



CRYPTO-AS-A-SERVICE PLAYBOOK:

How Banks, Telcos, and Fintechs Launch Crypto Products Fast, Safely, and Compliantly



Provided by WhiteBIT
and  CryptoSlate

INTRODUCTION

Crypto-as-a-Service (CaaS) is the “build crypto products without building a crypto exchange” approach. Your institution keeps the customer relationship, product governance, and brand experience; a specialist provider supplies wallet infrastructure, execution rails, custody options, and operational tooling to run crypto safely at scale.

This matters because most regulated institutions do not fail on “can we build it.” They fail on operational risk: custody controls, fraud, reporting, and the day-two responsibilities that come after launch.

In this guide, you will learn:

- Why banks, telcos, and fintechs are revisiting crypto products now, without relying on hype
- What CaaS includes (and what it does not) for procurement, risk, and compliance teams
- A reference architecture for integrating a CaaS stack into identity, core ledger, and support tooling
- A phased rollout plan for a “minimum viable crypto product,” including the guardrails that prevent regrets
- How to evaluate security, custody, compliance workflows, payments rails, economics, and vendors

Who this guide is for: fintechs, banks, neobanks, telcos, payment providers early in crypto adoption, plus brokerages and smaller exchanges adding rails.

Disclaimer: Informational only, not financial, legal, or compliance advice. Regulations vary by jurisdiction; involve your legal and compliance teams early.

Timing shift

WHY CAAS NOW FOR BANKS, TELCOS, AND FINTECHS

A few years ago, “adding crypto” often meant bolting a volatile asset class onto a consumer app and hoping demand carried the product. That era is fading. Today, institutions revisiting crypto are doing it with more pragmatic goals and tighter controls.

Demand is real, but needs governance

Customer demand exists across multiple use cases, and it is rarely “just trading.” Common asks include trading and conversion, transfers, spending, and treasury utility. The challenge is not demand, it is delivering a controlled experience with clear disclosures, predictable operations, and compliant workflows.

Competitive pressure is structural

Neobanks and super-app style fintechs increasingly bundle more financial services under one roof. Crypto is often on the shortlist because it can lift engagement and retention, but only if the product is reliable and supportable at scale.

Monetization is measurable

Crypto products can be evaluated like any other financial product line. Common levers include conversion take rate, spreads (with transparent disclosure), transaction fees, premium tiers, and retention-driven revenue per user expansion. The key is to model unit economics alongside risk and operational cost from day one.

Partnerships shorten the path

For many newly launching banks and fintech programs, the most realistic path is integration: white-label partners and core-banking providers can connect to a CaaS provider so a new institution can receive crypto functionality without standing up every component internally.

WhiteBIT tie-in: CaaS is positioned as a faster, lower-risk route than building a full stack, especially when you want to keep governance inside the institution while outsourcing specialized infrastructure.

Clear lines

CAAS EXPLAINED, WHAT IT IS AND WHAT IT IS NOT

In procurement-friendly terms, Crypto-as-a-Service (CaaS) is a packaged set of capabilities that lets a bank, fintech, or telco offer crypto functionality without operating an exchange stack in-house.

What CaaS typically includes

- **Wallets and address generation:** creating deposit addresses, tracking balances, orchestrating transactions
- **Custody options:** platform custody, third-party custody integrations, or hybrid designs
- **Pricing and execution:** fiat to crypto conversion, quote formation, execution rules, slippage and limit logic
- **Compliance tooling:** KYB and KYC alignment, sanctions checks, monitoring outputs, recordkeeping support
- **Reporting and reconciliation:** ledger feeds, statements, audit logs, operational exports
- **Operational support:** onboarding coordination, incident response processes, ongoing technical account support

What CaaS is not

CaaS does not outsource accountability. Your institution still owns customer outcomes, product governance, disclosures, complaint handling, fraud policy, and regulator relationships. Treat CaaS as infrastructure, not a compliance shield.

It is also not “set and forget,” and it is not one-size-fits-all. Crypto products remain operationally alive: networks change, fraud patterns evolve, and compliance expectations shift. Your implementation must be designed for ongoing operations, not just launch.

Build vs buy vs partner

Decision path	Best when	Watch-outs
Build in-house	You have deep crypto engineering plus 24/7 operations and want full control over custody and execution	Long time-to-market, higher security and compliance burden, harder to maintain across chains
Buy point solutions	You want best-of-breed vendors (custody, analytics, payments) and can manage multi-vendor integration	Integration complexity, vendor sprawl, unclear incident ownership, slower delivery
Partner via CaaS	You want fast, controlled launch with fewer moving parts and clearer shared processes	Must negotiate strong SLAs and evidence, confirm jurisdictional permissions, plan exit strategy

Optional add-on, yield style products

Some institutions explore yield-like features for eligible users and jurisdictions, such as crypto lending. Treat this as a separate risk decision with its own approvals, disclosures, and controls.

WhiteBIT tie-in: WhiteBIT positions “one place for institutional crypto needs” with modular services and tailored onboarding, which can be helpful when your roadmap expands from conversion to custody and payments.

System map

THE REFERENCE ARCHITECTURE, HOW A CAAS STACK FITS INTO YOUR SYSTEMS

A successful CaaS launch starts with a clear integration map, not just API endpoints. The question is: where does crypto live in your operating model, and how does it connect to identity, ledger, and support workflows?

Core systems to connect

Most institutions integrate CaaS across four layers:

- **Channels:** mobile app, web app, agent tools, or telco channels
- **Identity and risk:** KYC and KYB, MFA, device intelligence, fraud scoring, step-up auth
- **Core ledger and finance:** sub-ledgers, GL mapping, fee logic, reconciliation, reporting exports
- **Operations and support:** case management, investigations, customer support tooling, incident playbooks

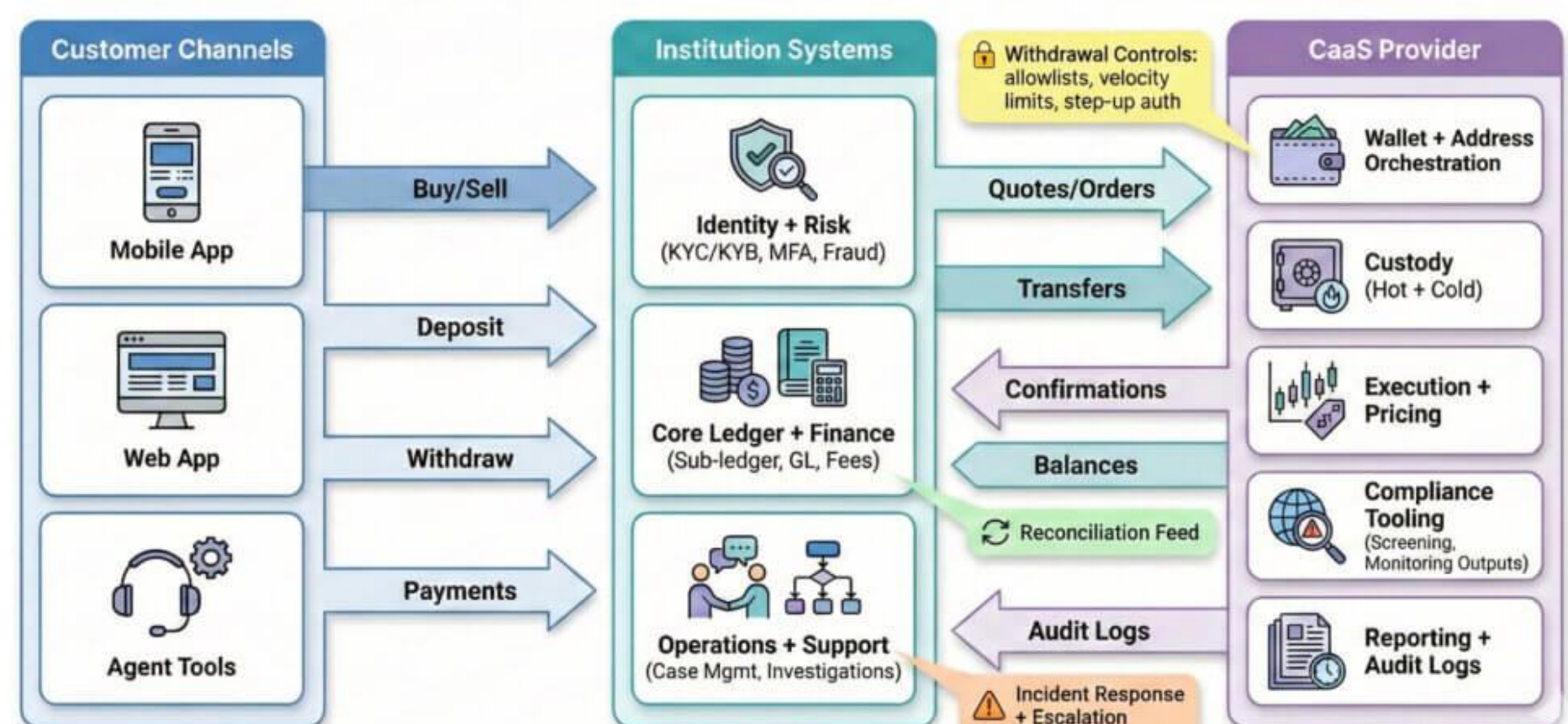
Wallet orchestration is the hard part

The tricky part is not “making a wallet.” It is address management and transaction orchestration across networks: deposit address generation, withdrawal controls (whitelists, velocity limits), chain incident handling, fee volatility, and operational visibility.

Execution, reconciliation, and reporting

Even for a simple “buy and hold” product, finance and audit teams will ask how prices are formed, how conversion is executed, how balances reconcile between your ledger and custody environment, and what logs exist for every administrative action and customer transaction.

Crypto-as-a-Service (CaaS) Reference Architecture



How WhiteBIT approaches it

Industry challenge: Institutions often underestimate day-two operations. Chain incidents, reconciliation edge cases, and support workflows become the bottleneck, not the API.

What institutions should require: Clear system boundaries, deterministic ledger feeds, strong logging, and an incident response model with defined ownership and escalation paths.

WhiteBIT approach: WhiteBIT positions a comprehensive institutional stack across CaaS, custody, and payments, with a relationship-led onboarding model, integration-first posture, and a fast go-live narrative supported by implementation planning.

LAUNCH PATH, THE “MINIMUM VIABLE CRYPTO PRODUCT” IN PHASES

The safest institutional pattern is to launch crypto in phases. Each phase expands surface area, assets, networks, corridors, only after controls prove stable and operations can support real usage.

Phase 1, convert and hold

Start with buy and sell conversions and custody, using a limited asset allowlist and conservative limits. Keep the experience simple, optimize onboarding and disclosures, and verify reconciliation and support readiness before expanding features.

Phase 2, deposits and withdrawals

Add deposit addresses and withdrawals on approved networks. This is where operational complexity increases: chain fees, address mistakes, fraud attempts, and compliance workflows will surface. Expand networks slowly, and ship “withdrawal safety” features early.

Phase 3, advanced utility

Recurring buys, broader conversion paths, B2B payouts, merchant settlement, and treasury workflows come last. These features can be valuable, but they magnify compliance and operational demands.

Guardrails that prevent regrets

Regardless of phase, the core guardrails are consistent: asset allowlists, transaction limits, network risk scoring, and step-up authentication for high-risk actions.

Phase	What customers get	Controls and KPIs to gate expansion
Phase 1, convert plus hold	Fiat to crypto conversion, custody portfolio, basic statements	Controls: small allowlist, conservative limits, step-up auth, clear disclosures. KPIs: conversion success rate, fraud rate, support tickets per 1,000 users, reconciliation breaks.
Phase 2, transfer rails	Deposits and withdrawals on approved networks, address book	Controls: withdrawal whitelists, velocity limits, network risk scoring, recordkeeping for transfers. KPIs: withdrawal failure rate, time-to-resolution for incidents, suspicious activity alert backlog.

Phase 3, utility plus B2B	Recurring buys, B2B payouts, merchant settlement, treasury conversion	Controls: counterparty controls, enhanced KYB, payout screening, settlement rules, stronger SLAs. KPIs: retention uplift, revenue per user uplift, payout SLA adherence, audit findings severity.
------------------------------	--	--

How WhiteBIT approaches it

WhiteBIT positions partner-led implementation and a scalable expansion path, which aligns with phased launches that start conservative and widen scope once operations are proven.

Safety rails

SECURITY AND CUSTODY DESIGN CHOICES INSTITUTIONS MUST GET RIGHT

Custody is usually the biggest blocker because it concentrates operational, legal, and reputational risk in one place. Start by choosing a custody model aligned to your governance requirements, then focus on the controls that govern day-to-day operations.

Custody models to consider

Model	Strengths	Risks to mitigate
Platform custody	Fastest go-live, fewer vendors, simpler customer UX	Provider concentration risk, require evidence of controls, segregation clarity, withdrawal governance
Third-party institutional custody	Clear separation, aligns with some governance models	Integration overhead, operational handoffs, slower incident response if roles are unclear
Hybrid custody	Segmented risk and flexibility by segment or asset type	More complex reconciliation, higher governance burden, avoid shadow processes

Controls that matter most

Security discussions often over-focus on “cold vs hot.” For institutions, the non-negotiables are operational controls:

- Withdrawal whitelisting and address books
- Multi-approver withdrawals with segregation of duties
- Role-based access controls for internal operators
- Incident response playbooks plus audit-ready logging
- Strong customer authentication and account takeover defenses

Non-negotiable controls checklist

- Withdrawal allowlists plus velocity limits
- Maker-checker approvals and segregation of duties
- RBAC plus privileged access management
- Incident response, defined escalation paths, post-incident reviews
- Audit logging for administrative actions and fund movements

If a vendor cannot evidence these controls, “fast launch” becomes an institutional liability.

How WhiteBIT approaches it

Industry challenge: Institutions need enterprise-grade custody controls, but many crypto stacks were built for retail speed over institutional governance.

What institutions should require: Clear custody documentation, withdrawal governance, access controls, and independent validation that matches the scope of services used.

WhiteBIT approach: WhiteBIT positions custody as part of a broader institutional stack, including integrations with institutional custody infrastructure, alongside an onboarding model designed to align operational controls with institutional requirements.

Control plane

COMPLIANCE AND AML, RESPONSIBILITIES, WORKFLOWS, AND REPORTING

Crypto compliance is not a single checkbox. It is an operating workflow spanning onboarding, monitoring, investigations, and audit-ready recordkeeping. A CaaS model can provide tooling and support, but the institution must still own governance decisions and regulator-facing accountability.

What “compliance” looks like in practice

- **KYB and KYC alignment:** onboarding, risk tiering, beneficial ownership for business accounts
- **Sanctions screening:** counterparties, jurisdictions, and relevant indicators
- **Transaction monitoring:** typologies, structuring patterns, mule behavior, unusual flows
- **Recordkeeping:** audit trails for decisions, approvals, and administrative actions
- **Investigations:** case management, escalations, SAR or STR workflows (as applicable)

Travel Rule and recordkeeping, high-level considerations

Transfer rules and recordkeeping requirements differ by jurisdiction and can affect user experience, especially for withdrawals and transfers involving self-custody. Treat these obligations as product requirements, not back-office details, because they directly impact funnel conversion and support load.

RACI snapshot, who does what

Process	Institution owns	Provider supports
Asset and network allowlist	Governance, approvals, disclosures	Asset availability, technical constraints, network risk inputs
Customer onboarding	Clear separation, aligns with some governance models	KYC and KYB policy, risk tiering, communications
Monitoring and investigations	Case handling, filing decisions, audit responses	Monitoring outputs, logs, data exports, escalation support
Incident response	Customer comms, product decisions (pauses, limits)	Technical incident handling, restoration updates, root-cause inputs

How WhiteBIT approaches it

Industry challenge: Institutions need compliance processes that are audit-ready, not “best effort” dashboards.

What institutions should require: Clear workflows for KYB and KYC alignment, sanctions and monitoring outputs, recordkeeping, and data exports designed for audits.

WhiteBIT approach: WhiteBIT positions compliance posture and AML-oriented support as part of its institutional offering, alongside a relationship-led onboarding model designed to help regulated clients map responsibilities clearly.

PAYMENTS AND CORRIDORS, WHERE WHITEPAY FITS

For many institutions, crypto becomes real when it becomes money movement: merchant acceptance, treasury conversion, and payouts across borders. That is where acquiring and rails turn crypto into a product line, not a feature.

Merchant and PSP use cases

- **Accept crypto payments:** offer crypto as a payment method at checkout or invoice
- **Treasury conversion:** convert inflows under defined FX and settlement policies
- **Settlement choices:** settle into crypto, stable assets, or preferred balances depending on setup
- **Mass payouts:** creator payouts, affiliate payouts, rewards, and cross-border disbursements

Why corridors and payout options matter

Corridors shape adoption. The more predictable the path from “customer pays” to “merchant settles,” the easier it is to operationalize. Institutions should define which corridors are allowed, how counterparties are screened, and what settlement timing customers and merchants can expect.

Operational considerations

Payments introduce real-world messiness that must be designed in:

- **Refund handling:** define how refunds work and how FX is treated
- **Settlement timing:** define SLAs and handling for delayed or failed settlement
- **Rate transparency:** define how rates are set, when they are locked, and how spreads are disclosed
- **Reconciliation:** ensure finance receives clean, audit-ready exports

ECONOMICS AND KPIS, HOW LEADERS EVALUATE SUCCESS

The economics of a crypto product are easy to overestimate if you look only at trading fees. Leaders should evaluate a broader model that includes conversion, retention, operational cost, and risk outcomes.

Revenue drivers

- Conversion take rate for fiat to crypto and crypto to fiat
- Spread capture, with transparent disclosure and governance
- Payments economics, acquiring fees, settlement spreads, treasury conversion
- Premium tiers, higher limits, advanced features, priority support
- B2B pricing, bespoke commercial terms for corridors, payouts, and treasury

Cost drivers

- Compliance operations, investigations, staffing, audits
- Fraud and account takeover losses, plus prevention tooling
- Support burden, especially around withdrawals and verification
- Chain fees and network operations
- Vendor costs, minimums, and ongoing maintenance

KPI dashboard template

KPI	Definition	Why it matters
Activation rate	Percent of eligible users who complete onboarding and make first conversion	Measures funnel health and flags KYC or UX friction
Retention, 30 and 90 days	Users returning to convert, hold, transfer, or pay	Validates product fit and supports LTV modeling
Crypto balances held	Total customer crypto balances held, by asset	Signals adoption and informs custody and liquidity planning
Incident rate	Count of security or compliance incidents per month	Board-level risk signal and control maturity indicator
Reconciliation breaks	Count and severity of ledger mismatches	Core finance risk, should trend toward zero
Support burden	Tickets per 1,000 active users plus satisfaction proxy	Signals UX clarity and operational readiness

WhiteBIT emphasizes fair pricing positioning and customizable commercial models, which should be evaluated against your unit economics, SLAs, and operational requirements.

VENDOR EVALUATION CHECKLIST, QUESTIONS TO ASK IN PROCUREMENT AND SECURITY REVIEW

A CaaS vendor may look complete in a demo, but institutions should evaluate evidence, not claims. The goal is to answer three questions:

- Can this provider support your operating model and regulator expectations?
- Are responsibilities and incident paths crystal clear?
- Can you exit or change scope without being trapped?

Due diligence checklist

Area	Questions to ask	Evidence to request
Technical	Is the API mature? Is there a sandbox? How are breaking changes communicated? What logs and webhooks exist?	API docs plus changelog, sandbox access, uptime history, sample logs and webhooks
Security	What is the custody model? How are withdrawals governed? How is access controlled? What is the incident response process?	Security overview, withdrawal policy, RBAC model, incident runbook, audit or certification scope
Compliance	How do KYB and KYC workflows integrate? What monitoring outputs exist? What reporting exports support audits?	Workflow documentation, export formats, sample case fields, data retention and audit logging description
Commercial	What are fees and minimums? What are SLAs? What is the implementation timeline and post-launch support coverage?	MSA plus SLA, pricing schedule, implementation plan, named escalation path and support model

How WhiteBIT approaches it

Industry challenge: Procurement and security reviews often stall because vendors cannot produce audit-ready evidence quickly.

What institutions should require: Clear SLAs, defined custody controls, compliance workflow documentation, and a named escalation path for incidents and operational issues.

WhiteBIT approach: WhiteBIT positions a comprehensive institutional suite across CaaS, custody, and payments, with a relationship-led model intended to reduce procurement friction when paired with clear evidence, documentation, and implementation planning.