
SHIVAI TOKEN PLATFORM PHASED DELIVERY BIBLE

Private Placement | Compliance-First | Wallet-Custodiated | Incentive-Ready

1. STRATEGIC RESTRUCTURE

1.1 Immediate Objective (*Phase 1 Go-Live Start date 23rd Feb – Ready 25th March*)

Launch a controlled private placement platform enabling:

1. Introduction of ShivAI Token
2. Full KYC onboarding
3. Investor capital subscription
4. Custodial wallet allocation
5. Minting of tokens into platform-controlled wallets
6. Admin-controlled Token Drop engine

This is **not** a public marketplace at launch.

It is a controlled issuance + allocation system.

Marketplace extensibility remains architecturally intact but inactive.

2. PHASE 1 – CORE TOKEN ISSUANCE PLATFORM

2.1 Functional Scope Phase 1 includes:

A. Public Layer [Investor App]

- ShivAI Token Introduction Page
- Token economics explanation
- Legal disclaimers
- Invite-based access gating (via link and/or QR code)

B. Investor Layer [Investor App]

- Account creation
- Full KYC

- Investment commitment
- Fiat / USDT payment
- Wallet creation (custodial)
- Token minting
- Portfolio display

C. Admin Layer [Super Admin]

- KYC approvals
 - Investment approvals
 - Payment reconciliation
 - Mint control
 - Token Drop management
 - Full audit logging
-

3. TOKEN MODEL (PHASE 1)

3.1 Token Nature

- Digital token representing SPV economic exposure
- Minted on Polygon (ERC-3643 recommended)
- Permissioned
- Non-publicly tradable
- Transfer-restricted

3.2 Supply Structure

Configurable parameters:

- Total authorized supply
- Initial mintable supply
- Reserve allocation
- Marketing allocation
- Drop allocation pool

Admin dashboard must allow visibility of:

- Total supply
- Minted supply
- Allocated supply
- Remaining supply
- Dropped Minted Tokens (segmented from Investment Mints)
- Burned tokens (if ever activated)

4. INVESTOR FLOW (PHASE 1) [Investor App]

4.1 SCREEN 01 – ShivAI Token Introduction

Purpose:

- Establish legitimacy
- Explain what token represents
- Clarify non-trading nature
- Display minimum and maximum investment limits

Must include:

- Token supply
- Lock-in terms
- Jurisdiction disclaimer
- Risk statement

CTA:

“Request Access” or “Enter Invite Code”

4.2 SCREEN 02 – Invite & Access Validation

APIs:

POST /invite/validate

POST /invite/consume

Edge cases:

- Expired invite
- Reused invite
- Jurisdiction blocked

4.3 SCREEN 03 – Profile Creation

Required fields:

- Full legal name
- Nationality
- Country of residence
- Phone (validate via OTP)
- Email (validate via OTP)
- Wallet agreement acceptance

Backend validation:

- Sanctions list
 - Restricted geography
-

4.4 SCREEN 04 – KYC Flow

Integrated provider: Sumsub / equivalent

States:

- NOT_STARTED
- IN_PROGRESS
- AUTO_APPROVED
- MANUAL REVIEW
- APPROVED
- REJECTED

Rules:

- No investment intent allowed before APPROVED
 - Manual override requires reason + document upload
 - Every change logged
 - Token Drops are allowed only after KYC status = APPROVED.
-

4.5 SCREEN 05 – Investment Intent

Min: Configurable (e.g. \$500)

Max: Configurable (e.g. \$20,000)

API:

POST /investment/intent

System validates:

- Remaining allocation cap
- Investor tier limits
- Jurisdiction caps

Creates:

- Unique investment record
 - Pending payment state
-

4.6 SCREEN 06 – Payment Layer

Option A – Fiat

- Bank transfer
- Manual or API reconciliation
- Status: PENDING → CONFIRMED

Option B – USDT (TRC20)

- Unique TRON address per intent
 - Confirm ≥ 20 confirmations
 - Under/over payment handling
-

SECTION 4.7 – CUSTODIAL WALLET CREATION & ACTIVATION

4.7 Custodial Wallet Creation – Definitive Flow

4.7.1 Architectural Principle

Investors do NOT:

- Create wallets manually
- Manage private keys
- Sign blockchain transactions
- Activate wallets themselves

Wallet lifecycle is 100% platform-managed.

4.7.2 When Is the Wallet Created?

Wallet creation must occur automatically at:

Trigger:

KYC Status = APPROVED

The system generates a custodial blockchain wallet immediately upon KYC approval.

Reason:

- Ensures drop eligibility
 - Ensures investment readiness
 - Avoids mint delay
 - Keeps drop engine deterministic
-

4.7.3 Wallet Status Model

Wallet states:

1. NOT_CREATED
2. CREATED
3. ACTIVE
4. FROZEN
5. SUSPENDED

Lifecycle:

Event	Resulting State
KYC Approved	CREATED
Wallet registered on-chain + whitelisted	ACTIVE
Compliance issue	FROZEN
Sanctioned / flagged	SUSPENDED

Wallet becomes ACTIVE only after:

- Blockchain address generated
- Whitelisted in contract
- Stored securely in vault/HSM
- Linked to investor_id

This is automatic and backend-driven.

The investor never performs activation.

4.7.4 Technical Execution

Upon KYC APPROVED:

1. Generate wallet keypair
2. Encrypt private key using vault/HSM
3. Store public address in wallets table
4. Call smart contract whitelist(address)
5. Update wallet_status = ACTIVE
6. Log audit event

Table: wallets

- wallet_id
- investor_id
- public_address
- encrypted_private_key
- status
- created_at
- activated_at

4.8 SCREEN 08 – Token Minting

Trigger conditions:

- KYC = APPROVED
- Payment = CONFIRMED
- Compliance clearance passed
- For DROP mints, Payment confirmation is not required.

Execution:

- Whitelist wallet
- Call mint()
- Apply lock timestamp
- Record blockchain tx hash

Ledger entry created:

- investor_id
- wallet_id
- amount
- mint_tx
- lock_expiry

Token Classification Requirement

Every mint must be classified at creation time as:

- INVESTMENT (capital-backed mint)
- DROP (non-capital allocation mint)

This classification must be stored in the ledger record and cannot be modified post-creation.

Additional Ledger Field:

- mint_type (ENUM: INVESTMENT | DROP)

This ensures permanent differentiation between:

- Capital subscription tokens
- Incentive / marketing tokens

4.9 SCREEN 09 – Portfolio Dashboard

Displays:

- Total Token Balance
- Breakdown:
 - Investment Tokens
 - Drop / Incentive Tokens
 - Lock expiry
 - Allocation history with badge:
 - [INVESTMENT]
 - [DROP – Campaign Name]
 - Investment history
 - Token Market Suggested current reference value

Investment and Drop tokens must be visually distinguishable in history and summary.

Differentiation must not rely only on color. A textual badge/tag is mandatory.

5. ADMIN DASHBOARD – PHASE 1 (Master Admin)

5.1 Role Types

1. Compliance Admin
2. Finance Admin
3. Super Admin

Strict RBAC enforced.

5.2 Module A – KYC Control Panel

Features:

- View investor queue
- Approve / Reject
- Manual override
- Document upload
- Audit log view

Every override requires:

- Mandatory reason
 - Attachment
 - Immutable log entry
-

5.3 Module B – Investment & Payment Control

Displays:

- Pending payments
- Reconciliation mismatches
- Confirm / Reject

No minting allowed before payment confirmation.

5.4 Module C – Token Mint Control

Super Admin only.

Features:

- View mint queue
- Emergency pause minting
- Global mint freeze
- Manual mint (exception case)

Admin dashboard must display mint totals segmented by:

- Investment Mints
 - Drop Mints
 - Total Minted Supply
-

6. PHASE 1 ADDITIONAL FEATURE

TOKEN DROP ENGINE

This is a new mandatory component.

6.1 Purpose

Allow Admin to allocate tokens to approved wallets without capital contribution.

Use cases:

- Marketing campaigns
 - Referral rewards
 - Strategic barter
 - Incentive programs
 - Partner allocations
-

SECTION 6.2 – TOKEN DROP PRECONDITIONS

- Wallet status = ACTIVE (system-generated custodial wallet created automatically upon KYC approval)

A wallet is considered ACTIVE when:

- It has been system-generated
- Successfully whitelisted on-chain
- Not frozen or suspended
- Linked to an approved investor

Investors are not required to perform any wallet action to receive token drops.

DROP ELIGIBILITY LOGIC (DETERMINISTIC RULE SET)

Drop is permitted ONLY if:

IF

KYC_status = APPROVED
AND wallet_status = ACTIVE
AND investor_flag != TRUE
AND sanctions_status != TRUE

THEN allow_drop = TRUE
ELSE reject_drop

EDGE CASE HANDLING

Case 1 – Investor only wants drop, not investing

Flow:

1. Investor completes KYC
2. Wallet auto-created
3. Wallet auto-whitelisted
4. Admin can drop tokens

No capital required.

Case 2 – KYC Approved but Wallet Creation Fails

System must:

- Set wallet_status = ERROR
- Block minting

- Block drops
- Notify admin
- Log failure

Drop engine must validate wallet_status = ACTIVE only.

Case 3 – Investor Flagged After Drop

If investor_flag becomes TRUE:

- wallet_status → FROZEN
- Transfers disabled
- Further drops blocked

Already dropped tokens remain but are non-transferable.

IMPORTANT ARCHITECTURAL DECISION

Create wallet only after KYC approval

Recommended for compliance purity.

Wallet creation occurs automatically upon KYC approval.

This ensures:

- Compliance gating
 - Clean drop logic
 - No ambiguous activation state
 - Predictable backend behavior
-

6.3 Drop Types

1. Manual Individual Drop
 2. Bulk Drop (CSV upload)
 3. Campaign-Based Drop
-

6.4 Admin Flow – Manual Drop

Fields:

- Investor ID / Wallet
- Amount
- Reason category
- Notes
- Optional campaign tag

Process:

1. Validation
2. Supply check
3. Mint to wallet
4. Record drop ledger entry
5. Notify investor

6.5 Admin Flow – Bulk Drop

Upload CSV:

- investor_email
- token_amount
- campaign_code

System:

- Validates each
- Previews summary
- Requires Super Admin confirmation
- Executes sequential minting

Partial failure handling required.

6.6 Drop Ledger Table

New table:

token_drops

- drop_id
- investor_id
- wallet_id
- amount
- reason
- campaign_id
- created_by
- tx_hash
- timestamp

Must appear separately in portfolio UI.

Drop entries must always correspond to a mint record in token_mints where:
mint_type = DROP.

6.7 Supply Protection

Drop allocation reduces available supply.

System must enforce:

- Cannot exceed authorized supply
- Cannot exceed campaign allocation pool
- Cannot mint beyond reserve bucket

Supply buckets:

- Public allocation
- Marketing pool
- Strategic pool
- Admin reserve

These must be configurable.

System must track supply consumption separately for:

- Investment allocation pool
- Drop allocation pool

Super Admin override required to reassign between pools. Override must be logged.

7. SECURITY REQUIREMENTS

Phase 1 must include:

- HSM-based private key management
 - Role-based admin access
 - Full audit trail
 - Immutable logs
 - Emergency mint freeze
 - Multi-sig contract control recommended
 - Smart contract audit before mainnet
-

8. DATABASE ADDITIONS FOR PHASE 1

Core Tables:

investors

kyc_records

investment_intents

payments

wallets

token_mints

token_drops table must include field: mint_type (INVESTMENT | DROP)

audit_logs

supply_tracker

9. BLOCKCHAIN RULES (PHASE 1)

- Whitelisted wallets only
- Transfer disabled initially (recommended)
- 12-month lock-in
- Gas paid via relayer
- Emergency pause function enabled

No peer-to-peer transfer in Phase 1.

10. OUT OF SCOPE (FOR LATER PHASES)

- Secondary transfers

- Reference valuation engine publication
 - Marketplace with multiple issuers
 - Trading UI
 - Order book
 - Yield display
 - Price charts
-

11. DELIVERY STRUCTURE

Phase 1A

- Token intro page
- Invite gating
- Profile & KYC
- Wallet creation
- Investment intent
- Payment integration

Phase 1B

- Mint automation
- Portfolio dashboard
- Admin dashboard
- Audit logging

Phase 1C

- Token Drop engine
 - Bulk drop support
 - Supply bucket management
 - Notification system
-

12. GO-LIVE REQUIREMENTS

Must be completed before production:

- Smart contract audit
- Load test (10k concurrent users)
- KYC sandbox testing
- Payment reconciliation testing
- Drop simulation testing

- Mint freeze test
 - Disaster recovery drill
-

This structure gives engineering:

- Clear module separation
- Deterministic mint logic
- Strict compliance gating
- Controlled token distribution
- Scalable base for future marketplace expansion

If required, the next step can be:

- Technical architecture diagram
- Smart contract specification draft
- API contract definitions
- Sprint breakdown with epics and story mapping