PHPR

Whitepaper

PHPR (PHP Remit)

PHPR is a fiat-referenced remittance token priced at ₱1 for minting and redemption, backed 100% by Philippine pesos held in segregated escrow at VBank. It is not marketed as an investment or trading asset, pays no yield, and is solely intended for remittance use.

Version v1.2

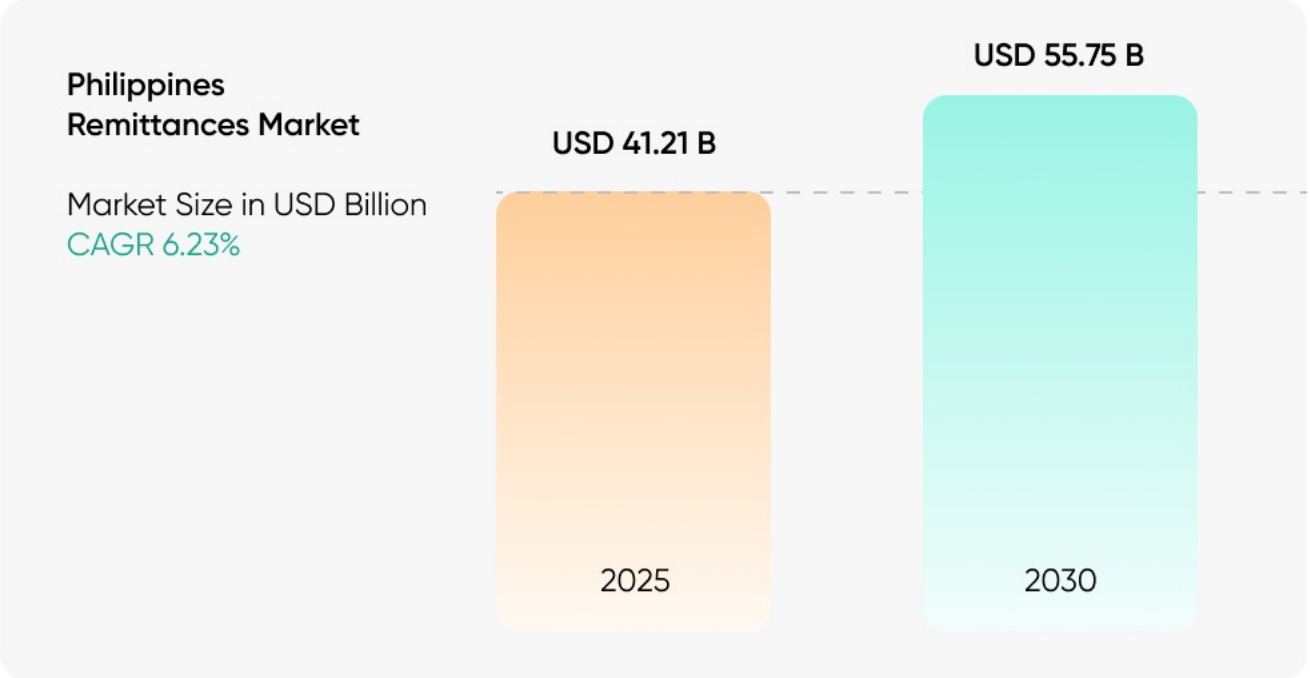
Abstract

The Philippines remittances market stands at USD 41.21 billion in 2025 and is projected to reach USD 55.75 billion by 2030, reflecting a forecast CAGR of 6.23%.

The growth projection is supported by the development of foreign exchanges driven by the peso's depreciation, the high demand for Filipino labor worldwide, and the growing use of digital wallets. A large global diaspora that exceeds 2.1 million overseas Filipino workers (OFWs) continues to remit steadily, making this particular market the world's fourth-largest corridor that supports 8.3% of national GDP. Yet families consistently lose substantial value to inefficient legacy infrastructure that charges multiple fees, offers poor transparency, and requires 1-5 business days for settlement.

Instant channel digitalization reduces transfer friction and draws in new users; in 2024, digital payments made up 52.8% of domestic retail transactions. Although there is still a significant geographic concentration in the US, Singapore, and Saudi Arabia, new labor agreements and infrastructural initiatives are allowing for the expansion of emerging corridors throughout the GCC and ASEAN.

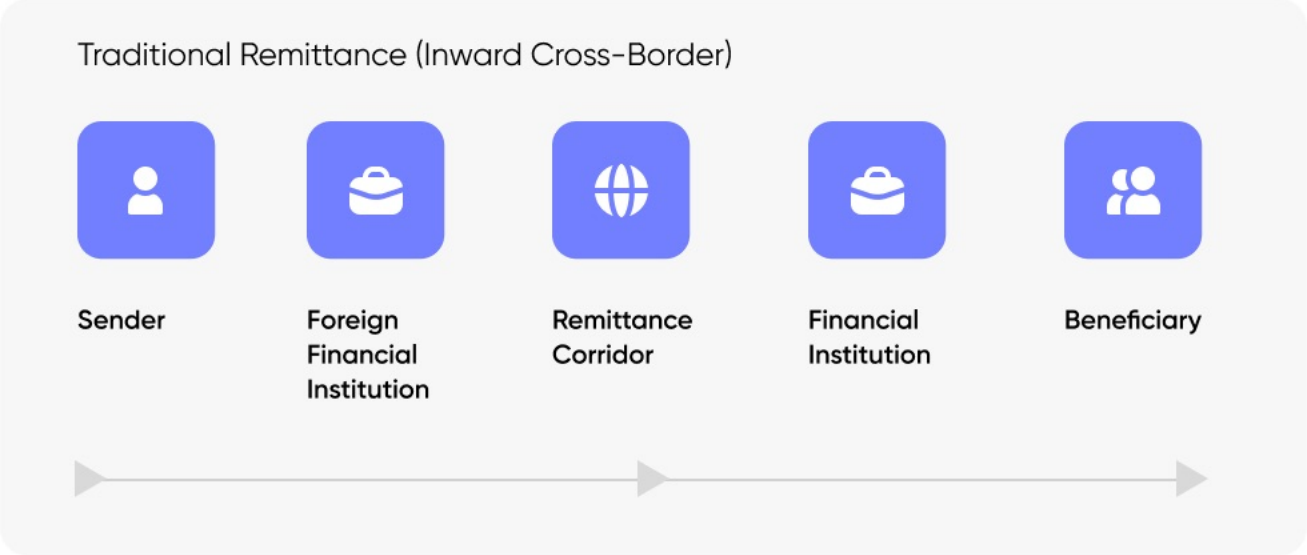
PHPR is a fiat-referenced remittance utility token priced at one Philippine peso (₱1 = 1 PHPR) issued by OpenPay on the Venom Blockchain to compress cross-border transfers for Filipinos into near-instant, low-cost, transparent flows. Each PHPR is controlled to equal one peso with 100% Philippine peso (PHP) reserves held in segregated escrow at VBank and designated partner financial institutions. PHPR is not an investment product, not a security, and does not pay any yield.



1. Introduction

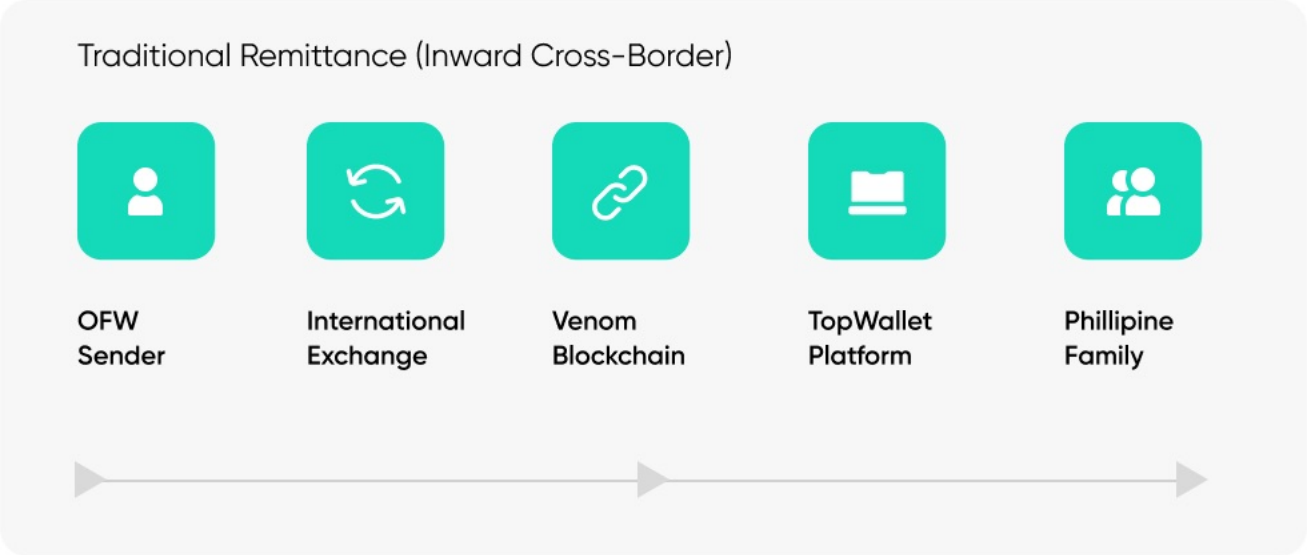
1.1 Problem

Traditional vs PHPR Remittance Flow



Inward remittances typically suffer from multi-day settlement, opaque fees (FX spreads + layered charges), fragmented rails, and compliance friction. Families bear the cost in delays and leakage.

1.2 Solution



Channel	Period	Cause of Delay
Bank Transfer	3-5 business days	Interbank settlement, compliance checks, and processing queues
Money Transfer Operator	1-2 business days	Cut-off time, and payout location availability
Digital Remittance Platform	1 business day	Reliant on local disbursement partners, and regulatory compliance
PHPR Token	<1 hour	Blockchain settlement in 0.2-0.3 seconds

PHPR provides an escrow-backed, on-chain representation of PHP that travels at network speed while preserving bank-grade compliance and face-value redemption. The token lives on Venom with an audited mint/burn smart contract linked to fiat escrow accounts.

Access Requirements: Users must sign up with both VBank and TopWallet to access PHPR. Both accounts are required to use the service, ensuring the lowest costs and fees through this controlled ecosystem.

2. Design Goals

- **Priced at one peso:** 1 PHPR priced as ₱1 at issuance/ redemption
- **Safety:** 100% cash reserves in segregated escrow (no lending, no rehypothecation).
- **Compliance first:** Full KYC/KYB, sanctions screening, monitoring, Travel Rule with partner VASPs.
- **Transparency:** Monthly Proof-of-Reserves (PoR), live supply telemetry, named reserve venues.
- **Low friction:** Zero protocol fee on transfers; simple, published program terms.
- **Governance with guardrails:** DAO-set parameters within compliance-enforced bands; operator multisig for execution & emergencies.

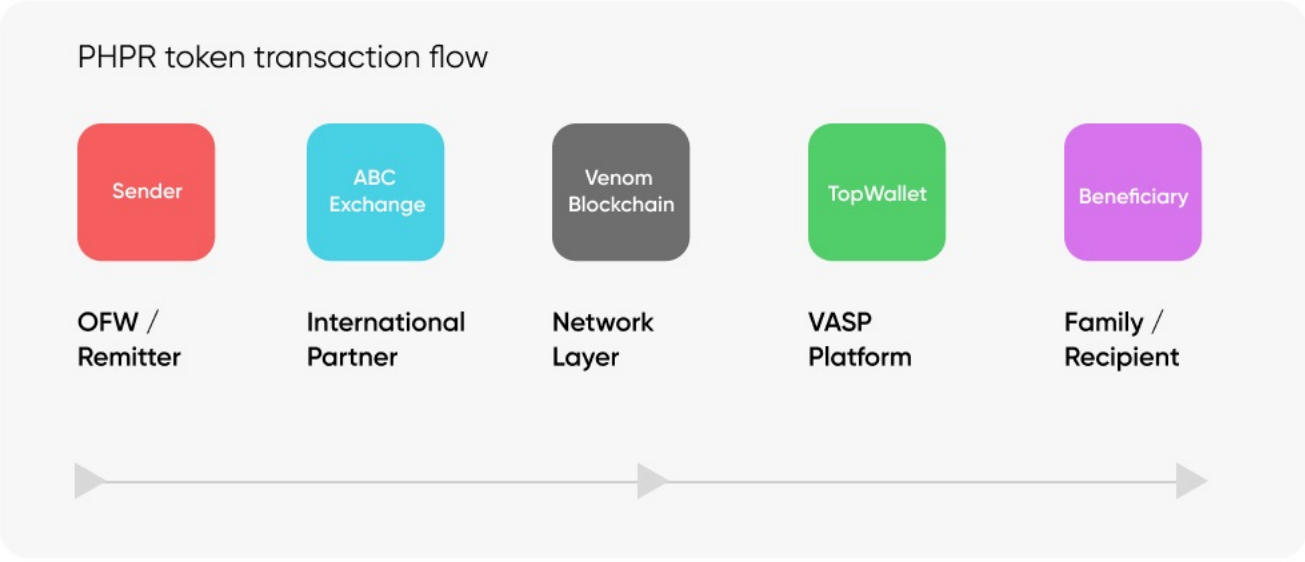
3. System Overview

3.1 Roles & Parties

- **Issuer:** OpenPay
- **Escrow Banks:** VBank (primary custody and user accounts).
- **Network:** Venom Blockchain (smart-contract settlement).
- **Exchanges / VASPs:** TopWallet (primary platform); additional regulated venues to be announced.
- **Partner Examples:** 1Satoshi (Hong Kong) for regional expansion; NSTPay, Sphere, Ripple-based rails (under evaluation).

3.2 High-Level Flow

1. **Mint:** PHP arrives into VBank escrow → oracle-free verification of fiat receipt → authorized mint to user/partner wallet.
2. **Transfer:** Users move PHPR on Venom (P2P, P2B) through TopWallet with 0% protocol fee (network gas only).
3. **Redeem (Burn):** User submits PHPR for redemption → burn on-chain → PHP paid out at peso pricing via VBank.



Sender Purchases PHPR
OFW deposits foreign currency with authorized international exchange partner and requests PHPR tokens

Currency Conversion
Exchange converts foreign currency to PHP at transparent rates and prepares escrow deposit

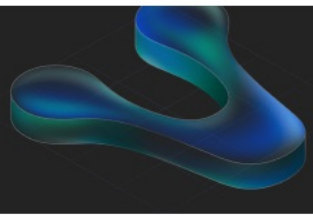
Escrow Deposit
PHP equivalent deposited into segregated escrow account at VBank

Token Minting
TopWallet verifies escrow deposit and mints equivalent PHPR tokens on Venom blockchain

KYC & Compliance
Travel Rule compliance, KYC verification, and AML screening completed for transfer

Token Delivery
PHPR tokens transferred to beneficiary's wallet with options to hold or redeem for PHP

Venom blockchain
0.2–0.3 second finality • 100K+ TPS capacity • $0.0002 transaction cost



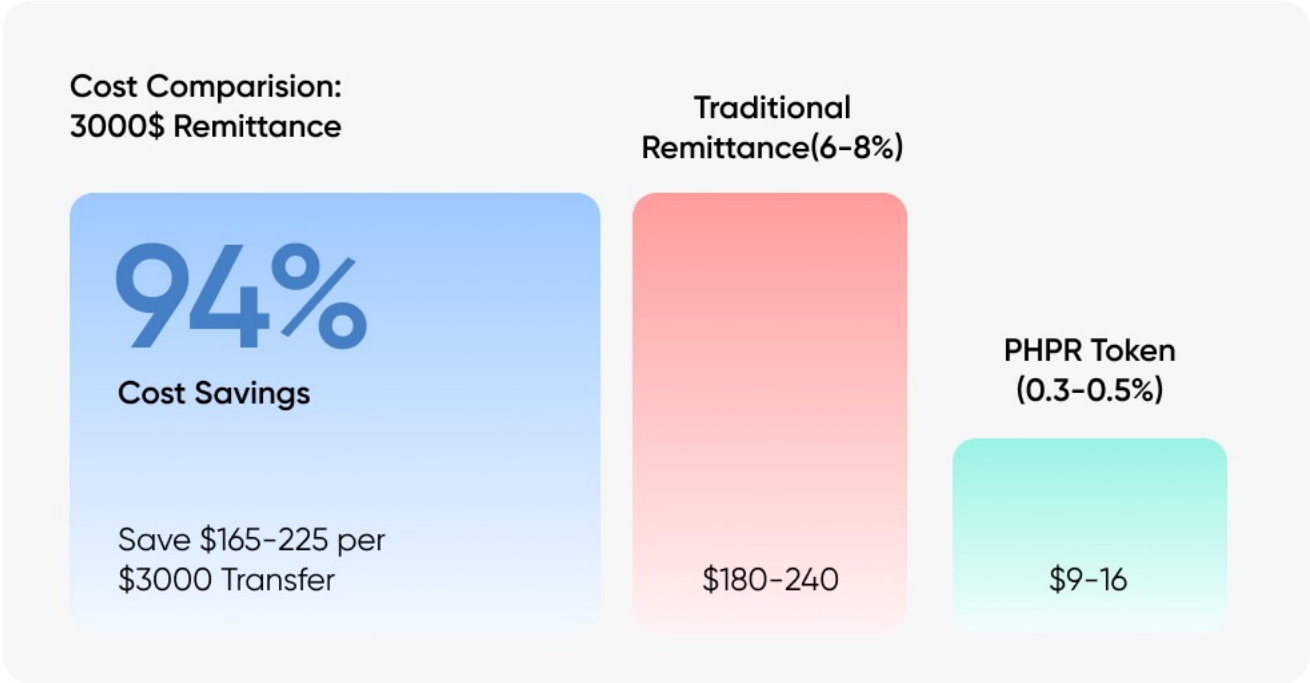
Process Details:

A six-step process facilitates compliance and security with speed:

- Steps 1-2: OFW initiates purchase through TopWallet
- Step 3: PHP conversion and escrow deposit at VBank for reserve backing
- Step 4: Smart contract verification and token minting on Venom
- Steps 5-6: Compliance verification and token delivery to beneficiary

This flow eliminates traditional correspondent banking delays while preserving regulatory compliance. By keeping users within the VBank-TopWallet ecosystem, we ensure the lowest costs and minimal fees at official exchange rates.

4. Token Specification



4.1 Network & Standard

- **Chain:** Venom Blockchain
- **Contract:** PHPR smart-contract (addresses published prior to GA)
- **Decimals:** 6 (industry standard)
- **MPC/HSM scheme:** HSM-backed MPC key custody. Signing policy: 2-of-3 Operator key shares + 1 Compliance signer (i.e., execution requires signatures from at least two Operator HSM keys AND the Compliance key). All private key material is stored in FIPS-level HSMs (or equivalent MPC vault). Critical actions (contract upgrade, parameter change, emergency unpause) require 3-of-3 Operator signatures OR 2-of-3 Operator + Compliance signer per documented SOP. Key custody provider to be named on the transparency page and in security annex.

4.2 Peg & Pricing

- **Pricing:** 1 PHPR priced as ₱1 for minting and redemption.
- **Oracles:** Not used for determining redemption value. External rates may be used for dashboards/quotes, never for solvency or peso pricing redemptions.

4.3 Fees & Limits

Token Economics & Fee Structure

Transparent pricing and sustainable economic model

Fee Structure

Transfers
0%
Protocol fee (network gas only)

Issuance (Mint)
0.30% - 0.50%
DAO-governed within compliance band

Redemption
0%
Protocol fee (partner rails may charge pass-through fees)

Network Gas
~$0.0002
Venom blockchain transaction cost

Reserve Backing

1:1

PHP Reserve Ratio

- 100% cash reserves in segregated escrow
- No lending or rehypothecation
- Monthly proof-of-reserves
- VBank custody with partner institutions
- Interest income ring-fenced to liquidity buffers

- **Transfers:** 0% protocol fee (minimal network gas applies).
- **Issuance (Mint):** 0.30%–0.50% of minted notional (DAO-governed within band).
- **Redemption:** 0% protocol fee; partner rails (bank/e-money) may charge pass-through fees, published transparently.
- **Limits:** Risk-based per-transaction, daily, and program caps for mint and redeem; configurable by DAO within compliance maxima.

Operation	Example	Fee
Minting	₱10,000 → 10,000 PHPR	0.35% issuance fee = ₱35
Transfer	10,000 PHPR P2P	0% protocol fee, only gas (<₱0.01)
Redemption	10,000 PHPR → ₱10,000	0% protocol fee; pass-through rails may apply

Compare vs Legacy Remittance

Typical remittance costs ~5–6% in fees with 1–3 day delays; PHPR compresses this to near-instant, low-cost flows.

4.4 Supply Policy

- **Elastic & fully reserved:** On-demand mint against escrowed PHP at VBank; burn on redeem.
- **No seigniorage / no yield:** Any interest that may accrue on reserve accounts is ring-fenced to liquidity buffers; it is not corporate income.
- **Controlled supply:** Each token is controlled to equal one peso through VBank escrow management.

Next
5. Smart-Contract Architecture

5. Smart-Contract Architecture

5.1 Roles (on-chain)

- **IssuerRole:** executes `mint` upon fiat escrow confirmation.
- **TreasuryRole:** initiates programmatic `burn` on redemption.
- **ComplianceRole:** can `pause`, `unpause`, and blacklist sanctioned addresses under published policy.
- **Governor (DAO):** sets parameters (fees within a 30–50 bps band, program limits, disclosure cadence).
- **Operator Multisig:** MPC/HSM custody; 4-eyes approvals on sensitive actions.

Technical Details

- **Mainnet Contract Address:** 0:3c8e5fbd...7e21 (to be published before GA)
- **ABI / Bytecode Hash:** `[PHPR_ABI.json]/TokenRoot.abi.json [BYTECODE_HASH_PLACEHOLDER]`

Upgrade Policy:

IMMUTABLE

Deployed TokenRoot contract is immutable — no administrative/upgrade keys are retained. Any future protocol modification requires deployment of a new contract and an on-chain migration procedure coordinated with VBank and TopWallet. Migration workflows and finality guarantees will be published on the transparency page.

MPC/HSM Scheme:

MPC/HSM scheme: HSM-backed MPC key custody. Signing policy: 2-of-3 Operator key shares + 1 Compliance signer (i.e., execution requires signatures from at least two Operator HSM keys AND the Compliance key). All private key material is stored in FIPS-level HSMs (or equivalent MPC vault). Critical actions (contract upgrade, parameter change, emergency unpause) require 3-of-3 Operator signatures OR 2-of-3 Operator + Compliance signer per documented SOP. Key custody provider to be named on the transparency page and in security annex.

Next
5.2 Ecosystem Architecture & Token Flow

5.2 Ecosystem Architecture & Token Flow

The PHPR ecosystem operates through interconnected components that ensure secure token issuance, transfer, and redemption while maintaining full reserve backing at VBank. The system is designed to minimize cost and risk for customers by working through one primary exchange (TopWallet) and one escrow bank (VBank).

Core Components:

- **Token Treasury:** Central smart contract module that manages PHPR supply, handling both minting operations when PHP deposits are confirmed and burning operations when redemption requests are processed.
  [CONTRACT_ADDRESS_PLACEHOLDER]

- **Venom Blockchain:** The network layer that facilitates all token operations, providing 0.2-0.3 second finality and enabling seamless transfers between wallets and platforms.
- **International Exchange:** External partners that receive foreign currency deposits from OFWs and initiate the conversion process to PHP for escrow deposit.
- **Nominated Settlement Bank Account:** Intermediate account held by international exchange partners for PHP conversion and preparation for escrow transfer.
- **VBank Trust Bank (Escrow Account):** Segregated escrow accounts that hold 100% PHP reserves backing all issued PHPR tokens, with each token controlled to equal one peso.
- **OpenPay:** Issuance authority and system operator responsible for smart contract governance, compliance oversight, partner integrations, and maintaining the overall PHPR ecosystem integrity.

Key Functions & Flow:

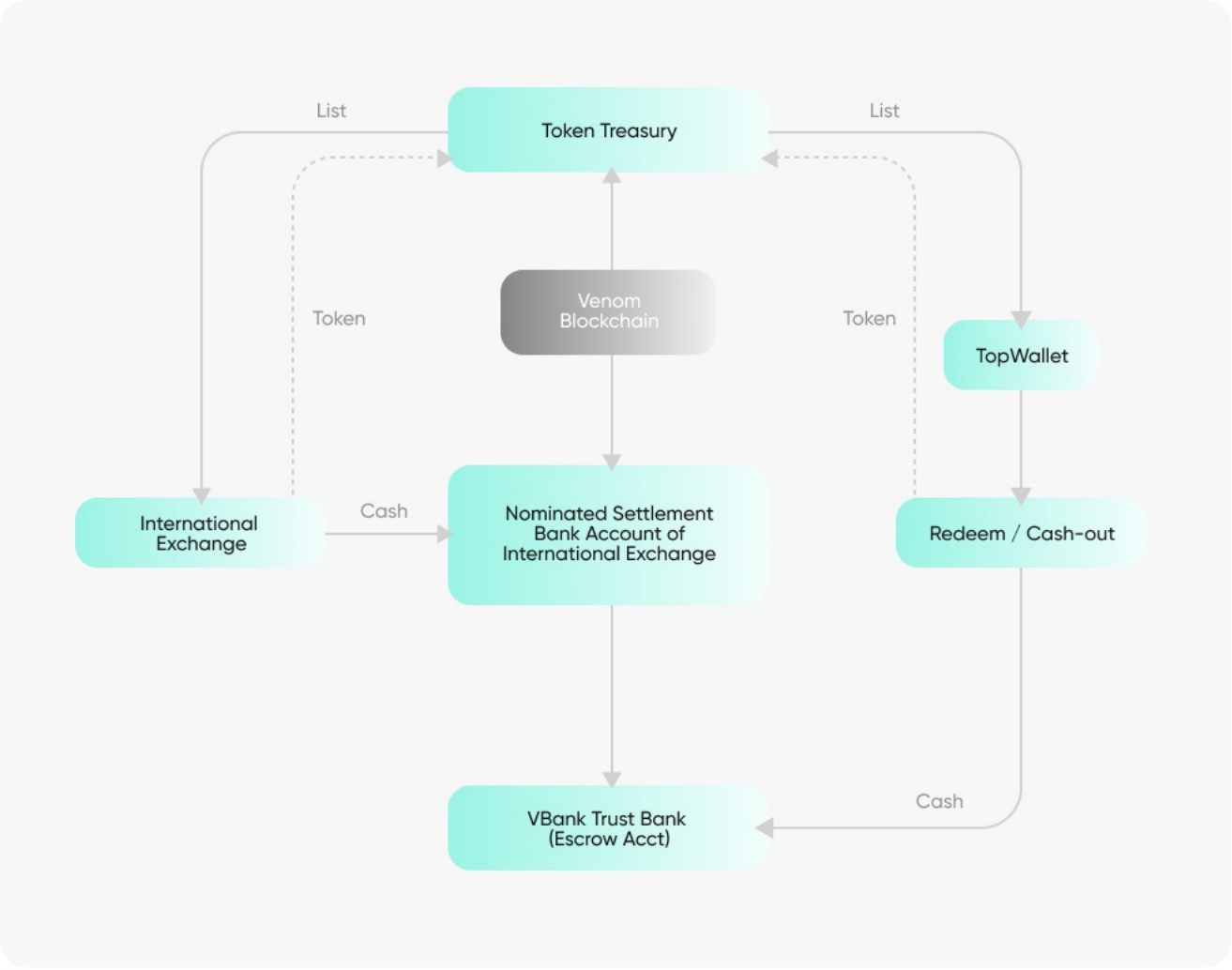
```
mint(address to, uint256 amount)          // IssuerRole only, after escrow credit
burn(uint256 amount)                      // user burn prior to redemption
pause() / unpause()                       // ComplianceRole (emergency only)
setFee(uint16 bps)                        // DAO-governed, 30–50 bps
setLimits(Limits cfg)                     // per-tx, daily, program caps
blacklist(address a, bool isBlacklisted)// sanctions/AML events
```

Next
Operational Flow:

Operational Flow:

1. **Listing Phase:** Topwallet maintains updated PHPR availability and pricing at official rates
2. **Token Creation:** PHP deposits at VBank trigger automated minting through the token treasury
3. **Network Transfer:** PHPR moves across the Venom blockchain between TopWallet users
4. **Redemption Process:** Token burning releases equivalent PHP from the VBank escrow
5. **Cash Settlement:** Funds flow from the VBank escrow to the beneficiary via VBank cash withdrawal

Reserve Integrity: The architecture ensures that every PHPR token in circulation corresponds to exactly ₱1 held in segregated escrow at VBank. This structure minimizes cost and risk for customers by maintaining a controlled, single-exchange ecosystem.



5.3 Security

- MPC/HSM for operational keys; threshold signatures; hardware-backed secrets.

MPC/HSM scheme: HSM-backed MPC key custody. Signing policy: 2-of-3 Operator key shares + 1 Compliance signer (i.e., execution requires signatures from at least two Operator HSM keys AND the Compliance key). All private key material is stored in FIPS-level HSMs (or equivalent MPC vault). Critical actions (contract upgrade, parameter change, emergency unpause) require 3-of-3 Operator signatures OR 2-of-3 Operator + Compliance signer per documented SOP. Key custody provider to be named on the transparency page and in security annex.

- **Audit & Verification:** Pre-GA, formal checks on mint/burn/role controls using [CONTRACT_ADDRESS_PLACEHOLDER] and [BYTECODE_HASH_PLACEHOLDER].
- Bounty: Coordinated vulnerability disclosure and bounty program.
- Change control: Versioned deployments; immutable references pinned from the program site.

Upgrade Control:

IMMUTABLE

Deployed TokenRoot contract is immutable — no administrative/upgrade keys are retained. Any future protocol modification requires deployment of a new contract and an on-chain migration procedure coordinated with VBank and TopWallet. Migration workflows and finality guarantees will be published on the transparency page.

6. Reserves, Redemption & Transparency

6.1 Reserve Structure

- 100% PHP cash, segregated escrow at VBank.
- No lending/no hypothecation/no derivatives.
- **VBank custody:** All escrow operations managed through VBank for maximum security and transparency.

6.2 Redemption Policy (Priced at Peso Value)

- **Eligibility:** KYC/KYB verified users with both VBank and TopWallet accounts.
- **Method:** Submit PHPR → on-chain burn → fiat payout priced as peso via VBank withdrawal.
- **Cash withdrawals:** Users must go through VBank for all cash withdrawal operations.
- **Cut-offs & SLAs:** Redemptions submitted before 3:00 pm PHT are settled on the same business day (T+0). Submissions after cutoff are processed the next business day (T+1). Disputes are resolved within 3–5 business days. In case of corridor outages, contingency settlement paths are activated.

Consumer complaint / escalation path :

1. **Stage 1 — Merchant/Wallet support:** Customer opens ticket via TopWallet support (response SLA: initial acknowledgement within 24 hours, resolution target T+3 business days).
2. **Stage 2 — OpenPay Operations/Compliance:** Unresolved tickets escalate to OpenPay Compliance (response within 48 hours).
3. **Stage 3 — VBank (escrow / settlement issues):** For settlement/payout disputes, escalate to VBank case owner (response per SLA in Appendix C).
4. **Regulator escalation (BSP):** If unresolved after internal escalation, customers may file with BSP Consumer Assistance (BSP CAMS / BOB). BSP contacts: consumeraffairs@bsp.gov.ph; BSP Consumer Protection & Market Conduct Office phone: (02) 5306-2584 (alternative BSP contacts listed on BSP site). bsp.gov.ph+1

Users must maintain both VBank and TopWallet accounts to access PHPR services.

6.3 Proof-of-Reserves (PoR)

Proof-of-Reserves is attested monthly by [Named Auditor], with attestations published by the 7th business day of each month. Scope includes escrow account confirmation (with partial redaction), reconciliation with on-chain supply, and optional Merkle liability proofs. All attestations will be available via the Transparency page.

Proof-of-Reserves (PoR) — operational statement

- **Attestor:** [Independent Auditor — e.g., KPMG Philippines / PwC Philippines / RSM Philippines] (final auditor to be named; attestation contract executed prior to GA).
- **Cadence & publication:** Monthly attestations published no later than the 7th business day following each month-end; attestation package includes: PDF attestation, machine-readable JSON, and (optionally) per-customer Merkle proofs.

Scope of attestation:

1. **Escrow confirmations:** bank confirmations for all segregated PHPR escrow accounts at VBank and partner banks. Account numbers are partially redacted (show last 4 digits) in public materials; full account statements are available to the named auditor and regulators on request.
2. **On-chain supply snapshot:** on-chain token supply (Venom) snapshot included with exact block height and UTC timestamp used for reconciliation.
3. **Reconciliation methodology:** auditor reconciles bank ledger balances (statement balances as of statement date) to on-chain supply, listing reconciling items (pending inbound/outbound items) and providing an attestor opinion that reserves ≥ circulating supply on the statement date.
4. **Merkle liabilities (optional):** if enabled, a Merkle tree of outstanding PHPR balances is generated and its root is published alongside the attestation; customers may verify inclusion via provided proofs.

- **Publication & anchoring:** Attestation PDF + JSON + Merkle root will be published on | transparency page and an immutable reference (URL hash / small on-chain anchor) will be recorded on Venom for auditability.

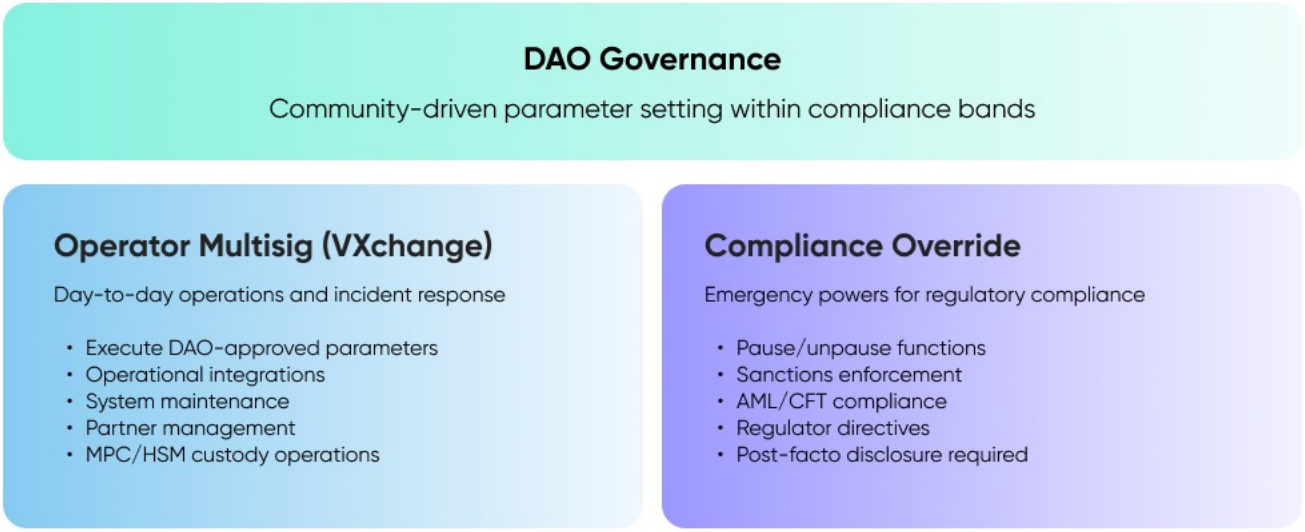
- **Example attestation header (to appear at top of PDF/JSON):**
  - Statement date: 2025-09-30
  - Attestor: [NAME]
  - Escrow venues: VBank (Escrow: XXXX-1234), [PartnerBank-2: XXXX-5678]
  - On-chain supply (Venom snapshot): 10,000,000 PHPR (block: #1234567, UTC: 2025-10-01T00:00:00Z)
  - Merkle root (if used): 0x...

Next
7. Governance

7. Governance

PHPR Governance Structure

Decentralized decision-making with compliance guardrails



- **No public governance token:** PHPR program does not issue a public governance token. DAO processes control program parameters only; there is no transferable token that confers financial rights or profit expectation.
- **OpenPay / DAO governance power & quorum:** Operational governance is provided by a stewarding DAO (parameter-setting & oversight). Quorum: changes require 3 of 5 (3/5) authorized governance members to approve DAO-set parameter changes (fees within the published band, corridor activation, non-emergency limits).
- **Operator accountability:** Operational responsibilities (execution of mint/burn, incident response, reserve custody coordination) rest with OpenPay (Operator multisig) and VBank (escrow). Regulators may hold OpenPay accountable for operator actions.
- **Emergency scopes (operator/compliance only):** Only OpenPay (Operator multisig) and the named Compliance Officer may immediately perform pause, blacklist, and mint-halt actions to address AML/CFT incidents, sanctions directives, or material security incidents. Emergency actions are narrow, documented, and limited to immediate mitigation.
- **Timelocks & change control:** All non-emergency parameter changes (fees, program caps, economic parameters) are subject to a 72-hour on-chain timelock from proposal to execution. Emergency compliance actions may be executed immediately but require:

1. Public disclosure of the action and rationale within 24 hours;
2. Retrospective DAO review and formal ratification within 7 calendar days.

- **Transparency & records:** All governance proposals, votes, timelock expiries, and emergency actions will be logged in a public governance changelog on \ transparency page for audit and regulator review.

7.1 Model

- **DAO-led parameterization:** Fee band (0.30%–0.50%), corridor activation, program caps, disclosure cadence (≥ monthly).
- **Operator Multisig (OpenPay):** Executes operations, incident response, and integrations.
- **Compliance Override:** Narrowly scoped emergency powers (pause/blacklist/mint-halt) to satisfy AML/CFT, sanctions, regulator directives; post-facto public disclosure required.
- **No public governance token:** DAO parameters are set without tokenized voting; control is limited to program parameters only.
- **Governance Power & Quorum:** X of Y members required to approve DAO-set changes.
- **Emergency scopes:** Only OpenPay/Compliance can pause, blacklist addresses, or halt mint operations.
- **Timelocks:** All parameter changes are subject to timelocks (48–72h) except compliance emergency actions.

7.2 Voting & Quorum (summary)

Proposal
Community submits parameter change within compliance bands

Review
Legal and compliance validation of proposed changes

Voting
DAO members vote with established quorum requirements

Timelock
48–72 hour delay before implementation (except emergencies)

Execution
Operator multisig implements approved changes

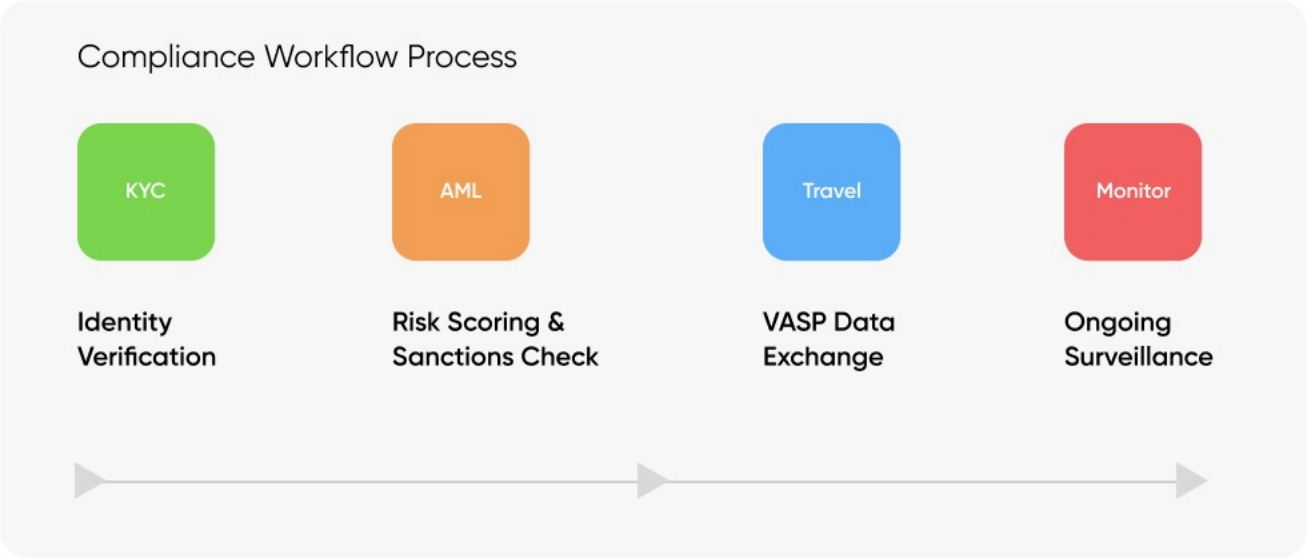
Emergency Powers & Constraints

Scope of Emergency Actions
Limited to: pause/blacklist functions, mint halts, sanctions compliance, and regulator directives. Cannot modify core economic parameters.

Transparency Requirements
All emergency actions require immediate public notification and post-facto community disclosure with justification and remediation timeline.

- **Quorum:** N% of circulating governance power (published in DAO docs).
- **Timelocks:** Changes to economic parameters are timelocked (e.g., 48-72h) except for urgent compliance actions.

8. Compliance & Risk



- Licensing posture per corridor.
- Outsourcing agreements (TopWallet distribution, VBank escrow).
- MLRO/DPO (names/roles).
- AML/CTF program summary.
- Travel Rule vendor (e.g., Notabene/Chainalysis).
- SAR/CTR procedure summary.
- Retention policy.
- Geofencing rules.
- Consumer complaint/escalation path (including BSP CA contact)

Corridor / Country	Local Partner	Licensing Type	License Number / Status
Philippines	VBank	BSP-licensed EMI / BSP supervision	[VBank_BSP_EMI_ID] (to be mentioned after licence approval)
United States	OpenPay USA (MSB)	FinCEN MSB / State MSB (where applicable)	MSB_REG_[STATE_OR_FINCEN] (registered through FinCEN MSB)
Hong Kong	1Satoshi (partner)	Licensed VASP / MSB (TBC)	[HK_LICENSE_ID] (application submit process)

Outsourcing Agreements (Summary)

- **VBank (escrow)** — Escrow Agreement: OpenPay <> VBank (Escrow Agreement dated [YYYY-MM-DD], Agreement ID: [VBank_EA_ID]). Escrow holds 100% PHP reserves; OpenPay and VBank legally designate PHPR holders as beneficial claimants in insolvency language (published in Annex).
- **TopWallet (distribution / customer onboarding)** — Distribution & Service Agreement: OpenPay <> TopWallet (Agreement ID: [TW_AGR_ID]) — TopWallet performs customer KYC/KYB, distribution UI, and integration; reserves remain in OpenPay/VBank control.

MLRO / DPO :

- **MLRO (Money Laundering Reporting Officer):** Head of Compliance — contact: mlro@openpay.ph, primary AML oversight & STR filing owner.
- **DPO (Data Protection Officer):** {Full Name}, DPO — contact: dpo@openpay.ph, responsible for DPA compliance and DPIAs.

AML / CTF program:

- Risk-based customer due diligence (CDD) and enhanced due diligence (EDD) for high-risk customers/corridors.
- KYC/KYB performed by TopWallet/VBank per BSP/AMLC standards; proof of identity + address + purpose of remittance required.
- Sanctions/PEP screening (UN/OFAC/EU/PH lists) at onboarding and continuously on activity.
- Transaction monitoring (KYT): automated scoring, velocity checks, geolocation anomalies, and merchant risk profiling. Alerts escalate to MLRO for manual review.
- Travel Rule tooling integrated (see Travel Rule vendor below) to exchange originator/beneficiary data with counterparties for transfers above applicable thresholds.

Travel Rule vendor:

- Primary vendor (planned) - Notabene — Travel Rule messaging, VASP directory and interoperability for secure exchange of originator/beneficiary data. (Chainalysis integration recommended for counterparty wallet identification/KYT). notabene.id+1

SAR / CTR procedure :

- **Covered Transaction Reports (CTR)**: transactions meeting the definition of covered transaction are reported per AMLA/AMLC guidance (CTR threshold as per AMLC / BSP guidance; e.g., transactions ≥ PHP 500,000 within one banking day are considered covered transactions and subject to reporting). Sumsub+1
- **Suspicious Activity Reports (SAR/STR):** STRs/SARs submitted to AMLC per statutory timeline; covered institutions must file STRs/CTRs in accordance with AMLC/BSP rules (reporting window: within 5 working days from detection/occurrence for covered transactions / as required by AMLC). amlc.gov.ph+1
- MLRO owns STR submission; SAR workflow and escalation documented in Annex.

Retention policy (records & personal data):

- **KYC / customer identification records:** retain 5 years after end of business relationship (AMLA / AMLC guidance).
- **Transaction records & supporting docs:** retain 5 years from date of transaction (unless local law requires longer — exceptions handled by DPO).
- Personal data handling follows the Philippines Data Privacy Act (DPA 2012); DPO contact and DPIA results available on request. amlc.gov.ph+1

Geofencing & access rules:

- Service access restricted to eligible jurisdictions listed in the Eligibility map; access denied for jurisdictions where VA/e-money is prohibited or where OpenPay/VBank lack regulatory clearance. Geofencing enforced at onboarding (KYC country) and at runtime (IP/location checks + KYT).
- Eligibility list published and versioned on /docs/corridors.

Consumer complaint / escalation path :

1. **Stage 1 — Merchant/Wallet support:** Customer opens ticket via TopWallet support (response SLA: initial acknowledgement within 24 hours, resolution target T+3 business days).
2. **Stage 2 — OpenPay Operations/Compliance:** Unresolved tickets escalate to OpenPay Compliance (response within 48 hours).
3. **Stage 3 — VBank (escrow / settlement issues):** For settlement/payout disputes, escalate to VBank case owner (response per SLA in Appendix C).
4. **Regulator escalation (BSP):** If unresolved after internal escalation, customers may file with BSP Consumer Assistance (BSP CAMS / BOB). BSP contacts: consumeraffairs@bsp.gov.ph; BSP Consumer Protection & Market Conduct Office phone: (02) 5306-2584 (alternative BSP contacts listed on BSP site). bsp.gov.ph+1

8.1 Controls

- **KYC/KYB:** Identity verification, PEP screening, sanctions lists (UN, OFAC, EU, AU, PH).
- **Monitoring:** Transaction risk scoring, velocity checks, anomaly detection.
- **Travel Rule:** Messaging with partner VASPs/exchanges where applicable.
- **Geofencing:** Access restricted to permitted jurisdictions; eligibility list versioned and published.
- **Recordkeeping:** Retention per statutory requirements.

Multi-Layered Security Architecture

Regulatory Compliance Layer

Foundational regulatory compliance ensuring legal operation within all jurisdictions

- BSP Licensing
- KYC/KYB AML/CFT
- Sanctions Screening
- Travel Rule

Smart Contract Security Layer

Technical safeguards protecting token operations and user funds

- Third-party Audits
- Formal Verification
- Bug Bounty
- Role-based Access
- Pause Functions

Operational Security Layer

Day-to-day operational controls and monitoring systems

- MPC/HSM Custody
- Multisig Requirements
- Incident Response
- Transaction Monitoring
- Anomaly Detection

Reserve Protection Layer

Safeguards ensuring 100% reserve backing and fund segregation

- Segregated Escrow
- Monthly PoR
- No Lending Policy
- Bank Partners
- Real-time Reconciliation

Next
8.2 Risk Factors (non-exhaustive)

8.2 Risk Factors (non-exhaustive)

PHPR Risk Mitigation Framework

Comprehensive multi-layered security and compliance controls

Regulatory Risk

VA/E-money Rule Changes
Mitigation: BSP-licensed infrastructure, proactive regulator engagement

Cross-border Requirements
Mitigation: Travel Rule compliance, international regulatory monitoring

Securities Classification
Mitigation: Legal opinion validation, utility-first design

Operational Risk

Smart Contract Bugs
Mitigation: Third-party audits, formal verification, bug bounty program

Escrow Bank Outages
Mitigation: Multiple partner institutions, contingency procedures

Key Compromise
Mitigation: MPC/HSM custody, multisig requirements, role separation

Technical Risk

Network Congestion
Mitigation: Venom's scalable architecture, dynamic fee adjustment

Infrastructure Attack
Mitigation: Distributed architecture, monitoring systems, incident response

Data Breaches
Mitigation: Encryption at rest/transit, zero-trust architecture, access controls

Market Risk

Low Adoption
Mitigation: Gradual corridor opening, partnership strategy, user education

Liquidity Constraints
Mitigation: Market-maker agreements, transparent limits, reserve buffers

FX Volatility
Mitigation: Real-time conversion, minimal exposure windows

- **Regulatory risk:** Changes in VA/e-money rules could impact issuance or redemption.
- **Bank/partner risk:** VBank or payout partners may experience outages or restrictions.
- **Operational risk:** Smart-contract or operational error; mitigated via audits, multisig, and pause controls.
- **Cybersecurity risk:** Key compromise or infrastructure attack; mitigated via MPC/HSM, segregation, and monitoring.
- **Liquidity risk:** Temporary corridor or exchange illiquidity; mitigated via VBank-TopWallet partnership and transparent limits.
- **Market/usage risk:** Adoption may be lower than anticipated; corridors may open gradually.
- **Force majeure:** Sovereign, network, or systemic events.

9. Business Model

9.1 Revenues

- **Issuance fee:** 0.30%–0.50% on minted notional.
- **White-label (WL):** Token-as-a-service for licensed fintechs/e-wallets under OpenPay reserve/compliance umbrella (rev-share per corridor/integration).
- Available only to licensed counterparties with regulatory approvals.
- Reserves remain under OpenPay/VBank control.
- Counterparties undergo full due diligence and onboarding checks before access.
- **Remittance corridors:** Programmatic fees per corridor, where applicable.

9.2 What We Do Not Do

- No float or yield from reserves.
- No proprietary trading with reserve funds.
- No unbacked issuance.
- No investment product features.
- No trading or floating of tokens.

10. Partners & Distribution

PHPR Partner Ecosystem Map

Strategic partnerships driving global remittance innovation

Blockchain Infrastructure

Venom Foundation CONFIRMED

Custody & Escrow

VBank (Primary) CONFIRMED

Partner Banks IN PROGRESS

Wallets & Platforms

TOPWallet CONFIRMED

Compatible Wallets IN PROGRESS

Exchanges & VASPs

TOPWallet CONFIRMED

International Partners IN PROGRESS

Custody & Escrow

NSTPay EVALUTION

Sphere EVALUTION

Ripple-based Rails EVALUTION

Next
10.1 Confirmed

10.1 Confirmed

- Venom (network)
- VBank (escrow)
- TopWallet (consumer wallet)

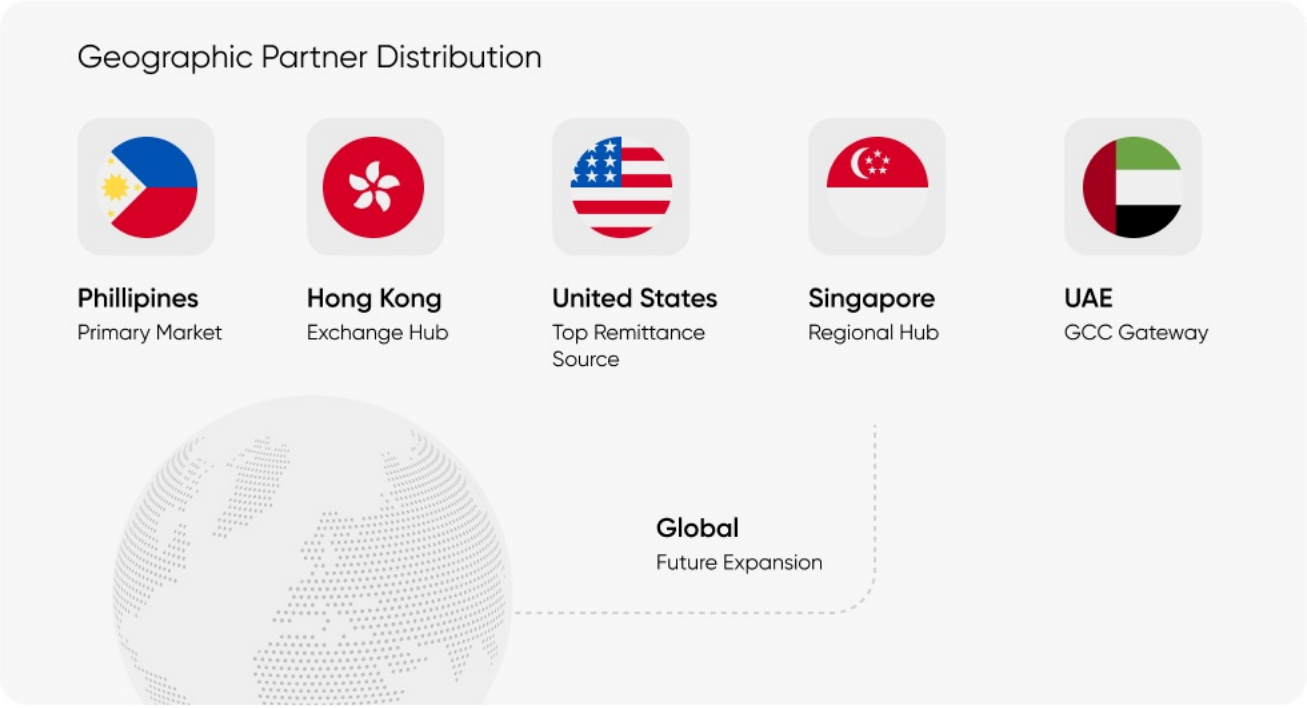
10.2 In Progress (Evaluation/BD)

- NSTPay, Sphere, Ripple-based rails for specific corridors.

10.3 Exchanges / VASPs

- **Primary access:** The TopWallet platform ensures the lowest costs and fees through a controlled ecosystem.
- **Regional partners:** 1Satoshi (Hong Kong) for Hong Kong market expansion, subject to standard due diligence and regional compliance.
- **International access:** Distribution via licensed/regulated VASPs for remittance purposes only (at par, non-speculative); priority target 1Satoshi (Hong Kong) subject to standard due diligence and regional compliance.

No market-making, trading, or price speculation allowed on any venue.



Ecosystem Benefits: By keeping users within the VBank-TopWallet ecosystem, PHPR ensures faster, cheaper, and simpler remittances with minimal fees at official exchange rates. This structure minimizes cost and risk for customers compared to multi-exchange alternatives.

11. Operations

11.1 Incident Response

- **Triggers:** Sanctions hit, anomaly, partner outage, contract bug.
- **Actions:** Rate-limit → pause (if needed) → public incident note → root-cause analysis → post-mortem with remediation plan.

11.2 Service Levels (summary)

- **Mint/Redeem windows:** Business days; published cut-offs per venue.
- **Support:** Tiered support for WL partners; consumer support via VBank and TopWallet verified channels.

12. Privacy & Data Protection

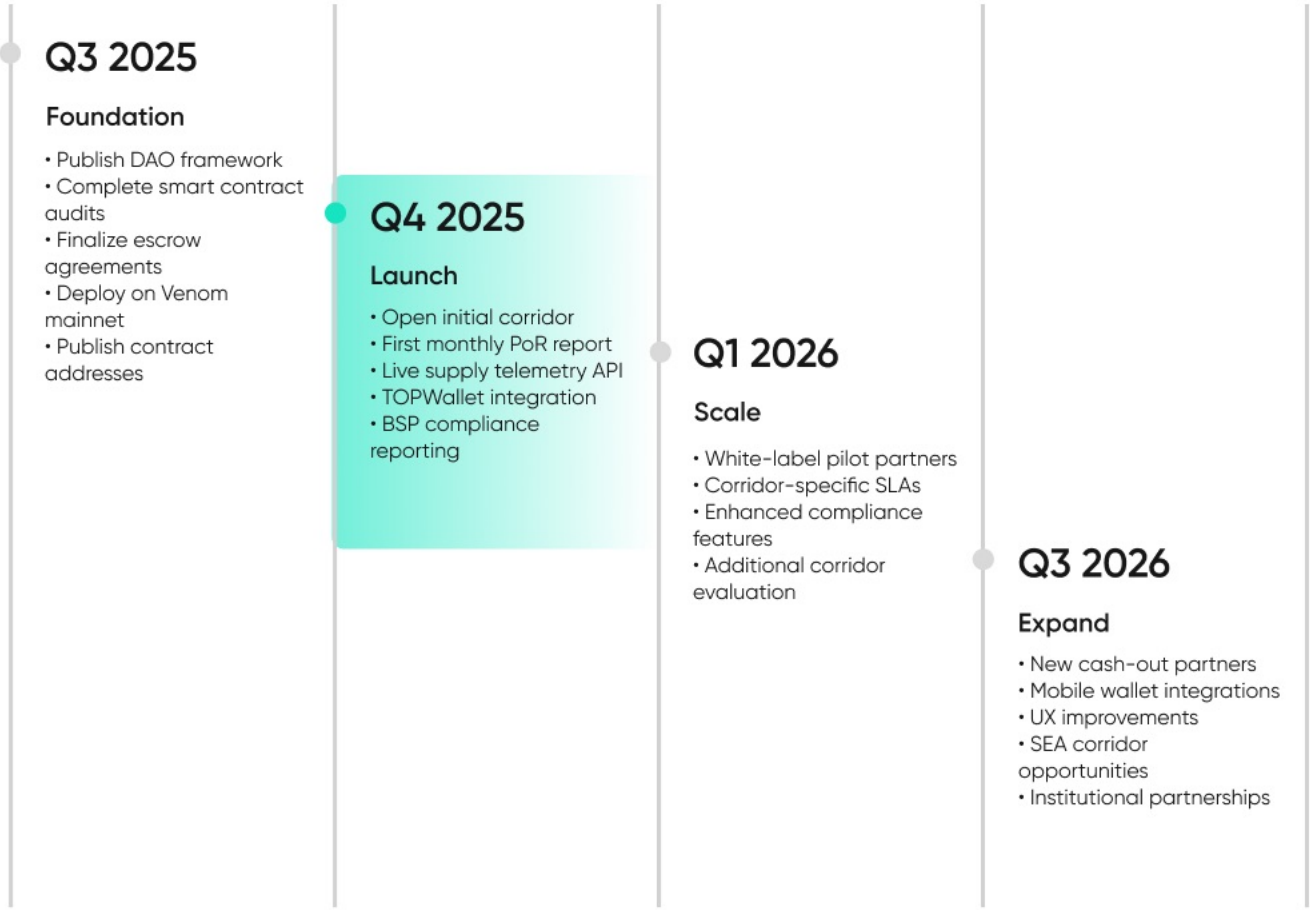
- **Data minimization:** Collect only what is necessary for compliance and service delivery.
- **Storage & security:** Encryption at rest and in transit; role-based access; audit trails.
- **Sharing:** With regulators and partner financial institutions, where required by law and program operation.
- **User rights:** Access, correction, and deletion requests per applicable law.

Next
13. Roadmap

13. Roadmap

PHPR Development Roadmap

Strategic milestones for launching the future of Filipino remittances



- Publish DAO framework (mandate, quorum, timelocks, emergency powers).
- Finalize audits; publish contract addresses; launch on Venom mainnet.
- Open initial corridor(s) with VBank-TopWallet integration.
- First monthly PoR; open telemetry API (supply/reserve snapshots).
- Onboard WL pilots; expand exchange listings.
- Add corridor-specific SLAs and cash-out partners.

Next
Glossary (select)

14. Glossary (select)

- **Escrow:** Segregated bank accounts at VBank holding PHP 1:1 against outstanding PHPR.
- **Mint/Burn:** On-chain increase/decrease of PHPR supply tied to VBank fiat flows.
- **Pricing:** Redemption of PHPR priced as one peso (1 PHPR priced as ₱1).
- **DAO:** Decentralized governance setting program parameters within compliance guardrails.
- **Travel Rule:** VASP-to-VASP originator/beneficiary data exchange requirement.

15. Disclaimers

CRITICAL DISCLAIMERS:

- PHPR is a fiat-referenced remittance token priced at ₱1 for minting and redemption, backed 100% by Philippine pesos held in segregated escrow at VBank. It is not marketed as an investment or trading asset, pays no yield, and is solely intended for remittance use.
- Account requirements: Users must maintain both VBank and TopWallet accounts to access PHPR services.

- **Jurisdictional limits:** Access, mint, and redeem are subject to KYC/KYB, eligibility, and local laws.
- **Program changes:** Limits, fees (within DAO-set bands), venues, and SLAs may evolve; the latest Terms of Use & Redemption Policy govern.
- **Risk acknowledgement:** Users and partners must review the Risk Factors (§8.2).

Next
16. Legal & Compliance Annex

16. Legal & Compliance Annex

16.1 Licensing & Regulatory Basis

- **Philippines:** PHPR is issued and distributed under the regulatory framework of the Bangko Sentral ng Pilipinas (BSP), pursuant to:

1. Circular No. 649 – Electronic Money Issuers (EMI).
2. Circular No. 1108 – Virtual Asset Service Providers (VASPs).

- PHPR issuance and redemption are conducted through BSP-licensed entities (TopWallet, VBank, and designated partners).
- **United States:** Cross-border corridors are supported under FinCEN Money Services Business (MSB) Registration, enabling issuance/redemption activities for remittance purposes in compliance with the U.S. Bank Secrecy Act. State licensing requirements are observed where applicable.
- **International Corridors:** Access and redemption are subject to host jurisdiction rules (e.g., MAS in Singapore, HKMA in Hong Kong, FCA in the UK, DFSA in UAE). PHPR will only be listed or distributed through licensed VASPs or e-money institutions in each jurisdiction.

16.2 Escrow & Reserve Protection

- All PHPR tokens are backed 1:1 with PHP held in segregated escrow accounts at VBank (BSP-supervised) and designated partner banks.
- Escrow agreements legally designate PHPR holders as beneficiaries with priority claims over reserves in the event of insolvency of the issuer or custodian.
- Reserves are never pledged, lent, or commingled with corporate funds.

Users must maintain both VBank and TopWallet accounts to access PHPR services.

16.3 Redemption Rights & Consumer Protection

- Redemption is a legal right for all KYC/KYB-verified users in eligible jurisdictions, priced as one peso (1 PHPR priced as ₱1).
- Redemption SLAs, fees, and payout rails (bank, e-wallet, OTC partners) are published and subject to regulatory oversight.
- **Dispute Resolution:** Errors, failed transactions, or complaints are handled under BSP's Consumer Protection Standards and through partner VASPs' customer support frameworks.
- Users may escalate unresolved complaints directly to BSP Consumer Assistance, or relevant regulators in their jurisdiction.

16.4 Data Privacy & Security

- PHPR adheres to the Philippines Data Privacy Act of 2012, including data minimization, access rights, and mandatory breach notifications.
- For EU/UK corridors, GDPR/UK DPA compliance applies, with user rights to access, correct, and erase personal data.
- Data is encrypted in transit and at rest; access is role-based and fully logged.

16.5 Non-Security Classification

- PHPR is structured to avoid classification as a security:
  - Fully redeemable priced as one peso (1 PHPR priced as ₱1).
  - No expectation of profit or yield.
  - No reliance on entrepreneurial/managerial efforts for appreciation.
- This aligns with Howey Test exemption under U.S. law and with BSP's treatment of e-money and payment tokens.

16.6 Jurisdictional Limits

- Access to PHPR may be restricted or prohibited in certain jurisdictions where virtual assets are banned or unregulated.
- OpenPay, VBank, and partners will geofence such jurisdictions and enforce eligibility restrictions.

16.7 Legal Disclaimers (Expanded)

- PHPR is not an investment product.
- Redemption and settlement are subject to regulatory approval, corridor availability, and partner bank/e-money operations.
- Changes in law or regulation may impact issuance, redemption, or corridor operations.
- Users accept all risks described in Section 8.2 (Risk Factors).

Appendix A - Contract Events (indicative)

- `Minted(address to, uint256 amount, bytes32 fiatRef)`
- `Burned(address from, uint256 amount, bytes32 fiatRef)`
- `Paused(address by) / Unpaused(address by)`
- `FeeUpdated(uint16 bps, address by)`
- `LimitsUpdated(Limits cfg, address by)`
- `Blacklisted(address a, bool state, address by)`

Appendix B - Reserve Attestation (template)

- Statement date & reporting period
- VBank escrow confirmations
- PHP balances by institution & account type
- On-chain supply snapshot & reconciliation method
- Attestor identity and procedures
- Merkle root (if customer-verifiable flow is provided)

Proof-of-Reserves (PoR) — operational statement

- Attestor: [Independent Auditor — e.g., KPMG Philippines / PwC Philippines / RSM Philippines] (final auditor to be named; attestation contract executed prior to GA).
- Cadence & publication: Monthly attestations published no later than the 7th business day following each month-end; attestation package includes: PDF attestation, machine-readable JSON, and (optionally) per-customer Merkle proofs.
- Scope of attestation:

1. Escrow confirmations: bank confirmations for all segregated PHPR escrow accounts at VBank and partner banks. Account numbers are partially redacted (show last 4 digits) in public materials; full account statements are available to the named auditor and regulators on request.
2. On-chain supply snapshot: on-chain token supply (Venom) snapshot included with exact block height and UTC timestamp used for reconciliation.
3. Reconciliation methodology: auditor reconciles bank ledger balances (statement balances as of statement date) to on-chain supply, listing reconciling items (pending inbound/outbound items) and providing an attestor opinion that reserves ≥ circulating supply on the statement date.
4. Merkle liabilities (optional): if enabled, a Merkle tree of outstanding PHPR balances is generated and its root is published alongside the attestation; customers may verify inclusion via provided proofs.

- Publication & anchoring: Attestation PDF + JSON + Merkle root will be published on \ transparency page and an immutable reference (URL hash / small on-chain anchor) will be recorded on Venom for auditability.

- **Example attestation header (to appear at top of PDF/JSON):**

1. Statement date: 2025-09-30
2. Attestor: [NAME]
3. Escrow venues: VBank (Escrow: XXXX-1234), [PartnerBank-2: XXXX-5678]
4. On-chain supply (Venom snapshot): 10,000,000 PHPR(block: #1234567, UTC: 2025-10-01T00:00:00Z)
5. Merkle root (if used): 0x...

Appendix C - Redemption SLA (template)

- Accepted payout rails (VBank withdrawal, e-wallet, cash partner)
- Cut-off times & processing windows
- Fees disclosure (if any), FX (when cross-currency)
- Dispute & error resolution through VBank channels

Redemptions submitted before 3:00 pm PHT are settled on the same business day (T+0). Submissions after cutoff are processed the next business day (T+1). Disputes are resolved within 3–5 business days. In case of corridor outages, contingency settlement paths are activated

Consumer complaint / escalation path:

1. **Stage 1 — Merchant/Wallet support:** Customer opens ticket via TopWallet support (response SLA: initial acknowledgement within 24 hours, resolution target T+3 business days).
2. **Stage 2 — OpenPay Operations/Compliance:** Unresolved tickets escalate to OpenPay Compliance (response within 48 hours).
3. **Stage 3 — VBank (escrow / settlement issues):** For settlement/payout disputes, escalate to VBank case owner (response per SLA in Appendix C).
4. **Regulator escalation (BSP):** If unresolved after internal escalation, customers may file with BSP Consumer Assistance (BSP CAMS / BOB). BSP contacts: consumeraffairs@bsp.gov.ph; BSP Consumer Protection & Market Conduct Office phone: (02) 5306-2584 (alternative BSP contacts listed on BSP site). bsp.gov.ph+1