BTRFLY
WHITEPAPER

1. Executive Summary

BTRFLY represents a new generation of social applications built on a decentralized internet where users own their identities, data, and interactions.

The project is powered by zkSync's zero-knowledge infrastructure, creating a private, secure, and community-governed dating network without centralized data extraction.

Traditional dating platforms have suffered from the same issues for more than a decade: fake identities, data leaks, and manipulative algorithms. BTRFLY solves these problems through verifiable identity proofs, end-to-end encrypted communication, and tokenized rewards that maintain a balance between platform growth and user benefit.

The $BFLY token (ERC-20, supply 1B) is the backbone of the ecosystem — powering boosts, staking, governance, and implementing a deflationary model inspired by the BNB burn mechanism.

---

2. Problem Statement

The online dating industry continues to grow, but suffers from structural and systemic weaknesses:

- Up to 40% of profiles are fake
- More than 12,000 data breaches in the last decade
- Agorithms encourage impulsive behavior rather than authentic connections
- Existing Web3 alternatives fail due to poor UX and weak identity infrastructure

The result is a need for a complete redesign — a platform that is authentic,
scalable, and owned by its users.

The online dating industry is expanding, yet remains limited by structural flaws: high volumes of fake profiles, recurring data breaches, and engagement-driven algorithms that prioritize swipes over meaningful connections. Existing Web3 attempts suffer from poor UX and immature identity frameworks, making them unusable for mainstream audiences.

These constraints highlight the need for a redesigned model—one that delivers authenticity, verifiable identity, and user ownership at scale.

---

3. Solution Overview

3.1 Core Concept

BTRFLY is a decentralized ZK-based dating ecosystem built on zkSync Era. Identities are verified using ZK proofs without revealing private data. Messages are encrypted using E2EE standards (AES-256 + ECDH).

3.2 Identity Layer

- Circom circuits
- zk-SNARK verification
- DIDs (Decentralized Identifiers)
- Soulbound reputation

The identity stack combines Circom-based ZK circuits, zk-SNARK verification, decentralized identifiers (DIDs), and soulbound reputation primitives to provide secure, non-transferable, and verifiable user credentials.

3.3 Migration to L3

A future transition to a dedicated L3 hyperchain via zkStack will enable sovereign scaling.

3.4 Monetization & Utility

$BFLY provides:

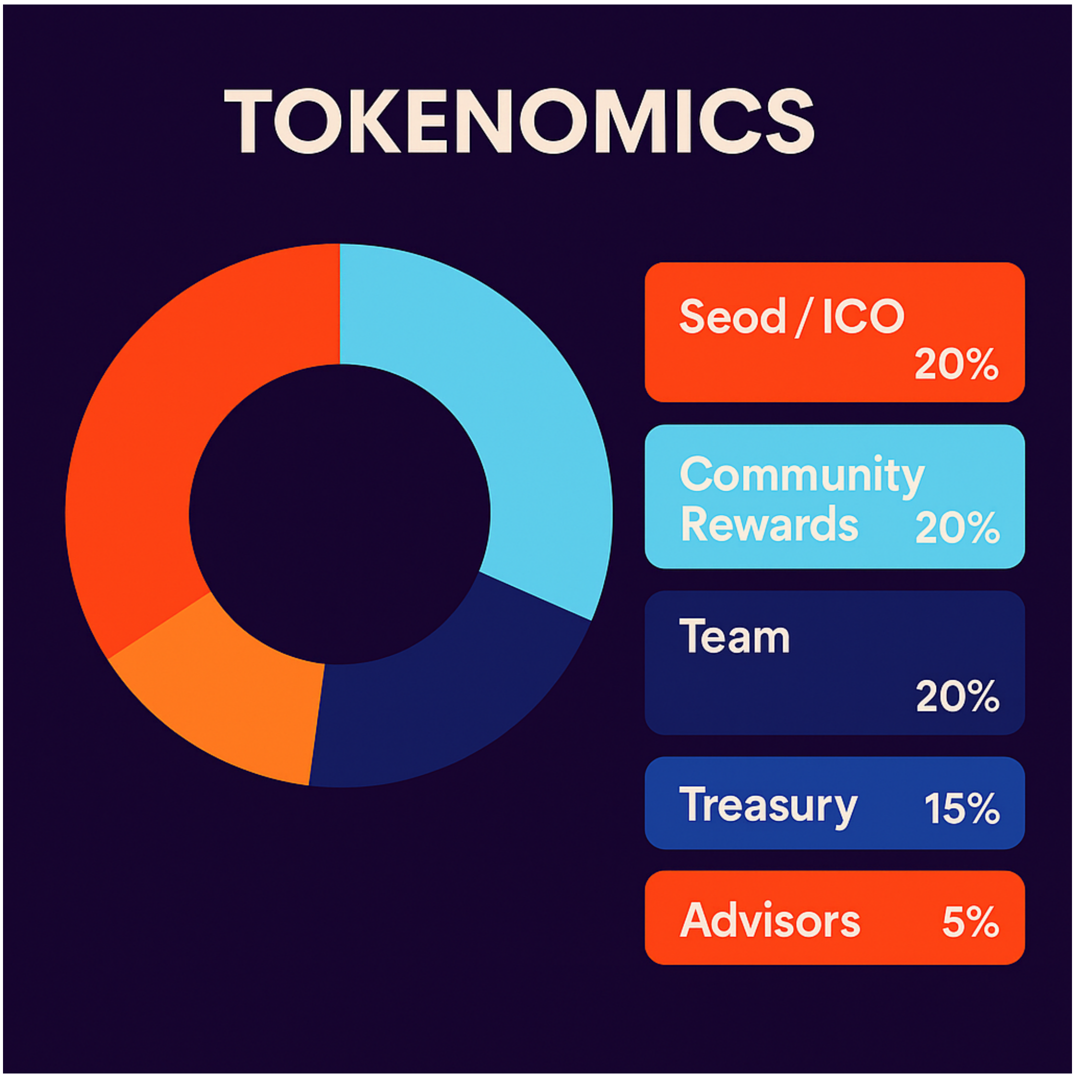
- matchmaking boosts
- staking yields
- governance voting
- deflationary mechanics (burns + buybacks)

3.5 User Experience

BTRFLY's user experience integrates on-chain identity, verifiable interactions, and a modular gamification layer. ERC-1155 badges function as blockchain-native reputation assets, dynamically issued based on user behavior, verification status, and interaction quality. These badges feed into a reputation scoring model that influences discovery, trust signals, and matchmaking relevance. All core actions—profile verification, interactions, boosts, and reputation events—are recorded through lightweight on-chain proofs, ensuring auditability without compromising privacy. The result is a streamlined UX where user identity, trust, and engagement are anchored in cryptographically verifiable data.

---

4. Tokenomics



4.1 Allocation

Total supply: 1,000,000,000 $BFLY

- **20%** Seed/ICO
- **30%** Community Rewards
- **20%** Team
- **15%** Treasury
- **10%** Liquidity
- **5%** Advisors

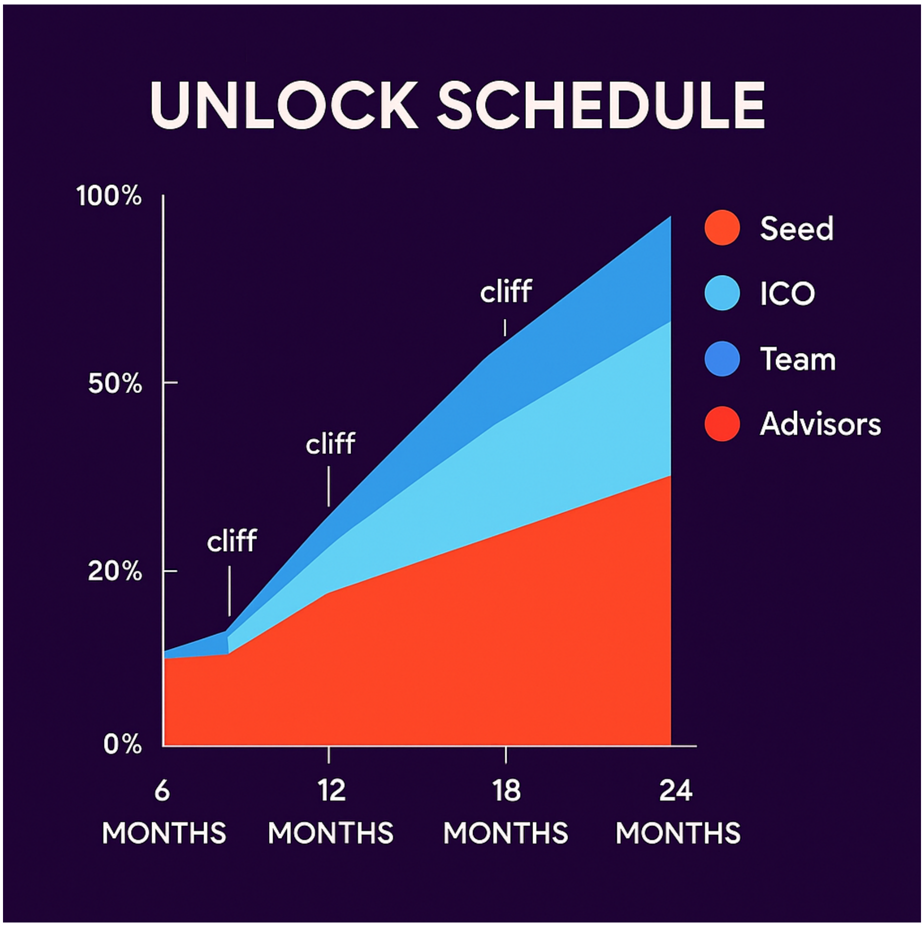
This allocation model establishes a balanced token economy optimized for liquidity, community incentives, and long-term operational viability.

The Seed/ICO tranche secures initial capital formation, while Community Rewards drive early network effects and user acquisition.

Team and Advisor allocations are subject to vesting schedules to ensure aligned incentives over time.

Treasury and Liquidity reserves provide stability, enabling market support, protocol development, and sustainable ecosystem growth.

4.2 Vesting & Unlocks



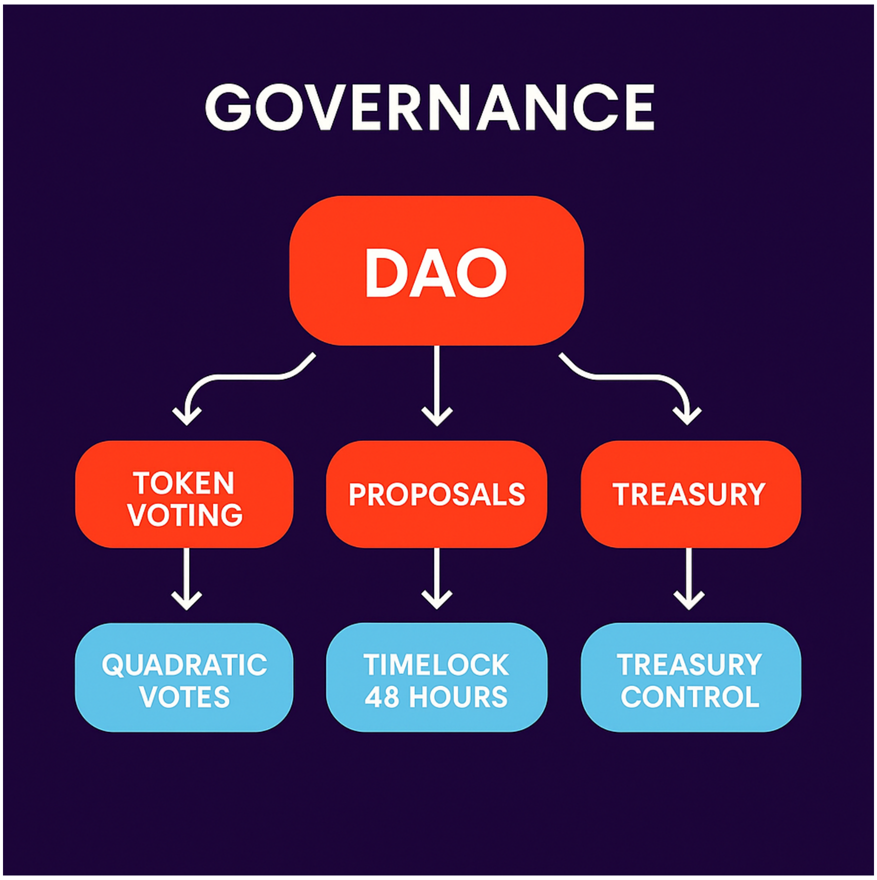
Team:	24-month linear unlock
Advisors:	short cliff
Seed + ICO:	phased unlocking
Community Rewards:	adoption-based release schedule

4.3 Circulating Supply Model

The model includes:

- gradual release of Seed/ICO tokens
- growth of Community Rewards
- quarterly burns (1%)
- supply stabilization by 2027–2028

4.4 Governance



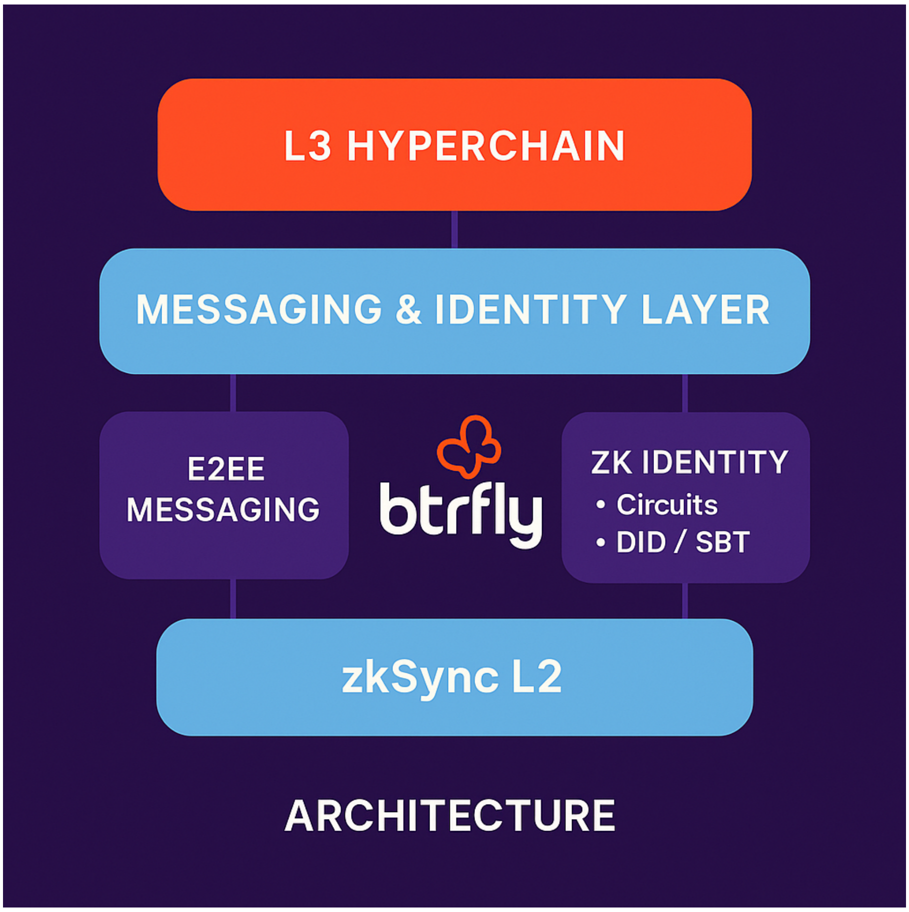
The DAO is built on Aragon modules with on-chain execution and a 48-hour timelock.

Quadratic voting prevents dominance by large holders.

Token holders decide on:

- treasury management
- partnerships
- upgrades
- token mechanics

5. Platform Architecture



<u>The architecture consists of three layers:</u>

L2 — zkSync:

– high throughput

– low fees

– fast finality

Messaging & Identity Layer:

- end-to-end encrypted messaging
- ZK identity circuits
- DIDs and SBTs

L3 Hyperchain (2027+):

- sovereign chain for BTRFLY
- isolated mempool
- custom governance logic

This three-layer architecture enables scalable performance, privacy-preserving identity, and long-term sovereignty. zkSync L2 provides throughput and low-cost settlement, while the messaging and identity layer adds encrypted communication and ZK-based verification. The future L3 hyperchain gives BTRFLY dedicated blockspace, custom governance, and full control over protocol evolution.

6. Roadmap


ROADMAP
Short-Term Milestones
ICO raise 8,5 M USD
Medium-Term Goals
• MVP deployment on zkSync testnet
• ZK identity audits
• CEX & DEX listing
Long-Term Vision
2027+: L3 hyperchain migration

Short-Term (Q1 2026):

– ICO 8.5M

– smart contract + ZK circuit audits

– beta onboarding & wallets

Medium-Term (Q3–Q4 2026):

– MVP on zkSync testnet

– AI matching engine

– NFT badges

– staking & governance releases

– CEX & DEX listing

Long-Term (2027+):

– L3 hyperchain

– partnerships with zkSync Foundation & AI modules

– decentralization of messaging & identity (IPFS / Arweave)

---

7. Migration Plan (Web2 → Web3)

Phase 1 — Hybrid Layer (Q1–Q3 2026):

Web2.5 onboarding, smart wallets, gasless transactions.

Phase 2 — Decentralized Identity (Q3–Q4 2026):

DIDs, ZK credentials, staking incentives.

Phase 3 — Full Autonomy (2027+):

L3 chain, DAO treasury.

BTRFLY transitions from a Web2-compatible onboarding flow to a fully decentralized architecture in structured phases. The hybrid stage introduces smart wallets and gasless actions to ensure mainstream usability.

The decentralized identity phase adds DIDs, ZK credentials, and staking incentives to anchor trust on-chain. In the final phase, the ecosystem moves toward full autonomy through an L3 chain and DAO-governed treasury, completing the migration to a user-owned network.

8. Conclusion

BTRFLY sets a new benchmark for digital relationship platforms by combining privacy-preserving identity, decentralized architecture, and verifiable interactions. Traditional dating systems rely on opaque algorithms, unverifiable data, and centralized control; BTRFLY replaces these limitations with a trust framework anchored in zero-knowledge proofs and cryptographic guarantees.

Through ZK identity, E2EE messaging, and a tokenized incentive layer, the platform transforms authenticity into measurable on-chain reputation, improving match quality and user safety. As the ecosystem evolves toward decentralized identity primitives and a dedicated L3 chain, governance and ownership progressively transition to the community, enhancing resilience and long-term sustainability.

By uniting Web3 infrastructure with a user-centric product vision, BTRFLY positions itself as the next generation of social networks—secure, transparent, and powered by the users who participate in it.