Vihaan: A Whitepaper

A Protocol for a Fair, Stable, and Participatory Global Currency

Priyank Jhaveri

September 5, 2025

Contents

Abstract

Vihaan is a novel Layer-1 blockchain protocol engineered exclusively to function as a decentralized, equitable, and participatory global digital currency. Diverging from general-purpose, Turing-complete "world computer" blockchains, Vihaan's sole mandate is to facilitate the transfer of value with maximum fairness, efficiency, and long-term economic stability. This paper introduces **Proof of Economic Contribution (PoEC)**, a holistic consensus mechanism designed to mitigate plutocracy and resist Sybil attacks. PoEC determines a node's weight in a probabilistic lottery for block production based on a multi-factor score encompassing Capital Commitment (Stake), Network Loyalty (Time), and Economic Velocity (Activity).

The protocol's monetary policy is governed by a stabilizer mechanism designed to maintain a target annual inflation rate of 1-3%, encouraging circulation while counteracting the deflationary pressures inherent in fixed-supply assets. A defining feature of Vihaan is its mandatory node-centric architecture; to participate, every user must operate a full or pruned node, which fundamentally aligns the incentives of all participants with the security and decentralization of the network. The protocol is designed to be **immutable**: all core parameters are fixed at genesis, ensuring absolute predictability and resistance to governance capture. Through a system of non-linear rewards, robust in-protocol Sybil resistance, and a commitment to stability, Vihaan is designed to be a self-sustaining economic system where genuine, long-term participation is the dominant and most rational economic strategy.

Part I
Introduction

1 Motivation: A Fiat-Inspired Digital Currency

The advent of Bitcoin successfully solved the Byzantine Generals' Problem, presenting a paradigm shift in distributed systems. However, its design as a deflationary, "digital gold" asset disincentivizes its use as a medium of exchange. Subsequent "world computer" protocols like Ethereum, while powerful, serve competing use-cases beyond simple value transfer, leading to network congestion and volatile fees. Many Proof-of-Stake (PoS) implementations, while more efficient, can devolve into plutocratic systems where network control is directly proportional to capital.

Vihaan is proposed as a return to the vision of a peer-to-peer electronic cash system, but with a fundamentally different economic philosophy. It is designed not as a scarce commodity but as a **circulation-focused, fiat-like currency** where constant flow is essential for economic health. The primary goal is to create a reliable medium of exchange that can underpin employment, services, and trade. To achieve this, a controlled, mild inflation is considered a necessary feature, not a flaw, as it prevents hoarding and sustains economic growth. Vihaan is therefore designed with three specific goals:

- **Equitable Participation:** To design a consensus mechanism that mitigates plutocracy and rewards holistic economic contribution, not just wealth.
- **Economic Stability:** To implement an autonomous monetary policy that maintains a stable, low-inflation environment and avoids deflationary spirals.
- **Transactional Utility:** To build a system that is scalable, affordable, and accessible for global macro- and micropayments.

Part II
Protocol Architecture

2 The Node-Centric Network

Vihaan's architecture is predicated on the principle of **mandatory participation**. There are no standalone "wallet" applications that act as passive clients. To create an account, hold a balance, and transact, a user must operate node software, thus contributing directly to the network's decentralization and security.

This design presents a significant user experience challenge. To achieve mass adoption, the standard pruned node client must be exceptionally lightweight, efficient, and user-friendly. The target is a **mobile-first (PCs too) client** with auto-updates and minimal storage and bandwidth requirements, enabling non-technical users to participate seamlessly.

- **Full Nodes:** These nodes download and validate every block and transaction, maintaining the full state of the UTXO set. They form the backbone of the network, providing the highest level of security and acting as data hubs for pruned nodes.
- **Pruned Nodes:** The standard client for most users. This node downloads all block headers and a recent window of full blocks, but prunes older transaction data. Using **Simplified Payment Verification (SPV)**, a pruned node can still validate its own transactions with a high degree of security by referencing the Merkle Root in the block header.

3 Accounting Model and Data Structures

3.1 The UTXO Model

Vihaan utilizes the Unspent Transaction Output (UTXO) model, similar to Bitcoin. This offers several key advantages for a currency-focused protocol:

- **Enhanced Privacy:** Encouraging the use of new addresses for receiving change from transactions makes it more difficult to link a user's entire transaction history.
- **Parallel Processing Potential:** Since transactions consume unique inputs (UTXOs), multiple transactions that do not share inputs can be validated in parallel.
- **Conceptual Simplicity:** The stateless nature of UTXOs reduces the complexity of transaction validation compared to stateful account models.

3.2 Block Structure and Merkle Trees

A Vihaan block is composed of a header and a list of transactions. The header contains the hash of the previous block's header, a timestamp, the validator's signature, and a **Merkle Root**. This structure is critical for the efficiency of pruned nodes, allowing them to confirm a transaction's inclusion in a block by requesting only a small Merkle branch proof.

Part III

Consensus: Proof of Economic Contribution (PoEC)

PoEC is a novel consensus mechanism for validator selection. Instead of a deterministic process, PoEC is probabilistic and designed to be computationally trivial to verify. It calculates a **Validator Score (Vscore)** for each participating node based on three pillars. This score determines the node's weight in a lottery for the right to produce the next block.

4 Pillar I: Influence from Stake (IS)

Rationale: Capital commitment is necessary to secure the network. However, a linear relationship between stake and influence leads to plutocracy. To mitigate this, the influence of a node's stake is subject to diminishing returns via a logarithmic function.

$$IS = \log_{10}(S + 1)$$

Where S is the total amount of Vihaan Coin (VHN) staked. The logarithm ensures that while more stake always yields a higher score, the marginal benefit decreases significantly.

5 Pillar II: Influence from Time (IT)

Rationale: This pillar provides Sybil resistance by rewarding long-term, uninterrupted participation. To prevent network ossification and the creation of a permanent "aristocracy" of early nodes, influence from time grows at a sub-quadratic rate and is capped.

$$IT = \min((T_{age})^k, IT_{max})$$

Where T_{age} is the Node Age in epochs, k is a sub-quadratic exponent (e.g., 1.5), and IT_{max} is a maximum value corresponding to a long period of service (e.g., 3 years). A node must maintain high cumulative uptime to increment its T_{age}. This formula rewards loyalty but ensures new, dedicated participants can eventually become competitive.

6 Pillar III: Influence from Economic Activity (IE)

Rationale: This pillar rewards nodes for using the network for its intended purpose: transferring value. It is designed to favor genuine economic velocity over spam or wash trading through several mechanisms. The base score, E_{base}, is calculated as:

$$E_{base} = D_{tx} \cdot (\alpha \cdot \log_{10}(V_{tx} + 1) + \beta \cdot N_{tx})$$

Here, D_{tx} is a Transaction Diversity Score that incorporates diminishing returns for repeated interactions with the same counterparties within an epoch. To combat wash trading, the protocol incorporates further defenses:

- Transactions below a dynamic **dust threshold** are ignored for IE calculation.
- The protocol penalizes rapid, circular transaction patterns indicative of **self-looping**.

The final influence includes a compounding bonus for consistency:

$$IE = E_{base} \cdot (1 + r)^{N_{streak}}$$

Where N_{streak} is the number of consecutive epochs a minimum E_{base} threshold has been met.

7 Validator Selection Algorithm

The final Vscore is a weighted sum of the three pillars, with weights fixed at genesis:

$$Vscore = w_s \cdot IS + w_t \cdot IT + w_e \cdot IE$$

Deterministic selection of the highest-scoring node creates a target for DoS attacks and encourages centralization. Therefore, Vihaan employs a probabilistic selection method using a **Verifiable Random Function (VRF)**. In each slot, every participating node calculates its Vscore and uses the VRF to generate a pseudorandom number. If this number is below a threshold determined by the node's Vscore relative to the network's total Vscore, the node is selected as the block producer.

This method is equivalent to a lottery where a node's 'Vscore' represents its number of tickets. To further prevent centralization, a single node is capped on the number of blocks it can produce within any given epoch.

Part IV
Tokenomics and Monetary Policy

8 The Vihaan Coin (VHN)

Vihaan's monetary policy is designed to be autonomous, predictable, and geared towards long-term economic stability.

8.1 Monetary Stabilizer and Target Inflation

The protocol's primary goal is to maintain a long-term annual net inflation rate within a stable band of **1-3%**. This is achieved not by a simple issuance decay, but by an active **Monetary Stabilizer Mechanism**. This mechanism functions as a multi-epoch smoothing controller. It observes the net inflation rate (Total Issuance - Total Burn) over a trailing window and algorithmically adjusts the block issuance reward (I_{new}) up or down. This gradual adjustment process prevents volatile swings in monetary policy, providing a predictable economic environment for users. During periods of extremely high economic activity, the burn rate may exceed the issuance rate, making VHN temporarily deflationary.

8.2 Fee Mechanism: An EIP-1559 Inspired Model

The fee structure provides a deflationary counter-pressure and predictable transaction costs.

- **Base Fee:** A protocol-determined fee, algorithmically adjusted based on network congestion, which is **burned**.
- **Loyalty Discount:** A discount on the Base Fee, reinforcing the economic benefits of a single, reputable identity, calculated as a function of T_{age} and N_{streak}.

8.3 Initial Distribution and Sybil Resistance

8.3.1 Bootstrapping Value: A Philosophical Benchmark

A new currency faces the fundamental "cold start" problem: it begins with no established value. To solve this and to imbue the initial VHN grants with immediate, understandable utility, Vihaan is launched with a philosophical purchasing power benchmark. The size of the Genesis Grant and the initial UBP Stipend is calibrated with the **intention** that they should represent a meaningful amount of a globally recognized essential good, such as a quantity of clean water.

This benchmark serves as a powerful statement of design intent. It is, however, **not a formal peg**. There is no central entity or smart contract that will enforce this exchange rate. Instead, it is a philosophical anchor designed to frame Vihaan's primary purpose as a medium of exchange for the real economy, rather than a purely speculative asset. By anchoring its initial value proposition to a real-world necessity, the protocol signals its focus on transactional utility from genesis.

The ultimate purchasing power and market price of VHN will be determined by the free market, shaped by the organic supply and demand of its users and guided by the long-term stability objectives of the protocol's Monetary Stabilizer mechanism.

8.3.2 Fair Launch and Sybil-Resistant Mechanics

Vihaan is committed to a fair launch with no pre-mine or private investor sales. Bootstrapping the economy requires a robust Sybil-resistant distribution mechanism, as a simple one-time

"Genesis Grant" is highly vulnerable to attack. Therefore, Vihaan will employ a multi-layered defense-in-depth strategy:

- **Staggered Genesis Grants:** The initial grant claimable by each unique user is staggered, unlocking in tranches over several epochs to prevent a coordinated dump and allow for network observation.
- **Activity Locks:** Users must demonstrate genuine economic participation (e.g., by paying a certain amount in transaction fees) before they can claim their full grant.
- **Universal Basic Participation (UBP) Stipend:** To incentivize broad participation, 15% of all block issuance rewards is diverted to a Community Pool and distributed equally among all active, non-validating nodes at the end of each epoch.

Part V
Layer 2 and Scalability

9 Vihaan Lightning Channels (VLC)

To achieve global-scale throughput and facilitate practical micropayments, Vihaan's protocol includes a specification for a Layer 2 scaling solution: the VLC network, conceptually based on the Bitcoin Lightning Network. Users can lock VHN into bidirectional payment channels to conduct a virtually unlimited number of instant, near-zero fee transactions off-chain using **Hashed Timelock Contracts (HTLCs)**.

The VLC specification will be designed to address known challenges in existing Lightning implementations. This includes mitigating risks such as HTLC griefing attacks and routing centralization. The design will incorporate solutions such as **trampoline routing** to simplify pathfinding for light clients, robust economic incentives for **watchtower services**, and protocols to facilitate automated channel rebalancing and liquidity management.

Part VI
Security, Governance, and Validation

10 In-Protocol Sybil Resistance

The primary security challenge in a permissionless system is the Sybil attack. Vihaan's PoEC model is designed to make such attacks economically irrational. The non-linear, capped rewards from the Time and Stake pillars, the wash-trading resistant Activity pillar, the Loyalty Discount, and the multi-layered Genesis Grant mechanism all work in concert. This system creates a powerful incentive for any rational economic actor to consolidate all capital and activity into a single, long-standing identity, as the economic value of such an identity is mathematically superior to the sum of multiple, low-reputation splinter accounts.

11 Protocol Immutability and Pre-Launch Validation

Vihaan is founded on the principle of **protocol immutability**. After genesis, the core rules and parameters of the protocol—such as the PoEC weights (w_s, w_t, w_e), the inflation target band, and the IT pillar cap—are permanent and cannot be altered. There is no on-chain or off-chain governance mechanism for tuning these constants.

This approach offers absolute predictability and prevents governance capture, but it places immense importance on the pre-launch validation phase. The viability of the entire system depends on setting sound initial parameters. This will be achieved through a rigorous, multi-stage process:

- **Agent-Based Economic Simulation:** Extensive modeling of the protocol's economy with different types of actors (honest participants, Sybil attackers, colluding validators) to fine-tune the PoEC weights and monetary policy constants.
- **Adversarial Network Testing:** A dedicated security team will conduct continuous adversarial tests against private networks, attempting to exploit the consensus and economic models (e.g., through grinding, wash trading, and collusion attacks).

- **Long-Running Incentivized Testnet:** A public testnet will run for an extended period, offering bug bounties and rewards to encourage community participation in identifying potential flaws.
- **Third-Party Audits:** The final codebase and economic model will undergo multiple comprehensive audits from reputable security firms.

Part VII
Conclusion

12 Building a Fair and Stable Future

Vihaan represents a focused effort to create a purpose-built global digital currency. By moving away from the "world computer" paradigm and embracing a philosophy of protocol immutability and managed economic stability, the system can be optimized for its sole purpose: value transfer. The Proof of Economic Contribution consensus mechanism redefines network contribution beyond mere capital, creating a more equitable and Sybil-resistant system. Its node-centric design ensures that every user is a stakeholder in the network's security and decentralization.

Combined with a stable, adaptive monetary policy and a clear path to scalability via Layer 2, Vihaan is designed not as a speculative asset, but as a functional and reliable medium of exchange for the global economy. The project's success will be measured by its utility, its stability, and the breadth of its active user base.

A Appendix: PoEC Variable Definitions

S The total amount of VHN staked by the node.

T_{age} The node's age in epochs (e.g., 24-hour periods) meeting uptime requirements.

k The sub-quadratic exponent for the IT calculation (e.g., $k = 1.5$), fixed at genesis.

IT_{max} The maximum possible score from the Time pillar, fixed at genesis.

V_{tx} The total volume of VHN sent from the node in the last epoch.

N_{tx} The total number of unique transactions sent by the node in the last epoch.

N_{unique} The number of unique addresses the node has transacted with in the last epoch.

D_{tx} The node's Transaction Diversity Score, calculated as $1 - (1/(N_{unique} + 1))$, which approaches 1 as diversity increases. Also incorporates diminishing returns for repeat counterparties.

α, β Genesis-defined constants weighting transaction volume vs. count in the E_{base} calculation.

N_{streak} The number of consecutive epochs in which the node has met a minimum E_{base} threshold.

r The small compounding bonus rate for N_{streak} (e.g., $r = 0.01$).

w_s, w_t, w_e The genesis-defined weights for the three Vscore pillars.