



Mudrika: A Tokenized Ecosystem for Stable Finance and Real-World Commitment.



1. Introduction

1.1 Abstract and Vision (MDK & Staking)

Cryptocurrency, despite its reach and innovation, remains the most uncertain market for investors. The expanding revolution of **stable digital assets** and asset-backed coins supports stability over speculative growth, creating scope for reliable payment systems and secure stores of value.

The Problem: Current decentralized staking models are often rigid. They reward short-term token holders with the same rates as committed long-term partners, leading to token churn and unstable network velocity. Furthermore, many stable digital assets lack transparent, dual-asset backing and a direct, verifiable utility in financing tangible economic growth.

The Solution: Mudrika (MDK) is a multi-chain stable digital asset pegged to the ₹1 INR equivalent. It achieves stability through a 1:1 reserve backing of crypto reserves (for immediate liquidity) and real-world securities/tangible assets (for fundamental, long-term stability). The core utility is the flexible, **NFT-tokenized staking system (MDK-SP)**, designed to reward genuine commitment. Reward rates (APY) scale based on the user's locked duration and stake size, with the purpose of deploying this locked capital to finance vetted real-world projects.

Project Vision: To establish MDK as India's premier stable digital asset for payments, remittances, and commerce, while leveraging its staking mechanism to incentivize long-term capital commitment, secure the network, and provide transparent funding for innovation and growth in the domestic economy.

1.2 Target Audience

The Mudrika ecosystem is designed for a diverse set of participants:

- **Long-Term MDK Holders:** Seeking optimized, predictable passive income streams and wishing to contribute to and fund real-world projects.
- **DeFi Participants:** Looking for high-yield, liquid, NFT-based staking positions that can be collateralized or traded.
- **Merchants and Users:** Requiring a stable, low-fee digital asset for commerce, payments, and global settlements.
- **Developers and Integrators:** Requiring a rich read-surface (Lens V3) for building high-utility dApps and tracking staking positions off-chain.

2. The Mudrika Stablecoin Ecosystem (MDK)

2.1 MDK Tokenomics and Stability

Parameter	Value	Rationale
Ticker	MDK	The native asset of the ecosystem.
Stability Goal	Pegged to ₹1 INR equivalent	Focuses on stability and utility for the domestic market.
Backing Mechanism	1:1 Reserve Backing	Dual liquidity pools: Crypto Reserves (e.g., stablecoins for digital stability) and Real-World Securities/Tangible Assets (for fundamental stability).
Primary Use Cases	Merchandising, Payments, Remittances, Staking	Provides high utility to anchor the token's value.

2.2 Transparency and Governance

Mudrika is built on the principle that "Trust is the currency, transparency is the ledger.

- **Treasury Governance:** Reserves are managed via transparent multi-sig wallets and are subject to mandatory, regular third-party audits. Real-time reporting mechanisms are utilized to ensure the community can verify the 1:1 backing ratio at any time.
- **Security & Scalability:** The platform emphasizes verifiable transactions and disclosed reserves. To maximize utility and reach, MDK features multi-chain bridging across EVM compatible chains, including Polygon, BSC, and Ethereum.

2.3 Revenue Streams and Holder Benefits

The protocol is designed for sustained economic health and direct holder value:

- **Protocol Revenue:** Generated from staking rewards, a portion of transaction fee allocations, and fees from future DeFi integrations.
- **Holder Value:** Beyond staking yield, holders benefit by staking in pools that finance real projects. This connection offers the potential to earn dividends tied to the success of those projects, allowing the community to contribute directly to innovation and the growth story of the domestic economy.

3. Core Mechanism: Staking Position NFT (MDK-SP)

3.1 The ERC-721 Position Token

Every individual staking transaction within the Mudrika protocol creates a unique ERC-721 NFT, known as a **Staking Position NFT (MDK-SP)**.

This NFT is a financial primitive that represents the staker's complete ownership of:

1. The original staked principal amount.
2. All accrued, unclaimed rewards.
3. The associated lock-up period and corresponding APY rate.

Benefits of Tokenization: This mechanism introduces **liquidity, composability, and transferability** to staked positions. Stakers can sell or collateralize their MDK-SP mid-lock, ensuring capital efficiency without compromising the original commitment.

The NFT metadata exposes critical on-chain data points, including the pid (Pool ID), amount (Principal), unlockAt (Timestamp), and pending rewards calculation data.

3.2 Position Management

Transfer: MDK-SP NFTs are fully transferable via the standard ERC-721 `safeTransferFrom()` function. The new owner inherits the principal, the remaining lock duration, and all accrued, unclaimed rewards.

Splitting: The contract supports a `split()` function, allowing a staker to divide a single large MDK-SP position into two smaller NFTs. To execute this, rewards must be settled and claimed before the split. The original NFT is burned, and two new NFTs are minted, each inheriting the original, immutable lock-up duration.

4. Adaptive Reward Model

The reward model is engineered to actively incentivize long-term commitment and is governed by high-precision, continuous accrual logic.

4.1 Per-Second Accumulator (The Index)

Rewards are calculated using a per-second accumulator index (known as `accRewardPerTokenX` or "The Index"). This index is scaled to 1027 to provide high precision and minimize rounding errors during calculations.

Continuous Accrual: The pool index grows continuously based on the pool's effective, real-time APY rate.

Reward Debt: When a user stakes, their position records a checkpoint known as `rewardDebtX` (calculated as $\text{amount} \times \text{current index} / X$). The claimable reward is the precisely calculated difference between the current index value and this recorded debt checkpoint.

4.2 Variable APY Structure

The protocol supports adaptive reward rates to reward long-term commitment. The contract supports three modes for customizing APY based on the user's committed lock duration (`commitmentDays`).

- **Base APY:** A minimum APY (e.g., 6%) defined by the pool configuration parameters (`apyBps`) serves as the floor.
- **Commitment Multiplier:** The final APY is determined by the length of the lock, according to one of the following modes:
 - **NONE (Flat Rate):** The APY remains strictly at the Base APY, regardless of the commitment length.
 - **LINEAR:** The APY scales linearly between the pool's minimum and maximum commitment days based on a defined slope (`linearSlopePerX1e4`).
 - **TABLE (Tiered):** The APY increases in distinct, pre-defined tiers. Specific `commitmentDays` (e.g., 90 days, 180 days) are mapped to unlock corresponding higher `apyBps` levels.

4.3 Claiming Rewards

Rewards are not automatically compounded or paid out.

Claim-on-Demand: Rewards are minted to the user only when they manually call one of the core transaction functions: `claim()`, `withdraw()`, or `split()`.

Minting: Rewards are minted directly via the `rewardMinter` interface (controlled by the MDK token contract or a dedicated module), ensuring secure, visible, and quantifiable inflation. This visibility helps manage the reward rate ($\text{total staked} \times \text{avg bps}$) with full transparency.

5. Operational & Economic Controls

5.1 Governance and Roles

The protocol utilizes OpenZeppelin's AccessControl to manage governance roles:

DEFAULT_ADMIN_ROLE: Holds the highest control, including the ability to set system-wide pause/unpause states and activate the Emergency Exit flag.

OPERATOR_ROLE (POOLS_MANAGER_ROLE): Manages pool configuration, including setting APY parameters, defining minimum/maximum stake days, and adjusting global/pool/user staking caps.

PAUSER_ROLE: A dedicated role for pausing the contract in extreme or critical security situations.

5.2 Capital Guardrails (Risk Mitigation)

To prevent economic instability and ensure sound protocol behavior, the contract employs specific guardrails:

- **Time Guards:** Enforce reasonable boundaries for staking periods (e.g., minimum 30 days, maximum 720 days).
- **APY Guards:** Enforce floor and ceiling boundaries for APY (e.g., minimum 6%, maximum 30%) to maintain financial viability.
- **Staking Caps:**
 - **Global Stake Cap:** A protocol-wide limit on the total MDK that can be staked.
 - **Pool Stake Cap:** A per-pool limit.
 - **User Stake Cap:** A per-user limit per pool, serving as an anti-sybil control.

5.3 Withdrawal and Exit Mechanics

Standard Withdrawal: Withdrawal requires the staked position to be unlocked (i.e., $\text{block.timestamp} \geq \text{unlockAt}$). The `withdraw()` function can be used for full withdrawal.

Partial Withdrawal: Allows stakers to retrieve a portion of their principal after the lock period has expired. The MDK-SP NFT is maintained, and the reward debt and lock remain active on the remaining principal.

Emergency Exit: An administrative flag (`emergencyExitEnabled`) allows stakers to bypass the lock-up period if activated. Policy: When exiting during an emergency, rewards for that position are not paid out; they are either slashed or discounted proportional to the remaining time left in the lock.

6. Security and Architecture

6.1 Technology Stack

To prevent economic instability and ensure sound protocol behavior, the contract employs specific guardrails:

Platform: EVM compatible chains (Polygon, BSC, Ethereum).

Framework: Solidity 0.8.x with battle-tested OpenZeppelin libraries for robust control mechanisms (AccessControl, Pausable) and security (ReentrancyGuard).

Accounting: The contract uses delta-received accounting (checking the change in contract balance after a transfer) to accurately handle staked tokens, even if the token has deflationary tax mechanics.

6.2 Architectural Principles

Checks-Effects-Interactions (CEI): All core functions adhere to the CEI pattern. Rewards are settled, and state variables are updated before any external token transfer or minting occurs, significantly reducing attack vectors.

Reentrancy Protection: Core transaction functions (stake, claim, withdraw, split) are protected by the nonReentrant guard to prevent one of the most common DeFi attack vectors.

Custom Errors: Utilization of Solidity custom errors (e.g., Locked(), GlobalCap()) instead of string reverts to optimize gas consumption upon failure.

7. Integration and Future Development

7.1 Lens V3 Read Surface

To maintain gas efficiency and keep the smart contract simple, the protocol relies on external indexing for tracking user positions.

Off-Chain Tracking: The contract removes in-contract enumeration logic, relying on services like The Graph or a dedicated Lens V3 contract to efficiently track all MDK-SP tokens owned by a specific address.

Event-Driven Data: Key information is emitted via standard ERC-721 Transfer events and custom events (Staked, Claimed, Split) for reliable off-chain data aggregation.

7.2 Future Roadmap

The Mudrika staking protocol is the foundational pillar for the broader ecosystem expansion:

Phase	Timeline	Milestones
Q1 2025	Foundation	Token launch, Treasury setup, Security Audit, Whitepaper v1 Release.
Q2 2025	Expansion	Multi-chain bridge, Merchant integration pilot, Staking V3 Launch.
Q3 2025	Innovation	Airgap Wallet support, Oracle-based DEX integration, DAO Voting live.
Q4 2025	Scaling	Rollup Chain Pilot, Exchange Listings, Global Partnerships established.
2026+	Growth	Industrial financing pools, RWA tokenization, Full DeFi integration.

“India is not just a market — it’s the engine of global growth.
Mudrika mirrors that rise: stable, strong, and global.”

Executive Summary: Mudrika Staking V3 Protocol

The Future of Stable Finance and Real-World Asset Commitment

The **Mudrika (MDK)** project introduces a pivotal solution to two primary challenges in the decentralized finance space: volatility and capital inefficiency. MDK is a multi-chain stable digital asset pegged to the ₹1 INR equivalent, distinguished by its 1:1 dual reserve backing—combining crypto liquidity with fundamental stability derived from real-world securities and tangible assets.

Core Value Proposition:

Mudrika is not just a payment token; it is a mechanism for channeling committed digital capital into the domestic real economy.

Pillar	Description
Stability & Backing	MDK is ₹1 INR-pegged, utilizing transparent multi-sig wallets and mandatory third-party audits to verify the 1:1 backing of crypto reserves and real-world assets.
The Problem Solved	Eliminates token churn and rewards rigidity by moving away from flat-rate staking models.
Real-World Utility	Staked MDK is explicitly earmarked to finance vetted real-world projects, offering holders the potential to earn dividends tied to project success.

Key Innovation: Tokenized Staking (MDK-SP)

The core innovation is the **NFT-tokenized staking system (MDK-SP)**. Every staking commitment generates a unique ERC-721 NFT, representing the staked principal, the original lock duration, and all accrued, unclaimed rewards.

- **Liquidity and Composability:** This tokenization transforms a traditionally locked asset into a **liquid financial primitive**. Holders can sell or collateralize their MDK-SP NFT mid-lock, ensuring capital efficiency without breaking the original commitment.
- **Adaptive Reward Model:** Rewards are calculated using a high-precision **per-second accumulator index**. The Annual Percentage Yield (**APY**) is not flat; it scales adaptively based on the user's committed lock duration, governed by **LINEAR or TABLE** (Tiered) modes to actively incentivize long-term partnership.

Economic and Operational Control

The protocol is secured by robust capital guardrails and OpenZeppelin framework controls:

Risk Mitigation: Time, APY, and Staking Caps (Global, Pool, and User) are implemented to prevent economic instability.

Withdrawal Policy: Withdrawal is standard after the lock period, but an administrative Emergency Exit flag allows users to bypass the lock (with the policy that accrued rewards are slashed or discounted upon emergency withdrawal).

Governance: Utilizes DEFAULT_ADMIN_ROLE and OPERATOR_ROLE to manage configuration and ensure security, with future plans to transition key decisions to DAO governance.

Conclusion

Mudrika is positioned to become India's premier stable digital asset by blending financial stability with DeFi innovation. The MDK-SP protocol transforms locked staking from a static commitment into a liquid, high-yield investment vehicle that fuels tangible economic growth. This scalable architecture, supported by EVM compatibility and a transparent read-surface (Lens V3), paves the way for global partnerships and the next generation of asset-backed finance.

“India is not just a market — it’s the engine of global growth.
Mudrika mirrors that rise: stable, strong, and global.”

Appendix — Contact & Community

 www.mudra.ink

 info@mudra.ink | partners@mudra.ink

 Follow us on Twitter · Telegram · LinkedIn · Facebook (@MudrikaToken)