Wave Protocol

Protocol overview

Off-chain trading with on-chain portfolio shares

Direction draft v2.1 / 12 November 2026
Presentation updated 13 November 2026



Live market. Proposed protocol.

The WAVE token is trading on BNB Chain. A market swap is not a deposit into the proposed portfolio-share system described here. Issuance, redemption, accounting and custody operations remain proposed; this document does not establish asset backing for the live token.

Live WAVE: 0x2Bf84642a3F5EC5d9b8d5D67179A968fD89e2AC3

Review the model, assumptions and risks before participating.

Contents

01 Protocol overview
02 System components and terminology
03 Custody across chain and exchange accounts
04 Portfolio value and WAVE price
05 Deposits minting and dilution
06 Asset algorithms and AI selection
07 Allocation and portfolio constraints
08 Rebalancing and order execution
09 Withdrawals and liquidity reserves
10 Returns reporting and numerical example
11 Risk governance and economic policy
12 Research map and implementation path
Symbols, research bibliography and official references

01 / Protocol overview

Purpose

Wave pools deposited capital into a transparent crypto portfolio. WAVE is the transferable ownership share of that portfolio. An AI recommendation engine evaluates approved asset-specific strategies; a constrained allocator determines portfolio weights; an execution service translates the approved allocation into orders. Users can inspect holdings, weights, net asset value and performance. This overview specifies the proposed economic model; the trading algorithms will be supplied separately.

One token and one common portfolio

All WAVE holders participate in the same pooled portfolio and receive the same return per share over the same holding interval, before user-specific costs. A holder owns a fraction of the pool, not an individually segregated collection of coins. Only assets deposited into Wave enter this system; Wave does not allocate a user's entire external net worth. Personalized risk profiles require distinct share classes, separate pools or managed accounts and are outside this initial model.

What changes from the existing prototype

The existing WaveToken is an optional voting token; existing WaveBasket contracts issue separate basket shares and do not run AI. This proposal instead makes WAVE the portfolio share. It requires a new issuance, redemption and accounting design. This document does not change contracts, migrate tokens, establish a deployment or claim the proposed engine already operates.

Working assumptions

The proposed model now uses the founder's off-chain trading terminals connected to dedicated Wave exchange accounts. WAVE ownership and a deposit and payout gateway remain on BNB Chain. The initial scope is one spot-only, long-only portfolio without leverage. Settlement asset, exact venues, account ownership, numerical risk limits and algorithms still require specification. The terminal is an execution interface; custody rests with the exchange or any separately designated custodian.

02 / System components and terminology

Vault and reserve pool

The vault is the accounting and custody boundary for assets backing WAVE. A reserve pool is the liquid settlement-asset portion of that same portfolio, used for withdrawals, transaction costs and future allocations. It is included in portfolio value once; it is neither extra collateral nor a guarantee against losses. Pending deposits and finalized withdrawal claims must be recorded separately.

Recommendation and allocation

An asset algorithm produces a timestamped signal or forecast for one asset under a declared horizon. The recommendation engine selects or combines eligible algorithms. The allocation engine converts their outputs into joint portfolio weights using risk, correlation, liquidity and cost constraints. It can assign zero to an asset even if its local algorithm is bullish.

Order punching and token placement

Order punching means submitting validated orders through an execution adapter. Order placement concerns orders; asset placement concerns where the resulting inventory is held. An order book is a venue's list of bids and asks, not a custody account. Algorithm budgets are internal limits, not separate funds unless custody and accounting explicitly create separate strategy sleeves.

Minting, providing and statistics

Minting creates WAVE only against recognized contributed value. Burning removes WAVE at finalized redemption. Providing WAVE liquidity on a secondary market is distinct from subscribing to the vault. The statistics service reconciles balances, reports NAV, calculates flow-adjusted returns and publishes valuation timestamps and execution history.

One portfolio across two systems

BNB holds the share ledger and gateway reserve. Your terminal sends orders; the exchange holds the trading balances. Dashed lines carry instructions or reports, not assets.



Solid: portfolio assets. Dashed: instructions, balances or NAV reports.

Read the flow

1. BNB gateway reserve - Accepted deposit and payout token
2. Treasury settlement - Approved funding route
3. Wave exchange accounts - BTC · ETH · SOL · XRP + cash
4. Your trading terminal - Off-chain order submission
5. Reconciliation + NAV - Balances, fills and liabilities
6. WAVE share ledger - Supply, holders and funded claims

03 / Custody across chain and exchange accounts

Where each thing lives

BNB Chain records WAVE supply, holder balances, pending subscription records and withdrawal claims. Native BTC, ETH, SOL and XRP are bought through exchange order books using your own trading terminals. While left on an exchange they are exchange-account balances and claims on that venue, not coins controlled by the WAVE contract or by the terminal. If later withdrawn to native-chain wallets, custody moves to those wallets and must be reconciled separately.

Dedicated backing accounts

Use dedicated Wave accounts or subaccounts whose balances can be attributed entirely to this pool. Your terminal can remain the trading interface, but personal balances and unrelated strategies must not be mixed with WAVE backing. Record each venue's free and order-locked balances once, plus fills, fees, transfers and liabilities. Who legally owns these accounts and what holders can enforce must be specified before accepting public funds.

The settlement connection

A treasury service moves admitted portfolio capital between the BNB gateway and approved exchange deposit routes. The exact asset, token contract and network must be supported by the receiving venue. BNB finality, transfer submission and exchange credit are distinct milestones. If no direct route exists, a separately approved conversion or transfer route is needed; WAVE does not itself bridge assets or make incompatible addresses work. [S4, S5]

Authority and reporting

Your terminal receives approved orders through an order-management adapter. Give its exchange credentials trading permissions without withdrawal authority wherever supported. A separate treasury process authorizes transfers to approved destinations, while a read-only reconciliation service checks balances and fills. An accounting or NAV signer reports off-chain state to the chain under disclosed permissions; its report is an attestation, not a trustless proof of custody. [S6]

What the token can enforce

An on-chain gateway can enforce its own escrow, minting rules, share locks and funded payout claims. It cannot force an exchange to release funds, validate every hidden liability or undo an off-chain trade. Custody, accounting and NAV-reporting operators remain part of the trust model. A reserve improves liquidity only when its assets are available on the required payout network.

04 / Portfolio value and WAVE price

One inventory across all locations

Use one valuation numeraire, U. Each non-cash asset i is recorded by reconciled location v: q_i,v,t units at price P_i,v,t in U per unit. C_chain and C_v are cash values on BNB Chain and at each venue, converted into U; stablecoins are not assumed to equal one dollar. T_rec is conservatively valued recoverable transfers in transit, counted only after removal from the source inventory and before destination credit. Uncertain recovery reduces this value.

$$G_t = C_t^{\text{chain}} + \sum_v C_{v,t} + \sum_v \sum_{i=1}^{N} q_{i,v,t} P_{i,v,t} + T_t^{\text{rec}}$$

Value attributable to WAVE

G_t is gross portfolio value, including pending subscription cash and funded withdrawal cash. D_pending is the pending-deposit liability, W_pay the fixed withdrawal liability, and F accrued unpaid expenses. Net assets A_t back outstanding WAVE. Never remove a reserved asset from G and also subtract its payable. Spent costs already reduce cash and must not remain as unpaid expense liabilities.

$$A_t = G_t - D_t^{\text{pending}} - W_t^{\text{pay}} - F_t$$

Share value and holder value

S_t is outstanding WAVE, including locked but not yet burned shares. With A_t>0 and S_t>0, p_t is NAV per WAVE; n_u,t is user u's share balance. A bootstrap share price is a denomination choice. Zero or negative NAV requires a separate resolution policy.

$$p_t = \frac{A_t}{S_t}, \qquad V_{u,t} = n_{u,t} p_t$$

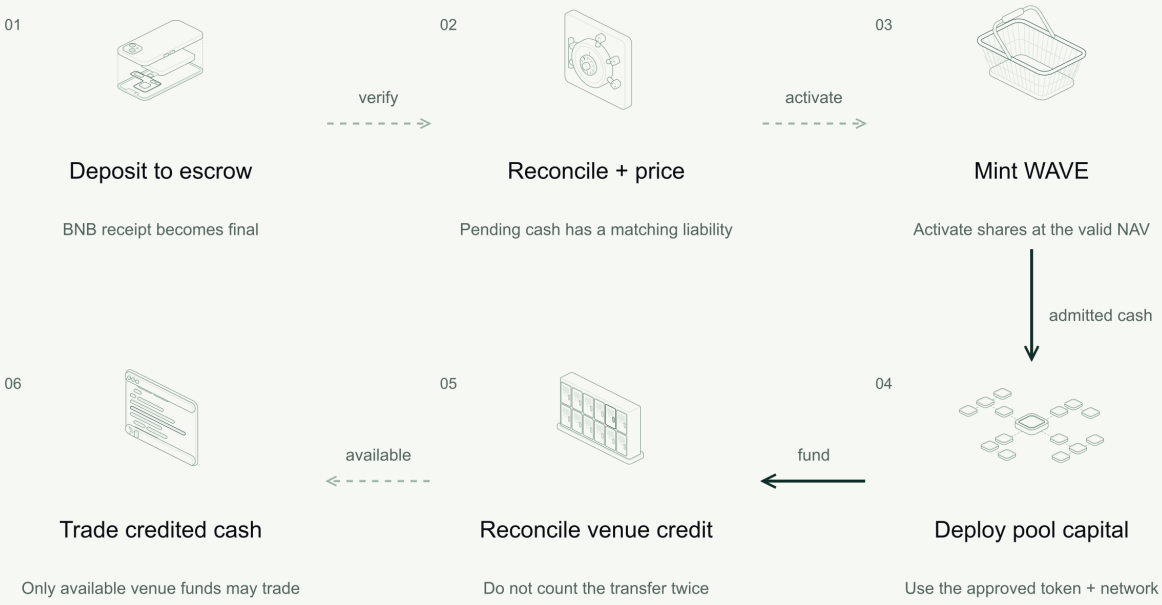
Returns and secondary price

With no rebasing, gains and losses change p rather than the number of shares held. A secondary market price m can diverge from p. Buying WAVE from another holder transfers existing shares and does not itself fund the pool. The NAV report must disclose its cutoff and data age.

$$r_t = \frac{p_t}{p_{t-1}} - 1, \qquad \pi_t = \frac{m_t}{p_t} - 1$$

Deposit to WAVE to deployed capital

Mint against admitted, verified backing at the pricing cutoff. Only then deploy the portfolio’s cash to an exchange; venue credit precedes trading.



The subscription starts at the pricing cutoff. Deployment happens after activation.

Read the flow

1. Deposit to escrow - BNB receipt becomes final
2. Reconcile + price - Pending cash has a matching liability
3. Mint WAVE - Activate shares at the valid NAV
4. Deploy pool capital - Use the approved token + network
5. Reconcile venue credit - Do not count the transfer twice
6. Trade credited cash - Only available venue funds may trade

05 / Deposits minting and dilution

1 Deposit into BNB escrow

The user deposits an approved settlement token U into the BNB gateway with a request identifier and minimum-share condition. The service waits for the network finality policy and confirms the amount actually received. Pending capital is not traded. It appears once as cash in gross assets and once as a matching pending-deposit liability, so existing WAVE does not gain value merely because someone is waiting to subscribe.

2 Price and activate the subscription

At a disclosed batch cutoff, reconcile existing backing, use fresh valuations and calculate pre-subscription NAV per share p minus. Measure the admitted net contribution D_net after explicitly charged entry costs. Release that amount from the pending-deposit liability and mint the corresponding shares. The backing can still be cash in the BNB gateway: it need not already have been spent on BTC or any other asset.

$$D_{\text{net}} = D - c_{\text{in}}, \qquad \Delta S = \frac{D_{\text{net}}}{p^{-}}$$

3 Preserve the share price

In real arithmetic, admitting value D_net and issuing Delta S leaves NAV per share unchanged. Implementation rounds share issuance down in share subunits and enforces minimum output and dust limits. If a subscription fails before activation, resolve or refund the pending request rather than issuing unbacked WAVE. The pricing cutoff starts the new holder's portfolio exposure.

$$A^{+} = A^{-} + D_{\text{net}}, \qquad S^{+} = S^{-} + \Delta S, \qquad p^{+} = p^{-}$$

4 Deploy admitted capital

After activation, the treasury releases approved portfolio cash to an allowlisted exchange funding route. Track approved, sent, in transit, credited and reconciled states under one transfer identifier. Count the value once as it moves, recognizing actual costs and any impairment. Only credited, available venue balances may fund orders. A transfer is not a profit and exchange credit does not create a second asset.

Timing and pre-funding

The initial model admits subscriptions only at valid pricing events; the user cannot retrospectively choose the best NAV after seeing a delayed report. An operator may pre-fund venue cash, but that funding must be recorded as paid-in equity or a loan payable, with disclosed terms. It is not free WAVE backing. Subscription cutoffs, cancellation and refund rules remain implementation decisions.

06 / Asset algorithms and AI selection

Per-asset strategy registry

Each strategy version declares its asset, forecast horizon, data inputs, required latency, eligible market regimes, allowed actions and estimated trading costs. The user will supply the actual algorithms. This overview does not invent BTC or ETH trading rules. A cash or no-trade action must remain available when evidence is weak or data is invalid.

Comparable outputs

For asset i and strategy k, let mu_hat_i,k,t be a forecast of simple return over the common horizon and a_i,k,t its nonnegative selection weight. Weights sum to one over eligible candidates for that asset. The blended forecast is an input to allocation, not an instruction to buy. Forecast uncertainty, liquidity and cross-asset covariance remain separate inputs. [R3, R4]

$$\widehat{\mu}_{i,t} = \sum_k a_{i,k,t}\widehat{\mu}_{i,k,t}, \qquad a_{i,k,t} \geq 0, \quad \sum_k a_{i,k,t} = 1$$

An interpretable selection baseline

One research baseline updates eligible strategy weights using bounded, delayed out-of-sample losses ell_i,k,t. Eta controls responsiveness. Losses should measure a declared prediction objective or comparable risk-normalized, cost-adjusted shadow strategy outcome; raw profits from unequal budgets cannot be compared directly. Multiplicative weights is a starting point for testing, not the selected production AI. [R3]

$$a_{i,k,t+1} = \frac{a_{i,k,t}\exp(-\eta\ell_{i,k,t})}{\sum_j a_{i,j,t}\exp(-\eta\ell_{i,j,t})}$$

Training and authority boundaries

Features at decision time may use only information then available. Candidate evaluation must record every trial and model version. A model chooses among registered strategies; it cannot add an unknown asset, change custody, increase leverage or bypass risk controls. An LLM-generated explanation is not authorization for a trade.

07 / Allocation and portfolio constraints

Joint optimization

Let w tilde be current marked-to-market weights of the assets economically attributable to WAVE, including net cash. All pending-deposit and withdrawal obligations in this initial model are cash-collateralized. Let mu hat be the expected-return vector and Sigma a positive semidefinite covariance estimate over the same horizon. Define J as expected return minus risk and estimated trading costs, in return units. The allocator selects feasible weights; it does not send orders directly. [R1, R2]

$$J_t(\mathbf{w}) = \widehat{\boldsymbol{\mu}}_t^{\top}\mathbf{w} - \frac{\lambda}{2}\mathbf{w}^{\top}\Sigma_t\mathbf{w} - \hat{c}_t(\mathbf{w} - \widetilde{\mathbf{w}}_t)$$

$$\mathbf{w}_t^{\star} = \arg\max_{\mathbf{w}\in\mathcal{W}_t} J_t(\mathbf{w})$$

Feasible weights

For the initial long-only proposal, cash is asset 0. b_i caps concentration, rho is the minimum reserve fraction and T_max bounds one-way traded weight. Set caps using liquidity and custody exposure as well as market risk. A cash-dominant feasible fallback is required. Numerical values are not fixed in this overview.

$$\sum_{i=0}^{N} w_i = 1, \qquad 0 \le w_i \le b_i, \qquad w_0 \ge \rho$$

$$\frac{1}{2}\sum_{i=0}^{N} |w_i - \widetilde{w}_{i,t}| \le \tau_{\max}$$

Costs and units

Cost_hat is a fraction of NAV, including estimated fees, spread, impact and gas. Returns, covariance and costs must use a common decision horizon. Lambda sets risk aversion; it is not a guaranteed risk level. Available cash, minimum order sizes, instrument precision, venue exposure and settlement constraints also restrict executable trades.

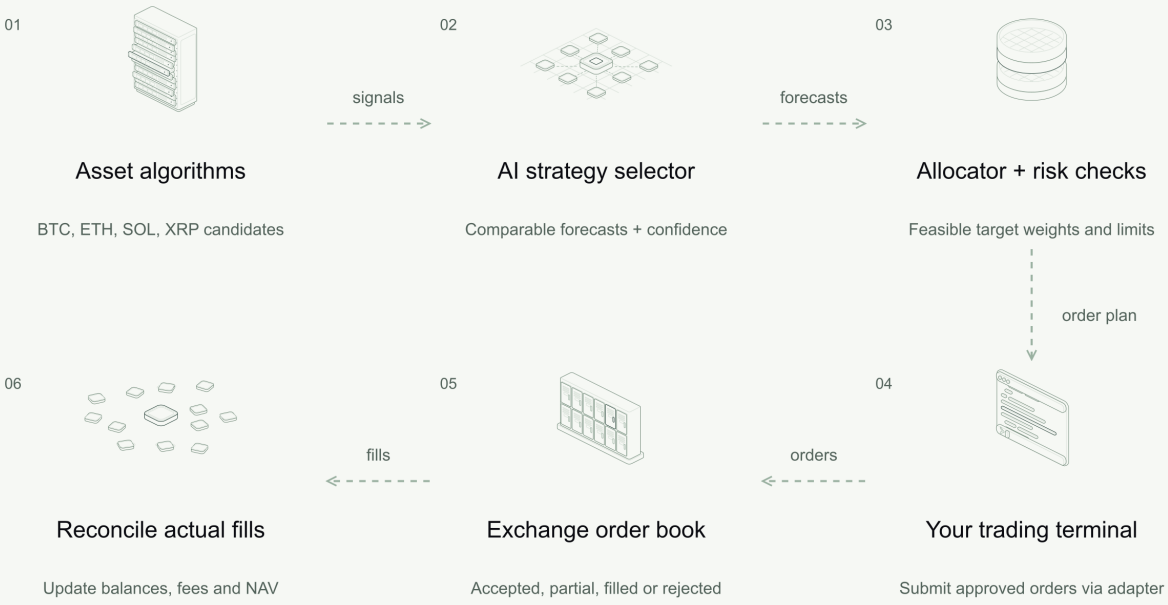
When no trade is correct

Candidate improvements can be smaller than execution costs and forecast error. Require the estimated gain in net objective to exceed a policy margin epsilon and satisfy a drift or scheduled-review condition before trading. This reduces unnecessary turnover; it does not establish that a forecast is profitable. Risk breaches trigger an independent constrained response rather than waiting for model confidence.

$$J_t(\mathbf{w}_t^{\star}) - J_t(\widetilde{\mathbf{w}}_t) > \varepsilon$$

Your terminal is the execution layer

Algorithm selection, allocation and risk checks lead to an off-chain order. Only reconciled fills change portfolio inventory; acknowledgements and target weights are not holdings.



No BNB transaction is required for each exchange order. Report reconciled outcomes separately.

Read the flow

1. Asset algorithms - BTC, ETH, SOL, XRP candidates
2. AI strategy selector - Comparable forecasts + confidence
3. Allocator + risk checks - Feasible target weights and limits
4. Your trading terminal - Submit approved orders via adapter
5. Exchange order book - Accepted, partial, filled or rejected
6. Reconcile actual fills - Update balances, fees and NAV

08 / Rebalancing and order execution

From weights to quantities

For trade sizing only, Q_i is reconciled total units of asset i across venues and approved custody wallets, with no duplicated transfers. The equation assumes a common reference price P_i across locations; NAV may use a distinct conservative valuation for impaired claims. Delta q is a pre-cost aggregate target. The terminal adapter splits it into venue orders using actual available inventory and quote balances; real costs and fills require re-solving. Positive Delta q means buy and negative means sell.

$$\widetilde{w}_{i,t} = \frac{Q_{i,t}P_{i,t}}{A_t}, \qquad \Delta q_{i,t} = \frac{w^{\star}_{i,t}A_t - Q_{i,t}P_{i,t}}{P_{i,t}}$$

Execution sequence

The recommendation and allocation services produce a versioned plan. An independent risk check validates it. Your order-management adapter then sends approved instructions to your own terminals, which submit orders to the exchange order books off-chain. No BNB transaction is required for each buy or sell. The exchanges return acknowledgements and fills; the accounting service reconciles them before publishing updated holdings and NAV. Separate periodic on-chain NAV reports do not execute the trades. [S7]

Orders and partial fills

Track proposed, approved, submitted, partially filled, filled, cancelled, rejected and unknown order states. Persist unique client identifiers and reconcile venue status before retrying a timeout. Deduplicate fills by venue execution identifier. An open order reserves inventory but is not a new asset; a partial fill changes balances only by its executed quantity and fees. Any manual terminal trades must enter the same reconciliation ledger; unrecognized orders or balances block new subscription and redemption pricing.

Costs and protective controls

Pre-trade controls bound notional size, price deviation, slippage, venue exposure and available inventory. Execution may split orders across time or liquidity, balancing market impact against delay risk. Record actual fees, spread and impact after completion. Almgren-Chriss motivates that tradeoff; its assumptions require adaptation to crypto venues. [R5] Here x_j is filled asset quantity, d_j is +1 for a buy and -1 for a sell, and both prices are in the same settlement units per asset unit. The equation measures the filled portion; report unfilled opportunity costs separately.

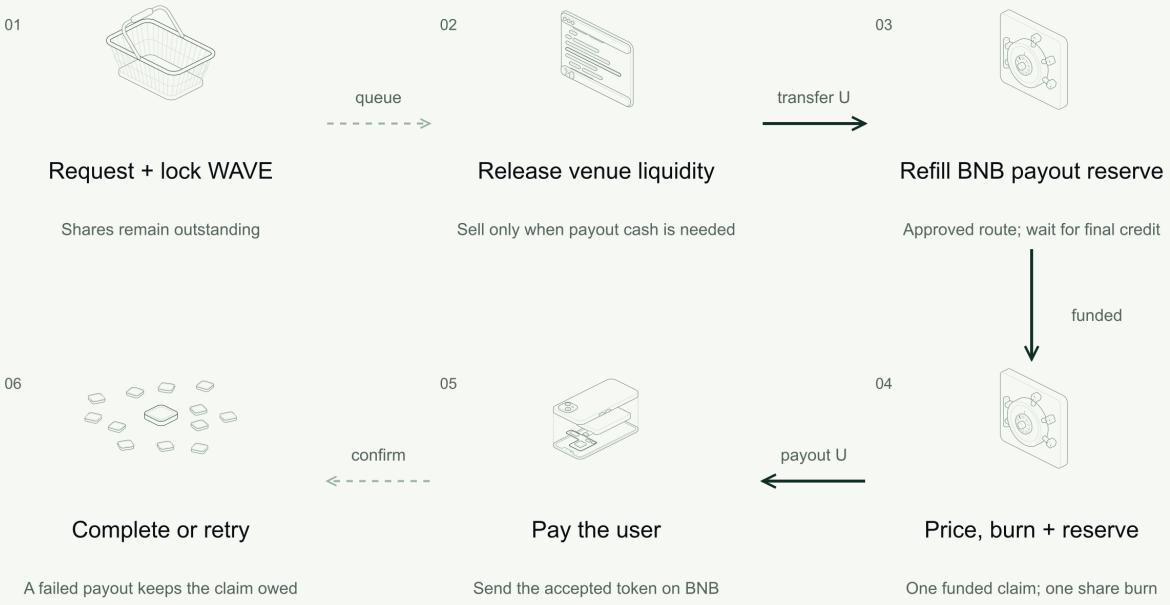
$$\mathrm{IS}_{\mathrm{filled}} = \sum_j d_j x_j \left(P_j^{\mathrm{fill}} - P_j^{\mathrm{arrival}}\right) + f_{\mathrm{venue}} + f_{\mathrm{network}}$$

Existing contract limitations

The current contract has a one-hour notice and 24-hour cooldown, fixed components, at most eight trades, 20% sell turnover and a 60% concentration cap. It cannot simply become a fast AI trader by adding an API. New execution cadence, authorization, cancellation, settlement and protective limits must be designed and tested. None of its existing limits is silently carried into this proposal.

A withdrawal is a funded settlement

Lock shares, obtain payout cash on BNB, then price and burn into a funded claim. A failed transfer keeps the claim owed; it does not mint or burn again.



Before pricing: locked shares remain exposed. After burn: the fixed claim is owed.

Read the flow

1. Request + lock WAVE - Shares remain outstanding
2. Release venue liquidity - Sell only when payout cash is needed
3. Refill BNB payout reserve - Approved route; wait for final credit
4. Price, burn + reserve - One funded claim; one share burn
5. Pay the user - Send the accepted token on BNB
6. Complete or retry - A failed payout keeps the claim owed

09 / Withdrawals and liquidity reserves

1 Lock shares without burning

The user requests redemption and locks s WAVE in the BNB gateway. Locked shares remain in outstanding supply and retain exposure to portfolio gains and losses until the pricing and finalization event. The request is not yet a fixed cash liability. Cancellation rules must prevent duplicate use of locked shares and define when a request becomes irrevocable.

2 Fund the payout on BNB

Use free payout reserves on BNB when available. If needed, your terminals sell assets on exchange, the venue settles the fills, and a separate treasury process withdraws the accepted payout token through an approved network route. Wait for actual credit and finality in the BNB payout reserve. Cash visible only in an exchange account cannot fund an immediate BNB claim. If it cannot be moved, the request stays queued and the shares are not burned under this proposed policy.

3 Price burn and establish a funded claim

At a valid finalization cutoff, compute gross entitlement E from s and pre-event NAV p minus. In one proposed on-chain state transition, burn s shares, reserve E in the gateway and record a claim identifier. The recipient receives E minus a newly charged exit processing fee f_out; the fee is paid or reserved separately. Total value assigned out of the pool remains E. Fees or liquidation costs already recognized in NAV must not be charged again.

$$E = s\,p^{-}, \qquad R_{\text{user}} = E - f_{\text{out}}$$
$$A^{+} = A^{-} - E, \qquad S^{+} = S^{-} - s$$

4 Pay the recorded claim

Pay the user from the gateway reserve. Paying a gross claim E across user and fee recipients reduces cash by E and discharges its payables by E; it does not reduce WAVE NAV a second time. A failed payout keeps the funded claim owed and uses the same identifier on retry. Native-coin delivery is outside this initial route; it would need separate chain-specific payout and pricing rules.

$$\Delta G = -E, \qquad \Delta W^{\text{pay}} = -E, \qquad \Delta A = 0$$

Available liquidity is location specific

For each venue or chain location v, available cash is its cash balance minus disjoint pending-deposit, funded-payout, open-order and other earmarks. These categories must not overlap. BNB withdrawals use free BNB cash, not the sum of every exchange balance. Exchange outages, frozen withdrawals or mismatched token networks can delay payout even when reported pool NAV is positive.

$$C_v^{\text{free}} = C_v - D_v^{\text{cash}} - W_v^{\text{cash}} - O_v^{\text{cash}} - H_v^{\text{cash}}$$

10 / Returns reporting and numerical example

Worked pool example

Assume 100,000 settlement units of net assets and 100,000 WAVE: NAV is 1.00 per WAVE. A user contributes 1,000 with zero entry cost in this example and receives 1,000 WAVE. Net assets become 101,000 and supply becomes 101,000. The deposit itself creates no return.

$$p^{+} = \frac{100{,}000 + 1{,}000}{100{,}000 + 1{,}000} = 1.00\ U/\mathrm{WAVE}$$

Gains and losses

Suppose the portfolio then grows to 111,100 after all accrued costs, with unchanged supply. NAV becomes 1.10 and the user's 1,000 WAVE is worth 1,100 at NAV. No extra WAVE is minted for that gain. If net assets instead fall to 90,900, NAV is 0.90 and that holding is worth 900. These are arithmetic examples, not forecasts.

$$p_{\text{gain}} = \frac{111{,}100}{101{,}000} = 1.10, \qquad p_{\text{loss}} = \frac{90{,}900}{101{,}000} = 0.90$$

Exit consistency

In the gain scenario, redeeming 1,000 WAVE with zero exit cost establishes a 1,100 payable and burns 1,000 shares. Assets attributable to remaining WAVE become 110,000 and supply becomes 100,000, preserving NAV at 1.10. Payout discharges the liability; it must not reduce NAV a second time.

$$p_{\text{after burn}} = \frac{111{,}100 - 1{,}100}{101{,}000 - 1{,}000} = 1.10$$

Flow-adjusted performance

Pool performance should use the compounded NAV-per-share return across periods, provided share issuance, burns and fee accrual are correct. Total assets growing through deposits is not investment performance. Report realized weights, NAV age, transaction costs, reserve fraction, custody exposure and drawdown. Holder profit must include purchases, sales and transfers; share balance alone does not reveal cost basis.

$$\mathrm{TWR}_{0:T} = \prod_{t=1}^{T}(1 + r_t) - 1, \qquad \mathrm{DD}_t = 1 - \frac{p_t}{\max_{0 \le s \le t} p_s}$$

11 / Risk governance and economic policy

Independent risk authority

A deterministic policy layer validates model output before execution. It enforces approved instruments, concentration, liquidity, turnover, venue exposure and order limits. Trading can be disabled independently of share accounting. Authority over strategy registration, policy changes, custody permissions and emergency action must be disclosed; the AI cannot grant itself permissions.

Operational failure modes

Incorrect prices, compromised API keys, strategy errors, stale reconciliation, depegged representations, venue insolvency and partial execution can impair NAV and redemption. Price or balance uncertainty should block new pricing events until a defined recovery process establishes a valid value. A model-confidence score does not resolve missing collateral or unavailable custody.

Fees and incentives

No fee schedule is selected here. Management fees, performance fees, entry costs and exit costs must be distinguished. A performance fee needs an explicit high-water-mark and equalization policy so later depositors do not pay for someone else's earlier gains. Fee-share minting dilutes other shares and must be included in reported net performance. There is no assumed separate governance-token reward scheme.

Validation before capital deployment

Require deterministic replay, reconciliation tests, accounting invariants, cost-aware walk-forward studies, paper trading, execution failure drills and independent review. Record all tested variants to assess selection bias. Backtest overfitting and distribution changes mean favorable historical results are insufficient evidence of future profit. [R6, R7]

What remains undecided

The custody direction is now exchange-held native exposures executed through the founder's terminals, with WAVE and the gateway on BNB Chain. Exact venues, dedicated account ownership, settlement token and supported networks, strategy algorithms, decision horizon, risk limits, reserve targets, fee schedule, NAV-signing authority and redemption deadlines remain to be specified. This paper makes no claim that off-chain balances are fully enforceable by the token contract.

12 / Research map and implementation path

How to use the research

The reading list is a curated starting set, not every paper in the field. It links allocation, strategy selection, execution and validation literature to concrete design choices. The equations above are proposed Wave accounting definitions and adaptations of general methods, not a claim that any cited author designed or validated Wave. Empirical paper results are not Wave performance estimates.

Read in this order

Start with pooled NAV and share accounting, then portfolio allocation [R1, R2], online strategy selection [R3], crypto deep reinforcement learning as an alternative [R4], execution costs [R5], and validation [R6, R7]. The companion research file includes additional reading and explicit limitations for discussion.

Implementation sequence

First settle the pooled ownership and custody model. Next specify algorithms and common data horizons, then build a reproducible research and paper-trading environment. Implement a reconciliation ledger and share accounting before connecting execution. Add a constrained allocator, bounded order adapters and withdrawal settlement. Only then consider a restricted live pilot after the required reviews and operational checks.

Immediate design questions

Which exchange accounts are the backing accounts, and can the terminals submit and reconcile every order through an adapter? Which exact token and network connect those accounts to the BNB gateway in both directions? Who authorizes transfers and NAV reports? These are the remaining custody implementation questions; trading execution itself is confirmed as off-chain.

Symbols and units

U

Common valuation unit; the accepted token and its pricing must be specified.

G, A

Gross assets and net assets attributable to outstanding WAVE, measured in U.

q, P

Reconciled asset quantity and its value per unit in U, indexed by asset and location.

C, T

Cash value and conservatively recoverable value of transfers in transit.

D pending, W pay, F

Pending deposits, fixed withdrawal payables and accrued unpaid expenses.

S, p, n

Outstanding shares, NAV per share and an individual holder’s share balance.

w, mu, Sigma

Portfolio weights, expected returns and covariance over one common horizon.

E, f out

Gross finalized redemption entitlement and a newly charged processing fee.

Accounting convention

Pending-deposit and payout cash remains in gross assets until it moves. Its matching liability is deducted once. Every transfer occupies exactly one source, transit or destination bucket at a time. Costs already paid reduce cash; only unpaid accrued costs belong in the expense liability.

Research bibliography

Primary papers and official documentation. Academic methods motivate allocation, selection, execution and evaluation; they do not validate Wave custody or investment performance. Venue API references illustrate interfaces without selecting an exchange.

[R1] Markowitz (1952), Portfolio Selection

Foundation for joint expected-return and covariance-risk allocation; estimates and constraints still need specification.

Open primary source

[R2] Boyd et al. (2017), Multi-Period Trading via Convex Optimization

Separates forecasts from constrained trading and explicitly includes costs. Closest starting point for the allocation layer.

Open primary source

[R3] Arora, Hazan and Kale (2012), The Multiplicative Weights Update Method

A transparent candidate for combining eligible strategy experts; regret results do not guarantee investment profits.

Open primary source

[R4] Jiang, Xu and Liang (2017), A Deep Reinforcement Learning Framework for the Financial Portfolio Management Problem

Crypto portfolio-weight learning research; historical experiments do not establish live feasibility for this design.

Open primary source

[R5] Almgren and Chriss (2001; manuscript 2000), Optimal Execution of Portfolio Transactions

Execution risk and market-impact tradeoff; venue-specific calibration is required.

Open primary source

[R6] Bailey et al. (2017; manuscript revised 2015), The Probability of Backtest Overfitting

A framework for evaluating how strategy selection can overfit historical backtests.

Open primary source

[R7] Bailey and Lopez de Prado (2014), The Deflated Sharpe Ratio

Adjusts performance assessment for selection bias and non-normal returns; complements chronological out-of-sample evaluation.

Open primary source

[R8] Black and Litterman (1992), Global Portfolio Optimization

A framework for combining prior allocations, views and confidence; crypto-specific priors require justification.

Open primary source

[R9] Freund and Schapire (1997), A Decision-Theoretic Generalization of On-Line Learning and an Application to Boosting

Expert combination and online resource allocation; comparable feedback is essential.

Open primary source

[R10] Auer et al. (2002), The Nonstochastic Multiarmed Bandit Problem

Algorithm selection under partial feedback; exploration has real costs in a live portfolio.

Open primary source

[R11] Rockafellar and Uryasev (2000), Optimization of Conditional Value-at-Risk

A scenario-based tail-risk optimization approach; modeled limits cannot bound all real losses.

Open primary source

[S1] BNB Chain, BNB Smart Chain

Official network overview. A deployment network is not a cross-chain custody mechanism.

Open primary source

[S2] BNB Chain, BEP-20 token standard

Official share-token interface context; the protocol still needs backing and settlement rules.

Open primary source

[S3] ERC-4626, Tokenized Vaults

Useful share and asset API reference for a single settlement asset. This proposal does not assert compliance, particularly for asynchronous or external-custody settlement.

Open primary source

[S4] BNB Chain, What Sub-Second Finality Means for BSC Settlement

Use the finalized block tag where supported; network finality and exchange credit are distinct.

Open primary source

[S5] Bybit API, Get Coin Info

Illustrative venue documentation for per-asset, per-network deposit and withdrawal status, confirmations and fees. No venue is selected here.

Open primary source

[S6] Kraken, How to create an API key on Kraken Pro

Illustrates separation of order permissions from withdrawal permissions.

Open primary source

[S7] Coinbase Advanced Trade, Create Order

Illustrative primary order API documentation; the founder’s terminal and actual venues still need their own adapters.

Open primary source

[D1] Lucas Marques, Hairline documentation

MIT-licensed SVG figures used in the custody, deposit, execution and withdrawal diagrams.

Open primary source