# VeraMoney: Building a Sanctuary of Security in Web3 Finance

**Abstract** *VeraMoney is a community-driven crypto project designed around the principles of peace, security, and decentralized trust. With its symbolic monk figure as the guiding archetype, Vera aims to reshape how the world perceives digital finance—less as speculation, more as a conscious movement. Unlike many tokens that prioritize hype and rapid market gains, Vera distinguishes itself by integrating philosophical values with utility-driven design, including staking, governance, and a focus on long-term ecosystem tools.*

*The name VeraMoney is derived from the Sanskrit word veramani, meaning "to refrain from." This principle is at the heart of the project: Vera urges developers to refrain from writing insecure, vulnerable smart contracts and instead encourages mindful, secure, and responsible innovation. The mythical monk named Vera—a silent guardian who walked between worlds, protecting both wisdom and wealth—embodies this ideal.*

*As part of this vision, Vera will develop a static code analysis tool focused on detecting smart contract security vulnerabilities. This tool will empower developers to identify and fix issues early, promote secure coding practices, and make high-quality security feedback more accessible.*

*Through careful innovation and enduring vision, Vera is more than a currency; it is a statement of intent and a step toward redefining financial mindfulness in the decentralized age.*

## Problem Statement

The crypto space is increasingly driven by hype cycles, quick profits, and short-lived utility. This volatility, combined with poor security practices and unsustainable models, has led to a growing gap between the ideals of decentralization and the reality experienced by users.

Despite popular narratives about returning power to the people and breaking free from traditional banking monopolies, a significant portion of today's crypto infrastructure is controlled or influenced by those same centralized giants. True decentralization remains an ideal—not a norm.

Moreover, if you're a developer trying to build trust with the public through smart contracts, you're expected to undergo audits or obtain certifications. But professional audits are expensive, often inaccessible for independent

developers or small teams. And even when audits are secured, they take days or weeks, with feedback that is rarely immediate or educational. Developers may fix issues mechanically without learning how to avoid such vulnerabilities in the future.

There is a clear need for a solution that empowers developers early in their journey—offering real-time, accessible, and educational feedback that promotes secure coding from the ground up.

VeraMoney is grounded in the belief that integrity must precede innovation. Derived from the Sanskrit word *veramani*, meaning "to refrain from," Vera encourages developers to refrain from writing insecure smart contracts and promotes responsible, mindful building. This philosophy not only defines Vera's technical direction but also its cultural vision: to realign crypto with its foundational promises.

## Project Overview

VeraMoney is a twofold project: a balance between the expressive power of meme culture and the concrete utility of a real-world security tool. Inspired by the calm wisdom of the monk figure, Vera presents itself as a meme coin on the surface—but beneath that lies a powerful mission.

At its core, Vera is dedicated to building tools that serve the decentralized community, starting with its flagship moonshot project: a public-owned static code analysis tool for detecting security vulnerabilities in smart contracts. Every day, new tokens flood the ecosystem—many developed by inexperienced or first-time builders. Our challenge is to provide them with a tool that not only detects bad code but prevents it from reappearing. This includes teaching developers in real-time how to write secure contracts, fostering true learning and responsibility.

The primary goal of this tool is to make smart contract audits cheaper, more accessible, and more educational. By reducing dependence on expensive, delayed, and opaque external audits, Vera aims to level the playing field for independent developers and small teams—empowering them to ship secure code with confidence and clarity.

The Vera token (VERA) plays a critical role. More than 60% of revenue generated by audits will be returned to the community, creating a model of profit-sharing and collective ownership. The remaining 40% will go toward token buybacks, reinforcing value for long-term holders.

The Vera ecosystem is designed to support:

- Long-term holding with purpose — giving holders a share in the profit generated by the audit tool
- Community-led decisions — while a separate governance token hasn't been finalized, the VERA token may be used for governance as the system evolves
- A culture of quiet innovation
- Security-first tools and practices

Vera serves as the native token in a network built around clarity, education, protection, and empowerment. It's a playful entry into crypto—with serious intent underneath.

**Tokenomics**

- **Token Symbol**: VERA
- **Total Supply**: 1,000,000,000 VERA

Designed with transparency and equality — every token starts in the hands of the community.

- **Distribution**:
  - 10% — Allocated to the Liquidity Pool for market stability
  - 5% — Reserved for Community Rewards to encourage active participation
  - 10% — Assigned to the Development Fund and Core Team for ongoing innovation
  - 10% — Dedicated to Marketing and Strategic Partnerships
  - 30% — Public Sale for early adopters and supporters
  - 35% — Burned to reduce supply and enhance token value

  Here's the pie chart showing the token distribution for VERA, highlighting the proportions allocated to each category including liquidity, community, development, marketing, public sale, and the burned portion.

## VERA Token Distribution
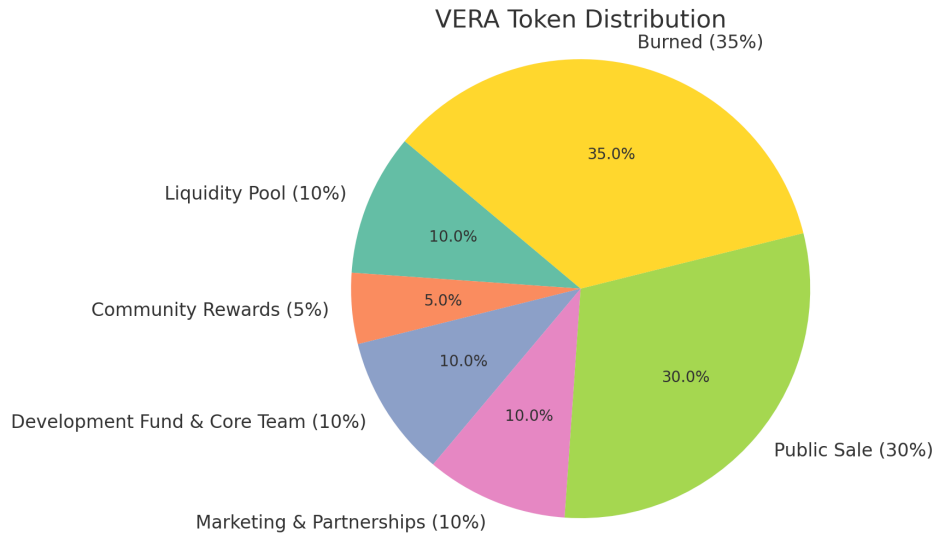


Following table shows how the tokens will be released over time. The second table shows how the tokens will be cumulatively unlocked over the coming 5 years every month.

| Allocation | Percentage | Total Unlock Type | Unlock Timeline |
| --- | --- | --- | --- |
| 🔥 Burned | 35% | Burned | Immediately removed from supply at TGE (T=0) |
| 🌊 Liquidity Pool | 10% | Fully Unlocked | Immediately at TGE (T=0) |
| 🎁 Community Rewards | 5% | Fully Unlocked | Immediately at TGE (T=0) |
| 👥 Public Sale | 30% | Fully Unlocked | Immediately at TGE (T=0) |
| 🛠️ Development & Core Team | 10% | Linear Vesting (monthly) | Over 5 years (60 months) |
| 📣 Marketing & Partnerships | 10% | Linear Vesting (monthly) | Over 5 years (60 months) |

Stacked Token Unlock Schedule Over 60 Months
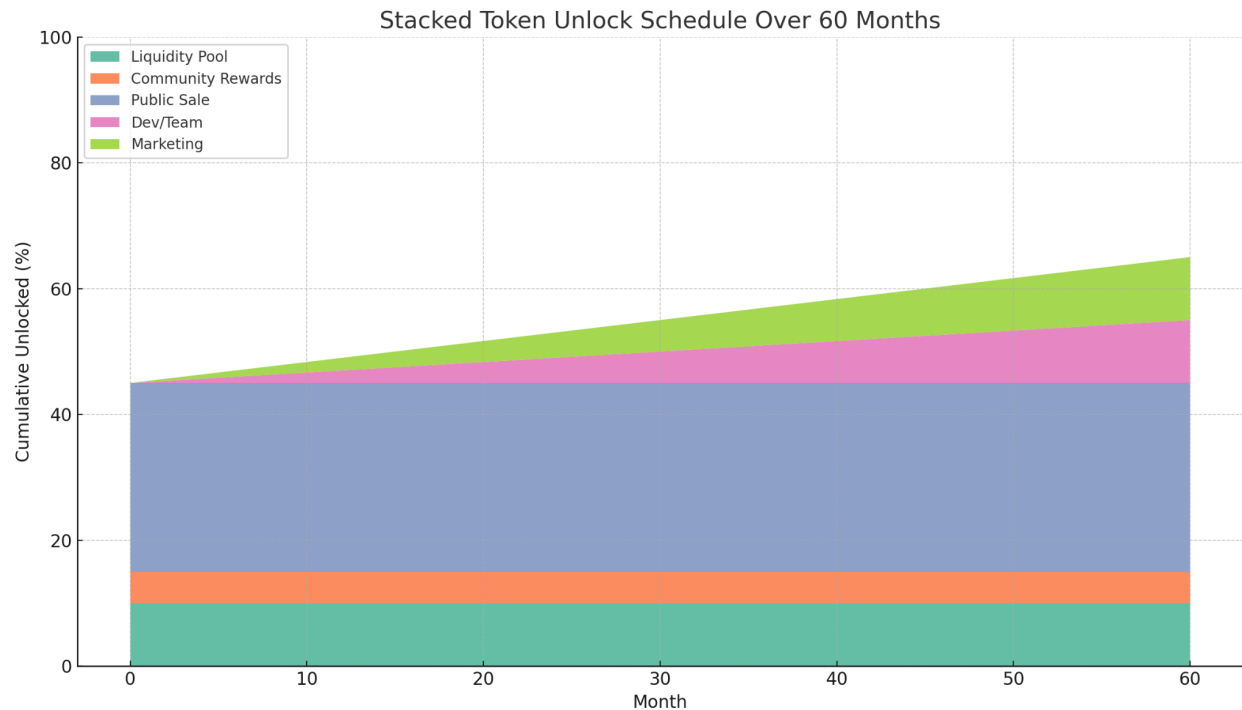
**Architecture**

  VeraMoney is deployed on the Arbitrum network, leveraging its scalability, low transaction costs, and Ethereum compatibility. This choice ensures high performance for users while maintaining access to a vibrant Layer 2 ecosystem.

At the heart of Vera's technical vision lies the Moonshot Project — a decentralized, community-aligned static code analysis tool built to detect vulnerabilities in smart contracts. This tool is not just a utility, but a movement: it aims to make smart contract audits affordable, educational, and accessible to all, especially for new developers launching tokens in today's chaotic crypto landscape.
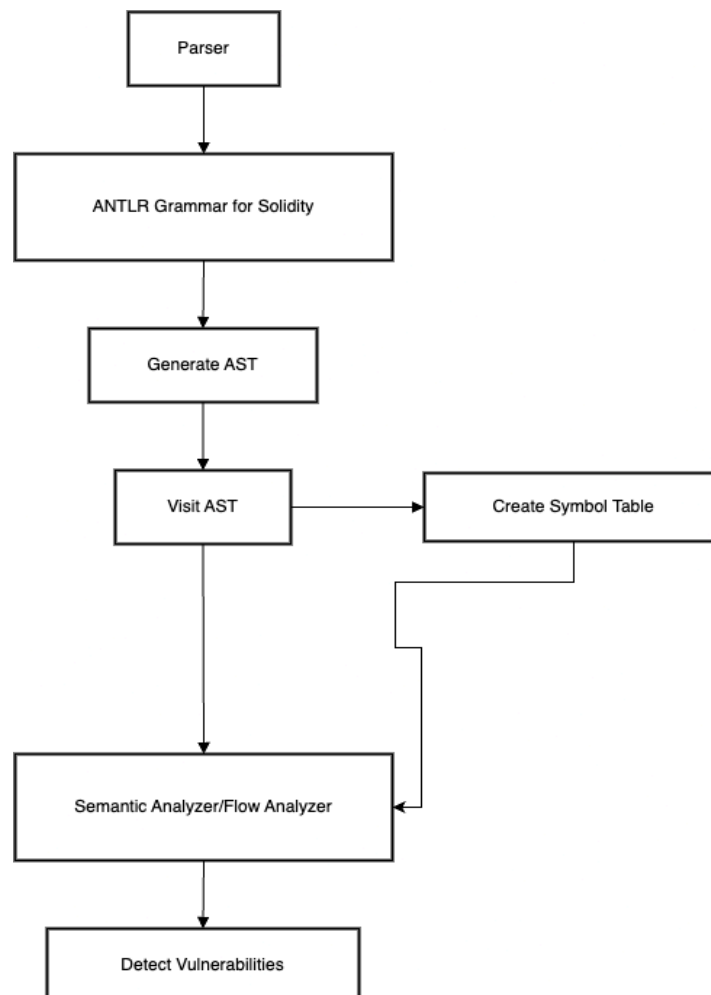
Key principles of the Moonshot Project include:

- **Real-time vulnerability detection**, highlighting insecure patterns as developers write code
- **Actionable feedback**, helping devs not only fix but understand what went wrong
- **Public ownership**, where VERA token holders represent percentage ownership in the tool's future revenue and governance

- **Open access**, encouraging transparency, peer learning, and community evolution of the tool

Technically, the platform will rely on a custom-built Solidity code parser and a semantic analyzer developed from the ground up. To accelerate development, we will utilize the official Solidity grammar for ANTLR published by Ethereum, enabling rapid generation of the parsing layer. On top of this, our custom semantic analyzer will be implemented to track control flows and recognize insecure code structures.

Rather than re-validating code-level constraints handled by the Solidity compiler itself, the system will assume that input contracts are already syntactically valid and compilable. The tool's mission is laser-focused on identifying security vulnerabilities in deployable smart contracts before they reach the public, giving developers proactive, real-time security awareness.

```
┌─────────────────┐
│     Parser      │
└─────────────────┘
         │
         ▼
┌─────────────────────────┐
│ ANTLR Grammar for Solidity │
└─────────────────────────┘
         │
         ▼
┌─────────────────┐
│  Generate AST   │
└─────────────────┘
         │
         ▼
┌─────────────────┐        ┌─────────────────────┐
│   Visit AST     │───────▶│ Create Symbol Table │
└─────────────────┘        └─────────────────────┘
         │                          │
         ▼                          │
┌─────────────────────────────┐     │
│ Semantic Analyzer/Flow Analyzer │◀───┘
└─────────────────────────────┘
         │
         ▼
┌─────────────────────┐
│ Detect Vulnerabilities │
└─────────────────────┘
```

The above flow diagram shows the high-level design of how the analyzer would work. The detailed explanation of how each component will work is explained below.

Overview

The **Semantic Analyzer / Flow Analyzer** serves as the core analysis module in our vulnerability scanner. Its primary responsibility is to analyze the **Abstract Syntax Tree (AST)** and associated **Symbol Table** to detect semantic anomalies and insecure coding patterns in Solidity smart contracts. This module is extensible and modular, allowing for new vulnerabilities to be identified by implementing specific visitor strategies that adhere to a shared abstraction layer.

Design Pattern: Abstract Vulnerability Visitor

At the heart of the Semantic Analyzer is the **AbstractVulnerabilityVisitor**—an abstract base class that encapsulates the visitor pattern. Each specific vulnerability rule (e.g., reentrancy, uninitialized storage pointer, timestamp dependence) inherits from this base class and implements targeted logic for AST node traversal and vulnerability condition detection.

```
              +-----------------------------+
              | AbstractVulnerabilityVisitor |
              +-----------------------------+
                            ▲
                            |
         +-------------------+------------------+
         |                   |                  |
+------------------+ +-----------------+ +--------------------+
| ReentrancyVisitor| | TimestampVisitor | | IntegerOverflowVisitor |
+------------------+ +-----------------+ +--------------------+
```

AST Traversal and Rule Execution

The AST, generated from the Solidity source code, is traversed recursively by the specific visitor implementation. The traversal respects the structural semantics of Solidity code and allows deep inspection of contract components such as function definitions, state variable declarations, control flow constructs, and inter-contract calls.

Each visitor implements a `visit(Node)` function, where `Node` represents a specific AST node type (e.g., `FunctionDefinition`, `IfStatement`, `CallExpression`). The `AbstractVulnerabilityVisitor` provides common utility methods for resolving identifiers, accessing symbol table information, and interpreting control/data flow contexts.

## Example: Reentrancy Vulnerability Detection

The `ReentrancyVisitor` overrides the `visit(FunctionDefinition node)` method and performs the following high-level checks:

- Identify external calls (e.g., `call.value()()`).
- Track changes to state variables.
- Determine if a state-changing operation occurs after an external call, signaling a potential reentrancy vector.

Pseudocode:

```
def visit(FunctionDefinition node):
    for stmt in node.body:
        if is_external_call(stmt):
            if state_change_occurs_after(stmt):
                report_vulnerability("Reentrancy", stmt.location)
```

This visitor is run over the entire AST. If a match is found, the location and type of the vulnerability are logged and later included in the final vulnerability report.

## Integration with the Analyzer Pipeline

Once all relevant visitors are instantiated, the Semantic Analyzer iterates through them sequentially, each receiving the AST and Symbol Table as inputs:

```
for rule in registered_vulnerability_visitors:
    rule.visit(ast_root)
```

This approach decouples rule logic from the core engine and provides high extensibility, enabling rapid inclusion of new detection rules without altering the analyzer's structure.

**Roadmap**

The VeraMoney roadmap outlines our strategic path to build both cultural momentum and technical credibility, anchoring the meme-driven energy of the project with a foundation of utility and community governance. The roadmap for the token is already mentioned in the website. Here we will be specifically focussing on the roadmap of the moonshot project. Gradually we will be building a world-class security platform and as the first phase of it, we will be starting with developing the moonshot.

**Phase 0 — Conception and Launch**

- Website launch: https://vera.money
- Token deployment on Arbitrum
- Initial community formation through Discord, X (formerly Twitter), and Telegram

**Phase 1 — Token Distribution & Awareness**

- Public token sale with a fair, community-first allocation
- Meme storytelling and branding campaigns
- Launch of ambassador and contributor programs

**Phase 2 — Moonshot R&D Begins**

- Kickoff of core research and architectural design
- Integration of Ethereum's official Solidity ANTLR grammar
- Framework development for the Abstract Visitor Pattern and vulnerability rule creation

**Phase 3 — MVP Release of Moonshot Tool**

- Release of the MVP version of the analyzer tool with key vulnerability detection rules
- Establish developer feedback and reporting loop
- Introduce VERA token utility: profit share access and audit participation

**Phase 4 — Governance and Utility Expansion**

- Profit-sharing model launch (60% to community holders)
- Launch of DAO or token-based governance model

- Open platform contributions: add rules, raise proposals, submit feature requests

**Phase 5 — Scaling and Ecosystem Growth**

- Support for additional languages, frameworks, and chains
- Release of SDKs, APIs, and CI/CD integration tools
- Educational initiatives for secure smart contract development
- Expand into enterprise and cross-chain security collaborations

Each of these phases reflects a milestone on our journey to make smart contract security accessible, community-owned, and transparently governed. Vera is here not to speculate—but to serve.

**Use Cases and Applications**

VeraMoney exists at the intersection of culture and utility, offering a dual-layered purpose that transcends typical meme tokens. While the token draws energy and reach from its cultural narrative — inspired by the calm wisdom of a monk in a chaotic crypto world — its deeper value emerges through its direct integration into the Moonshot auditing platform.

**1. Public Ownership in Audit Infrastructure**
 VERA tokens represent fractional ownership in a decentralized vulnerability analysis tool. Holders benefit from the platform's revenue via a profit-sharing mechanism where 60% of earnings from audits are distributed to the community, reinforcing long-term holding incentives.

**2. Incentivized Security Participation**
 Developers and auditors can earn rewards by contributing new vulnerability rules, test cases, or code improvements to the analyzer framework. This transforms VERA into a tool of engagement for the security research community.

**3. Governance and Rule Evolution**
 VERA is designed to serve as a governance token, empowering the community to propose and vote on major decisions — such as new audit rules, feature rollouts, and funding allocations. This ensures the analyzer evolves in alignment with its user base.

**4. Educational Guidance for Developers**
 New developers often struggle with understanding the intricacies of smart contract security. The Moonshot tool powered by Vera provides real-time

feedback and educational insight, helping devs learn secure coding practices as they build. This transforms audit tooling from a black box into a mentorship mechanism.

**5. Lowering Barriers to Entry**
Traditional security audits can cost thousands of dollars and take weeks. Vera democratizes access by providing free or low-cost static analysis, especially targeting early-stage projects that can't afford centralized audit firms. This opens the door for more innovation and fairness across the ecosystem.

**6. Meme Utility with Financial Substance**
Beyond its technological mission, VERA leverages its meme identity to build an active, loyal community. That momentum feeds into platform usage and token velocity, reinforcing a symbiotic loop between cultural capital and functional utility.

**7. Community Contributions and Developer Ecosystem**
With future plans for SDKs and APIs, third-party developers will be able to integrate the Moonshot engine into IDEs, CI/CD pipelines, and custom workflows. VERA tokens will be used to unlock premium features, prioritize scans, or receive advanced analytics.

Together, these use cases form a complete ecosystem where VeraMoney is not merely a speculative asset but a core component of an open, community-driven movement in smart contract safety.


**Governance**

Governance lies at the heart of VeraMoney's decentralized philosophy, with the **VERA** token serving as the primary instrument for community-led decision-making. As a governance token, VERA empowers holders to actively participate in shaping the direction of the protocol. Token holders are granted the right to propose changes, vote on important upgrades, allocate treasury funds, and help determine the future of the VeraMoney ecosystem. This model ensures that the project remains aligned with its foundational values of transparency, inclusivity, and peaceful progress.

The governance process follows a token-weighted voting system, where each VERA token equates to one vote. Proposals may cover a wide range of topics including protocol enhancements, ecosystem grants, integration decisions, and governance rule changes. To be enacted, proposals must meet defined quorum

thresholds and gain majority support. The lifecycle of a proposal begins in the community forum or governance platform, where ideas are discussed and refined. Once a formal proposal is drafted, it undergoes a temperature-check via an off-chain vote (e.g., using Snapshot). If the community expresses sufficient support, the proposal advances to an on-chain vote, where it can be approved and implemented through verifiable smart contract logic.

In anticipation of future scaling needs, VeraMoney will also adopt a **delegated governance model**, allowing VERA holders to delegate their voting power to trusted community representatives. These delegates will be transparent in their decisions and accountable to the voters who empower them, ensuring a more agile and representative governance structure. Delegation helps amplify the voices of passive or smaller holders without diminishing their influence in critical decisions.

The VeraMoney protocol includes a **community treasury**, funded through tokenomics and protocol revenue. This treasury is governed by VERA token holders and is designed to support initiatives that foster ecosystem growth, security audits, partnerships, and innovation. Community members may propose funding for projects that align with the values of peace, security, and decentralization.

Ultimately, VeraMoney governance is built upon key principles: **inclusivity**, where every token holder has the right to participate; **transparency**, with all votes and decisions recorded on-chain for full auditability; and **peaceful resolution**, promoting dialogue and consensus over conflict. By embedding governance directly into its structure, VeraMoney enables a truly democratic and resilient financial ecosystem.

## Conclusion

VeraMoney is more than just a digital asset — it is a movement built on the principles of transparency, collective responsibility, and inner peace reflected in financial systems. At a time when trust in centralized institutions is eroding and the world searches for balance, VeraMoney emerges as a symbol of harmony between technology and humanity. With the VERA token at its core, the ecosystem offers not just a tool for economic empowerment but a platform for thoughtful governance, ethical innovation, and a more mindful approach to decentralized finance.

By embedding peace into its protocols, transparency into its data, and democracy into its governance, VeraMoney sets a new standard for what a crypto

project can and should be. We invite builders, thinkers, and believers to join us — not just to participate in a system, but to help shape a more conscious financial future. Together, with VERA as our shared voice, we can forge an ecosystem where security is sacred, growth is purposeful, and every action echoes the values we hold.

The journey has just begun. Welcome to VeraMoney — **where value meets virtue**