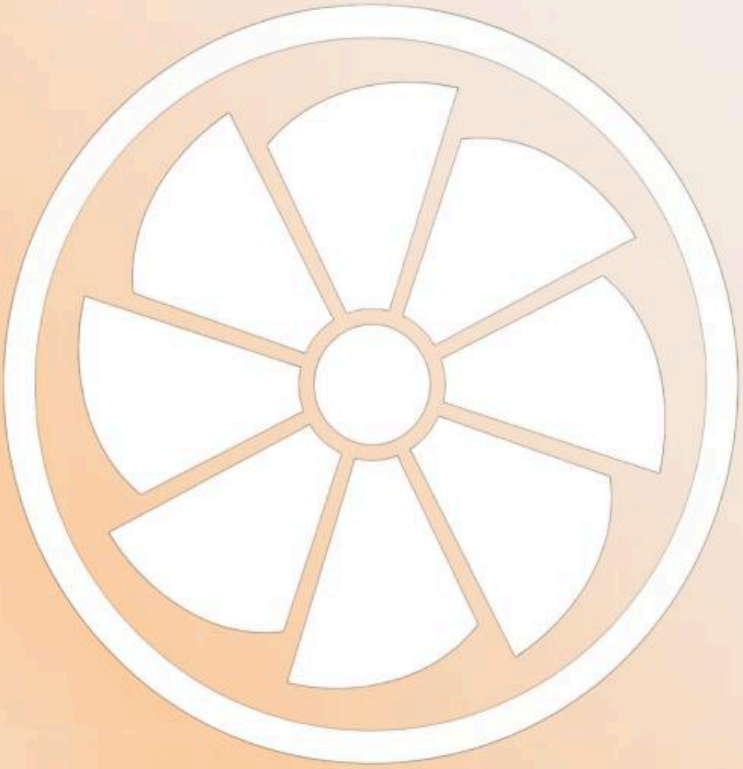
New Filing:

Turbine

powered by

Blockworks



B1

ICO **Token Transparency Filing**

Table Of Contents

Total Score: 40/40

Project & Team

1. Description of Project

Instructions: Provide a concise narrative that clearly states:

- (a) **Problem the project solves** — the problem the project is solving,
- (b) **Operational priorities** — Provide a high-level description of how the project expects to support ongoing development and operations over time,
- (c) **High-level project overview** — how the project works at a high level,
- (d) **Primary token functions** — the primary functions of the token (e.g. gov participation),
- (e) **Control surface reliance** — if any, briefly describe the anticipated or possible evolution of the protocol's governance/control model.

Score: 5/5

Answer:

(a) **Problem the project solves**

- On-chain transparency — one of blockchain's core strengths — is simultaneously its greatest privacy liability. Every wallet, transfer, swap, and DCA strategy is permanently visible on the public ledger, creating a suite of real-world risks:
- **Identity Exposure** — High-profile individuals, institutions, and everyday users have no native mechanism to transact without linking activity to a known wallet. Once a wallet is associated with an identity, every past and future transaction becomes traceable.
- **Trade Surveillance & Copy-Trading** — Monitored wallets are routinely exploited by adversaries who replicate or front-run trades in real time, directly eroding the trader's alpha and profitability.
- Today, there is no unified, yield-preserving privacy layer on Solana that addresses these interconnected problems. Users are left choosing between financial privacy and capital efficiency — a trade-off that shouldn't exist.

(b) **Operational priorities** — Provide a high-level description of how the project expects to support ongoing development and operations over time

- **Operational Priorities**
  - The core team operates with a high-velocity, product-first development philosophy. In under three months since inception, the team has delivered all originally planned protocol components to production — private transfers, swaps, LST, and DCA — alongside multiple additional products that emerged from user feedback and market opportunity.

- **Development Cadence**
    - The team maintains a rapid ship-iterate-improve cycle, prioritizing production-grade releases over prolonged development phases. This velocity is enabled by deep domain expertise in zero-knowledge cryptography, Solana smart contract development, and distributed systems — allowing the team to move from concept to deployment with minimal overhead.
- **Ongoing Operational Focus**
    - **Protocol Hardening** — Continuous security audits, circuit reviews, and stress testing to ensure the privacy layer remains robust as usage scales and adversarial sophistication increases.
    - **Product Expansion** — Identifying and developing new privacy-preserving primitives that address unmet needs within the Solana DeFi ecosystem, guided by on-chain usage data and community feedback.
    - **Integration & Ecosystem Growth** — Building composability with existing Solana protocols, wallets, and aggregators to reduce friction for end users and expand the protocol's addressable market.
    - **Infrastructure Scalability** — Ensuring relayer infrastructure, proof generation pipelines, and backend systems scale reliably with growing transaction volume and user adoption.
- **Sustainability** — Ongoing development is funded through the DAO treasury and protocol fee revenue. As adoption grows, the self-reinforcing relationship between usage, fee generation, and treasury capitalization is expected to provide a sustainable funding model for long-term operations without reliance on external capital raises.
- **Team Commitment** — The founding team is deeply mission-aligned, with the conviction that on-chain privacy is not a niche feature but a fundamental infrastructure requirement for mainstream DeFi adoption.

(c) **High-level project overview**

- We offer a comprehensive suite of privacy-preserving tools designed to protect on-chain activity:
- **Private Transfers** — Generate fresh wallets with no traceable link to your identity. Ideal for high-profile individuals and institutions seeking to transact without exposing their on-chain footprint.
- **Private Swaps** — Execute trades without leaking intent. Prevent copy-trading and front-running by adversaries monitoring your wallet activity.
- **Private LST (Liquid Staking Tokens)** — Solve the fundamental mixer paradox: longer pool residency improves privacy, but at the cost of foregone yield. By depositing LSTs, users continue earning staking rewards while maintaining privacy.
- **Private DCA (Dollar-Cost Averaging)** — The first privacy-preserving DCA implementation. On-chain DCA strategies are typically high-visibility transactions

that telegraph your accumulation plan. Keep your strategy confidential and eliminate front-running risk.

(d) **Primary token functions**

- **Primary Token Functions**
    - The governance token serves as the foundational ownership and control instrument of the protocol, operating within MetaDAO's futarchy-based governance framework. Its primary functions are:
- **Governance Participation**
    - The token enables holders to participate in protocol decision-making through MetaDAO's market-driven proposal system. Rather than traditional stake-weighted voting, holders trade on proposal outcomes using the governance token or USDC, ensuring that governance influence is aligned with informed conviction about what creates long-term protocol value.
- **Intellectual Property Ownership**
    - The token represents collective ownership over all protocol IP, including smart contracts, zero-knowledge circuits, SDKs, branding, and proprietary research. No individual or entity holds IP rights independent of the DAO.
- **Treasury Control**
    - Token holders govern the protocol treasury, which accumulates all protocol-generated fee revenue. Through governance proposals, holders direct treasury allocation toward development, audits, partnerships, ecosystem growth, and any future distribution mechanisms.
- **Fee Accrual**
    - All fees generated across the protocol's privacy services — transfers, swaps, LST, and DCA — flow into the token-controlled treasury, creating a direct link between protocol usage and the value governed by token holders.
- **Summary**
    - The token is not merely a governance vote — it represents comprehensive ownership of the protocol's economic output, intellectual property, and strategic direction. Its value is fundamentally tied to protocol adoption, fee generation, and the quality of governance decisions made through the futarchy mechanism.

(e) **Control surface reliance**

- The protocol currently operates under a managed governance model with a clear roadmap toward progressive decentralization.
    - **Current State** — High-impact decisions are governed through MetaDAO proposals, ensuring transparency and community input on critical protocol parameters such as fee structures, pool configurations, and upgrade

paths. Day-to-day operations and development remain with the core team to maintain agility during the protocol's early growth phase.
    - **Progressive Decentralization** — As the protocol matures and demonstrates stability across its core primitives (private transfers, swaps, LST, and DCA), we intend to systematically reduce core team reliance by:
    - Expanding the scope and frequency of on-chain governance proposals as TVL and fee revenue grow, giving stakeholders greater authority over protocol direction.
    - Transitioning operational responsibilities — such as parameter tuning, fee adjustments, and pool management — to community-governed mechanisms.
    - Open-sourcing key protocol components as they reach production-grade maturity, enabling independent verification and community-driven development.
- **Philosophy** — We believe premature decentralization introduces unnecessary risk to users and protocol integrity. Our approach is to decentralize deliberately — component by component — once each surface area has been battle-tested and the community has developed sufficient context to govern it effectively. The end goal is a protocol where the core team is no longer a critical dependency for continued operation.

2. Known Project Team & Investors

Instructions: For each existing entity: Labs/DevCo (e.g., Founder, CEO, CTO, COO), Foundation (e.g., President, Executive Director, CFO, COO), and DAO / onchain governance leadership (if applicable) list the:
    - (a) full names,
    - (b) official titles,
    - (c) and prior experience of key team members.
- For any non-existent entity, explicitly mention it does not exist. External links may be included but they will not factor into the score. Edge note: A compound role (e.g., Founder/CEO) counts as one person with a compound title.

Score: 3/3

Answer:

Labs/DevCo

Full Name	**Official Title**	**Prior Experience**
Ohad Dahan	Founder	15+ years in high tech (Apple/Synopsys/Ansys/others) Bootstrapped startups successfully in the past

Amir Cohen	Front End	10+ years in high tech, operates a Solana validator since 2021
Vadym Pasternak	Marketing Lead	Marketing lead of multiple protocols
Libi Directovich	COO	15+ years in finance

Foundation

Full Name	Official Title	Prior Experience
Ohad Dahan	Managing Member	15+ years in high tech (Apple/Synopsys/Ansys/others) Bootstrapped startups successfully in the past

DAO/Onchain Governance

Full Name	Official Title	Prior Experience
No designated governance leadership exists; governance is conducted via MetaDAO futarchy with no named leaders		

3. DAO Structure

Instructions: Provide a structured description of the DAO's governance, powers, and economic rights. If a DAO does not exist, state so. Address the lettered items below. Item (c) may be left absent if not applicable.

- (a) **IP ownership & control** — State what IP the DAO owns or controls (e.g., codebases/repos, trademarks/brands). Note any license if relevant.
- (b) **Contract/admin powers** — List on-chain or administrative authorities and limits: pause/upgrade roles (e.g., multisig pause), governance-executor authorities, and the method of authority for each (e.g., veto, majority, super-majority).
- (c) **Locked-token rights (conditional)** — If locking/staking for additional rights exists, explain the additional rights and what tokenholders can and cannot decide. If no locking mechanism exists, leave absent.

- (d) **Value accrual & holder rights** — If any, describe the current rights of tokenholders over revenue distribution and the treasury.
- (e) **Dissolution authority** — State who can dissolve/wind up the DAO and by what mechanism (e.g., on-chain vote threshold, board resolution of a legal wrapper).

Score: 5/5

Answer:

(a) IP ownership & control

- All intellectual property associated with the protocol is owned and controlled by the ZKFG token holders. This encompasses:
  - **Codebases & Repositories** — All protocol smart contracts, zero-knowledge circuits, SDK libraries, and supporting infrastructure repositories are owned by the DAO. The core team develops and maintains these assets on behalf of the DAO, with no independent IP claims retained by individual contributors or the founding entity.
  - **Brand & Trademarks** — The protocol's name, logo, visual identity, and all associated branding assets are DAO-controlled IP. Any licensing, partnership usage, or brand extensions require governance approval.
  - **Proprietary Research** — Novel cryptographic implementations, circuit designs, and protocol architecture documentation produced in the course of development are considered DAO-owned intellectual property.
  - **Licensing** — The codebase is currently maintained under a proprietary license controlled by the DAO. Future decisions regarding open-source licensing (e.g., transitioning specific components to BSL, MIT, or Apache 2.0) will be subject to governance proposals as part of the broader decentralization roadmap.
  - **Summary** — The ZKFG token represents ultimate authority over all protocol IP. No single entity, team member, or external party holds independent ownership rights over any protocol asset. This structure ensures that the community retains sovereign control over the protocol's most valuable resources as governance progressively decentralizes.

(b) **Contract/admin powers**

- **Contract & Administrative Powers**
  - The core development team currently holds administrative authority over the protocol's on-chain contracts. This is a deliberate design decision driven by operational security requirements — privacy protocols handling user funds demand rapid incident response capabilities that are incompatible with the latency of on-chain governance deliberation.
- **Current Administrative Authorities**
  - **Emergency Pause** — The core team retains the ability to pause protocol contracts in the event of a critical vulnerability, exploit attempt, or

anomalous activity. This authority is exercised unilaterally to ensure sub-minute response times when user funds are at risk.
    - **Contract Upgrades** — Program upgrades are currently authorized by the core team via a controlled upgrade authority. All upgrades undergo internal audit and testing prior to deployment. Non-emergency upgrades are communicated to the community in advance.
    - **Parameter Configuration** — Fee structures, pool parameters, and operational thresholds are configurable by the team to allow for iterative tuning as the protocol scales and market conditions evolve.
- **Rationale**
    - Emergency scenarios — such as zero-day vulnerabilities, oracle manipulation, or novel attack vectors targeting the privacy layer — require immediate action. Routing critical response decisions through governance proposals introduces unacceptable delay that could result in loss of user funds. Given the nascent and highly specialized nature of on-chain privacy systems, we believe centralized emergency authority is the responsible approach at this stage.
- **Planned Evolution**
    - As the protocol matures, we intend to progressively constrain and distribute administrative powers:
    - **Short-term** — Introduce a multisig structure for admin operations, distributing key authority across core team members and trusted community participants to eliminate single points of failure.
    - **Medium-term** — Transition non-emergency parameter changes and routine upgrades to governance-approved execution, reserving only emergency pause capability for the multisig.
    - **Long-term** — Implement timelocked upgrades with governance veto rights, and explore immutability for battle-tested contract components where the risk profile justifies removing upgrade authority entirely.

  The goal is to minimize the trust surface progressively — retaining only the administrative powers that are strictly necessary for user protection at each stage of the protocol's maturity.

(c) **Locked-token rights (conditional)**

- **Locked-Token Rights**
    - The protocol does not employ a traditional token locking or staking mechanism for governance participation. Instead, governance operates through MetaDAO's futarchy-based decision market model.
- **How It Works**
    - Rather than locking tokens to vote, participants express governance preferences by trading on proposal outcomes using the governance token or USDC. This market-driven approach aggregates collective intelligence

through price discovery — proposals that the market expects to create value are approved, while those expected to be detrimental are rejected.

- **What Token Holders Can Decide**
    - Through the proposal market mechanism, participants can influence high-impact protocol decisions including fee adjustments, protocol upgrades, treasury allocations, and strategic direction changes.
- **What Token Holders Cannot Decide**
    - As outlined in the administrative powers section, emergency operations such as contract pauses and urgent security responses remain under core team authority due to the time-sensitive nature of these actions. These decisions are not routed through the proposal market.
- **Why No Staking**
    - Futarchy-based governance aligns incentives more directly than stake-weighted voting. Participants put capital at risk based on their conviction about a proposal's outcome, meaning governance influence is tied to informed conviction rather than passive token lockup. This reduces the plutocratic dynamics common in traditional stake-to-vote models and discourages uninformed or apathetic governance participation.

(d) **Value accrual & holder rights**

- **Value Accrual & Token Holder Rights**
    - All protocol-generated revenue accrues directly to the DAO-controlled treasury. There is no value extraction by the core team independent of governance oversight.
- **Revenue Sources**
    - The protocol generates fees from its privacy-preserving services, including private transfers, swaps, LST deposits, and DCA executions. As usage scales and TVL grows, fee revenue is expected to increase proportionally.
- **Treasury Ownership**
    - The treasury is fully controlled by ZKFG governance token holders. All accumulated fees, reserves, and protocol-owned assets fall under the DAO's sovereign authority.
- **Current Token Holder Rights**
    - - Through MetaDAO's futarchy-based proposal mechanism, token holders can influence decisions regarding:
        - Treasury deployment — funding development, audits, partnerships, grants, and ecosystem growth initiatives.
        - Fee parameter adjustments — modifying fee structures across protocol services.
        - Revenue allocation strategy — directing how accumulated revenue is utilized, whether for reinvestment, reserves, or future distribution mechanisms.

- **Current Limitations** — There is no direct revenue distribution or dividend mechanism to token holders at this time. Revenue is retained within the treasury to fund ongoing protocol development, security audits, and operational sustainability during the growth phase.
- **Future Considerations** — As the protocol reaches maturity and achieves sustainable revenue generation, governance proposals may introduce direct value distribution mechanisms such as buyback programs, revenue sharing, or other token holder benefit structures. Any such changes would be subject to the standard governance process and applicable regulatory considerations.

(e) **Dissolution authority**

- **Dissolution Authority**
  - The protocol can only be dissolved through a governance proposal passed via MetaDAO's futarchy-based decision market. No individual, core team member, or external entity holds unilateral authority to wind up the DAO or its operations.
- **Mechanism**
  - A dissolution proposal would follow the same market-driven governance process as any other protocol decision. Participants would trade on the proposal outcome using the governance token or USDC, with the market determining whether dissolution is in the best interest of the protocol and its stakeholders.
- **Scope of Dissolution**
  - A successful dissolution proposal would authorize:
    - Cessation of active protocol development and operations.
    - Liquidation and distribution of treasury assets to token holders on a pro-rata basis.
    - Transfer, open-sourcing, or sunsetting of protocol IP as specified within the proposal terms.
    - Orderly wind-down of relayer infrastructure, backend services, and any remaining operational dependencies.

4. Primary Foundation and Dev Co

Instructions: For each entity — Primary Foundation and Primary DevCo — do the following independently. If an entity does not exist, state that explicitly. Items (a)–(e) apply only if that entity exists; state explicitly that the entity doesn’t exist.

- (a) **Entity** — type and jurisdiction.
- (b) **IP ownership & control** — what IP the entity owns/controls (repos/code, trademarks/brand; license optional) and an explanation of any subsidiary entities.
- (c) **Powers over DAO/treasury** — If any, describe the current powers over DAO governance/treasury and the method/threshold (veto/majority/super-majority, etc.).

- (d) **Powers over DevCo/Foundation** — explain whether the DevCo can exert direct or indirect influence over decision-making of the foundation and vice versa.
- (e) **Contract/admin powers** — pause/upgrade/governance-executor authorities and the method/threshold for each (e.g., veto/majority/super-majority; “3/5 multisig”).

Definitions: The primary Foundation and DevCo can be explained as those entities which are directly involved in the issuance of the native token at launch.

Score: 5/5

Answer:

(a) **Entity**

- Turbine Cash DAO LLC, Marshall Island.

(b) **IP ownership & control**

- **Legal Structure** — The protocol operates under a single legal entity: **Turbine Cash DAO LLC**. There is no separate development company, foundation, or subsidiary entity. This unified structure eliminates complexity and ensures clear, undivided ownership of all protocol assets.
- **Entity Obligations** — The Turbine Cash DAO LLC is legally bound by its operating agreement to operate in accordance with futarchy-based governance proposals. This is not a discretionary commitment — the entity is contractually obligated to respect and execute any proposal that passes through the MetaDAO futarchy mechanism. This creates an enforceable legal bridge between on-chain governance outcomes and real-world entity actions.
- **IP Ownership** — All intellectual property is owned by ZKFG token holders through the DAO LLC, including:
    - All protocol smart contracts, zero-knowledge circuits, and supporting codebases.
    - The Turbine Cash brand, name, logo, and associated trademarks.
    - Proprietary cryptographic research, documentation, and architectural designs.
    - Any future IP produced in the course of protocol development.

No individual contributor, team member, or external party retains independent IP rights.

- **Treasury Custody**
    - The protocol treasury is held entirely on-chain, managed and enforced by the futarchy smart contract. All treasury operations — including expenditures, allocations, and disbursements — are governed by the proposal mechanism. There is no off-chain treasury, discretionary fund, or team-controlled wallet outside of the governance-enforced structure.
- **Subsidiary Entities**

- None. The Turbine Cash DAO LLC is the sole entity associated with the protocol. There are no affiliated companies, offshore entities, or special-purpose vehicles.

(c) **Powers over DAO/treasury**

- The protocol treasury is fully controlled by the DAO through MetaDAO's futarchy-based governance mechanism. There is no individual, team, or external entity with unilateral authority over treasury funds.
    - **Treasury Custody**
        - All treasury assets are held on-chain and governed by the futarchy smart contract. There are no off-chain reserves, discretionary team wallets, or custodial arrangements outside of the governance-enforced structure. The on-chain treasury address is publicly auditable at all times.
    - **Governance Mechanism: Futarchy**
        - Treasury operations are governed through MetaDAO's decision market system rather than traditional token-weighted voting. The process works as follows:
            - **Proposal Creation** — Any token holder can create a proposal requesting treasury expenditure, allocation changes, or disbursements.
            - **Decision Market Trading** — Upon proposal submission, conditional PASS and FAIL markets open. Participants trade using the governance token (ZKFG) or USDC to express their conviction about whether the proposal will increase or decrease the token's value.
            - **Price-Based Resolution** — After a defined trading period (typically 3 days), the proposal outcome is determined by comparing the Time-Weighted Average Price (TWAP) of the PASS and FAIL tokens. If the PASS market price exceeds the FAIL market price by the defined threshold, the proposal passes. Otherwise, it fails.
            - **Automatic Execution** — Passed proposals are executed on-chain without requiring additional approval or manual intervention.
    - **Threshold Mechanism**
        - Futarchy does not use traditional majority or super-majority vote counts. Instead, the "threshold" is a price spread — proposals pass when the market collectively signals that the proposed action would create value for the token relative to the alternative (not taking the action). This mechanism aggregates economic conviction rather than counting votes, ensuring that outcomes

reflect informed market intelligence rather than passive token holder sentiment.

- **What the DAO Can Decide**
  - Through passed futarchy proposals, the DAO can authorize:
    - Treasury disbursements for development, audits, grants, partnerships, and operational expenses.
    - Creation or modification of incentive programs funded by treasury assets.
    - Allocation of protocol revenue to specific initiatives or reserves.
    - Return of treasury funds to token holders (any holder can raise such a proposal at any time).
    - Any other treasury-related action within the scope of the DAO LLC's operating agreement.
- **What the DAO Cannot Decide Unilaterally**
  - Emergency contract operations (pause, urgent upgrades) remain under core team authority due to the time-sensitive nature of security incidents, as outlined in the administrative powers section.
- **Safeguards**
  - **Capital-at-Risk Participation** — Traders must commit real capital to influence outcomes, discouraging frivolous or malicious proposals.
  - **TWAP-Based Resolution** — Time-weighted pricing prevents manipulation through sudden large-volume trades at the end of the trading period.
  - **On-Chain Enforceability** — The DAO LLC is legally obligated to respect and execute any proposal that passes through the futarchy mechanism, creating an enforceable bridge between on-chain governance outcomes and real-world treasury operations.
  - **Full Transparency** — All proposals, trading activity, and execution are publicly visible on-chain before, during, and after the governance process.

-

(d) **Powers over DevCo/Foundation**

- **Powers Over DevCo/Foundation**
- As outlined above, the protocol operates under a single legal entity — the Turbine Cash DAO LLC — with no separate foundation or development company.
- **Direct Influence** — The development team holds no special governance privileges, elevated voting weight, or veto authority within the futarchy mechanism. The DAO is the sole and final authority over all protocol decisions.

The team participates in governance on the same terms as any other token holder.

- **DAO Authority Over the Development Team** — The DAO retains full authority to direct, modify, or terminate the development team's engagement through governance proposals. This includes the ability to redirect treasury funding, onboard alternative development contributors, or restructure operational arrangements entirely.
- **Indirect Influence — Power of Exit** — The development team's primary form of indirect influence is its institutional knowledge and specialized expertise in zero-knowledge cryptography and protocol architecture. In practice, this means the team's most significant leverage is the ability to discontinue its engagement with the protocol — the "power of exit." While this would create short-term operational disruption, it does not compromise the DAO's sovereign authority. All IP, codebases, and treasury assets remain under DAO ownership regardless of the development team's involvement, ensuring the protocol can onboard new contributors and continue operations independently.
- **Mitigating Factors** — The risk of development team departure is mitigated by the DAO's outright ownership of all code and IP, the open and documented nature of the protocol architecture, and the ability of governance to allocate treasury resources toward alternative development capacity at any time.
-

(e) **Contract/admin powers**

- **Administrative Authorities**
  - **Emergency Pause**
    - Holder: Core dev team
    - Method: Unilateral
    - Rationale: Sub-minute response required to protect user funds during active exploits or critical vulnerabilities
- **Contract Upgrades**
  - Holder: Core dev team
  - Method: Unilateral (non-emergency upgrades communicated in advance)
  - Rationale: ZK circuit and smart contract upgrades require specialized expertise and rapid iteration during the protocol's growth phase
- **Parameter Configuration**
  - Holder: Core dev team
  - Method: Mixed dev team and Futarchy proposals
  - Rationale: Fee structures, pool parameters, and operational thresholds require ongoing tuning as usage patterns evolve

Token Supply & Allocations

5. Initial Allocation

Instructions: Disclose launch and initial supply details in a single initial allocation schedule covering the token's launch. Include:

- (a) **Launch supply totals** — the total number of tokens issued at launch, the total number of tokens locked at launch, and the total number of tokens unlocked at launch;
- (b) **Recipient categories & use of funds** — the recipient categories with brief explanations as to how the category will use the tokens so an auditor can distinguish each bucket;
- (c) **Initial price per token** — the expected initial price per token;
- (d) **Ticker / market symbol** — the ticker/market symbol;
- (e) **Total supply & supply regime** — the total supply and whether the supply is fixed (if not explain inflation rate or deflation rate);
- (f) **Initial vesting / release schedules** — the initial vesting/release schedules (identify which categories/recipients are subject to vesting and the high-level timing logic).

Score: 2/2

Answer:

(a) **Launch supply totals**
- Total supply is 12.9M, no locked tokens exists

(b) **Recipient categories & use of funds**
- All ZKFG tokens are functionally identical — there are no distinct token classes, tiers, or variants with differing rights or restrictions. Every token carries the same governance participation rights, IP ownership claims, and treasury control authority regardless of how or when it was acquired.

(c) **Initial price per token**
- 0.096942$/token

(d) **Ticker / market symbol**
- ZKFG - https://jup.ag/tokens/ZKFHiLAfAFMTcDAuCtjNW54VzpERvoe7PBF9mYgmeta

(e) **Total supply & supply regime**
- 12.9M fixed supply, can only mint if a proposal to raise more funds via minting is approved by the DAO.
- 100% of the supply was minted via the ICO, all held by individuals that purchased during the ICO or in the free market after the ICO.

(f) **Initial vesting / release schedules**
- No vesting, all tokens are liquid.

6. Airdrop Process

Instructions:

If the project has planned but not yet airdropped, it must:

- (a) commit to publish, in a public channel **and** provide to Blockworks **quarterly** a recipient wallet list until the initial TGE airdrop is fully completed,
- (b) Generally state the possible target user segments (e.g., “stakers of X,” “Aave users”) and the allocation method (e.g., proportional to ve-balance or net position).

If the project has already airdropped, it must:

- (a) For executed airdrops, point to an per-address source such as CSV/TSV/JSON files, a Dune table, a full Merkle dump, GitHub repo files embedding per-address allocations, or RPC endpoints that expose claim/amount data; explorer links alone don’t count.
- (b) Clearly state covered user segments (e.g., “stakers of X,” “Aave users”) and the allocation method (e.g., proportional to ve-balance or net position).

If the project does not plan to do an airdrop for TGE, it must:

- (a)If no airdrop has ever been conducted, say so plainly (“We have never conducted an airdrop to date and do not plan to execute one”).

Score: 3/3

Answer:

NONE

Transactions & Market Structures

7. Market Maker Agreements & Deals

Instructions: Projects must disclose all material terms of market-making arrangements that affect token liquidity. If the project has no agreements or deals with market makers, state that explicitly; doing so earns full credit. For each market maker, include in a table:

- (a) **Market maker’s name** — the market maker’s name;
- (b) **Token allocation or loaned amount** — the token allocation or loaned amount as a percentage of total supply;
- (c) **Duration/term of agreement** — the duration/term of the agreement; and, where applicable,

- (d) **Name of agreement structure** — label the financial vehicle being used in the agreement (i.e. loan, option/call, retainer model) without describing trading strategy or expected outcomes.

If the project has no agreements or deals with market makers, state that explicitly; doing so earns full credit. If no native tokens were loaned or allocated to market makers, state that explicitly; cash/fiat retainers or fees are not required for this item.

Score: 5/5

Answer:

No agreements or deals with third-party market makers that include a loan or allocation of ZKFG tokens have been conducted.

8. CEX / DEX Agreements & Deals

Instructions: Projects must disclose all material terms of centralized or decentralized exchange listings that affect token liquidity. For each listing, include in a table:

- (a) **Exchange name / DEX pool** — the exchange name (and, for DEX, the specific pool/pair);
- (b) **Token allocation for listing** — the token allocation supplied or committed for listing as a percentage of total supply;
- (c) **Term Duration** — the duration/term of any listing lockups, liquidity, or incentive programs; and, where applicable,
- (d) **Native-token listing fees** — whether any listing fees were paid in native tokens, with amounts (tokens or % of supply), recipients, and any vesting or lock terms tied to the partnership.

If the project has no agreements or deals with CEX or DEX, state that explicitly; doing so earns full credit. If no native-token listing fees were paid, state that explicitly; cash/fiat fee amounts are not required for this item.

Score: 5/5

Answer:

(a) Exchange Name / DEX Pool

(1) We have no deals with CEX / DEX - we only have the ZKFG/USDC AMM pool to provide liquidity.

(2) The ZKFG token trades on a ZKFG/USDC AMM **pool** on Solana and is accessible through all major Solana routing and aggregation platforms, including:

a) Jupiter
b) Titan Exchange

c) DFlow

(3) Any user can trade ZKFG by selecting their desired sell token and purchasing ZKFG through any of the above platforms using the token's mint address: **ZKFHiLAfAFMTcDAuCtjNW54VzpERvoe7PBF9mYgmeta**

(ii) Listing Terms

(1) There are no special listing agreements, market-making requirements, or exchange-specific obligations associated with the ZKFG token's availability on these platforms. The token is routable through standard Solana AMM infrastructure on a permissionless basis.

(iii) **Liquidity Provision**

(1) Initial liquidity for the ZKFG/USDC AMM pool was established as part of the token's ICO launch through MetaDAO. 20% of the USDC raised during the ICO was allocated directly to seeding the AMM liquidity pool, ensuring immediate tradability upon launch. This liquidity allocation was defined as part of the ICO terms and is not subject to separate market-making contracts or third-party liquidity provider agreements.

(b) **Token allocation for listing**

(i) No CEX listings

(c) **Term Duration**

(i) None

(d) **Native-token listing fees**

(i) None

Financial Disclosures & Risks

9. Prior Token Sales & Fundraising

- Instruction: Disclose all prior token sales by the Project — including fundraising rounds, any material OTC sales to investors, and any discounted market-maker sales. For each sale, provide:
  - (a) Series Name / Early-Stage Investment Instrument used (i.e. SAFT, STAMP, SAFE, SAFE+Token Warrant, etc.)
  - (d) Date of sale (at least month & year).
  - (d) Number of tokens sold (or % of total supply)
  - (e) Vesting schedule
- If no prior sales occurred, state that explicitly (e.g., “No prior fundraising, OTC, or discounted MM sales have occurred.”)

Score: 5/5

Answer:

[Turbine Cash (formally ZKLSOL)]

Series Name / Investment Vehicle	Date Of Sale	Number of tokens sold	Capital Committed	Capital Raised	Vesting Schedule
MetaDAO launch	10/23/2025	12.9M No external funds were raised outside of the ICO	$15M	$969,420	none

10. Previous Exploits Affecting The Project

Instructions: If any, list prior exploits/incidents that affected protocol funds. For each incident, provide:

- (a) **Date & component affected** — date (YYYY-MM or YYYY-MM-DD), chain(s)/component affected;
- (b) **Exploit vector summary** — plain-language summary of the exploit vector (what the hack was);
- (c) **Quantified impact** — quantified impact (assets/tokens affected or a clear “no loss of funds” statement);
- (d) **Remediation/response taken** — remediation/response taken (patches, upgrades, governance actions, compensation);
- (e) **Current status** — current status (resolved, in litigation, under investigation, refunded, etc.);
- (f) **References (optional)** — references (optional): link(s) to post-mortem/advisory/PR.

- If **no prior incidents**, state this explicitly (e.g., “No exploits affecting tokenholders or protocol funds as of YYYY-MM-DD”).

Score: 2/2

Answer:

No exploits as of 2026-02-05

11. Material Risk Factors (Regulation, Technology, Token Economics)

Impact of Regulatory Change on TGE and Listings:

- The Protocol and its governance token operate in an evolving and uncertain global regulatory landscape. The following regulatory changes could materially impact the Protocol or token:
    - **Token classification**
        - The governance token may be classified differently across jurisdictions. If any regulator classifies it as a security (rather than a utility or governance token), the Foundation and token holders could face registration requirements, trading restrictions, or enforcement actions. The U.S. SEC's evolving position on governance tokens, and similar regulatory developments in the EU (MiCA), Singapore (MAS), and other jurisdictions, create ongoing uncertainty.
    - **Anti-money laundering (AML) and sanctions compliance**
        - The Protocol implements OFAC sanctions screening through an Ed25519 signature-based oracle verification system on deposits.
    - **DeFi-specific regulation**
        - Proposals to regulate decentralized finance protocols (e.g., the EU's MiCA framework, proposed U.S. legislation) could impose requirements on the Foundation or DAO governance structure that are incompatible with the Protocol's current design or operational model.

Entity-Level Regulatory Impact:

- The Foundation is incorporated in the Marshall Islands. While this jurisdiction has adopted favorable digital asset legislation, it carries specific entity-level risks:
    - **OFAC**
        - The Foundation's OFAC compliance system — while implemented on-chain — relies on an external oracle to verify that depositors are not on the OFAC Specially Designated Nationals (SDN) list.
    - **External compliance tooling**
        - The Foundation intends to utilize third-party compliance tools (Range and CipherOwl) for privacy pool monitoring and analytics. Reliance on third-party services introduces vendor dependency risks: if these services discontinue support, change terms, or face their own regulatory challenges, the Protocol's compliance posture could be impacted.

Tokenholder Tax Treatment:

- Token holders should be aware that the tax treatment of governance tokens and liquid staking tokens is uncertain and varies significantly across jurisdictions. The following considerations apply:
    - **No tax advice**
        - The Foundation does not provide tax advice and makes no representations regarding the tax treatment of the governance token ZKFG or ZSOL (the Protocol's liquid staking token). Token holders are solely responsible for determining and complying with their own tax obligations.
    - **Potential taxable events**
        - Depending on the jurisdiction, the following activities may constitute taxable events: (a) receipt of governance tokens at TGE or through airdrops; (b) minting or redeeming ZSOL (which involves depositing SOL and receiving a representative token, or vice versa); (c) trading, staking, or transferring governance tokens; (d) receiving yield or rewards from staking via the Sanctum pool; (e) participation in DCA (dollar-cost averaging) operations that involve token swaps through Jupiter or Titan DEX integrations.
    - **Reporting obligations**
        - As regulatory frameworks mature, jurisdictions may impose reporting obligations on token holders, DAOs, or protocol foundations. Token holders should consult qualified tax advisors regarding their specific circumstances.

Jurisdictional & User Access Restrictions:

- The Protocol applies the following jurisdictional restrictions:
    - **OFAC sanctions compliance**
        - The Protocol implements on-chain OFAC sanctions screening for deposit transactions. This screening uses an Ed25519 signature verification oracle that checks depositors against the OFAC Specially Designated Nationals (SDN) list. Persons or entities on the SDN list, or located in OFAC-sanctioned countries (currently including Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk, and Luhansk regions of Ukraine), are restricted from depositing into the Protocol.
    - **Front-end restrictions**
        - IP based restrictions apply, no OFAC based IP is allowed to access the front end.

Bugs and Design Flaws:

- **Smart Contract Vulnerabilities**
    - **Unauthorized Withdrawals** — Logic errors in the on-chain verification of zero-knowledge proofs could potentially allow malicious actors to withdraw funds they did not deposit, resulting in direct loss of user assets.

- **Zero-Knowledge Circuit Vulnerabilities**
    - **Privacy Leakage** — Flaws in the Circom circuit design or constraint definitions could inadvertently expose the link between deposit and withdrawal transactions, revealing the public key of the depositor or recipient. This would compromise the core privacy guarantee of the protocol without necessarily resulting in fund loss — but would constitute a fundamental failure of the protocol's primary value proposition.
- **Dependency Risks**
    - **Oracle and Price Feed Failures** — For privacy-preserving swaps, LST, and DCA functionality, the protocol relies on external price data. Stale, manipulated, or incorrect price feeds could result in unfavorable execution for users or create arbitrage vectors that drain protocol value.
- **Solana Runtime Dependencies** — The protocol relies on Solana's runtime environment for proof verification and program execution. Changes to compute limits, syscall behavior, or runtime updates could potentially disrupt proof verification or contract execution.

Security Measures & Their Limitations:

- **Smart contract security practices**
    - **Arithmetic overflow protection**
        - `overflow-checks = true` is enabled in release build profiles. All fee and amount calculations additionally use Rust's safe math methods.
    - **Reentrancy protection**
        - A RAII-pattern guard (`SettingsReentryGuard`) prevents recursive calls during critical operations.
    - **CPI (Cross-Program Invocation) detection**
        - The `InsideCPI` error code prevents certain operations from being called within CPI context, reducing composability attack vectors.
    - **Account validation:**
        - PDA (Program Derived Address) seeds, bump verification, and discriminator checks are enforced throughout both programs via Anchor framework constraints.
    - **Responsible disclosure program**
        - The programs includes `solana-security-txt` metadata with contact information and a project URL for responsible vulnerability disclosure.
    - **OFAC sanctions screening**
        - On-chain Ed25519 signature verification for on-chain OFAC compliance, as described above.
    - **Community testing and audits**
        - The Protocol has undergone community testing and internal code review.

Critical Economic Assumptions:

    - The protocol's economic sustainability, security, and governance effectiveness rest on several interconnected assumptions. Below we outline each assumption and the consequences of its failure.
    - **Primary Assumption: Demand for On-Chain Privacy**
        - The protocol's entire revenue model is predicated on the assumption that a meaningful and growing segment of Solana users value financial privacy sufficiently to pay fees for privacy-preserving services. This includes individuals seeking transaction confidentiality, traders protecting their strategies from surveillance, and institutions requiring operational discretion. If this assumption fails — whether due to shifting user preferences, regulatory pressure that discourages privacy tool usage, or the emergence of native privacy features at the chain level — protocol revenue would be significantly lower than projected, potentially undermining long-term operational sustainability.
    - **DCA and Swap Volume**
        - The Private DCA and Private Swap products assume consistent on-chain trading activity and that users executing large or recurring strategies are willing to pay a premium for confidentiality. If on-chain trading volume migrates to alternative venues, or if users determine the privacy premium is not justified relative to the cost, fee revenue from these products would decline.
    - **Consequences of Assumption Failure**
        - **Revenue Shortfall** — Insufficient fee generation would reduce treasury inflows, constraining the DAO's ability to fund ongoing development, security audits, and ecosystem growth.
        - **Operational Sustainability** — In an extreme scenario where multiple assumptions fail simultaneously, the protocol may lack the treasury resources to sustain ongoing operations, necessitating either emergency governance proposals for restructuring or, ultimately, an orderly wind-down.

Governance Control over Monetary Policy & Rewards:

- The DAO exercises full authority over all monetary policy, fee parameters, and reward allocations through the futarchy-based governance mechanism. Any modifications to these parameters require a proposal to pass through MetaDAO's decision market process before execution.
    - **Scope of Governance Authority**
        - Through passed proposals, the DAO can modify:
            - **Fee structures** across all protocol services (private transfers, swaps, LST, DCA).
            - **Treasury allocation and disbursement** — directing funds toward development, audits, grants, ecosystem incentives, or future distribution mechanisms.

        - **Token minting** — new ZKFG tokens can only be created through governance proposals, with no automatic inflation mechanism or scheduled unlocks outside of governance control.
        - **Incentive programs** — creation, modification, or discontinuation of any liquidity mining, user acquisition, or ecosystem reward programs.
        - **Revenue allocation strategy** — decisions on whether protocol revenue is reinvested, reserved, or distributed.
- **Built-in Safeguards Against Adverse Outcomes**
    - The futarchy mechanism provides a structural safeguard against proposals that would adversely affect token holders. Unlike traditional one-token-one-vote governance — where apathy, voter manipulation, or whale dominance can lead to value-destructive outcomes — futarchy requires participants to put capital at risk based on their conviction about a proposal's impact on token value.
- This means:
    - **Proposals that the market expects to decrease token value are rejected.** The decision market mechanism inherently filters out proposals perceived as value-destructive, because traders are economically incentivized to trade against them.
    - **Token holders are the DAO.** The same stakeholders who would be affected by monetary policy changes are the ones evaluating and trading on those proposals. There is no separation between governance participants and affected parties.
    - **Skin in the game eliminates uninformed governance.** Participants must commit capital to influence outcomes, discouraging frivolous or malicious proposals and ensuring that governance decisions reflect informed economic conviction.

Regulatory, Legal & Tax Risks

Token classification. The governance token may be classified differently across jurisdictions. If any regulator determines it constitutes a security rather than a governance or utility token, the project and token holders could face registration requirements, trading restrictions, or enforcement actions. The U.S. SEC's evolving position on governance tokens, and parallel developments in the EU (MiCA), Singapore (MAS), and other jurisdictions, create ongoing uncertainty that the project cannot resolve unilaterally.

Entity-level regulatory risk. The project operates under a Marshall Islands DAO LLC structure. While the Marshall Islands has adopted favorable digital asset legislation, this jurisdiction may face diplomatic, banking, or regulatory pressure that creates operational friction. Regulatory changes in any jurisdiction where the development team operates, token holders reside, or users access the protocol could impose licensing requirements, restrict operations, or compel structural changes to the DAO LLC or its governing arrangements.

MetaDAO protocol dependency. The project's governance infrastructure is provided by MetaDAO, which is currently in beta. MetaDAO's documentation discloses that the MetaDAO team currently retains the ability to override decision markets in extreme scenarios. Changes to MetaDAO's protocol, terms, or operational status could affect the project's ability to conduct governance or complete token-related actions.

Protocol, Technology & Security Risks

Smart contract vulnerabilities. Logic errors or implementation flaws in the project's on-chain programs could result in loss of funds or unintended behavior. No audit process eliminates all risk; vulnerabilities may exist that audits, internal review, or community testing fail to detect, including novel attack vectors that emerge after deployment.

Solana runtime dependency. The project's contracts execute on Solana. Changes to Solana's compute limits, runtime behavior, validator set, or network stability could disrupt contract execution or proof verification. A Solana network outage or consensus failure would render on-chain governance and treasury operations temporarily inaccessible.

MetaDAO decision market dependency. Governance, including all treasury actions and token issuance, is routed through MetaDAO's decision market infrastructure. A bug, exploit, or operational failure in MetaDAO's contracts could prevent proposals from being created, resolved, or executed, effectively freezing governance until the issue is resolved.

Decision market liquidity and manipulation risk. Proposal markets rely on sufficient trading participation to produce accurate price signals. Thin liquidity in PASS or FAIL markets, particularly for smaller or less actively traded projects, could allow a single large participant to influence a TWAP outcome. MetaDAO's lagging TWAP mechanism mitigates but does not eliminate this risk.

AMM liquidity pool risk. A portion of ICO proceeds and tokens are deployed to an AMM liquidity pool at launch. Impermanent loss, pool imbalances, or low liquidity depth could affect the tradability of the token and the value of treasury-held liquidity positions**.**

Token Economics, Unlocks & Incentive Risks

Performance tranche unlock pressure. Team tokens, where applicable, unlock in tranches tied to price milestones (2x, 4x, 8x, 16x, and 32x of ICO valuation). Each milestone, if reached, creates a discrete unlock event that may result in selling pressure as recipients become able to claim and liquidate tranches.

Governance can authorize new token issuance. Mint authority over the token sits with the DAO treasury, governed by MetaDAO's decision market mechanism. A governance proposal that passes could authorize the issuance of additional tokens, which would dilute existing holders. Token holders cannot assume the current supply is a permanent ceiling.

Governance participation risk. Decision markets require active, capitalized participation to function as intended. If governance markets are thinly traded, due to low token holder engagement, small float, or poor market depth, proposal outcomes may reflect the preferences of a small number of participants rather than the broader holder base. Apathetic or concentrated governance could lead to outcomes that are adverse to the majority of token holders.

Treasury concentration risk. All ICO proceeds flow into a single on-chain treasury governed by decision markets. A successful malicious proposal, a smart contract exploit targeting the treasury, or a sustained period of governance dysfunction could result in partial or total loss of treasury assets with limited recourse.

Protocol revenue assumptions. Value accrual to the token depends on the protocol generating meaningful usage and, over time, revenue that governance allocates toward token holders. If the protocol fails to attract sustained usage, the treasury will not grow beyond ICO proceeds, and there is no mechanism guaranteeing any return to token holders other than a governance-authorized liquidation proposal**.**