

Project Research Dossier — Miden

Author: kalhintz (Aquila Vanguard) **Date:** 2026-09-27 **Status at time of writing:** pre-mainnet (testnet v0.16), pre-TGE, no public token sale found.

0. Eligibility check (pre-TGE / no public raise)

- **No public sale.** The only disclosed raise is a private \$25M seed (a16z crypto, 1kx, Hack VC) at the Polygon Labs spin-out on 2025-04-29 [1]. No token sale appears on the official blog or docs [16][19].
- **No TGE yet.** The official Kaito article (2026-01-06) places Miden in Kaito's "Pre-TGE Arena" and says rewards are "granted on TGE" [3]. The Sept 2026 v0.16 post is the "last major testnet release before mainnet", and its only fee asset is faucet "testnet MIDDEN" [2]. No official token contract has been published [2][8][16].
- **Enough to evaluate.** Open-source repos (Apache-2.0/MIT) with daily commits [8], and three published audit write-ups [12][13][14].

1. Goal

Miden is a ZK rollup ("edge blockchain") spun out of Polygon Labs [1]. Users execute and prove transactions on their own devices, and the network only verifies and settles, so account state can stay private [16]. It bridges to Ethereum via Agglayer [2][7]. The target is compliant private payments: a private-by-default USDC-backed stablecoin (USDCx) via Circle's xReserve [4], plus programmable assets with callbacks for regulated issuers [7].

2. Tokenomics

Item	Published?
Total supply, TGE price, FDV, circulating at TGE	Not published
POL-staker airdrop	"expected to airdrop around 10% of native tokens to POL stakers" [1]. Snapshot rules and lockup not published
Kaito creator rewards	"0.2% of the total token supply, fully unlocked at TGE" [3]
Team, investors, Polygon Labs, treasury, ecosystem (roughly 90% of supply)	Not published
Seed instrument (equity vs. token rights), valuation	Not published [1]
Emissions / inflation	Not published
Token utility	Not published. Mainnet fees "will be denominated in USDCx" [2], and the fee asset is fixed at genesis [5]. The 2025 roadmap had fees "in the native token" [6], so the design has moved away from gas demand for the token.

3. Unlock + dilution risk

Modelled from published figures only:

- **Day-1 float from known buckets:** at least 0.2% (Kaito [3]), up to about 10.2% if the POL airdrop is also liquid on day 1 (undisclosed) [1].
- **FDV vs. market cap:** at about 10% circulating, FDV is about 10x market cap. Every unpublished bucket is future overhang.
- **Cliffs vs. linear:** no insider schedule is published, so the first insider unlock can't be dated. That gap is itself a risk signal.

Questions to get answered, and why:

1. **Total supply and TGE circulating %?** Sets the FDV/market-cap gap.
2. **Team and investor %, cliff, linear length? Did the seed carry token rights, and at what FDV?** Sets the first overhang and insiders' cost basis.
3. **Polygon Labs allocation? Is "around 10%" final, and is it locked?** Hidden supply and zero-cost sell pressure.
4. **Emissions for validators or provers, when fees are paid in USDCx?** Dilution with no fee offset.
5. **Token utility (staking, governance, prover collateral)?** With no sink, demand is purely speculative.
6. **Issuing entity, jurisdiction, any planned public sale?** Regulatory exposure, and whether retail buys above the seed price.

4. Team verification signals

Verifiable:

- **Named co-founders:** Bobbin Threadbare, Dominik Schmid, Azeem Khan [1].
- **bobbinth ("Bobbin Threadbare"):** #1 contributor to miden-vm (1,529 commits) and protocol (476), and author of the roadmap and engineering updates [6][7][8][17].
- **Dominik1999 (Dominik Schmid):** 151 protocol commits [8][17].
- **Azeem Khan:** co-founder per his own LinkedIn [18]. Business role, no code to check.

- **Engineering depth:** 161 miden-vm contributors. In the 30 days to 2026-09-27: 122 commits (VM), 95 (protocol), 92 (node), 212 (compiler). At least 50 distinct accounts committed to VM, protocol and node in 90 days [8]. Node v0.16.0 shipped 2026-09-07 [11].
- **Audits:**
 - **OpenZeppelin, standards library** (May 18 to Jun 30, 2026): 0 critical, 0 high, 11 medium, 17 low. 50 of 60 resolved, 4 partially [12].
 - **OpenZeppelin, multisig** (Feb 2026): 2 high, both resolved [13].
 - **Trail of Bits, VM core library:** found a way for a malicious prover to "forge Falcon signatures and drain any Miden account" [14]. Matching fixes merged Mar–Apr 2026 [15].

Marketing or unverified:

- **Ex-Facebook leadership:** the "formerly worked on the blockchain team at Facebook" claim [1] is unverified. The lead founder is pseudonymous, with no primary source tying him to that record.
- **Spearbit audit:** claimed in the founder's update [7], but no public report was found.
- **Guardrails:** "would have made most identified issues un-exploitable" [7] is the team's own assessment.
- **Investors:** names come from the announcement [1]. Terms are undisclosed.

5. Key risks

- **Technical: core crypto is still changing before mainnet.**
 - The founder wrote that Poseidon2 "was found to have serious security vulnerabilities in March" [7].
 - Eidos hashing arrived in v0.33.0 (2026-09-16), and "existing Poseidon2 variants remain available" [9].
 - v0.34.0 (2026-09-26) closed decoder soundness gaps, invalidating older proofs [9].
 - SECURITY.md still says the VM "has not been audited" [10].
 - OpenZeppelin left fee-deduction and replay items partly resolved [12].
 - Every audit covers a code snapshot that has since changed.
- **Execution: repeated delays.** Mainnet was due "later this year" (Apr 2025) [1], then "mainnet alpha by the end of July" (Apr 2026) [7]. It is still on testnet in Sept 2026 [2][11], about 9 months past the first target and 2 past the second.
- **Centralization and governance.** The team will run the validator internally after mainnet [7]. Third-party Gateway runs the RPC, explorer, remote provers and AggLayer proxy [7]. No governance framework is published [6].
- **Incentives.** USDCx fees remove gas demand for the token [2][5]. USDCx depends on Circle's xReserve [4]. The roughly 10% airdrop is built-in sell pressure [1].
- **Legal and regulatory.** A private-by-default payments chain draws scrutiny, and the issuer entity and jurisdiction are unpublished.

6. Disclosure

No holdings, no position, no compensation from the project. Written as part of a rewarded Legion Republic education quest.

7. Sources

1. Polygon Labs blog, "Miden raises \$25M from a16z crypto, 1kx, and HackVC to Build the Edge Blockchain" (2025-04-29): <https://polygon.technology/blog/miden-raises-25m-from-a16z-crypto-1kx-and-hackvc-to-build-the-edge-blockchain>
2. Miden blog, "Miden Testnet v0.16: Last Stop Before Mainnet" (Sep 2026): <https://www.miden.xyz/blog/testnet-v0-16>
3. Miden (@0xMiden) official X article, "Announcing the Miden Kaito Campaign" (2026-01-06): <https://x.com/0xMiden/status/2008524030215622820>
4. Miden blog, "USDCx on Miden: Stablecoins with Privacy": <https://www.miden.xyz/blog/usdcx-on-miden-stablecoins-with-privacy>
5. Miden protocol docs, "Fees": <https://github.com/0xMiden/protocol/blob/next/docs/src/fees.md>
6. Miden roadmap (HackMD, @bobbinth): <https://hackmd.io/@bobbinth/ByhShQBEGg>
7. "Engineering update – April 2026" (HackMD, @bobbinth): https://hackmd.io/@bobbinth/rk_YT47AZx
8. Miden GitHub org and core repos (miden-vm, protocol, node, compiler; contributor and commit data via GitHub API, 2026-09-27): <https://github.com/0xMiden>
9. miden-vm CHANGELOG (v0.33.0, v0.34.0): <https://github.com/0xMiden/miden-vm/blob/next/CHANGELOG.md>
10. miden-vm SECURITY.md: <https://github.com/0xMiden/miden-vm/blob/next/SECURITY.md>
11. Miden node releases (v0.15.0 2026-06-10; v0.16.0 2026-09-07): <https://github.com/0xMiden/node/releases>
12. OpenZeppelin, "Miden Smart Contracts Audit" (2026-08-26): <https://www.openzeppelin.com/news/miden-smart-contracts-audit>
13. OpenZeppelin, "Miden Multisig Cryptography Audit" (2026-03-19): <https://www.openzeppelin.com/news/miden-multisig-cryptography-audit>
14. Trail of Bits, "Auditing in the age of (good enough) AI" (2026-09-18): <https://blog.trailofbits.com/2026/09/18/auditing-in-the-age-of-good-enough-ai/>
15. miden-vm PRs #2808 (merged 2026-03-14) and #2968 (merged 2026-04-15): <https://github.com/0xMiden/miden-vm/pull/2808>, <https://github.com/0xMiden/miden-vm/pull/2968>
16. Miden documentation: <https://docs.miden.xyz/>
17. Founder GitHub profiles: <https://github.com/bobbinth>, <https://github.com/Dominik1999>
18. Azeem Khan, LinkedIn (own profile): <https://www.linkedin.com/in/theazeemkhan>
19. Miden blog index (checked 2026-09-27): <https://www.miden.xyz/blog>
20. MegaETH, MEGA token page (used in Rejected Candidates): <https://www.megaeth.com/token>
21. Aztec blog, "The ticker is \$AZTEC" (used in Rejected Candidates): <https://aztec.network/blog/the-ticker-is-aztec>
22. Tempo developer docs (used in Rejected Candidates): <https://tempo.xyz/developers>