MySocial

A Peer-to-Peer Social Attention Economy

The Social Proof Foundation, LLC.

May 2, 2025

Abstract

MySocial is delivering a new social financial framework in which users' social attention is rewarded through economic incentives. As a purpose-built Layer-1 blockchain, MySocial uses permissionless cryptography and decentralization to ensure that users control their content and creators get fairly paid. Instead of the traditional social model where companies profit by selling user data, MySocial enables a direct path for value to flow back to the creators and communities that make the platform thrive. MySocial is powered by a consensus model based on Byzantine fault tolerance algorithms, ensuring high security, low latency, and fault resistance even under adverse network conditions. The socioeconomic framework is anchored by an automatic market maker (AMM) that uses a quadratic bonding curve for a new type of token called a Social Proof Token (SPT). The SPT design enforces a fair token distribution, prevents early manipulation, and establishes a healthy, stable social economy. The framework ensures an equal playing field where participants can confidently build and invest while eliminating the risk of rug pulls or inequitable concentration of power. Together, these innovations provide the technical and economic strength necessary to sustain a fully decentralized, user-owned social network at global scale.

Contents

Introduction

We have always been told that users are the product of social networks. Our attention, our creativity, and our data became commodities for corporations to sell, while we were left with nothing. MySocial changes that by empowering individuals to own the value they create and to be compensated for the impact they generate. Through decentralization and cryptographic security, MySocial establishes a new social architecture where the rewards stay with the creators, the communities grow stronger, and the foundation of digital interaction becomes more sustainable, fair, and free.

MySocial offers a new approach by flipping the traditional social network model upside down, shifting power from corporations to creators and communities. At the core of this system is the MySocial (MySo) token, the native asset that powers transactions, governance, and network fees. Alongside it, the Social Proof Token (SPT) introduces a new asset class designed to ensure fair distribution, equal tokenomics, and trust across all ecosystems. Together, these tokens ensure that ownership, governance, and economic rewards remain within the community, forging a stronger, more sustainable foundation for digital interaction.

MySocial promotes a dual growth strategy by leveraging the psychology of the social network effect along with an economic system that rewards participation and creator support. Every interaction strengthens both the community and its financial foundation, creating a self-sustaining ecosystem where growth and value move together. This model builds a more fair and more resilient social economy unlike anything we have seen before.

MySocial is more than just a new blockchain or a social app. It is the foundation for a new kind of digital economy where creativity, ownership, and financial opportunity are tightly connected and owned by the community itself.

1 Tokenomics

1.1 MySo Token Specifications

The MySo token is the native utility asset of the MySocial blockchain. It serves as the core unit of value for transaction fees, governance participation, staking rewards, and liquidity provisioning. The total supply is capped immutably at 1 billion tokens, ensuring no future inflation. Token standards follow custom Move modules tailored for high-throughput decentralized environments, leveraging Byzantine fault-tolerant consensus for secure validation.

Token Allocation:

- Community Incentives: 51%
- Social Proof Foundation Treasury: 24%

- Pre-sale and Marketing: 12.5%
- Core Contributors: 12.5%

1.2 Economic Model

The MySocial economy is fundamentally deflationary. No new tokens will ever be minted beyond the initial 1 billion supply. Token holders retain full custody and freedom of their assets without lockups, ensuring a community governed purely by conviction rather than coercion. Incentives are structured around active participation: staking yields, governance voting, ecosystem grants, and community-driven initiatives. This sustainable economic design prioritizes long-term value capture by aligning the growth of the network with the scarcity of the token.

1.3 Pre-Sale Analysis

The MySo token pre-sale was conducted on Base network across three phases:

- Phase 1: January 23rd, 2025 – January 30th, 2025
- Phase 2: February 6th, 2025 – February 13th, 2025
- Phase 3: February 20th, 2025 – February 27th, 2025

Token Contract: 0xFdD6013Bf2757018D8c087244f03e5a521B2d3B7

Throughout the pre-sale, $ 13,240.13 was raised, distributing roughly 5 million MySo tokens at an average price of $ 0.00265 per token. All participants received a 25% bonus. The token was subsequently listed on Uniswap on April 24th, 2025, with $ 6,620.06 allocated to initial liquidity provisioning; the remainder supported server infrastructure and ongoing R&D.

At the time of this writing, 7,245,539.36 MySo tokens are in circulation, accounting for only 0.72% of the total supply. Due to the lower-than-anticipated pre-sale volume, MySocial is strategically expanding the circulating supply through onboarding incentives, social verification rewards, airdrops, and community sharing programs. Unsold pre-sale tokens earmarked for marketing have been reallocated to support these initiatives, ensuring gradual distribution without flooding the market.

1.4 Social Proof Tokens

Complementing the MySo token is the introduction of the Social Proof Token (SPT), a new asset class designed to restore trust in tokenized ecosystems by enforcing transparent, rules-based value creation tied directly to a user's social

presence. Operating under a permissionless quadratic bonding curve formula, SPTs ensure fair distribution without centralized control, consistent tokenomic structure across all users, and strong incentives for authentic engagement and network growth.

The current default parameters of Social Proof Tokens (SPTs) enforce a rug-pull resistant economic design. Creators or content owners do not own or pre-mint any portion of their token supply. Instead, they collect a transaction fee on trades, currently set at 1% per buy and sell. This ensures that their success is tied directly to ongoing engagement rather than initial speculation.

Key safeguards include:

- Maximum Individual Purchase Cap: No single user can purchase more than 5% of a token's total supply, preventing whales from dominating or manipulating markets.
- Fair Launch Cliff: Upon deployment, a mandatory one-hour pre-sale cliff establishes an even playing field for all buyers, reducing early sniping and manipulation before true price discovery begins.
- Threshold-Based Minting: Content and creator profiles must meet a minimum threshold of engagement before minting an SPT, ensuring only verified and active users participate. Profile-issued tokens may have reduced bonding curve scales relative to content tokens to reflect their auxiliary role.

By utilizing Social Proof Tokens (SPTs), creators and communities can build micro-economies based on authentic social impact, enabling a trust-first, manipulation-resistant environment where attention translates to fair economic opportunity. The SPT framework is a fundamental pillar of MySocial's mission to create a decentralized, sustainable, and fairer digital society.

2 Validators and Staking

2.1 Validator Role and System Overview

Validators on MySocial are responsible for securing the network, processing transactions, and maintaining consensus through a delegated proof-of-stake system. Validators operate independently but coordinate using Byzantine fault-tolerant mechanisms to guarantee safety, liveness, and high throughput without compromising decentralization.

The MySocial blockchain progresses through epochs. Each epoch is governed by a validator committee whose membership and stake distribution are determined at the start of the epoch through community delegation. Validators participate in transaction consensus, checkpointing, and network governance activities. Validators are required to provide both availability and correctness

guarantees. A quorum of greater than two-thirds of the total delegated stake is necessary to ensure network safety.

2.2 Consensus and Execution Model

MySocial employs a dual consensus system. For owned and read-only objects, validators use a Byzantine consistent broadcast protocol, enabling rapid processing without the overhead of full consensus. For shared objects that require global consistency, validators engage a high-throughput DAG-based consensus mechanism optimized for parallelism and reduced latency.

MySocial employs a hybrid execution and agreement model. For transactions involving owned or read-only objects, validators use a Byzantine consistent broadcast protocol, allowing for low-latency processing without engaging global consensus. For shared objects that require coordination across validators, MySocial uses a high-throughput DAG-based consensus protocol that ensures atomic sequencing and consistency across conflicting transactions.

Transactions are divided into two phases:

- Locking phase: Validators acquire object version locks without global coordination, enabling horizontal scalability.
- Execution phase: Once object versions are locked, transactions are executed independently and their effects are committed.

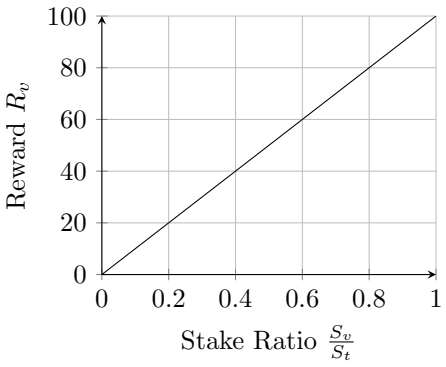
This separation between broadcast, consensus, and execution enables MySocial to achieve parallel transaction processing and low-latency finality, while scaling validator performance with minimal coordination overhead.

2.3 Staking and Delegation

To formalize the staking reward distribution, MySocial defines the reward for a validator in an epoch as:

$$R_v = \frac{S_v}{S_t} \cdot R_t$$

where S_v is the stake delegated to a validator, S_t is the total stake across all validators, and R_t is the total rewards for the epoch.



Delegators receive rewards proportionally to their contribution to, net of any validator commission fees.

Holders of the MySo token participate in network security by delegating their tokens to validators. Delegation is flexible, allowing participants to choose validators based on performance, reputation, and governance alignment. Delegated tokens remain fully owned by the users, and rewards are proportionally distributed based on validator performance and total stake.

Validators earn staking rewards through:

- Transaction fee sharing
- Participation in checkpointing and consensus
- Contribution to overall network stability

A portion of transaction fees is automatically distributed to validators and their respective delegators at the conclusion of each epoch.

2.4 Epoch Transitions and Validator Rotation

In MySocial, epochs are finite periods during which a fixed validator set operates the network. The voting power of the validator during each epoch is proportional to their delegated stake. At the end of an epoch, committee membership is re-evaluated based on changes in stake distribution. This allows the validator set to dynamically evolve, optimizing for performance and ensuring alignment with delegator preferences.

- Validator performance metrics are evaluated
- Delegators can reallocate their stakes
- New validators may enter or existing ones may exit based on stake changes

Validators with insufficient performance or stake may be removed, and new validators can join the committee if they meet staking thresholds, ensuring continuous optimization of network performance. Epoch transitions are secured by certified checkpoints created through validator consensus, preserving the safety and finality of transactions across committee reconfigurations.

2.5 Rewards and Economic Alignment

Validator incentives reinforce network health, performance, and decentralization. Each epoch distributes transaction fees and additional network emissions to validators based on their stake-weighted contribution. Validators then share rewards proportionally with their delegators. Validators that fail to meet participation or uptime requirements risk losing rewards for the epoch, incentivizing continuous high performance and reliability.

2.6 Light Clients and Trust Minimization

MySocial supports trust-minimized light clients that verify state transitions without downloading the full blockchain history. Validators provide cryptographically authenticated data to light clients, enabling secure and efficient verification of transaction finality. This feature ensures accessibility and scalability for users who do not operate full validator nodes but wish to interact with the network securely.

3 DAO Governance Model

3.1 Decentralized Governance Framework

The MySocial blockchain operates under a decentralized governance framework embedded entirely on-chain. Governance responsibilities are distributed across a structured system consisting of the Ecosystem DAO, optional Platform DAOs, and specialized governance committees. Token holders possessing at least one MySo token are eligible to participate directly in voting processes. Governance is enforced through smart contract rules that guarantee transparency, immutability, and fairness.

There are four main governance domains:

- Ecosystem Governance: Oversees platform-wide upgrades, economic parameters, and strategic initiatives.
- Reputation Governance: Manages social trust scoring, user reputation algorithms, and moderation standards.
- Intellectual Property Governance: Handles Proof-of-Creativity ownership disputes and intellectual property claims.
- Community Notes Governance: Supports decentralized fact-checking and content annotation systems.

3.2 Proposal Lifecycle

1. Community Proposal Submission: Any user may submit a governance proposal by providing a well-formed, evidence-backed argument aligned with MySocial's core values. To discourage spam, a minimum submission fee is required. This fee is refunded automatically if the proposal does not pass delegate review and is not escalated to a community vote.
2. Delegate Review Stage: Delegates, elected by the community and meeting minimum staking requirements, review incoming proposals. Delegates have the authority to accept or reject proposals based on alignment with ecosystem objectives. This mirrors a representative model similar to a

congressional review system. Delegates act independently based on their community mandate.

3. Community Voting Stage: If a proposal is accepted by the delegate review, it advances to a full community vote. All eligible token holders (users holding one or more MySo tokens) may cast one vote per proposal. A proposal passes based on quorum and majority thresholds defined within the governance contracts.

This structure ensures that only vetted, coherent proposals reach public voting, while preserving universal suffrage and direct participation for final decision-making.

3.3 Delegate System and Responsibilities

Delegates serve as the critical link between the broader community and the governance process. Participation as a delegate requires meeting a minimum MySo token threshold set by the protocol and securing majority support through a formal community vote. Once registered, delegates are expected to remain active in all governance procedures, including regular voting and proposal review.

Each delegate carries the responsibility of vetting incoming proposals for legitimacy, coherence, and alignment with the long-term goals of the ecosystem. They have the authority to approve or reject proposals before they are escalated to a full community vote. As part of this duty, delegates must maintain transparency by publicly communicating their rationale behind major decisions. This ensures that their performance can be openly assessed by the users they represent.

Delegates can be removed from their position if they repeatedly fail to participate in required governance activities or if the community votes for their dismissal through a delegate removal proposal. At any point during a delegate's active term, their profile is associated with a live like or dislike vote count, which reflects ongoing community sentiment. This public feedback mechanism enables users to express their trust or dissatisfaction continuously, without waiting for the end of a term.

At the conclusion of each term, which is defined dynamically by governance parameters, the current roster of delegates is re-evaluated. Delegates with high community disapproval or weak engagement may be replaced by pending candidates from the delegate pool. This dynamic structure ensures that representation remains accountable, performance-driven, and closely aligned with the evolving interests of the community.

3.4 Platform DAO Creation

MySocial supports the creation of optional Platform DAOs. When a new social platform is launched on MySocial, the developer may choose to establish a

Platform DAO to govern the platform's specific policies, content standards, monetization strategies, and ecosystem incentives.

Platform DAOs operate independently under the broader Core DAO structure but can define their proposal standards, voting thresholds, and governance policies tailored to their community's needs. This modular governance model allows flexibility without compromising the integrity of the core network.

3.5 Proof-of-Creativity and Dispute Governance

The Proof-of-Creativity framework within MySocial is a fundamental advancement in protecting the rightful ownership of digital content. It establishes an on-chain method to verify the originality of user-generated content by cryptographically linking submissions to creators at the time of creation. Rather than relying on traditional third-party arbitration or centralized platforms, Proof-of-Creativity shifts authority directly to the network.

When users submit content, they can optionally anchor their work by generating a content proof composed of metadata, timestamps, and cryptographic hashes. This proof establishes an immutable claim to authorship. If a dispute arises over ownership, any party can initiate a challenge by submitting competing proofs. The protocol then triggers a decentralized dispute resolution process.

Disputes are evaluated by the DAO through an open voting process in which users review competing claims and supporting evidence. Users cast votes to determine their rightful ownership, with rewards distributed to those who vote correctly according to the final consensus. Additionally, AI-powered bots may act as key proponents within the delegate system to assist in vetting disputed content and ensuring evidence is fairly presented. This decentralized system ensures that ownership is determined transparently, without relying on centralized authorities or traditional intermediaries.

This mechanism ensures that creators have an enforceable economic and cryptographic claim over their original work. It fosters an environment where content authenticity is verifiable and rewardable without centralized gatekeepers. By linking attention, attribution, and rewards, Proof-of-Creativity redefines intellectual property enforcement for decentralized ecosystems, protecting creators while promoting broader community trust and engagement.

4 Technical Architecture

4.1 Consensus Mechanism

MySocial utilizes a high-throughput DAG-based consensus architecture composed of two distinct layers. Narwhal[1] serves as the transaction dissemination and data availability layer, ensuring reliable propagation and cryptographic storage of

transaction certificates across the validator set. Built atop Narwhal, Tusk acts as the consensus engine, sequencing certificates into a globally agreed ledger under a Byzantine fault-tolerant protocol. This separation between data availability and consensus ordering enables parallelism, scalability, and low-latency finality, even under adversarial conditions. Tusk guarantees both safety and liveness under partial synchrony, tolerating up to one-third of Byzantine validators.

The execution model distinguishes between two classes of transactions: those involving exclusively owned or read-only objects, and those involving shared objects. Transactions on owned or read-only objects bypass full consensus and instead rely on a Byzantine consistent broadcast protocol, allowing validators to independently process and commit them based on client-signed transaction effects. This approach significantly reduces coordination overhead and latency for common operations. In contrast, transactions involving shared objects must be globally ordered to preserve consistency. These transactions are sequenced through Tusk consensus after certificate broadcast through Narwhal, ensuring deterministic and atomic execution across authorities.

Transaction finality time depends on this bifurcated model. It can be expressed as:

$$T_f = \begin{cases} T_b + T_e & \text{(owned/read-only objects)} \\ T_d + T_c + T_e & \text{(shared objects)} \end{cases}$$

where T_f is the transaction finality time, T_b is the latency of Byzantine broadcast, T_d is Narwhal data availability time, T_c is Tusk consensus ordering time, and T_e is the execution latency of the transaction.

This hybrid execution and consensus model is foundational to MySocial's scalability and performance. By minimizing the use of global consensus and embracing object-centric parallelism, MySocial inherits the ability to process many transactions concurrently without introducing bottlenecks or compromising safety.

4.2 Networking and Nodes

MySocial's network topology consists of validator nodes, full nodes, and light clients. Validators form the core consensus committee, proposing and validating transaction certificates. Full nodes maintain a full replica of the ledger and serve transaction requests without participating in consensus. Light clients verify transaction finality and account state proofs through validator signed checkpoints without maintaining full ledger history.

The transaction validation lifecycle progresses through the following stages: users submit transactions to validators, validators batch and broadcast transactions via Narwhal[1], validators collaboratively order transactions through

Tusk consensus, and once finalized, validators execute transactions and produce certified state changes.

Let n be the total number of validators. The minimum quorum required for safety under Byzantine fault assumptions is given by:

$$q = \left\lceil \frac{2n}{3} \right\rceil$$

where n is the total number of validators, and q is the minimum quorum required to maintain safety under Byzantine fault assumptions. This threshold ensures that no minority coalition can disrupt finality or data availability.

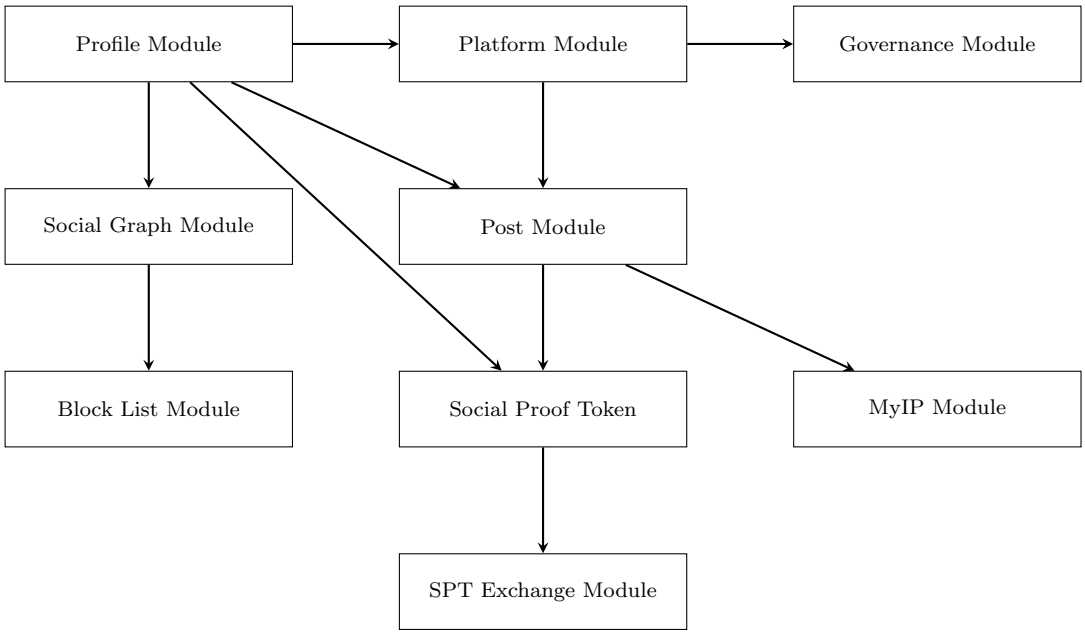
4.3 Move Smart Contract Language

The Move programming language underpins MySocial's execution environment. Move provides formal resource safety, deterministic execution, and strong access control semantics. Unlike traditional smart contract languages, Move enforces that digital assets cannot be implicitly copied or discarded, drastically reducing the attack surface for vulnerabilities such as reentrancy and integer overflow.

Custom extensions to Move have been developed to support social media-specific primitives, including profile objects, post metadata, reaction tracking, encrypted content payloads, and user moderation rights. MySocial maintains a closed smart contract environment, where only protocol-level modules are permitted and general third-party contract publishing is restricted. This controlled design prevents arbitrary contract risks, enforces system coherence, and allows social structures and interactions to be defined natively at the protocol level with verifiable guarantees of authenticity and ownership.

4.4 Core Social Features

MySocial's protocol defines a modular hierarchy that governs every aspect of social interaction, content creation, and user governance natively at the blockchain level.



Profiles serve as the foundation of the user identity system. Each profile is immutable once created, with attached usernames that cannot be altered, and only one profile may be associated with each wallet. Profile ownership can be transferred through asset sales, allowing high-value usernames or accounts with substantial followings to be exchanged. However, content such as posts or social interactions are not transferred with the sale of a profile, preserving the distinction between identity and authored history.

Posts represent independent content objects linked to wallets. Users can create posts, comments, sub-posts, sub-comments, reactions, re-posts, and quote-reposts. Each action submits a new transaction to the blockchain, ensuring a verifiable, on-chain record of engagement.

The social graph module maintains user relationships, including following and followers. It enables traversal and querying of the social topology through indexers and RPC services, forming the basis for future recommendation engines and reputation models built atop off-chain infrastructure.

Intellectual property and content authenticity are protected through the Proof-of-Creativity framework. Users can anchor proofs of authorship, file claims on disputed works, and resolve ownership challenges through decentralized community voting.

The Platform Module anchors individual social networks within MySocial, each with its own treasury, optional DAO, and governance rules. These platforms can define localized policies for moderation, monetization, and incentives without altering the global ledger. Treasury balances are held at the platform level and governed through on-chain voting, enabling communities to fund growth, rewards, or contributor efforts.

Content access controls are enforced through encrypted storage references that allow users to selectively share posts or media assets with chosen audiences, leveraging on-chain encryption key management.

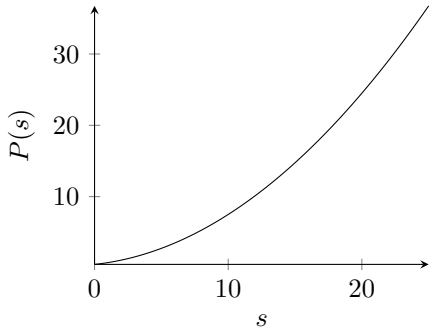
All social modules are integrated into a cohesive architecture that ensures user rights, social mobility, and platform neutrality are protected by verifiable, censorship-resistant smart contracts.

4.5 SPT Exchange and AMM Bonding Curve

MySocial implements a decentralized quadratic bonding curve mechanism for the minting of Social Proof Tokens. The AMM pricing logic is embedded at the protocol level through programmable logic, ensuring real-time price discovery without centralized intermediaries.

$$P(s) = as^2 + bs + c$$

where $P(s)$ is the token price based on supply s, and a, b, and c are curve constants that determine the slope and curvature of the function.



Each token purchase or sale dynamically updates the bonding curve state, ensuring real-time liquidity provision without relying on centralized order books or custodians. This model requires no fixed token supply caps where issuance is determined entirely by initial and ongoing demand, allowing tokens to be created and redeemed seamlessly as interest fluctuates.

This demand-driven framework provides a universal, rug-pull-resistant tokenomics system that enforces fairness at the contract level. Because creators cannot pre-mint or withdraw liquidity from their bonding curves, all value flow is on-chain and permissionless. Dynamic curve parameters such as slope, spread, and fees are governed by the DAO, enabling real-time tuning based on network feedback and evolving market conditions.

By embedding AMM logic directly into the smart contract layer, MySocial guarantees transparent, censorship-resistant trading for Social Proof Tokens, providing users with native access to fair, auditable market dynamics that reward authentic social engagement.

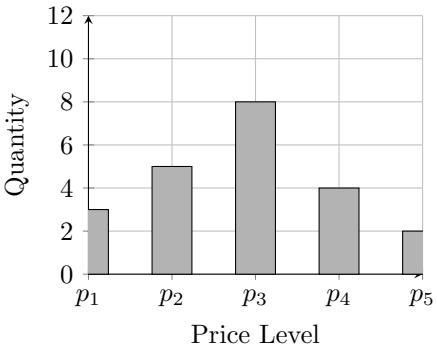
4.6 Order Book Execution for Protocol-Level Assets

The MySocial protocol includes a deterministic, on-chain central limit order book (CLOB) implementation to support high-throughput trading for core ecosystem assets. This order book is reserved exclusively for protocol-level assets such as MySo, USDC, Ethereum, and Bitcoin, and is not used for Social Proof Token markets.

The matching engine operates using price-time priority across a globally shared order state. Users may submit limit and market orders, with execution occurring via validator-submitted transactions that directly mutate the order book state. Each order action, match event, or cancellation emits structured transaction logs that can be consumed by indexers or clients to reconstruct full depth-of-book state in real time.

$$F = \min(Q_o, Q_b)$$

where F is the matched fill amount, Q_o is the quantity on the incoming order, and Q_b is the quantity at the top of book. Matching iterates until the incoming order is fully filled or no valid price levels remain.



The CLOB module is implemented entirely in Move with configurable parameters for tick size, fee logic, execution latency constraints, and event granularity. Matching occurs deterministically within a validator-executed call path, enabling transparent settlement and reproducibility across nodes without requiring external relays or trusted off-chain sequencers.

The order book exists to facilitate deep liquidity entry and exit points for ecosystem-native and bridged assets. Social Proof Tokens, by contrast, are exclusively traded through quadratic bonding curve AMMs, which remain the dominant and intended market mechanism within the network. The two systems are complementary: the AMM layer supports long-tail creator economies and issuance-linked pricing, while the order book enables price formation and aggregation for assets with cross-chain velocity and external demand.

4.7 Cross-Chain Bridging and Interoperability

To extend the reach and liquidity of the MySocial ecosystem, a native trust-minimized bridging protocol enables secure asset migration between MySocial and external chains such as Ethereum. This bridge architecture relies on validator-signed checkpoints, cryptographic proofs, and deterministic transaction verification to prevent spoofing or double spends.

MySo tokens and USDC are supported for cross-chain transfers, with planned expansion to additional major assets including USDT, Bitcoin, Ethereum, Solana, and Cardano. These assets can be locked and mirrored as wrapped tokens on MySocial. Once wrapped, they behave identically to native tokens, supporting all system functions including trading, staking, and governance. When users burn a wrapped asset, the original is unlocked on its originating chain.

This bridging layer is implemented using modular Move smart contracts, enabling developers to define custom routing logic, asset types, and transfer conditions. It serves as the foundation for MySocial's multi-chain architecture, allowing creators and users to engage seamlessly across diverse blockchain ecosystems.

5 Social and Economic Incentives

5.1 Monetization Pathways

MySocial provides direct monetization opportunities for users through decentralized, verifiable mechanisms. Users can generate revenue through Social Proof Token trading, tipping systems, subscription models, profile sales, and Proof-of-Creativity dispute voting. Validators and delegators also earn rewards directly from transaction fee distributions and network staking incentives. Economic value is captured transparently through user-driven market actions and validator node operations.

5.2 Content Creation Incentives

Content creators are incentivized to produce unique, high-value material by being able to mint Social Proof Tokens tied to verified engagement thresholds. Posts themselves may generate attention, but do not carry intrinsic monetary rewards unless tied to active token economies such as tipping or associated Social Proof Token issuance. Content remains individually owned and monetizable based on user-driven market demand rather than platform-sponsored incentive schemes.

Profile ownership, reputation, and follower base can increase profile market value, enabling users to sell profiles as transferable assets without transferring the original content history. Profiles serve as scarce identity anchors that can be appreciated based on social impact and network recognition.

5.3 Reputation Scoring and Moderation Incentives

Reputation within MySocial affects social standing, but does not by itself, yield direct monetary rewards. However, maintaining a strong reputation can increase

visibility, trust, and market value for profile-based monetization strategies.

Moderators and community participants engaged in Proof-of-Creativity disputes and platform governance proposals can earn economic rewards through participation fees and dispute voting outcomes. Validators remain the primary recipients of transaction fees, and staking participants earn proportionate yields based on delegation performance.

MySocial's social and economic framework prioritizes transparency, verifiability, and user ownership without artificial inflationary mechanisms, creating a resilient and merit-based digital economy.

6 Use Cases and Real World Applications

MySocial provides the infrastructure for developers to build decentralized social platforms that prioritize user ownership, transparency, and long-term sustainability. The protocol supports programmable identity, on-chain content ownership, and integrated monetization mechanisms, giving builders the foundational tools to create applications that are governed and operated by the communities that use them.

Developers can launch text-based social networks that support real-time interaction, native tipping, and reputation models that are transparent and verifiable on-chain. In an era where trust in mainstream media and corporate platforms continues to erode, MySocial enables systems where speech, identity, and influence are rooted in proof rather than centralized curation. Media platforms for videos, music, or imagery can be designed to combat piracy and content theft through wallet-based licensing and cryptographic attribution. Article based applications can introduce token-backed fact verification and community curated truth scoring, building an ecosystem where accurate reporting is rewarded and misinformation has a cost. Developers can also build prediction markets grounded in identity and trust, allowing users to express collective sentiment without the manipulative friction of intermediaries or traditional gambling systems.

These examples illustrate how MySocial enables a shift away from centralized Web2 infrastructure toward open, economically aligned ecosystems where users govern, build, and benefit from the platforms they rely on.

7 Security and Auditing

7.1 Move Language Security Framework

MySocial utilizes the Move programming language developed by Meta in 2018. Move treats digital assets as first-class resources and applies strict rules around

how they are created, owned, and transferred. These restrictions ensure that assets cannot be duplicated, destroyed, or moved without explicit authorization.

Move's linear type system and module-level encapsulation provide strong guarantees for memory safety and resource correctness. All asset behavior is scoped to the rules of its module, preventing unauthorized interactions across trust boundaries. The language enforces deterministic execution and strict access control, eliminating vulnerabilities common in general-purpose platforms.

Transactions in Move are isolated, verifiable, and deterministic. State transitions are confined to clearly defined modules, and modifications require proper authority. Runtime checks and rollback mechanisms ensure that any transaction failing safety guarantees is automatically reverted, preserving the integrity of on-chain operations.

7.2 Threat Modeling and Protocol-Level Mitigations

MySocial applies a multi-layered threat model that prioritizes determinism, access control, and validator integrity. Every transaction must reference authorized objects and is subject to deterministic validation, reducing exposure to unpredictable side effects and race conditions.

Smart contract access is strictly regulated through a capability-based permission model. Each module is isolated and must pass on-chain verification for memory safety, type constraints, and resource integrity. Unauthorized mutation or privilege escalation is structurally prevented.

Key components of the system undergo formal verification and testing. Protections such as replay prevention, transaction sequencing, gas metering, and execution bounding guard against denial-of-service attacks and runtime abuse. Transaction effects are atomic and only finalized upon consensus, ensuring that state transitions are consistent, secure, and recoverable.

Together, these layers form a robust security architecture where trust is enforced by code, not intermediaries. MySocial ensures that every interaction is safe by design, verifiable on-chain, and resistant to manipulation at every level of the protocol.

8 Roadmap and Project Timeline

MySocial is advancing through a structured development roadmap designed to replace legacy social networks with decentralized, creator-first infrastructure. The protocol's trajectory reflects rapid technical execution paired with long-term ecosystem alignment.

8.1 Achieved Milestones

- Pre-sale Campaign: MySocial conducted a phased public pre-sale between January and February 2025, successfully onboarding early supporters and distributing over 5 million MySo tokens. More details available at www.mysocial.network/pre-sale.
- Uniswap Token Launch: The MySo token was deployed on Uniswap on April 24, 2025, marking the first public market availability of the asset.
- Public Testnet Launch: MySocial's testnet was made public to developers and early users, featuring core infrastructure such as staking, profile minting, post creation, and validator onboarding.

8.2 Short-Term Roadmap

- Testnet Expansion: Release of the MySocial testnet faucet, CLI tools, SDKs, APIs, and community-driven feedback integrations.
- zkLogin Integration: Rollout of MySocial's zkLogin prover system, allowing users to onboard with traditional Web2 OAuth providers while maintaining full non-custodial control of their cryptographic keys. This feature simplifies access while preserving decentralization and privacy.
- Sponsored Gas: Implementation of sponsored gas features to improve accessibility and encourage onboarding through fee abstraction.
- Bridge Deployment: Rollout of a trust-minimized bridge for asset migration between MySocial and compatible chains like Ethereum.
- Mainnet Launch: Scheduled deployment of the MySocial mainnet, complete with multiple validators and staking.

8.3 Medium and Long-Term Roadmap

- Ecosystem Growth Initiatives: Grants, hackathons, and builder support programs to accelerate third-party development on the protocol.
- Proof-of-Creativity Modules: Launch of the decentralized authorship verification system to anchor content provenance and dispute resolution.
- Ad Monetization Infrastructure: Rollout of user-controlled ad rails with transparent revenue flows directly for the viewer and platform.
- Autonomous Agents and AI Moderation: Integration of intelligent agents to assist with moderation, identity scoring, and content curation at scale.

9 Future Development and Technical Enhancements

MySocial's core protocol is designed with performance scalability and modular extensibility in mind. Several technical upgrades aim to position the network for long-term decentralization and global throughput.

9.1 Rorqual: TEE-Enhanced DAG Consensus

Rorqual[3] is a consensus-layer enhancement that integrates Trusted Execution Environments (TEEs) into the DAG-based Narwhal[1] mempool architecture. By leveraging TEEs, Rorqual streamlines the process of incorporating vertices into the DAG, reducing communication complexity and achieving significant reductions in latency while increasing throughput. This integration allows for more efficient block production without compromising security or decentralization.

Incorporating Rorqual[3] into MySocial's consensus protocol will enhance validator throughput and transaction parallelism. The use of TEEs enables secure and efficient processing of transactions, minimizing the risk of Miner Extractable Value (MEV) attacks and ensuring robust performance even under adversarial conditions.

9.2 Shoal++: Advanced DAG-Based BFT Consensus

Shoal++[2] is a next-generation DAG-based Byzantine Fault Tolerant consensus protocol that significantly enhances both throughput and latency. MySocial is integrating Shoal++ as a core upgrade to its existing consensus layer, replacing legacy consensus bottlenecks with a more scalable, responsive, and efficient system.

Shoal++ introduces fast anchors, allowing validators to commit earlier by observing 2f+1 uncertified proposals, reducing commit latency from six to four message delays. All nodes are treated as anchors, and multiple Bullshark instances operate in parallel to eliminate commit bottlenecks. Shoal++ also staggers multiple DAGs, reducing queuing latency from 1.5 to 0.5 message delays. These innovations enable consistent sub-second finality at high transaction volumes.

By adopting Shoal++, MySocial increases validator performance during high-load periods while preserving safety and composability. The protocol's dynamic scheduler and conflict resolution mechanisms support parallel transaction execution without compromising consensus guarantees. This ensures that MySocial can scale securely while supporting millions of users and meeting the demands of decentralized social infrastructure.

9.3 Decentralized Media Storage and Content Provenance

As the volume of creator-generated media on MySocial scales, the need for decentralized, censorship-resistant, and verifiable media infrastructure becomes foundational to the long-term sustainability of the network. MySocial plans to implement a distributed content storage layer in which all media objects—images, videos, and audio—are referenced via deterministic content hashes and validated through cryptographic proofs. Each asset will be linked to immutable metadata stored on-chain, encoding authorship, timestamps, content fingerprints, and version history. This metadata will support trustless verification of ownership, enable reproducible attribution, and ensure consistent references across forks, re-uploads, or platform frontends.

To ensure long-term availability and resilience, media payloads will be redundantly stored across decentralized nodes using content-addressed blobs and chunked encoding mechanisms. These chunks will be organized within a Merkle tree structure, enabling efficient Proof-of-Retrievability[4], partial streaming, and cryptographic integrity without centralized indexing. Lightweight clients and indexers will be able to confirm file validity and access integrity proofs without needing to download or store the entire media file. This system reduces the burden of full-node storage while maintaining verifiable access to media assets across the network.

The decentralized storage layer is designed to operate in direct coordination with the existing Proof-of-Creativity and MyIP modules, which govern attribution, monetization, and creator rights. Together, these components form a vertically integrated media architecture capable of preserving originality, resisting tampering, and enabling a fully decentralized social publishing stack. This foundation supports not only media permanence, but also interoperable licensing, remixability, and downstream provenance, ensuring that creators retain control over their work at every step of the content lifecycle.

10 Conclusion

MySocial is not just a re-imagining of how social platforms function. It is an entirely new digital economy rooted in trust, ownership, and verifiable interaction. By architecting a blockchain tailored specifically for social media, it offers a platform where creators are no longer exploited, users are not commodified, and value is not siphoned upward into centralized corporations. Instead, every technical mechanism from bonding curves to validator staking is optimized to support a sustainable creator-first model that aligns economic incentives with community growth.

The protocol's foundation in the Move language and Byzantine fault-tolerant consensus ensures not only resilience and scalability, but also verifiability and safety at every level of the stack. Core primitives such as Social Proof Tokens, permissionless staking, and quadratic bonding curves empower users to monetize

their influence while preserving fair distribution and preventing manipulation. DAO based governance and Proof-of-Creativity mechanisms add additional layers of integrity and innovation to the system.

However, MySocial is not built for passive consumption. It is built for participation. Developers, creators, researchers, and validators each have an opportunity to shape the network's trajectory. Whether building social networks atop the MySocial stack, minting new Social Proof Tokens, or contributing to community governance, every action taken in the system strengthens the feedback loops between social capital and economic reward.

The centralized social media model is no longer sustainable. As users demand transparency, fairness, and direct ownership, the shift to decentralized infrastructure is inevitable. MySocial provides the foundation. What comes next is what we build together.

11 References

References

[1] George Danezis, Sam Blackshear, Kevin Qian, and Adeniyi Abiodun. *The Sui Whitepaper*. Mysten Labs, 2023. Available at: `https://docs.sui.io/paper/sui.pdf`

[2] Haoyu Zhang, Yang Zhang, Matei Zaharia, and Mohammad Alizadeh. *Shaarl++: High-Throughput DAG BFT Can Be Fast*. arXiv preprint arXiv:2408.14099, 2024. Available at: `https://arxiv.org/html/2408.14099v1`

[3] Kaituo Liu, Pedro Moreno-Sanchez, and Mahimna Kelkar. *Rorqual: Speeding Up Narwhal with TTEEs*. arXiv preprint arXiv:2405.20488, 2024. Available at: `https://arxiv.org/html/2405.20488v1`

[4] Alan Szepieniec and Maxim Orlovsky. *Walrus: Secure, Verifiable, and Decentralized Media Infrastructure*. WAL Protocol Whitepaper, 2023. Available at: `https://docs.wal.app/walrus.pdf`

[5] Mysten Labs. *Sui Developer Documentation*. Available at: `https://docs.sui.io/`

We are the network.