

Project Research Dossier

FHENIX / CoFHE | Encrypted computation, unresolved token economics

1. Scope and eligibility

Research cutoff: 30 September 2026. Candidate: Fhenix / CoFHE. No official public fundraising offer, active ICO, completed TGE, or native-token launch terms were identified in the reviewed official site, documentation, blog and contract repository. This is a bounded search finding, not proof of absence; a future token is not guaranteed. Recheck official announcements before submission. Disclosed VC funding is distinct from a public token raise. [1-4,7]

2. What it builds and why it matters

CoFHE adds encrypted computation to applications on existing EVM chains: clients encrypt inputs, contracts manipulate ciphertext handles, and an offchain service performs FHE operations. This can protect financial amounts while preserving programmable application logic. The thesis is useful privacy without requiring every application to migrate to a separate chain. [2]

Evidence of a buildable product includes a public Solidity library and SDK documentation listing Ethereum, Arbitrum and Base Sepolia. These are test networks, not evidence of production adoption or sustainable revenue. Research on decryption performance is also not a production service benchmark. [3-5]

3. Tokenomics: disclosed facts versus missing inputs

Native-token price, maximum supply, initial circulating supply, team/investor/community allocations, vesting, cliffs, emissions, mint authority and tokenholder rights were not located in the reviewed primary materials. Therefore actual FDV, circulating market cap and dated unlock amounts are not estimable here. Unknown is not zero. Demo assets and confidential-token standards are not evidence of a Fhenix investment token. [1-4,7-8]

At price P , $FDV = P \times \text{fully diluted supply}$; circulating market cap = $P \times \text{circulating supply}$. A private financing amount is neither of these. Before assigning value, require official allocations summing to 100%, enforceable vesting contracts, treasury release rules, mint controls and a clear link between product usage and token value.

4. Unlock and dilution sensitivity - assumptions only

Illustrative model, NOT Fhenix tokenomics: normalize fixed supply to 100 units; 10 circulate initially, 20 are released in the first year, and 70 remain locked through month 12. No additional emissions or burns. Assume every released unit joins circulating supply. Compare the same 20-unit allocation under linear release versus a month-12 cliff.

Time after hypothetical TGE	Linear: circulating	Cliff: circulating
At launch	10 units	10 units
Month 6	20 units	10 units
Month 12, before cliff	30 units (limit)	10 units
Month 12, after cliff	30 units	30 units

For $0 \leq t \leq 12$ months, $C_{\text{linear}}(t) = 10 + 20t/12$. $C_{\text{cliff}}(t) = 10$ before month 12 and 30 from month 12. Both imply +200% circulating supply over the first year; the cliff concentrates the increase at one instant. At launch $FDV/\text{circulating cap} = 10x$; at month 12 it is $3.33x$. If circulating market cap stayed constant, the price would fall to one-third of its initial level (-66.7%). This is arithmetic sensitivity, not a price forecast: demand, liquidity, actual sales and circulation definitions can change the outcome.

Evidence, risks and decision

5. Team and implementation verification

The official team page names Guy Zyskind as founder and Guy Itzhaki as CEO; these roles are project statements. The original research paper names Zyskind, Doron Zarchy, Max Leibovich and Chris Peikert with affiliations, providing an attributable technical contribution. The public contract repository is inspectable but warns that interfaces change frequently. None of this verifies every biography, company finances, or deployed bytecode. [1,4,5]

6. Key risks and what would resolve them

Technical / trust: the overview FAQ rejects TEE dependence, while current architecture documentation explicitly describes Teecryptor decrypting inside a hardware-attested enclave. This is a material documentation conflict. For diligence, assume the documented TEE dependency until deployment-specific evidence resolves it; request attestation, key-share custody and signer-control details. FHE computation privacy does not remove decryption-system trust. [2,7]

Privacy / application design: the dual-mode design leaves sender, receiver and timing visible. Access-control mistakes can expose values: allowPublic permits anyone to request decryption, and a valid signed plaintext can subsequently be published. Require a threat model and tests for metadata leakage and unintended disclosure. [6,8]

Execution / security: the SDK documents breaking version changes. Require version-pinned releases, mainnet addresses mapped to audited commits, audit findings and remediation, plus measured end-to-end latency and uptime. This review did not establish an audit-to-deployment match; it does not claim that no audits exist. [3,4]

Governance / incentives: token allocation, treasury release powers and value capture remain unresolved. Map upgrade, pause, mint and signer powers to controllers and timelocks. Product adoption could benefit the company without creating tokenholder returns. Legal / regulatory: confidentiality does not establish compliance; assess any future offer and application by jurisdiction and actual terms, with selective disclosure where needed. These are diligence questions, not findings of illegality.

7. Decision and disclosure

Decision: a technical research watchlist candidate, with insufficient evidence for a token valuation. Reassess after verified launch status, complete token schedules, deployment-linked audits and a reconciled trust model. A large early unlock or privileged control without safeguards would weaken the case even if the product works.

Disclosure: I hold no position or investment rights in Fhenix, have not participated in its testnet or airdrop activities, and have received no compensation or incentives from Fhenix. This research was prepared with AI assistance for a Republic quest; quest-related rewards may apply. Statements above reflect the submitter's confirmed disclosure.

Primary-source register - links checked 30 September 2026

[1] Project / team / funding | www.fhenix.io

[2] CoFHE architecture | cofhe-docs.fhenix.zone

[3] Versions and networks | cofhe-docs.fhenix.zone

[4] Public contract library | github.com

[5] Original cryptography paper | eprint.iacr.org

[6] Access-control semantics | cofhe-docs.fhenix.zone

[7] Project overview / trust roadmap | www.fhenix.io

[8] Dual-mode privacy boundaries | www.fhenix.io