Crownridge Protocol

Permanent capital, on-chain. — Whitepaper, V1

Crownridge is a reserve-backed treasury protocol on Robinhood Chain. USDG reserves enter a protocol-owned Treasury, CRWN is issued against those reserves, protocol revenue compounds net asset value, and disciplined below-NAV buybacks burn CRWN — increasing NAV per remaining token.

Robinhood Chain · chain ID 4663 · reserve asset USDG · token CRWN (18 decimals)
Version 1 · Status: pre-launch, unaudited, not deployed to mainnet

1. Abstract

Most reserve-token designs fail on one of two axes: they mint tokens without matching reserves (dilution disguised as growth), or they present market price as if it were backing. Crownridge takes the opposite discipline. CRWN is minted *only* when reserve assets actually enter the Treasury, atomically

and verifiably. Net asset value is defined as recognized reserves divided by a conservatively-defined circulating supply, computed identically in the contracts and every interface. Protocol revenue is retained as reserve rather than siphoned away, so backing per token compounds. When the market discounts CRWN below NAV, the Treasury may buy and burn it — but only when a full risk engine proves the purchase is accretive, and never on a manipulated or stale price.

This document specifies V1 precisely: the economic model, the deterministic accounting, the access-control and emergency architecture, the buyback risk engine, and — stated plainly rather than hidden — the founder Treasury authority and the risks a depositor takes on. Crownridge is not an OHM fork; it shares only the intellectual lineage of treasury-backed tokens and implements its own contracts, economics, and controls.

---

2. The mechanism in thirty seconds

```
USDG enters the Treasury
   ↓
CRWN is issued against reserves      (never without them — no naked minting)
   ↓
Protocol revenue is retained as reserve → NAV per CRWN compounds
   ↓
When market price sits sufficiently below NAV, and only when provably accretive:
   ↓
Treasury buys CRWN on Uniswap v3 and burns it → NAV per remaining CRWN rises
```

---

3. Assets and accounting

The single reserve asset is USDG (canonical `0x5fc5360D0400a0Fd4f2af552ADD042D716F1d168`, 6 decimals, verified on-chain), a dollar-backed stablecoin whose infrastructure Robinhood documents as provided by Paxos. CRWN has 18 decimals. All on-chain accounting uses raw integer units; USD is 1e18 fixed point; 6↔18 normalization is explicit and floor-rounded in the Treasury's favor. USDG is treated as 1:1 USD — an assumption, not a guarantee (§9).

QUANTITY	DEFINITION
Recognized reserve	USDG recognized as backing. Always ≤ actual Treasury USDG balance (conservation).
NAV	Recognized reserve normalized to 1e18 USD, minus recognized liabilities (zero in V1).
Circulating supply	CRWN total supply minus CRWN held by protocol contracts. The Uniswap pool is *not* excluded — pool-held CRWN counts as circulating.
NAV per CRWN	NAV ÷ circulating supply (zero, i.e. N/A, when nothing circulates).
Protocol-owned liquidity	Valued at **zero** in NAV — the conservative treatment of the CRWN/Treasury circularity.

A single anchored library (`CrownridgeMath`) implements these definitions; the Treasury, the buyback engine, the accounting lens, the indexer, and the website all derive from it, so no two components can disagree.

4. Genesis — issuance

Genesis is the only path by which CRWN enters circulation. It is atomic: the depositor's USDG lands directly in the Treasury, the Treasury recognizes the exact measured amount, and only then is CRWN minted — all in one transaction that reverts on any failure. A protocol fee is retained in the Treasury as reserve (not siphoned to an account), so it raises backing for every holder.

```
deposit gross USDG            (≥ minDeposit, within cap and per-wallet cap, window
open)
fee  = gross × feeBps / 10000  → retained in Treasury as reserve
net  = gross − fee
CRWN = normalize6→18(net) × rate / 1e18     (floor; dust favors the Treasury)
recognize the full gross; mint CRWN to the depositor
```

Proposed V1 parameters (subject to founder + independent economic-review sign-off): rate 1 CRWN per 1 USDG net; fee 0.50% (1.00% hard cap); cap 250,000 USDG; min deposit 10 USDG. There is no pre-mint, no fixed maximum supply, and no founder/team/investor CRWN allocation — the founder's economic interest is expressed through the Treasury controller (§7), not allocated tokens.

5. Buyback and burn

The buyback is a risk engine, never "if price < NAV then buy". Each execution must pass, in one transaction, every gate below or revert (fail closed). It ships **disabled**; enabling is a timelocked action taken only after the market and oracle have a usable history.

- Time-weighted average price from the Uniswap v3 pool, with a minimum observation cardinality and a spot-vs-TWAP deviation bound (manipulation in progress → revert).
- Minimum pool liquidity; minimum discount to NAV; a slippage floor derived from the TWAP.
- Per-transaction, per-day, and maximum-Treasury-percentage-per-day spend caps, plus a cooldown.
- **Accretion enforced on measured deltas:** after the swap, USD spent ÷ CRWN received must not exceed NAV per CRWN, or the transaction reverts. A buyback can never dilute.

Worked example: Treasury $1,000,000, supply 1,000,000, NAV $1.00, market $0.80. Spend $80,000, buy 100,000 CRWN, burn. Treasury $920,000, supply 900,000, NAV ≈ $1.0222. This behavior is covered by a test.

6. The Contract

The following invariants are enforced by the contracts and covered by unit, fuzz, and property tests. They are reproduced here verbatim and must not be weakened.

Enforced invariants

1. Unauthorized accounts can never mint CRWN.
2. CRWN cannot be minted without a corresponding reserve entry (no naked minting; deposit→mint is atomic).
3. Treasury reserve accounting can never become negative.
4. Buyback cannot spend above its configured limits.
5. Burned CRWN cannot return to circulation.
6. Genesis cannot exceed its configured cap.
7. Decimal normalization (6↔18) remains correct.
8. A failed reserve transfer cannot produce CRWN.
9. Recognized reserve is always ≤ the Treasury's actual USDG balance (conservation).
10. A founder withdrawal reduces recognized reserve and NAV immediately, never changes CRWN supply, and emits a dedicated event.

---

7. Governance, access control, and the founder authority

The economic core is **immutable** — no proxies, no upgrade path. Configuration is governed by a 48-hour `TimelockController` (administered by a protocol multisig as proposer) with a security-multisig guardian that holds both an immediate per-subsystem pause and a `CANCELLER` veto over queued timelock actions. The deployer configures the system and then permanently renounces all authority.

> **Founder Treasury authority — disclosed.** Crownridge includes a Founder Treasury Controller that can withdraw the reserve asset from the Treasury. Every withdrawal immediately reduces recognized reserve and NAV per CRWN, never mints CRWN, and emits a `FounderTreasuryWithdrawal` event. It is narrowly scoped — it can do nothing but withdraw the approved reserve asset, with no arbitrary calls, minting, or role changes. Depending on the deployed configuration it is *capped* (per-withdrawal, rolling, floor, and cooldown limits) or *uncapped* (up to the full recognized reserve). The guardian can pause this path immediately; the timelock can revoke the controller. The active mode is published in the deployment manifest and on the transparency page. “Permanent capital” describes the vehicle's structure — no maturity, no redemption schedule — not a promise that reserves can never be withdrawn, and it does not imply a guaranteed floor.

---

8. Verification

V1 ships with unit tests for every external function, bounded fuzz tests, a property/invariant suite exercising the invariants above across thousands of randomized action sequences, a deploy-path test that asserts the deployer renounces all authority, and a fork suite that runs against live Robinhood Chain mainnet using the real USDG and real Uniswap v3 contracts. Two independent internal adversarial reviews were run (a pre-implementation design review and a post-implementation code review); their confirmed findings were folded into the design and code. This is internal assurance, not a substitute for the independent external audit and economic review required before mainnet.

9. Risks

RISK	CONSEQUENCE & RESPONSE
USDG depeg / issuer / freeze	NAV overstated until a timelocked write-down reduces recognized reserve; Genesis paused; buybacks fail closed on price sanity. USDG≈USD is an assumption.
Oracle failure / manipulation	Buyback reverts (TWAP + deviation + cardinality). No automated action on bad price.
DEX liquidity loss	Buyback fails closed; Genesis and Treasury unaffected.
Founder-key compromise	Guardian pauses the founder-withdraw path immediately; timelock revokes the controller. In uncapped mode the founder can withdraw the entire recognized reserve — a real trust assumption.
Smart-contract exploit	Immutable core limits blast radius; per-subsystem pause; coordinated disclosure.
Admin-key compromise	Multisig + 48h timelock + guardian CANCELLER veto; no single key can drain or mint.

CRWN is not redeemable for reserves in V1 and carries no guaranteed value, yield, floor, or appreciation. Legal/regulatory characterization has not been reviewed; obtain counsel before public launch.