, and where feasible, on-chain wallet messaging;
 - iv. Records preservation and production of project, wallet, and exchange records relevant to token issuance, treasury, transfers, and sales;
 - v. A full accounting of all wallets, smart contracts, pools, and off-chain accounts used to receive, hold, or distribute proceeds;
 - vi. Establishment of any escrow/constructive trust necessary to effect restitution or rescission;
- g. Such further equitable relief as the Court deems just and proper (including constructive trust, tracing, and equitable lien);
- h. Certification of the proposed Class and any appropriate subclasses, appointment of Plaintiff as Class representative, appointment of appropriate subclass representative(s) as the Court deems proper, and appointment of Plaintiff's counsel as Class counsel; classwide notice; and classwide monetary and equitable relief;
- i. Reasonable attorneys' fees, costs, and expenses as permitted by law;
- j. Pre- and post-judgment interest at the maximum rate allowed by law; and
- k. Such other and further relief as the Court may deem just and proper.

VIII. JURY DEMAND

265. Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: February 9, 2026
New York, New York

Respectfully submitted,

BURWICK LAW, PLLC

/s/ Max Burwick

Max Burwick, Esq.

1 World Trade Center, 84th Fl.

New York, NY 10007

(646) 762-1080

max@burwick.law

Counsel for Plaintiff and the Proposed Class