ERC-20E

Elevado Labs
elevado.xyz

Abstract

In this paper, we propose ERC-20E, a token standard that generalizes a new class of assets: reserve-backed, collateral-denominated, yield-bearing, oracle-free monetary instruments whose net asset value (NAV) is cryptographically enforced to be non-decreasing over time. ERC-20E embodies the Elevado Standard, an asset framework that integrates issuance, redemption, collateral custody, accounting, and market mechanics into a single economic system. By internalizing monetary policy, reserve management, and value accrual within immutable code, ERC-20E enables the creation of assets that were ontologically impossible prior to Ethereum: assets that are transparently collateralized, insolvency-proof, oracle- and governance-free, and structurally accretive.

1 Introduction

The history of money and finance is inseparable from the history of institutions. For millennia, monetary instruments have relied on centralized authorities to define issuance, custody reserves, enforce convertibility, and manage monetary policy. Even in the modern era, where fiat money dominates and digital representations of value proliferate, the underlying architecture remains institutional, discretionary, and opaque.

The introduction of smart contracts marked a structural break in this history. Ethereum, as a general-purpose settlement layer with native programmability, enabled economic rules to be expressed directly in code and enforced by consensus. This innovation transformed assets from static ledgers into dynamic systems. The ERC-20 standard became the foundational primitive for fungible assets on Ethereum, abstracting balances, transfers, and allowances into a common interface.

Yet ERC-20, by design, is economically agnostic. It specifies how tokens move, not what they represent. Monetary policy, collateralization, issuance discipline, and value preservation are left entirely to external logic, governance, or off-chain entities. As a result, most ERC-20 assets reproduce legacy fragilities: discretionary issuance, opaque backing, reliance on oracles, and insolvency risk.

We believe Ethereum's true innovation is not merely tokenization, but asset programmability. For the first time, it became possible to define assets whose economic properties are enforced at the protocol level rather than promised by issuers. This opens the door to a new generation of assets that were previously impossible: assets that are self-custodial, self-auditing, and self-stabilizing by construction.

ERC-20E emerges from this lineage. It is a formal extension of ERC-20 that embeds an entire economic system – issuance, redemption, reserve accounting, yield mechanism, value accrual, and market mechanics – into a single, deterministic contract.

1.1 The Creation of the Holy Grail of Money

Throughout history, economists and philosophers have converged on an idealized conception of money: a medium that is fully collateralized, resistant to debasement, transparent in issuance, and capable of preserving – if not increasing – purchasing power over time. Gold standards attempted to approximate this ideal, but failed under institutional fragility. Fiat systems optimized flexibility, but at the cost of systematic depreciation.

The defining limitation was not conceptual, but technological. No prior technology could simultaneously enforce collateral backing, eliminate discretionary issuance, and automate value accrual without relying on trusted intermediaries.

ERC-20E represents the first credible materialization of this long-sought ideal. It defines money as a cryptographic institution: collateralized by design, insolvency-proof by construction, and governed by immutable rules rather than policy committees. Each ERC-20E asset is backed by a verifiable reserve held directly by the contract, with issuance and redemption governed by deterministic equations.

Crucially, ERC-20E introduces a structural innovation: value accrual through activity. Users pay fees to mint and redeem the asset. These fees are not extracted as profit, but retained within the collateral pool. As a result, each unit of the asset becomes increasingly over-collateralized relative to its initial issuance. The asset does not merely resist depreciation; it mechanically accumulates value.

This architecture produces a form of money that is simultaneously collateralized and yield-bearing, without exposure to credit risk, leverage, or external yield strategies. The "interest" earned by the asset is endogenous: it is the by-product of its own usage.

ERC-20E assets are issued by decentralized entities (i.e., immutable contracts) that cannot default, alter their rules, or misrepresent their balance sheets. Issuance is transparent. Monetary policy is cryptographically enforced. Purchasing power does not fall below a mathematically defined floor and, under continued usage, monotonically increases.

As a result, the ERC-20E standard represents a structural change in the ontology of money.

2 Elevado Standard

The Elevado Standard is the conceptual and mathematical asset framework that underpins ERC-20E.

The Elevado Standard is a framework that formalizes a class of assets defined by invariant relationships between supply, collateral, and value, yielding assets with deterministically enforced net asset value.

Fundamentally, the Elevado Standard is defined at the level of economic theory and mathematical structure rather than at the level of implementation. It is a language-agnostic asset framework that specifies the necessary and sufficient conditions under which a collateralized asset can be self-sufficient, value-accretive, and structurally insolvency-proof.

The Elevado Standard does not prescribe a particular collateral type, execution environment, or market context, nor does it depend on any specific programming language or virtual machine. Instead, it formalizes invariant relationships between collateral, supply, issuance, redemption, and value accumulation that must hold regardless of implementation.

In turn, ERC-20E represents one concrete instantiation of the Elevado Standard on the Ethereum Virtual Machine (EVM), but the asset framework itself exists independently of Solidity, Ethereum, or even blockchains more broadly, as a generalizable framework for asset design.

2.1 Understanding the Elevado Standard

At its core, the Elevado Standard defines an asset as a claim on a pool of collateral held by an entity. The asset's unit of account is the collateral itself. Issuance and redemption occur exclusively against this collateral, at ratios and fees defined at launch.

The Elevado Standard is built upon two fundamental principles. First, full collateralization: at all times, the aggregate supply in circulation is backed by a collateral reserve. Second, monotonic NAV: the net asset value per unit can never decrease as a function of system activity.

2.2 The Asset Framework

The Elevado Standard specifies a minimal yet complete asset framework. Within this framework, an asset is fully characterized by a set of structural definitions that jointly determine its economic behavior.

Each asset is defined by a designated collateral asset. This collateral asset establishes the unit of account of the system: all value, issuance, and redemption are expressed directly in units of the collateral itself. The collateral simultaneously functions as the quoted asset against which the native asset is issued and redeemed.

At launch, an initial issuance ratio is specified, expressed as 1:N, where one unit of the native asset corresponds to N units of collateral. This ratio defines the initial exchange relationship between supply and reserves and serves as the starting point from which all subsequent value dynamics evolve. In addition, fixed deposit and withdrawal fees are defined. These fees constitute the system's endogenous interest mechanism, governing how value accrues to the asset through usage rather than through external yield sources.

Finally, the asset's decimal precision is defined and must match that of the collateral asset. This constraint ensures accounting coherence and preserves numerical fidelity across issuance, redemption, and reserve calculations.

Taken together, these definitions form a complete asset framework that is invariant to the choice of collateral. Whether expressed in ETH or USD, systems following the Elevado Standard exhibit the same underlying economic logic: value is defined internally, enforced structurally, and evolves deterministically as a function of supply, collateral, and activity.

3 The ERC-20E Token Standard

The ERC-20E token standard represents the concrete, operational embodiment of the Elevado Standard on the Ethereum Virtual Machine (EVM).

While the original ERC-20 token specification defines balances, allowances, and transfers, ERC-20E extends this framework to embed full economic logic directly into the token contract.

The ERC-20E formalizes mechanisms for issuance, redemption, collateral custody, deterministic valuation, and internal accounting, effectively transforming the token from a simple ledger entry into a self-contained, algorithmic financial instrument.

Fundamentally, the ERC-20E standard is intended to operationalize the theoretical principles of the Elevado Standard into a programmable asset framework. By encoding all critical economic functions on-chain, ERC-20E removes reliance on external oracles, intermediaries, or off-chain computations. The native token's value, collateralization, and yield mechanics are fully deterministic and verifiable.

As a result, the ERC-20E standard enables assets that are structurally reserve-backed, insolvency-proof, yield-bearing, and resistant to dilution, representing a new paradigm for on-chain finance.

3.1 Functionality

ERC-20E contracts are structurally monolithic, consolidating a full economic system into a single contract. Core functionalities include:

- **Collateral Custody** Secure and verifiable storage of the designated collateral, either ETH or ERC-20 tokens, which denominates both the unit of account and the quote asset.

- **Minting and Issuance** Deterministic creation of new native tokens against deposited collateral, adhering to the initial ratio and adjusting dynamically according to protocol-defined fees.

- **Redemption and Burning** Symmetrical removal of tokens in exchange for underlying collateral, ensuring that net asset value remains above the collateral base.

- **Internal Accounting and Querying** Publicly callable functions to determine NAV, total collateral, effective ratios, issuance fees, withdrawal fees, and other economic parameters. All calculations are performed on-chain and are provably consistent with the protocol's invariants.

- **Built-in Yield Mechanism** Deposits and withdrawals carry protocol-defined fees that operate as an endogenous interest mechanism (or "yield"), ensuring value accrual to the asset through usage rather than external yield sources.

3.2 Properties

The ERC-20E standard is defined by a set of core economic and structural principles.

3.2.1 Monolithic

All economic logic resides within a single contract to ensure determinism and eliminate systemic interdependencies.

3.2.2 Immutable and Permissionless

Once public minting is enabled, all state transitions occur without discretionary intervention, governance, or administrative override.

3.2.3 Oracle-Free

All critical variables – including NAV, total collateral, effective ratios, and protocol parameters – are computed entirely on-chain, with no reliance on external price feeds or off-chain data.

3.2.4 Insolvency-Proof

The contract enforces a strict balance between liabilities (supply of native tokens) and reserves (collateral held). By design, the net asset value can never fall below, and structural mechanisms ensure that all obligations are fully collateralized at all times.

3.2.5 Deterministic and Auditable

All operations follow deterministic rules that are publicly verifiable, providing full transparency and auditability to all participants.

3.2.6 Decentralized and Governance-Free

After deployment and initial bootstrapping, no privileged authority can alter the token's fundamental economic behavior.

3.3 Protocol Design

The ERC-20E token standard, when expressed as a protocol, defines deterministic state transitions governing issuance, redemption, and reserve accounting.

The protocol maintains a single collateral pool and a circulating supply variable, from which all economic quantities are derived.

3.3.1 Mint

Minting occurs when a user deposits collateral into the contract.

Let C_d denote the deposited collateral amount, and let f_m be the mint fee. The effective collateral credited to the pool is:

$$C_{\text{net}} = C_d$$

The fee is not removed from the system; rather, it increases the collateral per unit of supply by reducing the number of tokens minted. The number of tokens issued is:

$$\Delta S = \frac{C_d \cdot (1 - f_m)}{R}$$

Where R is the current collateral-to-token ratio.

3.3.2 Redemption

Redemption is the inverse operation. A user burns ΔS tokens to receive collateral.

Let f_r be the redemption fee. The collateral returned is:

$$C_r = \Delta S \cdot R \cdot (1 - f_r)$$

The difference remains in the collateral pool, increasing the backing of the remaining supply.

3.3.3 Fees as an Interest Rate

Fees in ERC-20E constitute an endogenous interest mechanism embedded directly into the asset's issuance and redemption logic. They represent the price of immediate liquidity and the sole channel through which value is transferred from transactional users to long-term holders.

Unlike conventional interest, which arises from credit extension, leverage, or reinvestment of capital, ERC-20E fees do not depend on borrowers, counterparties, or external yield strategies. Instead, they are mechanically retained within the collateral pool, increasing the collateral backing of the outstanding supply.

As a result, value accrual is deterministic, non-probabilistic, and denominated in the same asset that defines the unit of account, rendering the mechanism structurally risk-free and fully self-contained.

3.3.4 Collateral, Unit of Account, Quoted Asset

The definition of the collateral asset establishes the fundamental unit of account for any ERC-20E asset.

All quantities related to issuance, redemption, and valuation are expressed and settled directly in units of the collateral itself, ensuring internal consistency and preserving accounting integrity.

By denominating the native asset in the same units as its backing collateral, the system enforces a deterministic relationship between supply, reserves, and value. The native asset represents a direct, proportional claim on the underlying collateral pool, and its economic properties – including net asset value and yield accrual – are fully determined by this relationship. This design ensures that the asset's valuation is intrinsic and self-contained, independent of external price feeds, benchmarks, or oracles, thereby creating an internally enforceable monetary mechanism.

Beyond simple denomination, the collateral defines the structural and operational boundaries of the asset. All state transitions – including minting, redemption, and protocol-level adjustments to the collateral pool – adhere to invariant accounting identities defined in units of the collateral. These invariants guarantee that net asset value cannot fall below the value of the underlying reserves, providing insolvency-proof characteristics that are mathematically verifiable.

3.3.5 Initial Ratio

The definition of the initial issuance ratio establishes the foundational exchange relationship between the native asset and its underlying collateral at deployment.

Expressed as 1:N, the ratio specifies the initial amount of collateral required to mint one unit of the native asset and, conversely, the amount of collateral returned upon redemption. Importantly, this ratio is a structural parameter, not a price peg: it defines the starting point of the system's internal accounting.

By explicitly defining the relationship between supply and reserves at inception, the initial ratio ensures that all subsequent calculations of net asset value, collateralization, and protocol-mediated yield are internally consistent and mathematically verifiable.

3.3.6 Decimals

The definition of decimal precision establishes the granularity with which an ERC-20E asset can be issued, redeemed, and accounted for relative to its collateral.

From a technical perspective, the native token must match the decimals of the collateral to ensure correct on-chain calculations. Mismatched decimals would lead to rounding errors, inaccurate issuance and redemption amounts, and inconsistencies in the collateral-to-token ratio, compromising the deterministic operation of the protocol. For example, if the collateral is USDC, which has 6 decimals, the native ERC-20E token must also have 6 decimals to guarantee precise on-chain arithmetic and reliable state transitions.

Beyond these technical constraints, matching decimals is also economically essential. It preserves exact proportional claims on the underlying collateral and ensures that the asset's net value and yield calculations remain deterministic and internally consistent. Maintaining consistent decimal precision prevents distortions in net asset value even for very large or very small token denominations.

3.4 Calculations

The central metric of the ERC-20E standard is Net Asset Value (NAV).

$$\mathrm{NAV} = \frac{C_{\mathrm{total}}}{S_{\mathrm{circulating}}}$$

Where C_{total} is the total collateral held by the contract and $S_{\mathrm{circulating}}$ is the supply in circulation.

Because minting and redemption fees are retained within C_{total} while reducing effective issuance or payout, it follows that:

$$\frac{d(\mathrm{NAV})}{dt} \geq 0$$

Under any non-zero protocol activity. Insolvency is structurally impossible, as redemptions are bounded by available collateral and issuance cannot occur without deposits.

3.5 ERC-20E Variants

The ERC-20E standard is designed to be flexible across different collateral while preserving its core economic invariants: deterministic NAV, structural insolvency-proofing, and endogenous yield accrual.

The baseline ERC-20E standard is natively collateralized with ETH.

Extensions of the baseline ERC-20E standard are formalized as standard variants that modify specific foundational assumptions while preserving the core invariants.

3.5.1 ERC-20E2 (ERC-20 Collateral-compliant)

ERC-20E2 generalizes the baseline standard to support ERC-20 tokens as collateral.

The fundamental modification from ERC-20E to ERC-20E2 is that the collateral is an ERC-20 token (e.g., USDT, WBTC), whose decimal precision must match that of the native asset to ensure computational fidelity on-chain. This is made possible through the implementation of the SafeERC20 library.

3.5.2 ERC-20E3 (Programmable Compliance)

ERC-20E3 introduces optional compliance and governance mechanisms such as conditional transfer restrictions, external fee management, and selective pause functionality. The key distinction is that these mechanisms are modular and do not compromise the fundamental invariants of the ERC-20E framework: NAV determinism, full collateralization, and structural insolvency-proofing remain intact.

At its core, the ERC-20E3 variant is designed for contexts requiring additional control, such as regulated environments or institutional applications, while preserving the baseline standard's deterministic and self-contained economic behavior.

4 Implementation Notes and Disclosures

4.1 Codebase

The ERC-20E codebase is planned for release after the launch of Elevado Labs' first asset primitive, which will be the first protocol to adopt ERC-20E.

4.2 Slippage Management

Slippage controls are implemented at the front-end and user interface layers, rather than within the ERC-20E protocol itself. User-facing systems, such as Elevado Markets built by Elevado Labs, provide configurable slippage parameters and execution safeguards when interacting with ERC-20E contracts.

This architectural separation preserves the protocol's minimalism without introducing additional complexity or discretionary logic at the contract level.

4.3 Contract Bootstrap and Genesis State

Each ERC-20E contract is initialized through a deliberate bootstrap procedure designed to ensure mathematical continuity and structural integrity across all possible system states.

At deployment, the contract owner is required to mint a single genesis unit of the native asset in strict accordance with the predefined issuance ratio. For example, under a 1:1 ratio, the owner must deposit one unit of collateral to mint one native token. This genesis token is permanently locked within the contract, and its corresponding collateral is likewise retained perpetually.

This initialization serves a critical structural purpose. By ensuring that at least one unit of supply and a corresponding amount of collateral are always present within the system, the contract maintains a well-defined ratio and avoids undefined edge states. In scenarios where all circulating supply is redeemed and burned, the contract does not collapse or reset arbitrarily;

instead, it deterministically converges to its genesis state. The collateral remaining within the contract reflects the ratio defined by the final redemption, and the system is capable of resuming issuance from that state without loss of accounting continuity.

This design cryptographically guarantees that the ERC-20E contract remains mathematically well-posed at all times, even under extreme or degenerate conditions.

4.4 On Secondary Market Dynamics and Price Convergence

The economic design of ERC-20E assets imposes strong constraints on secondary market behavior, ensuring that market prices converge tightly around the asset's net asset value (NAV).

Because the contract allows any participant to mint new tokens directly against collateral at a deterministically defined rate, secondary market prices above NAV are inherently unsustainable. Rational participants would instead acquire exposure more efficiently by minting directly through the contract, placing immediate downward pressure on any premium pricing.

Conversely, secondary market prices below NAV create immediate arbitrage opportunities. Market participants can acquire the asset at a discount and redeem it directly with the contract for its full collateral value, net of fees. This mechanism enforces a lower bound on price and ensures rapid convergence back to NAV on secondary markets. As a result, conventional liquidity provision strategies – such as automated market maker pools – are structurally unattractive for ERC-20E assets, as liquidity providers would be systematically exposed to adverse selection and arbitrage losses.

Crucially, every unit of an ERC-20E asset transacted on secondary markets is fully collateralized at its point of origin. No token can exist without corresponding collateral locked within the contract, and no unit can be minted or redeemed outside the protocol's deterministic rules. Secondary market activity therefore represents the transfer of fully collateralized claims, not synthetic exposure or leverage layered on top of the system.

5 Conclusion

ERC-20E constitutes a relevant advance in the design of programmable assets on Ethereum by formalizing a class of monetary instruments whose economic properties are enforced structurally rather than assumed implicitly.

By embedding collateralization, issuance, redemption, valuation, and a yield mechanism directly at a contract level, ERC-20E transforms the token from a passive representation of value into an autonomous economic system.

Assets instantiated under the ERC-20E standard are fully collateralized by construction, resistant to dilution, and capable of deterministic value accretion through protocol-native mechanisms. In doing so, ERC-20E demonstrates that monetary soundness, transparency, and solvency can be achieved not through governance, discretion, or external enforcement, but through invariant relationships encoded at the protocol level.

As Ethereum matures into a global settlement and execution layer, standards such as ERC-20E point toward a future in which money and financial assets function as programmable infrastructure – self-auditing, insolvency-proof, and natively aligned with long-term value preservation.

By reconciling rigorous economic principles with deterministic on-chain execution, ERC-20E expands the design space of money itself, enabling forms of value organization that were previously unattainable. In this sense, ERC-20E is not merely an extension of the ERC-20 paradigm, but a foundational step toward institutionally robust, algorithmically governed monetary systems.

5.1 Rethinking Financial Architecture: The Transformative Potential of ERC-20E

The ERC-20E standard represents a fundamental departure from conventional assumptions in financial infrastructure, which have historically relied on modular, intermediary-dependent architectures.

In traditional systems, issuance, market formation, accounting, and collateral management are dispersed across multiple agents and protocols, generating layers of operational risk, opacity, and systemic fragility. ERC-20E consolidates these functions into a single, deterministic, self-contained contract, thereby internalizing the full economic lifecycle of the asset and eliminating entire classes of execution, counterparty, and oracle-related risk.

By embedding the rules of issuance, redemption, and collateralization directly within the contract, ERC-20E enforces structural invariants that guarantee solvency, anti-dilution, and deterministic yield accrual. This design ensures that assets follow a predictable, upward-trending value trajectory while remaining fully auditable and transparent.

In effect, ERC-20E substitutes the traditional reliance on trust, judgment, and discretionary interventions with cryptographically enforced proofs of solvency and value, creating a paradigm in which the integrity of the monetary or financial instrument is verifiable at all times.

From the perspective of quantitative finance, ERC-20E provides a frictionless, fully deterministic economic environment, where risk-adjusted valuations, collateral ratios, and NAV calculations can be computed on-chain in real time without external dependencies. By collapsing market mechanics, reserve management, and protocol-level interest into a single on-chain framework, ERC-20E not only streamlines operational complexity but also establishes a new benchmark for institutional-grade, trust-minimized, and yield-bearing financial instruments.

In doing so, the ERC-20E standard represents a profound innovation in decentralized monetary engineering, reconciling rigorous economic theory with the practicalities of programmable finance.

A Formal model, invariants, and economic Proofs of the Elevado Standard

This appendix formalizes the Elevado Standard and its ERC-20E implementation as a deterministic economic system. We define the state variables, derive the governing equations, and prove the core properties that distinguish ERC-20E assets: monotonic net asset value, structural insolvency-proofness, and endogenous value accrual.

A.1 State variables and definitions

Let an ERC-20E contract at time t be fully described by the following state variables:

- C_t: total collateral held by the contract, denominated in units of the collateral asset
- S_t: total circulating supply of the native ERC-20E token
- R_t: effective collateralization ratio, defined as collateral per unit of supply
- $f_m \in [0, 1)$: mint (deposit) fee
- $f_r \in [0, 1)$: redemption (withdrawal) fee

All variables are stored and computable internally by the contract. No external data sources are required.

A.2 Net Asset Value (NAV)

The Net Asset Value per unit of ERC-20E token is defined as:

$$\mathrm{NAV}_t = \frac{C_t}{S_t}$$

This quantity is expressed in the unit of account of the collateral asset. It is not a price, not a peg, and not a target; it is a balance-sheet identity enforced by the contract.

The NAV is fully observable, verifiable, and exact.

A.3 Minting dynamics

Consider a mint operation at time t, where a user deposits an amount $\Delta C > 0$ of collateral.

The number of tokens minted is:

$$\Delta S = \frac{\Delta C \cdot (1 - f_m)}{\mathrm{NAV}_t}$$

The post-mint state becomes:

$$C_{t+1} = C_t + \Delta C$$
$$S_{t+1} = S_t + \Delta S$$

Substituting:

$$\mathrm{NAV}_{t+1} = \frac{C_t + \Delta C}{S_t + \frac{\Delta C(1-f_m)}{\mathrm{NAV}_t}}$$

A.4 NAV monotonicity under minting

We now show that minting cannot reduce NAV.

Define:

$$\mathrm{NAV}_{t+1} - \mathrm{NAV}_t \geq 0$$

This inequality holds because the fee f_m ensures that fewer tokens are minted than would be required to keep NAV constant. Intuitively, the protocol absorbs the fee as surplus collateral rather than distributing it as supply.

Formally, since:

$$\frac{\Delta C}{\Delta S} = \frac{\mathrm{NAV}_t}{1 - f_m} > \mathrm{NAV}_t$$

Each marginal token is issued at an effective premium, increasing average backing.

A.5 Redemption dynamics

Consider a redemption at time t, where a user burns $\Delta S > 0$ tokens.

The collateral returned is:

$$\Delta C = \Delta S \cdot \mathrm{NAV}_t \cdot (1 - f_r)$$

The post-redemption state becomes:

$$\begin{aligned} C_{t+1} &= C_t - \Delta C \\ S_{t+1} &= S_t - \Delta S \end{aligned}$$

A.6 NAV monotonicity under redemption

We again examine:

$$\mathrm{NAV}_{t+1} = \frac{C_t - \Delta C}{S_t - \Delta S}$$

Because the redeemer receives less than their proportional share of collateral due to f_r, the remaining supply becomes more collateralized.

Formally:

$$\frac{\Delta C}{\Delta S} = \mathrm{NAV}_t(1 - f_r) < \mathrm{NAV}_t$$

Hence:

$$\mathrm{NAV}_{t+1} \geq \mathrm{NAV}_t$$

A.7 Core invariant: non-decreasing NAV

From sub-sections A.4 and A.6, we obtain the central invariant of the Elevado Standard:

$$\forall t_2 > t_1, \quad \mathrm{NAV} t_2 \geq \mathrm{NAV} t_1$$

This holds for all admissible state transitions, independent of transaction ordering, user behavior, or market conditions.

This invariant is enforced not by governance or incentives, but by algebra.

A.8 Insolvency impossibility

An ERC-20E contract is structurally insolvency-proof.

At any time:

$$\text{Total Liabilities} = S_t \cdot \mathrm{NAV}_t = C_t$$

Redemptions are constrained by actual collateral balances. There is no mechanism by which claims on collateral can exceed reserves, as issuance requires prior deposit.

Unlike fractional systems, leverage is mathematically impossible.

A.9 Endogenous yield and value accrual

The effective yield of an ERC-20E asset is not paid externally, nor sourced from borrowers or strategies. It is endogenous and arises from protocol usage.

Define cumulative protocol activity over time as a sequence of mint and redemption events e_i.

Then:

$$\lim_{n\to\infty} \mathrm{NAV}_{t+n} > \mathrm{NAV}_t \quad \text{if protocol usage } > 0$$

In plain terms: holding the asset entitles the holder to a growing share of the same collateral base, without dilution, risk, or dependency.

This is best described as “stacking more coins from the same amount of coins.”

B State-space representation of an ERC-20E contract

An ERC-20E contract can be modeled as a discrete-time dynamical system:

$$X_t = (C_t, S_t)$$

Where C_t is collateral and S_t is circulating supply. The state transition function F is deterministic:

$$X_{t+1} = F(X_t, u_t)$$

Where u_t is a user action (mint, redeem, or null). This places ERC-20E within the class of closed, deterministic financial automata, a category largely unexplored in traditional finance.

C Proof of absence of reflexive collapse

Let redemptions increase without bound. Since each redemption reduces supply faster than collateral, the marginal redemption becomes increasingly expensive in opportunity cost.

Formally, the redemption elasticity satisfies:

$$\frac{d\Delta C}{d\Delta S} < \mathrm{NAV}_t$$

This prevents reflexive death spirals characteristic of algorithmic stablecoins.

D NAV as a Martingale with positive drift

Define NAV as a stochastic process driven by protocol usage:

$$\mathrm{NAV}_{t+1} = \mathrm{NAV}_t + \epsilon_t$$

Where:

$$\mathbb{E}[\epsilon_t] \geq 0$$

Unlike yield strategies with fat-tail risk, ERC-20E NAV exhibits positive drift without volatility injection.

E ERC-20E vs pegged systems: a formal contrast

Pegged systems enforce:

$$P_t \approx P^*$$

ERC-20E enforces:

$$\frac{C_t}{S_t} \geq \mathrm{NAV}_0$$

The former targets price; the latter enforces solvency – these are orthogonal objectives.

F Time consistency and the elimination of policy risk

Since fees and ratios are immutable, ERC-20E eliminates the time inconsistency problem:

$$\arg\max_t U(\pi_t) \neq \arg\max_{t+1} U(\pi_{t+1})$$

Policy is fixed ex ante and enforced cryptographically.

G Fee accrual as deterministic seigniorage

Define cumulative fees:

$$F_T = \sum_{t=0}^{T} f_m C_t + f_r C_t$$

This is seigniorage without discretionary issuance, paid entirely to holders via NAV accretion.

H Absence of duration risk

Traditional yield-bearing instruments expose holders to duration:

$$\frac{dP}{dr} \neq 0$$

ERC-20E has no interest rate sensitivity because value accrues in-kind:

$$\frac{d\text{NAV}}{dr} = 0$$

I ERC-20E as a non-probabilistic yield instrument

Yield does not depend on stochastic processes:

$$Y = f(\text{usage})$$

not

$$Y = f(\text{default probability})$$

This places ERC-20E outside classical fixed-income risk models.

J Market microstructure: internalized AMM vs external liquidity

ERC-20E issuance/redemption functions replicate a virtual constant-sum market:

$$\Delta S = \frac{\Delta C}{\text{NAV}}$$

But without liquidity providers, impermanent loss, or arbitrage externalities.

K Slippage bounds and deterministic execution

Slippage is a function of NAV evolution, not pool depth:

$$\text{Slippage} \leq f_m + f_r$$

Thus execution risk is bounded and transparent.

L ERC-20E as a collateral-denominated numéraire

ERC-20E assets define their own numéraire.

Value comparisons are internal:

$$1 \text{ Token} = \text{NAV}_t \cdot \text{Collateral}$$

This eliminates unit mismatch errors common in DeFi.

M Composability with risk-free primitives

ERC-20E tokens can serve as base assets in lending without liquidation risk:

$$\text{Liquidation threshold} = 100\%$$

Since insolvency is impossible.

N Stress testing under extreme redemption scenarios

Let $S_t \to 0$.

By bootstrap constraint:

$$\lim_{S_t \to 0} \text{NAV}_t = \text{finite}$$

The system converges gracefully rather than collapsing.

O Long-run monetary dynamics

As $t \to \infty$:

$$\text{NAV}_t \to \text{NAV}_0 + \sum F_t$$

ERC-20E behaves as a monotonic reserve accumulator, not an inflationary currency.

P Asymmetric payoff structure and bounded downside risk

A defining characteristic of assets instantiated under the ERC-20E standard is the asymmetric structure of their economic payoff.

From a risk-return perspective, the downside exposure of an ERC-20E asset is explicitly bounded by protocol-defined fees, while the upside remains unbounded and accumulative. This asymmetry arises not from discretionary policy or external market dynamics, but from the deterministic mechanics governing issuance, redemption, and collateral retention.

Consider a participant who acquires exposure to an ERC-20E asset. Upon minting, the participant deposits collateral and receives native tokens net of a deposit fee. This fee represents the maximum immediate reduction in principal relative to the deposited collateral. Similarly, upon redemption, a withdrawal fee is applied, defining the maximum additional reduction in collateral returned. Importantly, beyond these explicitly defined fees, the protocol contains no mechanism through which principal value can be eroded. The asset is fully collateralized at all times, and the accounting invariants enforced by the contract guarantee that the net asset value per token cannot fall below the post-fee collateral backing.

Let f_d and f_w denote the deposit and withdrawal fee rates, respectively. For a participant entering the system at time t, the maximum downside relative to the deposited collateral is bounded by:

$$\Delta_{\text{downside}} \leq f_d + f_w$$

This bound is deterministic and known ex ante. No stochastic shocks, liquidation cascades, or adverse price movements can push realized value below this threshold.

By contrast, the upside of an ERC-20E asset is unbounded. Each instance of protocol usage – whether through minting or redemption – retains fees within the collateral pool, increasing collateral without proportionally increasing supply. As a result, net asset value evolves monotonically over time:

$$\text{NAV}_{t+1} \geq \text{NAV}_t$$

This inequality holds strictly whenever protocol activity generates net fees. Because there is no upper bound on cumulative protocol usage, fee accrual, or time horizon, there is likewise no upper bound on NAV growth. Value accretion is permanent, irreversible, and fully retained within the system.

From a portfolio construction and risk management perspective, this payoff profile is highly atypical. Traditional financial instruments with bounded downside often achieve such protection through options, insurance, or counterparties, each introducing additional layers of risk. In ERC-20E, the asymmetry is structural and endogenous: downside risk is capped by design, while upside accrues mechanically through system activity.

As a result, ERC-20E assets have explicitly bounded downside and theoretically infinite upside.