

Project Research Dossier

Miden / Technical progress, unresolved token economics

1 / Problem / Question

Does Miden's client-side privacy architecture justify further research before token economics are verifiable?

Eligibility and scope. Screened 28 September 2026. The reviewed official website, release materials and funding announcement [1,3,7] did not identify a public token raise, active ICO/TGE or competitor-launchpad commitment. This is a bounded search result, not proof of absence; reconfirm before submission. Miden already raised a \$25m seed round [3], so it is NOT pre-funding. It is a candidate only under the mission's explicit no-public-raise interpretation.

2 / Data & Evidence

Goal and delivered evidence. Miden targets private financial applications by moving execution to user devices. Official developer documentation supplies a testnet contract workflow [6]. The v0.16 update describes testnet fees, encrypted private inputs and migration requirements [1]. These are inspectable engineering signals; they do not establish production adoption or investment returns.

Team verification. The official team page names Bobbin Threadbare, Azeem Khan and Dominik Schmid [2]. Polygon's historical announcement and the protocol release history add organizational and shipped-code evidence [3,4]. Profiles establish attributed identities and claimed backgrounds, not independently verified employment or proof that every founder wrote the code.

Audit scope. OpenZeppelin's 26 August 2026 report covers specified smart-contract library files at commit 2ef8056. It reports 60 issues: 50 resolved and four partially resolved, with 11 medium findings and no high/critical findings in that scope [5]. This does not certify the VM, bridges, later commits or the whole network.

Tokenomics disclosure gap. No verified native-token sale price, full supply/allocation table, circulating supply, team/treasury vesting schedule, emissions rule or next three dated unlocks was located in the reviewed sources. FDV and circulating market cap are therefore NOT CALCULABLE, not zero. Polygon's 2025 statement anticipated roughly 10% for POL stakers [3]; that is a historical expectation, not a final allocation or vesting schedule. Testnet MIDEN is not a tradable-token valuation input. The v0.16 article says mainnet fees will be denominated in USDCx [1]; native-token value capture remains unproven.

3 / Interpretation: unlock and dilution model

Illustrative sensitivity only - NOT Miden tokenomics. Assume fixed supply $S = 1\text{bn}$, initial float $C_0 = 100\text{m}$ (10%), and hypothetical price $p_0 = \$0.10$. Initial $\text{FDV} = p_0 \times S = \100m ; circulating cap $= p_0 \times C_0 = \$10\text{m}$; ratio = 10x.

Release pattern	Day 30 float	Day 60 float	Day 90 float	Day 360 float
100m cliff at day 90	100m	100m	200m (+100%)	200m
100m / 12 monthly tranches	108.33m	116.67m	125m (+25%)	200m

Float changes are relative to C_0 . Monthly tranches are assumed every 30 days; day numbers are hypothetical, not launch dates.

Project Research Dossier

Miden / Decision, risks and primary-source trail

3 / Interpretation (continued)

At an unchanged \$10m circulating cap, price = \$10m / C: the cliff case implies \$0.05 at day 90; the linear case implies \$0.08 at day 90 and \$0.05 at day 360. These are constant-cap sensitivities, not forecasts. Unlocking releases existing supply; minting expands supply. Separately, a hypothetical 5% annual issuance rate makes 1bn become 1.157625bn in three years, reducing a non-participating holder's supply share by 13.62%. Actual emissions are unknown.

Key risks. Technical/privacy: v0.16 states validators decrypt private inputs and re-execute transactions while Miden operates the validator set [1]; privacy from other users is not privacy from validators. Execution: breaking migrations and a new toolchain create integration and recovery risks [1,6]. Governance/incentives: treasury controls, upgrade authority and token-holder rights need explicit documentation. Regulatory: privacy features alone do not establish jurisdiction-specific compliance. The last two are diligence questions, not findings of misconduct.

4 / Conclusion and rating

WATCHLIST / ECONOMICS UNRATED. Public engineering evidence merits further research, but it cannot support a token valuation today. Revisit after final allocation and vesting documents, dated unlocks, emissions authority, verified deployed addresses, upgrade controls and audit-to-deployment mapping are available. Eligibility remains conditional on a fresh public-sale/TGE check; exclude the project if a disqualifying event is found.

5 / Disclosures

No position, investment, paid promotion or current buy/sell plan, as declared by the submitter. Prepared for The Republic research quest; approval may earn 50 VP. No project compensation declared. Sources reviewed on 28 September 2026; no private team confirmation, independent code audit or on-chain deployment verification was performed.

Primary sources / clickable reference register

[1] Miden: Testnet v0.16 (live official page)

<https://www.miden.xyz/blog/testnet-v0-16>

[2] Miden: founders (live official page)

<https://www.miden.xyz/about>

[3] Polygon Labs: seed funding, 29 Apr 2025

<https://polygon.technology/blog/miden-raises-25m-from-a16z-crypto-1kx-and-hackvc-to-build-the-edge-blockchain>

[4] Miden protocol release history

<https://github.com/0xMiden/protocol/releases>

[5] OpenZeppelin: scoped audit, 26 Aug 2026

<https://www.openzeppelin.com/news/miden-smart-contracts-audit>

[6] Miden: first smart contract documentation

<https://docs.miden.xyz/builder/get-started/your-first-smart-contract>

[7] Miden: official homepage

<https://www.miden.xyz/>