

Identity-native infrastructure. Enduring accounts.

A Layer 1 architecture for recoverable ownership,
governed operations and transparent token economics.

IDENTITY

Human-readable access

CONTROL

Recoverable accounts

ACCOUNTABILITY

Bounded authority

DOCUMENT SCOPE

How to read this paper

An institutional product vision grounded in a working development network.

DESIGN & IMPLEMENTATION

Purpose and audience

This paper presents the Vayos protocol, its economic rules and its intended institutional service layer. It is written for technology leaders, infrastructure operators, prospective integration partners, custody teams and stakeholders assessing the project. It is not a representation that these organizations already use or endorse Vayos.

Three distinct evidence levels

Label	Meaning
DEVNET VERIFIED	A named capability has supporting local-chain execution evidence. This is not public-network acceptance.
IMPLEMENTED / TESTED	Code and development tests exist. Coverage varies; not every scenario has been exercised on the persistent devnet.
PLANNED	A proposed product capability or deployment requirement. Not delivered, contracted or independently certified.

The reference deployment is the private, single-validator vayos-devnet-1. Separate four-validator rehearsals run on one host; they do not establish independent operator distribution. The latest development changes are not yet a clean, tagged public release.

Important limitations

No independent security audit, regulatory approval, production availability commitment, guaranteed token value or guaranteed investment return is asserted. Do not use real funds or real identity documents in the development environment. Token prices and yield figures describe design assumptions, not an offer.

CONTENTS

The document map

A system view first, then economics, controls and delivery requirements.

DESIGN & IMPLEMENTATION

Part	Sections / pages
I. Institutional proposition	03-06 Contents, thesis, audiences and operating journeys
II. Protocol and identity	07-12 Architecture, stable accounts, KYC, recovery, staking and fees
III. Economic design	13-18 Allocation, sale phases, vesting, fund controls, liquidity and governance
IV. Operations and products	19-23 Multisig custody, portal, integrations, security and privacy
V. Delivery and assurance	24-27 Roadmap, status matrix, evidence and risk
VI. Capability expansion	28-33 Proposed extensions, institutional workflows and acceptance gates
Reference appendix	34 Sources, terminology and publication notes

The central distinction

Vayos aims to make account continuity a protocol concern while keeping sensitive identity processing outside public consensus. An identity points to a stable account. A controller key authorizes actions, but is not the account itself. Recovery changes authority without requiring a new public financial identity.

Read by responsibility

- Institutional decision-makers: start with the thesis, target audiences, risk register and gated roadmap.
- Engineers and custody teams: focus on account semantics, signer separation, trust boundaries and integration requirements.
- Economic and governance reviewers: examine supply, unlock schedules, budget authority and the distinction between VAY reserves and external company capital.

Diagrams are explanatory architecture views. Planned components are labeled. The source appendix identifies the project records used to prepare this edition.

01 / INSTITUTIONAL THESIS

Designed for continuity

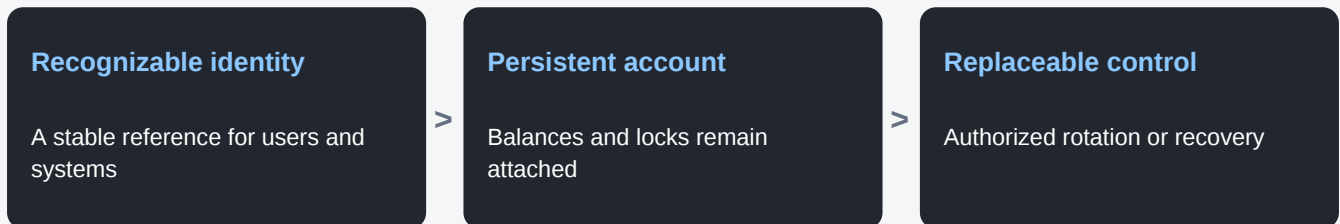
A blockchain account should outlast the device or key that currently controls it.

DESIGN & IMPLEMENTATION

Vayos is being developed as an identity-native Layer 1: a network where readable identities, stable accounts and controlled recovery are first-class protocol capabilities. The institutional ambition is not simply faster asset transfers. It is a more manageable operational relationship between users, keys, balances and accountable authority.

The problem the architecture addresses

A raw key-based account couples access and ownership tightly. Losing a signing key can disrupt operations; rotating it can force counterparties to update addresses and internal records. Vayos separates a persistent identity and account from the replaceable controller that authorizes activity.



Institutional design principles

- Continuity: preserve account references through authorized key changes.
- Bounded authority: assign operational roles without unrestricted access to every fund.
- Reviewability: make budgets, vesting and execution evidence inspectable.
- Data minimization: keep documents and biometrics out of public chain state.

Institutional orientation is a design goal

A working devnet is the foundation, not proof of enterprise readiness. Legal onboarding, privacy controls, service operations, independent security review and partner validation remain delivery gates.

02 / AUDIENCES

Who Vayos is intended for

Multiple institutional roles, with different responsibilities and adoption conditions.

TARGET AUDIENCES / PROPOSED ADOPTION

Audience	Potential value	Required before adoption
Banks and payment institutions	Stable customer references, controlled recovery and inspectable transfers.	Licensing analysis, payment integration, risk controls and private data operations.
Custodians and wallet providers	Account continuity, role separation and customer recovery workflows.	Signing compatibility, custody policies, independent key control and audit.
Enterprises and treasury teams	Governed allocation, planned disbursements and transparent VAY budgets.	Accounting integration, authorization workflows and reconciliation.
Fintechs and applications	Readable identities, user-facing wallets and limited gas sponsorship.	SDKs, reliable public endpoints, onboarding and abuse controls.
Institutional ecosystem partners	Integration grants with acceptance and vesting conditions.	Defined deliverables, contracts, evidence review and support processes.
Validators and infrastructure providers	Network operation, delegated security and transparent rewards.	Independent infrastructure, secure signing and operating standards.

End users and delegators remain essential participants. Institutional distribution must not obscure who controls an account, what is public, which tokens are locked or what recovery powers have been enabled.

03 / USE CASES

Institutional operating journeys

Illustrative workflows, not announced customers or live institutional deployments.

PROPOSED JOURNEYS / PARTIALLY SUPPORTED BY PROTOCOL

Customer account continuity

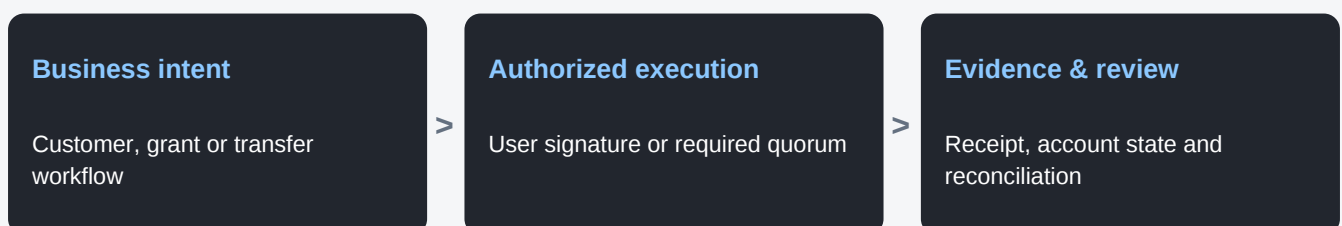
A wallet provider creates a readable identity and a stable account for a customer. A private identity process may attest KYC status. The customer explicitly enables an approved recovery route. If access is lost, fresh verification and a delayed on-chain process can replace the controller while preserving the account and its vesting state.

Enterprise allocation and partner delivery

An authorized treasury quorum approves an allocation within a named VAY fund and category. Commitments consume available limits. Partner grants require an acceptance reference and the configured delay before activation. The chain enforces token rules; a separate business process establishes whether work was genuinely delivered.

Application-led onboarding

An application can present usernames and wallet balances without requiring users to reason about raw addresses. A bounded gas sponsorship pilot supports a narrow stable-account transfer path. A broad application platform, identity onboarding experience and transaction-signing interface remain planned work.



What is not being claimed

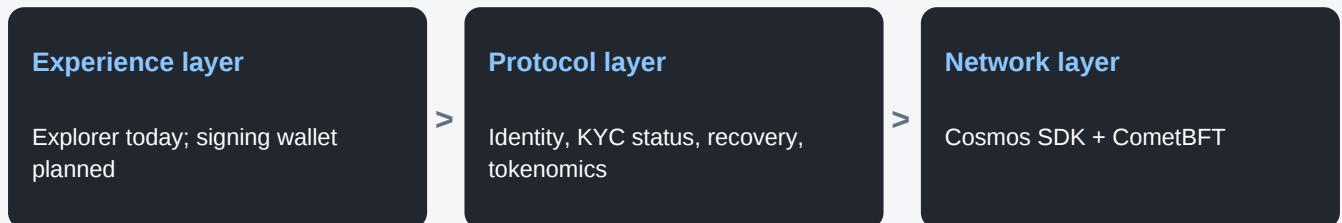
Vayos does not currently provide a bank account, licensed payment service, deposit insurance, confidential settlement, a stablecoin or a production tokenized-securities platform. These require separate product, legal and technical decisions.

04 / ARCHITECTURE

One chain, distinct trust zones

Keep public consensus, signing authority and private identity processing separate.

DESIGN & IMPLEMENTATION



Zone	Contents	Boundary
Public on-chain state	Identities, balances, locks, KYC metadata, requests, budgets and receipts.	Visible and linkable. No personal documents or face templates.
Signing environment	User controllers, operational multisigs and validator consensus keys.	Separate duties and key stores. Private keys never belong in genesis or portal inputs.
Private institutional services	Document checks, liveness, evidence retention and case management.	Planned. Access-controlled storage outside validator replication.

The implementation boundary

The existing chain wires custom identity, KYC, recovery and tokenomics modules into SDK account, bank, staking, distribution and governance behavior. Registered messages and keeper checks enforce authority and economic constraints. The portal reads a bounded set of local endpoints; it is not a general transaction relay.

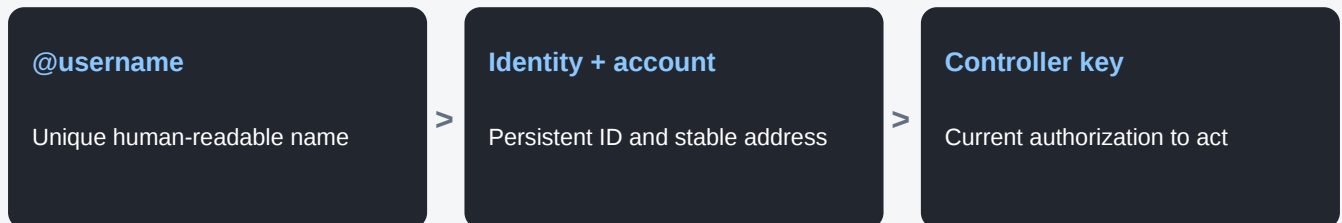
A KYC issuer bridges private verification and public attestations. Consensus verifies that an authorized issuer signed the appropriate statement. It cannot independently establish that a document or a liveness session was genuine.

05 / STABLE ACCOUNTS

Identity is not the private key

A persistent reference with a replaceable authorization layer.

IMPLEMENTED / DEVNET IDENTITY & TRANSFERS VERIFIED



The identity record includes `identity_id`, `username`, `controller_address`, `status` and `created_at`, with a deterministic stable account address. Unique mappings prevent duplicate usernames and conflicting controller assignments under current rules. Queries resolve an identity by ID or username.

Two balances must not be confused

The stable account owns the identity-linked balance. The controller address is a separate technical account and ordinarily pays transaction fees. Displaying only the controller balance would hide funds held by the stable account. Wallets must make this distinction explicit.

Supported account actions

- Create and resolve an identity; inspect its current controller and status.
- Rotate control through authorized paths without changing the stable address.
- Send unlocked funds from the stable account using the active controller.
- Manage supported stable-account staking actions while preserving lock checks.

Scope of continuity

Recovery preserves the on-chain stable account. External applications must still refresh controller caches and review their own sessions, permissions and off-chain records. A unique username is not proof of a unique human.

06 / IDENTITY ASSURANCE

KYC without publishing documents

Public status, private evidence, explicit issuer responsibility.

ON-CHAIN IMPLEMENTED / PRIVATE VERIFICATION SERVICE PLANNED

Public chain	Private service - planned
Identity ID, KYC status and issuer	Document evidence and verification case records
Credential commitment, issue time and expiry	Liveness session evidence and review decisions
Revision and recovery-related commitments	Retention rules, access logs and authorized disclosure workflows

An authorized issuer attests a credential status and expiry. An operational issuer cannot overwrite another issuer's record. Credential updates increment a revision so a stale recovery request cannot silently reuse an earlier assurance state. A stored VERIFIED label must be evaluated together with its expiry and issuer authorization.

Planned institution-operated verification

The intended private service would be operated under Vayos-defined governance and security procedures rather than embedding personal records into the chain. It would combine document checks, liveness, exception handling and human review. Model choice, deployment, testing and operational accountability are not yet completed.

- Use unpredictable session challenges and bind recovery verification to the identity, new key, chain and purpose.
- Prevent replay and video injection; test false acceptance, false rejection and accessibility impacts.
- Use opaque, salted commitments, not unsalted hashes of names, passport numbers or face templates.

Privacy boundary

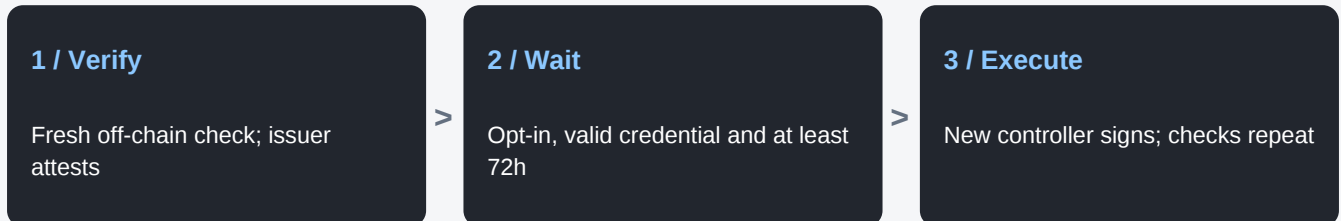
This is not zero-knowledge KYC or anonymous payments. Identity links, status, issuer and recovery timing remain public. An institution must decide whether that disclosure is acceptable for each product.

07 / ACCOUNT RECOVERY

Recovery with time to respond

A controlled change of authority, not a transfer to a new financial account.

IMPLEMENTED / LIVE FINAL EXECUTION PENDING



KYC recovery requires explicit owner opt-in to an authorized issuer, an active identity, a valid credential and a fresh proof commitment. Guardian recovery remains an independent option. KYC-enabled configurations require a delay between 72 hours and 30 days.

The request binds the original controller, new controller, issuer and credential revision. At execution the chain rechecks relevant state. Execution must occur before the earlier of credential expiry and seven days after the execution deadline. The new controller must sign; the issuer cannot simply forge that signature.

Cancellation and invalidation

The current controller, issuer or proposed new controller can cancel a KYC request. Changed credential revisions, expiry, revoked assurance or a changed controller can invalidate execution. Used proof commitments remain used after cancellation and export/import.

Live development evidence

The synthetic fixture verified KYC issuance, owner opt-in, premature-execution rejection and cancellation. Request recovery-000002 becomes executable on 1 October 2026 at 01:41:12 UTC. Final live execution and post-recovery checks remain pending as of this edition.

Issuer compromise remains a takeover risk for opted-in accounts: an attacker controlling the issuer and a destination key may succeed if no cancellation occurs. Independent signers and customer alerts are important production requirements.

Delegation and reward ownership

Separate the delegated principal, earned rewards and validator commission.

IMPLEMENTED / DEVELOPMENT TEST COVERAGE

Delegators commit their own unlocked VAY to a validator. Validators participate in consensus and earn commission from delegator rewards, not from the delegated principal. Slashing, validator performance, liquidity constraints and market risk remain relevant.

Rule	Current design
Gross annual target	6% on active delegated stake; a target, not a guaranteed APR.
Reserve subsidy	Fills the eligible reward gap subject to available funds and approved budgets.
First-year subsidy ceiling	18M VAY, time-proportional; no automatic second-year budget.
Validator commission	5-20%, with maximum daily increase of one percentage point.
Unbonding	21 days under the current policy. Not instant withdrawal.
Locked allocations	Locked sale grants and undistributed funds do not create staking or voting power.

Stable-account staking

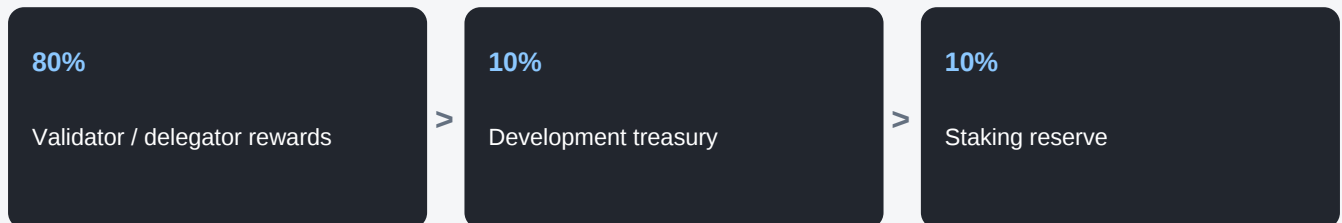
The current controller can delegate unlocked stable-account funds, undelegate and withdraw supported rewards. Rewards must return to the stable address, including hook-triggered withdrawals. A controller change does not move stake or unbonding ownership to the controller address.

Stable-wallet governance voting, redelegation, unbonding cancellation and browser staking controls are not delivered by this implementation. These must be designed and tested separately.

09 / TRANSACTION ECONOMICS

Fees fund security and operations

The transfer amount belongs to the recipient. Only the transaction fee is divided.

DESIGN & IMPLEMENTATION

For an illustrative 0.001 VAY transaction fee, 0.0008 VAY routes toward rewards, 0.0001 VAY to development treasury and 0.0001 VAY to the staking reserve, before downstream reward and commission behavior. This illustration is not a universal fixed-price fee quotation.

Subsidy is a separate flow

Reserve top-ups flow entirely to rewards and are not split again by 80/10/10. Fee income reduces the required reserve contribution toward the target. Both 10% portions round down in base units; the remainder belongs to rewards. The subsidy calculation caps its elapsed interval at 60 seconds to avoid a large retroactive payout after a chain halt.

Gas sponsorship pilot

An authorized treasury quorum can reserve a quota for a particular identity and budget year, with total and per-transaction limits, expiry and an initial delay. The current pilot accepts a narrow, single-message stable-account transfer. It is not unrestricted sponsorship for arbitrary applications or message bundles.

Economic accountability

Sponsorship still pays a real protocol fee from an existing fund. It does not make execution free for the network. Recovery does not reset a quota, and validly signed transactions that fail during business execution may still consume fees.

10 / SUPPLY ARCHITECTURE

One billion VAY, fully allocated

Fixed issuance under the current software, with distinct purposes and controls.

DESIGN & IMPLEMENTATION

Base staking reserve		300M / 30%
Conditional reserve		150M / 15%
Ecosystem		100M / 10%
Partnerships		20M / 2%
Development treasury		100M / 10%
Team		100M / 10%
Pre-seed		30M / 3%
Seed		50M / 5%
Presale		50M / 5%
Liquidity & market making		50M / 5%
DAO		30M / 3%
Strategic reserve		20M / 2%

Total: 1,000,000,000 VAY. One VAY equals 1,000,000,000 nvay. The reference supply policy uses existing tokens for disbursements and prohibits subsequent minting or reissuing burned units. A future hard fork can change software; these are not physically immutable promises.

Liquidity is represented by three module accounts, producing 14 fund accounts across the allocation structure. Other subfunds are accounting categories within parent funds, not additional issuance.

11 / DISTRIBUTION DESIGN

Sale rounds and external capital

Protocol token allocation and company proceeds are separate systems.

DESIGN & IMPLEMENTATION

Round	VAY	Working price	Full-sale gross
Pre-seed	30M	\$0.08	\$2.4M
Seed	50M	\$0.10	\$5.0M
Presale	50M	\$0.12	\$6.0M
Total	130M	Not market pricing	\$13.4M

These prices are working design assumptions. Full-sale arithmetic assumes every allocated token is sold at its stated round price, before expenses, refunds or other adjustments. It is not committed funding, validated demand or a public offer. The project owner has stated that external funding has not yet been secured.

Immediate allocation, restricted availability

A sale grant transfers the full allocated amount to the buyer's identity-linked stable account. Vesting locks restrict the spendable amount and prevent delegation of locked principal. A buyer can inspect the balance without receiving a transferable balance before the applicable release schedule.

Company proceeds

The intended policy assigns allocation of pre-seed, seed and presale cash or stablecoin proceeds to authorized company management, not token-holder voting. This does not relax VAY fund restrictions or turn company funds into the founder's personal funds. Final documents must define buyer rights and applicable obligations.

Before accepting payments

Select the legal entity, jurisdictions, accepted networks and token contracts, custody addresses, authorized signers, reconciliation and refund procedures. USDT/USDC collection, deposit verification and external custody are not yet implemented.

12 / UNLOCK DESIGN

Vesting that survives recovery

The schedule follows the identity-linked allocation, not the current device.

DESIGN & IMPLEMENTATION

Allocation	At T0	Cliff	Linear release after cliff
Pre-seed / Seed	0%	12 months	36 months
Presale	20%	None	36 months for remaining 80%
Founders / core team / advisors	0%	18 months	36 months
Future hires	0%	18 months	36 months; later start rule
Partners	0%	6 months	24 months; later acceptance rule

Release mechanics

T0 is a one-time, treasury-multisig scheduled launch reference intended to follow completion of sales and mainnet preparation with a planned exchange debut. The software does not establish that a CEX listing occurred, does not watch price and does not move T0 in response to markets. T0 remains unset on the current development fixture.

A model month is 2,628,000 seconds and a model year is 31,536,000 seconds. Linear release uses consensus time rather than a calendar-month approximation in an interface. There is no cliff-end catch-up lump sum for the linear portion.

Future-hire schedules start no earlier than the later of T0 and engagement start. Partner schedules start no earlier than the later of T0 and accepted delivery. Sales and most team allocations close at T0; later hires and partners have separately controlled paths.

Lock preservation

Sales unlock automatically without a claim. Team and partner claims require the current active controller. Rotation or recovery cannot restart the cliff, increase the grant or erase amounts already claimed. Unsold sale allocations remain locked.

13 / FUND ADMINISTRATION

Budgets are enforceable boundaries

An allocation is not permission to spend the full amount immediately.

DESIGN & IMPLEMENTATION

Control	Protocol behavior
Parent and category limits	A payment or grant must fit both its parent allocation and the relevant subfund.
Reserved commitments	Promised amounts consume availability so funds cannot be committed twice.
Annual budgets	Future years require explicit approval; unused allowance does not automatically roll forward.
Delayed disbursement	VAY payments use a seven-day timelock, purpose reference and expiry rules.
Execution	Anyone may execute an already authorized mature payment without changing amount or recipient.
DAO / strategic opening	Spending begins only after T0 plus 24 model months and an eligible budget-year boundary.

First-year parent ceilings include 18M ecosystem, 2M partnership commitments, 10M treasury and 18M staking subsidy. Market-maker and DEX ceilings are 5M each; the liquidity reserve ceiling is 10M. These are upper bounds, not automatic releases.

Conditional reserve: 150M VAY

Controlled reallocation requires governance authorization, a 30-day wait and a 15M annual limit, with a rule protecting 180M for future staking subsidies. The base staking reserve is 300M. Reallocation moves existing tokens within the approved design; it does not mint new supply.

Approved budgets and economic limits require careful review before launch. Current future-year budget rules do not simply expand when fees arrive or market-making loans are repaid.

14 / PRODUCTIVE ALLOCATION

Partnerships, ecosystem and liquidity

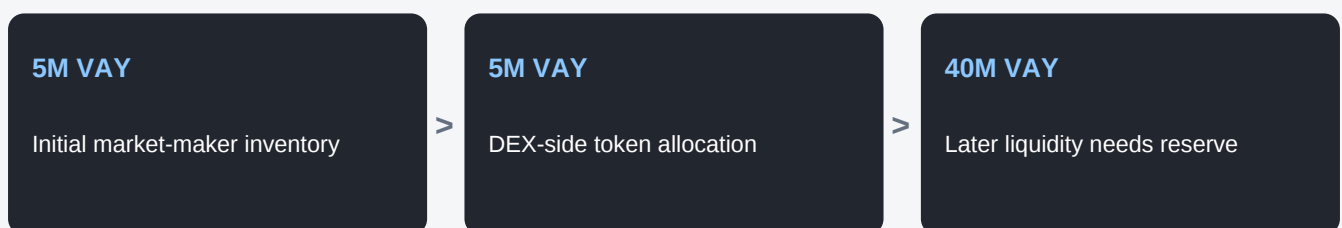
Funding growth must be distinguishable from buying market support.

DESIGN & IMPLEMENTATION

Ecosystem and institutional partnerships

The 100M ecosystem allocation includes applications, developer tools, validator bootstrap, community, education, security bounties and gas sponsorship. The separate 20M partnership allocation includes 10M business integrations, 5M wallet/custody, 3M institutional research and 2M distribution channels.

Partner grants reserve the obligation before activation. Acceptance requires the operational authority, at least seven days and a public reference to accepted delivery within the budget year. The chain records that reference; it does not judge the quality of an integration. Separate milestones should use separate grants.



Token inventory is not market depth

The 50M liquidity allocation does not supply the cash or stablecoins for buying orders, pay exchange charges or guarantee depth across many venues. Those require external capital, custody and agreements. The allocation also does not mean a DEX, bridge or exchange listing is implemented.

Market-maker transfers are modeled as loans with recorded repayments and a maturity of up to one year from first permitted execution. There is no automatic collateral liquidation, forced recovery or replenished spending allowance after repayment.

No price defense promise

Vesting and budgets can pace supply; they cannot prevent volatility, manipulation or losses. No minimum market price, anti-sniper guarantee or automatic price-support mechanism is delivered.

15 / DECISION RIGHTS

Governance with a limited mandate

Community authority where intended; operational execution where necessary.

DESIGN & IMPLEMENTATION

Decision	Authority
DAO annual budget and payments	Restricted on-chain governance
Staking-reserve budgets	Restricted on-chain governance
Conditional-reserve reallocation	Governance with protocol limits and delay
Development, ecosystem, team and partnerships	Treasury operational multisig within fund rules
Pre-seed, seed and presale grants	Sales operational multisig within lock rules
Liquidity budgets, payments and loan terms	Liquidity operational multisig
Customer KYC attestations	Authorized KYC issuer; no per-customer DAO vote
Use of external company sale proceeds	Authorized company management under final obligations

The governance message router is deny-by-default. It does not grant proposals unrestricted bank transfers, operational key replacement or arbitrary module parameter changes. Governance parameter updates have their own allowed path. Text proposals are non-binding.

Supply, fee split and the gross staking target remain software rules, not freely editable proposal parameters. Changing those rules requires a reviewed software upgrade and deployment process. Token ownership does not, by itself, confer equity or corporate control.

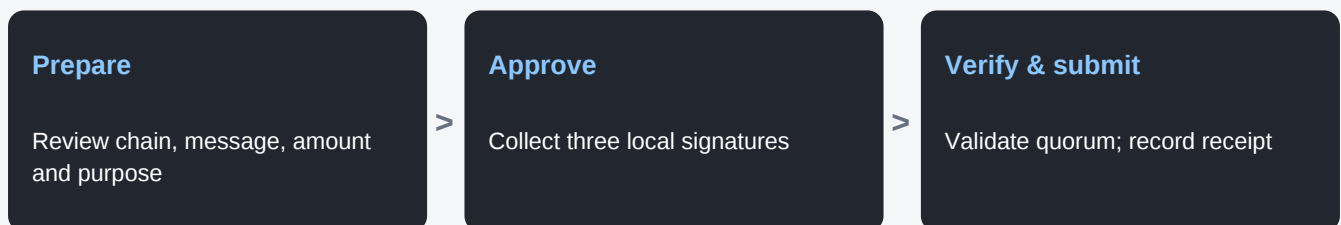
Ordinary delegated voting follows the SDK governance model. A dedicated voting path from stable accounts is not yet implemented and must not be presented as a completed wallet feature.

Custody is an operating model

Three signatures are meaningful only when control is genuinely separated.

LOCAL MULTISIGS ACTIVE / PRODUCTION CUSTODY PLANNED

Treasury, sales, liquidity and KYC use separate 3-of-5 test multisigs. For operational fund roles, configured public-key overlap is restricted so a single three-key quorum cannot control two roles. Independent people and devices must provide the real-world separation; software cannot prove custody independence.



Why development Keychain prompts occurred

The old and new locally built executables had distinct code-signing identities. Keychain permissions apply to individual items, including signer records, address indexes and multisig metadata. Access to one item did not authorize the others. Targeted owner-approved permissions resolved the blocked test path without enabling access for all applications.

Target production model

- Separate node binaries from a stable signing application and its release identity.
- Keep operational private keys off public RPC, explorer and validator servers.
- Evaluate hardware signing against actual Vayos message compatibility before claiming support.
- Distribute encrypted backups and signers; practice restoration and authorized rotation.

The backup passphrase decrypts exported backup files; it is not a multisig password. Possession of enough encrypted keys plus their passphrase can collapse the intended quorum separation.

17 / EXPLORER AND WALLET EXPERIENCE

A usable view of chain state

The existing portal provides visibility; transaction signing is the next product layer.

DESIGN & IMPLEMENTATION

Available locally	Planned extension
English explorer, latest blocks and block lookup	Public HTTPS deployment and scalable indexing
Transaction outcome, message types, gas and fees	Complete address-level transaction history
Identity, username and address lookup	Onboarding and controller-aware signing wallet
Locked, spendable and total stable balances	Send, stake, recover and review grant actions
Delegations, unbonding and rewards	Validator metadata and paginated user workflows
Isolated test faucet with quotas and receipts	Public abuse defenses and separated faucet signer

The portal is read-only except for its explicitly configured local faucet. It has no seed or private-key input. It uses bounded endpoints and rejects wrong-chain, catching-up or stale-node responses rather than reporting misleading zero balances. Query caps are disclosed in the interface.

Design language

This edition proposes a refreshed Vayos identity: graphite #111318, space grey #22262E, chrome-inspired silver #E6EAF0 and ice blue #8CC8FF. It retains the portal's VAYOS typographic wordmark. The explorer itself has not been recolored by this document update; a separate logo asset remains subject to confirmation.

Deployment boundary

The current portal runs on loopback. Public exposure requires a dedicated non-validator node, reverse proxy, TLS, firewall rules, external rate limiting, logging and load testing. Local controls alone are not DDoS protection.

An integration surface institutions can use

Protocol primitives become products only when operational interfaces are complete.

PLANNED / NO PRODUCTION SERVICE COMMITMENT

Proposed capability	Intended function	Delivery condition
Developer SDKs	Resolve identities and build supported transactions with clear errors.	Versioned APIs, examples, compatibility and security tests.
Institutional console	Review allocations, sign requests and track approvals by role.	Strong operator authentication and independently held signing keys.
Events and reconciliation	Connect chain receipts to internal ledgers and case IDs.	Idempotency, finality handling, replay and discrepancy procedures.
KYC case management	Manage verification, exceptions, expiry and credential issuance.	Private storage, reviewed models, audit logs and retention controls.
Recovery notifications	Alert users and operators during the challenge window.	Verified contact channels, delivery monitoring and abuse response.
Service operations	Versioned endpoints, maintenance notices and incident handling.	Measured capacity and formal operating responsibility.

Additional assets, stablecoin rails, confidential transaction products, IBC/bridge services and tokenized financial instruments are potential evaluation areas, not committed features in this release. Each requires its own threat model, interoperability testing and legal/product assessment.

19 / THREAT MODEL

Security starts with trust boundaries

Consensus correctness and safe institutional operation are related, but not interchangeable.

DESIGN & IMPLEMENTATION

Threat	Existing control	Remaining requirement
Stolen controller	Authorized rotation, delayed recovery and cancellation.	Alerts, session controls and user response procedures.
Compromised KYC issuer	Dedicated quorum, owner opt-in and timelock.	Independent custody, case review and issuer administration.
Fund misuse	Role restrictions, budgets, reservations and delayed execution.	Independent review, signer separation and audit.
Replay or stale recovery evidence	Proof reuse restrictions and credential revisions.	Fresh off-chain checks and evidence integrity.
Node or infrastructure failure	Backup/restart rehearsals and deterministic state checks.	Multi-host testing, monitoring and incident exercises.
Portal abuse	Bounded APIs, quotas and isolated faucet journal.	Public rate limiting, abuse detection and load testing.

A quorum of compromised signers remains a quorum. A valid attestation can still be false in the real world. Public metadata can be correlated. A software upgrade can introduce bugs. These risks cannot be eliminated by visual interfaces, fixed supply or a nominal multisig threshold.

Independent assurance required

Development tests are not an audit. Before production, commission protocol, wallet, custody and private-service reviews; remediate findings; test emergency procedures; and document who can authorize each response.

20 / PRIVACY AND OPERATING OBLIGATIONS

Data stewardship and institutional readiness

Design for minimum disclosure, explicit authority and verifiable responsibility.

REQUIREMENTS / NOT A COMPLIANCE CERTIFICATION

Private identity evidence

The proposed private KYC system must define collection purpose, retention, access, encryption, deletion and disclosure procedures before processing real people. Documents and biometric evidence should not be replicated to validators. Public transaction fields, including failed transactions, must never carry raw personal data.

Institution-specific obligations

Each deployment must assess the jurisdiction, legal role and product being offered. A credential label does not by itself satisfy a bank's onboarding policy or an issuer's obligations. Screening, ongoing monitoring, exception escalation and authorized disclosure may require additional workflows. This paper does not provide a legal determination.

Accountability by design

- Name the responsible legal entity and owners of private systems.
- Separate customer verification, approval, signing and audit responsibilities.
- Document access reviews, incident reporting and customer communications.
- Publish clear terms for recovery, locks, fees, service limits and dispute handling.

Public metadata is persistent

Removing a private evidence file does not erase an identity's historical public transactions or previously published commitments. Data minimization must be designed before submission, not added after launch.

21 / DELIVERY ROADMAP

A gated path to public operation

Progress should be accepted against evidence, not calendar promises.

PROPOSED DELIVERY SEQUENCE

Gate	Scope	Exit evidence
A / Baseline release	Reconcile documentation, rerun full tests, commit and tag the release.	Clean reproducible release, checksums and changelog.
B / Recovery completion	Finish the live 72-hour fixture after its real deadline.	New controller works; old key rejected; stable balance and vesting preserved.
C / Public testnet	Independent validators, public read node and persistent services.	Multi-host launch, restore drill, monitoring and external connectivity tests.
D / User products	Signing wallet, staking controls and recovery notifications.	Usability and security acceptance with explicit lock/fee displays.
E / Private KYC pilot	Verification service, evidence handling and issuer lifecycle controls.	Evaluated liveness, review workflows, privacy approval and adversarial tests.
F / Production decision	Custody, audits, legal sale terms, external capital operations and readiness review.	Findings closed and explicit launch authorization; no automatic mainnet promotion.

These gates may run partly in parallel, but dependencies cannot be waived by branding or a listing target. Mainnet genesis, production keys and external-asset custody require new decisions. Development tokens do not automatically convert into mainnet claims.

22 / DELIVERY INVENTORY

Capability status at a glance

A compact distinction between code, live evidence and planned product work.

DESIGN & IMPLEMENTATION

Capability	Status at 28 September 2026
L1 / VAY / original devnet	Running locally; single validator.
Identity and stable account	Implemented; identity and transfer paths exercised on devnet.
Tokenomics policy 7	Activated on original devnet; 1B supply and fund checks recorded.
Vesting and buyer grants	Implemented; locked buyer fixtures verified.
Stable-account staking	Implemented with signed integration tests; not every path live-rehearsed on persistent devnet.
Restricted governance / operator roles	Implemented; local multi-validator and multisig tests recorded.
KYC credential / dedicated issuer	Activated; synthetic credential issued with real multisig signatures.
KYC recovery	Start/cancel/early-rejection live checks passed; final 72-hour execution pending.
Explorer and local faucet	Implemented; funded local payout and persistence checks recorded.
Public testnet / independent custody	Not deployed in this reference environment.
AI liveness / private evidence service	Planned; no real-person verification delivered.
USDT/USDC collection / CEX / DEX	Not implemented or established by VAY allocations.
Signing wallet / institutional console	Planned; current portal is read-only.
Independent audit / production SLA	Not completed or offered.

What the development evidence proves

Real signatures and state checks, with bounded conclusions.

DESIGN & IMPLEMENTATION

Protocol and economic testing

Recorded development work includes Go tests, builds, static checks, manifest comparisons and signed application tests. Local four-validator rehearsals exercised governance and economic paths, rejection cases, restarts and common-height state agreement. They are not evidence of geographically independent network resilience.

Existing-network continuity

The original devnet received narrowly scoped, checkpoint-bound upgrades after cold-copy rehearsals. Reports record preserved historical state, validator identity, supply and fund checks, and restart without the one-time activation flag. These adapters are not a generic migration framework for arbitrary networks.

Current recovery fixture

Checkpoint	Live block / result
Identity and locked grant	18082 / 18083; successful
Synthetic KYC / owner opt-in	18365 / 18366; successful
Early execution	18374; rejected as expected
Owner cancellation / cancelled execution	18375 successful / 18376 rejected
Fresh pending recovery	18377; recovery-000002
Execution deadline	1 October 2026, 01:41:12 UTC

The fixture holds 100 locked test VAY plus 10 spendable nvay at its stable account. Final execution must verify new-controller authority, old-controller rejection and unchanged vesting. No automatic completion monitor was installed at the evidence cutoff.

Risks and explicit non-promises

Institutional credibility requires visible limits, not implied guarantees.

DESIGN & IMPLEMENTATION

Risk	Implication
Technology and upgrade risk	Code may contain defects; consensus or migrations may fail. Audit and staged rollout remain necessary.
Custody concentration	Several keys on one device do not provide independent quorum security.
Issuer trust	False or compromised attestations may enable unauthorized recovery for opted-in users.
Market and liquidity risk	Fixed supply, vesting and reserves do not ensure demand, liquidity or price stability.
Reward sustainability	The 6% gross target depends on stake, fees, budgets and reserves; it is not a contractual yield.
Privacy and correlation	Public identifiers, status and transaction links can reveal relationships even without documents.
External service dependency	Verification, alerts, custody hardware and public infrastructure need separate assurance.
Regulatory and contractual uncertainty	Permitted products, token rights and operating duties require jurisdiction-specific assessment.
Delivery risk	Planned features, integrations and venue access may change, be delayed or not launch.

No inference of endorsement

Audience descriptions do not indicate bank partnerships, regulator approval, exchange acceptance or third-party certification. Nothing in this paper establishes an entitlement to future tokens, services or returns.

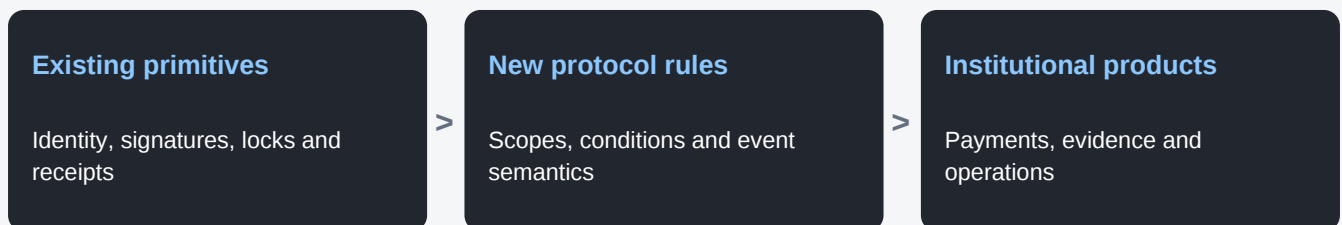
25 / CAPABILITY EXPANSION

From primitives to institutional products

A proposed portfolio, not an announcement of completed features.

PROPOSED EXTENSIONS / NOT IMPLEMENTED

Stable accounts, identity-linked state, bounded authority and delayed execution provide a foundation for additional products. The following six pages extend the product vision without changing the live chain, allocating new tokens or creating a delivery commitment. Each proposal requires a specification and an explicit development decision.



Extension family	Possible capabilities	Primary dependency
Account policies	Scoped session keys, organizational accounts and spending limits.	New authorization paths and recovery-safe revocation.
Business payments	Batch payouts, invoice references, mandates and conditional escrow.	New execution semantics and reconciliation tooling.
Credential services	Reusable attestations and narrowly disclosed eligibility proofs.	Credential schemas, privacy design and issuer lifecycle.
Asset workflows	Permission-aware assets and conditional asset exchange.	Asset modules, custody model and legal assessment.
Integration operations	Durable events, reconciliation exports and approval workspaces.	Indexer, authenticated services and signer separation.

Preserve the core contract: extensions must not bypass vesting, duplicate recovery rights or silently modify the 1B VAY policy. Every service must distinguish consensus-enforced rules from application controls.

26 / ACCOUNT POLICY EXTENSIONS

Programmable authority, bounded risk

Let organizations delegate specific tasks without handing over the account.

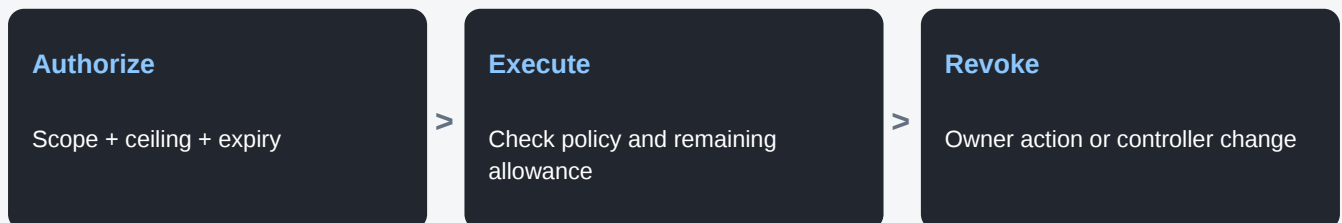
PROPOSED / CURRENT CONTROLLER MODEL REMAINS UNCHANGED

Scoped session keys

A future authorization module could let the current controller issue a short-lived key for selected message types, recipient sets and spend limits. A payment application could then perform a narrowly authorized action without receiving the master controller key. Limits should apply to cumulative use, not just individual transactions.

Organization accounts and approval policies

An institutional account could model preparers, reviewers and signers separately. Policies might require additional signatures above a threshold or for a new beneficiary. The existing operational 3-of-5 roles are not a general corporate account framework; organizational policies would require new account semantics and tests.



Safety requirement	Proposed acceptance criterion
Recovery interaction	All session permissions are revoked or explicitly revalidated after controller recovery.
Lock enforcement	Scoped authorization cannot spend or delegate vesting-locked principal.
Replay resistance	A signed mandate binds the chain, identity, purpose, nonce and expiry.
Operator clarity	Wallets show who can act, remaining limits and when authority ends.

No unrestricted account freeze or universal administrator key is proposed here. Any emergency policy must have a defined scope, activation authority, expiry and user-visible consequences. It must not be introduced implicitly through an interface.

Payments with business context

Make transactions easier to authorize, reconcile and explain.

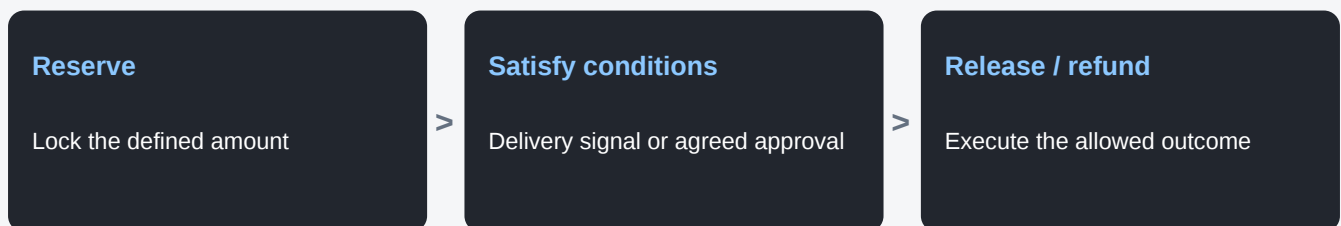
PROPOSED / NO PAYMENT SERVICE OR STABLECOIN RAIL DELIVERED

Batch payouts and invoice references

A bounded batch-payment message could support supplier payouts, grants or payroll-like distribution in VAY. The specification must choose atomic execution or clearly reported partial results, cap batch size and prevent duplicate submission. On-chain references should be opaque identifiers or commitments, never invoices containing personal information.

Recurring mandates, not automatic debits

A future mandate could authorize a recipient, maximum amount, interval and expiry. A keeper service would submit eligible transactions; validators would check the mandate. Blockchains do not wake up like a calendar application without an execution mechanism. Revocation, missed intervals and service failure must be explicit.



Conditional escrow

A new escrow module could hold a defined amount until both parties approve, a deadline passes or an agreed attestation arrives. Dispute resolution would require a separately chosen authority and process. The chain can enforce recorded conditions but cannot independently verify physical delivery or contract performance.

Deployment constraints

Start with existing transferable VAY and preserve vesting guards. Stablecoin payments require separately verified asset and custody rails. Refund semantics, fees, rounding, cancellation and recovery of each party must pass adversarial tests before public use.

28 / CREDENTIAL EXTENSIONS

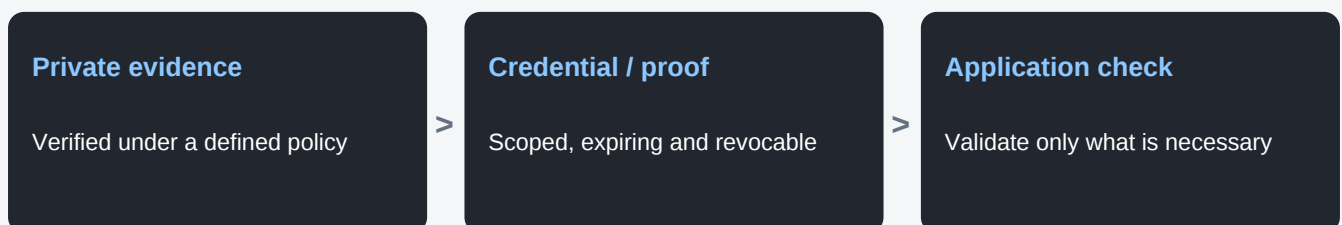
Reusable assurance with less disclosure

Verify the required claim without turning the chain into a document database.

PROPOSED / SELECTIVE DISCLOSURE AND ZK NOT IMPLEMENTED

The current KYC record is a status linked to one identity and an authorized issuer. A future credential framework could represent separate attestations such as business verification, authorized representative status or eligibility for a particular application. These would need explicit schemas, expiry and revocation behavior rather than overloading a single VERIFIED flag.

Proposed capability	Institutional use	Constraint
Business credentials	Associate an organization with reviewed representatives.	Legal authority must be checked off-chain and periodically refreshed.
Purpose-specific eligibility	Let an application check a defined claim.	A claim is not universal regulatory clearance.
Selective disclosure	Present only the attributes needed for an interaction.	Choose and audit a credential format and verifier implementation.
Zero-knowledge proofs	Explore proof of a predicate without exposing its inputs.	Research track; cryptography, revocation and metadata leakage require review.
Issuer registry lifecycle	Onboard, rotate, suspend and remove issuers safely.	Current runtime administration is incomplete; governance and recovery impact must be specified.



More privacy is not the same as anonymity. Reusing an identity, credential or public address can still link activity. A production design must evaluate correlation, user consent, verifier abuse, lost credentials and the consequences of issuer compromise.

Asset and settlement building blocks

Optional products built on explicit rights, not a claim that every asset belongs on-chain.

EXPLORATORY / NOT COMMITTED OR IMPLEMENTED

Permission-aware assets

An optional asset framework could define issuer authority, supply limits, transfer eligibility and redemption references for a particular product. Any transfer restrictions, freezes or forced actions would need to be explicit to holders and confined to that asset. They must not silently grant an issuer control over unrelated VAY accounts.

Conditional exchange

An atomic exchange message could swap two supported on-chain assets only when both legs satisfy their conditions. This is different from real-world delivery-versus-payment: external cash or asset delivery still needs trusted confirmation, custody and reconciliation. A protocol receipt alone cannot prove off-chain settlement.

Candidate workflow	Potential benefit	Unresolved dependency
Institution-issued claims	Inspectable ownership and lifecycle records.	Legally defined rights, servicing and redemption.
Business-to-business exchange	Conditional transfer of supported assets.	Asset standards, eligibility and failure handling.
External stablecoin connectivity	A possible payment unit distinct from volatile VAY.	Authentic contracts, custody or bridge model and risk review.
Cross-network messaging	Connect approved external systems or chains.	Light-client/bridge design, upgrade compatibility and incident response.

No implied financial product

These are architecture candidates, not issued securities, bank deposits, redeemable stablecoins or licensed settlement services. No partnership, reserve backing or bridge safety is implied. Each product needs its own authorization and delivery gate.

30 / PRIORITIZATION AND ACCEPTANCE

Build the operational layer first

Select extensions that strengthen the existing chain before expanding its trust surface.

PROPOSED PRIORITIES / NO CALENDAR COMMITMENT

Priority	Proposed work	Why it comes first
1 / Reliability	Durable event index, reconciliation exports, alerts and recovery status tracking.	Institutions need correct state and actionable incidents before new products.
2 / Usability	Controller-aware signing wallet, multisig workspace and hardware-signing evaluation.	Reduce signing mistakes and show authorization clearly.
3 / Control	Issuer lifecycle, scoped authority and organization account policies.	Make responsibility and revocation explicit.
4 / Business flows	Batch payouts, invoice commitments and narrowly defined escrow.	Extend existing assets without immediately adding external custody.
5 / Research	Selective disclosure, additional assets and cross-network settlement.	Introduce only after the new trust assumptions can be independently assessed.

Minimum acceptance for every extension

- A written specification states actors, permissions, public data, invariants and failure modes.
- Tests cover wrong keys, expiry, replay, duplicate execution, recovery interaction and vesting bypass attempts.
- Operations include audit trails, alerts, restore drills and a documented upgrade procedure.
- An independent review is required before exposing sensitive data or accepting real value.

This product expansion does not authorize code changes, alter live funds or broaden governance. It is a decision framework for selecting the next modules and services. Existing token economics remain unchanged.

Reference appendix

Project-grounded sources, version context and precise definitions.

DESIGN & IMPLEMENTATION

Prepared from the local Vayos repository and recorded development receipts on 28 September 2026. The last committed baseline observed was f1efc4a; this edition also describes uncommitted development changes. It is not a release attestation. Revalidate all status claims before external publication.

Project record	Primary subject
README.md; app.go; x/identity	Architecture, identity records and application wiring.
TOKENOMICS_V3.md; tokenomics/v3.json	Policy 7 allocations, budgets, fees and vesting.
TOKENOMICS_IMPLEMENTATION.md; GOVERNANCE.md	Enforcement boundaries and authority restrictions.
WALLET_VESTING.md; STABLE_STAKING.md	Stable-account locks and supported staking actions.
KYC_RECOVERY.md; KYC_ISSUER_ACTIVATION.md	Credential trust model and live issuer activation.
LIVE_KYC_RECOVERY_TEST.md	Synthetic live recovery evidence and pending deadline.
TOKENOMICS_TESTNET_RESULTS.md; DEVNET_MIGRATION.md	Local rehearsals, migration and restart evidence.
TESTNET.md; TESTNET_PORTAL.md; FAUCET_ACTIVATION.md	Deployment gates, portal boundaries and faucet evidence.

Controller: key-authorized account permitted to act for an identity. Stable account: persistent identity-linked balance address. Issuer: authorized attestation signer. T0: one-time launch reference for schedules. Cliff: delay before linear release begins. Multisig: an account requiring a configured signing quorum.

Version 0.2 introduces the proposed space-grey, chrome-silver and ice-blue palette while retaining the explorer wordmark. Pages 28-33 are new product proposals, not implementation evidence. Confirm the final logo, legal entity and release identifier before publication. No private keys, passwords or personal KYC evidence are included.