

Project Research Dossier

FHENIX / CONFIDENTIAL COMPUTATION

Prepared for kimchi_swap | Sources accessed 2026-10-01 KST

Research question

Can Fhenix make confidential EVM applications practical, and what must be verified before its technology can support an investment thesis? This dossier separates the currently documented product from promotional claims and undisclosed token economics.

Product and evidence

The official site describes a shift from an FHE Layer 2 to confidential DeFi infrastructure. CoFHE moves encrypted computation offchain while Solidity contracts use ciphertext handles. Client-side encryption, input proofs, access controls and controlled decryption are documented components. The homepage lists Ethereum, Arbitrum and Base Sepolia testnets and says mainnet is forthcoming [1,2]. These are project disclosures, not an independently executed deployment test.

Material finding: clarify the decryption trust model

The homepage says the coprocessor operates without trusted hardware [1]. The detailed documentation instead describes Teecryptor running in an Intel TDX trusted execution environment. It verifies access permissions and ciphertext commitments, then decrypts within the enclave. A 3-of-6 key-share arrangement reconstructs the key inside that enclave; it is not the same as a live multiparty decryption network [3].

Interpretation and technical risk

FHE computation over ciphertext and TEE-based authorized decryption are different stages. The sources may describe different versions or scopes; this is a documentation inconsistency to resolve, not evidence of an exploit. The documented runtime concentrates the reconstructed key in one attested machine. Review hardware/attestation assumptions, approved image control, custodian independence, access-control correctness and service availability. The docs describe threshold multiparty decryption as a future replacement, not a completed safeguard [3].

Team and delivery verification

The site identifies Guy Zyskind as founder, Guy Itzhaki as CEO and Ravital Solomon as head of research, and links developer tools and documentation [1]. Named people and inspectable technical materials are useful verification leads. Their biographies, current production deployments, audit scope, deployed versions and commercial adoption were not independently validated in this review. Neither funding nor a named team proves execution or safety.

Tokenomics and eligibility: unresolved

The official pages reviewed do not provide an investable token price, circulating supply, diluted supply denominator, allocation table, vesting calendar, emissions policy or tokenholder rights. FDV, circulating market cap and project-specific unlock amounts therefore remain unquantifiable. Private financing mentioned on the homepage is not evidence of a public token sale [1]. No public raise or active TGE was identified on these reviewed pages; that limited search does not establish their absence. The official blog index was also checked; no Fhenix public-sale or TGE announcement was identified. This is a bounded eligibility finding as of 1 October 2026, not proof of absence [4].

Dilution model: explicitly hypothetical

Let C be current circulating supply and U an additional unlock. Supply growth is U/C . If $C=10$ million and $U=5$ million, tradable supply grows 50%. At an assumed unchanged \$1 price, circulating market cap rises from \$10 million to \$15 million; with an assumed 100 million diluted denominator, FDV is \$100 million. These numbers are teaching assumptions, not Fhenix data or a price forecast. Selling pressure depends on recipients, demand, liquidity and market behavior. A real model needs dated unlocks, recipient categories, transfer restrictions and emissions.

Decision criteria and conclusion

The useful research lead is confidential application infrastructure with a concrete documented workflow. A token valuation is not supported by the reviewed evidence. Before upgrading that conclusion, obtain official token terms and sale status; reconcile the homepage with the current Teecryptor architecture; verify relevant audits against deployed code; and request production performance, availability and adoption measurements. Research benchmark speed should not be presented as end-to-end application performance.

Proposed discussion question

Which deployed network and software version currently use Teecryptor, and what evidence demonstrates its approved image policy and custodian independence? Separately, when will allocation and unlock schedules be published? Those answers would make this analysis project-specific rather than a generic dilution framework.

Disclosures

The submitter, kimchi_swap, confirms no Fhenix holdings, investment rights, testnet or airdrop participation, or project compensation. Prepared with Codex for a Republic quest; quest rewards may apply. No independent code audit or production deployment test was performed. This document does not claim teammate review or verifier approval.

Primary sources

1. Fhenix official website and FAQ: <https://www.fhenix.io/>
2. What is CoFHE?: <https://cofhe-docs.fhenix.zone/get-started/introduction/what-is-cofhe>
3. Teecryptor: <https://cofhe-docs.fhenix.zone/deep-dive/cofhe-components/teecryptor>
4. Official blog index: <https://www.fhenix.io/blog>