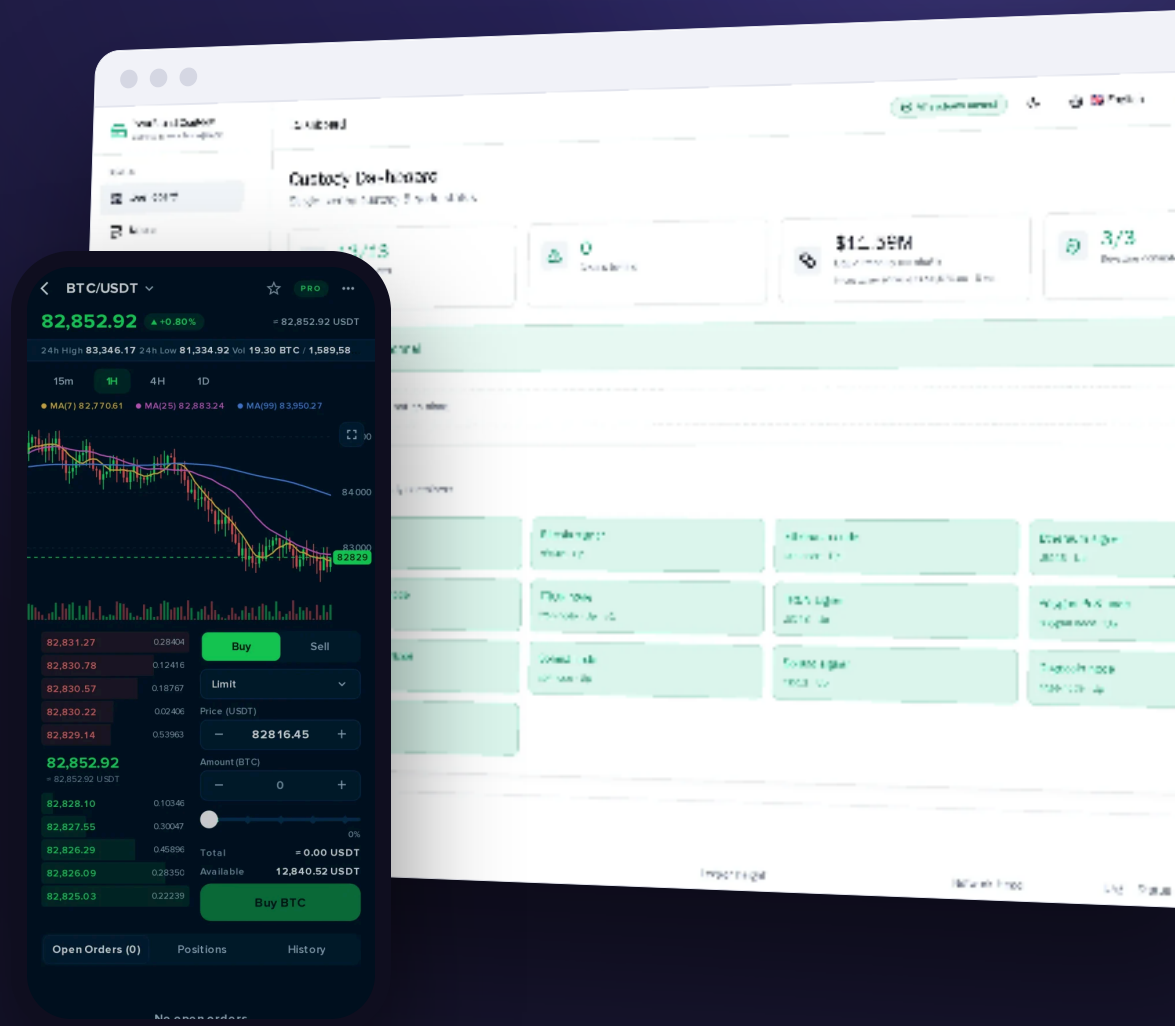
TECHNICAL OVERVIEW

How the platform is built, secured and run.

Architecture, liquidity, custody, TRON energy, RPC, security, wallet and mobile apps, monitoring and delivery of the BitPolaris software, with the numbers we measured running the reference exchange in production.

November 2026 · bitpolaris.com



CONTENTS

What this document covers.

01 Architecture and deployment

02 Exchange core and liquidity engine

03 Reference prices

04 Custody and treasury

05 TRON energy

06 RPC gateway and costs

07 Security and identity

08 Operations console and compliance

09 Payments

10 Wallet app

11 Exchange mobile app

12 Monitoring and Proof of Reserves

13 Engineering notes

14 Live demos and product films

15 Delivery, releases and migrations

01 · ARCHITECTURE

Five layers, cleanly separated.

CLIENTS	Web exchange · Easy + Pro	iOS · Android apps	Desktop wallet · macOS, Windows	Merchant checkout	REST · WebSocket API		
EDGE	Cloudflare WAF, bot and DDoS protection	TLS termination	Rate limits per user and IP				
APPLICATIONS	Exchange and terminal	Operations console (130+ screens)	Wallet back office	Payments + merchant panel	Custody console		
CORE SERVICES	Identity, 2FA, KYC orchestration	Matching engine and ledger	Liquidity mirror + hedging	Payments API + signed webhooks	Custody engine: scan, sweep, sign	RPC gateway	Price oracle
DATA AND CHAINS	MySQL · PostgreSQL	Redis · InfluxDB	RabbitMQ	Vault for secrets	Bridges for 9 chains		

Signing keys live apart from the applications. Chain bridges and signers are reachable only from inside the deployment; web and API traffic passes Cloudflare first.

Same software, three operating models.

Every component runs in containers. Cloud installs run on our infrastructure under the client's brand; self-hosted and source installs run inside the client's perimeter.

DESIGN

Isolation

Exchange, wallet, payments and custody run as separate services with separate databases. Signing keys live in the custody layer only, never in web-facing services.

WHERE

Infrastructure

Dedicated servers (EU) or the client's cloud account, for example AWS in Frankfurt, Bahrain or Singapore with KMS-backed secrets. HSM support (Thales Luna, YubiHSM) scoped per deployment.

CONTINUITY

Backups and recovery

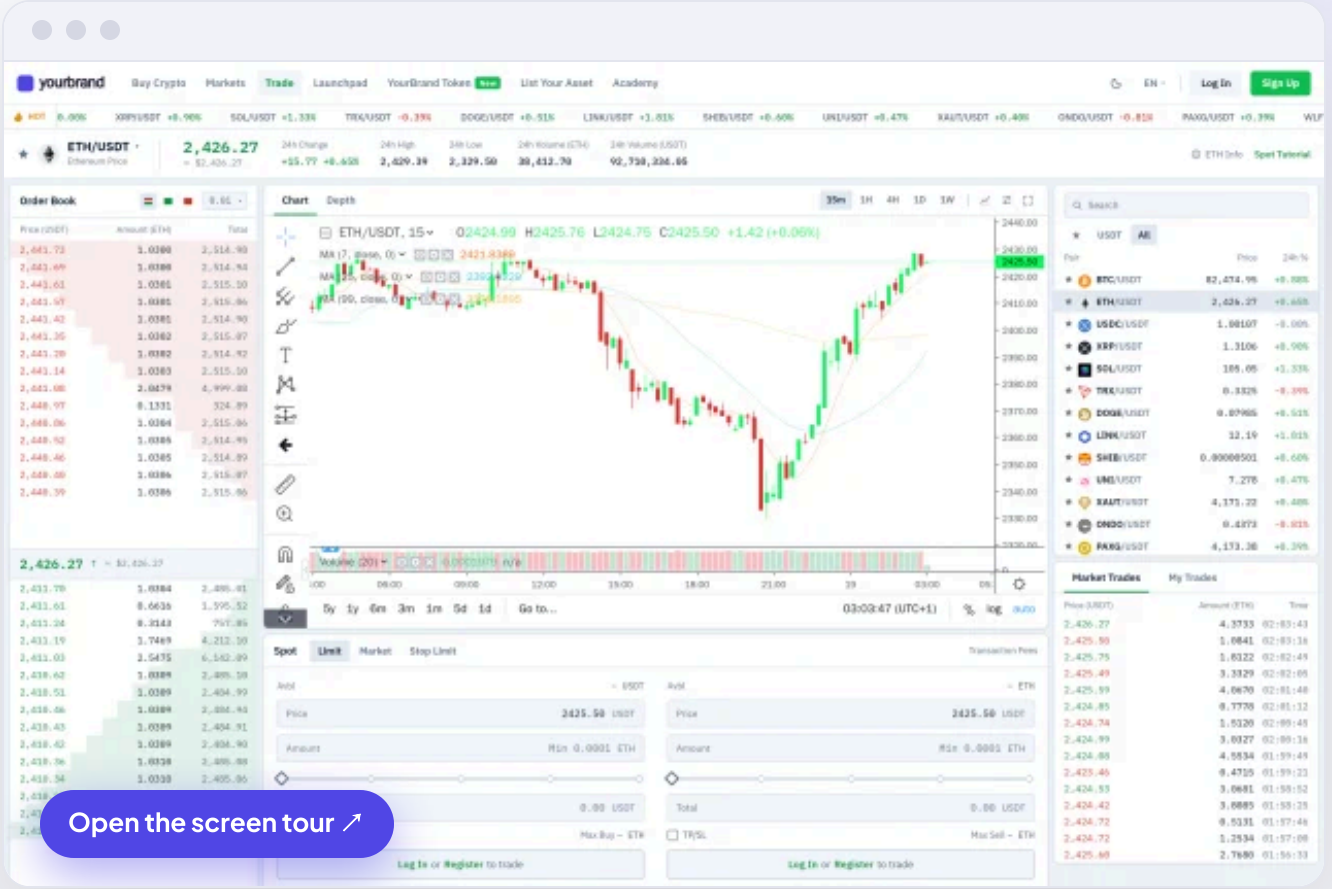
Encrypted backups sent off-site every night, restore drills with a written record, documented recovery runbooks. The restore drill record is part of the technical file.

STACK	Ruby on Rails and Go on the trading path · TypeScript, React, Next.js, React Native · Python · Rust on the desktop · MySQL, PostgreSQL, Redis, InfluxDB, RabbitMQ, Vault · Docker, Traefik
ACCESS	Self-hosted: no standing access for us; support sessions use time-limited credentials the client issues and can revoke

02 · EXCHANGE CORE

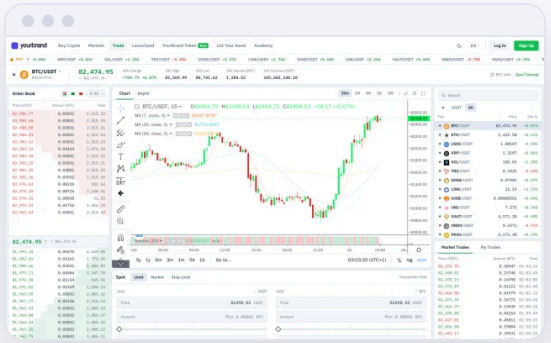
Orders, ledger, market data.

- Matching engine in Go: an in-memory order book per side, price then time priority, trades at the maker's price
- Limit, market, post-only (rejected if it would cross) and fill-or-kill (checked before matching); balances locked before an order reaches the book
- Every trade, fee and transfer posted to a double-entry ledger: assets, liabilities (main and locked), revenue, expense
- Fees resolved by user group and market; per-user order rate limits; live book, trades and balances over WebSocket
- Easy Trade for first-time buyers and the Pro terminal, on the same liquidity

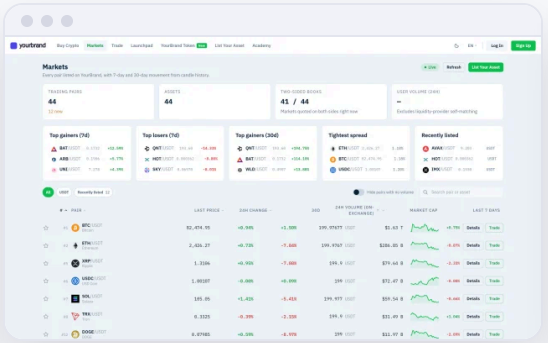


More: bitpolaris.com/products/exchange ↗

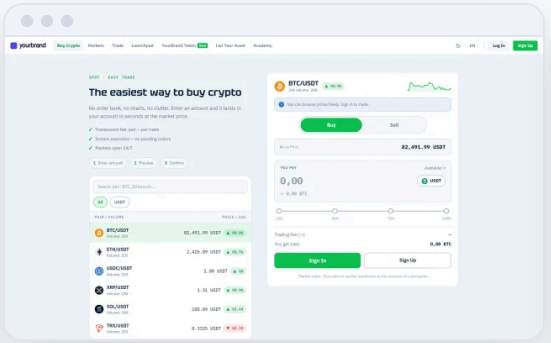
What your customers use.



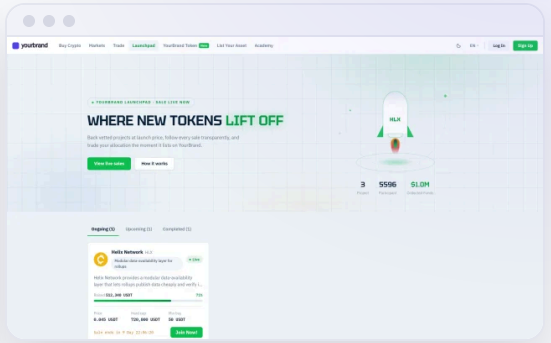
Trading terminal book, chart, order form



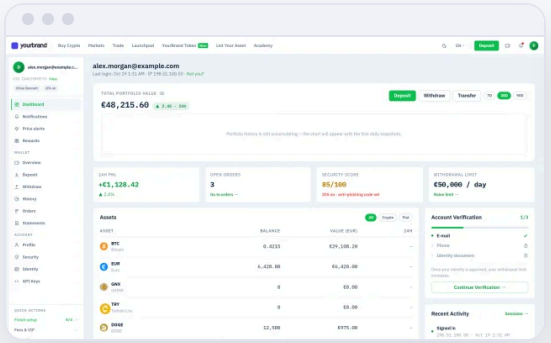
Markets every pair, 24-hour change



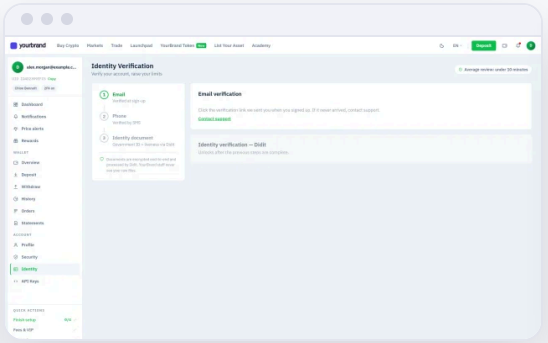
Easy Trade buy in a few taps



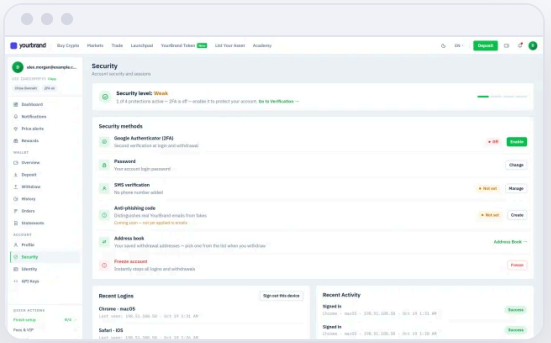
Launchpad token sales



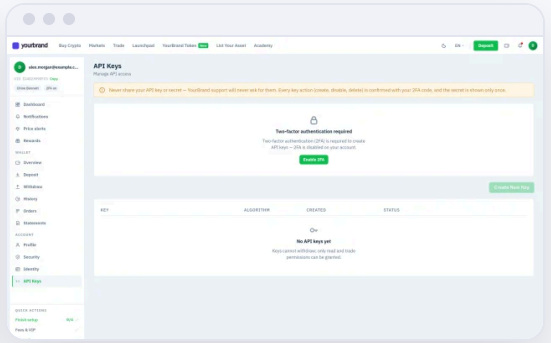
Account balances and activity



Verification KYC tiers in the app



Security 2FA, devices, sessions



API keys for algorithmic traders

02 · LIQUIDITY

A full book on day one, with far less prefunding.

The mirror engine builds each book from a reference venue's live depth with a markup and starts a hedge for every fill at once.

Deposit
a buffer stays hot; the excess goes to the hedging venue

→

Trade
the customer fills against the mirrored book

→

Hedge
the opposite order is placed on the venue immediately

→

Withdraw
exactly the amount needed is pulled back and paid out

PRICING

Cost floor

Per market: venue taker fee, transfer amortisation and a buffer. Below the floor a market is not quoted, and there is no override.

VISIBILITY

Open-exposure queue

Every fill not yet hedged is visible with age, attempts and reason. Fills awaiting funding are tracked, aged and alerted until hedged.

LIMITS

Exposure breaker

Above the exposure cap every book is pulled until measured exposure clears; exposure is measured before the first quote.

CONTROL

Gates and panic control

Replenishment sits behind four independent gates and daily USD caps. One button pulls all books; position tracking stays on.

How the mirrored book is built and watched.

QUOTING

Every 15 seconds

Each market reads a 100-level source book, splits it into price bands and quotes the VWAP of each band, up to 20 levels a side. Orders are replaced only when price moves 0.05% or size 25%. A source older than 120 s pulls that market.

PRICING

A floor, not a hope

Floor = venue taker fee + transfer amortisation + safety buffer, per market; an unknown fee is never treated as zero. Below the floor the market stops quoting and the API refuses the setting.

HEDGE

Idempotent hedge orders

Each fill is copied on the venue with a client order ID derived from the trade, after a slippage check on the venue book. It reconciles before any retry; after three attempts it stays as open exposure with a critical alert.

PRODUCTION

Measured

1,596 resting orders across the mirrored markets, up to 20 levels a side (12 October 2026). Realised margin is measured per trade, after venue fee and slippage.

VENUES

Scoped venue keys

Venue API keys sit in an AES-256-GCM vault with read and trade scope; withdrawal is a separate per-key permission behind four gates. Eight venue adapters; production hedging on Binance.

VISIBILITY

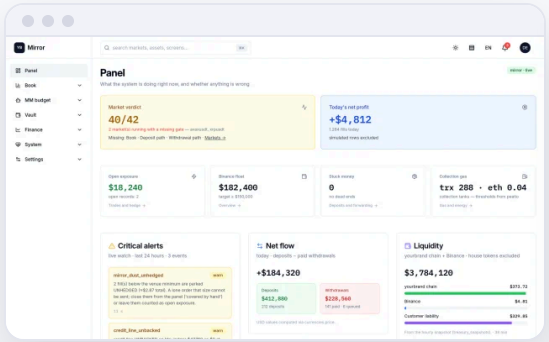
13 reasons, never silence

When a market is not quoting the console says why: below floor, balance starved or unreadable, one-sided, exposure halt, emergency pull and more. Unknown values are never shown as zero.

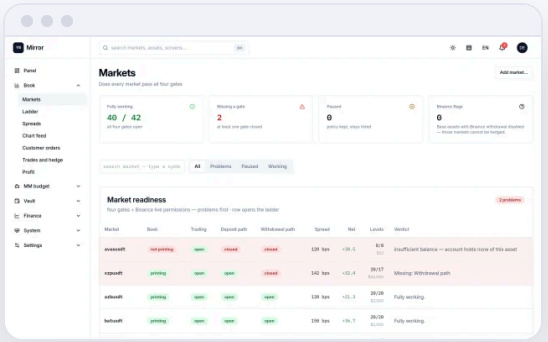
MIRROR CONSOLE

Status · Alerts · Treasury · Deposits · Withdrawals · Gas · Reconciliation · Markets · Ladder · Orders · Trades + hedge · Profit · Spreads · Inventory · Funding · Floor · Ledger · Audit · Logs · Engine · Keys · Telegram

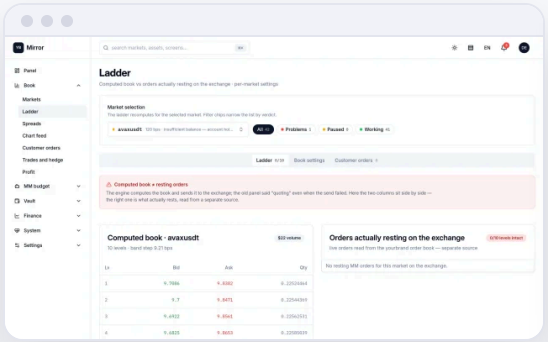
The liquidity engine, fully observable.



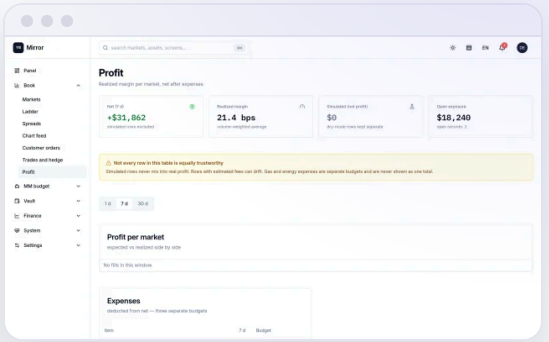
Status panel verdicts, profit, exposure



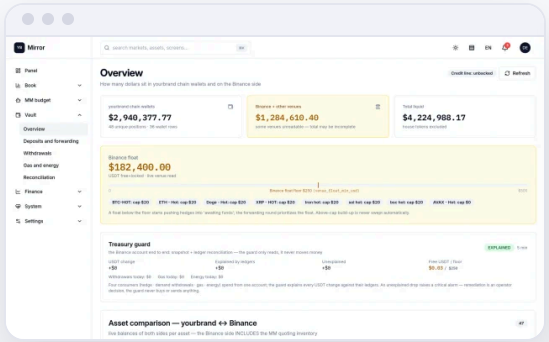
Markets quoting status per market



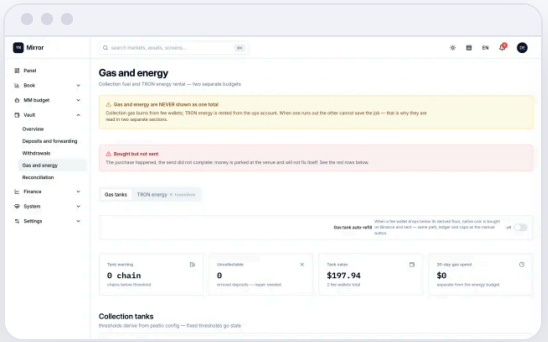
Ladder target book level by level



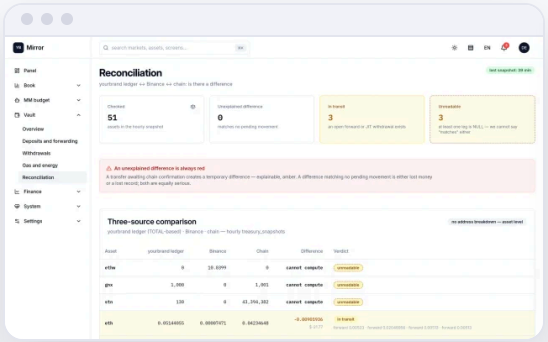
Profit realised markup in bps and USD



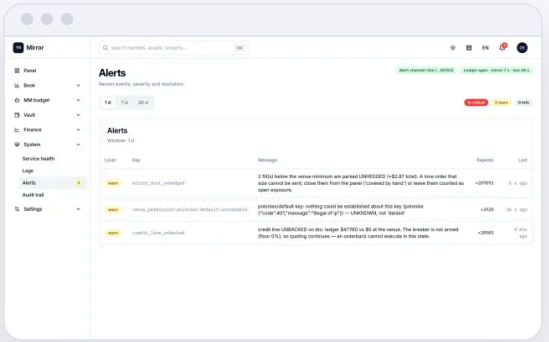
Treasury wallets and venues



Gas station collection gas and TRON energy



Reconciliation ledger against the chain



Alerts persistent log, repeats recorded

Hot-wallet balances are kept deliberately small.

The exchange keeps only a working buffer in each hot wallet. Deposits above it go to the hedging venue; a withdrawal the hot wallet cannot pay is funded from the venue on demand.

Skipped
the ledger skips a withdrawal it cannot fund and records the shortfall per currency

→

Gated
four independent gates must all be open; the destination is re-read just before the call

→

Pulled
exactly the shortfall moves from the venue to the hot address

→

Paid
the original withdrawal is processed again, with no human step

GATES

Four gates

The demand flag, engine in live mode, the venue key's own withdrawal flag, and the asset armed with address, network, buffer, minimum and a daily USD cap. A missing USD price means refuse.

FAILURE

Cooldowns that expire

Per asset 300 s, doubling up to an hour; a venue-wide pause after repeated failures. None become permanent, and an operator re-arm clears them. Raising the cap for one UTC day requires a written reason.

PRODUCTION

Measured

An ETH withdrawal the hot wallet could not cover was funded from the venue and paid within one replenishment cycle, fully automatically. Every transfer leg is matched at both ends; an unmatched leg raises one alarm.

An hourly three-way snapshot compares ledger, venue and chain, and classes every difference as reconciled, in transit, unexplained or unreadable.

One broken source cannot move the price.

Every 15 minutes the oracle asks seven keyless crypto sources (six exchanges and one aggregator) and three fiat sources, with our own order book as a cross-check only. For BTC all seven answer, typically within about 0.1%.

1

Median

A median limits the influence of a single broken source; an average or a two-source rule cannot tell which one is wrong.

2

Outliers out

Any quote more than 2% from the median is dropped and the median recomputed. Each source's distance is its health signal.

3

Enough sources

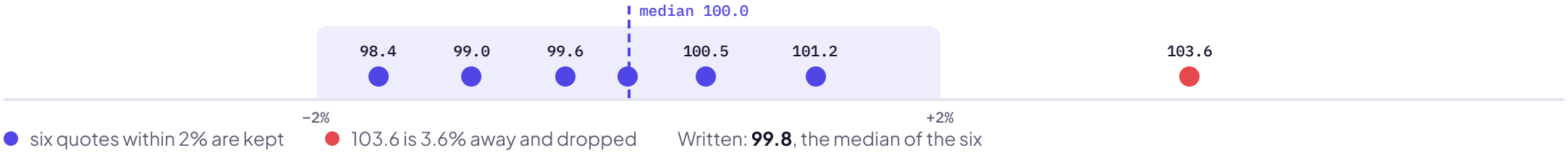
Three or more surviving quotes, or exactly two that agree within 2%. A single source writes nothing.

4

Deviation brake

A move of more than 15% against the last written price is held back. Arithmetic stays in exact decimals end to end.

ILLUSTRATION · SEVEN QUOTES FOR ONE ASSET



Every brake needs a release.

The reference price drives USD withdrawal limits and the hot, warm and cold sweep thresholds. A wrong price is a money problem, not a display problem.

Fetch
one retry on a rate limit, server error or timeout before a source counts as down

→

Filter
median, 2% outlier band, per-source distance on the admin screen

→

Count
3+ sources, or exactly two that agree; one source blocks

→

Brake
a move over 15% is held; release only on consistent evidence

→

Write
skipped if the change is under 0.5%; exact decimals; audit log

DESIGN

Thin markets

Some assets trade on only three venues, so exactly two sources that agree within 2% are accepted. A single source, or two that disagree, never write a price.

DESIGN

Automatic release

A held price releases itself after 4 consecutive runs (about an hour), all in the same direction and within 5% of each other. Stale history releases nothing, and every release is audited.

CONTROL

Policy per currency

Each currency follows the median, prefers an official source (the ECB for EUR, the central bank for TRY), is pinned (a stablecoin at 1) or takes a manual price with a written reason.

Seen, confirmed, credited, swept.

Scan
a bridge per chain reads each new block for the platform's addresses

→

Confirm
credited at a confirmation depth set per asset and chain

→

Credit
posted to the ledger; the customer sees the depth on the deposit screen

→

Collect
token deposits move to the hot wallet, paid from watched gas tanks

PER CHAIN

Bridges that restart safely

Each bridge scans, credits, builds and broadcasts withdrawals, and reports health. Bridges run under systemd with restart-loop protection.

VISIBILITY

Every state has an age alarm

Deposits below the minimum are shown, not dropped. Accepted for 6 hours or processing for 30 minutes is a warning; processing for 2 hours is critical.

MEASURED

Finality, measured

On TRON the distance from chain head to the last solidified block held at 18 blocks, so exchange confirmations went from 50 to 30 and deposits from about 150 to about 90 seconds.

Gas-tank thresholds are derived from each chain's own fee parameters. When a tank runs dry, collection does not stop silently: it raises an alert.

Money moves only through deliberate, audited steps.

REQUEST	User, merchant or API request	USD limits per verification level, 24 hours and monthly	Travel Rule fields on exchange withdrawals
APPROVAL	New address activated by an e-mailed PIN, then 2FA	Automatic only below a limit; above it an operator approves	One panic switch sends everything to manual approval
SIGNING	The chain bridge signs; keys encrypted at rest, HSM on request	EVM: one lock per sending address, nonce never goes backwards	Hot wallet kept short; shortfall funded from the venue
PROOF	An uncertain outcome never creates a second payment; the chain is checked first	Paid only when the chain confirms	Unknown outcome stops the next step

NO DOUBLE PAY

TRON broadcast reconciliation

The transaction ID is known before broadcast. On any error the bridge checks the chain three times, re-broadcasts the same bytes once and treats a duplicate as success.

AUTOMATION

Four gates before anything moves by itself

Automatic replenishment and sweeps need an environment switch, live mode, a per-key flag and a per-asset policy row, plus a daily USD cap and a justified record.

One bridge per chain, each with its own scanner.

Upstream calls go through the RPC gateway; an optional full node can be used first.

CHAIN	MODEL	HOW DEPOSITS ARE FOUND
Bitcoin · Litecoin	UTXO	wallet history through Electrum, refused while the server is not synced; wallet material restored from the secrets vault at start-up
Ethereum · BNB Chain · Avalanche	EVM	block by block; receipts fetched only for our own token contracts and addresses
TRON	account · energy	up to 20 blocks per call, head cached 30 s; token transfers read from transaction info
Solana	account	finalized slots; the scanner never passes the slot the address poller has fully covered
XRP Ledger	account · tags	validated ledgers; one hot address with a destination tag per customer
Dogecoin	UTXO	new transactions since the last block; a pruned block returns a named error, never an empty one

TRON solidified guard

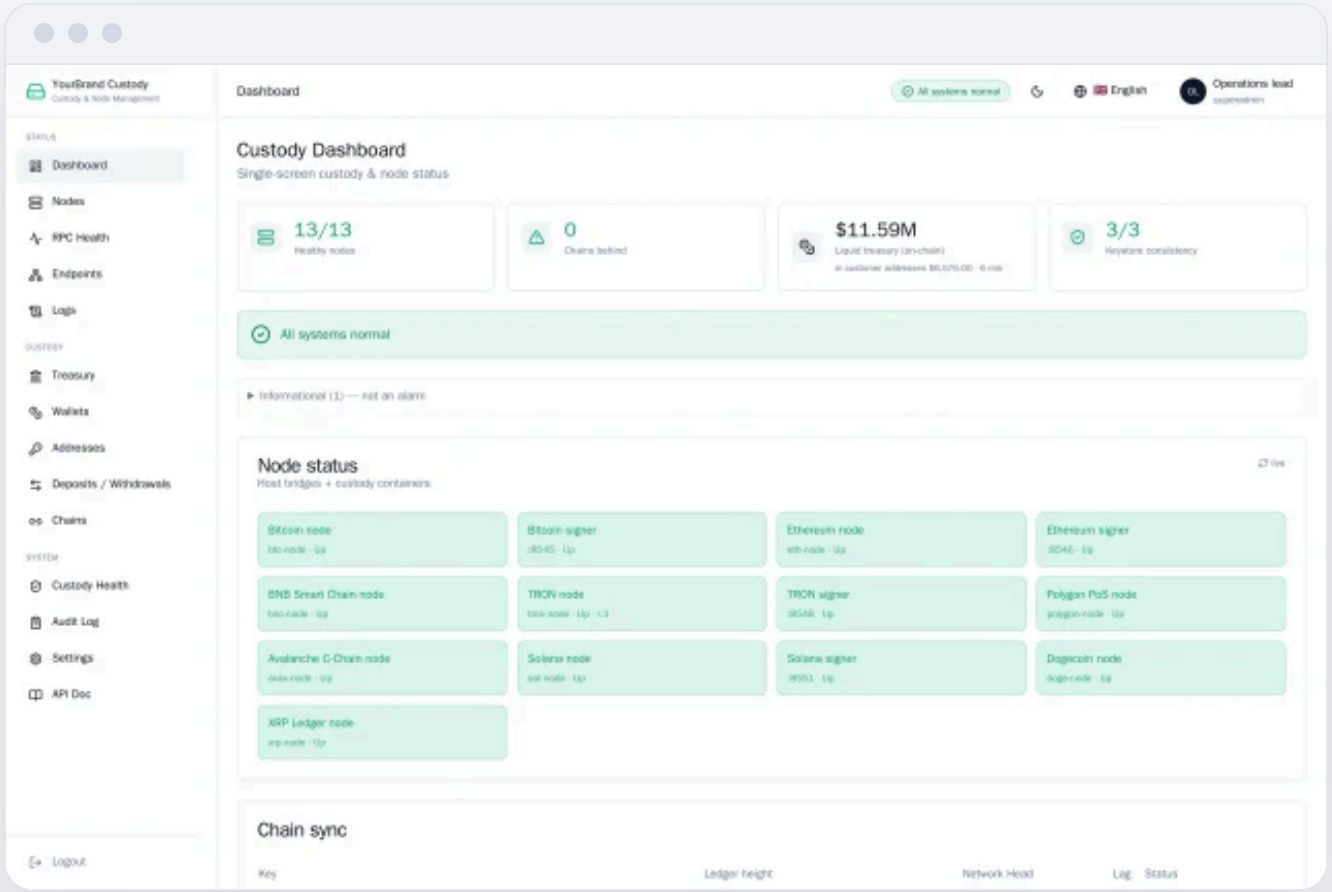
The gap between head and last solidified block alarms at 25 blocks (warning) and 60 (critical), so a reversible block is never credited when solidification stalls.

Keys that cannot be overwritten

Each deposit address gets its own key, encrypted and written exclusively with owner-only permissions, so a funded key can never be overwritten.

Never a fake empty block

A skipped Solana slot counts as empty only if all five endpoints omit it; otherwise the scanner retries. Pruned and missing blocks are errors, not gaps.

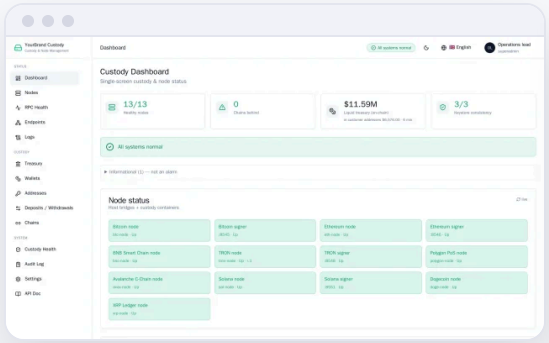


04 · CUSTODY: THE OFFICER PANEL

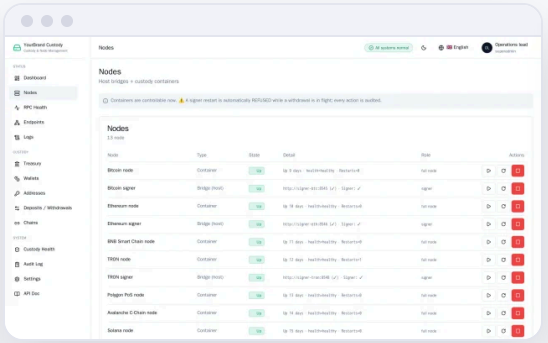
A console that cannot move money.

- By design it cannot withdraw, generate addresses or rotate keys: a deliberate boundary that shrinks the attack surface
- No session without a TOTP code verified against the secrets vault, and no remember-this-device
- Node start, restart and stop are audited; a restart is refused while a withdrawal is in flight
- Treasury: custody wallets and deposit addresses measured on-chain, venue balances read from the venue
- Keystore consistency: signing addresses compared with keystore files by existence only, without reading a key

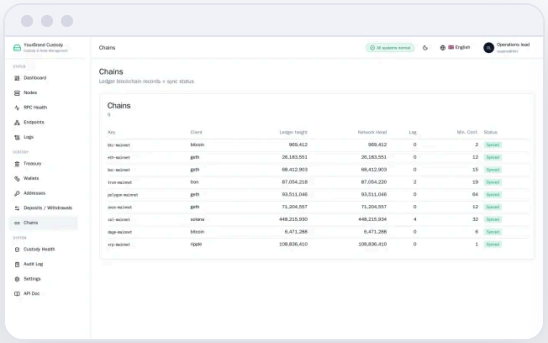
Nodes, chains, endpoints and treasury.



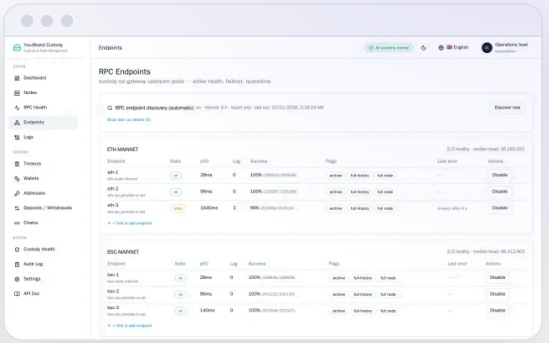
Dashboard health of every chain at a glance



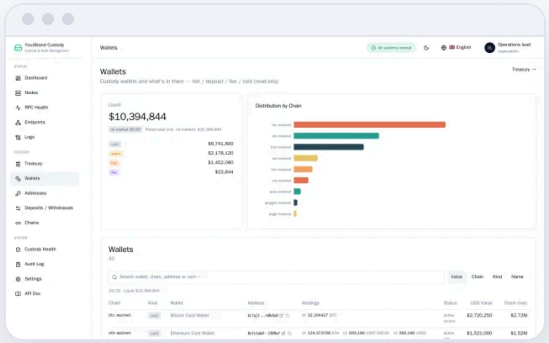
Nodes audited start, restart, stop



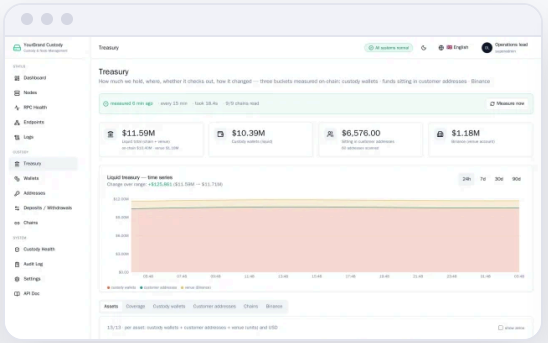
Chains scanner height against the chain



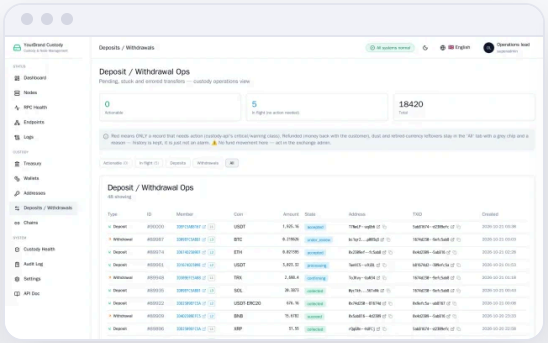
RPC endpoints pools, failover, quarantine



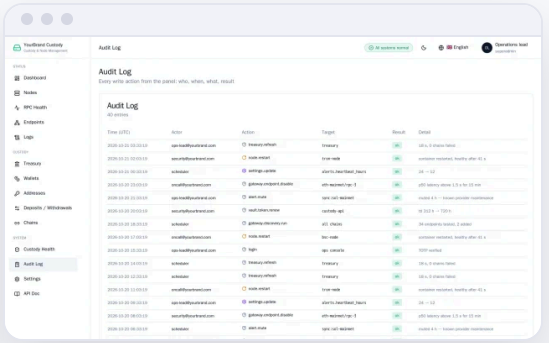
Wallets hot, fee and deposit wallets



Treasury balances measured on-chain



Transfers deposits and withdrawals



Audit log every action recorded

Unmeasured is not the same as fine.

A separate, read-only watchdog asks the chain about every movement the database calls done, so a record that says 'moved' is never taken on trust.

STRANDED	balances left on addresses the database calls collected, read in one Multicall
MISSING	transactions that should be on chain; 'missing' needs three independent negatives and honest-RPC checks
DELIVERY	custody alerts confirmed as delivered to a person
STUCK	deposits and withdrawals in processing: warning at 30 minutes, critical at 2 hours
BLIND	no successful measurement for 2 hours is a warning, 6 hours is critical

OK
the claim and the chain agree

MISMATCH
they disagree: a finding with evidence

UNKNOWN
the check could not run: raised, never counted as fine

Read-only by construction: fixed SQL templates over a seven-table allowlist, allowlisted RPC methods within a budget of 25 calls a run, and no ability to move money, write data or restart anything. Exceptions need chain evidence that is re-checked every round.

05 · TRON ENERGY

The recipient sets the price of a USDT transfer.

Priced from on-chain receipts on 16 October 2026: energy 100 sun per unit, bandwidth 1,000 sun per byte, TRX at $0.3353.

WHAT	RESOURCE	TRX	USD
USDT transfer to an address that already holds USDT	64,285 energy	6.43	$2.16
USDT transfer to an address with zero USDT	130,285 energy	13.03	$4.37
First TRX sent to a new address (activation)		1.1	$0.37
Bandwidth of one USDT transfer	345 bytes	0	free daily allowance

Why it doubles

The USDT contract stores each balance in a slot, and writing a zero slot costs more. 49,635 of the 64,285 energy is TRON's dynamic-energy surcharge on heavily used contracts.

Amount does not matter

1 USDT and 100,000 USDT cost the same energy. The sweep receipt reads 13,028,500 sun: all energy, with bandwidth from the free daily allowance.

Where it bites

Withdrawals to new customer wallets pay double and the fee must absorb it. Sweeps pay double only when the hot wallet sits at exactly zero USDT: that one you control.

One setting halves sweep cost; one limit prevents paid failures.

Unoptimised, the first deposit to a new address costs 14.13 TRX to collect. Two settings bring it to 7.53.

SETUP	HOT WALLET SENDS	BURNED	LEFT ON DEPOSIT ADDRESS	BURNED, USD
fee_limit 20, hot wallet at 0 USDT (before)	21.1	14.13	6.97	$4.74
fee_limit 20, hot wallet holds ≥ 1 USDT	21.1	7.53	13.57	$2.52
fee_limit 15, hot wallet at 0 USDT	16.1	14.13	1.97	$4.74
fee_limit 15, hot wallet holds ≥ 1 USDT (now)	16.1	7.53	8.57	$2.52

SWEEPS

The 1 USDT reserve

withdraw_reserve = 1 on TRC-20 USDT: the withdrawal job never takes the hot wallet below one USDT, so the next sweep writes a non-zero slot. 6.6 TRX ($2.21) saved per sweep, for one unwithdrawable USDT. The same rule applies to every receiving address you own.

WITHDRAWALS

Sizing fee_limit

Above the limit a transfer fails OUT_OF_ENERGY and the energy used is still paid: a failed transfer costs the full limit and moves nothing. 15 TRX, not 10, because a zero-balance withdrawal needs 13.03. At 15 a double-rate transfer clears up to about 115 sun per unit, a normal one up to 233.

Burn, rent or stake: volume decides.

WAY TO PAY	PER TRANSFER	CAPITAL	MAIN RISK
Burn	6.43 TRX ($2.16)	none	price set by governance
Rent (quotes)	1.9–3 TRX	prepaid balance with a provider	provider fails or reprices
Stake	0 TRX burned	6,703 TRX for one transfer a day	TRX price, 14 days to unstake

At low volume, burning with the reserve and a sized limit is enough. As volume grows, rent with burning as the automatic fallback; stake only TRX you would hold anyway. Rental figures are provider quotes.

10,000 TRANSFERS / MONTH (TRX)	NO RESERVE	RESERVE + BURN	RESERVE + RENT
Energy for 5,000 sweeps	65,143	32,143	9,395–14,835
Energy for 5,000 withdrawals	42,042	42,042	12,289–19,404
Activations and bandwidth	2,825	2,825	2,825
Total	**110,010**	**77,010**	**24,510–37,064**
In USD	≈ $36,900	≈ $25,800	≈ $8,200–12,400

Assumes 30% of withdrawals go to addresses that never held USDT. The same energy by staking would need about 2.6 million TRX locked (~$865,000): at this size most operators rent.

05 · TRON ENERGY

Renting energy without trusting the provider.

Energy rental is built into the liquidity engine's operations service. It pays the provider per order from a separate account and never sits in a withdrawal's path.

SIGNING

Verify before signing

The provider's payment transaction is built by a full node, then its raw bytes are decoded at protocol level: recipient, amount and owner must match before our key signs it.

KEYS

A separate payer

Orders are paid from a low-balance operations account, encrypted with AES-256-GCM. The hot wallet key is never used, and nothing is held by the provider.

SAFETY

Falls back to burning

Withdrawals never depend on this module. If it is unavailable, transfers simply burn TRX. Unreadable energy skips a round; three blind rounds raise an alert.

GUARDS

PRICE	unit price capped at 100 sun, the burn tariff: above it burning is cheaper
CAPS	50 TRX a day, a 15-minute cooldown, 131,000 energy for one hour per order
DEMAND	only token withdrawals count; native TRX transfers use bandwidth, not energy

MEASURED · 13 AUGUST 2026

131,000 energy for 8.81 TRX

At 67.25 sun per unit, against about 13 TRX to burn the same transfer: 32% cheaper. Automatic renewal is enabled per deployment once transfer volume justifies it.

Gas you can see before it runs out.

WATCH

Collection-gas alert

Per chain: can the fee wallet pay for the next sweep? Need = fee_limit × sweep legs; warning below 2.5×, critical below 1.1×, thresholds read from platform config. If the config cannot be read, a separate 'blind' alert fires.

VISIBILITY

Failed collections are never silent

A deposit that is credited but could not be collected is raised as critical on its own, so coins never sit unmoved without someone knowing.

PRICING

Fees that cover cost

A withdrawal to an empty address costs twice the energy of one to a funded address; the fee schedule is set from the real mix, not from the cheap case. On Ethereum, at a 0.5 gwei floor, a USDT transfer costs about $0.08.

HOT AND FEE WALLETS APART

The fee wallet that pays gas for collections is a separate account from the hot wallet that pays withdrawals, so customer withdrawals can never drain sweep gas. The deployment checklist enforces it.

TRC-20 COST AUDIT

For operators on any platform: last 30–90 days priced from on-chain receipts, funded vs empty recipients, fee limits and failed transactions, the cheapest burn, rent and stake mix. Your addresses only, never your keys.

06 · RPC GATEWAY

A load balancer that understands blockchains.

Scanners and signers never talk to nodes directly; the gateway scores every endpoint and routes each call.

Scoring

Success rate as a moving average (weight 0.3 for the newest result), latency against the pool median (up to −20 points), block-height staleness and an operator weight per endpoint.

Circuit breaker

Five consecutive failures, or a success average below 0.2, open the circuit for 30 s; three good probes close it. New endpoints pass 20 probes first. Rate limits back off 5 → 60 s.

Correct network

Chain ID verified for EVM endpoints, genesis hash for Solana. A proven wrong network is removed from all traffic, even as a last resort.

Errors inside HTTP 200

XRP Ledger reports tooBusy or noCurrent in a 200 body; some providers return quota errors the same way. Bodies are parsed per protocol, so these trigger failover.

No double send

A broadcast goes to one endpoint. It moves to another only when the transaction certainly never left: a connection failure before the body was sent, or an explicit 429/403.

Endpoints earn their place

Discovery runs every 6 hours; a new endpoint must return the same block ID as two healthy members 60 blocks below the head, and enters below reviewed ones. API keys are never logged.

CALLS PER MINUTE	ETHEREUM	SOLANA	TRON	XRP LEDGER	AVALANCHE	TOTAL
BEFORE	107	55	49	30	61	302
AFTER	20	12	4	31	62	**129**

RPC call volume cut by more than half.

The calls came from loops, not features: a balance job, block scanners and a safety poller. Each fix went out behind its own setting, with its own rollback.

58,953 VALUES VERIFIED

Balance job

One read per chain, address and currency, shared across rows, on a configurable interval. Verified in a shadow test of 1,000 scenarios × 3 rounds: 58,953 values identical to the old path.

49 → 4 CALLS A MINUTE

TRON head cache and range fetch

The head is cached up to 30 seconds; on a miss one call fetches up to 20 consecutive blocks, trusted only if the run is gap-free. In a 30-minute offline replay, upstream calls fell from 967 to 117 with no block skipped.

55 → 12 CALLS A MINUTE

Solana poller tied to the scanner

The bridge reports as finalized only the slot the poller has fully checked, so the scanner can never run ahead; the poller went from every 10 to every 60 seconds. Chaos test: 5 seeds × 400 rounds, 15% failing requests, lagging nodes, no signature missed.

CHANGE CONTROL

Safe rollout

Every change went out behind its own setting with its own rollback, one at a time, while deposit and withdrawal services stayed unchanged.

Call volume is driven mainly by chains, blocks and monitored addresses, so it is measured per chain and per job before any plan is sized.

Defence in layers.

LAYER	CONTROLS
Accounts	2FA for customers, required for withdrawals; TOTP on the custody and wallet consoles with step-up for risky actions; sessions and devices visible and revocable
Staff	Role-based access that starts from no access; every internal action recorded with the operator's identity; a written reason for every money movement
Transfers	New addresses activated by e-mailed PIN plus 2FA; automatic approval only below a limit; operator approval above it; a panic switch sends everything to manual
Keys and network	Keys apart from apps; chain bridges and signers reachable only from inside; Cloudflare WAF and DDoS protection at the edge; API keys and sensitive settings encrypted through the secrets vault
Reserves	An independent monitor reads balances on-chain and alerts on any mismatch; a check that cannot complete is reported as unknown, never as fine
Assurance	Architecture document, pen-test summaries and runbooks shared under NDA after the first call; HSM and on-site key ceremony when required

Keep the bots out, keep the record.

SIGN-UP

Verify first

No account row exists until the e-mail is confirmed; the pending sign-up waits 24 hours with a hashed password. The 6-digit code is stored hashed with per-code and daily attempt limits; a maintained list of disposable domains is refused.

ABUSE

Bot check that degrades by design

The web sign-up requires a Cloudflare Turnstile pass bound to the action and host. If Cloudflare itself is down, sign-ups fall back to a small, rate-limited allowance instead of opening or closing completely.

VERIFICATION

Two KYC providers

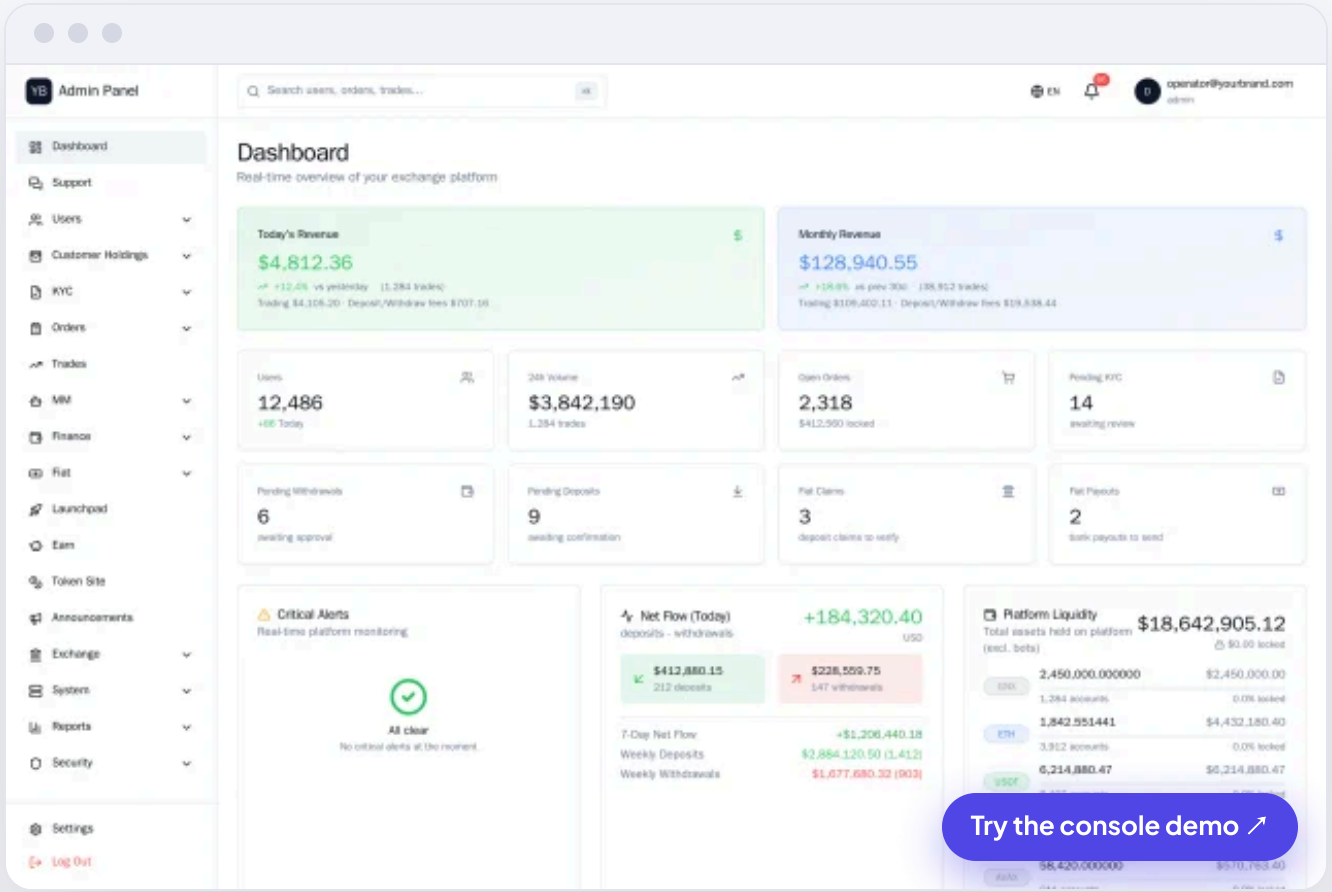
Sumsub and Didit, switchable from the panel; a user mid-verification stays with the same provider. Provider webhooks are HMAC-verified within a 300-second window.

SESSIONS

Changing the password or turning 2FA off ends every other session; a reset ends all of them. Reset requests always answer the same and are throttled; identity endpoints are rate-limited at the edge.

KYC ARCHIVE

Every decision is stored encrypted with AES-256-GCM. The data key is wrapped twice, by the secrets vault and by the operator's offline GPG key, so the archive survives the loss of either. A failed archive alerts the panel.



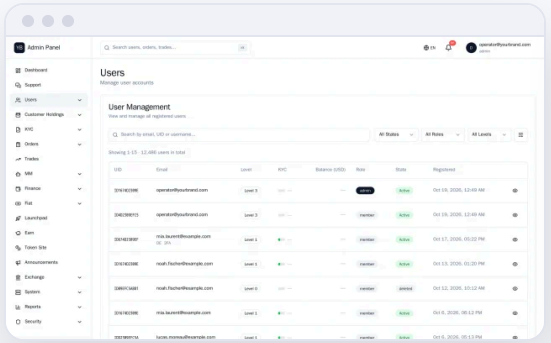
08 · OPERATIONS CONSOLE

Everything the team does, in one place.

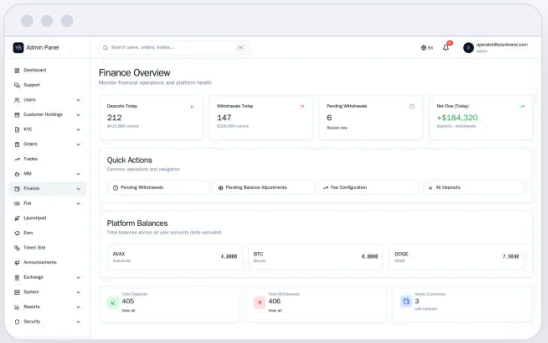
130+	5	2	100%
operator screens	consoles	KYC providers	money actions audited

- One exceptions list for every transfer that needs attention, so nothing waits unnoticed
- Balance adjustments carry a stated reason and the operator who made them
- System health: about fifty services, scanner heights against real chain heights, queue depths, database growth with a yearly capacity projection
- Roles start from no access; support sees customers and KYC read-only and no finance screens; a second approver can be required for balance adjustments

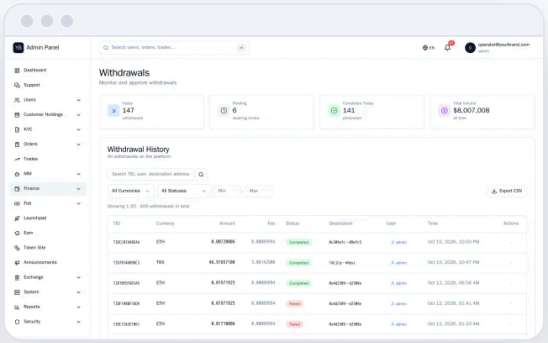
130+ operator screens. Eight of them.



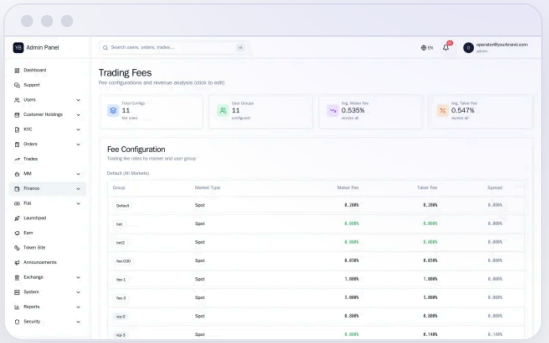
Users search, levels, labels



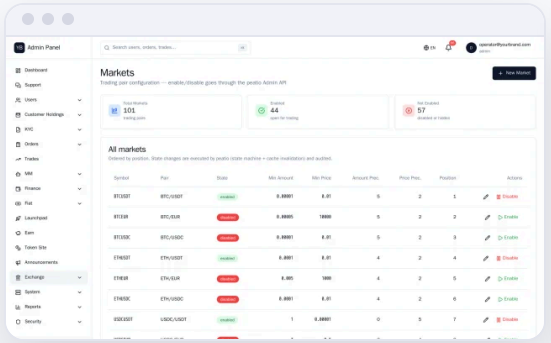
Finance assets, liabilities, revenue



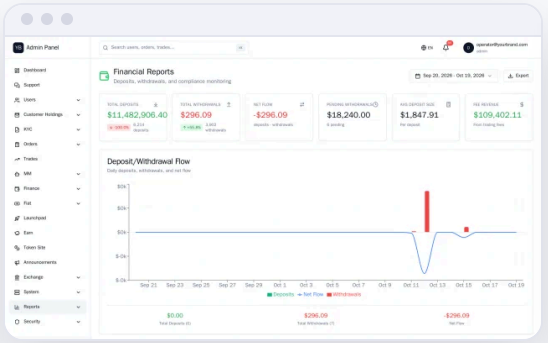
Withdrawals approve, reject, track



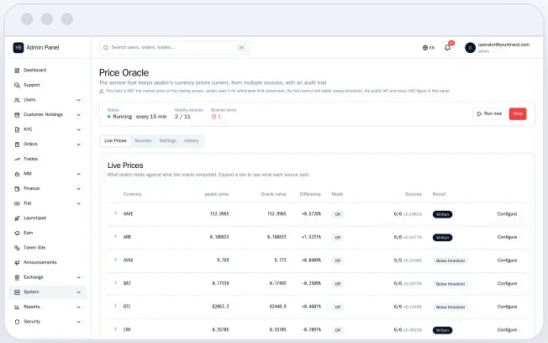
Fees per market and user group



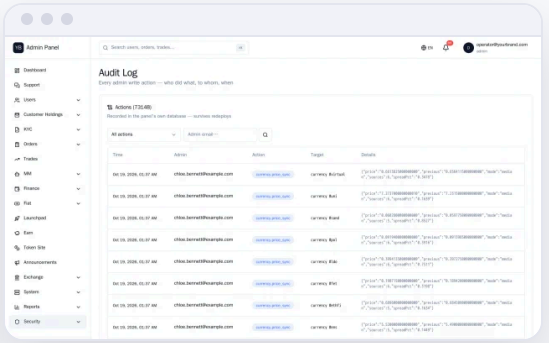
Markets precision, limits, status



Financial report from the ledger



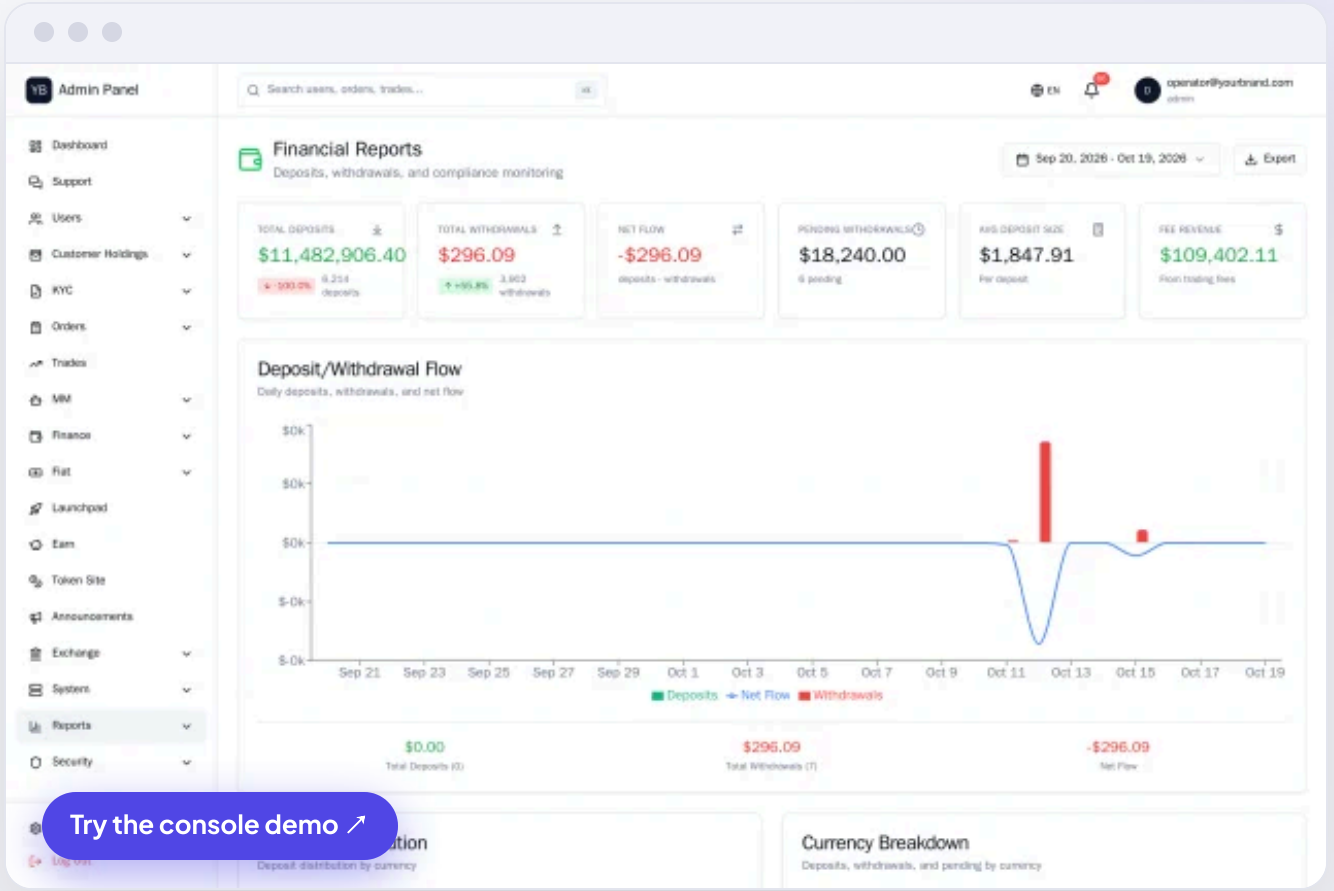
Price oracle sources and freshness



Audit log who, what, when

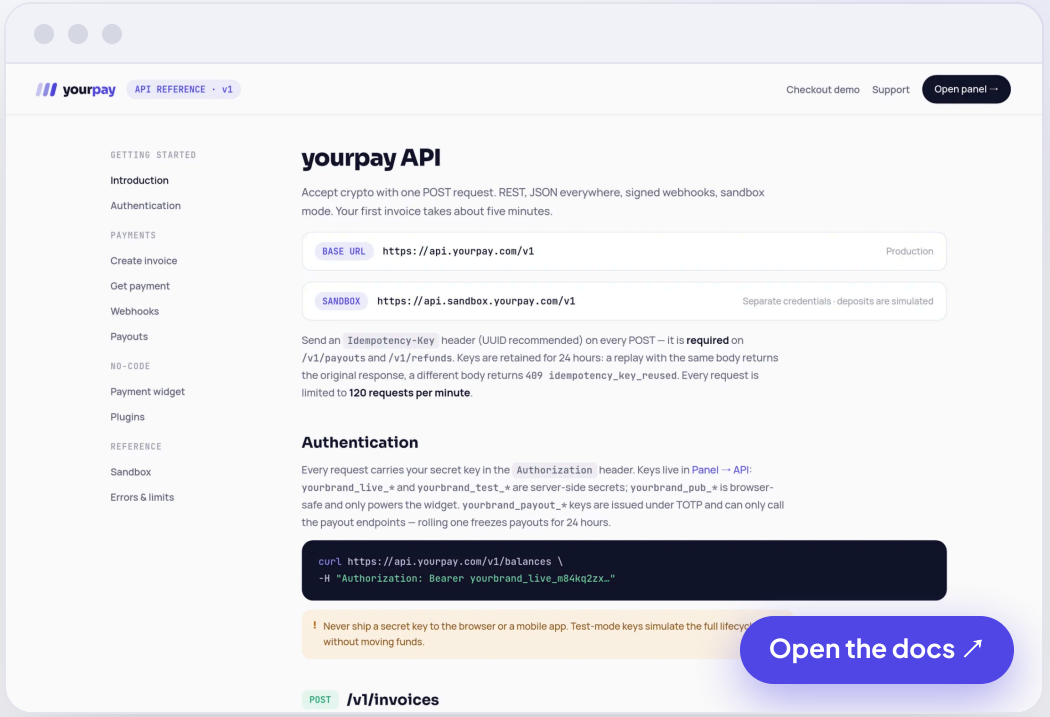
Evidence, not promises.

- Identity checks with Sumsub and Didit; decisions from either provider stay on record
- Country rules and tier limits edited in the console; every change versioned
- Travel Rule data captured on deposits and withdrawals, exportable for your provider
- Volume-split reports and market-making disclosure for market-integrity reviews
- Financial reports from a double-entry ledger: asset, liability, revenue, expense
- Technical file with control mappings for MiCA and DORA, VARA (Dubai), the Central Bank of Armenia or Türkiye's Capital Markets Board (SPK); a mapping, not a certification



Built for the merchant's developer.

ASSETS	USDT on TRON and Ethereum, USDC on Ethereum, TRX, ETH
INVOICES	a fresh address per invoice, a permanent address for repeat customers; rate locked for 15 to 120 minutes
WEBHOOKS	HMAC-SHA256 over timestamp and body, 300-second window, event ID; secrets encrypted at rest
DELIVERY	11 attempts over about 40 hours with back-off, then a dead-letter queue and audited replay
SAFETY	the target address is re-checked against internal networks at every delivery; rotated secrets overlap for 24 hours
KEYS	bearer keys stored hashed; idempotency keys kept 24 hours; a separate key for payouts



Never 'paid' before the chain proves it.

Detect
the custody scanner sees the payment and books it double-entry at once

→

Match
underpayment up to 0.5% accepted; overpayment up to 5% credited, more goes to suspense

→

Confirm
confirmation depth per network (TRON 19, Ethereum 12); a reorg is reversed

→

Settle
signed webhook; late or unconfirmed payments move to recovery handling

→

Pay out
only to an allowlisted address; 'broadcast' is not 'paid'

INVOICES

11 states, allowlisted moves
Every invoice moves through a state machine with allowed transitions only. Late payments, wrong assets and unknown addresses become orphans with a 72-hour recovery window; refunds go through a claim link.

PAYOUTS

Payout controls
A new payout address needs TOTP, an e-mail link and a 24-hour hold that cannot be shortened. Daily caps per merchant tier. Finance approval above set amounts, a second approver for the largest; approvals expire after 72 hours.

OPERATIONS

Honest status
No receipt within 60 minutes turns a payout into 'unknown', a critical alert a person resolves. A 38-point health check runs every 5 minutes and reconciliation every 10.

10 · WALLET APP

One wallet engine, five surfaces, no keys on the device.

SURFACES	iOS	Android	macOS	Windows	Web
MOBILE	React Native with Expo · New Architecture with Hermes	expo-router · Redux Toolkit; only session and preferences persisted, KYC data never	42 screens · 4 languages, every key translated		
DESKTOP	Tauri 2 (Rust) · React 19 · not Electron	178 engine files shared with mobile, locked by checksum			
BACKEND	Versioned API, so old builds keep working through store review	Custody, ledger, limits and signing server-side			

No keys on the phone

Address generation, signing, limits and the ledger live on the server: a compromised phone cannot sign alone, and a client bug cannot create money.

Money is never a float

Every amount is a decimal string with BigInt arithmetic, on every surface; floating point is banned from money code.

No blind resend

If a send's outcome is unknown, the app re-reads the transaction list at +1.5 s and +5 s instead of sending again.

Recoverable like any app, hard to steal from.

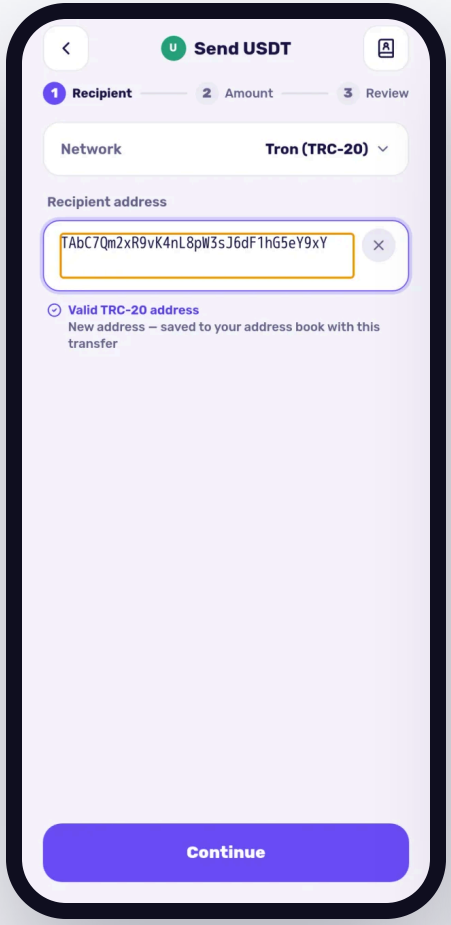
Custodial by design: the customers of an exchange, broker or payment company need 'forgot password' and support, not a seed phrase.

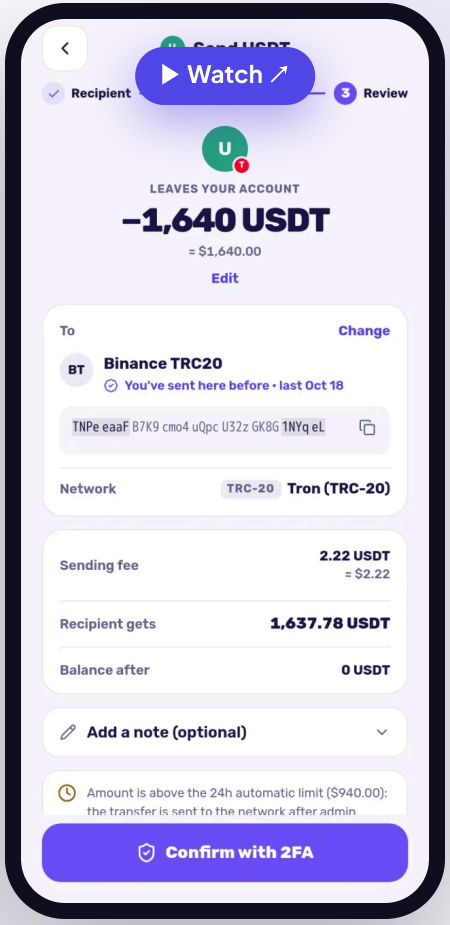
SIGN-UP	the account exists only after the e-mail link is clicked; disposable domains refused; sign-ups rate-limited per IP
RESET	answers the same whether or not the account exists; link valid one hour; success signs out every session and PIN device
HOLD	withdrawals held 24 hours after a password reset or after 2FA is switched on; receiving is never blocked
EDGE	per-IP rate limits on identity, sign-up, withdrawal and OTP endpoints
DELETE	in-app account deletion, blocked while funds or anything pending remain

PIN	6 digits, verified on the server; 5 wrong tries revoke the device; biometrics share the same attempt budget
IDLE	automatic sign-out after inactivity, tunable from the server; leaving the app brings back the lock
SEND	a TOTP code on every send; 2FA is required before a PIN device can be registered
LIMITS	sends within the daily limit are automatic; above it an operator approves
GUARDS	cold start fails closed; a lost session resets the whole navigation stack; late 401s from an old session are ignored

The send screen that says no.

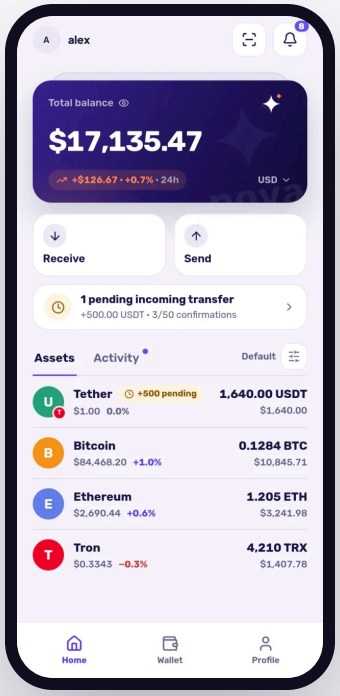
- Address format is checked per network: an Ethereum address in a TRON send shows 'This is an Ethereum (ERC-20) address' with a Change network button
- Lookalike check against saved, recent and own addresses: same length, same first and last four characters, different middle
- Payment links (BIP-21, EIP-681, tron:) never accept a token contract as the recipient; only allowlisted tokens; invisible characters stripped
- Desktop reads a paste twice, 250 ms apart, to catch clipboard swaps, and clears the clipboard after 60 seconds if it still holds our text
- Receive recommends the cheapest open network; the app says 'sending fee', not 'network fee'





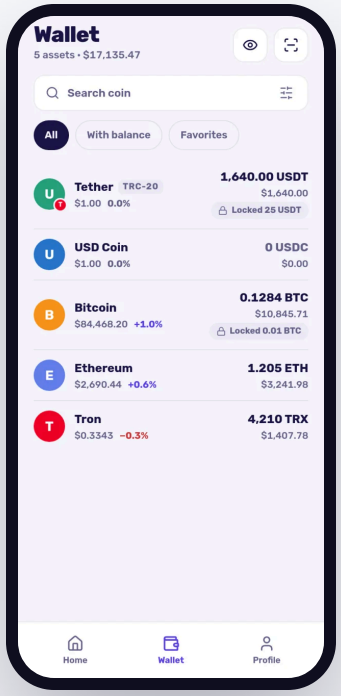
Screen by screen.

The wallet under a demo brand. Your colours, icon, name and languages replace it.



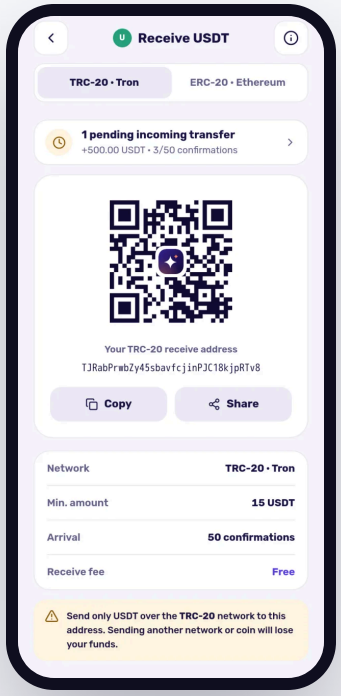
Home

Total balance, 24-hour change, quick actions



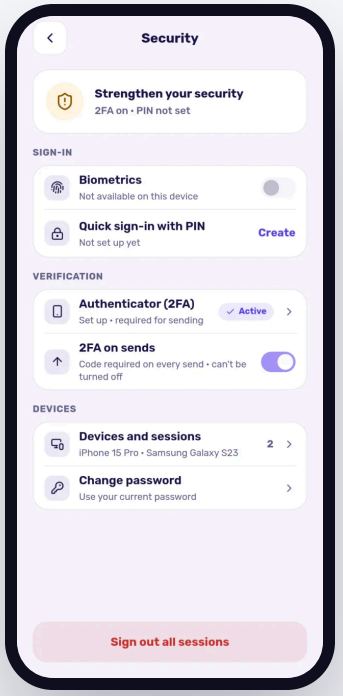
Assets

Every coin and network in one list



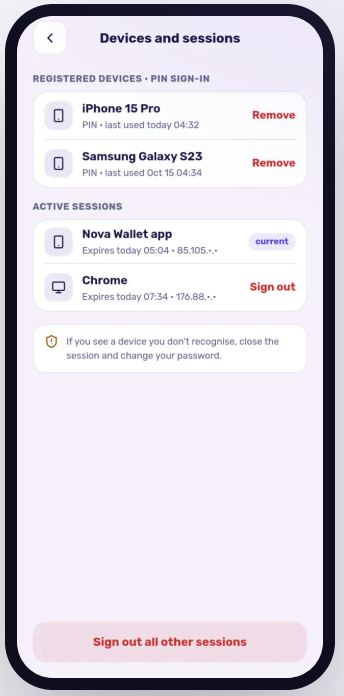
Receive

Network named on the address, QR, minimum and depth



Security

PIN, biometrics, 2FA on sends

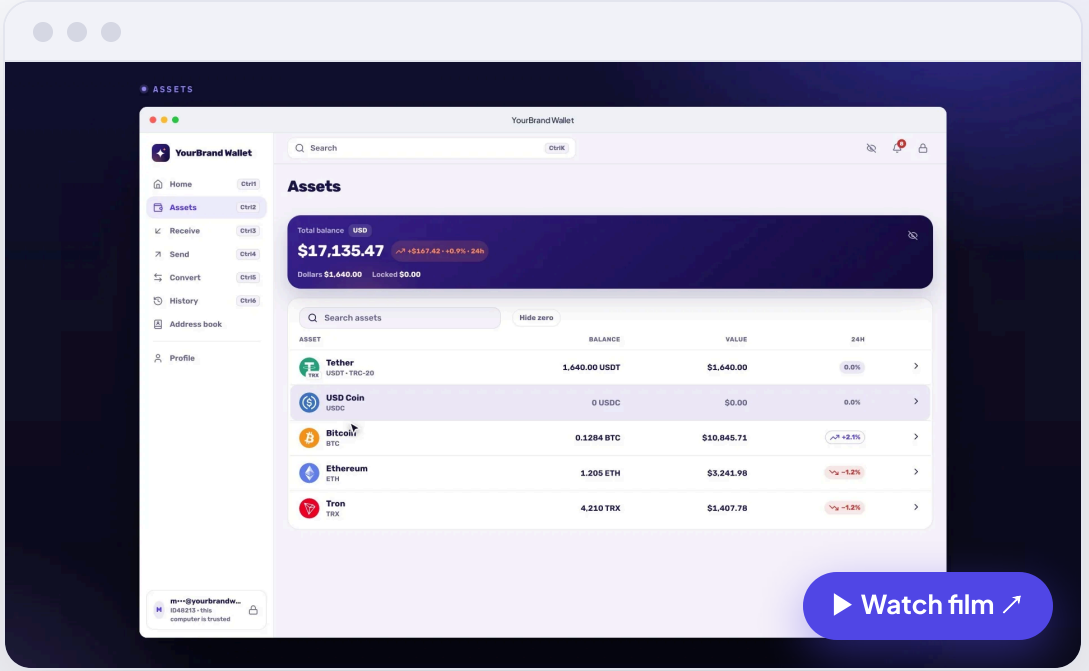


Devices

Sessions per device, remote sign-out

Small, fast, and the web view cannot reach the network.

- Tauri 2 in Rust with a React interface, not Electron. All networking runs in Rust behind a 35-rule allowlist; the web view has no network at all
- Secrets in the macOS Keychain or Windows Credential Manager; cookies in memory only; sensitive IPC commands limited to the main window
- 6-digit PIN, local vault wiped after 5 wrong tries; idle lock after 35 minutes; sleep or a clock jump locks at once; balances blur out of focus
- Tray mini-wallet that never calls the API; a command palette that understands '100 usdt send Alex'
- Signed auto-updates; macOS DMG notarised and stapled; Windows code signing in the client's name through Azure Artifact Signing



4.8 MB
Windows installer

796 ms
warm start, 2.5 s budget

517 + 50
TypeScript and Rust tests

10 · YOUR BRAND

One brand file builds every app.

Each client is one brand.yaml. The mobile app, desktop app, website, admin panel, e-mails and server configuration are generated from it.

BRAND PACK

What changes per client

Names, domains and support links; a 16 × 2 colour palette for light and dark, font, logos, icon and splash; app scheme, bundle IDs and packages; the secure-storage prefix. Raw colours in screens are banned, so nothing is missed.

STACK

Proven byte for byte

81 server files (60 e-mail templates, edge configs, app-link files) are rendered from templates; the reference exchange's output is identical to the original, 81 of 81. An unknown brand stops the build.

LEAK GUARD

No source-brand leakage

Automated tests fail on any trace of the reference brand in another brand's build; every screen of the demo brand is checked. Desktop builds stop if the config and the pack disagree.

THE CLIENT'S OWN ACCOUNTS

Apple and Google developer accounts, Cloudflare, e-mail, push, exchange API keys, Telegram, RPC providers and signing keys are opened in the client's name, so the client owns the apps and the infrastructure.

OVER-THE-AIR, MEASURED

JS-only fixes ship over the air on pinned runtime versions with one-command rollback. Every over-the-air release is verified against the update manifest before it counts as shipped.

From your brand to both stores.

Rebrand
brand file, icon, splash, store listing

→

Build in your accounts
certificates and profiles in your Apple and Google accounts; EAS profiles, build scripts and CI handed over

→

Review package
the one that passed for the reference exchange: listing in four languages, privacy labels, review notes and accounts, country lists

→

Release
over-the-air for JS-only changes, store releases for native ones, scheduled with your approval

Measured on the reference wallet
Approved on Google Play in under a day after the production submission, in 135 countries chosen by licence, not market size; review times depend on the store. Convert and Earn are compiled out of store builds, and the build fails closed if the switch is missing.

Review lessons
A dedicated store-review account is prepared with every release. Permissions are kept to the minimum and unused ones blocked explicitly. In-app account deletion meets Apple's rule 5.1.1(v).

Android 16 KB pages
The exchange app build targets SDK 36 with 16 KB page alignment, measured on the build: 36 of 36 native libraries aligned on arm64.

Quotes with limits, an admin with a matrix.

CONVERT ENGINE · REQUEST FOR QUOTE

A signed 15-second quote

PRICE	Binance order-book average plus a spread (60 bps, 20 for stablecoins); price under 5 s old and within ±5% of the oracle
BOOKING	one atomic internal transfer between user and treasury; nightly reconciliation
LIMITS	$1–2,000 per quote, $10,000 per user a day, $500 net exposure; 30 quotes and 10 accepts a minute per user
ROLLOUT	off → shadow → rehearsal → live; the panel can never go above the mode ceiling set on the server
HEDGE	an uncertain hedge order is queried, never resent

Convert is enabled per deployment where the licence allows; store builds include only licensed modules.

WALLET ADMIN

56 pages, 136 API routes

ROLES	owner, admin, finance, treasury, support, auditor; 25 permissions; 94 route rules, default deny, locked in a matrix file
LOGIN	session plus TOTP, step-up TOTP for risky actions; 5 wrong codes lock for 15 minutes
RECORDS	audit and login history append-only, enforced by database triggers; four-eyes rule on balance adjustments
SECRETS	the panel holds no vault token; stored secrets encrypted with AES-256-GCM and masked in errors
PAYOUTS	auto-approved only below a per-withdrawal limit; one panic switch sends everything to manual approval

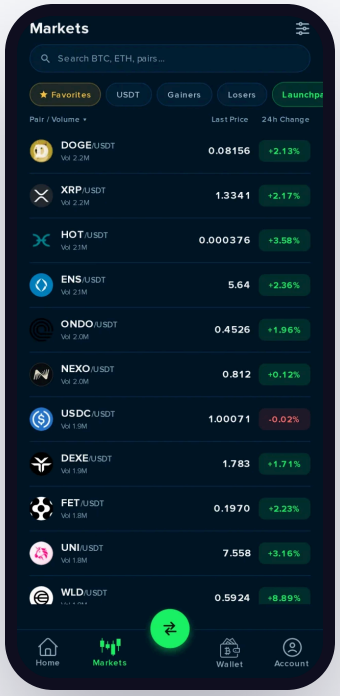
The whole exchange, one-handed.

- Four tabs (Home, Markets, Wallet, Account) and 48 screens; light, dark or follow the system, in your brand colours
- Candlestick chart with MA 7/25/99, live order book that reconnects on its own, order form and an advanced TradingView chart
- Limit and market orders on the same matching engine as the web; Convert as a market order with a 6-second rate lock
- Earn, Launchpad, internal transfers, fiat deposits with a reference code, support tickets with chat
- Deep links for confirmations and Launchpad projects; push for deposits, withdrawals, fills and security events

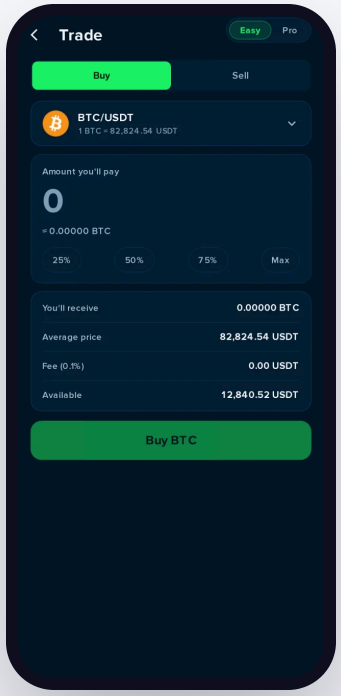


Screen by screen.

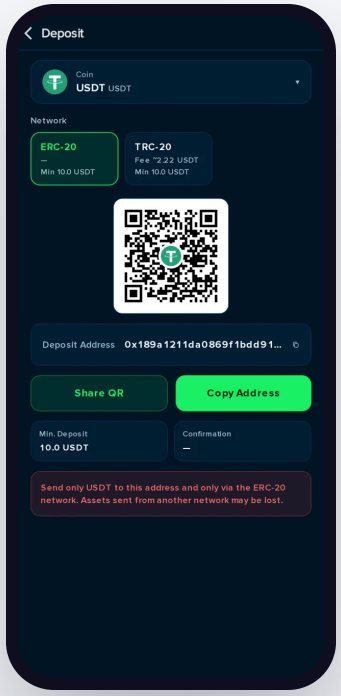
iOS and Android from one React Native codebase, under a demo brand.



Markets
filter chips, favourites, search



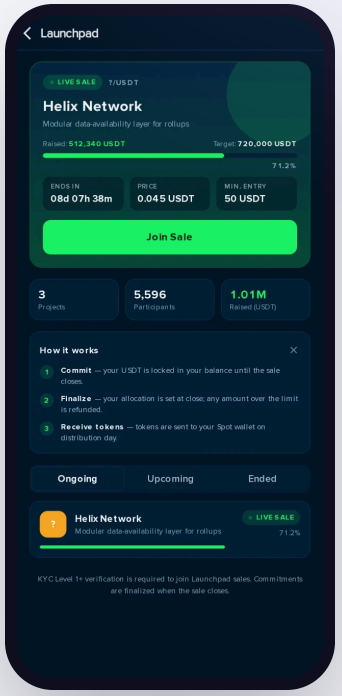
Easy Trade
buy in a few taps



Deposit
network named, QR, memo



Earn
flexible and locked products



Launchpad
live sales and progress

Built like the money app it is.

ARCHITECTURE

Stack

Expo SDK 58, React Native 0.88, React 19.3, Redux with sagas, React Navigation 7. Live data over public and private WebSockets. Three languages, 1,894 keys each.

SECURITY

Biometric sign-in

Biometric sign-in uses a keychain entry the OS invalidates when a new fingerprint or face is enrolled, bound to the account. Session tokens and the install ID live in Keychain or Keystore.

SECURITY

Withdrawals

Deposits and trading open at once; withdrawals need phone, identity and 2FA. A new address is activated with a 6-digit PIN sent by e-mail, then 2FA. 19 money and account routes are guarded.

MONEY FLOW

Memo and tag gate

XRP and other memo-based assets require a destination tag before a withdrawal can be sent, because an untagged transfer to an exchange may not be credited automatically. Tags in QR codes are parsed.

COMPLIANCE

KYC and Travel Rule

The KYC provider is chosen in the admin (Sumsub or Didit today); ID documents never pass through the platform's servers. Travel Rule fields with a list of destination exchanges.

OPERATIONS

Flags never block funds

Earn, Launchpad, Easy Trade, KYC and other modules switch from the panel. A failing flag service can never hide the exchange or block access to a user's money.

16 KB
page alignment, 36 of 36 native libraries

75
REST endpoints audited against the live server

191
automated app tests; a secret guard in CI

OTA
EAS channels, checked on every launch

Know before the customer does.

MONITORING

Alerts that mean something

A warning opens after 3 consecutive bad measurements, a critical after 2, and closes after 3 clean ones. A check that cannot measure freezes the counters instead of closing the incident.

RECONCILIATION

Books against the chain

Every 15 minutes a read-only snapshot reads every custody and deposit address on chain: drift above both $5 and 1%, unswept and unrecorded deposits raise alerts.

RESERVES

Proof of Reserves

Liabilities and reserves matched and published with a verification page customers and auditors can check (pilot).

CHANNELS

Telegram, in separate topics for the money path, market making, infrastructure and operations; e-mail for incidents that need a person; a public status page with real measurements.

WHAT IS WATCHED

Node heights against the deposit scanners, containers, the message queue, the secrets store, the KYC provider and the price feeds, once a minute.

Alerts are tested before they ship.

Every alert rule follows the same discipline: measured, debounced, routed to the right channel, and tested before it ships.

Units and sampling

Every threshold is set in the chain's own unit and above one polling round, so normal scanner movement never pages anyone, while a real stall pages within minutes.

Crash loops

Docker shows 'restarting' only during back-off, so a consecutive count misses it. The rule fires on 3 or more restarting ticks in a window of 10.

Routing

E-mail is for incidents that need a person; the operations channel is for everything else. Opens go to e-mail and Telegram, closes to Telegram only; informational notices never go to e-mail.

Self-test

Every rule replays tick sequences before it ships: one bad tick, two bad then good, three bad, flapping, held ticks mid-incident, a crash loop with gaps.

Exactly once

Each incident has a unique key in the database, so it is announced once across restarts; an open critical is reminded every 6 hours in chat only.

One summary, not a dozen

The price job sends one summary per run instead of one message per token per problem, and retries once before a source counts as down.

Reserves a customer can check in the browser.

Liabilities

A Merkle sum tree of every balance, from a CSV export or a read-only SQL query. Only the root and per-asset totals are published; positions are shuffled daily.

Customers

An inclusion proof in the account area, checked in the browser: signature, path to the root, root against the published snapshot.

Reserves

The block height and hash of every reading are recorded. Unreadable wallets are listed, never counted.

Ownership

Officers sign one challenge per audit period with the auditor's nonce; EVM, TRON and Bitcoin signatures are verified. Multisig and custodian wallets take manual evidence.

Snapshot

Canonical JSON signed with your Ed25519 key, every day at 00:05 UTC, kept 400 days. Change one number and the signature fails.

Auditor pack

HTML report in English and Turkish with CSV annexes; negative balances, unreadable wallets, unverified ownership and shortfalls listed as exceptions.

CHAIN FAMILY	HOW A READING IS PINNED
EVM: Ethereum, BNB Smart Chain, Polygon, Avalanche C	one block number for every read, hash checked again after reading
TRON	head block recorded at the start of the read
Bitcoin	tip checked before and after, read again if a block arrived; xpub, ypub, zpub with gap-limit scan
Solana · XRP Ledger	slot and blockhash per reading · one validated ledger for every read

Works on BitPolaris or on any other exchange software. Pilot: we install it with each of the first customers. Proofs and signed snapshots support an independent audit; they do not replace it.

Numbers we measured, published in full.

Our engineers publish how the platform is run, with the method and the receipts, on bitpolaris.com/insights.

302 → 129
RPC calls per minute after the gateway and job changes

6.43 / 13.03
TRX per USDT transfer on TRON, depending on the recipient

15 min
on-chain treasury reconciliation cycle

6 + 1
exchanges and an aggregator behind every reference price

Blockchain RPC failover
What a normal load balancer gets wrong.
Read the article ↗

Cutting TRON energy costs
Measured receipts; burn, rent or stake.
Read the article ↗

Mirroring and JIT hedging
Deep books with far less prefunding, kept safe.
Read the article ↗

Why USDT deposits get stuck
The states and alerts that keep deposits moving.
Read the article ↗

When three sources are not enough
Why a median, and why every brake needs a release.
Read the article ↗

Building a wallet app
Recovery, send safety and two app stores.
Read the article ↗

Open it now, not after the meeting.

Click any tile in the PDF, or scan the code with a phone. The reference exchange runs this software in production; it is named under NDA and shown live in a guided session.



IN THE BROWSER

Screen tour

Trading, consoles, custody and mobile screens, captured from the running system.

bitpolaris.com/demo#tour ↗



TEST BUILDS

Wallet app

iOS and Android test builds of the wallet, shared after the first call.

bitpolaris.com/demo#wallet ↗



IN THE BROWSER

Payment demo

An invoice, the on-chain confirmation and the signed webhook, step by step.

bitpolaris.com/demo#payments ↗



IN THE BROWSER

Console demo

Markets, verification, treasury and support screens you can click through.

bitpolaris.com/demo#demo-ops ↗



PUBLIC

Documentation

Getting started, trading API, payments API and webhooks, custody policy.

bitpolaris.com/docs ↗



MEASURED

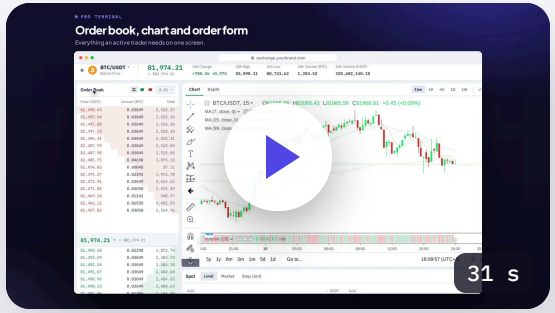
Status page

Availability of the platform's services, measured automatically.

bitpolaris.com/status ↗

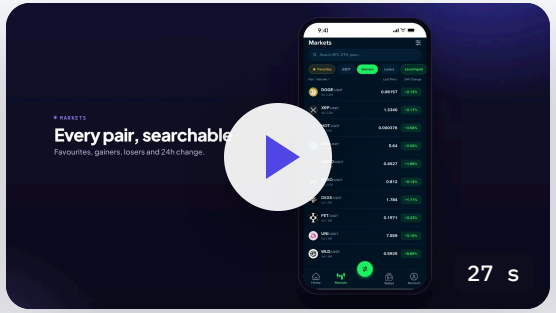
Watch the products run.

Recorded in the real applications under a demo brand with sample data, with English subtitles.



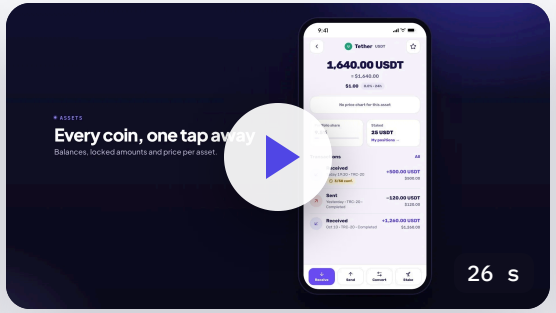
Exchange

Markets, the Pro terminal, Easy Trade and Launchpad.



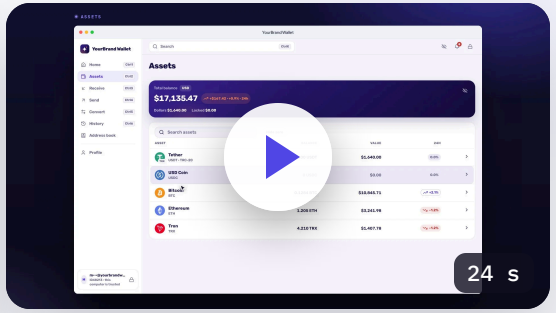
Exchange app

iOS and Android: markets, trading, deposit, Earn.



Wallet app

Balances, Earn, Convert, receive and an address-checked send.



Desktop wallet

macOS and Windows, keyboard-first send, device sessions.

Films, the payment demo and the console demo

bitpolaris.com/demo ↗

Want it live with your data? A guided session takes 45 minutes, with the engineers who run the system.

From assessment to a running system.

Assess
markets, chains, licence regime, integrations

→

Propose
written scope and fixed price in about a week

→

Configure
brand, markets, fees, KYC, chains, environments

→

Rehearse
staging run, data migration dry run if moving

→

Launch
go-live with close watch, then handover

≈ 1 week
from the first call to a written scope and fixed price

2 days
remote training on admin, support and treasury tools

24/7
on-call in year one with the cloud model

20%
of the licence fee a year for self-hosted updates and support

Handover includes the architecture document, runbooks, operator guides and the technical sections of the licence application. Managed operations are available on request.

Releases you approve, migrations reconciled.

Build and test
1,000+ automated tests must pass

→

Staging
changelog and test report posted in the client portal

→

Your approval
security fixes can be expedited with your sign-off

→

Production
a service release rolls back in one command, in seconds

CONTINUITY

Restore drills

Backups are encrypted and sent off-site every night. A restore drill on new hardware is part of every delivery, with timings recorded for the licence file.

MIGRATION

Moving from another platform

One dry run on a copy, two reconciliations (before and after), 100% of balances matched before go-live. Old deposit addresses are watched and swept for an agreed period. If the numbers do not match, we do not go live.

EXIT PATH

Cloud to self-hosted

A dress-rehearsal restore reconciled against the chain, trading paused for under an hour, the cloud instance kept read-only for 30 days, then destroyed with a certificate.

NEXT STEP

Bring your hardest technical question.

We answer in writing, from the system we run. For due diligence we share architecture documents and, under NDA, code walkthroughs.

E-MAIL	WEB	INSIGHTS	LIVE DEMO
sales@bitpolaris.com	bitpolaris.com	bitpolaris.com/insights	bitpolaris.com/demo

BitPolaris is a brand of KSA Global Danışmanlık A.Ş., Istanbul. We are a software vendor: we do not operate an exchange for clients, hold their assets or give investment advice.