Universe Dollar (UVD)

A Bitcoin Secured, Basket Indexed, Fixed Supply Stable Currency

Kiyan Sasan
ks@ala.xyz
www.uvd.xyz

Abstract. Universe Dollar (UVD) is a fixed supply, Bitcoin-collateralised currency issued on a zero-knowledge rollup that anchors to the Bitcoin base layer. UVD is designed to be stable in the short term, harder in the long term, neutral between nations and trust-minimised between people. Short-term stability is achieved by indexing UVD to the Universe Reserve Basket (URB), a fixed basket of 40% gold (XAU), 30% Swiss franc (CHF) and 30% Singapore dollar (SGD). Each week, the protocol reindexes the satoshi backing of 1 UVD so that its purchasing power tracks URB within an explicit, bounded band. Long-term strengthening arises from three structural choices: (1) fixed UVD supply set at genesis so that no new units can ever be minted, (2) pure BTC collateral held in verifiable vaults anchored to Bitcoin and (3) a surplus BTC vault that accumulates excess collateral from protocol operations and favourable reindexing. As Bitcoin monetises and appreciates relative to URB, the effective BTC backing per UVD can gradually ratchet upward, subject to strict solvency constraints. Over multi-year horizons, UVD transitions from URB-like stability to a systemically harder currency than URB itself, while remaining usable for everyday pricing. UVD is minted only when users lock BTC into the collateral vault. UVD is redeemed only when users return UVD and withdraw BTC at a transparent, rules-based rate. A separate credit layer allows UVD to be lent and BTC to be posted as collateral for UVD borrowing at conservative loan-to-value ratios. Yield flows to UVD lenders and to the protocol's surplus without rehypothecating the base BTC backing. The protocol is released as open source, without admin keys, upgrade switches or kill functions. Once deployed, it runs as long as Bitcoin runs and at least one implementation continues to produce rollup proofs. Not even its creators can arbitrarily change the rules, mint more tokens or shut it down. Beyond technical design, UVD is motivated by a civilizational aim: to end the recurring pattern where each empire in turn controls the unit of account, and instead root monetary gravity in a neutral base asset (Bitcoin) and transparent rules. This aligns with old Abrahamic concerns about just weights and measures, translated into the language of modern cryptography.

---

1. Introduction

1.1 The problem: monetary gravity captured by each empire in turn

For as long as complex trade has existed, there has been a dominant unit of account and a dominant issuer behind it.

Historical examples include silver and gold standards in ancient kingdoms, Roman and Byzantine coinage, Venetian and Florentine bills of exchange, the Spanish silver real, the Dutch guilder, the British pound and, in the most recent cycle, the US dollar.

Each of these reserve currencies sat at the centre of its era's trade network and brought real benefits: smoother long-distance commerce, common pricing and accounting, and a reference point for contracts and savings. Every empire, for a time, stabilised its world.

But the pattern repeats. First, the centre gains the privilege to issue the unit of account at near-zero marginal cost. Over generations, war, crisis, politics and human nature (greed, short-termism, weak successors) lead to over-issuance and debasement. Eventually, trust erodes, capital migrates and trade gradually reorients around a new centre and a new unit.

Rome debased its denarii. City-states overextended credit. European powers inflated away promises through war and reconstruction. None of this is uniquely modern or uniquely American; it is a structural property of any system where a single political centre controls the base money for everyone else.

Historically, there was no way around it. To coordinate a civilization, one needed a focal point: an empire, a capital, a mint. Debasement was the recurring price of having a standard at all.

Today, two facts are different. First, there exists a neutral, non-state base asset, Bitcoin, with a transparent, fixed issuance schedule. Second, we have programmable settlement and cryptography that allow monetary rules to be defined and enforced in code rather than in councils.

The problem is not that one particular currency is uniquely bad. The problem is the recurring pattern: whenever one centre owns the scale, sooner or later the scale tilts.

Universe Dollar is a proposal to break this cycle without denying that earlier reserve currencies served their purpose. They were necessary stages in coordination. The next stage is to keep the coordination while removing the monopoly over the mint.

UVD attempts this by rooting backing in Bitcoin rather than any state balance sheet and indexing to a basket spanning gold and conservative currencies from different regions, instead of anointing any single empire as the reference.

The aim is not to punish a particular currency, but to preserve the benefits of a common unit of account while making the underlying rules neutral, transparent and resilient to the weaknesses of any single generation.

1.2 Goal: BTC at the root, fair stability at the surface

Universe Dollar aims to construct a currency that anchors to Bitcoin at the collateral and security layer, behaves like a stable currency in the short term, inherits Bitcoin's monetisation in the long term, explicitly refuses to crown any single state as issuer of the global unit of account and cannot be altered or shut down by its own creators.

If Bitcoin is the digital bedrock, UVD is meant to be the habitable layer above it: a relatively stable climate for trade and savings, sitting on the tectonic plate of BTC.

1.3 Ethical frame: just weights in a programmable age

Across Judaism, Christianity and Islam, three themes recur: condemnation of false scales, skepticism toward exploitative money and limits on human authority.

Texts criticise dishonest weights and measures. In modern terms, silently changing the unit of account is structurally similar to moving the scale under a trader's feet. Practices where one party extracts

value purely because it controls the medium of exchange are treated with suspicion or prohibition. Earthly power is expected to sit under higher constraints, not above them.

In a global digital economy, the base currency and its issuance rules function as the shared scale. If one actor can dilute that unit at will, everyone else is trading on tilted ground.

UVD is designed so that supply cannot be increased by decree, backing is visible and auditable, and the relation between UVD, BTC and the reference basket is fixed in code, not in committees.

The protocol does not claim religious status. It simply attempts to embody a straightforward idea: the scale used in trade should not secretly move to favour those closest to the mint.

2. Design goals and constraints

2.1 Design goals

1. **Stable unit of account.** UVD should exhibit relatively low volatility against a conservative reference basket in day-to-day terms. It should be suitable for denominating prices, wages and contracts.
2. **Bitcoin-rooted collateral.** All core backing is BTC. Collateral is visible as UTXOs or equivalent commitments on Bitcoin.
3. **Fixed supply.** UVD total supply is set at genesis and never increases. There is no emergency mint, bailout ability or monetary expansion lever.
4. **Deterministic rule set.** The currency's behaviour is determined by explicit formulas and protocol state. The weekly reindex is algorithmic and bounded; no committee can override it.
5. **Permissionless and censorship resistant.** Anyone able to use Bitcoin and the rollup can hold and transfer UVD. The protocol embeds no blacklist or freeze functionality.
6. **Long-term strengthening.** Over multi-year arcs, as BTC appreciates relative to the basket and surplus grows, the effective BTC backing per UVD should tend to increase. UVD becomes "harder" without ceasing to be "stable".
7. **Immutability in practice.** No admin keys and no upgrade hooks for the monetary core. Upgrades, if any, require new deployments and voluntary social migration, as in Bitcoin forks.

2.2 Constraints

Constraints include: no dependence on bank accounts or off-chain fiat assets for the core collateral; no authority able to confiscate or freeze balances at the protocol level; no function capable of silently introducing new UVD units; oracles limited in influence per unit time and unable to override solvency rules; and no central roadmap that assumes the authors can force changes later.

3. Universe Reserve Basket (URB)

3.1 Definition

UVD does not stabilise against USD, EUR or any single state currency. Instead, it tracks the Universe Reserve Basket (URB), a supra-national index combining gold (XAU), Swiss franc (CHF) and

Singapore dollar (SGD).

Let the weights be

$$w_{\mathrm{XAU}} = 0.40, \quad w_{\mathrm{CHF}} = 0.30, \quad w_{\mathrm{SGD}} = 0.30,$$

with

$$w_{\mathrm{XAU}} + w_{\mathrm{CHF}} + w_{\mathrm{SGD}} = 1.$$

Intuitively, 1 URB represents a synthetic purchasing power unit composed of 40% gold, 30% CHF and 30% SGD.

3.2 Why CHF and SGD?

CHF and SGD are chosen for structural reasons. CHF is the currency of a small, export-driven state with a long-standing reputation as a Western safe haven and conservative monetary policy. SGD is the currency of a small, trade-heavy city-state, managed as a band against a basket of foreign currencies and functioning as an Asian safe haven disciplined by external competitiveness.

In short: Switzerland of the West, Switzerland of the East.

Adding gold, a supra-sovereign, non-political metal used as a store of value across empires and faiths for thousands of years, yields a basket that spans metal, a Western safe haven and an Eastern safe haven, avoids dependence on any single major reserve issuer and leans on regimes structurally incentivised toward currency stability.

3.3 BTC priced in URB units

Let $P_{\mathrm{BTC/CHF}}(t)$ be the price of 1 BTC in CHF at week t, $P_{\mathrm{BTC/SGD}}(t)$ be the price of 1 BTC in SGD at week t and $P_{\mathrm{BTC/XAU}}(t)$ be the price of 1 BTC in units of gold at week t.

Then the price of BTC in URB units is

$$P_{\mathrm{BTC/URB}}(t) = w_{\mathrm{XAU}} \cdot P_{\mathrm{BTC/XAU}}(t) + w_{\mathrm{CHF}} \cdot P_{\mathrm{BTC/CHF}}(t) + w_{\mathrm{SGD}} \cdot P_{\mathrm{BTC/SGD}}(t).$$

This is the number of URB units one BTC is worth at time t. A decentralised oracle mechanism supplies or aggregates these values and provides $P_{\mathrm{BTC/URB}}(t)$ to the UVD protocol.

4. Monetary model

4.1 Fixed UVD supply

At genesis, the UVD supply is defined as

$$N_{\max},$$

the total UVD tokens created once and for all. By construction, $N = N_{\max}$, and never increases.

Initially, a protocol Treasury address holds all UVD. UVD enters circulation only when users deposit BTC and receive UVD from Treasury at the current backing rate. Let M_t be the circulating UVD at week t. Treasury holdings are $N_{\max} - M_t$.

4.2 BTC vaults

The protocol tracks two logical BTC vaults: a Backing Vault and a Surplus Vault. The Backing Vault holds BTC explicitly allocated to back circulating UVD at the current satoshi rate. The Surplus Vault holds BTC above the target overcollateralisation level of the Backing Vault and accumulates liquidation penalties and protocol fees.

Let B_t be BTC in Backing Vault at time t and S_t be BTC in Surplus Vault at time t. Total BTC under protocol control is $B_t + S_t$.

4.3 Satoshis per UVD

At week t, define s_t as the number of satoshis corresponding to 1 UVD according to the protocol. Since 1 BTC equals 10^8 satoshis,

$$1 \text{ UVD} \approx \frac{s_t}{10^8} \text{ BTC}.$$

Given the BTC price in URB units $P_{\text{BTC/URB}}(t)$, the neutral satoshi rate making 1 UVD approximately 1 URB is

$$s_t^{\text{neutral}} = \frac{10^8}{P_{\text{BTC/URB}}(t)}.$$

If the protocol set $s_t = s_t^{\text{neutral}}$, then 1 UVD would approximately equal 1 URB at that point, up to spreads and fees.

4.4 Collateralisation ratio

The BTC required to back all circulating UVD at rate s_t is

$$\text{RequiredBTC}_t = M_t \cdot \frac{s_t}{10^8}.$$

The Backing Vault collateralisation ratio is

$$C_t = \frac{B_t}{\text{RequiredBTC}_t} = \frac{B_t \cdot 10^8}{M_t \cdot s_t}.$$

The protocol enforces $C_t \geq C_{\min}$ for some configured $C_{\min} > 1$.

4.5 Minting and redemption

At week t with satoshi rate s_t, minting works as follows. A user deposits x BTC into the Backing Vault. The protocol mints

$$x \cdot \frac{10^8}{s_t}$$

UVD from Treasury to the user. Then B_t increases by x and M_t increases by the minted amount.

For redemption, a user sends y UVD back to the protocol. The protocol returns

$$y \cdot \frac{s_t}{10^8}$$

BTC from the Backing Vault to the user. Then M_t decreases by y and the Treasury receives y UVD. These formulas are hard-coded. There is no override function.

4.6 Weekly reindexing of s_t

Reindexing aligns UVD with URB and preserves solvency once per week. A specific Bitcoin block height defines the boundary between weeks.

Parameters include: growth share $g \in [0, 1]$, max weekly log-change bound $k_{\max} > 0$, minimum collateral ratio $C_{\min} > 1$ and target collateral ratio $C_{\text{target}} > C_{\min}$.

At week t the procedure is:

1. Oracle provides $P_{\text{BTC/URB}}(t)$.

2. Compute neutral satoshi rate: $s_t^{\text{neutral}} = \frac{10^8}{P_{\text{BTC/URB}}(t)}$.

3. Compute log difference: $\Delta = \ln\left(\frac{s_t^{\text{neutral}}}{s_t}\right)$.

4. Clamp the adjustment: $\Delta_{\text{clamped}} = \text{clip}(\Delta, -k_{\max}, k_{\max})$.

5. Apply growth share: $\tilde{s}_{t+1} = s_t \cdot \exp\big((1-g) \cdot \Delta_{\text{clamped}}\big)$.

6. Compute provisional collateralisation: $C_{t+1}^{\text{provisional}} = \frac{B_t \cdot 10^8}{M_t \cdot \tilde{s}_{t+1}}$.

7. If $C_{t+1}^{\text{provisional}} \geq C_{\min}$, set $s_{t+1} = \tilde{s}_{t+1}$. Otherwise, set $s_{t+1} = \frac{B_t \cdot 10^8}{M_t \cdot C_{\min}}$.

In normal or favourable conditions, UVD tracks URB while slowly accumulating BTC convexity if $g > 0$. In adverse conditions, solvency dominates: the protocol refuses to tighten s_t in a way that breaks $C_{\min}$. The reindexing is mechanical, not discretionary.

4.7 Surplus vault dynamics

After reindexing, the Backing Vault collateralisation ratio is

$$C_{t+1} = \frac{B_t \cdot 10^8}{M_t \cdot s_{t+1}}.$$

If $C_{t+1} > C_{\text{target}}$, the protocol moves BTC from Backing Vault to Surplus Vault until $C_{t+1} = C_{\text{target}}$. The Surplus Vault also accumulates BTC from liquidation penalties in the credit layer and any BTC-denominated protocol fees defined at launch.

Surplus BTC can be moved back to Backing Vault if C_t approaches $C_{\min}$ and may support rule-based mechanisms (defined at launch) that raise the minimum effective backing per UVD as surplus grows. The Surplus Vault is part of the protocol's balance sheet, not a treasury for a team or DAO; there is no discretionary withdrawal function.

5. Architecture: zero-knowledge rollup on Bitcoin

5.1 Overview

UVD runs on a zero-knowledge rollup that anchors to Bitcoin. The rollup provides a deterministic execution environment for UVD contracts, periodic state commitments on Bitcoin, validity proofs for state transitions and an escape hatch to exit to Bitcoin in case of censorship or failure.

5.2 State commitments and proofs

In each rollup batch, users submit transactions on the rollup. A sequencer orders them and computes the new state root. A prover generates a zero-knowledge proof that the transition from old root to new root is valid under the VM and UVD contract rules. The new root and proof commitment are embedded in a Bitcoin transaction.

Once the commitment is mined and has sufficient confirmations, that rollup state is considered finalised. Security reduces to the correctness of the zk proving system, the integrity of the state commitment mechanism and the persistence of Bitcoin consensus.

5.3 Exit mechanism

If sequencers fail or censor users, any user can use a previously finalised state root on Bitcoin, construct a proof of their assets relative to that root and follow a predefined exit procedure to reclaim BTC or UVD to a target address.

The exact rollup design (data availability, proof system, sequencing) can vary by implementation. For UVD, the critical part is that the monetary rules are fully enforced inside the VM and that users retain a way to exit to Bitcoin if the rollup layer misbehaves.

6. Credit and yield layer

The credit layer operates on top of UVD and is separate from the monetary safety of UVD itself.

6.1 Lending and borrowing

Independent lending protocols on the rollup can accept UVD deposits from lenders, accept BTC deposits as collateral and allow borrowers to draw UVD loans against BTC. Borrow characteristics include loan-to-value caps based on BTC price vs URB and liquidation thresholds where undercollateralised positions can be liquidated by third parties.

Upon liquidation, liquidators repay some or all of the UVD debt, receive BTC collateral at a protocol-defined discount and a portion of the seized BTC (the liquidation penalty) flows into the Surplus Vault.

6.2 Yield

UVD holders can hold UVD and remain exposed only to long-term strengthening or lend UVD in the credit layer to earn periodic interest in UVD. Protocol-level BTC fees and liquidation proceeds further strengthen the system's surplus over time. The credit layer can fail independently. A bug in a lending protocol does not change UVD supply, its BTC backing or the monetary rules.

7. Immutability, governance and forks

7.1 No admin keys

UVD contracts are deployed without privileged owners. There is no pause function for the currency, no arbitrary freeze or confiscation function and no function that can modify $N_{\max}$, basket weights or

core collateral parameters. Once deployed, UVD's monetary logic is as immutable as the underlying platforms (Bitcoin and the rollup).

7.2 No protocol governance over money

There is no on-chain governance token, no DAO and no voting mechanism that can mint UVD beyond $N_{\max}$, modify the Universe Reserve Basket composition or weights, override the weekly reindex rules or spend the Surplus Vault arbitrarily. Governance, if present at all, is restricted to off-chain client and UX choices and to optional higher-layer protocols built on UVD (DEXs, lenders and similar). To change monetary rules, a new protocol must be deployed and migration is voluntary.

7.3 Forks

If a subset of users believes a different design is superior, the path is to publish new open source code, deploy new contracts and persuade people to move BTC and UVD into the new system. As with Bitcoin, the original Universe Dollar system remains available for those who prefer its rules. Monetary sovereignty is at the user and market level, not in a governor's hands.

8. Risks

8.1 Oracle risk

URB and BTC prices are supplied by oracles. Risks include manipulated price feeds, outages or delays and bad aggregation logic. Mitigations include multiple independent data sources, median or consensus aggregation, time-weighted averages, conservative bounds on weekly adjustments ($k_{\max}$) and encoded fail-safes to skip reindexing when inputs are obviously inconsistent. Oracle risk cannot be eliminated; it can only be constrained.

8.2 BTC price risk

Fast drawdowns in BTC vs URB stress collateralisation: the Backing Vault may approach $C_{\min}$ and the protocol may be forced to accept temporary deviations from URB to maintain solvency. The reindex rule is collateral-aware; it will not tighten s_t in a way that violates $C_{\min}$ and it prioritizes survival of backing over perfect tracking.

Conservative initial settings for $C_{\min}$, C_{target} and g, plus healthy surplus, reduce risk but do not remove it. UVD is still rooted in BTC; any BTC-based system inherits BTC's fundamental risk profile.

8.3 Implementation and rollup risk

Bugs in smart contracts, rollup execution or consensus or zk proving systems can cause loss of funds or inconsistent state. Mitigations include independent audits, formal verification where feasible, staged rollout and bug bounties. There is no central authority with the power to roll back or arbitrarily reverse errors. This is a design choice: the system trades paternal safety nets for predictable rules.

9. Positioning and impact

Universe Dollar sits between and apart from existing designs.

Unlike fiat-custodial stablecoins, UVD does not rely on dollars, treasuries or bank accounts as core backing. Unlike empire-pegged designs, UVD does not treat any single state's currency as the definition of value; it stabilises against a multi-polar basket of metal, CHF and SGD. Unlike purely algorithmic systems without hard collateral, UVD is backed by explicit BTC, visible on Bitcoin, with overcollateralisation constraints. Unlike CBDCs, UVD does not embed state surveillance, KYC at protocol level or programmable censorship.

Instead, UVD offers Bitcoin as base collateral, a conservative supra-national stability reference, explicit equations instead of policy meetings and no admin or issuer with special privileges.

If Bitcoin continues its trajectory toward global collateral status, then UVD can increase structural demand for BTC as deposited collateral, provide a stable surface for everyday commerce in a BTC-centric world, dilute the structural privilege of any one nation over the global unit of account and instantiate an old principle with new tools: let weights and measures be honest, and let the issuer be bound by the same rules as everyone else.

From that angle, UVD does not compete with Bitcoin. It extends Bitcoin into the domain of stable units of account in a way that supports rather than dilutes Bitcoin's role.

10. Conclusion

Universe Dollar is a proposal for a new monetary instrument with these core properties: fixed maximum supply, Bitcoin-only core collateral, basket-indexed stability against a 40% gold, 30% CHF, 30% SGD basket, algorithmic weekly reindex with explicit solvency constraints, separation of an immutable monetary core from optional credit and DeFi layers and no admin keys or protocol-level governance over money.

It is intended to be published once, open to scrutiny and criticism and then left to the world. No emperor, committee or foundation sits above it. The only authority is the code and the social consensus of those who choose to use it.

If adopted at scale, UVD could weaken the historical cycle of empire-bound reserve currencies, distribute monetary power away from capitals and toward neutral rules, offer a fairer, more transparent unit of account to billions of people and act as a bridge between the old world of political money and a new world anchored on Bitcoin.

If not adopted, it still serves as one concrete step in the broader search: a worked example of how technology, economic incentives and deep human intuitions about justice in exchange might be aligned.

The arc of monetary history has always moved between order and abuse, stability and debasement. For the first time, we possess tools that allow us to encode the weights and measures themselves as transparent, globally verifiable rules. Universe Dollar is one attempt to write such rules on top of Bitcoin and then get out of their way.

The propagation of this system is driven by self-interest and cannot be halted by decree. The nation that first integrates this standard secures a strategic advantage in the resulting fair playing field. The equilibrium is inevitable. For woman, life and liberty.