April 30, 2026

Mr. Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581

Re:	**Comment on Prediction Markets, 91 FR 12516 (March 16, 2026), RIN 3038-AF65**
Submitted:	**VIA CFTC COMMENTS PORTAL: https://comments.cftc.gov**
Primary Contact:	**jordan.wain@chainalysis.com**

Dear Mr. Kirkpatrick:

Chainalysis Inc. ("Chainalysis") appreciates the opportunity to respond to the Commodity Future Trading Commission's (“Commisson” or “CFTC”) Advance Notice of Proposed Rulemaking (“ANPRM”).

Background on Chainalysis Inc.

Chainalysis is a blockchain data platform that enables safer, more secure use of public blockchains by banks, businesses, and governments. We provide blockchain analytics, investigative, and risk management technologies used by financial institutions, regulators, and law enforcement agencies to support compliance with anti-money laundering (“AML”), countering the financing of terrorism (“CFT”), economic sanctions, and other financial integrity requirements.

Foreword

We limit our response to the questions where we have differentiated knowledge and perspective: market surveillance, manipulation detection, inside information, and the specific considerations relevant to blockchain-based prediction markets. We do not comment on questions of legal classification, public interest determinations, or procedural aspects of CEA section 5c(c)(5)(C), which are better addressed by other commenters.

We recognize the Commission does not currently oversee any purely blockchain-based prediction markets; we are not taking a position regarding the legality or permissibility of such markets within the United States. Our response aims to identify the features and characteristics of existing blockchain-based prediction markets and suggest relevant approaches to oversight.

Our core position is the transparency of blockchain-based prediction markets provide regulators and market participants with unique surveillance and compliance capabilities as compared to a traditional, centralized derivatives market. Every on-chain transaction creates a permanent, publicly auditable record and blockchain analytics tools can cluster related addresses, trace fund flows, detect abnormal trading patterns, and correlate on-chain activity across platforms, in near-real time. The Commission should consider the unique features of blockchain-based prediction markets in its

regulatory guidance and recognize blockchain analytics as a core component of the market surveillance program for any designated contract market ("DCM") that lists event contracts on a blockchain and its own oversight.

Our response is organised into five areas:

- **I.** Core principles and Commission regulations, including market surveillance, manipulation prevention, abusive trade practices, operational risk, and blockchain-specific considerations;
- **II.** Swap data reporting and trade practices, including wash sale detection and disruptive trading;
- **III.** Inside information, including information advantage, cross-market manipulation, and government employee trading;
- **IV.** Cost-benefit considerations; and
- **V.** The quality and evidentiary standards of the blockchain analytics on which the foregoing capabilities depend (Annex A).

Responses to Questions

I. CORE PRINCIPLES AND COMMISSION REGULATIONS

Question 1: Guidance on DCM Core Principles for Prediction Markets

The Commission should provide guidance on how the DCM Core Principles apply to prediction markets. We respectfully urge the Commission to focus on Core Principles 3 (contracts not readily susceptible to manipulation), 4 (market surveillance), and 20 (operational risk), where prediction markets present considerations that differ most materially from traditional derivative contracts. Guidance should specifically address blockchain-based prediction markets, which present distinct challenges (oracle dependency, smart contract risk, pseudonymous participation) and distinct advantages (transaction transparency, immutable audit trails, cross-platform visibility) that existing guidance does not cover. The Commission's own enforcement record provides a useful starting point for identifying where that guidance is most needed.

Question 2a: Abusive Trade Practices

The Commission's enforcement experience provides useful guidance on which abusive trade practices are most pressing for prediction markets. In February 2026, the Division of Enforcement issued an advisory (Release No. 9185-26) following two enforcement cases involving misuse of nonpublic information on KalshiEX.[6] Both cases involved insider trading: a political candidate trading on his own candidacy, and a YouTube channel editor trading on upcoming video content to which he had advance knowledge. These are the first publicized enforcement actions specific to prediction markets, and both concern the same abuse type: trading on material nonpublic information about the event underlying the contract.

With these cases in mind it is clear how prediction markets differ from other exchange-traded instruments in ways that make some forms of abuse more salient and others less so:

Insider trading is a primary risk. Prediction markets are, by design, markets in event-specific information. Unlike a commodity futures market where the underlying is a fungible asset, a prediction market contract is tied to a discrete real-world event whose outcome may be known, or knowable, by a small number of people before it becomes public. The categories of potential insiders are broad:

political decision-makers, corporate executives, event organizers, journalists with embargoed information, oracle operators, and platform employees. The CFTC's own enforcement actions confirm that this risk is not theoretical.

Probability Signal Manipulation. Beyond insider trading, prediction markets are susceptible to a second category of abuse that has no direct parallel in traditional commodity markets. Their primary output is not a commodity price but a probability signal, one that is increasingly consumed by media outlets, financial terminals, policy analysts, and algorithmic trading systems as an authoritative indicator of event likelihood. This creates a category of manipulation with no direct parallel in traditional commodity markets: activity designed not to profit from a mispriced asset, but to distort the perceived probability of a real-world event. This can take at least two forms, attacking from opposite directions.

The first is wash trading for probability distortion. On an exchange platform, wash trading is typically motivated by volume inflation to attract traders or capture fee rebates. On a prediction market, these incentives are largely absent and there is an additional motivation: Wash trading is used to fabricate consensus on the platform itself, creating a false impression of market belief in a particular outcome to mislead external observers who rely on the probability signal. The Commission's surveillance guidance should recognize that the motivation differs from traditional wash trading.

The second is information seeding. An actor takes a directional position and then attempts to move the implied probability by feeding false or misleading narratives to journalists, social media influencers, or algorithmic news aggregators. Here, the manipulation targets the information environment outside the platform: real traders respond to a fabricated signal, and the market moves because genuine participants are acting on false information.

Both forms exploit the same underlying vulnerability, the growing reliance of external decision-makers on prediction market prices as authoritative probability estimates, but they require different detection approaches. Wash trading is primarily an on-chain analytics problem. Information seeding requires correlating on-chain position changes with off-chain information events.

Recommendation - The Commission should consider whether DCMs should:

1. Implement surveillance programs that can distinguish between wash trading on their platforms that is motivated by volume inflation and wash trading motivated by probability distortion, recognizing that the latter may involve smaller volumes but carry outsized influence given the growing external reliance on prediction market prices as probability estimates.
2. Maintain a capability to correlate on-chain position changes with off-chain information events, to cooperate with other DCMs and, where appropriate, OTHER partners to identify cases where significant position-building precedes or coincides with the dissemination of misleading information about the underlying event.

Front-running and MEV are relevant but secondary. On blockchain-based prediction markets, pending transactions may be visible in the mempool before confirmation, creating opportunities for actors to insert their own transactions ahead of pending orders. The Commission should consider requiring DCMs to disclose the extent to which their market structure exposes participants to these risks and what mitigations are in place. Preventing front-running and MEV extraction is primarily a question of platform design, but detecting and quantifying it after the fact is a surveillance function:

blockchain analytics can identify front-running and sandwich attacks retrospectively through single-block transaction sequencing analysis, enabling DCMs to measure the extent of MEV extraction on their platform and identify the addresses responsible.

Question 2b: Resolution Criteria and Dispute Resolution

The integrity of event contract resolution is closely related to the abuse risks previously discussed: if the mechanism that determines event outcomes can itself be compromised, trading surveillance alone cannot protect market integrity. Many blockchain-based prediction markets depend on external data feeds, commonly referred to as "oracles," to determine event outcomes and trigger contract resolution. Oracle integrity is therefore foundational to the enforceability of contract terms under Core Principle 2.

Recommendation

In light of this, the Commission should consider whether DCMs should use oracle-based resolution mechanisms to:

1. Document the oracle infrastructure and data sources used for each event contract;
2. Implement redundant oracle sources where feasible, so that no single data feed determines resolution; and
3. Maintain oracle integrity monitoring, that is, the ability to detect anomalous oracle data that could indicate manipulation or error before it triggers contract settlement.

Blockchain analytics can support oracle integrity monitoring by tracking addresses associated with oracle operators and data providers for prediction market trading activity, and by detecting patterns consistent with oracle data manipulation, such as anomalous oracle updates that coincide with large position changes.

Question 2c: Susceptibility to Manipulation

Building on the abuse types in our response to Question 2(a), the question of whether an event contract is "readily susceptible to manipulation" requires analysis specific to prediction markets rather than wholesale application of frameworks developed for traditional commodity or derivatives markets. The relevant question is which prediction-market-specific risks apply to a given contract and whether adequate surveillance tools exist to detect and deter them.

The Division of Market Oversight's Prediction Markets Advisory (Staff Letter No. 26-08, March 12, 2026) reinforces this point, underscoring that DCMs bear front-line responsibility for ensuring that listed contracts, including sports-related event contracts, comply with Core Principle 3 and the associated Appendix C guidance. The Commission should assess susceptibility to manipulation with reference to: the nature of the underlying event, the availability of surveillance tools to detect and deter manipulation, and the feasibility of addressing susceptibility.

1. **Manipulation risks specific to prediction markets:**
    i. **Insider trading and misuse of nonpublic information.** As described in our response to Question 2(a), this is a dominant risk for prediction markets, confirmed by the Commission's own enforcement record.[6] It is potentially detectable through wallet clustering, pre-event fund accumulation monitoring, and post-event fund flow tracing to

identify connections between trading wallets and entities with plausible access to nonpublic information.

ii. **Information manipulation.** As discussed under probability signal manipulation in our response to Question 2(a), this involves disseminating misleading information to move market-implied probabilities. Detection requires having some systematic way to correlate on-chain position changes with off-chain information events.

iii. **Oracle manipulation.** Blockchain-based prediction markets that rely on external data feeds for event resolution are susceptible to manipulation of those feeds. The 2022 Mango Markets case, in which a trader manipulated spot prices on centralized exchanges to inflate oracle-derived collateral values on a decentralized platform, illustrates the risk posed by this vector.[5] Detection requires oracle data integrity monitoring capabilities, including comparison across redundant oracle sources and systematic tracking of oracle-linked addresses for suspicious trading activity.

iv. **Wash trading for probability distortion.** As discussed in our response to Question 2(a), wash trading on prediction markets serves a different purpose than on exchanges: fabricating consensus to distort the probability signal rather than inflating volume. Detection requires address clustering and circular flow analysis to identify fabricated trading patterns.

v. **Cross-market manipulation.** An actor may attempt to move a prediction market price to influence a correlated traditional financial market, or vice versa. For example, manipulating a prediction market on a regulatory decision to affect the equity price of companies exposed to that decision. Blockchain analytics is well-suited to detect this because on-chain fund flows between prediction market wallets and related spot or derivatives market activity are visible through a single analytical platform.

vi. **Risks that are less applicable to prediction markets:** Traditional manipulation vectors such as cornering, squeezing deliverable supply, and spoofing/layering are less relevant to prediction markets. Prediction market contracts have binary outcomes, are typically fully collateralized, and resolve to known values ($0 or $1). Spoofing is possible on prediction markets that operate central limit order books, but the binary structure and position limits constrain its impact relative to traditional commodity markets.

Recommendation - The Commission should require DCMs listing event contracts to demonstrate that they maintain surveillance capabilities tailored to prediction-market-specific manipulation vectors, particularly insider trading detection and information manipulation detection, rather than applying a generic manipulation framework developed for traditional commodity markets. For blockchain-based markets, this should include address clustering and entity attribution, oracle integrity monitoring, cross-market activity correlation, and the ability to correlate on-chain position changes with off-chain information events.

The reliability of these capabilities depends on the quality of the underlying analytical methodology, and the Commission may wish to consider whether DCMs should be expected to demonstrate that the blockchain analytics they rely on meet the same standards described in Annex A, Section 7.

Question 2d: Market Surveillance

The abuse types identified in our response to Question 2(a), including insider trading, probability signal manipulation, and information seeding, each require specific surveillance capabilities that traditional exchange surveillance was not designed to provide. Effective market surveillance for blockchain-based prediction markets requires a fundamentally different approach, one that exploits

the transparency of blockchain data rather than relying solely on trade data submitted by intermediaries.

The surveillance stack. We submit that a market surveillance program for blockchain-based prediction markets should incorporate four layers:

Layer 1	On-chain data collection. Raw blockchain transaction data, smart contract event logs, and oracle data feeds. This data is publicly available on the blockchain and does not require cooperation from intermediaries to collect.
Layer 2	Blockchain analytics and attribution. Address clustering (grouping wallet addresses controlled by the same entity), entity attribution (linking clusters to known entities), risk scoring (assessing exposure to illicit activity or high-risk counterparties), and fund flow tracing (following the movement of value across addresses and platforms).
Layer 3	Market surveillance logic and heuristics. Abnormal trading pattern detection, pre-event position accumulation alerts, wash trading detection, and cross-market activity correlation. This layer can also incorporate model-driven risk scoring, where individual accounts are evaluated against behavioral baselines and flagged when their trading patterns, profitability, or timing deviate from what would be expected of an uninformed participant. This layer applies surveillance logic to the enriched data produced by Layers 1 and 2.

These 3 layers enable regulatory reporting and enforcement, including suspicious activity reporting, position reporting, and large trader reporting.

Datasets required. Effective market surveillance in crypto and digital asset markets requires several categories of data, as identified in research on regulatory surveillance frameworks for digital asset markets:[1]

Dataset	Source	Relevance to Prediction markets
On-chain blockchain data	Indexed and labeled blockchain data, including transaction records and event logs, from chains of interest. Available through blockchain analytics providers	Core surveillance substrate for blockchain-based prediction markets. Enables cross-platform visibility, fund flow tracing, and entity attribution
CeFi trade and order data	Collected from centralized market operators	Necessary for surveillance of prediction markets operating centralized order books, and for cross-referencing with on-chain activity
Oracle data feeds	Collected from oracle providers or extracted from on-chain oracle contracts	Essential for oracle integrity monitoring and detecting oracle-based manipulation

Social media and communications data	Curated data from providers of social media analysis	Relevant to detecting information-based manipulation and coordinated pump-and-dump activity
Listing announcements and material project information	Collected from market operators or aggregators	Necessary for constructing insider trading timelines and identifying pre-announcement trading

Cross-domain information sharing. The Commission's recent Memorandum of Understanding with Major League Baseball (Release No. 9199-26, March 19, 2026) reflects an important principle: effective surveillance of prediction markets cannot rely solely on trading data. Because a number of events underlying certain prediction market contracts originate outside the financial system, in sports, politics, corporate decisions, and other domains, comprehensive market integrity requires information-sharing arrangements with the entities closest to those events. The CFTC-MLB MOU establishes a framework for exchanging information about incidents that could affect both the integrity of professional baseball and the integrity of related prediction markets. This model could be extended to other event domains. Blockchain analytics supports this cross-domain approach by providing the on-chain leg of the surveillance picture: when a sports league, government agency, or other event-domain partner identifies suspicious activity on their side, blockchain analytics can endeavour to trace the corresponding trading activity, identify the wallets involved, and reconstruct the fund flows that connect the informed actor to the prediction market position.

Comparison with centralized market surveillance. Blockchain-based prediction markets offer surveillance advantages over centralized derivatives markets that the Commission should weigh in its rulemaking:

- **No subpoena required for transaction tracing**. In traditional markets, tracing the flow of funds typically requires legal process against multiple intermediaries. On a public blockchain, the complete transaction history of any address is visible to anyone with appropriate analytics tools.
- **Cross-platform visibility.** In traditional markets, trade surveillance is typically siloed within individual exchanges, and cross-market surveillance requires complex data-sharing arrangements. On a public blockchain, a single analytics platform can observe activity across all venues simultaneously.
- **Immutable audit trail.** On-chain records cannot be altered retroactively. For enforcement proceedings, this eliminates the risk of lost, corrupted, or tampered trade records.
- **Real-time capability.** On-chain transactions can be monitored in near-real time, enabling proactive detection rather than retrospective investigation.

Research on regulatory surveillance frameworks for digital asset markets supports this conclusion. As our consortium's report to the Australian Securities & Investments Commission observed:

"To be comprehensive, regulators need to be equipped to monitor and investigate misconduct across both CeFi and DeFi platforms, because abuse can take place on both... a comprehensive surveillance program would not just need to understand activity within platforms, but to be able to join up activity across those platforms, to understand that suspicious activity here was underpinned by other activity there."

This conclusion applies in the same manner to prediction markets. IOSCO's Policy Recommendations for Crypto and Digital Asset Markets (2023)[2] similarly emphasize the need for market surveillance across both centralized and decentralized venues, and for regulators to develop capabilities to detect market abuse using on-chain data. The UK Financial Conduct Authority's forthcoming crypto-asset market abuse regime (MARC), according to current consultation trajectory, appears to be shaping up to take a comparable approach, proposing that on-chain monitoring forms a core obligation for regulated crypto-asset trading platforms. The direction of travel internationally is consistent with the surveillance framework we describe here.

Analytic quality and reliability. The effectiveness of any blockchain analytics-based surveillance program depends on the quality of the underlying analytical operations, particularly address clustering and entity attribution, which form the foundation on which all surveillance alerts, position limit enforcement, and manipulation detection rest. A false positive in address clustering, incorrectly grouping an address into a cluster with which it shares no common key control, propagates to every downstream label, risk score, and exposure calculation. The Commission should therefore consider, in setting surveillance expectations, not only whether a DCM employs blockchain analytics, but whether the analytics meet demonstrable quality standards. We address the evidentiary framework for analytical quality in Annex A, Section 7, and note that only some providers' methodologies have been successfully tested under both judicial scrutiny (the Daubert standard in United States federal courts) and independent academic evaluation.

Recommendation - The Commission should:

- **i.** Recognize the integration of blockchain analytics as a core component of the market surveillance program of a blockchain-based DCM, not merely as an optional supplement to traditional surveillance.
- **ii.** Recognize cross-platform surveillance capabilities as a key function of a market surveillance program of a DCM, particularly the ability to trace fund flows between the prediction market and related cryptocurrency venues.
- **iii.** Provide guidance that recognizes blockchain analytics tools as meeting or exceeding the surveillance expectations of Core Principle 4 when properly implemented.
- **iv.** Encourage data sharing and common surveillance standards across DCMs operating prediction markets on the same blockchain, to facilitate cross-market manipulation detection.

Question 2e: Position Limits

On position limit enforcement specifically, blockchain-based prediction markets present a challenge in that a single beneficial owner may control multiple wallet addresses, each of which individually falls within position limits but which, in aggregate, exceed them. Blockchain analytics offers some way of addressing this challenge through the address clustering capability described in our response to Question 2(d), which identifies groups of addresses controlled by the same entity. The Commission should consider requiring implementation of address clustering as part of the position limit enforcement program of a DCM, and should recognize that this capability provides a level of beneficial ownership transparency that exceeds what is available in traditional intermediated markets, where position limits rely on trusting the veracity of self-reporting by market participants.

Question 2g: Operational Risk

Blockchain-based prediction markets present sources of operational risk that the Commission should consider in its guidance. We highlight three:

i. **Smart contract risk.** The market logic of blockchain-based prediction markets is typically encoded in smart contracts, self-executing code deployed on a blockchain. Smart contracts are generally immutable once deployed, meaning that bugs, vulnerabilities, or design flaws cannot be easily corrected. Exploits of smart contract vulnerabilities have resulted in significant losses across decentralized finance, with over $3.4 billion stolen through crypto hacks and exploits in 2025 alone. Static, point-in-time security measures such as pre-deployment audits, while necessary, are not sufficient on their own: industry data indicates that effectively all major smart contract exploits in 2024 and 2025 occurred on projects that had undergone pre-deployment security audits. Vulnerabilities may be introduced through upgrades, governance changes, or novel attack vectors that post-date an initial audit. The Commission may wish to consider whether DCMs that operate through smart contracts should be expected to maintain not only pre-deployment audits but continuous, real-time monitoring of smart contract interactions for anomalous behavior, including the ability to detect unauthorized changes to contract governance, unusual transaction patterns that may indicate exploits, and conditions that could trigger incorrect event resolution. Automated response capabilities, such as the ability to pause or circuit-break smart contract functions when anomalous behavior is detected, can enable DCMs to respond within minutes rather than after losses have already been incurred.

ii. **Oracle dependency.** As discussed in our response to Question 2b, many blockchain-based prediction markets depend on external oracle systems to deliver event-outcome data. Oracle failure, whether due to manipulation, technical fault, or data source unavailability, is a significant operational risk that can result in incorrect contract resolution. The Commission should require DCMs to document their oracle infrastructure, implement redundancy, and maintain oracle integrity monitoring.

iii. **Composability risk.** Blockchain-based prediction market positions may, by virtue of the open and permissionless nature of blockchain protocols, be integrated into other decentralized finance protocols, for example, used as collateral in lending protocols or incorporated into structured products. This "composability" can create complex, opaque risk profiles and novel manipulation vectors that the DCM may not be aware of. The Commission should require DCMs to monitor and disclose known composability risks, and should consider whether additional disclosure obligations regarding the use of prediction market positions in other protocols are warranted to manage systemic risk.

Question 2h: Blockchain-Based Prediction Markets

The Commission should provide specific guidance on the application of existing regulations to blockchain-based prediction markets. The key challenges and advantages are as follows:

i. **Advantages of blockchain-based markets for regulatory compliance:** The surveillance advantages described in our response to Question 2(d), including transaction transparency, cross-platform visibility, immutable audit trails, and real-time monitoring capability, apply with particular force to blockchain-based prediction markets. The blockchain analytics industry has developed sophisticated tools for address clustering,

entity attribution, risk scoring, and fund flow tracing that are directly applicable to market surveillance and that do not exist in traditional markets.

ii. Challenges of blockchain-based markets for regulatory compliance:

- **Pseudonymity.** Blockchain addresses do not inherently identify their controllers. While blockchain analytics can deterministically link addresses to real-world identities based on observed connections to services used for on- and off- ramping, there is a behavioral analysis component that can be used to supplement this, which is probabilistic. As such, as with any of the markets and entities that it has oversight of, the Commission should consider how know-your-customer ("KYC") requirements interact with blockchain analytics capabilities to ensure adequate participant identification.
- **Privacy-enhancing technologies**. Mixers and privacy-preserving protocols can obscure fund flows. While blockchain analytics has developed capabilities to trace through many of these technologies, they can increase the difficulty and cost of surveillance. The Commission should require DCMs to demonstrate that their surveillance program can identify and assess the use of privacy-enhancing technologies by market participants.
- **Cross-chain complexity.** Prediction market participants may fund their activity through assets bridged from other blockchains, creating multi-chain fund flows that require multi-chain analytics capabilities. The Commission should require DCMs to maintain surveillance coverage across the chains relevant to their platform.
- **Decentralized governance.** Some blockchain-based prediction markets may operate through decentralized governance mechanisms that complicate the identification of a responsible entity for compliance purposes. The Commission should provide clarity on the compliance obligations of entities involved in the governance and operation of blockchain-based DCMs.

Recommendation - The Commission should issue guidance that recognizes blockchain transparency as a regulatory asset, not merely a challenge, and should establish clear expectations that DCMs operating on blockchains leverage blockchain analytics as part of their compliance infrastructure.

Question 3: DCO Core Principles

We do not comment on clearing mechanics generally, but note that the considerations we have outlined regarding smart contract risk (Question 2g) and oracle dependency (Questions 2b and 2g) apply equally to derivatives clearing organizations that clear event contracts settled through blockchain-based mechanisms.

II. SWAP DATA REPORTING AND TRADE PRACTICES

Question 5a: Swap Data Reporting and Standardization

Blockchain-based prediction markets that list event contracts as swaps produce, by their nature, a richer and more granular data trail than traditional swap markets. Every trade, position change, and settlement event is recorded on-chain as a verifiable, timestamped transaction. This data is inherently standardized at the protocol level (transaction hashes, block numbers, contract addresses, event logs) and is accessible to the Commission, swap data repositories, and third-party analytics providers without requiring data submissions from the DCM.

Recommendation - The Commission should consider how this inherent transparency can complement or streamline traditional swap data reporting requirements under CEA section 2(a)(13). Specifically:

- On-chain transaction data could serve as a primary data source for swap data repositories, reducing the reporting burden on DCMs and improving data accuracy.
- Standardized on-chain identifiers, such as smart contract addresses for event contracts, could function alongside or in place of traditional identifiers (CUSIP/ISIN) for blockchain-based event contracts.

To the extent the Commission requires market participant identification for reporting purposes, it should consider how blockchain analytics-based attribution (linking wallet addresses to legal entities through exchange touchpoints and other on-chain indicators) can supplement traditional LEI-based identification.

Question 5b: Pre-arranged Trades and Wash Sales

Wash trading on blockchain-based prediction markets differs structurally from wash trading on traditional derivatives markets, but is also more readily detectable. (We discuss wash trading as an abusive trade practice in our response to Question 2a; here we address the specific provisions of CEA section 4c(a).)

The increased susceptibility arises because the cost of creating new blockchain wallet addresses is effectively zero. A single actor can create hundreds of addresses and trade between them, producing the appearance of broad-based market activity and inflated volume. Unlike traditional markets, where wash sales require collusion between accounts held at intermediaries (who may detect the activity through KYC records), blockchain-based wash trading can be executed by a single individual without any intermediary involvement.

However, the detectability is also materially higher. Blockchain analytics can identify wash trading using heuristics that identify:

- **Address clustering:** identifying wallets funded from the same source, or that share other behavioral indicators of common control.
- **Circular flow detection:** tracing patterns where value moves in a circle (from address A to B to C and back to A) without any change in economic ownership.
- **Temporal pattern analysis:** identifying trades that occur in suspiciously rapid or regular intervals between wallets that share no apparent economic relationship.

For prediction markets, the risk is different in kind: inflated volume could mislead participants and external observers about the reliability of market-implied probabilities, which are increasingly consumed as authoritative signals by media, financial terminals, and policy analysts.

Recommendation - The Commission should recommend DCMs operating blockchain-based prediction markets to implement wash trading detection programs that incorporate address clustering and circular flow analysis, among others, and should consider establishing surveillance standards for this purpose.

Question 5c: Disruptive Trading Practices

Blockchain-based prediction markets are susceptible to some disruptive trading practices that have no direct comparison in traditional derivatives markets. The most significant of these is MEV extraction, in which actors exploit knowledge of pending transactions, visible in the public mempool before block confirmation, to insert their own transactions in a way that profits at the expense of other market participants. Common MEV strategies on exchange platforms include front-running (trading ahead of a known pending order) and sandwich attacks (placing orders both before and after a pending transaction to profit from the resulting price impact).

In addition, flash loan-based attacks, in which an actor borrows a large amount of capital within a single blockchain transaction, uses it to manipulate market prices or oracle values, and repays the loan within the same block, represent a novel form of disruptive trading practice. These attacks can be executed without any capital outlay by the attacker and can occur faster than traditional circuit breakers can respond. Preventing flash loan attacks is primarily a question of oracle design and protocol architecture, but detecting them is a surveillance function: blockchain analytics can reconstruct the full sequence of borrow, manipulate, and repay within a single block to determine which accounts profited and through which protocols the attack was routed.

Detecting these practices requires single-block transaction analysis capabilities (identifying complex multi-step transactions executed within a single block) and mempool monitoring (observing pending transactions and detecting front-running patterns).

Recommendation. The Commission should recommend DCMs explore and disclose the extent to which their market structure exposes participants to MEV-related risks, and to implement transaction ordering protections or other mitigations where technically feasible.

III. INSIDE INFORMATION

Question 29: Information Advantage and Public Interest

The Commission asks whether there is public interest utility if people with an asymmetric information advantage on a particular event contract are able to trade on prediction markets. From a market surveillance perspective, the central tension is between price discovery and fairness. Prediction markets derive much of their informational value from the participation of individuals who are better informed about the likely outcome of an event. To the extent that informed trading improves the accuracy of prediction market prices as probability estimates, there is a legitimate public interest in permitting it.

However, as the enforcement cases discussed in our response to Question 2(a) illustrate, the line between "informed trading" and "insider trading" in prediction markets can be crossed. The "insider" in a prediction market context is not limited to the traditional securities-law concept of a corporate insider, but extends to anyone whose relationship to the underlying event provides a systematic information advantage, whether a political candidate, a content creator, an oracle operator, or a platform employee.

For prediction markets, the categories of individuals who may possess material non-public information about event outcomes are broader than in traditional securities markets. These include:

i. **Event participants:** individuals with non-public knowledge of the outcome of the underlying event (e.g., a political decision-maker trading on a political event contract)

ii. **Platform operators:** individuals with knowledge of upcoming contract listings, modifications, suspensions, or operational changes
iii. **Oracle operators and data providers:** individuals or entities that determine or provide the data used to resolve event contracts
iv. **Large position holders:** individuals whose trading activity itself may materially affect the market price

These categories cover individuals close to the event itself. But the insider trading risk also extends beyond the platforms to the broader regulated financial sector. As prediction markets grow in liquidity and contract diversity, employees of traditional financial institutions, including investment banks, prime brokerages, asset managers, and credit rating agencies, may use prediction markets as a channel for trading on MNPI obtained through their employment. For example, an employee with advance knowledge of a pending merger, a regulatory decision, or a large institutional trade could take a position on a related prediction market contract rather than trading the underlying security. Institutions subject to CFTC Rule 166.3 have a duty to diligently supervise their employees' handling of commodity interests, and CEA Section 2(a)(1)(B) provides for vicarious liability for violations committed within the scope of employment. This creates a compliance obligation for financial institutions to monitor their employees' prediction market activity, and a corresponding need for surveillance tools that can detect such activity across both traditional and blockchain-based venues.

The Commission should recognize that the appropriate response to information asymmetry is not to prohibit prediction markets, but to require adequate surveillance and enforcement tools that can detect and deter the misuse of material non-public information. Blockchain analytics provides these tools: wallet clustering and entity attribution can link trading wallets to the services and platforms through which insiders transact; pre-event accumulation monitoring can flag abnormal position-building ahead of event resolution; and fund flow tracing can reconstruct the source of funds used to take positions.

To illustrate, consider a prediction market contract on a regulatory decision that resolves at a known date. On-chain surveillance can flag a pattern in which a wallet with no prior prediction market activity is funded via a privacy-enhancing service 48 hours before resolution, takes a large directional position at favorable odds, and redeems the winning position immediately after resolution, then routes the proceeds through a chain of intermediary wallets to a centralized exchange. Each step in this pattern is individually unremarkable; the combination, surfaced through automated signal scoring and analyst review, constitutes a high-priority alert.

Blockchain analytics can then trace the funding source backward to determine whether it links to an address associated with a known entity, such as an exchange, service provider, or prediction market platform that holds know-your-customer records on its users. Identifying the individual behind the address requires cooperation from that entity, whether through the platform's own compliance processes or through law enforcement channels. Blockchain analytics provides the on-chain trail; the identity link depends on the KYC data held at the point where the on-chain trail meets a regulated service.

Because every trade on a blockchain-based prediction market is permanently recorded, blockchain analytics can track the on-chain activity of any account, including what positions were taken, when they were taken relative to event resolution, and where the proceeds were sent. Accounts that repeatedly redeem winning positions close to resolution, particularly where the proceeds are routed to the same services over time, can be flagged for further investigation. Identifying the individual

behind the account requires the cooperation of the service with whom the account holder has been verified.

Question 30: Events Controlled by Small Groups; Cross-Market Manipulation

Where the outcome of an event underlying a prediction market contract is under the control of a single individual or small group (for example, a corporate decision, a regulatory action, or a policy announcement), the risk of insider trading is heightened. Enhanced surveillance standards are warranted for event contracts where the underlying event outcome is determinable by a small, identifiable group.

A related concern is cross-market manipulation, where an actor seeks to move the prediction market to influence another market or vice versa. On a public blockchain, blockchain analytics is uniquely well-suited to detect this behavior. On a public blockchain, cross-market activity by the same actor is visible through fund flow tracing: an analyst can observe the same wallet (or cluster of related wallets) taking positions on a prediction market while simultaneously trading in related spot or derivatives markets. This cross-market visibility is a significant advantage over traditional derivatives surveillance, where cross-market manipulation requires data-sharing arrangements between self-regulatory organizations and often goes undetected.

Recommendation - The Commission should recommend DCMs to implement cross-market surveillance programs that correlate prediction market activity with related cryptocurrency spot and derivatives market activity, leveraging blockchain analytics to identify common actors across markets.

Question 31: What aspects of prediction markets are relevant to the application of this statute? Are prediction markets more or less likely than other derivative markets to be susceptible to "any manipulative or deceptive device or contrivance"?

Prediction markets may be *more* detectable environments for manipulative or deceptive devices than other derivative markets. As set out in our response to Question 2c, the manipulation vectors most relevant to prediction markets, including insider trading, information manipulation, oracle manipulation, and wash trading for probability distortion, each have on-chain signatures that blockchain analytics can identify, precisely because the underlying activity occurs on a public, immutable ledger. The application of blockchain analytics to prediction market surveillance enables the detection of manipulative activity that would be difficult or impossible to identify in traditional OTC markets, including coordinated trading across wallets, circular wash trading, oracle manipulation, and flash loan-based price distortion.

We note that the proviso in CEA section 6(c)(1), that "no rule or regulation… shall require any person to disclose to another person nonpublic information that may be material to the market price", creates a specific tension for prediction markets, where the informational value of the market depends in part on the participation of informed traders. The Commission should consider providing guidance that distinguishes between permissible informed trading (which enhances price discovery) and prohibited manipulation (which distorts it), and should recognize blockchain analytics as a tool that can help draw this distinction by identifying patterns of trading that are inconsistent with legitimate informed participation.

Question 32: Government Employee Trading

Prediction markets on political, regulatory, and governmental events are likely to be significantly affected by non-public information available to federal government employees and officials. Event contracts on policy decisions, regulatory actions, legislative outcomes, judicial rulings, and macroeconomic data releases all create direct opportunities for trading on government-sourced non-public information.

As per the example provided in response to question 29, blockchain analytics can support the enforcement of CEA section 4c(a)(3)-(4) by enabling investigators to identify wallets that built positions ahead of government announcements, trace the funding of those wallets to determine whether they are linked to known government-affiliated entities, and correlate trading patterns with the timing of non-public information access. While this analysis requires a triggering event (the announcement) and typically proceeds retrospectively, the immutable nature of blockchain records means that the evidence is preserved permanently and cannot be destroyed.

IV. COST-BENEFIT CONSIDERATIONS

Question 6: Costs and Benefits; Less Costly Alternatives

First, blockchain analytics provides a cost-effective market surveillance solution for blockchain-based prediction markets. Traditional market surveillance systems, designed for centralized order books, intermediation, and batch-processed trade data, require significant customization to function in blockchain-based market structures. By contrast, blockchain analytics platforms are purpose-built for on-chain data and serve as one component of a DCM's compliance infrastructure, providing the on-chain surveillance layer. A comprehensive surveillance program will also require trade data analysis, social media monitoring, and cooperation with partners, as described in our response to Question 2(d). The Commission should take this into account when evaluating the compliance burden of any proposed surveillance requirements.

Second, the inherent transparency of blockchain-based markets reduces certain regulatory costs that are significant in traditional derivatives markets. Trade reporting, position monitoring, and audit trail reconstruction, all of which impose substantial costs on traditional DCMs and their participants, are inherently facilitated by the public nature of blockchain data. To the extent the Commission considers prescribing surveillance and reporting requirements for prediction markets, it should recognize that blockchain-based markets bear these costs differently, and in many cases, more efficiently, than traditional intermediated markets.

V. CONCLUSION

Chainalysis supports the Commission's effort to develop a regulatory framework for prediction markets that is grounded in the specific characteristics of these markets and informed by the surveillance capabilities available today. We urge the Commission to recognize that blockchain-based prediction markets, when subject to appropriate surveillance requirements, offer a level of transactional transparency and auditability that exceeds what is available in traditional derivatives markets.

The Commission has an opportunity to establish a surveillance framework built on the transparency of blockchain technology, rather than one that ignores it. We recommend that any future rulemaking:

i. Recognize blockchain analytics, including address clustering, entity attribution, and fund flow tracing, as a vital component of DCM market surveillance programs for blockchain-based prediction markets.
ii. Set surveillance standards, calibrated to blockchain-native manipulation vectors, for manipulation detection, insider trading detection, and wash trading detection.
iii. Recognize the advantages of a cross-market surveillance which provides the cross-platform visibility unique to public blockchains.
iv. Treat blockchain transparency as a factor that weighs in favor of permitting event contracts, provided adequate surveillance tools are in place.
v. Address blockchain-specific operational risks, including smart contract vulnerabilities, oracle dependency, and composability, through tailored guidance.

Chainalysis is committed to supporting the Commission, prediction market operators, and market participants in building a market integrity infrastructure that enables these markets to operate safely, transparently, and in the public interest. We are available to engage with Commission staff on any of the matters raised in this submission, and would welcome the opportunity to contribute technical input as the Commission develops any proposed rules or guidance arising from this ANPRM.

We would welcome the opportunity to provide a technical briefing to Commission staff on the blockchain analytics capabilities discussed in this submission, including a demonstration of how these tools operate in practice in the context of market surveillance for blockchain-based trading venues. A summary of relevant capabilities is provided in Annex A.

Respectfully submitted,

Chainalysis Inc.

ANNEX A: Blockchain Analytics Capabilities Relevant to Prediction Market Surveillance

The following summarises the categories of blockchain analytics capability referenced throughout this submission. These capabilities are operational today and are used by government agencies and regulated financial institutions globally.

Capabilities

1. **Address Clustering and Entity Attribution**

   What it does. Groups blockchain addresses that are controlled by the same entity into "clusters" using co-spend analysis, common funding patterns, and behavioral indicators. Clusters are then linked to real-world entities, including exchanges, services, and named organizations, through a proprietary attribution database maintained via direct engagement with service operators, open-source intelligence, law enforcement cooperation, and on-chain analysis.

   Relevance to prediction markets. Enables DCMs and regulators to determine that multiple apparently independent wallet addresses participating in an event contract are in fact controlled by the same beneficial owner, critical for position limit enforcement (Question 2e), wash trading detection (Question 5b), and insider trading investigation (Questions 29–31).

2. **Transaction Monitoring and Risk Scoring**

   What it does. Monitors on-chain transactions in real time against configurable risk typologies. Each transaction is assessed for direct and indirect exposure to high-risk activity, including sanctions-listed entities, darknet markets, ransomware, fraud, and other illicit categories. Risk scores are computed based on the counterparty profile, the proportion of funds traceable to high-risk sources, and behavioral indicators.

   Relevance to prediction markets. Enables DCMs to screen prediction market participants and their transaction activity for AML/CFT compliance, and to generate alerts for suspicious patterns such as rapid accumulation of event contract positions funded by high-risk sources. Supports the "rules prohibiting abusive trade practices" required by Core Principle 2 (Question 2a).

3. **Fund Flow Tracing and Investigation**

   What it does. Traces the movement of value across blockchain addresses through multiple intermediary hops, including through cross-chain bridges, decentralized exchanges, and privacy-enhancing technologies such as mixers. Visualises the complete flow of funds from source to destination, enabling investigators to reconstruct the financial history of any on-chain actor.

   Relevance to prediction markets. Enables reconstruction of the funding trail behind suspicious prediction market positions; for example, tracing whether wallets that accumulated large positions ahead of an event resolution were funded by addresses linked to services or platforms associated with event insiders, oracle operators, or platform personnel (Questions 29–32). Also

enables cross-market manipulation detection by tracing common funding between prediction market wallets and related spot or derivatives market activity (Question 30).

4. **Cross-Market and Cross-Chain Surveillance**

   What it does. Correlates on-chain activity across multiple blockchain-based venues, including prediction markets, spot exchanges, decentralized exchanges, and lending protocols, to identify coordinated behavior by the same actor or actors. Detects patterns such as simultaneous position-building across related markets, circular fund flows between venues, and arbitrage activity that may indicate cross-market manipulation.

   Relevance to prediction markets. Directly addresses the Commission's question about cross-market manipulation (Question 30) and the requirement under Core Principle 4 that DCMs have the capacity to "prevent manipulation, price distortion, and disruptions of the delivery or cash-settlement process" (Question 2d). The public nature of blockchain data means that cross-market surveillance does not require bilateral data-sharing agreements between venues, a single analytics platform can observe activity across all blockchain-based markets simultaneously.

5. **Smart Contract and Protocol Monitoring**

   What it does. Monitors smart contract interactions in real time, detecting anomalous transaction patterns, contract exploits, flash loan activity, and oracle data anomalies. Includes the ability to simulate transactions to assess their economic effect before or after execution.

   Relevance to prediction markets. Addresses the operational risks identified in our response to Question 2g: smart contract risk, oracle dependency, and composability risk. Enables DCMs to detect smart contract exploits, oracle manipulation attempts, and flash loan-based market distortion in near-real time.

6. **Compliance Program Integration**

   What it does. Integrates with DCM compliance workflows through APIs and platform interfaces. Supports automated sanctions screening, suspicious activity report generation, case management, and audit trail documentation. Designed for deployment within regulated entity compliance programs.

   Relevance to prediction markets. Enables DCMs to operationalize the surveillance standards recommended throughout this submission, integrating blockchain analytics into their day-to-day compliance operations rather than treating it as a separate, ad hoc investigative tool.

7. **Evidentiary Standards and Methodological Quality**

   The surveillance capabilities described in Sections 1-6 above are only as reliable as the analytical methods that produce them. In the market surveillance context, false positives waste investigative resources and erode confidence, while false negatives create blind spots.

Without a quality framework, DCMs and regulators evaluating blockchain analytics providers are forced to compare along quantitative axes alone, coverage counts, entity counts, chain counts, metrics that reward scale over methodology. Quality should also be a basis for evaluation.

Blockchain analytics is not a single analytical operation. What the industry loosely calls "clustering" is in fact three distinct practices, each governed by its own evidence standard:

a. **Structural grouping (Tier 1 - Forensic Reliability):** determining which blockchain addresses share common key control. On UTXO-based blockchains such as Bitcoin, this can be established through co-spend analysis when addresses co-sign the same transaction. On account-based blockchains such as Ethereum and Polygon, different techniques are required, including contract deployment analysis, administrative key relationships, and operational pattern recognition, but the same standard applies: the grouping must be deterministic, reproducible, and independently auditable. Trained models cannot satisfy this standard because different training configurations may produce different conclusions from identical evidence.

b. **Attribution (Tier 2 - Analytic Confidence):** the linking of a structural group to a named real-world entity, based on off-chain intelligence including direct engagement with service operators, open-source intelligence, law enforcement cooperation, and corroborating on-chain evidence. Attribution claims should carry a confidence level, with explicit source characterization and documented analytic reasoning. Probabilistic outputs should not be presented in the same format as deterministic conclusions.

c. **Operator-beneficiary determination:** the analytical judgment distinguishing between an entity that controls the wallet infrastructure (the operator) and an entity that merely uses it (a beneficiary or customer). This distinction is critical: an exchange's hot wallet cluster contains addresses belonging to thousands of users, and incorrectly treating a user address as an exchange-controlled address would produce misleading exposure calculations and position limit assessments.

Each component carries different error characteristics. A false positive (an address incorrectly included in a group) propagates to any downstream analysis. An attribution error mislabels a correctly grouped set of addresses, a correctable mistake that does not compromise the structural integrity of the data.

Implications for the Commission. When considering surveillance standards for prediction market DCMs, the Commission may wish to consider whether DCMs should be expected to demonstrate that the blockchain analytics solutions they rely on have been subject to independent scrutiny, whether through court-tested evidence standards, academic peer review, or supervisory audit. Providers whose methodologies have been tested, for

example, under the Daubert standard in United States federal courts[3] or through independent academic evaluation such as the TU Delft study published at the USENIX Security Symposium[4], offer a materially different level of assurance than those whose methods have not been independently examined.

Notes

[1] Chainalysis, Putniņš & Piper Alderman, "Research on Market Misconduct in Crypto and Digital Asset Markets," commissioned by the Australian Securities & Investments Commission (ASIC), PROC1410 (2024). The program comprised three deliverables: a literature review and taxonomy of market misconduct; an exploratory consideration of a regulatory trade surveillance function for crypto and digital asset markets; and a scoping report on conducting a market cleanliness study.

[2] IOSCO, "Policy Recommendations for Crypto and Digital Asset Markets: Final Report" (November 2023). Recommendation 7 addresses market manipulation and Recommendation 8 addresses market surveillance obligations for crypto-asset trading platforms.

[3] United States v. Sterlingov , No. 1:21-cr-399 (D.D.C. 2024). The court evaluated the methodology under the Daubert v. Merrell Dow Pharmaceuticals, Inc. , 509 U.S. 579 (1993) framework, assessing whether the methods were testable, peer-reviewed, accompanied by known error rates, and generally accepted.

[4] Kelvin Lubbertsen, Michel van Eeten, and Rolf van Wegberg,"Ghost Clusters: Evaluating Attribution of Illicit Services through Cryptocurrency Tracing" Proceedings of the 34th USENIX Security Symposium (2025). The study evaluated clustering accuracy against ground-truth data derived from seized server infrastructure.

[5] See CFTC v. Avraham Eisenberg, No. 1:23-cv-00340 (S.D.N.Y. 2023); United States v. Avraham Eisenberg , No. 1:23-cr-00058 (S.D.N.Y. 2023). Eisenberg was convicted of commodities fraud and market manipulation in connection with the manipulation of the MNGO token price to extract approximately $116 million from the Mango Markets decentralized trading platform.

[6] CFTC Division of Enforcement, Advisory on Enforcement Authority over Event Contracts (February 25, 2026), Release No. 9185-26. The advisory followed two enforcement cases involving misuse of nonpublic information on KalshiEX, a CFTC-designated contract market.