

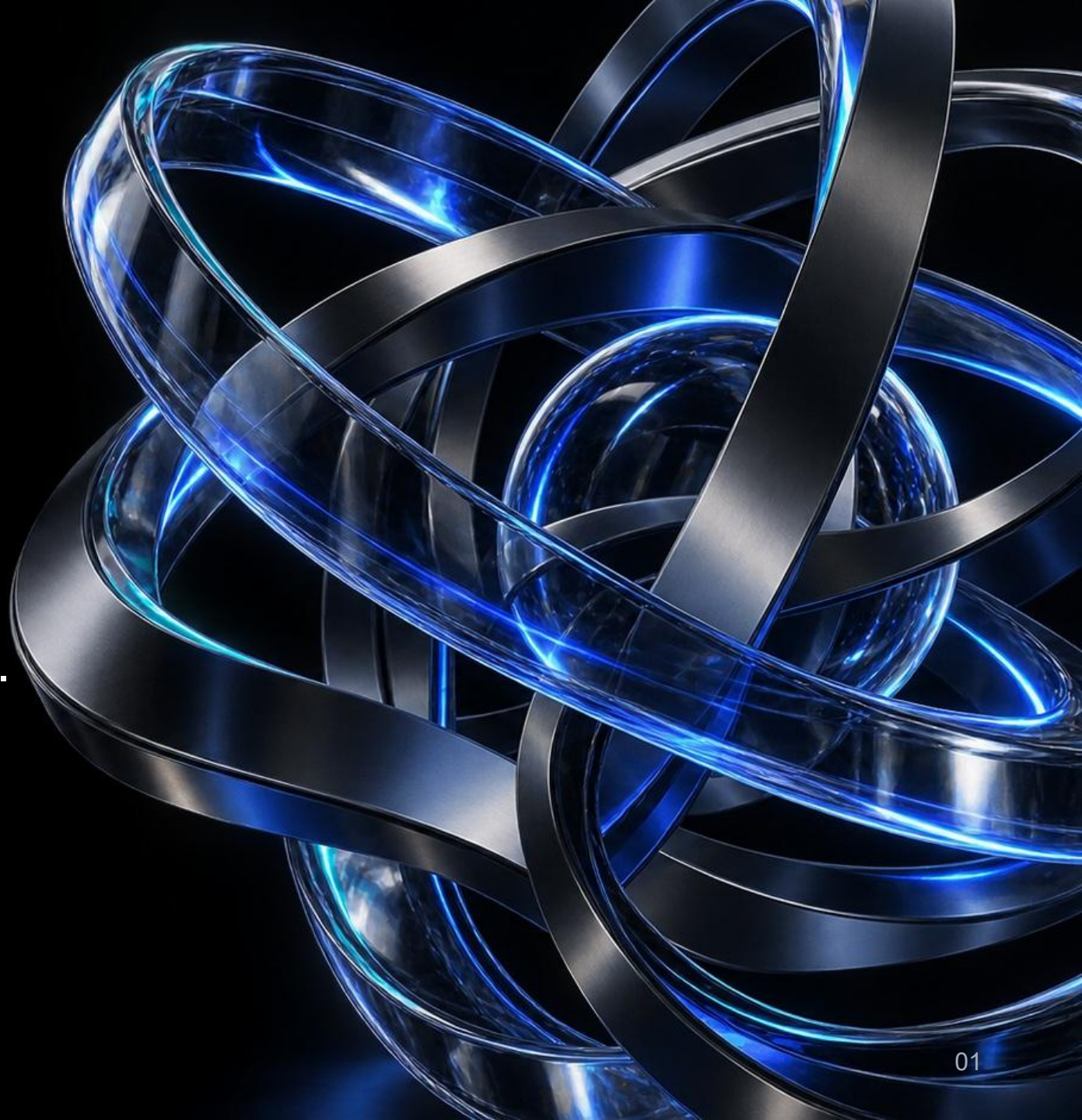
WardianEx Ltd

White Paper

Secure, transparent and scalable
infrastructure for digital asset markets.

WardianEx LTD

Version 3.0 / September 2021



Important notice

Scope, status and responsible use of this document

- | | | |
|-----------|------------------------------------|--|
| 01 | Intended operating model | Features may launch in phases, vary by jurisdiction or change with legal, operational and market requirements. |
| 02 | No investment solicitation | This document is not an offer, recommendation or promise of returns. Digital assets may involve partial or total loss. |
| 03 | Regulatory status | Service availability is subject to applicable rules. This document is not evidence of a particular authorization. |
| 04 | Forward-looking information | Future products, infrastructure and expansion plans are not guarantees of timing, performance or user outcomes. |
| 05 | Third-party references | References to service-provider categories do not imply a specific contractual relationship. |

Contents

The operating model, control framework and development priorities

04 Platform foundations

Executive summary, company overview and design principles

15 Risk & compliance

Market integrity, KYC, jurisdictional controls and asset listing

23 Transparency & governance

Reserves, privacy, continuity and the economic model

08 Technology & custody

Architecture, order handling, wallets and account security

19 Products & market access

User experience, institutional APIs and liquidity

27 Roadmap & risk factors

Capability maturity, principal risks and user responsibilities

Executive summary

A digital asset exchange designed around connected controls

WardianEx LTD is developing an exchange for retail, professional and institutional users.

Trading, custody, identity, monitoring and incident response are intended to operate as connected layers with auditable decision points.

- 01** **Protection of user assets**

- 02** **Resilient execution infrastructure**

- 03** **Transparent market rules**

- 04** **Compliance by design**

- 05** **Scalability with control standards**

Company & platform overview

WardianEx LTD is the operating entity described in this White Paper

Purpose

Develop and operate technology and services for digital asset markets.

WardianEx aims to make market access more accessible while preserving custody discipline, clear rules and user responsibility.

Web, mobile and API access

A consistent account, ledger, security and compliance framework across access channels.

Service perimeter

Spot, convert, institutional execution, payment connectivity and custody-related functions may be supported, subject to launch status and eligibility.

Operating principles

Control standards guide product development and commercial expansion

Security first	Security controls should be embedded into system design, privileged access, wallet operations, user authentication and incident response.
Rules before growth	Product rules, eligibility standards and risk limits should be defined before commercial expansion.
Separation of duties	Critical operations should require multiple control points and should not depend on a single individual, key, system or vendor.
Transparent access	Fees, order types, listing standards and material product risks should be communicated in clear language.
Measured scalability	System capacity, controls and observability should scale together, throughput alone is not treated as resilience.
Jurisdiction New products should launch only when supporting controls are sufficiently mature.	Products and onboarding pathways may differ by location to reflect applicable legal and regulatory requirements.

Market context & design principles

Continuous, distributed markets create distinct operating challenges

- | | | |
|-----------|-----------------------------------|--|
| 01 | 24/7 market activity | Automated monitoring, staffing, redundancy and escalation must support continuous operations. |
| 02 | Irreversible settlement | Key management, destination controls and withdrawal review are critical. |
| 03 | Fragmented liquidity | Thin markets may experience wider spreads, slippage and manipulation risk. |
| 04 | Variable asset standards | Token governance, smart contracts, bridges and administrator privileges create additional exposures. |
| 05 | Jurisdictional differences | Legal classifications and supervisory expectations may change across markets. |

WardianEx applies a layered-control model. No single technical control is sufficient.

Technology architecture

Logically separated services with coordinated controls and auditability

Access layer	Web, mobile and API gateways, session controls, rate limits, device and network risk signals.
Identity layer	Account state, verification status, permissions, geographic controls and institutional sub-account structures.
Trading layer	Order validation, matching, market data, trading limits, fee calculation and post-trade events.
Ledger layer	Double-entry accounting for user balances, fees, transfers, holds, settlements and internal adjustments.
Wallet layer	Deposit recognition, address management, signing workflows, withdrawal controls and blockchain monitoring.
Control layer	Security telemetry, transaction monitoring, market surveillance, audit logs, alerting and case management.
Data layer	Operational databases, event streams, reporting stores, backups and controlled analytics environments.

Engineering controls

Security, observability and capacity management support controlled scaling

- | | | |
|-----------|----------------------------------|---|
| 01 | Network separation | Defense in depth, service authentication and network segmentation. |
| 02 | Least-privilege access | Role-based access and logging for privileged operations. |
| 03 | Controlled change | Code review, testing, controlled deployment and rollback capability. |
| 04 | Centralized observability | Monitor latency, capacity, errors, wallet events, privileged actions and suspicious behavior. |
| 05 | Capacity testing | Stress scenarios identify saturation before it affects fair order handling. |

Throughput alone is not treated as resilience.

Trading engine & order lifecycle

Pre-trade checks govern access to the matching engine

01

Authenticate

Identity, authorization and account-state checks

02

Validate eligibility

Product permissions and balance or margin checks

03

Apply order controls

Price, size and rate-limit checks

04

Accept & identify

A unique internal identifier for accepted orders

05

Match

Published market rules determine matching priority

06

Record

Ledger entries, fees and account history update

Conventional order books are designed for price-time priority, unless the product specification states otherwise.

Orderly markets & post-trade processing

Execution controls continue after an order reaches the market

Market controls

Per-market configuration

Order sizes, tick sizes and quantity increments.

Erroneous-order safeguards

Price bands, fat-finger and notional controls.

Capacity and abuse controls

Throttling, eligible cancel-on-disconnect and API safeguards.

Auditable activity

Order, trade and account-event logging.

Post-trade processing

Ledger settlement

Executed trades adjust available and reserved balances and apply published fees.

Blockchain settlement

Deposits and withdrawals use controlled wallet processes, independently of internal settlement.

Execution limitations

Volatility, outages, maintenance and risk controls may affect acceptance, execution or cancellation.

Wallet & custody tiers

The design aims to limit online exposure while supporting operational liquidity

Online / hot layer	Limited operational balances for routine withdrawals, subject to automated and manual controls.
Warm or controlled layer	Intermediate operational storage used to manage replenishment and reduce direct interaction with deep cold storage.
Cold storage layer	Assets held in environments designed to minimize network exposure and require elevated approval for movement.

Custody risk

Digital assets should not be assumed to be bank deposits or government-insured funds.

Custody controls

Separation of duties

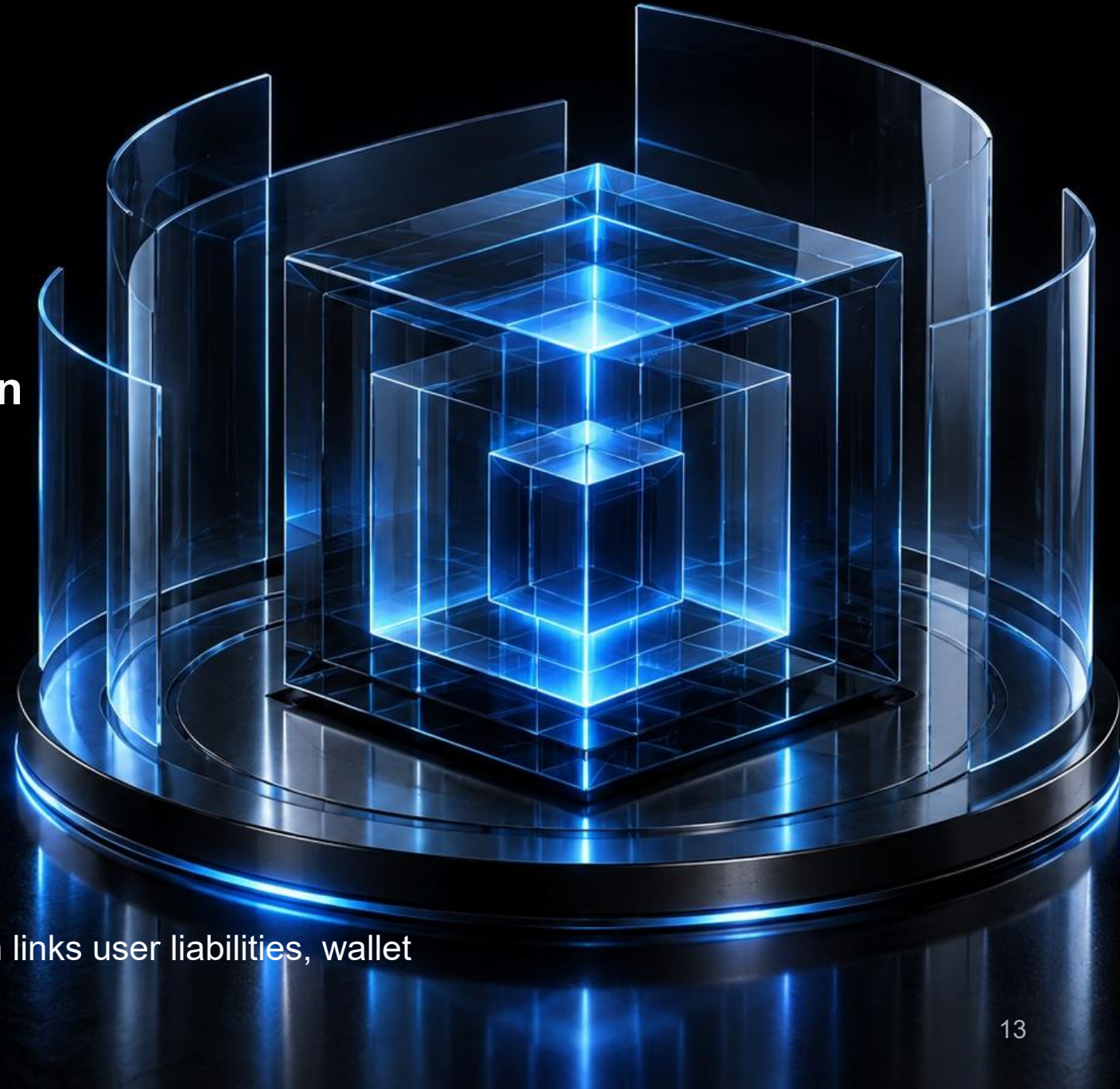
Critical signing should not depend on one person or one credential.

Hardened key environments and risk-aware withdrawal approvals

Reviewed wallet balances, privileged-action logs and exception handling

Asset accounting

The ledger records user entitlements. Reconciliation links user liabilities, wallet records and blockchain balances.



Cybersecurity & account protection

Defense in depth spans the platform, employees, users and vendors

Platform security

Segmented networks and restricted admin access

Encryption and secrets management

Security monitoring and vulnerability review

Backups and recovery procedures

User account security

Multi-factor and step-up verification where supported

Withdrawal-address and sensitive-change controls

Device, session and network monitoring

Account restriction and recovery procedures

Users remain responsible for credentials, authentication devices, API keys and endpoint security.

Risk management & market integrity

Material risks require ownership, controls, escalation thresholds and remediation

Surveillance

Self-trading and wash-like activity

Spoofing, layering and excessive cancellation

Unusual price impact, coordinated activity and misuse of multiple accounts

Potential control actions

Request information or source-of-funds evidence

Restrict products, transfers, API access or withdrawals

Cancel orders, suspend markets or apply limits

Escalate cases and report where legally required

Commercial relationships do not exempt accounts from surveillance. Conflicts of interest require active management.

Compliance, KYC & due diligence

Access and permissions may depend on identity, eligibility and risk assessment

- | | | |
|-----------|-------------------------------|--|
| 01 | Identity verification | Collect and verify information appropriate to the user type and applicable requirements. |
| 02 | Entity ownership | Review beneficial owners and control persons where required. |
| 03 | Enhanced due diligence | Apply additional review to higher-risk customers, locations, activities or transaction patterns. |
| 04 | Ongoing review | Reassess accounts when material information changes or risk indicators arise. |
| 05 | Record retention | Retain records in line with legal and operational requirements. |

Monitoring & jurisdictional controls

Products and onboarding pathways may vary by location

Transaction monitoring

Blockchain analytics, internal transactions, customer profiles, sanctions data and behavioral signals may inform case review.

An alert is an input to investigation, not a conclusion of wrongdoing.

Restricted activity

Sanctions, export controls, legal orders and internal risk policy may restrict access or transfers.

Service configurations, limits and product sets may change as legal requirements evolve.

A White Paper does not establish licensing or authorization status. Official disclosures govern.

Digital asset listing framework

Structured review before admission to trading, followed by ongoing monitoring

Technology	Network security, consensus design, smart-contract risk, upgrade mechanisms, bridges, administrator keys and implementation maturity.
Market	Liquidity, concentration, price discovery, exchange distribution, manipulation risk and dependence on a small number of counterparties.
Legal / compliance	Asset characteristics, distribution history, sanctions exposure, issuer or foundation structure, geographic restrictions and relevant legal analysis.
Operational	Wallet support, node stability, confirmations, forks, contract migrations, token redenominations and incident-response complexity.
Transparency	Availability and quality of technical documentation, governance information, supply data, material-risk disclosures and communication channels.

Listings may face limits, suspension or delisting. Admission is not an endorsement, and commercial arrangements do not replace review.

Products & service categories

Availability depends on launch status, user eligibility and jurisdiction

Spot markets	Order-book trading between supported digital assets or supported quote currencies.
Convert	Simplified request-and-execute functionality for eligible asset pairs, with a quoted rate presented before confirmation.
Institutional execution	Higher-touch or programmatic workflows for eligible professional counterparties, subject to onboarding and product rules.
Payments / fiat connectivity	Where supported, integrations with eligible payment methods or banking partners for deposits, withdrawals or conversion.
Future regulated products	Any leveraged, derivative, yield, lending, staking or structured product would require separate legal, risk and product documentation before launch.

User experience & fees

A common account and control layer across retail and professional workflows

Core experience

Account activity

Deposit supported assets, view balances, trade and request withdrawals.

Clear records

Accessible history for orders, trades, transfers and account actions.

Sensitive actions

Confirmations and risk warnings for security, account and withdrawal changes.

Service-status and maintenance communications should be available through official channels.

Fee transparency

Fees may vary by product, market, user tier, payment method and blockchain network conditions.

Users should review the current fee schedule and material promotional conditions before submitting a transaction.

Institutional services & APIs

Professional access remains inside the same risk and control perimeter

Institutional capabilities

Entity administration

Entity onboarding, beneficial owners, authorized users and supported permission groups.

API access controls

Key scopes, IP restrictions, withdrawal permissions and key rotation.

Operational transparency

Order, trade, balance and transfer reporting, with eligible escalation channels.

Programmatic integration

Interfaces

REST, WebSocket or other interfaces may support market data, trading and accounts.

Platform safeguards

Rate limits, permission scopes, order-size limits and account-level risk settings.

User safeguards

Retries, reconciliation, kill switches, monitoring and separate development credentials.

APIs may disconnect, delay data or fail partially. Professional users must plan for maintenance and failure handling.

Liquidity, execution & market quality

Market access follows disclosed rules, with no guarantee of depth or execution

Market-quality objectives

Reliable market data subject to system constraints

Consistent matching rules for eligible participants

Controls for disorderly orders and abusive behavior

Configuration reflecting liquidity and asset characteristics

Monitoring of spreads, depth, volatility and concentration

Fair access

**Commercial status
should not grant
undisclosed matching
priority.**

Market makers remain subject to trading rules and surveillance. Market orders can slip, and limit orders may not execute.

Transparency, reserves & reporting

Reserve information must be tied to reconciliation and clear scope

Wallet balances alone do not establish solvency.

Reserve disclosures should explain methodology, scope, date, limitations and the treatment of liabilities.

Proof of reserves does not replace liability accounting, governance or legal analysis of custody arrangements.

01 User liabilities

Reconcile user entitlements with internal ledger balances.

02 Custody assets

Reconcile wallet records with supported blockchain balances.

03 Exceptions

Investigate breaks, pending deposits, failed withdrawals and adjustments.

04 Public reporting

Rules, fees, service incidents and reserve methodologies may be disclosed.

Data protection & privacy

Documented purposes, controlled access and appropriate retention

Data governance

Account, identity, transaction, device, support and security information may support platform operations and legal or risk obligations.

A separate Privacy Notice governs personal-information handling and user-facing rights.

01 Role-based access

Limit information access to assigned duties.

02 Administrative oversight

Log and review sensitive actions.

03 Minimization and retention

Align practices with legal and operational requirements.

04 Vendor and incident controls

Govern third-party processing and respond to potential data exposure.

Business continuity & recovery

Ledger integrity and secure key control are central recovery priorities

Controlled recovery

Restore user access in a controlled manner and communicate clearly during material disruptions.

Continuity and disaster-recovery processes are intended for critical services.

01 Redundancy

Recovery reflects system criticality.

02 Restoration testing

Test backups and critical-data restoration.

03 Incident authority

Severity levels, escalation and decision rights.

04 Maintenance discipline

Control changes to production systems.

05 Post-incident review

Root causes, control gaps and remediation.

Governance & economic model

WardianEx LTD retains responsibility for platform operating decisions

Accountable governance

Defined ownership for technology, security, compliance, finance, operations and market integrity.

Escalation procedures for decisions across functional boundaries.

Service-based revenue

Disclosed fees and permitted commercial arrangements associated with exchange activity, payment connectivity and institutional services.

No native platform token is assumed.

Control over incentives

Growth targets should not override sanctions, identity, custody or market-integrity controls. Expansion requires operational and regulatory readiness.

Development roadmap

Capability maturity governs progression through five phases

Phase I - Core foundation	Account system, identity controls, core ledger, supported wallet infrastructure, spot-market engine, web interface, monitoring, customer support and baseline compliance controls.
Phase II - Market depth	Broader asset support, refined listing governance, mobile experience, improved market data, enhanced surveillance, operational automation and expanded liquidity relationships.
Phase III - Professional access	Institutional account structures, advanced APIs, reporting tools, permissioning, connectivity improvements and operational service layers for professional users.
Phase IV - Geographic expansion	Jurisdiction-specific onboarding, payment connectivity and localized product configurations where legal and operational requirements can be satisfied.
Phase V - Selective product expansion	Additional regulated or higher-complexity products only where separate risk, legal, liquidity, custody and technology frameworks have been completed.

Readiness gates & measures of progress

The roadmap does not promise fixed delivery dates

Readiness before expansion

Security readiness, liquidity, legal analysis, testing and third-party dependencies can change timing.

A product may be delayed, limited or discontinued if control maturity is insufficient.

- 01 System reliability and recovery performance
- 02 Security findings and remediation progress
- 03 Reconciliation and custody-control effectiveness
- 04 Market quality and surveillance outcomes
- 05 Compliance and jurisdictional readiness
- 06 Support performance and documentation clarity

Principal risks: assets & technology

Platform controls cannot eliminate material digital asset risks

Market risk

Prices can change rapidly. Assets may become illiquid or lose substantially all value.

Technology risk

Software defects, congestion, forks, protocol changes and smart-contract vulnerabilities can affect services.

Cybersecurity risk

Phishing, malware, credential theft, infrastructure attacks and key compromise can cause loss.

Custody risk

Failures in wallet processes, signing, vendors or supported networks can cause loss or delay.

Principal risks: operations & access

External dependencies and operating failures may disrupt service or execution

Regulatory risk

Changing laws or classifications may affect products, onboarding, transfers, asset support and geographic access.

Counterparty & vendor risk

Banks, payment providers, custodians, cloud providers, data vendors and market makers may fail or face restrictions.

Liquidity & execution risk

Spreads, volatility, slippage, gaps and insufficient depth may impair execution or prevent it entirely.

Operational risk

Human error, control failures, system changes and reconciliation breaks can disrupt service or create losses.

Responsible participation

Assess suitability and risk tolerance.
Protect credentials and devices.
Review current product disclosures.
Understand irreversible transactions.

Consult official WardianEx channels for the current Terms of Use, Risk Disclosure, Privacy Notice, Fee Schedule and local notices.

