BxbayEx

EXCHANGE WHITEPAPER

BxBayEx

Markets built on clear rules

Digital asset trading infrastructure

VERSION 1.0 / OCTOBER 2026

Platform profile

Digital asset markets, accountable infrastructure

BxBayEx Exchange is a proposed platform for individual traders, advanced participants and eligible institutions. Its scope covers account access, spot execution, asset transfers and support.

Proposed service experience

A coherent journey spans identity checks, account security, market access, execution records and customer support.

Design priorities

Availability, fair access, asset protection and understandable rules guide the product and its controls.

Forward-looking engineering targets, fee examples and financial forecasts remain distinct from operating results.

Whitepaper contents

01 **Market & product** 04-12

Market context, ecosystem, execution, liquidity and listing

02 **Safeguards & integrity** 13-20

Custody, cybersecurity, identity, surveillance and stress testing

03 **Experience & infrastructure** 21-26

User journey, APIs, architecture, privacy and governance

04 **Business & development** 27-33

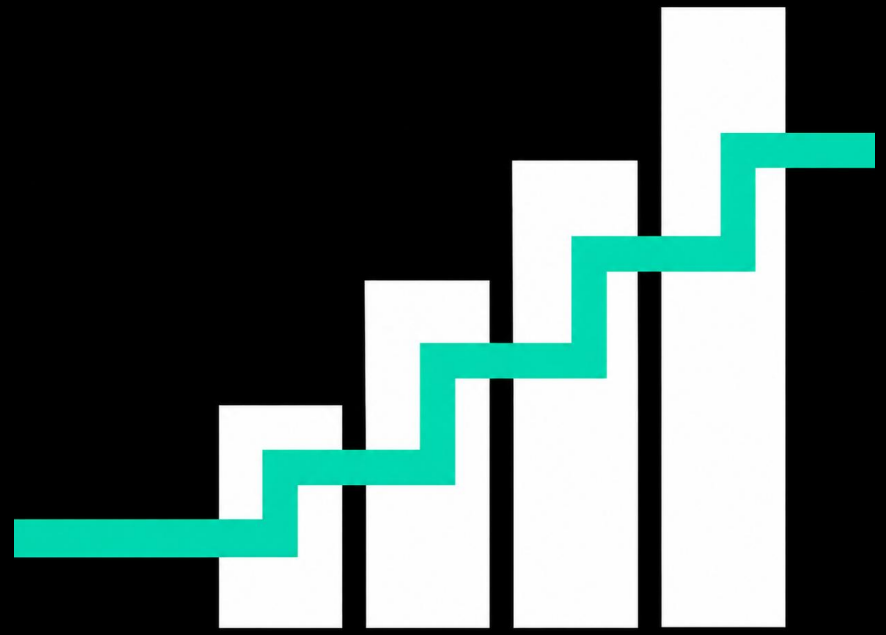
Fees, economics, planning, distribution and release criteria

Risk factors and legal notices conclude the whitepaper on page 34.

01

Market & product

Market structure, spot execution and the operating rules behind a dependable trading venue.



Market context and customer friction

Reliable access depends on the whole customer journey, not a single headline fee.

Visible trading costs

Commissions, spreads and withdrawal charges shape the price customers see before and after execution.

Operational friction

Failed transfers, unsupported networks, delayed reviews and unclear order status add costs that a headline fee does not capture.

Fragmented market structure

Continuous trading spans venues, networks, custody models and different standards for identity and market conduct.

Competitive response

Assess executable liquidity, retention under volatility, processing reliability and the clarity of incident communication.

Mission and service principles

Customers should understand what they trade and how the platform handles it

Product complexity must be justified by customer need and proportionate controls. Accessible records, consistent terminology and responsive support are part of the service.

Clarity

Understandable instruments, fees, confirmations and disclosures.

Integrity

Documented order rules and conflict-management procedures.

Resilience

Tested recovery, careful change management and accountable decisions.

Service availability follows applicable law and operating capacity in each supported location.

Platform ecosystem

Common identity, permissions and audit capabilities connect distinct service domains.

Service domain	Customer function	Operating focus
Account and access	Registration, verification and security	Consistent permissions and limits
Spot exchange	Order entry, matching and market data	Predictable order states and execution rules
Transfers and balances	Deposits, withdrawals and portfolio records	Ledger integrity and wallet reconciliation
Support and reporting	Statements, tickets and dispute escalation	Traceable decisions and clear review states

Margin, derivatives, lending and yield services require separate legal, risk and technical assessment.

Spot market structure

Market orders

Execute against available order-book liquidity, subject to applicable filters and execution protections. The execution price may differ from the last traded price.

Limit orders

Specify a price boundary and may rest in the order book. The venue applies executable price first and then order arrival time.

Common market protections

Self-trade prevention, minimum notional rules, permitted price increments, price collars and configurable rate limits reduce avoidable execution anomalies.

Market data should show recent trades, depth, 24-hour indicative metrics and notices. No execution price or fill is guaranteed.

Order lifecycle

01

Validate

Authenticate the request and check balances, symbol status, precision, compliance and risk limits.

02

Acknowledge

Confirm acceptance with an identifiable order state and sequence reference.

03

Match or rest

Apply price-time priority. Executable quantity trades and remaining valid quantity may rest.

04

Settle records

Book executions to the ledger and reconcile authoritative execution and balance records.

05

Notify

Publish state changes to market data, the customer interface and execution updates.

Idempotency, deterministic transitions, replayable logs and explicit sequencing prevent duplicate or ambiguous processing.

Matching and operational objectives

<15 ms

Median internal matching response target

99.95%

Monthly core trading availability objective

Validation programme

Deterministic regression, load, soak, failover and chaos scenarios should test burst conditions and degraded dependencies.

Engineering objectives apply after stabilization. They are not measured operating performance or unconditional service guarantees.

Liquidity and market quality

Measure	What it reveals	Operating use
Spread and 1% depth	Quoted price gap and nearby executable size	Assess market conditions at realistic trade sizes
Fill ratio and slippage	Realized execution and unfilled demand	Review customer outcomes beyond quoted spreads
Quote continuity	Consistency of firm, executable liquidity	Evaluate qualifying provider performance
Cancellation patterns	Order behavior and possible market-quality issues	Combine context, surveillance and provider review

Tighten filters, stage openings, restrict or suspend a pair when orderly conditions cannot be maintained. Wash trading is not adoption.

Asset listing and ongoing review

01

Application

Project identity, token function, public documentation, supply and concentration.

02

Technical review

Network finality, code maturity, upgrade controls, bridges and wallet support.

03

Legal screening

Jurisdictional exposure, sanctions, litigation and material disclosure concerns.

04

Market review

Price discovery, liquidity, unlock schedules and susceptibility to manipulation.

05

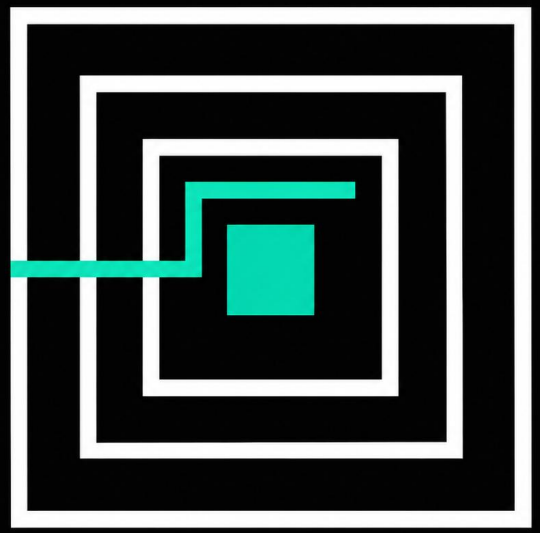
Committee decision

Document the decision and conditions. Monitor material changes after listing.

Ongoing review may lead to enhanced warnings, withdrawal-only status, restrictions or delisting, supported by customer notices.

02

Safeguards & integrity



Asset safeguarding, financial crime controls and resilience under normal and stressed conditions.

Custody and wallet architecture

90%

Reference isolated-storage target

Eligible safeguarded holdings in offline or otherwise strongly isolated storage.

Control area	Reference safeguard
Wallet layers	Controlled online liquidity and deeper isolated storage
Signing access	Least privilege, role separation and multisignature or MPC where appropriate
Asset movements	Dual control, thresholds, screening, limits and out-of-band checks
Assurance	Independent review when commissioned and completed

90% is a policy planning parameter, not a current composition claim. Cold-storage ratios alone do not establish solvency.

Ledger, reconciliation and fund separation

Customer entitlements, wallet positions and corporate resources serve different purposes.

Record or resource	Control objective	Reconciliation focus
Customer entitlements	Maintain append-only account records	Balances and executions agree with booked ledger entries
Wallet and custodial positions	Evidence the assets held or administered	Ledger totals reconcile to on-chain and other records
Corporate treasury	Separate operating cash, fees and other resources	No undisclosed use of customer assets for operations
Exceptions and assurance	Assign ownership and preserve decision records	Investigate breaks and track remediation

Liabilities, encumbrances, legal ownership and reconciliation quality matter alongside any future proof-of-reserves report.

Cybersecurity control layers

Control layer	Representative measures	Priority exposures
Customer identity	Authentication options, sessions and security notifications	Account takeover and phishing
Application and APIs	Secure development, scoped keys and controlled changes	Key misuse and application compromise
Infrastructure	Segmentation, patching, secrets protection and monitored access	Privileged access and supply-chain compromise
Wallet operations	Approval flows, address controls and fraud-aware recovery	Withdrawal fraud and signing-material exposure

Threat modelling informs architecture. Penetration testing, vulnerability management and third-party reviews support validation.

Incident response and continuity

15 min

Indicative critical-alert triage objective

Recovery objectives are defined by service rather than assumed to be identical across the platform.

01 **Triage and decision rights**

Classify severity and assign accountable incident leadership.

02 **Contain and preserve**

Limit impact while retaining evidence and decision records.

03 **Recover and communicate**

Test restoration, dependency failure and appropriate notifications.

04 **Review and improve**

Record causes, remediation and follow-up testing.

Response readiness requires recurring exercises. Legal and security constraints govern external incident communications.

Identity and financial crime controls

Control stage	Information and checks	Decision and evidence
Onboarding	Identity, eligibility and beneficial ownership where applicable	Risk-based standard, enhanced or institutional review
Screening	Sanctions, PEP exposure and geographic restrictions	Disposition with documented criteria and escalation
Ongoing monitoring	Behavior, transaction patterns and blockchain indicators	Contextual analyst review and preserved case evidence
Reporting and retention	Applicable reporting, travel-rule and record obligations	Jurisdiction-specific procedures and retention schedules

A flagged activity is a signal for review, not a presumption of illicit conduct. Service eligibility remains jurisdiction dependent.

Market surveillance and integrity

Surveillance coverage

Potential wash trading, spoofing, layering, self-dealing, coordinated manipulation, abusive API behavior and listing-related anomalies.

Evidence and interpretation

Rules-based alerts and statistical analysis feed analyst review. Legitimate market making requires contextual interpretation.

Case handling

Preserve data, apply consistent triage, document investigation decisions and use proportionate enforcement.

Conflicts and transparency

Information barriers, employee activity rules and equal treatment apply to internal and affiliated accounts.

Response options include warnings, enhanced monitoring, restrictions, suspension and external reporting where appropriate.

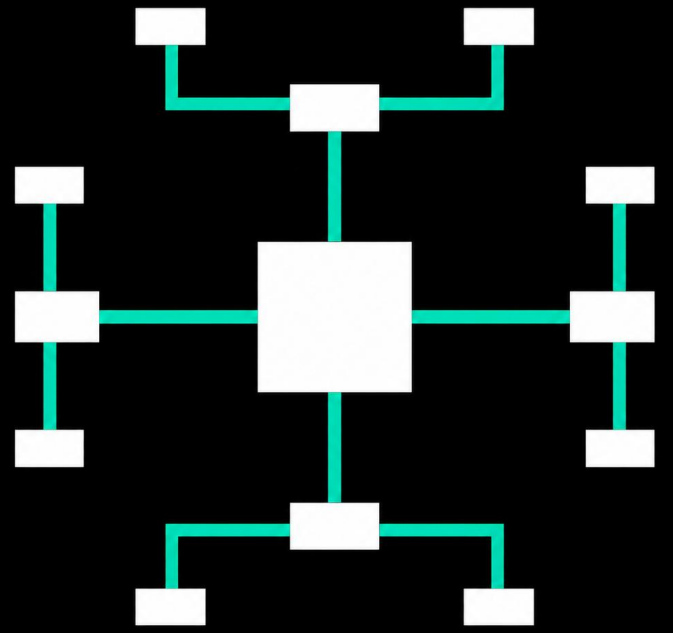
Enterprise risk and stress scenarios

Stress scenario	Exposure to assess	Required preparation
Price shock or stablecoin depegging	Market, liquidity and counterparty concentration	Triggers, risk limits and decision records
Network congestion or cloud outage	Transfers, processing capacity and service continuity	Dependency response and restoration exercises
Wallet compromise attempt	Signing access and asset-movement controls	Containment and evidence-preservation procedures
Concentrated withdrawals or provider loss	Available liquidity and execution quality	Withdrawal response, liquidity oversight and communications

Business owners, independent risk/compliance and independent assurance form three lines of accountability.

03

Experience & infrastructure



Customer workflows, institutional access, authoritative records and data governance.

Customer journey and accessibility

01

Register and verify

Explain eligibility, required identity information and review states.

02

Protect and fund

Account security, supported networks and clear deposit status.

03

Select and trade

Market terms, order descriptions and legible fee previews.

04

Review and withdraw

Execution records, statements and explicit transaction status.

05

Support and resolve

Tracked tickets, dispute escalation and understandable errors.

Accessibility includes contrast, keyboard navigation, screen-reader labels and localization. Measure completion and complaint recurrence.

Institutional connectivity and API access

Credential scope	Intended functions	Security treatment
Read-only	Market data, balances and reporting	Least privilege, monitoring and revocable access
Trading	Authenticated order and account workflows	Idempotency, explicit errors and rate controls
Withdrawal	Separately authorized asset movements	Permission segregation and additional policy controls

Institutional integration standards

Versioned changes, deprecation guidance, optional IP restrictions, key rotation and eligibility-based support make integrations predictable.

Dedicated service terms do not change price-time priority or exempt clients from surveillance and compliance requirements.

Reference technology architecture

Architecture domain	Principal functions	State and operating characteristics
Client interfaces	Web, mobile and authenticated APIs	Consistent entitlement model across entry points
Core records	Matching, ledger and reconciliation	Explicit ownership, strict ordering and integrity
Service projections	Market data, analytics and notifications	Observable lag where eventual consistency is appropriate
Operating infrastructure	Secure builds, deployments, telemetry and recovery	Capacity headroom, rollback and regional controls

Service boundaries follow control needs and recovery characteristics, supported by explicit schemas, access logs and reconciliation checkpoints.

Data governance and privacy

Collect only what the service needs

Identity records, device signals, financial data and blockchain-linked activity require defined purposes and accountable ownership.

01 **Collect and validate**

Define provenance, metadata and quality checks.

02 **Use and protect**

Apply purpose limits, encryption, role controls and logging.

03 **Retain and dispose**

Follow schedules, lawful retention and permitted deletion.

Data-subject requests, cross-border transfers and breach notifications depend on law. Mandatory records may outlast account closure.

Governance and accountability

Accountability line	Primary responsibility	Evidence of oversight
Business control owners	Own risks and day-to-day control performance	Policy ownership, approval thresholds and operating indicators
Independent risk and compliance	Challenge decisions and escalate tolerance breaches	Risk review, conflict handling and committee records
Independent assurance	Test control effectiveness and remediation	Testing plans, findings and tracked corrective actions

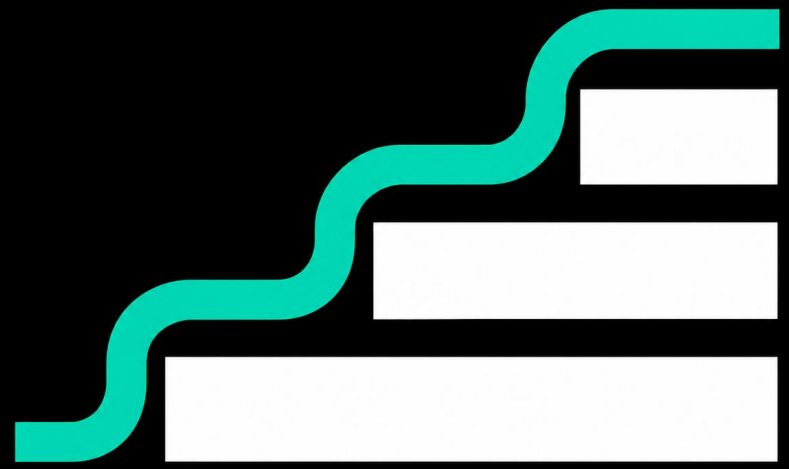
Decision rights and committees

Executive, listing, risk and incident groups need documented mandates, voting rules, conflict disclosures and authority to pause activities.

04

Business & development

Commercial economics, scenario planning and disciplined expansion of services and markets.



Revenue model and fee structure

Illustrative trading tier	Maker fee	Taker fee
Retail	0.10%	0.16%
Qualifying high volume	0.04%	0.08%

0.12%

Blended net take rate in the planning case

Commercial discipline

Transaction fees form the core revenue stream. Institutional connectivity and premium reporting require commercial justification and legal permissibility.

These are fee examples and planning assumptions, not a published customer tariff. Withdrawal charges need disclosure before confirmation.

Unit economics and fee revenue scenario

Illustrative net trading fee revenue equals annual spot volume multiplied by the 0.12% planning take rate.



Direct delivery costs

Processing, liquidity incentives, customer support, fraud, compliance, custody, cybersecurity and payment rails.

Contribution margin

Fee revenue must cover the direct costs of delivering and supervising the service.

Derived from source assumptions: $1.2B / $4.1B / $10.5B × 0.12%. Before costs. These are neither actual revenue nor profit forecasts.

Three-year financial planning scenario

Planning metric	Year 1	Year 2	Year 3
Verified users	80,000	220,000	480,000
Monthly active traders	18,000	48,000	105,000
Annual spot volume	$1.2B	$4.1B	$10.5B
Calculated net trading fees	$1.44M	$4.92M	$12.60M

Illustrative three-year planning scenario, not audited or historical performance. Calculated fees use 0.12% and exclude costs.

Planning sensitivities and operating KPIs

Forecast sensitivities

Active-user conversion, customer turnover, blended take rate, market cycles and jurisdictional availability drive the model.

Downside planning

Test lower liquidity, higher verification costs and deferral of product or market expansion.

Commercial indicators

Review funded and active users, retention, cohort contribution margin and risk-adjusted acquisition cost.

Safeguarding indicators

Track reconciliation breaks, failed withdrawals, complaints, slippage, security incidents and enforcement consistency.

Volume growth alone is not a sufficient success measure if execution quality, reconciliation or customer protection deteriorates.

Growth strategy and market entry

01

Eligible visitors

Reach permitted audiences through understandable, compliant communications.

02

Verified users

Complete proportionate identity and eligibility review.

03

Funded accounts

Provide dependable funding and transparent processing status.

04

Active traders

Support responsible use and measurable execution quality.

05

Retained users

Maintain support quality and a consistent operating experience.

Market entry also requires legal readiness, language, payments, liquidity, local support and fraud testing. Channels include content and qualified partners.

Development priorities and release gates

Development workstream	Priority scope	Release evidence
Phase I / 0–6 months	Architecture, security baseline, legal review and closed functional tests	Documented controls and tested end-to-end processing
Phase II / 6–12 months	Staged spot launch, wallet operations, surveillance and integrations	Stable reconciliation, monitoring and support playbooks
Phase III / 12–24 months	Institutional tooling, localization and additional markets	Legal readiness, liquidity and operational capacity

Every release needs a go/no-go decision

A visible interface is not the completion criterion. Operating controls, incident procedures, reconciliation and support need validation.

Timing and sequencing remain indicative and depend on testing, funding, legal assessment and third-party dependencies.

Risk factors and legal notices

Trading and asset risks

Abrupt price changes, disappearing liquidity, congestion, network reorganization, stablecoin reserves and bridge dependencies can cause losses, including total loss.

Operational and legal risks

Custody systems, cyber controls, counterparties and third parties can fail. Legal measures may restrict or prohibit services.

Forward-looking information

Features, engineering targets, storage ratios, fee examples, forecasts and future milestones are forward-looking planning inputs.

Terms and reliance

BxBayEx is a proposed platform. Availability and safeguards require confirmation. No license, audit opinion, token issuance or investment-return entitlement is asserted.

Informational material only. Not legal, tax, investment or financial advice. No guarantee of returns, security or uninterrupted service.