The Case for Crypto Dark Pools, or Not?

September 11, 2025

I. Introduction – The James Wynn Incident as a Cautionary Tale

The world of decentralized finance ("**DeFi**") recently witnessed a stark illustration of its inherent risks with the liquidation of James Wynn's 949 BTC (valued at $99 million at the time) leveraged long position on Hyperliquid, a decentralized perpetuals exchange. The loss stemmed from two compounding factors: extreme leverage (40x), which created a razor-thin margin of safety, and the radical on-chain transparency that is a hallmark of blockchain technology.[1] Because all critical data about his position—its size, direction, and liquidation price of BTC of approximately $104,580—was available on a public ledger, it became a visible and tempting target for adversarial traders.

The Wynn liquidation is part of a broader pattern where DeFi's transparency can be its own Achilles heel. Consider the March 2025 "Whale Hunting" liquidation—where a trader's 40x leveraged Bitcoin short (valued at ~$520 million at the time) was publicly exposed, prompting another trader to rally others to push BTC's price higher in an effort to try and trigger his liquidation[2]—or the $JELLY self-dealing price manipulation episode on Hyperliquid—where an attacker on Hyperliquid targeted the low-liquidity token $JELLY by simultaneously withdrawing on margin to force their own short liquidation.[3]

In the latter example, the attacker opened a large short position of $JELLY on Hyperliquid's perpetuals market and withdrew his own collateral—setting up a forced liquidation if the $JELLY price rose. Using separate wallets, the attacker simultaneously purchased $JELLY on the spot market, artificially pushing up the price just enough to trigger the protocol's oracle to markup $JELLY, showing how clearly observable positions can not only cause adversarial actors to exploit public data, but also enable self-dealing.[4]

Cases like these are examples of the "transparency paradox": While DeFi's openness is designed to create a trustless system, it also fosters an adversarial environment where every user's strategy is exposed.

---

[1] Dilip Kumar Patairya, *This Crypto Trader Just Lost $100M, but He's Still Not Done*, Cointelegraph (June 17, 2025), https://cointelegraph.com/explained/this-crypto-trader-just-lost-100m-but-hes-still-not-done.

[2] The whale opened the initial $368 million position at $84,043 and managed to turn a profit, despite having to add $5 million to his short when traders started to "hunt" his short position's liquidtion, *See* Zoltan Vardai, Whale Closes $516M 40x Bitcoin Short, Pockets $9.4M Profit in 8 Days, Cointelegraph (Mar. 18, 2025), https://cointelegraph.com/news/whale-516m-40x-bitcoin-short-9-4-m-8-days; Ryan S. Gladwin, Crypto Traders Are Hunting a $521 Million Bitcoin Whale—Here's Why, Decrypt (Mar. 17, 2025), https://decrypt.co/310220/crypto-traders-hunting-521-million-bitcoin-whale.

[3] Simon Seojoon Kim, $1.1B Liquidation: Why Do All Large Web3 Traders Get Hunted?, Hashed Team Blog (Medium) (May 31, 2025), https://medium.com/hashed-official/1-1b-liquidation-why-do-all-large-web3-traders-get-hunted-96b6f0149267.

[4] DeFi Faces New Test as Low-Liquidity Token Gets Manipulated, Kaiko Research (June 17, 2024), https://research.kaiko.com/insights/defi-faces-new-test-as-low-liquidity-token-gets-manipulated.

This adversarial environment is also driven by a core economic principle of many blockchains known as MEV. MEV refers to the maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding, and changing the order of transactions in a block. While MEV serves a useful purpose—it creates a financial incentive for "block builders" to perform the computationally intensive work of constructing blocks—it can also lead to the predatory strategies of front-running and sandwich attacks that exploit user transactions.

The Wynn incident, among others, highlights the need to consider whether DeFi markets should be structured in a way to protect market participants from adversarial exploitation by, for example, keeping private information that bad actors can use to effectuate malicious MEV strategies.

This raises a few critical questions: could private execution layers, such as encrypted mempools or private order flow mechanisms, have shielded Wynn by concealing the very data that enabled malicious MEV strategies? If so, what role can technologies like private order flow and encrypted mempools, play in the future of DeFi? To address these questions, crypto protocol developers have started to implement market structures similar to those that have long existed in traditional financial markets—dark pools.

II. Dark Pools: From TradFi Concept to Crypto Necessity

Markets in Traditional Finance ("**TradFi**") faced similar problems long before DeFi: traders executing large, visible orders—such as brokers routing institutional client flow—have long been vulnerable to front-running, price manipulation, and even targeted liquidation attempts.

In the equities markets in particular, concerns about information leakage and predatory trading led to the development of dark pools—regulated private trading environments—typically registered as Alternative Trading Systems ("**ATS**")—that allow institutions to transact large blocks of securities on a marketplace that does not reveal their order details to the public market until after the trade is complete. By concealing trade details prior to execution, dark pools minimize slippage and mitigate front-running risk.

While crypto lacks a single directly analogous formal market structure, a growing number of decentralized tools seek to fulfill similar functions under different design constraints, primarily by shielding transactions from public view during the execution phase. Three principal architectures have emerged, each with distinct technical models and risk profiles:

- **Private Order Flow to Block Builders via Proposer / Builder Separation:** Proposer / Builder separation ("**PBS**") is a design pattern in composing blocks for blockchain transactions that separates the role of proposing blocks from the role of building them, allowing aggregators to send transactions directly to block builders without broadcasting them publicly. It is currently the most prevalent and practical implementation for achieving execution privacy on transparent blockchains like Ethereum. By routing order flow privately through PBS-compatible builders, execution can be protected without relying on centralized intermediaries—an approach similar in spirit to dark pools in TradFi, but implemented through decentralized infrastructure. The technical lifecycle of a private transaction involves several key steps:

    1. **User to Wallet:** A user initiates a transaction, but instead of using a standard public Remote Procedure Call ("**RPC**") Application Programming Interface ("**API**") endpoint, which broadcasts to the

public mempool, they configure their wallet to use a private RPC API endpoint provided by a specialized service.

2. **Wallet to Relay:** The transaction is sent directly to a "relay," a trusted intermediary (fulfilled by a software program) that acts as an auctioneer. The relay's job is to receive transactions from users and "searchers" (entities who look for profitable MEV opportunities) and make them available to block builders.

3. **Relay to Block Builder:** "Block builders" are sophisticated entities that compete to construct the most profitable block. They receive transaction bundles from relays and use powerful algorithms to order them in a way that maximizes extractable value. Their business model is to capture this MEV and share a portion of it with the proposer, the final actor in block building, in the form of a bid. The core trust assumption here is that the relay will not unbundle transactions or reveal them to builders before an auction is finalized.

4. **Builder to Proposer:** The builder submits its completed, sealed block header along with a bid to the relay. The
"proposer" on the network (a validator chosen to propose the next block) requests the most profitable block header from the relay, signs it, and adds it to the blockchain. Only after the block is finalized are the transaction contents revealed to the public.
Key infrastructure like Flashbots' MEV-Boost software facilitates this auction between builders and proposers, with numerous providers like Beaver Builder and Blocknative operating as competitive builders.

- **Trusted Execution Environments ("TEEs"):** A TEE is a secure and isolated hardware chip (such as Intel SGX or AMD SEV) that guarantees the code and data loaded inside are protected from the host system, including its owner. The security model is based on a process called "remote attestation," where a user can cryptographically verify that they are communicating with an authentic TEE running specific, unaltered code. This provides trust that the encrypted transaction sent to the TEE will only be decrypted and processed according to the protocol's public rules. The primary risk of this model is its reliance on a centralized hardware manufacturer. Any hardware-level vulnerability, side-channel attack, or supply-chain compromise could break the entire security guarantee for all protocols relying on that TEE. Examples include the Oasis Network and the Secret Network.

- **Zero-Knowledge Proofs ("ZKPs") via Shielded Pools & Layer 2's ("L2s"):** ZKPs are a purely cryptographic method for privacy, allowing a user to prove a statement is true without revealing the underlying data. This is achieved by creating "shielded pools" where assets are held in an encrypted state. The core mechanism preventing double-spending of these private assets is the "nullifier hash." When a user spends a private asset, they reveal a unique, one-time-use serial number (the nullifier) derived from their secret key and the asset. The protocol checks that this nullifier has not been used before, ensuring the asset cannot be spent again, all without linking the spend to the user's deposit history. The two primary types of proofs are ZK-SNARKs, which are efficient but often require a complex and sensitive "trusted setup" ceremony to generate initial parameters, and ZK-STARKs, which are larger and less efficient but require no trusted setup, making them more transparent. Projects like Aztec and Penumbra utilize these techniques to build private execution environments.

III. The Case for Private Execution: Mitigating On-Chain Risks

While private execution layers cannot prevent market wide crashes due to all manipulative practices, they can neutralize targeted, predatory strategies that rely on public data. In the Wynn case, if the liquidation price of his BTC long position was hidden, it could not have served as a focal point for a speculative attack. These systems are a direct defense against malicious MEV, which is rampant on open ledgers. Key risks that could be mitigated include front-running, sandwich attacks, and forced liquidation cascades. Beyond risk mitigation for individual users, the availability of execution privacy is a critical factor for encouraging institutional adoption. Professional trading firms and institutions are hesitant to deploy complex strategies on public blockchains where their every move can be seen, copied, or countered. Dark pools offer a more familiar environment that provides the execution privacy they require to operate effectively.

IV. Broader Ecosystem Impacts & Trade-Offs

The rise of private execution layers, while beneficial for individual users, introduces profound systemic risks and trade-offs. The most critical trade-off is the "Risk of Centralization." The PBS model, while effective, encourages centralization around a small number of sophisticated block builders. This dominance is driven by the "latency game"—the need for sophisticated, co-located hardware and low-latency network connections to receive transaction data, build blocks, and win auctions faster than competitors. This creates a high barrier to entry and a winner-take-all market dynamic. A significant second-order risk is vertical integration, where large staking operators or centralized exchanges run their own exclusive, in-house builders. This would further concentrate power over transaction inclusion and censorship, directly threatening the underlying blockchain network's neutrality and decentralization ethos, a concern often voiced by figures like Ethereum's co-founder, Vitalik Buterin.

This centralization can lead to the creation of a two-tier market. Sophisticated players with access to dominant builders receive superior execution and privacy, while retail users are left on the public mempool—now a less liquid and higher-risk environment. MEV does not disappear; it simply evolves and becomes concentrated. The value once captured by thousands of public bots is now concentrated in the hands of a few builders, which can lead to complex, opaque off-chain agreements that further entrench their power.

V. A Cross-Chain Perspective: MEV and Privacy Beyond Ethereum

EVM-Compatible Layer 2s (L2s): A Temporary Reprieve

For most Ethereum Virtual Machine ("**EVM**") compatible Layer 2 networks, such as Arbitrum and Optimism, concern of predatory public MEV is mitigated given the role of a "sequencer". The sequencer is a single party responsible for L2 block building – receiving all transactions, ordering them, constructing and executing L2 blocks and posting them to the underlying Layer 1 chain. In this model, there is no public mempool for predatory bots to monitor. The sequencer itself functions as an execution environment—effectively a "default dark pool."

However, this protection comes at the cost of a significant trade-off: centralized censorship risk. The single sequencer has the unilateral power to reorder, delay, or even censor user transactions. This centralized model is widely considered a temporary, transitional phase. As these networks progress toward sequencer decentralization to minimize their trust assumptions, they will inevitably replicate the open, competitive, and adversarial

environment of Ethereum. At that point, they will face the exact same MEV problems and will almost certainly need to implement their own PBS-like systems and private order flow solutions.

High-Throughput Non-EVM Chains: A Different Arena, The Same Game

High-performance chains with different architectures, such as Solana, do not have a traditional mempool but are still intensely affected by MEV. On Solana, transactions are streamed directly to the current block producer (the "leader"). The competition to have transactions included at the precise moment of an arbitrage or liquidation opportunity often devolves into network spam, where bots flood the leader with transactions.

The market responded to this chaos with a solution analogous to Flashbots that mainly operates on Ethereum. Jito Labs created a system that allows traders to send transaction "bundles" directly to validators through a private channel. This enables validators to run an off-chain auction to capture MEV in an orderly fashion and share the revenue, all while reducing network spam.

This demonstrates that regardless of the specific on-chain architecture, any sufficiently valuable and decentralized network creates financial incentives for value extraction. In response, the market organically develops dark pool-like systems (private order flow) to mitigate the negative externalities of a transparent and adversarial transaction environment.

VI. Emerging Concepts and Future Directions

The market is already evolving toward more advanced solutions. A notable paradigm shift is the move toward intent-based architectures. In these systems, users declare their desired outcome (e.g., "I want to swap 1 ETH for at least 3,500 USDC") rather than crafting a specific transaction. A competitive network of third-party "solver" then determines the best way to fulfill this intent, often using private liquidity and dark pool mechanisms to achieve optimal execution without being front-run. Foundational protocols in this space include Anoma and SUAVE, a project by Flashbots aimed at creating a decentralized network for expressing and settling intents.

VII. Legal and Regulatory Challenges

The deployment of dark pool-like functionality in crypto raises complex and overlapping regulatory issues across four key dimensions:

- **Securities Law Considerations:**
    - **Exchange Classification:** A central regulatory question is whether the components of a dark pool system that deals in securities could be deemed an unregistered exchange under Section 3(a)(1) of the Securities Exchange Act of 1934, as amended ("**Exchange Act**").[5] Rule 3b-16 under the Exchange Act further defines terms used in the statutory definition of "exchange" to include any organization, association, or group of persons that: "(1) brings together the orders for securities of multiple buyers and sellers; and (2) uses established, non-discretionary methods (whether by providing a trading facility or by setting rules) under which such orders interact with each other, and the buyers and sellers entering such orders agree to the terms of a trade."[6]

[5] Securities Exchange Act of 1934 § 3(a)(1), 15 U.S.C. § 78c(a)(1) (2025).
[6] 17 CFR § 240.3b-16.

- Applying the Exchange Act's framework, which defines an exchange as a system that "brings together" purchasers and sellers of securities using "established, non-discretionary methods," to a PBS model reveals significant legal ambiguity. This applies in the context of digital assets that are considered securities, as defined by Section 3(a)(10) of the Exchange Act. An argument can be made that a block builder "brings together" orders by assembling them into a block. Similarly, a relay could be seen as bringing together builders and proposers. The underlying smart contracts of the protocol itself arguably enable this by providing established and non-discretionary methods. In this analysis, block builders and relays, as active intermediaries, face the risk of being classified as unregistered exchanges, particularly if they are operated as centralized, for-profit services.
- Prior to June 2025, this risk was heightened by the SEC's proposed amendments to Rule 3b-16, which would have expanded the "exchange" definition to include certain communication protocols and decentralized systems. However, the Securities and Exchange Commission ("**SEC**") ultimately withdrew the proposed amendment, narrowing the immediate regulatory threat to PBS-style architectures.[7] Earlier in the year, the SEC also closed, with no action, its multi-year investigation claiming that Uniswap Labs operated an unregistered securities exchange.[8]

  - **Regulation ATS:** In traditional finance, dark pools generally must comply with Regulation ATS, which imposes significant obligations, including the public filing of Form ATS-N detailing their operations and the establishment of fair access standards. A decentralized, permissionless system would find such compliance nearly impossible, as there is often no single "operator" to take on these responsibilities, and the concept of "fair access" is at odds with a system where access is determined by code rather than a centralized administrator.
  - **Broker-Dealer Status:** Traditionally, a broker-dealer is a person or entity engaged in the business of buying and selling securities either for its own account (dealer) or on behalf of customers (broker). In the DeFi context—particularly with respect to dark pools and intent-based execution models—regulatory concerns arise over whether certain participants may be operating as unregistered broker-dealers. For example, a "solver" in an intent-based system who sources liquidity and receives a portion of the spread could be viewed as receiving "transaction-based compensation," a key indicator of broker activity. Likewise, a builder that provides a dedicated RPC endpoint to users could be construed as acting as an agent on their behalf, further increasing its regulatory risk profile.

- **Anti-Money Laundering ("AML") and KYC Risks:**
  - **Privacy-Enhancing Tech Scrutiny:** In August 2022, the Office of Foreign Asset Control ("**OFAC**") designated Tornado Cash, a decentralized cryptocurrency mixer protocol, as a Specially Designated National ("**SDN**"). [9] After nearly three years of litigation and public debate, however, OFAC removed

[7] Withdrawal of Proposed Regulatory Actions, 90 Fed. Reg. 25531 (June 17, 2025).
[8] Uniswap Labs, A Win for DeFi — SEC Closes Investigation into Uniswap Labs, Uniswap Blog (Feb. 25, 2025), https://blog.uniswap.org/a-win-for-defi.
[9] Deep Dive Into Tornado Cash: The Nuances of Immutability and Its Legal Implications, Crypto Under the Hood, Cahill

those blockchain based addresses associated with Tornado Cash from the SDN list in March 2025, citing "novel legal and policy issues raised by use of financial sanctions against financial and commercial activity occurring within evolving technology and legal environments."[10] This action followed a Fifth Circuit ruling that the designation exceeded statutory authority as the immutable smart contracts at issue were not "property" under the International Emergency Economic Powers Act ("**IEEPA**").[11] OFAC, however, retained sanctions against developer Roman Semenov, and the Department of Justice ("**DOJ**") continues to pursue criminal charges against the protocol's founders. Thus, while the delisting reduces immediate sanctions exposure and may signal a more nuanced regulatory approach to decentralized protocols, the broader risk remains —arising not only from illicit use but also from the failure to implement effective compliance controls. Developers or operators of privacy-focused protocols using TEEs or ZKPs may consider implementing measures to show that the protocol includes effective compliance safeguards, even if decentralized. The fundamental tension between privacy, decentralization, and regulatory compliance remains yet to be resolved, and developers and operators of privacy-focused protocols must navigate this complex landscape carefully.

    - **Travel Rule Concerns:** The Financial Action Task Force's ("**FATF's**") Travel Rule, or Recommendation 16, mandates that virtual asset service providers must share information about the originator and beneficiary of certain virtual asset transfers, in order to combat money laundering and terrorist financing.[12] As a result, by requiring the transmission of originator and beneficiary information, the Travel Rule becomes fundamentally incompatible with the technical design of most privacy-preserving protocols.

    - **On/Off Ramp Compliance:** Even if privacy is maintained on-chain, exchanges and liquidity providers interfacing with dark pools will likely need robust KYC procedures to avoid facilitating illicit flows.

- **Fairness, Transparency, and Market Integrity:**

    - **Transparency vs. Exploitability:** This represents a core policy dilemma. While open mempools enable MEV and counter-trading, complete opaqueness risks undermining the public auditability and equal access that are foundational to blockchain systems. Other markets, however, have adapted to mitigate similar challenges. In the advent of modern foreign exchange ("**FX**") markets, for instance, a related practice known as "pre-hedging" emerged, in which a dealer takes offsetting positions in advance of

---

Gordon & Reindel LLP (Jan. 30, 2025), https://www.cahill.com/publications/crypto-under-the-hood/2025-01-30-deep-dive-into-tornado-cash.

[10] U.S. Department of the Treasury, "Cyber-related Designation Removal; North Korea Designation Update and Removal," March 21, 2025.

[11] See Office of Foreign Assets Control, Tornado Cash Delisting, U.S. Dep't of the Treasury, Mar. 21, 2025; Steven A. Levy, Van Loon v. Department of the Treasury – A Decision with Important Implications for Bitcoin,Yale J. on Regulation: Notice & Comment (Dec. 15, 2024), https://www.yalejreg.com/nc/van-loon-v-department-of-the-treasury-a-decision-with-important-implications-for-bitcoin-by-steven-a-levy/; see also Van Loon v. Dep't ofthe Treasury, No. 23-50669 (5th Cir. 2024) (holding Tornado Cash's immutable smart contracts not "property" under IEEPA).

[12] Fin. Action Task Force, The FATF Recommendations (Feb. 2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

executing a client's order to manage market risk. While this can serve a legitimate function, the FX Global Code now makes clear that pre-hedging is only appropriate when it is transparent, does not distort price discovery, and is aligned with the client's interests.[13]

- **Insider Trading and Preferential Access:** Regulators like the SEC and Commodities Futures Trading Commission ("**CFTC**") may raise concerns that dark pool protocols enable preferential treatment or insider strategies. A private order flow system could theoretically allow a builder or relay to give certain clients preferential treatment, front-run other users within their own private system, or selectively share order information.
- **Verifiable Fairness:** A major technical and compliance challenge is proving that trades are executed fairly without revealing them. This requires novel cryptographic solutions, such as commit-reveal schemes or threshold encryption, to provide verifiable assurances of fair ordering and execution without compromising user privacy.

- **Jurisdiction and Enforcement Complexity:**
  - **Decentralization and Liability:** Many dark pool implementations are decentralized to various degrees, creating significant ambiguity for regulators trying to assign accountability. Key questions arise: Who is the operator of the platform? Is it the developers who wrote the code, the token holders who govern a Decentralized Autonomous Organization ("**DAO**"), or the blockchain network participants that act as builders and relays?
  - **Factors for U.S. Jurisdiction:** Regulators could look at a variety of factors to assert jurisdiction over a nominally "decentralized" entity. These might include the location of the parties that are deemed to have control over the protocol, the location of key decision makers or developers or core team members, the physical location of servers for critical infrastructure (like a dominant builder or relay), the targeting of U.S. users through marketing, or the presence of a U.S.-based entity or foundation associated with the protocol.

VIII. Conclusion

Crypto dark pools and private execution layers should not be viewed as tools for illicit secrecy, but rather as a necessary response to the systemic exploitation enabled by radical transparency. Cases like Wynn's demonstrate that in a financial context, absolute transparency is not always synonymous with fairness. The emergence of similar private execution markets on other chains like Solana underscores that this transparency can be a fundamental challenge for any valuable blockchain network, not an issue unique to Ethereum. The future of DeFi will depend on responsible innovation that strikes a difficult balance between execution, privacy for users, long-term verifiability for the network, and overall market integrity. For these critical tools to mature safely, proactive and educated engagement with regulators is not just beneficial—it is essential.

[13] DeFi Faces New Test as Low-Liquidity Token Gets Manipulated, Kaiko Research (June 17, 2024), https://research.kaiko.com/insights/defi-faces-new-test-as-low-liquidity-token-gets-manipulated.

* * *

If you have any questions about the issues addressed in this publication, please reach out to the CahillNXT team at CahillNXT@cahill.com. To learn more about CahillNXT, the Digital Assets and Emerging Technology practice at Cahill Gordon & Reindel LLP, click here. For more insight on the state of crypto and blockchain see recent CahillNXT publications including: "USA Chapter of Chambers Blockchain 2025 Guide", "The One Big Beautiful (Crypto Tax) Bill", "Analysis: Reading the Tea Leaves - What Enforcement Actions Mean for the U.S. Taxation of Crypto", and "What Broker-Dealers Must Know Before Selling Bitcoin ETPs." Sign up to stay up to date on the latest Cahill publications here.