

Project Research Dossier: Miden

Pre-TGE ZK rollup with client-side proving · Research date: 30 Sep 2026 · Primary sources only (URLs in Sources)

Research question

Miden has private VC backing, a live testnet and a committed community allocation, but no token yet. **Is its dilution risk knowable today, and what must be published before anyone can price it?**

1. What the project builds

Miden is a zero-knowledge rollup where users execute and prove transactions on their own device (client-side STARK proving); the network verifies the proof instead of re-executing. Accounts are programmable (Rust compiled to Miden Assembly) and value moves as private “notes”. The team positions it as a private-finance (“PriFi”) stack: a self-custodial wallet, a recovery/compliance module (“Guardian”), a USDC-backed stablecoin (USDCx via Circle xReserve) and bridges (Agglayer, Epoch). Testnet v0.16 (14 Sep 2026) is described by the team as the last stop before mainnet [1][2]. **Why it matters:** privacy with compliance hooks and low fees is an unsolved problem, and Miden is one of the few STARK-VM stacks with multi-year development.

2. Tokenomics (published facts only)

Item	Status	Source
Total supply / FDV	Not published	Docs, blog, site [1][2]
Circulating at TGE	Not published	—
Team / investor allocation, vesting, cliffs	Not published	—
Emissions / inflation	Not published	—
POL stakers airdrop	“Expected” ~10% of native tokens	Polygon blog, 29 Apr 2025 [3]
Investor rights	SAFE + token warrants (2:1 equity-to-token); % undisclosed	The Block [4]
Fee token	Mainnet fees denominated in USDCx, not MIDEN	Testnet v0.16 post [2]

Reading: FDV vs. circulating cannot be computed because supply and TGE float are unpublished. Any FDV figure circulating on social media for MIDEN is not sourced from the team. A community allocation (Kaito creator campaign, reportedly 0.2%) has been referenced by aggregators but I could not verify the primary post, so it is excluded from the table.

3. Unlock & dilution risk

- **Known supply overhang:** a pre-committed ~10% to POL stakers. Snapshot and lockup terms are not officially published; if unlocked at TGE, this is a large liquid float held by an audience with no cost basis.
- **Unknown overhang:** investor warrants (seed \$25M, valuation undisclosed) and team allocation. Cliff length is the single most important missing number.
- **Value-capture gap:** with fees in USDCx, demand for MIDEN depends on staking/governance utility that has not been specified. Weak utility + early float = elevated sell-pressure risk.

4. Team verification

- **Co-founders (named in official announcement [3]):** Bobbin Threadbare, Dominik Schmid, Azeem Khan.
- **Bobbin Threadbare** (pseudonymous, verifiable track record): ZK research at Facebook/Novi (Winterfell STARK prover), led Polygon Miden since its 2021 announcement [5][6]. **Schmid / Khan:** prior roles not independently verified.
- **Funding:** \$25M seed (29 Apr 2025) led by a16z crypto, 1kx, Hack VC; plus Finality, Symbolic, P2, Delta Fund, MH Ventures [3][4]. No later round found.
- **Code:** github.com/0xmiden is highly active (pushes to miden-vm, protocol, node, compiler, wallet on 29 Sep 2026) [7].
- **Audits:** OpenZeppelin, *miden-standards* library, 18 May–30 Jun 2026: 0 critical, 0 high, 11 medium (7 resolved, 2 partial, 2 unresolved), 17 low; 50 of 60 findings resolved [8]. OpenZeppelin multisig/private-state audit (Mar 2026) [9]. Trail of Bits reviewed the VM core library and reported a high-severity underconstrained value that could enable forged signatures (fixed) [10]; no public report PDF found.

5. Key risks

- **Technical:** novel VM + client-side proving + custom cryptography; a fund-draining class bug was already found in review; some OZ mediums remain open.
- **Execution:** mainnet/TGE timelines have slipped repeatedly; no mainnet date as of v0.16. Small team.
- **Governance:** no governance or sequencer/prover decentralization design published; dependency on Polygon/Agglayer.
- **Incentives:** undefined token utility (fees in USDCx); undisclosed warrant terms; large pre-committed community float.
- **Regulatory:** privacy-chain scrutiny (mitigated by compliance positioning); airdrop and equity-plus-warrant structures carry securities-law exposure.

6. Conclusion

Miden scores well on verifiable signals (named lead with a real ZK track record, tier-1 seed, very active code, multiple published audits). It scores poorly on tokenomics transparency: supply, float, vesting and utility are all unpublished, so dilution risk is **not priceable yet**. **What would change my view:** a published allocation table with cliffs of 12+ months for team/investors, POL airdrop lockup terms, and a concrete MIDEN utility beyond fees. Until then, treat any pre-market valuation as speculation.

Disclosure

No MIDEN position exists (no token issued). No POL holdings. No relationship with, or compensation from, Miden or its investors. Not investment advice.

Sources (accessed 30 Sep 2026)

[1] docs.miden.xyz [2] miden.xyz/blog/testnet-v0-16 [3] polygon.technology/blog/miden-raises-25m-from-a16z-crypto-1kx-and-hackvc-to-build-the-edge-blockchain [4] theblock.co/post/352342/polygon-miden-funding-blockchain [5] app.devcon.org/speakers/bobbin-threadbare [6] polygon.technology/blog/polygon-unveils-miden-an-advanced-zk-starks-based-scaling-solution [7] github.com/0xMiden [8] openzeppelin.com/news/miden-smart-contracts-audit [9] openzeppelin.com/news/miden-multisig-cryptography-audit [10] blog.trailofbits.com/2026/09/18/auditing-in-the-age-of-good-enough-ai/