WHITEPAPER

2026

Zero-Knowledge Dating Protocol

Private by design. Owned by the community.

Built on zkSync Era · Powered by $BFLY

ICO Q3 2026 · $9.1M

FDV Target $70M

1B $BFLY · ERC-20

Contents

EIGHT CHAPTERS · 25 PAGES · WHITEPAPER

CHAPTER ONE

01

Executive Summary

BTRFLY is a zero-knowledge dating protocol on zkSync Era, turning an existing 2M+ download Web2 platform into a verifiable, user-owned Web3 network.

A new social primitive for the Web3 era.

PRIVATE. VERIFIABLE. USER-OWNED.

BTRFLY is a next-generation social protocol where users own their identities, data, and interactions. Built on zkSync's zero-knowledge infrastructure, it creates a private, secure, and community-governed dating network — eliminating centralized data extraction, fake-profile incentives, and engagement-maximising algorithms.

The opportunity

The global dating market generates over $10 billion annually, with 462 million users worldwide and structural distrust in centralized platforms. Up to 40% of profiles are fake, romance fraud cost victims $1.3B in 2023 (FBI), and 12,000+ breaches in the last decade exposed intimate user data.

BTRFLY converts an existing 2M+ download Web2 dating application into a ZK-native Web3 protocol — combining consumer-grade UX (seedless wallets, gasless onboarding) with cryptographically verifiable identity. This distribution advantage dramatically reduces CAC versus cold-start competitors.

Key protocol metrics

$9.1M	1B	$70M	10–12%
ICO Target Q3 2026	$BFLY Supply Fixed ERC-20	Target FDV Public @ $0.075	Circulating at TGE Low-float strategy

Three pillars

ZK

Private Identity

Zero-knowledge proofs verify identity without exposing personal data on-chain. Soulbound reputation SBTs anchor user trust.

Circom · zk-SNARKs · W3C DIDs

E2E

Encrypted Messaging

AES-256 + ECDH end-to-end encrypted peer-to-peer communication with zero metadata leakage and off-chain key management.

AES-256 · XMTP · WebRTC

DAO

Community Governed

Aragon DAO on-chain modules with quadratic voting and 48-hour execution timelock ensure token holder sovereignty.

Aragon · Quadratic voting

WHAT $BFLY DOES

Matchmaking boosts · staking rewards 5–15% APY · governance votes · deflationary burn & buyback capturing 45% of protocol revenue.

The BTRFLY approach

Where centralized platforms offer opaque algorithms, undisclosed data monetisation, and pay-to-win match dynamics, BTRFLY replaces each failure with a cryptographic primitive:

WHAT WE REPLACE	HOW WE REPLACE IT
Opaque algorithms	Verifiable ZK identity proofs, open-source matching engine
Centralized data extraction	User-owned on-chain reputation · Soulbound ERC-1155 badges
Engagement-maximising incentives	Token-aligned rewards tied to outcome quality, not time-on-app
Fake profile economy	ZK-verified identity with anti-Sybil circuit design
Platform lock-in	Portable reputation anchored to DIDs, usable across dApps

Why now

Three conditions converge in 2026 to make BTRFLY viable at scale:

- **ZK infrastructure maturity.** zkSync Era delivers sub-cent transactions and sub-second finality. Circom and Halo2 toolchains are production-ready. ZK onboarding no longer feels cryptographic — it feels invisible.
- **Account abstraction crossing the chasm.** ERC-4337 removes seed phrases and gas from the user's vocabulary. Smart wallets with social recovery and biometric auth make Web3 UX match Web2.
- **Privacy backlash at critical mass.** Post-Cambridge Analytica, post-GDPR, and after 12,000+ dating-data breaches, the market is actively seeking verifiable privacy guarantees — not terms of service.

> *"The application drives adoption. The identity layer enables trust and retention."*

Protocol highlights

Deflationary by design

1% quarterly token burn from circulating supply plus 45% of protocol revenue routed to buyback & burn. Supply stabilization projected 2028.

Gasless onboarding

ERC-4337 account abstraction with social recovery and Passkey/WebAuthn biometric auth. Users never see a seed phrase.

Community-governed

Aragon DAO with quadratic voting (anti-whale), 72-hour discussion, 5-day voting window, 48-hour execution timelock.

Low-float launch

Only 10–12% of supply circulating at TGE. Team tokens linear-unlock over 24 months. Adoption-driven community distribution.

CHAPTER TWO

02

Market Opportunity

A $10B+ industry plagued by distrust meets a Web3 infrastructure stack finally ready for mainstream consumer scale.

Industry scale and structural disruption.

GLOBAL DATING MARKET · WEB3 SOCIAL SEGMENT

Online dating has grown from niche novelty to global infrastructure, generating $10.4B in 2024 and projected to reach $17.8B by 2030. Beneath this growth, systemic failures in trust, identity, and data sovereignty have created conditions for a cryptographically-native alternative.

$10.4B	$17.8B	462M	2.9B+
Global market 2024	Projected 2030	Global users	Online daters by 2028

Global trends driving disruption

Several simultaneous shifts are reshaping the category. AI-enhanced matching is moving from novelty feature to baseline expectation, with platforms like Bumble reporting 4.2M paying users who cite AI-curated suggestions as a primary reason for subscription. Asia-Pacific markets are growing at 7.4% CAGR, while European users — conditioned by GDPR — demand provable privacy guarantees rather than terms-of-service promises. Gen Z, now the largest cohort of new dating-app users, explicitly prioritizes "authentic connection" over engagement volume, per Pew Research 2024.

Most significantly, the Web3 social segment is compounding at ~25% CAGR through 2030. Early dApps — Friend.tech, XO, Solmates — demonstrated user willingness to pay for on-chain social primitives, but each launched without production-grade identity infrastructure. BTRFLY enters with the opposite profile: existing consumer traction plus native ZK identity.

Competitive landscape

PLATFORM	SCALE	ARCHITECTURE	BTRFLY ADVANTAGE
Tinder	75M+ MAU	Centralized, algorithmic	ZK anonymity, no data harvest
Bumble	42M MAU	Centralized, paid tiers	DAO governance, user ownership
Hinge	28M MAU	Centralized, prompts	Verifiable identity, SBT reputation
XO	1.5M Base users	Web3, AI-focused	L3 hyperchain, full protocol stack
BTRFLY	**2M+ downloads**	**ZK-native on zkSync**	**Full-stack identity + existing users**

CATEGORY INFLECTION

The industry is shifting from engagement-driven platforms to trust-driven systems. BTRFLY is positioned at this inflection with distribution advantage, technical depth, and regulatory alignment.

SWOT analysis

Strengths

Cutting-edge ZK privacy · low-cost transactions (<$0.001 per ZK proof) · DAO-driven innovation cycle · elastic scalability up to 30,000 TPS on zkSync Atlas · proven 2M+ download distribution from existing Web2 app · experienced team with crypto-law and Web3 product expertise.

Weaknesses

Early-stage adoption requires Web3 education · ZK proof UX still evolving · regulatory ambiguity around dating-adjacent tokens in some jurisdictions · reputation SBTs depend on ecosystem-wide adoption for full portability.

Opportunities

Real-world-asset (RWA) tokenization of events and meetups · AI-Web3 synergy for hyper-personalized matching without data exfiltration · expansion to adjacent social verticals (friendship, professional networking) · cross-protocol identity reuse (DeFi, DAOs).

Threats

EU AI Act 2025 compliance overhead · potential big-tech entry (Meta, Bytedance) · crypto market cycles affecting token economics · privacy regulations evolving faster than implementation cycles.

Economic factors

The current macro environment favours utility-token protocols with real product-market fit. Persistent inflation and institutional crypto adoption (spot Bitcoin ETFs, corporate treasury policies) have expanded retail and institutional appetite for tokens backed by verifiable usage — not speculation.

BTRFLY's FDV target of $70M at public sale represents an attractive entry relative to comparable Web3 social protocols. Seed investors at $0.020 enter at 3.75× below the public ICO price, with vesting cliffs that align incentives across the first 36 months of operation.

Addressable market sizing

$10.4B
TAM · Total addressable online dating market globally

$2.1B
SAM · Privacy-conscious and crypto-native segment

$120M
SOM · Realistic 3-year capture at 50K DAU scale

"The existing Web2 user base is the moat. Web3-native primitives are the product."

CHAPTER THREE

03

Problem Statement

Four structural failures that centralized dating platforms cannot fix from within.

Trust cannot be solved within centralized systems.

FOUR STRUCTURAL FAILURES OF THE STATUS QUO

> The online dating industry continues to grow in revenue while trust, safety, and user outcomes erode. This is not a UX problem or a policy problem — it is an architectural problem. Four structural failures recur across every centralized dating platform, and none of them are fixable without re-architecting the underlying trust model.

~40%	12K+	$1.3B	54%
Fake profiles on major platforms	Breaches in dating apps last decade	Romance fraud losses FBI 2023	Users feel unsafe Pew 2024

1 · Identity is unverifiable

Approximately 40% of profiles on major dating platforms are fake, impersonation, or bot-operated (FTC 2024). Centralized KYC is a dead-end: it either deters 60% of legitimate users (Pew) or creates a honeypot of real-identity documents that attract the very breaches that erode trust. BTRFLY's ZK verification proves attributes (age, humanness, uniqueness) without revealing or storing raw data.

2 · Data is weaponised against the user

Ashley Madison (2015, 37M users exposed), Bumble (2024 leak, millions affected), and 12,000+ documented breaches reveal a pattern: centralized dating platforms store intimate user data indefinitely, monetise it through advertising partners, and repeatedly fail to protect it. GDPR fines and class actions are the after-the-fact consequences of an architecture that should never have stored the data in the first place.

3 · Algorithms optimise for engagement, not outcomes

Match algorithms on centralized platforms are trained to maximise time-on-app, not relationship formation. This creates perverse incentives: the more users find successful matches, the less revenue the platform generates. Gen Z users have noticed — 62% report feeling "tricked by the algorithm" (Pew 2024). On BTRFLY, matching is open-source and token-weighted: staking reputation aligns incentives with outcome quality.

4 · Existing Web3 alternatives lack product quality

The first wave of Web3 dating dApps launched with strong ideology and weak UX. They required seed phrases, gas fees, wallet switching, and technical literacy. BTRFLY addresses this by combining a production-grade Web2 app with gasless onboarding (ERC-4337), invisible key management, and progressive Web3 transition — so users gain the benefits of decentralisation without the cognitive load.

CHAPTER FOUR

04

Solution & Product

A consumer dating application powered by a native zero-knowledge identity and interaction layer.

Dual-layer architecture: app + protocol.

CONSUMER PRODUCT POWERED BY WEB3 PRIMITIVES

BTRFLY operates as a dual-layer system. The application layer drives adoption through familiar dating UX — matching, messaging, profile creation. The identity and interaction layer provides verifiable trust through zero-knowledge proofs, encrypted messaging, and on-chain reputation. Users benefit from both, without needing to understand either.

Core product features

Seedless wallet onboarding

ERC-4337 account abstraction + Passkey/WebAuthn. No seed phrase, no gas, no wallet switching. Signup in under 60 seconds.

ZK-verified profiles

Prove age, humanness, uniqueness, jurisdiction — without revealing raw data. Anti-Sybil circuits prevent fake accounts.

AI-powered matchmaking

TensorFlow-based collaborative filtering on anonymized preference vectors. Algorithm weights are on-chain and auditable.

E2E encrypted messaging

AES-256 + ECDH key exchange. XMTP protocol for decentralized message routing. WebRTC P2P for low-latency calls.

SBT reputation badges

ERC-1155 soulbound tokens record verification events, positive interactions, and community contributions portably.

Token-native boosts

Pay in $BFLY for priority matching, profile visibility, premium discovery. Revenue routes to buyback & burn.

Three identity pillars

ZK IDENTITY

Proof without exposure

Circom circuits generate zero-knowledge proofs verifiable on-chain in under 200ms. Users prove attributes without revealing underlying data.

Circom · Halo2 · zk-SNARKs

DID LAYER

Portable identity

W3C-compliant Decentralized Identifiers resolve to soulbound reputation NFTs. Identity survives account deletion and crosses applications.

W3C DIDs · ERC-1155 SBTs

E2E ENCRYPT

Zero metadata trust

Communication encrypted end-to-end. Protocol operators cannot access message content. Perfect forward secrecy with ECDH.

AES-256 · ECDH · XMTP

End-to-end user journey

A complete user flow from signup to interaction illustrates how cryptographic primitives disappear into consumer UX:

STEP 01

Onboard

- Biometric signup (Passkey)
- Smart wallet generated
- Gasless via Paymaster
- ~60 seconds

STEP 02

Verify

- ZK age proof circuit
- Anti-Sybil uniqueness
- Jurisdiction attestation
- Data never stored

STEP 03

Match

- AI preference matching
- Boost via $BFLY stake
- Match on encrypted vectors
- Mutual reveal only

STEP 04

Connect

- E2EE chat via XMTP
- Optional P2P video
- SBT badges accrue
- Portable reputation

Messaging architecture

Communication is the product. Every message sent through BTRFLY is end-to-end encrypted before it leaves the device, with session keys rotated via ECDH for perfect forward secrecy. The XMTP protocol handles decentralized delivery — neither BTRFLY's servers nor zkSync validators can read message content. For real-time voice and video, WebRTC establishes direct peer-to-peer connections through STUN/TURN relays, minimizing latency and eliminating centralized mediators.

Gamification through verifiable achievements

ERC-1155 soulbound tokens function as blockchain-native reputation assets — dynamically issued based on user behaviour, verification status, and interaction quality. Core actions (profile verification, positive interactions, boosts, community contributions) are recorded through lightweight on-chain proofs, ensuring auditability without compromising privacy. Users accumulate portable reputation that travels across the Web3 social graph.

SCALABILITY PATH

The 2027+ migration to a sovereign L3 hyperchain (via zkStack) enables 1M+ DAU with elastic throughput, dedicated blockspace, and custom governance logic — all inherited from Ethereum's security guarantees.

MONETIZATION LOOP

$BFLY pays for boosts and staking access. Fees fund 45% buyback & burn (deflationary pressure), 25% staker rewards, 20% treasury, 10% liquidity. Token velocity decreases as utility increases.

> *"A trust-native social experience, where cryptographic primitives replace terms of service."*

CHAPTER FIVE

05

Technical Architecture

A three-layer system: zkSync L2 settlement, encrypted messaging and ZK identity, future sovereign L3 hyperchain.

Three-layer protocol stack.

L2 SETTLEMENT · MESSAGING + IDENTITY · FUTURE L3

BTRFLY's architecture separates concerns across three layers. zkSync Era provides base-layer settlement with Ethereum security. A middleware layer handles encrypted messaging and ZK identity circuits. A future sovereign L3 hyperchain will provide dedicated blockspace with custom governance. Each layer is independently upgradeable.

Application Layer — FRONTEND

React Native mobile app (iOS / Android) · Next.js web client · Biometric auth

Messaging & Identity Layer — MIDDLEWARE

E2E encrypted messaging · ZK identity circuits · DIDs and SBTs · Reputation primitives

L2 Settlement — zkSync Era — SETTLEMENT

Smart contracts in Solidity 0.8.25 · 15K+ TPS · Sub-second finality · $0.001 per tx

L3 Hyperchain (2027+) — SOVEREIGNTY

Sovereign chain via zkStack · Isolated mempool · Custom governance logic · Dedicated blockspace

Blockchain integration

BTRFLY deploys on zkSync Era, leveraging the Atlas upgrade's RISC-V Airbender prover for sub-second finality and up to 30,000 TPS throughput. Full EVM compatibility means Solidity contracts deploy without modification, and account abstraction (ERC-4337) is native to the chain — enabling gasless user onboarding through Paymaster contracts. Costs are below $0.001 per ZK proof verification, making millions of daily interactions economically viable.

Smart contract modules

Core contracts are audited, UUPS-upgradeable, and protected by 3-of-5 multisig governance with 48-hour timelocks:

CONTRACT	PURPOSE	STANDARD
$BFLYToken	Utility token with burn function, revenue routing	ERC-20 · OpenZeppelin
BTRFLYIdentity	ZK proof verifier, DID registry, SBT issuance	ERC-1155 · W3C DID
BTRFLYStaking	Single-sided staking, variable APY 5-15%, reputation boost	Custom · Audited
BTRFLYGovernor	Aragon DAO proposals, quadratic voting, treasury execution	Aragon · Governor
BTRFLYPaymaster	Gasless tx sponsorship, meta-transaction validation	ERC-4337

Zero-knowledge proofs in detail

BTRFLY uses zk-SNARKs (succinct, non-interactive arguments of knowledge) for on-chain verification. Circuits are written in Circom 2.1 and compiled via the Halo2 proving framework. Users generate proofs off-chain (browser or mobile), the proof is submitted on-chain, and the verifier contract returns true/false in approximately 200ms — all without the user's underlying data ever touching a server or ledger.

A simple but illustrative example: proving that a user is above a minimum age without revealing their birthdate. The circuit takes the user's actual age as a private input and the required threshold as a public input, and outputs a single bit: valid or not.

EXAMPLE: AGE-THRESHOLD CIRCUIT (CIRCOM 2.1)

```
// Age-threshold circuit - proves user is over minimum age
// without revealing actual age

template AgeProof() {
    signal input privateAge;       // User's actual age (private)
    signal input ageThreshold;     // Required minimum (public)
    signal output valid;            // Result bit

    // Constraint: privateAge must be >= threshold
    component gte = GreaterEqThan(8);
    gte.in[0] <== privateAge;
    gte.in[1] <== ageThreshold;
    valid <== gte.out;
}

component main {public [ageThreshold]} = AgeProof();
```

The compiled circuit produces a verifier contract deployed on zkSync. Verifying a single proof costs under $0.001 on Atlas, and proof generation takes roughly 800ms on a typical smartphone. The same pattern scales to uniqueness proofs (preventing Sybil attacks), jurisdiction attestations, and income verification for premium tiers.

Security mechanisms

Contract security

OpenZeppelin base contracts, ReentrancyGuard on all state-mutating functions, Ownable2Step for admin transitions, UUPS upgrade pattern with timelocks. Independent smart contract audit completed prior to mainnet launch.

Key management

User private keys stored in hardware-backed secure enclaves (iOS Keychain, Android Keystore). Social recovery via trusted contacts. Optional self-custody with export at any time.

Circuit auditing

All Circom circuits reviewed by ZK specialists. Trusted setup ceremony with MPC contributions. Reference implementations published on GitHub under AGPL-3.0.

Bug bounty

Pre-mainnet bug bounty program with $100K maximum payout for critical findings. Ongoing bounty via Immunefi post-launch. Responsible disclosure with 90-day fix window.

CHAPTER SIX

06

Tokenomics

$BFLY — the utility layer of the ecosystem. Fixed supply, deflationary by design, aligned with protocol usage.

Fixed supply. Deflationary. Utility-aligned.

$BFLY · ERC-20 ON ZKSYNC ERA

> $BFLY is the native utility and governance token of the BTRFLY protocol. One billion tokens total, minted once, distributed across six tranches with vesting and unlock schedules designed for long-term alignment. The token captures 45% of protocol revenue via buyback and burn.

Token parameters

1B
Total supply
Fixed, no inflation

$70M
Target FDV
Public ICO

10–12%
Circulating at TGE
Low-float launch

1%
Quarterly burn
From circulating

Pricing rounds

ROUND	PRICE	TOKENS	RAISE	DISCOUNT VS. ICO	VESTING
Seed	**$0.020**	90M	$1.80M	3.75×	3mo cliff + 12mo linear
Presale	$0.050	30M	$1.50M	1.5×	10% TGE + 9mo linear
Community	$0.065	20M	$1.30M	1.2×	25% TGE + 6mo linear
Public ICO	**$0.075**	60M	$4.50M	1.0×	100% TGE
Total		**200M**	**$9.10M**	**20% of total supply**	

Supply allocation

30%
Community Rewards
300M $BFLY · Adoption-based release

20%
Seed / ICO
200M $BFLY · Phased vesting

20%
Team
200M $BFLY · 24mo linear unlock

15%
Treasury
150M $BFLY · DAO-controlled

10%
Liquidity
100M $BFLY · CEX / DEX market making

5%
Advisors
50M $BFLY · 6mo cliff + 12mo linear

Token utility

$BFLY serves four distinct economic functions, each with a direct cash-flow or value-accrual mechanism:

1 · Matchmaking boosts

Priority matching, visibility amplification, premium filters. 42% of projected revenue. All boost payments route through buyback & burn.

2 · Staking & rewards

Single-sided pools with 5–15% variable APY. 7-day unlock standard, 30-day lock boosted. Quadratic weighting against whale dominance.

3 · Governance

1,000 $BFLY minimum to propose. Quadratic voting on treasury, burn rate, upgrades. On-chain execution with 48h timelock.

4 · Reputation multiplier

Staked tokens amplify SBT badge weight — increasing match priority and discovery ranking. Staking improves outcomes, retaining stakers.

Deflationary mechanics

QUARTERLY BURN

1% of circulating supply burned each quarter from protocol treasury. Executed via on-chain transaction visible to all holders.

REVENUE BUYBACK

45% of all protocol revenue routes to automatic token buyback from DEX liquidity. Bought tokens are burned immediately, not held.

Revenue distribution & scenarios

DESTINATION	SHARE	FUNCTION
Buyback & Burn	45%	Deflationary token pressure
Staking Rewards	25%	Variable APY to stakers
Treasury	20%	DAO-controlled grants, partnerships
Liquidity & Ops	10%	Market making, operations

~$11M
Break-even · 20K DAU

~$27M
Base · 50K DAU

~$110M
Bull · 200K DAU

CHAPTER SEVEN

07

Governance & DAO

From founding team to fully community-owned protocol — a staged transition to on-chain sovereignty.

From founding team to protocol autonomy.

ARAGON DAO · QUADRATIC VOTING · ON-CHAIN EXECUTION

Governance authority transitions from the founding team to the BTRFLY DAO in three phases over 18 months post-TGE. The DAO is built on Aragon's modular framework, uses quadratic voting to prevent whale dominance, and executes on-chain with 48-hour timelocks. Token holders decide treasury allocation, partnerships, protocol upgrades, and token mechanics.

DAO architecture

Proposal & Discussion — PHASE 1

Any user with 1,000+ $BFLY can submit a proposal · 72-hour forum discussion period · Signalling via Snapshot

Quadratic Voting — PHASE 2

5-day on-chain voting window · Voting power = √(tokens) · Anti-plutocracy · Minimum 5% quorum

Timelock Execution — PHASE 3

48-hour timelock before execution · Emergency pause via 5-of-7 multisig · Full audit trail on-chain

DAO governs

Treasury — 150M $BFLY community pool, grants, partnerships, marketing. **Protocol parameters** — burn rate, staking APY, boost pricing, revenue splits, L3 timing. **Integrations** — cross-chain bridges, B2B licensing, audit partners. **Upgrades** — smart contract upgrades via UUPS, emergency pause authorization, dispute resolution.

Transition timeline

PHASE	WINDOW	GOVERNANCE SCOPE
Foundation	Q3 2026 — Q1 2027	Team + multisig, DAO advisory
Hybrid	Q2 — Q4 2027	DAO over treasury + parameters
Sovereign	Q1 2028 onward	**Full DAO including upgrades**

CHAPTER EIGHT

08

Roadmap & Team

From ICO to full protocol autonomy — phased decentralization over 24 months, led by a founding team with a decade+ across blockchain, growth, and crypto law.

From ICO to full protocol autonomy.

PHASED DECENTRALIZATION · Q3 2026 → 2028+

BTRFLY's roadmap is structured around four execution phases plus a long-term sovereignty horizon. Each phase has concrete deliverables, audit gates, and user milestones. The Web2-to-Web3 migration is designed to be invisible to end users: they gain benefits without needing to understand the underlying transitions.

Q3 2026

ICO & Audits

- Public ICO — $9.1M
- Independent smart contract audit
- ZK circuit verification
- Beta wallet onboarding

Q4 2026 – Q1 2027

MVP Testnet

- MVP on zkSync testnet
- AI matching engine v1
- On-chain reputation SBTs
- Beta rollout ~10K users

Q2–Q3 2027

Market Launch

- DEX listing (Uniswap v3)
- CEX integrations
- Staking module activation
- Mobile apps iOS + Android

Q1 2028

DAO Governance

- Aragon DAO full activation
- Quadratic voting live
- 48h timelock execution
- Community treasury control

Long-term vision (2028+)

Beyond the initial 24-month roadmap, BTRFLY migrates to a sovereign L3 hyperchain built via zkStack, providing dedicated blockspace with custom governance logic. Decentralized storage (IPFS + Arweave) replaces all remaining centralized components. A B2B API licensing program opens the identity and reputation primitives to other Web3 applications, while cross-protocol partnerships expand the reputation graph across the broader Web3 social layer. The target is 1M+ DAU by 2028.

Web2 → Web3 migration

The transition from the legacy Web2 application to the decentralized protocol is structured across three phases to ensure technological continuity, regulatory compliance, and uninterrupted user experience:

PHASE	WINDOW	MIGRATION SCOPE
Web 2.5 Hybrid	Q3 2026 — Q1 2027	ERC-4337 gasless onboarding, custodial smart wallets, IPFS-anchored metadata
Decentralized Identity	Q4 2026 — Q3 2027	W3C DIDs, Circom verification, Halo2 proofs, eIDAS 2.0 interoperability
Full Web3 Sovereignty	**2027+**	**L3 hyperchain via zkStack, IPFS/Arweave storage, DAO-only governance**

The team building BTRFLY.

FOUNDERS WITH A DECADE+ ACROSS BLOCKCHAIN, GROWTH, AND CRYPTO LAW

> The BTRFLY core team combines deep expertise across Web3 engineering, product strategy, business development, and regulatory compliance. The founders have previously built and launched multiple consumer products and tokens, and bring complementary strengths across the three disciplines required for a protocol of this scope.

Tomáš Krč

CEO & CO-FOUNDER

7+ years in blockchain and AI investing. Web3 product architect with multiple token launches. Leads product vision, strategy, and execution across technology, business, and user experience. Previously BPLAY and BTRFLY architect. MSc.

Peter Paluch

CBCO & CO-FOUNDER

10+ years in digital growth and community acquisition. Expert in viral marketing and Web3 growth strategies. Leads business development, partnerships, and user acquisition. Responsible for community scaling and ecosystem partnerships. MBA.

Jozef Janek

CLO & CO-FOUNDER

Chief Legal Officer specialising in crypto and DeFi legal strategy. Leads regulatory compliance, token structure under MiCA, corporate structuring, and ICO/STO advisory. Focused on building legally resilient Web3 infrastructure. LL.M.

Engineering & advisory

Lead Blockchain

Solidity · Rust · zkSync · ZK circuit design

ZK Engineer

Circom · Halo2 · zk-SNARK systems · trusted setup

Full-Stack Web3

React Native · IPFS / WebRTC · ERC-4337 abstraction

AI / ML Engineer

TensorFlow · federated learning · privacy-preserving matching

Risk disclosures

This whitepaper is for informational purposes only and does not constitute an offer to sell or a solicitation to buy any securities. $BFLY is a utility token intended for use within the BTRFLY protocol. Prospective purchasers should conduct independent due diligence and consult qualified legal, tax, and financial advisors before participating. Token holdings involve risks including but not limited to: smart contract vulnerabilities (mitigated through audits but not eliminated), regulatory changes affecting token utility or transferability, market volatility, protocol failure, key management failures, and third-party dependencies (zkSync, XMTP, oracle providers). The BTRFLY protocol is under active development and feature timelines may shift based on audit findings or market conditions. Past performance of related projects does not predict future results. No guarantees of token value, protocol revenue, or user adoption are expressed or implied. By participating, you acknowledge these risks and accept full responsibility for your decisions.

JOIN THE PROTOCOL

Built for the next billion relationships.

BTRFLY is the first dating protocol designed for a Web3-native world — where identity is cryptographic, data is user-owned, and communities govern their own experience. The ICO opens Q3 2026.

btrfly.app

ICO Q3 2026 · $9.1M TARGET · $70M FDV