CryptaCount

CryptaCount User Manual

Complete Guide to Crypto Accounting

for Professionals

CryptaCount, Inc.

docs.cryptacount.com

March 2026

Accounting Engine

The accounting engine is the core of CryptaCount. It transforms classified transactions into proper double-entry journal entries through a structured pipeline, maintains a chart of accounts, and manages accounting periods with formal close workflows.

Accounting Sidebar Sections

The Accounting section in the sidebar provides access to:

Sidebar Label	Feature
Accounting → Opening Balances	Set opening balances for existing positions
Accounting → Accounting Periods	Manage accounting periods
Accounting → Period Close	Period close workflow with validation checks
Accounting → Generate Journals	Batch journal generation (migration)
Accounting → Journal Entries	View and manage journal entries
Accounting → Impairment	Impairment testing
Manual Adjustments	Manual journal adjustments (approval workflow)
Audit Attachments	Supporting document attachments for audit trail

Accounting Pipeline

The pipeline processes events through a status workflow:

```
PENDING → CLASSIFIED → POSTED (or FAILED / MANUAL_REVIEW /
SKIPPED)
```

The pipeline processes:

- Raw blockchain events into classified accounting events
- Classified events into posted journal entries

- Multi-leg groups (complex transactions with multiple accounting legs)
- Hash chain verification for tamper detection

Double-Entry Bookkeeping

Every transaction processed by CryptaCount generates journal entries where debits equal credits.

Example — Purchasing 1 ETH at €2,100:

Account	Debit	Credit
Digital Assets — ETH	€2,100	
Cash / Fiat		€2,100

Example — Receiving 0.5 LINK as a staking reward (FMV €7.25):

Account	Debit	Credit
Digital Assets — LINK	€7.25	
Staking Income		€7.25

Example — Selling 1 ETH at €2,600 (cost basis €2,100 under FIFO):

Account	Debit	Credit
Cash / Fiat	€2,600	
Digital Assets — ETH		€2,100
Realized Gain — ETH		€500

Chart of Accounts

Manage GL accounts under **Accounting** → **Chart of Accounts**. The chart of accounts uses 8 account types with debit/credit normal balances:

Type	Normal Balance	Description
ASSET	Debit	Digital assets, cash, receivables

LIABILITY	Credit	Borrowings, payables
EQUITY	Credit	Retained earnings, reserves
REVENUE	Credit	Income from operations
EXPENSE	Debit	Operating costs, fees
CONTRA_ASSET	Credit	Accumulated depreciation
CONTRA_LIABILITY	Debit	Contra liability accounts
CONTRA_EQUITY	Debit	Treasury stock, etc.

The chart supports 30 account subtypes for detailed classification (Current Asset, Cash and Equivalents, Receivable, Inventory, Staking Reward, Mining Reward, Transaction Fee, etc.).

GL accounts can be imported, mapped to wallets, mapped to external addresses, and assigned to CEX accounts. Special accounts (like default gain/loss accounts) can be designated.

Journal Entries

View and manage journal entries under **Accounting → Journal Entries**:

- Create manual journal entries
- Post draft entries
- Reverse posted entries
- Search and filter by date, account, and transaction type
- Reassign GL accounts on existing entries via **Balances → Reassign GL**

Tamper-Evident Journal Hashing

Each journal entry is cryptographically hashed. The hash chain links each entry to its predecessor — any modification to a historical entry breaks the chain, making unauthorized changes immediately detectable.

Accounting Periods

Manage periods under **Accounting → Accounting Periods**:

- Create monthly or custom periods

- Open and close periods
- Year-end close workflow

Period Close Workflow

The period close follows a structured process:

1. **Run checks** — Automated validation checks verify data completeness
2. **Review results** — View which checks passed or failed
3. **Waive** — Optionally waive non-critical failed checks with justification
4. **Close** — Formally close the period, locking it from further changes
5. **Reopen** — If needed, reopen a closed period (with audit trail)
6. **Lock** — Permanently lock a period (prevents reopening)

Opening Balances

Set opening balances under **Accounting → Opening Balances** for wallets that had existing positions before connecting to CryptaCount:

- Import opening balances from a file
- Set balances as of a specific date
- Auto-populate suggested dates based on wallet activity

Generate Journals

The journal generation tool under **Accounting → Generate Journals** provides batch processing for:

- Migrating transactions that predate the accounting pipeline
- Regenerating journals after rule changes
- Status tracking with start/cancel/cleanup controls

Impairment Testing

Impairment testing under **Accounting → Impairment** supports:

- Running impairment calculations across the portfolio

- Viewing impairment results by asset

- Different impairment models based on cost basis method (one-way for historic FIFO methods, two-way for NRV methods)

Manual Adjustments

Manual adjustments support an approval workflow:

- Create adjustment entries with justification

- Pending adjustments await approval

- Approve or reject adjustments

- Post approved adjustments to the ledger

Audit Attachments

Upload supporting documents under **Audit Attachments**:

- Attach files to journal entries, transactions, or periods

- Upload and download attachments

- Maintain audit trail with document references

Accounting Rules

Configure rules under **Settings** → **Rules** to automate journal generation:

- Define rules with conditions and actions

- Test rules against sample data

- Version control for rule changes

Accounting Periods & Period Close

Accounting periods define the time boundaries over which CryptaCount aggregates transactions, calculates balances, and produces financial reports. The period close workflow ensures data completeness and integrity before finalizing each period.

Creating Accounting Periods

Navigate to **Accounting → Accounting Periods** to manage the period calendar for your workspace.

Monthly Periods

CryptaCount can auto-generate monthly periods for a fiscal year. Each period spans a calendar month (e.g., 2025-01-01 to 2025-01-31). Monthly periods are the most common configuration and align with standard reporting cadences.

To create monthly periods:

1. Navigate to **Accounting → Accounting Periods**
2. Select the fiscal year start month
3. Click **Generate Monthly Periods** — CryptaCount creates 12 periods

Custom Periods

For non-standard fiscal calendars (4-4-5, 4-week periods, stub periods), create periods manually:

1. Click **Create Period**
2. Set the start and end dates
3. Assign a period name (e.g., "Q1 2025" or "Stub — Jan 1–15")
4. Save

> *Caution: Periods must not overlap. CryptaCount validates that each new period's date range does not conflict with existing periods in the workspace.*

Period States

Each period moves through a lifecycle:

State	Description
Open	Transactions can be posted, journals created, balances calculated
Closed	No new postings allowed — period has passed close workflow
Locked	Permanently sealed — cannot be reopened

Monthly Close Workflow

The period close under **Accounting → Period Close** follows a structured four-stage process designed to match professional accounting practice.

Stage 1 — Initiate Close

Select the period to close and click **Initiate Close**. This triggers the automated check suite and moves the period into "closing" status. No new journal entries can be posted while the close is in progress.

Stage 2 — Run Checks

CryptaCount runs a series of validation checks against the period:

Check	What It Validates
Unmapped addresses	All wallet addresses have GL account mappings
Transaction counts	On-chain transaction counts match imported counts
Opening vs. closing balances	Opening balances for this period match closing balances of the prior period
Internal transfers	Internal transfer pairs are balanced (no orphans)
Fee completeness	All transactions with fees have fee amounts recorded
Price availability	All assets have price data for the period's date range
CEX matching	CEX import transactions are matched or accounted for

Double-entry integrity	Total debits equal total credits across the period
Ledger replay	Journal entries can be replayed from source transactions without discrepancy
Hash chain integrity	Journal hash chain is unbroken through the period

Each check returns a **pass**, **warning**, or **fail** status with details.

Stage 3 — Validate & Waive

Review the check results:

- **All passed** — Proceed directly to close
- **Warnings present** — Review each warning. Warnings do not block close but should be investigated.
- **Failures present** — Either fix the underlying issue and re-run checks, or **waive** the failed check with a written justification

Waived checks are recorded in the audit trail with the user who waived, the timestamp, and the justification text. This is visible to auditors reviewing the period.

Example: *Acme Digital Holdings* might waive a price availability check for an obscure governance token if the position is immaterial, documenting: "GOVXYZ position is €12.40 — immaterial, price manually verified."

Stage 4 — Complete Close

Click **Complete Close** to finalize:

- The period status moves to **Closed**
- A close timestamp and closing user are recorded
- Closing balances are frozen as the opening balances for the next period
- The period appears as "Closed" in the period list

Reopening a Closed Period

If an error is discovered after close:

1. Navigate to the period in **Accounting → Accounting Periods**

2. Click **Reopen**

3. Provide a justification (recorded in audit trail)

4. The period returns to **Open** status

5. Make corrections, then run the close workflow again

Note: Reopening a period may affect downstream periods. If Period 2's opening balances were derived from Period 1's close, reopening Period 1 invalidates Period 2's opening balances. CryptaCount warns about this cascade.

Year-End Close

The year-end close is a special close operation available on the last period of a fiscal year. In addition to the standard close checks, it:

1. **Closes all remaining open periods** in the fiscal year (runs checks on each)

2. **Generates closing entries** — Revenue and expense accounts are zeroed out to Retained Earnings

3. **Carries forward balances** — Balance sheet accounts (assets, liabilities, equity) carry forward as opening balances for the new fiscal year

4. **Locks the fiscal year** — All periods in the year are locked to prevent accidental reopening

To run year-end close:

1. Ensure all periods except the final one are already closed

2. Navigate to the final period's close workflow

3. Select **Year-End Close** instead of standard close

4. Review the generated closing entries before confirming

Opening Balances

Set the starting position for wallets that held assets before connecting to CryptaCount under **Accounting → Opening Balances**.

When to Use Opening Balances

- Migrating from another accounting system to CryptaCount

- Connecting a wallet that has historical activity predating your CryptaCount start date

- Starting a new fiscal year with carried-forward positions

Import Methods

File import:

1. Navigate to **Accounting → Opening Balances**

2. Click **Import**

3. Upload a CSV with columns: asset, quantity, cost basis, GL account, date

4. Preview the import and confirm

Auto-populate:

CryptaCount can suggest opening balance dates based on wallet sync history. Click **Suggested Date** to use the earliest synced transaction date minus one day. The system calculates positions from on-chain data up to that date.

Manual entry:

Set individual asset balances directly in the UI. Specify the asset, quantity, unit cost basis, and target GL account.

Opening Balance Rules

- Opening balances must be set **before** running balance calculations for the period

- Each asset's opening balance is recorded as a journal entry (debit asset account, credit opening balance equity account)

- Once a period is closed, its opening balances cannot be modified without reopening the period

Locking Periods

Locked periods are permanently sealed:

- Cannot be reopened

- No journal entries can be posted or reversed

- Opening balances cannot be modified

- Provides the strongest audit guarantee

To lock a period, it must already be in **Closed** status. Navigate to the period and click **Lock**. This action requires Owner or Manager role and is recorded in the audit trail.

> *Tip:* Lock periods after your external audit is complete. This ensures the audited figures cannot be accidentally altered.

Manual Adjustments & Audit Attachments

Not every accounting entry originates from a blockchain transaction or CEX trade. Manual adjustments handle accruals, corrections, reclassifications, and other entries that require human judgment. Audit attachments provide the supporting documentation trail. Transaction groups organize related transactions for clearer reporting.

Availability

These features are available on qualifying plans.

Manual Adjustments

Navigate to **Manual Adjustments** in the sidebar to manage adjustment entries.

Why Manual Adjustments

Common scenarios requiring manual adjustments:

Scenario	Example
Accruals	Recognize staking rewards earned but not yet claimed
Corrections	Fix a misclassified transaction after period close
Reclassifications	Move a balance from one GL account to another
Provisions	Record a provision for impairment or bad debt
Year-end entries	Closing entries, tax provisions, audit adjustments
Off-chain events	Record equity changes, OTC trades, or legal settlements

Creating an Adjustment

1. Click **New Adjustment**
2. Fill in the adjustment details:
    - **Date** — The effective date of the adjustment

- **Description** — Clear narrative explaining the purpose

- **Justification** — Why this manual entry is necessary (required for audit trail)

- **Journal lines** — Debit and credit lines with GL accounts and amounts

3. Submit for approval

The adjustment is saved in **Pending** status.

Example: *Acme Digital Holdings* records accrued staking rewards for December:

Account	Debit	Credit
Accrued Staking Receivable	€8,420	
Staking Income — Accrued		€8,420

Justification: "Accrue ETH staking rewards earned Dec 15–31, not yet claimed on-chain. 4.2 ETH at €2,005/ETH."

Approval Workflow

Manual adjustments follow a maker-checker workflow:

```
Created (Pending) → Approved → Posted
                  → Rejected
```

Pending adjustments:

- Visible to all workspace members with journal permissions
- The list shows a badge count of pending items

Approval:

1. A different user (not the creator) reviews the pending adjustment
2. Reviews the journal lines, justification, and supporting documents
3. Clicks **Approve** or **Reject**
4. If rejected, provides a reason

Posting:

Once approved, the adjustment can be posted to the ledger:

1. Open the approved adjustment

2. Click **Post**

3. CryptaCount creates the journal entry with a reference linking back to the adjustment

> *Note: The creator cannot approve their own adjustment. This separation of duties is enforced by the system and cannot be overridden.*

Adjustment States

State	Description
Pending	Awaiting approval from a different user
Approved	Reviewed and approved — ready to post
Rejected	Reviewed and rejected with reason
Posted	Journal entry created and posted to ledger

Audit Attachments

Navigate to **Audit Attachments** in the sidebar to manage supporting documents.

Supported Attachments

Upload any document that supports an accounting entry:

- **Invoices and receipts** — PDF, image files

- **Bank statements** — PDF exports from fiat accounts

- **Exchange confirmations** — Trade confirmations from CEX platforms

- **Board resolutions** — Approval documents for significant transactions

- **Valuations** — Third-party valuation reports for fair value assessments

- **Contracts** — OTC trade agreements, loan agreements

- **Correspondence** — Emails or letters relevant to transactions

Uploading

1. Click **Upload**

2. Select one or more files

3. Assign metadata:

    ○ **Related entity** — Link to a journal entry, transaction, or period

    ○ **Description** — Brief description of the document

    ○ **Tags** — Optional categorization tags

4. Upload

Files are stored securely and linked to the specified entity. Auditors can navigate from any journal entry to its supporting attachments.

Accessing Attachments

Attachments can be accessed from multiple points:

- **Attachment library** — Browse all attachments under **Audit Attachments**
- **Journal entry detail** — View attachments linked to a specific entry
- **Transaction detail** — View attachments linked to a transaction
- **Period close** — Review attachments relevant to the closing period

Download & Export

- Download individual attachments
- Bulk download all attachments for a period (useful for external audit)
- Attachment metadata is included in audit trail exports

Transaction Groups

Navigate to **Transaction Groups** in the sidebar to organize related transactions.

Why Group Transactions

Complex operations often span multiple on-chain transactions. Grouping them provides:

- **Clearer reporting** — View the full economic event, not individual fragments

- **Easier reconciliation** — Match grouped transactions against CEX or bank records
- **Audit trail** — Document why transactions are related

Common Groupings

Group Type	Example
Multi-step DeFi operation	Approve + swap + stake as one economic event
Bridge transfer	Bridge out on chain A + bridge in on chain B
OTC trade	Multiple wallet transfers constituting one off-exchange deal
Treasury rebalance	Series of swaps executed as a single rebalancing decision

Managing Groups

1. **Create a group** — Give it a name and description
2. **Add transactions** — Select transactions to include in the group
3. **Expand/Collapse** — Toggle between viewing individual transactions and the group summary
4. **Archive** — Archive completed groups to keep the active list clean

Groups display a summary showing:

- Total value of grouped transactions
- Net asset movement
- Date range
- Transaction count

Advanced Asset Management

CryptaCount's advanced asset module extends beyond standard crypto tokens to cover the full spectrum of digital and tokenized assets — from NFTs and real-world assets to custodial integrations, cross-chain transfers, and AI-powered classification.

Availability

All features on this page are available on qualifying plans.

NFT Portfolio

Track NFTs under **NFT** in the sidebar.

NFT Lifecycle

CryptaCount tracks the full lifecycle of each NFT:

Event	Accounting Treatment
Mint	Acquired at mint cost (gas + mint fee)
Buy	Acquired at purchase price
Sell	Disposed — realize gain/loss vs. cost basis
Transfer	Internal transfer (no gain/loss) or gift
Burn	Write off at carrying value

Portfolio View

The NFT portfolio shows:

- **Collection grouping** — NFTs organized by collection
- **Individual NFTs** — Token ID, image thumbnail, acquisition date, cost basis
- **Current valuation** — Floor price or last sale price (where available)

- **Unrealized P&L** — Difference between carrying value and estimated FMV
- **Disposal history** — Sold NFTs with realized gains/losses

NFT Sync

NFTs are discovered during wallet sync. CryptaCount detects ERC-721 and ERC-1155 token transfers and creates NFT records automatically. Manual NFT entries can be created for NFTs on unsupported chains.

Real World Assets (RWA)

Track tokenized real-world assets under **RWA** in the sidebar.

What RWA Covers

- **Tokenized securities** — Equity, debt, or fund tokens representing real-world instruments
- **Tokenized real estate** — Property tokens with rental income
- **Tokenized commodities** — Gold, carbon credits, or other commodity-backed tokens
- **Stablecoins backed by RWA** — Tokens collateralized by treasuries or bonds

RWA Tracking

Feature	Description
Portfolio	View all RWA positions with quantities and valuations
NAV updates	Track net asset value changes over time
Income	Record dividend, interest, or rental income from RWA tokens
Valuation	Manual or feed-based valuation for assets without liquid markets

---

Fund Management

Manage investment fund structures under **Funds** in the sidebar.

Fund Features

Feature	Description
Fund setup	Create fund entities with series (multi-class) support
Investors	Track investor subscriptions, redemptions, and capital accounts
Transactions	Record fund-level transactions (subscriptions, redemptions, distributions)
NAV calculation	Compute net asset value per share/unit
Management fees	Calculate and accrue management fees
Performance fees	Calculate performance fees with high-water mark tracking

Fund Accounting

Funds use a separate accounting layer:

- Each fund has its own set of capital accounts per investor
- NAV is calculated at configurable frequency (daily, weekly, monthly)
- Management fees are typically accrued monthly and paid quarterly
- Performance fees use high-water mark methodology to prevent double-charging

Example: *Acme Digital Holdings* manages a crypto venture fund with €50M AUM. Monthly NAV calculations feed into investor statements and fee calculations.

Custody Integration

Manage custodial wallets under **Custody** in the sidebar.

Supported Custodians

CryptaCount integrates with institutional custody providers:

Provider	Features
Fireblocks	Vault management, transaction approval workflows, auto-sync

Custody Features

Feature	Description
Connections	Configure connections to custody providers
Vaults	View vault structure and balances
Approvals	Track pending transaction approvals in the custody workflow
Sync	Automatic transaction sync from the custodian
Test	Test connectivity before going live

Real-Time Notifications

CryptaCount receives real-time notifications from custody providers for transaction updates. Transactions are automatically synced and classified.

Safe / Multisig Wallets

Manage Safe (formerly Gnosis Safe) wallets under **Safe** in the sidebar.

Safe Features

Feature	Description
Configuration	View Safe setup — owners, threshold, modules
Pending transactions	Track transactions awaiting sufficient signatures
Sync	Sync Safe transaction history
History	Full transaction history with signer details

Safe transactions are reconciled with on-chain data to ensure the accounting records match executed multisig operations.

Token Migrations

Track token swaps and migrations under **Token Migrations** in the sidebar.

What Token Migrations Cover

When a project migrates from one token contract to another (rebranding, upgrades, chain migrations):

Event	Treatment
Migrate out	Dispose of old token
Migrate in	Acquire new token at carried-over cost basis

Migration Detection

CryptaCount can auto-detect known token migrations and suggest matching. For custom or lesser-known migrations:

1. Navigate to **Token Migrations**
2. Click **Create Migration**
3. Link the outgoing and incoming transactions
4. Cost basis carries over from the old to the new token

Loss & Theft Tracking

Record loss and theft events under **Losses** in the sidebar.

Event Types

Type	Description
Lost	Assets permanently lost (e.g., sent to wrong address, burned accidentally)
Stolen	Assets stolen via hack, exploit, or unauthorized access
Recovered	Partial or full recovery of previously lost/stolen assets

Loss Workflow

1. **Record the event** — Specify the asset, amount, date, and circumstances

2. **Forensic details** — Document transaction hashes, addresses involved, and evidence

3. **Claims** — File insurance or legal claims linked to the loss event

4. **Recovery** — Record any assets recovered, reducing the net loss

Accounting Treatment

- Lost assets are written off at carrying value (debit Loss, credit Digital Assets)

- Stolen assets follow the same treatment with different classification for reporting

- Recovered assets are recorded at FMV at time of recovery (debit Digital Assets, credit Recovery Income)

- Net losses may be tax-deductible depending on jurisdiction

IBC Transfers (Cosmos)

Track Inter-Blockchain Communication transfers under **IBC Transfers** in the sidebar.

IBC Features

Feature	Description
Transfer tracking	Record IBC transfers between Cosmos chains
Denomination traces	Resolve IBC denominations to their original token
Timeout refunds	Track failed IBC transfers and refunded amounts
Relayer fees	Record relayer fees as transaction costs

Denomination Resolution

IBC denominations appear as hashed strings. CryptaCount resolves these to their original token symbols using denomination traces, so you see human-readable names rather than hash codes.

Avalanche P-Chain

Track AVAX P-Chain staking under **AVAX P-Chain** in the sidebar.

P-Chain Features

Feature	Description
Staking positions	Active validator and delegator stakes
Rewards	Staking rewards earned from validation
Summary	Aggregate staking statistics

The P-Chain uses a different transaction model from the C-Chain. CryptaCount handles both and reconciles cross-chain transfers between P-Chain and C-Chain.

L2 Fee Analysis

Analyze Layer 2 fees under **L2 Fees** in the sidebar.

What L2 Fee Analysis Covers

Metric	Description
L1 data fees	Cost of posting data to the L1 (calldata/blob fees)
L2 execution fees	Computation costs on the L2
Total fees by chain	Breakdown across Arbitrum, Optimism, Base, zkSync, etc.
Fee comparison	Compare L2 fees vs. equivalent L1 transactions

---

Account Abstraction

Track smart account operations under **Account Abstraction** in the sidebar.

Features

Feature	Description
Supported chains	View chains with smart account support
Entrypoints	Track entrypoint contract interactions
Operations	Individual smart account operation records
Paymaster fees	Gas fees paid by paymasters on behalf of the account
Bundler fees	Fees paid to bundlers for operation inclusion

Accounting Treatment

Account abstraction splits gas costs differently from traditional wallet transactions. CryptaCount tracks:

- Actual gas consumed by the operation
- Paymaster sponsorship (recorded as gas expense with a corresponding paymaster credit if applicable)
- Bundler fees as a separate fee line item

Privacy Transactions

Track privacy-preserving transactions under **Privacy** in the sidebar.

Privacy Features

Feature	Description
Shield/unshield	Track assets moving into and out of privacy pools
View keys	Manage view keys for auditor access to shielded balances

Auditor Access

For compliance and audit purposes, CryptaCount supports view key management. View keys allow authorized auditors to verify shielded balances without exposing transaction details to the public.

AI Classification

AI-powered transaction classification under **AI Classification** in the sidebar.

How AI Classification Works

1. CryptaCount's AI engine analyzes unclassified transactions

2. It suggests transaction types based on:

    - On-chain function signatures and event logs

    - Historical classification patterns for similar transactions

    - Protocol identification and known contract interactions

3. Review suggestions and accept or reject each one

4. Accepted classifications are applied; rejected ones go to manual review

Features

Feature	Description
Classify	Run AI classification on pending transactions
Suggestions	View classification suggestions with confidence scores
Accept/Reject	Approve or reject individual suggestions
Bulk actions	Accept or reject suggestions in bulk
Generate rules	Generate accounting rules from accepted classifications

Learning

The AI engine improves over time:

- Accepted classifications reinforce the model's patterns

- Rejected classifications are negative signals

- Generated rules codify learned patterns for deterministic future matching

---

Fiat Account Tracking

Track traditional fiat accounts under **Fiat Accounts** in the sidebar.

Fiat Features

Feature	Description
Accounts	Register bank accounts, payment processor accounts
Transactions	Record fiat deposits, withdrawals, and transfers
Balances	Track fiat balances alongside crypto positions
Reconciliation	Match fiat transactions against bank statements

Why Track Fiat

A complete accounting picture requires both crypto and fiat:

- Fiat on-ramps and off-ramps need matching entries

- Fiat balances appear on the balance sheet

- Fiat transactions flow through the same GL structure

- Reconciliation between fiat ramps and bank records

Analytics & Monitoring

CryptaCount's analytics suite provides portfolio performance tracking, price data health monitoring, and proof of reserves attestation — the tools that give management and auditors confidence in the accuracy and completeness of reported figures.

Portfolio Performance

Track portfolio performance under **Performance** in the sidebar.

Performance Metrics

CryptaCount calculates key portfolio metrics across configurable time windows:

Metric	Description
Total Return	Absolute return in reporting currency (realized + unrealized)
Return %	Percentage return over the selected period
Time-Weighted Return (TWR)	Return adjusted for cash flows (deposits/withdrawals) — standard for portfolio comparison
Volatility	Standard deviation of periodic returns
Sharpe Ratio	Risk-adjusted return relative to a risk-free rate
Max Drawdown	Largest peak-to-trough decline in portfolio value
Alpha / Beta	Performance relative to a benchmark (BTC, ETH, or custom index)

Performance Snapshots

Performance data is captured as periodic snapshots:

- **Daily** — End-of-day portfolio value and composition
- **Weekly** — Weekly performance summary
- **Monthly** — Monthly performance for reporting periods

Snapshots enable:

- Historical performance charts

- Period-over-period comparison

- Attribution analysis (which assets contributed to returns)

Attribution

Break down returns by:

- **Asset** — Which tokens drove performance

- **Category** — Returns from trading, staking, DeFi, etc.

- **Wallet** — Performance by wallet or custody account

- **Chain** — Returns by blockchain network

Example: *Acme Digital Holdings* Q4 2025 performance attribution:

Category	Return	Contribution
ETH holdings	+18.2%	+€142,000
Staking rewards	—	+€24,500
DeFi yield	—	+€11,200
Gas fees	—	-€3,800
Total	**+12.4%**	**+€173,900**

Benchmarking

Compare portfolio performance against:

- **BTC** — Bitcoin price return

- **ETH** — Ethereum price return

- **Custom basket** — User-defined weighted index

- **S&P 500 / traditional indices** — For cross-asset comparison (via FX rate conversion)

Price Health

Monitor price feed health under **Price Health** in the sidebar.

Why Price Health Matters

Accurate pricing is foundational to every calculation in CryptaCount — balances, P&L, impairment, tax, and financial reports. Price health monitoring ensures:

- All assets in the portfolio have reliable price data

- Price feeds are current and not stale

- Anomalous price movements are flagged before they corrupt calculations

Health Dashboard

Metric	Description
Coverage	Percentage of portfolio assets with active price feeds
Staleness	Assets with price data older than the acceptable threshold
Anomalies	Price movements that exceed normal volatility bounds
Missing prices	Assets with no price data at all

Alerts

CryptaCount generates price health alerts for:

Alert Type	Trigger
Stale price	No price update within the last 24 hours for an active position
Price spike	Price change exceeding 50% in 24 hours (configurable threshold)
Price gap	Missing price data for a date in a period being closed
Zero price	Asset priced at zero when it previously had a non-zero price
New asset	New asset detected in portfolio without a configured price feed

Price Audit

The price audit log records:

- Price source for each data point (CoinGecko, manual entry, pegged, etc.)

- Timestamp of each price update

- Historical price changes and corrections

- Manual overrides with justification

Tip: Run a price health check before each period close. The period close workflow includes a price availability check, but proactively reviewing price health helps resolve issues before they block the close.

Proof of Reserves

Generate proof of reserves under **Proof of Reserves** in the sidebar.

What Proof of Reserves Is

Proof of Reserves (PoR) is a verifiable attestation that an entity holds sufficient assets to cover its obligations. For crypto companies, this typically means proving that on-chain balances match reported holdings.

Attestation Process

1. **Initiate attestation** — Select the scope (all wallets, specific wallets, or a workspace)

2. **Snapshot balances** — CryptaCount captures current on-chain balances for all connected wallets

3. **Run verification checks:**

   - On-chain balance matches CryptaCount's recorded balance

   - Address ownership is verified (signed message or historical activity)

   - External wallet balances are cross-referenced

   - CEX balances are included where connections exist

4. **Generate report** — A timestamped attestation document with:

   - Total assets by token and chain

   - Wallet addresses and verified balances

   - Comparison against reported positions

   - Hash of the attestation data for tamper evidence

Verification Checks

Check	Description
Balance match	On-chain balance matches internal records
Address ownership	Wallet is controlled by the entity (verified via signature or activity)
Completeness	All known wallets are included in the attestation
Timestamp	Attestation reflects a specific point in time

Use Cases

Audience	Purpose
Auditors	Independent verification of asset existence
Regulators	Compliance with reserve requirements (e.g., MiCA)
Investors	Transparency and trust in reported holdings
Board / management	Internal assurance of treasury integrity

Scheduled Attestations

Configure automatic attestation runs on a schedule (daily, weekly, or monthly) to maintain a continuous audit trail. Each run is archived with its full dataset.

Example: *Acme Digital Holdings* runs weekly proof of reserves every Sunday at 00:00 UTC. The attestation covers 12 wallets across 5 chains plus 3 CEX accounts, totaling €48.2M in assets.

Volatility Analysis

CryptaCount also tracks asset volatility (accessible via the performance module):

Feature	Description
Calculate	Compute historical volatility for any asset
Latest	Current volatility reading

History	Volatility over time with trend analysis
Summary	Portfolio-level volatility metrics

Volatility data feeds into risk metrics (Sharpe ratio, VaR) and is used by the price health module to calibrate anomaly detection thresholds.

Asset Management

The Asset Registry provides a catalog of every token and coin discovered across your connected wallets, with tools for classification, spam management, and per-asset configuration.

Asset Registry

Navigate to **Settings → Asset Registry** to view and manage all discovered assets. Each entry shows:

- **Name and symbol** (e.g., "Ethereum — ETH")
- **Chain** (which blockchain network)
- **Contract address** (for tokens; native coins don't have one)
- **Classification** (native token, ERC-20, stablecoin, NFT, LP token, wrapped)
- **Total quantity** held across all wallets
- **Current FMV**
- **Spam status** (clean, flagged, or manually overridden)

Asset Actions

From the asset registry you can:

- Search and filter assets
- View asset statistics
- Review asset queue — assets needing classification review
- Bulk classify assets
- Manage spam status

Spam Token Management

CryptaCount automatically flags suspected spam tokens:

Detection methods:

- **Heuristic scoring** — Tokens scored on contract age, holder count, liquidity depth, transfer patterns, and metadata quality
- **Homoglyph detection** — Token names checked for Unicode look-alike attacks (e.g., "USDC" using Cyrillic characters)
- **Platform-wide spam list** — Maintained spam asset database

Managing spam:

- **Flagged tokens are hidden** by default from portfolio views, dashboards, and reports
- **Toggle visibility** — Use "Show spam tokens" to see everything
- **Override status** — Mark legitimate tokens as "Not spam" or manually flag missed spam
- **Spam tokens remain in data** — Hidden, not deleted. Unflagging restores them to all views

Per-Asset Settings

Click any asset to configure:

- **Cost basis method override** — Set a specific method, overriding asset class and workspace defaults (Level 1 in the three-level hierarchy)
- **Asset class assignment** — Change automatic classification
- **Custom labels/tags** — Organize assets (e.g., "DeFi", "Staking", "Treasury")
- **Visibility** — Hide from default views without marking as spam

Advanced Asset Types

Available on qualifying plans, specialized asset management modules include:

Sidebar Label	Feature
NFT	NFT portfolio — mint, sale, transfer, burn, collection, disposal tracking
RWA	Real-World Assets — management, NAV tracking, income recording
Funds	Fund management — series, investors, transactions, NAV, management/performance fees
Custody	Custody dashboard — institutional custody connections, vaults, approval workflows
Safe	Safe/Multisig wallet management — config, pending transactions, history

Restaking	Restaking positions — deposits, withdrawals, rewards, slashing
Token Migrations	Token migration tracking — detect and record migration events
Losses	Loss events and claims — lost/stolen assets, recovery tracking, forensic analysis

NFT Accounting

The NFT portfolio tracks:

- Minting events with gas and mint price as acquisition cost
- Sales with realized gain/loss calculation
- Transfers between wallets
- Burns as disposals
- Collection-level aggregation

Real-World Assets (RWA)

The RWA portfolio manages:

- Physical and tokenized real-world assets
- Net Asset Value (NAV) tracking
- Income from RWA holdings

Fund Management

Fund management supports:

- Fund series and investor tracking
- Transaction recording and NAV calculations
- Management fee and performance fee computation

Custody Integration

Custody connects to institutional custody providers:

- Connections with testing

- Vault management

- Multi-signature approval workflows

- Auto-sync with custody providers

Additional Advanced Features

Available on qualifying plans, additional modules provide:

Sidebar Label	Feature
Governance	Governance locks, rewards, delegation, bribes
IBC Transfers	Cosmos IBC transfer tracking and denomination resolution
AVAX P-Chain	Avalanche P-Chain staking positions
L2 Fees	Layer 2 fee analysis by chain
Account Abstraction	Smart account operation support
Privacy	Privacy transaction tracking (shield/unshield)
MEV	MEV event analysis — flash loans, arbitrage, sandwich attacks
Insurance	Insurance policy and claim management
Fiat Accounts	Fiat account tracking
Performance	Performance metrics and snapshots
Proof of Reserves	Proof of reserves attestation generation

Balance Calculations & Views

The Balances module computes asset holdings, cost basis, and GL-level balances across all wallets and exchange accounts. Every balance figure in CryptaCount derives from a calculation run — there are no estimated or cached numbers.

Triggering a Calculation

Start a balance calculation under **Balances → Calculate**.

Configuration Options

Before running a calculation, configure:

- **As-of date** — The point in time for the balance snapshot (end of month, quarter, or custom date)
- **Wallets** — All workspace wallets or a selected subset
- **Assets** — All discovered assets or specific ones
- **Cost basis method** — FIFO, Weighted Average (WAVG), Fair Market Value (FMV), Net Realizable Value (NRV), LIFO, HIFO, or Specific Identification. Defaults to the workspace accounting method.
- **Base currency** — Your reporting currency (typically set at workspace level)

Running the Calculation

Click **Calculate** to begin. The system:

1. Gathers all classified transactions up to the as-of date
2. Builds the lot inventory using the selected cost basis method
3. Computes per-asset balances (quantity, cost basis, fair market value)
4. Aggregates balances by GL account
5. Generates the balance record

Balance calculations run in the background. For workspaces with high transaction volumes, calculation may take several minutes. The progress indicator shows the current phase — you can

navigate away and return to check status.

> *Tip:* *Run balance calculations at the end of each accounting period before generating financial reports. The rollforward, trial balance, and balance sheet all depend on completed balance calculations.*

Stuck and Failed Calculations

If a calculation stalls or fails:

- **Retry** — Re-run the calculation with the same parameters
- **Diagnose** — View diagnostic details including which asset or phase caused the failure
- **Cancel** — Abort an in-progress calculation

The system also automatically detects and cleans up stuck calculations periodically.

Monthly Balances

View monthly balance snapshots under **Balances → Monthly**.

The monthly view shows:

- **Asset** — Token or coin identifier
- **Quantity** — Holdings at end of month
- **Cost Basis** — Total cost basis in your base currency
- **Fair Market Value** — Current FMV using end-of-period prices
- **Unrealized Gain/Loss** — Difference between FMV and cost basis
- **GL Account** — Which ledger account holds this balance

Period-over-Period

Select multiple months to compare balances across periods. This is useful for identifying:

- Significant position changes
- Cost basis shifts from disposals or rebalancing
- Assets entering or leaving the portfolio

Rollforward

The five-column rollforward under **Balances → Rollforward** shows how each asset balance changed during a period.

The Five Columns

Column	Description
Opening Balance	Balance at the start of the period
Additions	Inflows — purchases, transfers in, staking rewards, airdrops
Disposals	Outflows — sales, transfers out, fees, losses
Revaluation	Mark-to-market adjustments (FMV method) or impairment
Closing Balance	Balance at the end of the period

The rollforward verifies that:

```
Opening + Additions – Disposals ± Revaluation = Closing
```

Any imbalance indicates a data issue — missing transactions, classification errors, or unreconciled transfers.

Drill-Down

Click any cell in the rollforward to see the individual transactions that compose that figure. For example, clicking the "Additions" amount for ETH shows every ETH inflow transaction during the period.

The rollforward supports filtering by:

- **Balance ID** — View a specific calculation run's rollforward
- **Asset** — Focus on one asset
- **GL Account** — Filter to a specific ledger account

Balance Transactions

View the transactions underlying any balance under **Balances** → **Transactions**.

This view provides a flat list of all transactions that contribute to a balance calculation. It's the audit trail — every transaction that affected the balance is listed with its:

- Date and transaction hash
- Type (TRANSFER_IN, SWAP, STAKING_REWARD, etc.)
- Asset, amount, and FMV
- Cost basis contribution
- Wallet source

Use this view to verify that a balance figure is correct by inspecting its component transactions.

Lot Viewer

Examine individual tax lots under **Balances** → **Lots**.

A **lot** represents a specific acquisition of an asset — when it was acquired, how much, at what cost. The lot viewer shows:

- **Acquisition date** — When the lot was created
- **Asset** — Which token or coin
- **Quantity** — Original lot size and remaining quantity
- **Cost per unit** — Acquisition cost
- **Total cost basis** — Quantity × cost per unit
- **Current FMV** — Fair market value of remaining quantity
- **Status** — Open (still held), Partially Disposed, or Fully Disposed
- **Disposal details** — If disposed, which transactions consumed this lot

Lot Selection Methods

The lot viewer reflects whichever cost basis method was used for the balance calculation:

Method	Lot Selection Order
FIFO	First-In, First-Out — oldest lots disposed first

LIFO	Last-In, First-Out — newest lots disposed first
HIFO	Highest-In, First-Out — highest cost lots disposed first (minimizes gains)
WAVG	Weighted average cost — no individual lot tracking
Specific ID	Manual lot selection per disposal

Lot Selections

For Specific Identification method, the lot viewer allows you to:

1. View a disposal transaction

2. See available lots that could satisfy it

3. Select which specific lot(s) to assign to the disposal

4. Save the selection — this overrides the automatic lot matching

Scan for External Addresses

Discover untracked external addresses under **Balances → Scan External**.

This tool scans your transaction data for addresses that:

- Appear as counterparties in transactions

- Are not registered as internal or external wallets

- May need to be added for complete reconciliation

For each discovered address, the scanner shows:

- The address and its detected chain

- Number of transactions involving this address

- Total value transacted

- Whether it appears to be an exchange, contract, or unknown entity

Taking Action

From the scan results, you can:

- **Add as External Wallet** — Register the address for proper classification

- **Ignore** — Mark as reviewed and not relevant
- **Investigate** — View the transactions involving this address before deciding

Tip: Run the external address scan before your period-end reconciliation. Untracked counterparty addresses are one of the most common causes of reconciliation differences.

Reassign GL Accounts

Bulk-reassign GL accounts for existing balance data under **Balances → Reassign GL**.

When your chart of accounts changes — merging accounts, splitting accounts, or correcting misassignments — you may need to reassign which GL account holds existing balance and transaction data.

The reassignment tool allows you to:

1. **Select the source GL account** — The account currently holding the data
2. **Select the target GL account** — Where the data should move
3. **Filter by asset or date range** — Optionally narrow the scope
4. **Preview the change** — See how many balances and journal entries will be affected
5. **Execute** — Apply the reassignment

Caution: GL reassignment updates existing journal entries and balance records. This changes historical data. Use this for corrections only — not for routine reclassification. For ongoing changes, update the wallet or asset GL mapping instead.

Billing & Plans

CryptaCount uses a subscription-based pricing model with plan tiers that control access to features. Billing includes automatic invoicing and self-service management.

Plans

Plans are designed for different audience segments:

Business — For companies managing their own crypto accounting. Limits based on wallets, transaction volume, and features.

Practice — For accounting firms, auditors, and tax advisers managing multiple clients. Higher limits and client management features.

Plan details and current pricing are available at cryptacount.com/pricing.

What Plans Control

Plans determine access to feature modules and set usage limits:

- Number of connected wallets
- Monthly transaction sync volume
- Number of companies
- Number of team members
- Number of workspaces (Practice plans)
- Access to advanced feature modules (DeFi accounting, advanced assets, compliance, tax generation, derivatives)

When you reach a plan limit, CryptaCount indicates which limit was hit and which upgrade resolves it. Existing data and reports remain fully accessible — only new additions are blocked.

> **Note:** Plan enforcement is transparent. You'll never lose access to existing data because of a plan limit.

Managing Your Subscription

Navigate to **Settings → Billing** to:

- **View current plan** — Plan tier, usage against limits, billing cycle, feature access
- **Upgrade or downgrade** — Change plan tier. Upgrades take effect immediately with prorated billing. Downgrades take effect at end of current cycle.
- **Payment method** — Open the customer portal to update card, switch payment methods, or update billing address
- **Invoices** — View and download past invoices with proper tax documentation
- **Usage** — Track wallet count, transaction volume, and feature usage against plan limits

Payment Processing

All payment processing is handled securely:

- **Checkout** — Initial subscription setup
- **Customer portal** — Hosted portal for payment method management
- **Invoices** — Automatically generated with tax documentation

Practice Billing

Practice users (audit firms, accounting practices) have a separate billing portal under **Practice → Billing**:

- Practice-specific pricing and plan tiers
- Client management billing
- The standard Billing tab in Settings is hidden for Practice users

Billing Entities

CryptaCount operates through two legal entities for billing:

Your Location	Billed By	Tax Treatment
United States	CryptaCount, Inc.	US sales tax (nexus-based)

European Union	CryptaCount, Inc.	EU VAT via Luxembourg OSS
Rest of World	CryptaCount, Inc.	Applicable local tax

Entity assignment is automatic based on billing address.

Overage Handling

If usage exceeds plan allocations, overage charges are calculated at the end of each billing cycle and added to the next invoice. Overage packs can be purchased proactively to cover expected overages at a discounted rate.

Cancellation

To cancel, navigate to **Settings → Billing → Cancel Plan**:

- Subscription remains active until the end of the current paid period
- After expiration, workspace enters read-only mode
- Data is retained for 90 days, then scheduled for deletion
- Reactivate at any time during the retention period

Workspace Sharing and Billing

The "no double billing" principle: when a business shares workspace access with their auditor or accountant, only the business's subscription is charged. The professional accessing the shared workspace does not incur additional charges.

Blockchain Sync

The blockchain sync pipeline fetches, normalizes, and deduplicates on-chain data for each connected wallet. Progress is streamed in real time so you can monitor each sync as it happens.

How Sync Works

When you connect a wallet or trigger a sync, CryptaCount launches two parallel data streams:

Transactions — Fetches native currency transfers (ETH on Ethereum, MATIC on Polygon, etc.) and normal contract calls. These are direct transactions on the chain's base layer.

Token Transfers — Fetches token transfer events (ERC-20 and equivalents). These are contract-emitted events captured from transaction logs, synced independently from native transactions.

Each stream maintains its own progress tracker (last processed block number) and pagination cursor.

Sync Lifecycle

1. **Initialize** — CryptaCount checks if another wallet with the same address and chain is already syncing (prevents double-sync). Determines the starting block per stream.
2. **Fetch** — Request transaction data from blockchain providers in paginated chunks
3. **Normalize** — Convert chain-specific formats into CryptaCount's universal transaction model
4. **Deduplicate** — Check each transaction against existing records to prevent duplicates
5. **Store** — Write new transactions to the workspace
6. **Classify** — Run the transaction classification engine on new records
7. **Price** — Fetch FMV for each asset at each transaction timestamp
8. **Journal** — Generate double-entry journal entries

Deduplication

Every transaction is assigned a unique key based on the chain, block, transaction hash, and event index. CryptaCount checks for existing records before inserting, ensuring no duplicate data even if a sync is interrupted and restarted.

Smart Resume

After the initial full sync, subsequent syncs resume from the last processed block. Critically, the resume point is tracked **per stream** (transactions vs. token transfers):

- Each stream resumes independently
- This prevents the scenario where a fast-finishing stream's block number causes the other to skip data

Real-Time Progress

Sync progress is streamed in real time to the interface. The progress display provides:

- Current sync phase (fetching, normalizing, storing)
- Transactions processed / total estimated
- Block progress (current block / latest block)
- Per-stream status (Transactions, Token Transfers)
- Error messages if any

This enables live progress indicators without needing to refresh the page.

Multi-Wallet Dedup

When the same address is used across multiple workspace wallets (e.g., same address added under different labels), CryptaCount checks for duplicates and skips if another wallet with the same address is already synced or syncing. This prevents duplicate transaction data at the workspace level.

Rate Limiting and Resilience

Blockchain data providers impose rate limits. The sync pipeline handles this with:

- **Automatic backoff** — When rate limits are hit, the system backs off and retries automatically
- **Progress preservation** — If a sync is interrupted, progress is saved per stream and the next sync resumes from where it left off
- **Stuck sync cleanup** — A background job periodically detects and cleans up stuck syncs

Monitoring Sync Status

From the wallet detail view, the **Sync** tab shows:

- Current sync status per stream (Transactions, Token Transfers)

- Last processed block number per stream

- Total transactions fetched

- Any error messages

- Time of last successful sync

Triggering Manual Sync

- **Single wallet:** Open wallet detail → click **Sync Now**

- **Rescan:** Force a full rescan of a wallet from block 0

- **Sync request:** Users can request syncs, which workspace managers approve or reject

Sync Errors

Common sync errors and their resolution:

Error	Cause	Resolution
Rate limit exceeded	Too many requests to the provider	Wait and retry; automatic backoff handles this
Timeout	Large data batch taking too long	Automatic; next sync resumes from last block per stream
Invalid address	Wallet address doesn't match the selected chain	Verify address format and chain selection
Provider unavailable	Blockchain data provider temporarily down	Automatic retry after a waiting period
Double sync detected	Same address already syncing	Wait for existing sync to complete

For persistent issues, see the Sync & Connectivity troubleshooting guide.

Centralized Exchange Connections

CryptaCount connects to centralized exchanges (CEX) to pull trading history, deposits, withdrawals, and fee data. This data feeds into the same accounting pipeline as on-chain wallet transactions — unified classification, journal generation, and reporting.

CEX Accounts

Manage connected exchange accounts under **CEX** in the sidebar.

Each account entry shows:

- **Exchange name** — Binance, Coinbase, Kraken, etc.
- **Account label** — Your custom name (e.g., "Acme Digital Holdings — Binance Main")
- **Connection status** — Connected (API), Import Only (file-based), or Error
- **Last sync** — Timestamp of the most recent data pull
- **Transaction count** — Total transactions imported from this account

Adding an Exchange via API

To connect an exchange through its API:

1. Navigate to **CEX** and click **Add Exchange Account**
2. Select the exchange from the supported list
3. Enter a descriptive label for this account
4. Provide the **API Key** and **API Secret** from your exchange

> *Tip: Create read-only API keys on your exchange. CryptaCount never executes trades or withdrawals — it only reads transaction history. Disabling trade and withdrawal permissions on the key reduces risk.*

5. Click **Connect** — CryptaCount validates the credentials and begins the initial sync

API keys are encrypted at rest.

Supported Exchanges

CryptaCount supports API connections and CSV/XLS/PDF imports for major exchanges. The exact list of supported exchanges is available in the import interface — select "API Import" to see exchanges with direct API support, or "CSV/XLS Import" for file-based options.

CEX Transactions

View all imported CEX transactions under **CEX Transactions** in the sidebar.

The transaction list shows:

- **Date/Time** — When the trade or transfer occurred on the exchange
- **Exchange** — Which exchange account this transaction belongs to
- **Type** — BUY, SELL, DEPOSIT, WITHDRAWAL, FEE, TRANSFER, etc.
- **Asset(s)** — The asset pair involved (e.g., BTC/USDT for a trade)
- **Amount** — Quantity and direction
- **FMV** — Fair market value at the time of the transaction
- **Classification status** — Whether this transaction has been classified and mapped

Classifying CEX Transactions

CEX transactions follow the same classification pipeline as on-chain transactions. CryptaCount auto-classifies most CEX activity:

- **Trades** → BUY or SELL based on quote/base pair direction
- **Deposits** → TRANSFER_IN
- **Withdrawals** → TRANSFER_OUT
- **Fees** → FEE or TRADING_FEE

For transactions that need manual review, use the classification controls in the transaction detail to assign the correct type and economic intent.

Posting Journals from CEX Data

Once CEX transactions are classified and GL-mapped, you can post them as journal entries. Use the **Post Journals** action from the transactions view to generate double-entry journal entries for selected or all classified CEX transactions.

CEX Import

Import exchange data under **CEX Import** in the sidebar. Three import methods are available:

API Import

For exchanges with supported API integrations:

1. Select the exchange
2. Enter your API credentials
3. CryptaCount pulls all available history automatically

The system deduplicates against previously imported data, so re-importing is safe.

CSV Import

For exchanges without API support or when you have exported CSV files:

1. Select the exchange (to use the correct column mapping template)
2. Upload your CSV file
3. Preview the parsed data before confirming the import

CryptaCount provides **exchange-specific CSV templates** — download the template for your exchange to see the expected column format. A **generic CSV** option is also available for exchanges without a specific template.

XLS / PDF Import

For spreadsheet and PDF statement imports:

1. Upload the XLS or PDF file
2. CryptaCount parses the document structure
3. Preview the extracted transactions
4. Confirm the import

> **Note:** *PDF parsing works best with exchange-generated statements. Scanned documents or heavily formatted PDFs may require manual review of the extracted data.*

Import Preview

All import methods show a preview before committing. The preview displays:

- Number of transactions found

- Date range covered

- Potential duplicates flagged

- Any parsing errors or warnings

Review the preview carefully before confirming — once imported, transactions enter the standard accounting pipeline.

CEX GL Mappings

Configure how CEX transaction types map to your chart of accounts under **CEX GL Mappings** in the sidebar.

GL mappings control which general ledger accounts receive debit and credit entries when CEX transactions are journalized. For example:

CEX Transaction Type	Debit Account	Credit Account
BUY (crypto)	Digital Asset Inventory	Cash / Exchange Balance
SELL (crypto)	Cash / Exchange Balance	Digital Asset Inventory
DEPOSIT	Exchange Balance	Bank / Source Account
WITHDRAWAL	Bank / Destination	Exchange Balance
TRADING_FEE	Trading Fee Expense	Exchange Balance

Default Mappings

CryptaCount provides sensible default GL mappings when you first connect an exchange. These defaults follow standard accounting treatment for crypto trading activity.

Custom Mappings

To customize mappings for your organization's chart of accounts:

1. Navigate to **CEX GL Mappings**

2. Select the transaction type to configure

3. Choose the appropriate debit and credit GL accounts from your chart

4. Save — all future and existing unmapped transactions of this type will use the new mapping

> *Tip:* Set up GL mappings before importing large volumes of CEX data. This way, transactions are correctly mapped on import and can be journalized immediately.

CEX Transfer Matching

Match CEX deposits and withdrawals with corresponding on-chain wallet movements under **CEX Transfer Matching** in the sidebar.

When you deposit crypto to an exchange, the transaction appears in both your on-chain wallet data (as a TRANSFER_OUT) and in the exchange data (as a DEPOSIT). Without matching, these would be double-counted — appearing as both an outgoing transfer and an incoming exchange deposit.

Transfer matching links these pairs so the system recognizes them as a single internal movement.

Automatic Matching

CryptaCount automatically attempts to match transfers by comparing:

- **Amounts** — Same asset and quantity (within fee tolerance)
- **Timing** — Transactions within a reasonable time window
- **Addresses** — On-chain destination matches known exchange deposit addresses

Automatic matches are flagged with a confidence score.

Manual Matching

For transfers the system cannot auto-match:

1. Navigate to the **Unmatched** tab in **CEX Transfer Matching**
2. Select a CEX deposit or withdrawal
3. Find the corresponding on-chain transaction
4. Click **Match** to link them

Common reasons for unmatched transfers:

- The on-chain wallet hasn't been synced yet

- The exchange deposit address isn't registered as an external wallet

- Timing differences between exchange timestamps and block confirmation times

- Fee deductions causing slight amount mismatches

Why Matching Matters

- **Prevents double-counting** — The same economic event isn't recorded twice

- **Correct classification** — Matched transfers are classified as INTERNAL_TRANSFER rather than separate IN/OUT events

- **Clean reconciliation** — Unmatched transfers are flagged during reconciliation checks

- **Accurate reporting** — Financial statements reflect actual economic activity, not duplicated movements

Compliance & Screening

CryptaCount's compliance module helps organizations meet regulatory obligations for anti-money laundering (AML), EU crypto-asset regulations (MiCA), tax information exchange (DAC8), and environmental reporting (carbon/ESG).

Availability

All compliance features are available on qualifying plans.

Address Screening

Screen wallet addresses under **Screening** in the sidebar.

What Address Screening Does

Address screening checks wallet addresses against sanctions lists, known illicit actors, and risk databases. This is a core AML/CFT (anti-money laundering / counter-financing of terrorism) requirement for regulated crypto businesses.

Screening Workflow

1. **Configure screening** — Set up screening rules and thresholds
2. **Screen addresses:**
   - **Individual** — Screen a single address on demand
   - **Batch** — Screen multiple addresses at once
   - **Automatic** — Screen all new addresses as wallets are added or transactions are received

3. **Review results** — Each address returns a risk assessment
4. **Take action** — Flag, block, or document high-risk addresses

Screening Results

Each screened address receives:

Field	Description
Address	The wallet address screened
Risk score	Numeric risk rating (0–100)
Risk level	LOW, MEDIUM, HIGH, CRITICAL
Matches	Sanctions list matches (OFAC, EU, UN)
Exposure	Direct or indirect exposure to high-risk entities
Details	Specific list entries and match confidence

Screening Configuration

Setting	Description
Lists	Which sanctions lists to screen against (OFAC SDN, EU Consolidated, UN Security Council, etc.)
Threshold	Minimum match confidence to flag (reduces false positives)
Auto-screen	Enable/disable automatic screening on new addresses
Alert routing	Who receives alerts for high-risk matches

Export

Export screening results for compliance reporting:

- Full screening history with timestamps and results
- Filtered exports by risk level or date range
- Formatted for regulatory submission

Example: *Acme Digital Holdings* runs weekly batch screening on all counterparty addresses. The compliance officer reviews any addresses flagged MEDIUM or above and documents disposition decisions in the screening dashboard.

MiCA Compliance

The Markets in Crypto-Assets Regulation (MiCA) compliance tools are accessible under **Compliance** in the sidebar.

MiCA Token Classification

CryptaCount classifies crypto assets under MiCA categories:

MiCA Category	Description	Examples
E-Money Token (EMT)	Pegged to a single fiat currency	USDC, USDT, EURC
Asset-Referenced Token (ART)	Pegged to a basket of assets or commodities	—
Utility Token	Provides access to a service or product	UNI, AAVE, LINK
Other Crypto-Asset	Does not fit EMT, ART, or utility definitions	BTC, ETH

Classification Workflow

1. CryptaCount auto-classifies known tokens based on its token registry
2. Review auto-classifications and override where needed
3. New or unrecognized tokens are flagged for manual classification
4. Classification history is maintained for audit trail

MiCA Reporting

Based on token classifications, CryptaCount assists with:

- Reserve requirements for EMT and ART holdings
- Disclosure obligations for significant holdings
- Transaction reporting thresholds
- Whitepaper compliance tracking for issued tokens

DAC8 Reconciliation

The Directive on Administrative Cooperation (DAC8) extends tax information exchange to crypto-assets. CryptaCount handles DAC8 reporting from the **Compliance** section.

What DAC8 Requires

DAC8 mandates that Crypto-Asset Service Providers (CASPs) report user transactions to tax authorities across EU member states. Key obligations:

Requirement	Description
User identification	Verify and report user identity details
Transaction reporting	Report all crypto-asset transactions above thresholds
Cross-border exchange	Automatic exchange of information between EU tax authorities
Annual reporting	Submit reports by January 31 of the following year

DAC8 Reconciliation Workflow

1. **Run reconciliation** — CryptaCount matches internal transaction records against DAC8 reporting requirements
2. **Review results** — Identify gaps, discrepancies, or transactions needing additional data
3. **Export** — Generate DAC8-compliant XML export for submission

Reconciliation Checks

Check	Description
Completeness	All reportable transactions are included
Identification	User identity data is present and valid
Thresholds	Transactions meeting reporting thresholds are flagged
Consistency	Internal records match external data sources

Carbon / ESG Estimation

Estimate the carbon footprint of crypto operations under **Carbon** in the sidebar.

What Carbon/ESG Covers

Feature	Description
Carbon estimation	Estimate CO_2 emissions from blockchain transactions
By chain	Emissions broken down by blockchain (PoW vs. PoS)
By wallet	Emissions attributed to each wallet's activity
Summary	Aggregate emissions with period-over-period comparison

How Estimation Works

CryptaCount estimates carbon footprint based on:

1. **Chain consensus mechanism** — Proof of Work chains (Bitcoin) have significantly higher per-transaction emissions than Proof of Stake chains (Ethereum post-Merge)
2. **Transaction count** — Number of transactions on each chain
3. **Energy mix data** — Regional energy source data for mining (PoW chains)
4. **Network-level emissions** — Published emissions data from blockchain networks

ESG Reporting

The carbon module generates data suitable for ESG (Environmental, Social, Governance) reporting:

- **Scope 3 emissions** — Indirect emissions from crypto operations
- **Trend analysis** — Emissions trend as portfolio shifts between chains
- **Reduction strategies** — Identify high-emission chains and migration opportunities
- **Offset planning** — Estimate carbon offset requirements

Example: *Acme Digital Holdings* reports in their annual ESG disclosure that migrating 80% of operations from Ethereum (pre-Merge) to post–Merge Ethereum reduced estimated crypto-related emissions by 99.4%.

Carbon Summary

Metric	Description
Total estimated CO₂	Aggregate emissions in metric tons
Per-transaction average	Average emissions per transaction
Chain breakdown	Emissions by blockchain with PoW/PoS indicator
Year-over-year change	Trend comparison

Compliance Dashboard

The compliance dashboard provides a unified view:

- **Screening status** — Recent screening results and pending reviews

- **MiCA classification status** — Token classification coverage and overrides

- **DAC8 reporting status** — Reconciliation completeness and upcoming deadlines

- **Carbon summary** — Current period emissions estimate

- **Compliance alerts** — Items requiring attention

Cost Basis Methods

CryptaCount supports eight cost basis methods.

The choice of method determines how the platform calculates gains and losses when you dispose of an asset — and in many jurisdictions, this choice has direct tax implications.

Overview of Methods

Historic FIFO — Historic First In, First Out

The oldest acquired units are treated as disposed first. Uses one-way impairment (write down only, no write-up). This is the standard method for tax reporting in many jurisdictions (US, UK, several EU states).

Example: You purchased 2 ETH at €1,800 in January and 3 ETH at €2,400 in March. When you sell 1 ETH in June at €2,600, Historic FIFO uses the January cost (€1,800), resulting in a €800 gain.

Historic Weighted Average — Historic Weighted Average

All units of an asset are blended into a single average cost using weighted average. No impairment adjustments are applied. Simplified method suitable for tax reporting.

Example: After the two purchases above, the weighted average cost is: (2 × €1,800 + 3 × €2,400) / 5 = **€2,160**. Selling 1 ETH at €2,600 produces a €440 gain.

FMV — Fair Market Value (Mark-to-Market)

Assets are marked to market at their current fair market value. Unrealized gains and losses are recognized. This is primarily used by trading firms and certain fund structures.

NRV + FIFO — Net Realizable Value (FIFO Basis)

Applies the IAS 2 "lower of cost and net realizable value" principle using FIFO for lot ordering. Two-way impairment (write down and write-up, but not above original cost). This is the IFRS-aligned method for entities classifying crypto-assets as inventory.

NRV + Weighted Average — Net Realizable Value (WAVG Basis)

Same as NRV + FIFO but uses weighted average cost as the comparison basis. Also uses two-way impairment.

LIFO — Last In, First Out

The most recently acquired units are treated as disposed first.

> *Caution:* LIFO is not permitted in all jurisdictions. Verify with your tax adviser before selecting this method.

HIFO — Highest In, First Out

The highest-cost units are treated as disposed first. This minimizes realized gains (or maximizes realized losses), which can be advantageous for tax optimization where permitted.

Specific Identification — Specific Identification

The user (or their accountant) selects which specific lots to dispose in each transaction. This provides maximum control over gain/loss timing and is permitted in jurisdictions that allow taxpayer lot selection (including the US).

Specific lot selection is managed through the Lot Viewer under **Balances → Lots**.

> *Tip:* Specific Identification requires manual lot selection for each disposal. It is best suited for large, deliberate transactions where lot choice materially impacts the tax outcome — not for high-volume trading accounts.

Three-Level Resolution Hierarchy

You don't need to pick a single method for your entire portfolio. CryptaCount resolves the cost basis method through a three-level hierarchy:

Level 1: Per-asset override — Set a method on a particular asset. Example: "Use HIFO for LINK." This takes highest precedence.

Level 2: Asset class level — Set a method for an asset class. Example: "Use Historic Weighted Average for all stablecoins." This applies to all assets in that class unless overridden at Level 1.

Level 3: Workspace default — The workspace-level default set under **Settings → Workspace Accounting**. Example: "Use Historic FIFO." This applies to everything not overridden at Levels 1 or 2.

How to Configure

1. **Workspace default** — Go to **Settings → Workspace Accounting** and select the default cost basis method
2. **Asset class level** — Go to **Settings → Asset Registry**, select an asset class, and set the method override
3. **Per-asset** — Select an individual asset and set the method override

Practical Example

A Luxembourg accounting firm managing a client portfolio might configure:

- **Workspace default**: Historic FIFO (standard for Luxembourg)
- **Stablecoins asset class**: Historic Weighted Average (blended cost is more meaningful for stable-value assets)
- **ETH (specific asset)**: Specific Identification (client has a large position where lot selection matters)

When the platform calculates gains on an ETH disposal, it uses Specific Identification (Level 1). For a USDC disposal, it uses Historic Weighted Average (Level 2). For a LINK disposal, it uses Historic FIFO (Level 3).

Comparing Methods

You can run reports under multiple methods simultaneously to compare outcomes. This is useful for tax planning and audit purposes.

Jurisdiction-Specific Requirements

Some jurisdictions mandate a specific method. The platform's 73-jurisdiction tax profiles indicate which methods are permitted, recommended, or required.

Jurisdiction	Required/Recommended Method	Notes
France (individuals)	Historic Weighted Average (mandatory)	Portfolio-wide weighted average formula
Japan	Historic Weighted Average (required)	Total average method for all individuals
US	Historic FIFO (default)	Others permitted if consistently applied
Germany	Historic FIFO (standard practice)	Not strictly mandated but expected by Finanzamt
Australia	Historic FIFO, LIFO, HIFO, Specific Identification	Taxpayer's choice, must be consistent
UK	Section 104 pooling (Historic Weighted Average equivalent)	30-day bed-and-breakfast rule applies

Caution: Tax method requirements change. Always verify current rules with a qualified tax adviser for the specific jurisdiction. CryptaCount provides data — it does not provide tax advice.

Dashboard

The dashboard is your landing page after signing in. It provides an at-a-glance overview of your workspace's operational status, sync health, and accounting progress.

Top Bar

The persistent top bar includes:

- **Search** — Global search across wallets, transactions, and assets
- **Company selector** — Switch between companies you have access to
- **Workspace selector** — Switch between workspaces (common for practices managing multiple clients)
- **Theme toggle** — Switch between light and dark mode
- **Notifications** — Bell icon showing unread alerts (sync completions, errors, team invitations)
- **User menu** — Profile, settings, and logout

Plan Info

The top of the dashboard shows your current subscription plan, usage summary, and a link to upgrade if approaching limits.

Stat Cards

Four summary cards provide key workspace metrics:

Card	What It Shows
Wallets	Total number of connected internal wallets
Transactions (30d)	Transaction count over the last 30 days
Sync Status	Current sync state — how many wallets are synced, syncing, or errored
Pending Reconciliations	Number of items awaiting reconciliation review

Transaction Classification Progress

A progress indicator shows how many transactions have been classified vs. how many are still pending review. This helps you track the completeness of your accounting data before generating reports or closing periods.

Accounting Periods

The dashboard displays the status of your accounting periods — which periods are open, closed, or in the process of being closed. This gives a quick view of your period-end workflow progress.

Wallet Health

A summary of wallet sync health across the workspace:

- Wallets that are fully synced and up to date

- Wallets currently syncing

- Wallets with sync errors that need attention

Clicking any wallet health indicator navigates to the wallet detail view for troubleshooting.

Currency Rates & Crypto Prices

Accurate pricing is the foundation of fair market value calculations, gain/loss computation, and financial reporting. CryptaCount maintains both fiat exchange rates and crypto asset prices, with automated syncing and health monitoring.

Currency Rates

View fiat exchange rates under **Currency Rates** in the sidebar.

CryptaCount syncs fiat exchange rates from central bank and market data sources. These rates are used whenever the system converts between currencies — for example, when Acme Digital Holdings reports in EUR but an asset's primary market trades in USD.

What's Displayed

- **Currency pair** — Base / quote (e.g., USD/EUR, GBP/USD)
- **Current rate** — Latest available rate
- **Date** — Effective date of the rate
- **Source** — Data provider for this rate

Rate Types

- **Daily rates** — End-of-day rates used for balance calculations and period-end reporting
- **Monthly averages** — Average rate over a calendar month, used for income statement conversion in some jurisdictions
- **Historical rates** — Rates for any past date, used for historical cost calculations

Syncing Rates

Fiat exchange rates sync automatically:

- **Scheduled sync** — Runs at 6 PM UTC, Monday through Friday
- **Manual sync** — Trigger a sync from the currency rates interface for immediate updates

- **Backfill** — Request rates for specific date ranges if historical data is missing

Pegged Currencies

CryptaCount tracks pegged currency relationships (e.g., stablecoins pegged to USD). Pegged currencies are listed with their target currency, and the system uses the peg relationship when the specific stablecoin price is unavailable.

Crypto Prices

View current crypto asset prices under **Crypto Prices** in the sidebar.

Market Overview

The prices page shows:

- **Asset** — Token symbol and name
- **Current price** — Latest price in your base currency
- **24h change** — Price movement over the last 24 hours
- **Market cap** — Total market capitalization (where available)
- **Source** — Which pricing feed provided this data

Search and Filter

- **Search** — Find specific assets by symbol or name
- **Trending** — View currently trending assets by volume
- **Coverage** — Check which assets in your workspace have price data available

Price Syncing

Crypto prices sync automatically:

- **Daily sync** — Runs at 00:05 UTC to capture end-of-day prices
- **Live prices** — Current spot prices available on demand for supported assets
- **Missing prices** — The system tracks which assets and dates lack price data

Price Sources and Priority

CryptaCount aggregates prices from multiple sources with fallback logic:

1. **Primary market data providers** — High-reliability feeds for major assets
2. **Secondary providers** — Broader coverage for long-tail tokens
3. **DEX-derived prices** — On-chain pricing for DeFi tokens without centralized exchange listings
4. **Manual entry** — User-provided prices for assets with no automated source

Crypto Price History

View historical price data and charts under **Crypto Price History** in the sidebar.

Price Charts

Select an asset to view its price history:

- **Time range** — View data for the last week, month, quarter, year, or a custom range
- **Granularity** — Daily prices (default) with the option to view monthly aggregates
- **Currency** — Display prices in your base currency or USD

Historical Data Uses

Historical prices feed into several critical calculations:

Calculation	How Prices Are Used
Fair Market Value	FMV at transaction date determines cost basis for acquisitions
Realized Gain/Loss	Disposal price minus cost basis lot price
Unrealized Gain/Loss	Current price minus cost basis for open positions
Impairment Testing	Comparing carrying value against market value
Balance Calculations	End-of-period prices for balance sheet reporting

Price Coverage

The price history view also serves as a diagnostic tool. Check coverage for your workspace's assets:

- **Covered** — Price data exists for all required dates

- **Gaps** — Specific dates or ranges where prices are missing

- **No data** — Assets with no price data at all

For assets with gaps, you can request a backfill or manually provide prices.

Price Health Monitoring

Price health monitoring (available on qualifying plans) provides a deeper view into the reliability and completeness of price data.

Health Status

- **Alerts** — Assets where price data is stale, missing, or shows anomalies (e.g., sudden large spikes that may indicate bad data)

- **Audit trail** — History of price data changes, corrections, and backfills

- **Coverage stats** — Percentage of workspace assets with complete price coverage

Handling Missing Prices

When prices are missing for transactions or balance dates:

1. **Check the reconciliation** — The Price Availability check flags all instances

2. **Request backfill** — For supported assets, trigger a historical price fetch

3. **Manual entry** — For unsupported assets, enter prices manually

4. **Use proxy prices** — For pegged or wrapped assets, the system can derive prices from the underlying asset

> *Caution: Missing prices affect the accuracy of all downstream calculations. A balance calculation with missing prices will either fail or produce incomplete results. Resolve price gaps before running period-end balance calculations.*

DeFi Deep Dive: Pipeline, Positions & Derivatives

This page covers the full DeFi and derivatives suite in detail — from the accounting pipeline that classifies on-chain events, through position tracking and bridge resolution, to advanced instruments like margin trading, futures, options, restaking, and MEV analysis.

Availability

DeFi features are available on qualifying plans. Additional advanced features (restaking, governance, insurance, MEV) may require higher-tier plans.

Accounting Pipeline

The DeFi accounting pipeline under **DeFi → Pipeline** processes raw blockchain events into classified, posted journal entries.

Event Lifecycle

```
PENDING → CLASSIFIED → POSTED
                    → FAILED
                    → MANUAL_REVIEW
                    → SKIPPED
```

- **PENDING** — Raw event ingested from chain, awaiting classification
- **CLASSIFIED** — Engine has determined the transaction type and accounting treatment
- **POSTED** — Journal entries created and posted to the ledger
- **FAILED** — Classification or posting failed (check error details)
- **MANUAL_REVIEW** — Engine flagged the event for human review (ambiguous classification)
- **SKIPPED** — Explicitly skipped (e.g., spam, dust, or irrelevant contract interactions)

Pipeline Dashboard

The pipeline view shows:

- **Status counts** — Number of events in each stage
- **Pending queue** — Events awaiting classification with protocol and type details
- **Review queue** — Events requiring manual classification
- **Multi-leg groups** — Complex transactions spanning multiple accounting legs
- **Hash chain status** — Integrity of the journal hash chain

Processing Events

Events can be processed individually or in batch:

1. **Auto-classification** — The engine applies accounting rules and transaction analysis
2. **Manual classification** — For events in MANUAL_REVIEW, select the correct transaction type and GL accounts
3. **Batch processing** — Select multiple pending events and process them together
4. **Expression validation** — Test accounting expressions before posting

Accounting Rules

Rules under **Settings** → **Rules** automate classification:

- Define conditions based on protocol, function signature, asset, or amount thresholds
- Set the resulting transaction type, GL accounts, and economic intent
- Test rules against sample events before activating
- Rules are versioned — changes create new versions for audit trail

DeFi Position Tracking

Track all open DeFi positions under **DeFi** → **Positions**.

Position Types

Type	Description	Key Metrics

LP Positions	Liquidity pool stakes (Uniswap, Curve, Balancer)	Deposited value, current value, impermanent loss, fees earned
Lending Deposits	Assets deposited in lending protocols (Aave, Compound)	Principal, accrued interest, health factor
Lending Borrows	Outstanding borrows	Principal, accrued interest, liquidation threshold
Staking	Staked assets in validators or protocols	Staked amount, rewards earned, unbonding status

Position Details

Each position displays:

- **Protocol** — The DeFi protocol (e.g., Aave v3, Uniswap v3, Lido)
- **Pool/Vault** — Specific pool or vault identifier
- **Deposited assets** — What was deposited and quantities
- **Current value** — Mark-to-market value
- **P&L** — Unrealized gain/loss vs. deposited value
- **Rewards** — Accumulated but unclaimed rewards
- **Status** — Active, pending withdrawal, or closed

Rebase Token Tracking

For rebasing assets (stETH, aTokens), CryptaCount tracks:

- The underlying balance changes due to rebasing
- Rebasing income recognized at each rebase event
- Accurate cost basis maintained through balance changes

Configure rebase token settings in the DeFi position settings panel.

Bridge Resolution

Cross-chain bridges under **DeFi → Bridges** manage asset movements between chains.

How Bridge Tracking Works

When assets are bridged:

1. A BRIDGE_OUT transaction is recorded on the source chain

2. A BRIDGE_IN transaction is recorded on the destination chain

3. CryptaCount attempts to auto-match the pair based on amount, asset, and timing

Stale Bridge Detection

The bridge view highlights stale bridges — BRIDGE_OUT transactions without a matching BRIDGE_IN within the expected timeframe. Common causes:

- Destination chain wallet not connected to CryptaCount

- Bridge transaction still pending (slow finality)

- Failed bridge that needs manual resolution

Manual Resolution

For unmatched bridges:

1. Navigate to the stale bridge entry

2. Click **Resolve**

3. Select the matching BRIDGE_IN transaction from the destination chain

4. CryptaCount links the pair and carries the cost basis across

> *Caution: Ensure both the source and destination chain wallets are connected to your workspace. Without the destination wallet, CryptaCount cannot detect the BRIDGE_IN transaction.*

Gas Fee Analysis

Gas fee reporting under **DeFi → Gas Fees** provides detailed breakdown of transaction costs.

Report Contents

Metric	Description
Total gas spent	Aggregate gas fees across all wallets and chains
By chain	Gas fees broken down per blockchain
By wallet	Gas fees per wallet address
By transaction type	Gas fees by classification (swaps, transfers, staking, etc.)
Trends	Gas fee spending over time (daily/weekly/monthly)
As % of transaction value	Gas efficiency metric

Accounting Treatment

Gas fees are recorded as expenses in the general ledger. The gas fee report feeds into:

- Income statement under operating expenses

- Transaction-level cost tracking (gas is added to the transaction cost where applicable)

- Tax calculations where gas fees are deductible

Derivatives Dashboard

The derivatives overview under **Derivatives** in the sidebar shows a summary of all derivative positions.

Summary View

- **Total open positions** — Count and notional value

- **P&L summary** — Realized and unrealized P&L across all derivatives

- **Funding rate exposure** — Net funding payments/receipts

- **Margin utilization** — Collateral deployed vs. available

Margin Trading

Manage margin positions under **Derivatives → Margin**.

Position Lifecycle

Event	Accounting Treatment
Open position	Record position at notional value, lock collateral
Add collateral	Transfer from available to margin account
Remove collateral	Transfer from margin to available
Interest accrual	Recognize as finance cost
Close position	Realize P&L, release collateral
Liquidation	Force-close, realize loss, forfeit collateral

Margin Tracking

For each open position, CryptaCount tracks:

- Entry price and current mark-to-market price

- Collateral amount and margin ratio

- Accrued interest (funding costs)

- Unrealized P&L

- Liquidation price threshold

Futures & Options

Track futures and options positions under **Derivatives → Futures & Options**.

Futures

Event	Accounting Treatment
Open futures	Record at contract price
Funding payment	Recognize as income or expense
Close futures	Realize P&L
Settlement	Final settlement of expired contracts

CryptaCount marks futures positions to market each period, recognizing unrealized gains and losses. Funding rate payments are tracked separately.

Options

Event	Accounting Treatment
Buy option	Record premium paid as asset
Sell (write) option	Record premium received as liability
Exercise	Settle at strike price, realize P&L
Expire	Write off premium (buyer) or recognize income (writer)
Assignment	Obligation fulfilled, settle at strike

Derivatives Reports

Three dedicated reports available from the derivatives dashboard:

Report	Description
P&L Report	Realized and unrealized P&L by instrument and period
Funding Report	Futures funding rate payments and receipts over time
Open Positions	Current derivative exposure with mark-to-market values

Restaking

Track restaking positions under **Restaking** in the sidebar.

What Restaking Covers

Feature	Description
Positions	Track restaked ETH across operators and services
Rewards	Rewards earned from securing additional services
Withdrawal queue	Monitor pending unstaking and withdrawal requests

| Slashing | Record slashing events if an operator is penalized |

Governance

Track governance locks and voting under **Governance** in the sidebar.

Governance Tracking

Feature	Description
Lock positions	Tokens locked for voting power (veCRV, veBAL, etc.)
Lock duration	Time-weighted voting power based on lock period
Rewards	Governance rewards and bribes received
Delegation	Voting power delegated to other addresses

Insurance Policies

Track DeFi insurance under **Insurance** in the sidebar.

Insurance Tracking

Feature	Description
Active policies	Current coverage with protocols, amounts, and expiry
Premiums	Premium payments and accrual schedule
Claims	Filed claims and their resolution status
Coverage tokens	Tokens received representing coverage

MEV Analysis

Analyze MEV events under **MEV** in the sidebar.

What MEV Analysis Covers

Maximal Extractable Value (MEV) affects transaction outcomes. CryptaCount identifies and classifies MEV events:

Event	Description
Flash loans	Atomic borrow-and-repay within a single block
Arbitrage	Profit from price discrepancies across venues
Sandwich attacks	Front-running and back-running transactions
Victim losses	Loss incurred from being sandwiched

MEV Summary

The MEV dashboard shows:

- Total MEV profit/loss for the workspace
- Events by category (flash loan, arbitrage, sandwich)
- Transactions affected by MEV attacks
- MEV as a percentage of total transaction value

Accounting Treatment

- **Flash loan borrow/repay** — No net balance change (atomic). Fee recorded as expense.
- **Arbitrage profit** — Recognized as trading income
- **Sandwich front/back** — Profit recognized as trading income for the MEV actor
- **Victim loss** — Recorded as additional cost (slippage) on the affected transaction

DeFi Transactions

Decentralized finance (DeFi) interactions are among the most complex events to account for. CryptaCount provides a dedicated DeFi module with pipeline processing, position tracking, bridge reconciliation, gas fee analysis, and derivatives support.

Availability

The DeFi module is available on qualifying plans. When enabled, the following sections become available in the sidebar:

Sidebar Label	Feature
DeFi → Pipeline	Accounting pipeline — process and review DeFi events
DeFi → Positions	DeFi positions — LP, lending, staking positions
DeFi → Bridges	Bridge tracking — cross-chain transfers
DeFi → Gas Fees	Gas fee analysis and reporting

DeFi Accounting Pipeline

The pipeline under **DeFi → Pipeline** processes DeFi events through a status workflow:

```
PENDING → CLASSIFIED → POSTED (or FAILED / MANUAL_REVIEW /
SKIPPED)
```

Events enter as PENDING, are classified by the engine, and then posted as journal entries. Events that can't be auto-classified go to MANUAL_REVIEW for human intervention.

The pipeline view shows:

- Pending events awaiting classification
- Events in review status needing manual attention
- Status counts per stage
- Multi-leg transaction groups (DeFi operations that span multiple legs)

DeFi Positions

Track active DeFi positions under **DeFi → Positions**:

- **All positions** — Complete list of DeFi positions across protocols

- **Active positions** — Currently open positions

- **LP positions** — Liquidity pool positions with impermanent loss tracking

- **Lending positions** — Deposits and borrows in lending protocols

Position data includes:

- Protocol and pool/vault identifier

- Deposited assets and quantities

- Current value vs. deposited value

- Accumulated rewards

- Rebase token tracking for rebasing assets

DeFi Transaction Types

Swaps (DEX Trading)

Type: SWAP

Trading one token for another on DEXes (Uniswap, SushiSwap, Curve, etc.). The disposal triggers a realized gain/loss on the source token. The destination token is acquired at FMV.

Liquidity Provision

Types: LP_ADD, LP_REMOVE

- **Add:** Deposited assets are transferred to the pool. LP tokens acquired at the combined FMV.

- **Remove:** LP tokens are disposed. Received assets are acquired at current FMV. Difference represents gain/loss (may include impermanent loss).

Staking

Types: STAKE, UNSTAKE, CLAIM_REWARD

- **Stake:** Assets are locked but typically not disposed (still owned). No taxable event in most jurisdictions.
- **Unstake:** Assets unlocked and returned.
- **Claim Reward:** Reward tokens recognized as income at FMV at time of claim.

Lending and Borrowing

Types: BORROW, REPAY, LENDING_DEPOSIT, LENDING_WITHDRAW, LIQUIDATION

- **Lending deposits:** Assets deposited, receipt tokens received
- **Interest earned:** Recognized as income at FMV when claimed
- **Borrowing:** Not income — creates a liability. Repayment reduces the liability.
- **Liquidation:** Forced position closure — recorded with appropriate gain/loss

Wrapping and Unwrapping

Types: WRAP, UNWRAP

Converting between native and wrapped versions (ETH ↔ WETH). Treated as non-taxable conversion — cost basis carries over.

Yield Claims

Type: YIELD_CLAIM

Claiming accumulated yield from DeFi protocols. Recognized as income at FMV at time of claim.

Bridge Transactions

Types: BRIDGE_OUT, BRIDGE_IN

Bridge tracking under **DeFi → Bridges** manages cross-chain asset movements:

- **Stale bridge detection** — Identifies BRIDGE_OUT transactions without matching BRIDGE_IN

- **Resolution** — Manually resolve stale bridges by linking the corresponding transaction on the destination chain
- Cost basis carries over across the bridge. Bridge fees recorded as expenses.

> *Caution: Bridge transactions appear on different chains with different transaction hashes. Ensure both source and destination chain wallets are connected for automatic matching.*

Gas Fee Analysis

Gas fee reporting under **DeFi → Gas Fees** provides:

- Per-wallet gas fee totals
- Gas fees by chain
- Gas fee trends over time
- Gas fees as a percentage of transaction value

This data feeds into the expense categories in financial reports.

Derivatives

CryptaCount supports derivatives accounting with dedicated sections:

Sidebar Label	Feature
Derivatives	Derivatives dashboard — overview of all derivative positions
Derivatives → Margin	Margin positions — open/close, collateral tracking, interest, liquidations
Derivatives → Futures & Options	Futures and options — positions, funding rates, mark-to-market, premium tracking

Margin Trading

Track margin positions with collateral movements, interest accrual, and liquidation events.

Futures & Options

Track futures positions with funding rate payments, mark-to-market valuations, and settlement. Options tracking includes premium, exercise, and expiry events.

Derivatives Reports

- **P&L Report** — Profit and loss across all derivative positions
- **Funding Report** — Futures funding rate payments and receipts
- **Open Positions** — Current derivative exposure summary

Exports

CryptaCount exports accounting data in multiple formats for use in external systems, audit documentation, and regulatory filings. The exports module under **Exports** in the sidebar is the central hub for generating and downloading all exportable data.

Generating an Export

To create a new export:

1. Navigate to **Exports**
2. Select the **export type** — the data set to export
3. Configure **parameters** — date range, wallets, assets, and other filters depending on the export type
4. Choose the **format** — CSV, Excel, or PDF
5. Click **Generate**

Exports run in the background. Large exports (covering many transactions or long date ranges) may take a few minutes to generate. The status indicator shows progress, and completed exports appear in the export history.

Export Types

Transaction Data

Export raw or classified transaction data:

- All transactions for a date range
- Filtered by wallet, chain, asset, or transaction type
- Includes transaction hash, date, type, amount, FMV, cost basis, and classification details

Balance Data

Export balance snapshots:

- Monthly or as-of-date balances

- Per-asset quantities, cost basis, and fair market value

- GL account assignments

Journal Entries

Export the complete journal entry record:

- Double-entry journal lines with debit/credit amounts

- GL account codes and names

- Transaction references and posting dates

- Hash chain verification data

Financial Reports

Export formatted financial statements:

- Trial Balance

- Balance Sheet

- Income Statement

- General Ledger

- Cash Flow Statement

Financial report exports include proper formatting with headers, subtotals, and totals.

Rollforward

Export the five-column rollforward:

- Opening balance, additions, disposals, revaluation, closing balance

- Per-asset detail with GL account breakdown

Reconciliation

Export reconciliation reports:

- Check results and findings

- Resolution status and recommendations

Export Formats

CSV

Plain comma-separated values. Best for:

- Importing into spreadsheet applications

- Feeding into external data pipelines

- Quick data analysis

CSV exports use UTF-8 encoding with headers in the first row.

Excel (XLSX)

Formatted Excel workbooks. Best for:

- Sharing with auditors and stakeholders

- Reports that benefit from formatting (bold headers, number formatting, column widths)

- Multi-sheet exports (e.g., annual report with separate sheets per statement)

Excel exports include:

- Formatted column headers

- Proper number and date formatting

- Sheet names matching the report type

- Frozen header rows for scrolling

PDF

Formatted PDF documents. Best for:

- Formal report presentation

- Audit documentation that shouldn't be easily modified

- Reports requiring specific layout (e.g., tax forms)

Zoho Export

CryptaCount provides a dedicated Zoho Books integration export under **Exports → Zoho**.

Zoho CSV Format

The Zoho export generates CSV files formatted specifically for Zoho Books import:

- **Account mappings** — Maps CryptaCount GL accounts to Zoho chart of accounts codes
- **Journal format** — Exports journal entries in Zoho's expected import format
- **Date formatting** — Uses Zoho-compatible date formats

Configuring Zoho Mappings

Before exporting to Zoho:

1. Navigate to the Zoho export section
2. Map your CryptaCount GL accounts to Zoho account codes
3. Save the mapping configuration

Once configured, subsequent Zoho exports use the saved mapping automatically. Update the mapping if your Zoho chart of accounts changes.

Export History

The exports page maintains a history of all generated exports:

- **Export name** — Type and date range
- **Format** — CSV, Excel, or PDF
- **Generated at** — Timestamp of when the export was created
- **Size** — File size
- **Status** — Generating, Ready, or Expired

Downloading

Click **Download** on any completed export to save the file. Exports are available for download for a limited retention period — download promptly after generation.

Regenerating

If you need an updated version of a previous export (e.g., after correcting classifications), generate a new export with the same parameters. Previous exports are not modified — each generation creates a new file.

> *Tip:* For Acme Digital Holdings' monthly close process, generate exports in this order:

1. **Reconciliation report** (PDF) — Evidence of reconciliation procedures
2. **Journal entries** (Excel) — Complete journal record for the period
3. **Trial balance** (Excel) — Period-end account balances
4. **Financial statements** (PDF) — Balance sheet and income statement
5. **Zoho export** (CSV) — If syncing to Zoho Books for consolidated reporting

Fiat On/Off Ramp Tracking

The fiat ramp module under **Fiat Ramp** in the sidebar tracks the movement of fiat currency into and out of the crypto ecosystem. When Acme Digital Holdings deposits USD to an exchange to purchase crypto, or withdraws EUR from an exchange to a bank account, these movements are captured here.

Why Track Fiat Ramps

Fiat on/off ramps sit at the boundary between traditional banking and crypto — a critical reconciliation point:

- **Audit trail** — Demonstrates the source of funds entering the crypto ecosystem
- **Bank reconciliation** — Matches exchange fiat movements against bank statement entries
- **Completeness** — Ensures all fiat movements are accounted for in financial statements
- **Regulatory compliance** — Many jurisdictions require clear documentation of fiat-to-crypto conversions

Viewing Fiat Ramp Activity

The fiat ramp list shows all tracked fiat movements:

- **Date** — When the deposit or withdrawal occurred
- **Direction** — Deposit (fiat in) or Withdrawal (fiat out)
- **Amount** — Fiat amount and currency (USD, EUR, GBP, etc.)
- **Source / Destination** — Bank account or exchange
- **Status** — Reconciled, Unreconciled, or Pending
- **Reference** — Bank reference number or exchange transaction ID

Adding Fiat Ramp Entries

Automatic Detection

When CEX data is imported (via API or file), fiat deposits and withdrawals are automatically detected and added to the fiat ramp tracker. These appear with the exchange as the source and the fiat currency details populated from the exchange data.

Manual Entry

For fiat movements not captured by exchange imports — such as direct bank-to-bank transfers or off-platform OTC trades:

1. Click **Add Manual Entry**
2. Select **Deposit** or **Withdrawal**
3. Enter the amount and currency
4. Specify the source and destination (bank account name, exchange, etc.)
5. Add a reference number for matching against bank statements
6. Set the date
7. Save

Manual entries are marked as such in the list, distinguishing them from automatically imported records.

Reconciling with Bank Accounts

The core purpose of fiat ramp tracking is reconciliation against bank records.

The Reconciliation Process

1. **Export bank statement** — Download a statement from your bank covering the relevant period
2. **Compare entries** — Match each bank statement line item against fiat ramp entries in CryptaCount
3. **Mark reconciled** — For matched pairs, mark the fiat ramp entry as reconciled
4. **Investigate differences** — Unmatched items need investigation:
    - A bank entry without a CryptaCount record → add a manual entry

- A CryptaCount record without a bank entry → verify the source data
- Amount differences → check for fees or currency conversion differences

Reconciliation Status

Each fiat ramp entry has one of three statuses:

Status	Meaning
Unreconciled	Not yet matched against bank records
Reconciled	Matched and verified against bank statement
Pending	Entry is recent or awaiting bank settlement

Viewing Unreconciled Items

Filter the fiat ramp list to show only unreconciled entries. These are the items that need attention during the reconciliation process. A clean fiat ramp — with all entries reconciled — provides confidence that the boundary between fiat and crypto is fully accounted for.

Integration with Financial Statements

Fiat ramp data feeds into financial reporting:

- **Cash Flow Statement** — Fiat deposits to exchanges appear as investing activities; withdrawals appear as returns from investing
- **Balance Sheet** — Exchange fiat balances are tracked as current assets
- **Reconciliation checks** — The reconciliation module includes fiat ramp coverage in its completeness checks

Tip: Reconcile fiat ramps monthly as part of the standard close process. Waiting until year-end makes it significantly harder to match entries — bank references may no longer be easily accessible, and memory of specific transactions fades.

Fair Market Value & Pricing

Fair Market Value (FMV) is the price at which an asset would change hands between a willing buyer and seller. CryptaCount uses FMV data at multiple granularities and provides dedicated tools for price data management and currency rate tracking.

FMV Granularities

Transaction-time FMV — The market price at the exact timestamp of each transaction. Used for cost basis on acquisitions, proceeds on disposals, and income recognition on rewards. This determines the value recorded in journal entries.

Daily closing rate — The end-of-day price for each asset. Used for balance sheet valuations and FMV columns in the rollforward. The closing rate is the last available price as of 23:59 UTC.

Monthly average rate — The average of daily closing rates over a calendar month. Used for FMV revaluation per IAS 21 methodology.

FMV Sources

The platform sources price data from aggregated market feeds. For each asset and timestamp, the FMV reflects the volume-weighted average across major exchanges.

Price data provides:

- **Live prices** — Current market prices for all tracked assets
- **Historical prices** — Price at any historical timestamp
- **Price search** — Find price data for specific tokens
- **Market overview** — Trending assets and market summary
- **Coverage analysis** — Which assets have price data and which have gaps

Price Sync Schedule

- Crypto prices are synced daily at 00:05 UTC
- FX rates are synced at 6 PM Monday through Friday

- On-demand backfill is available for historical gaps

Multi-Currency FMV

All FMV data is stored in both USD (the primary pricing currency for crypto markets) and translated to the workspace's base reporting currency:

- **FMV (USD)** — Direct market price in US dollars
- **FMV (base currency)** — Translated using the applicable FX rate:
    - Transaction-time FMV uses the FX rate at the transaction timestamp
    - Daily closing FMV uses the daily closing FX rate
    - Monthly average uses the monthly average FX rate

Currency Rates

View fiat exchange rate data under **Currency Rates** in the sidebar:

- **Current rates** — Today's exchange rates between fiat currencies
- **Historical rates** — Rates for any historical date
- **Batch rates** — Bulk lookup for multiple currency pairs and dates
- **Daily/Monthly aggregates** — Average rates over periods
- **Pegged currencies** — Track currencies pegged to major pairs (e.g., stablecoins pegged to USD)

Rate data supports sync and backfill operations for filling historical gaps.

Price Health Monitoring

Price health monitoring (available on qualifying plans) under **Price Health** in the sidebar monitors the reliability and completeness of price data:

- **Status dashboard** — Overall health of price data across the workspace
- **Alerts** — Flagged assets with missing, stale, or suspicious price data
- **Audit** — Detailed log of price data sources and quality metrics

Missing prices for workspace assets can be identified and backfilled via the workspace-level price tools.

Viewing FMV Data

In transactions: Each transaction's detail view shows the FMV at the time of the event.

In the asset detail: Navigate to any asset to see its price history.

In reports: All reports display FMV-based columns where applicable (rollforward, balance sheet, unrealized gains/losses).

FMV and Cost Basis

FMV is distinct from cost basis:

- **Cost basis** = what you paid for the asset (historical cost)
- **FMV** = what the asset is worth now (current market value)
- **Unrealized gain/loss** = FMV − Cost basis (for assets still held)
- **Realized gain/loss** = Proceeds − Cost basis (for assets disposed)

The cost basis method (Historic FIFO, Historic Weighted Average, etc.) determines *which* cost is used when disposing of an asset. FMV provides the current valuation for marking to market.

Gains & Losses

Gain and loss calculations are the primary output of the cost basis engine. They determine the tax-relevant amounts for each disposal event and the mark-to-market position for assets still held.

Where Gains & Losses Appear

Gains and losses are reported through several views:

Sidebar Location	Content
Reports → Income Statement	Income statement including realized gains/losses and income
Tax → Disposals	Tax disposal schedule — detailed per-disposal gain/loss (available on qualifying plans)
Balances → Rollforward	Rollforward showing movement from opening to closing balance
Balances → Lots	Lot-level detail showing acquisition cost and remaining quantity

Realized Gains & Losses

A realized gain or loss occurs when you dispose of an asset — selling it, trading it for another asset, or using it to pay for goods or services.

Calculation: Proceeds − Cost Basis = Realized Gain (or Loss)

The **proceeds** are the FMV of what you received at the time of disposal. The **cost basis** is determined by the selected method (Historic FIFO, Historic Weighted Average, HIFO, LIFO, etc.).

Example (Historic FIFO): You bought 2 ETH at €1,800 (January) and 3 ETH at €2,400 (March). You sell 1 ETH in June at €2,600. Under FIFO, the oldest lot is used: Proceeds €2,600 − Cost €1,800 = **€800 realized gain**.

Example (Historic Weighted Average): Same purchases. Weighted average cost = (2 × 1800 + 3 × 2400) / 5 = €2,160. Selling 1 ETH at €2,600: Proceeds €2,600 − Cost €2,160 = **€440 realized gain**.

Unrealized Gains & Losses

Unrealized gains represent the paper profit or loss on assets you still hold.

Calculation: Current FMV − Cost Basis = Unrealized Gain (or Loss)

These are computed at any point in time for reporting purposes. Under the FMV cost basis method, unrealized gains are recognized in the income statement. Under historic cost methods (Historic FIFO, Historic Weighted Average), they are informational only.

Tax Disposals

The tax disposals view under **Tax → Disposals** (available on qualifying plans) provides:

- Every disposal event with calculated gain/loss
- Lot matching showing which acquisition lots were used
- Holding period for each disposal (short-term vs. long-term)
- Summary totals for tax reporting
- Export in formats required by tax authorities

Holding Period Classification

Many jurisdictions distinguish between short-term and long-term capital gains:

Jurisdiction	Short-Term	Long-Term	Threshold
United States	Ordinary income rates	0%/15%/20%	1 year
Germany	Taxable	Tax-free	1 year (with €600 exemption)
Australia	Full rate	50% CGT discount	12 months
Portugal	28%	Tax-free	1 year

CryptaCount tracks acquisition dates at the lot level and classifies gains based on the workspace's jurisdiction profile.

Income Events

Some transaction types generate income rather than capital gains:

Type	Treatment	FMV at Time of Receipt
STAKING_REWARD	Income	Yes — recorded as income at receipt FMV
MINING_REWARD	Income	Yes — recorded as income at receipt FMV
VALIDATOR_REWARD	Income	Yes — recorded as income at receipt FMV
AIRDROP	Income (in most jurisdictions)	Yes — recorded at FMV of airdrop
INCOME	Income	Yes
YIELD_CLAIM	Income	Yes — DeFi yield at claim time

The received assets enter the cost basis pool at the FMV recorded as income. If later disposed, the gain/loss is calculated from that income-recognized cost basis.

Method Comparison

You can compare gains outcomes across different cost basis methods. This is valuable for:

- **Tax planning** — Which method produces the most favorable result where the jurisdiction allows a choice?
- **Sensitivity analysis** — How much does the method choice affect total gains?
- **Audit evidence** — Demonstrating that the selected method is reasonable

Reports

Navigate to **Reports** in the sidebar to generate the key financial reports:

- **Reports → Income Statement** — Revenue, expenses, gains/losses, net income
- **Reports → General Ledger** — Full journal entry detail
- **Reports → Trial Balance** — Account balances at a point in time

Each report can be filtered by date range, wallet, and asset, and exported as CSV or Excel.

Impairment Testing

Impairment testing evaluates whether the carrying value of digital assets exceeds their recoverable amount. CryptaCount supports multiple impairment models aligned with different accounting standards and cost basis methods.

Why Impairment Matters

Digital assets are volatile. Under most accounting frameworks, if the fair market value of an asset drops below its carrying cost, the entity must recognize an impairment loss. The rules for when (and whether) that loss can be reversed depend on the accounting standard and cost basis method in use.

Example: *Acme Digital Holdings* acquired 10 ETH at €3,200 each (carrying value €32,000). At period end, ETH trades at €2,800. The fair value is €28,000 — an unrealized loss of €4,000 that may need to be recognized as impairment.

Running an Impairment Test

Navigate to **Accounting → Impairment** to run tests:

1. **Select the period** — Choose the accounting period to test
2. **Run test** — CryptaCount evaluates every asset position against current market prices
3. **Review results** — Each asset shows:
   - Carrying value (cost basis per the selected method)
   - Fair market value at period end
   - Impairment amount (if carrying value exceeds FMV)
   - Prior impairment already recognized
   - Net adjustment required

Results are broken down by asset, wallet, and GL account.

Impairment Models

CryptaCount applies different impairment logic based on the workspace's cost basis method:

One-Way Impairment (Write-Down Only)

Applies to: Historic FIFO, LIFO, HIFO, Specific Identification

Under one-way impairment, losses are recognized when FMV drops below carrying value, but **reversals are not permitted**. Once an asset is written down, the new lower value becomes the cost basis going forward.

This aligns with US GAAP treatment of indefinite-lived intangible assets and fair value guidance where impairment is permanent until disposal.

Condition	Action
FMV < Carrying Value	Recognize impairment loss
FMV > Carrying Value (after prior write-down)	No reversal — carry at written-down value
FMV > Original Cost	No adjustment — carry at original cost

Journal entry for impairment:

Account	Debit	Credit
Impairment Loss — ETH	€4,000	
Digital Assets — ETH		€4,000

Two-Way Impairment (Write-Down & Reversal)

Applies to: NRV + FIFO, NRV + Weighted Average

Under two-way impairment (Net Realizable Value methods), losses are recognized when FMV drops below carrying value, and **reversals are permitted** when FMV recovers — but only up to the original cost basis, never above it.

This aligns with IFRS treatment of inventory (IAS 2) where write-downs to NRV are reversed when the circumstances that caused the write-down no longer exist.

Condition	Action
FMV < Carrying Value	Recognize impairment loss (write down to NRV)
FMV > Carrying Value (after prior write-down)	Reverse impairment, up to original cost

| FMV > Original Cost | Carry at original cost — no write-up beyond cost |

Journal entry for reversal:

Account	Debit	Credit
Digital Assets — ETH	€2,000	
Impairment Reversal — ETH		€2,000

Fair Market Value (Mark-to-Market)

Applies to: FMV

Under the FMV method, assets are carried at fair value each period. Unrealized gains and losses are recognized in the income statement. There is no separate "impairment" concept — all value changes flow through the P&L as they occur.

Weighted Average (No Impairment)

Applies to: Historic Weighted Average

The weighted average cost method does not apply impairment. The cost pool is continuously reweighted as new acquisitions occur.

Reviewing Results

The impairment results view shows:

Column	Description
Asset	Token symbol and name
Quantity	Total held quantity
Carrying Value	Current book value per the cost basis method
Fair Value	Market value at the test date
Impairment	Loss amount to recognize (or reversal for NRV methods)
Prior Impairment	Cumulative impairment already recognized

Net Adjustment	Amount to post in this period

Assets with no impairment (FMV ≥ carrying value under one-way methods) show zero adjustment.

Posting Impairment Entries

After reviewing results:

1. Confirm the impairment amounts are reasonable
2. Click **Post Impairment Entries**
3. CryptaCount generates journal entries for each asset requiring adjustment
4. Entries are posted to the impairment loss (or reversal) GL accounts

Posted impairment entries appear in the journal ledger and are included in the period close checks.

> *Note: Impairment tests should be run **before** the period close workflow. The period close checks verify that impairment has been assessed for the period.*

Lot-Level Impairment

For lot-based methods (FIFO, LIFO, HIFO, Specific Identification), impairment is assessed at the individual lot level:

- Each lot's carrying value is compared against the current FMV
- Lots acquired at different prices may have different impairment amounts
- The lot viewer under **Balances** → **Lots** shows per-lot impairment status

Example: *Acme Digital Holdings* holds two ETH lots:

Lot	Quantity	Cost Basis	FMV	Impairment
Lot 1 (Jan purchase)	5 ETH	€3,200/ETH	€2,800/ETH	€2,000
Lot 2 (Mar purchase)	5 ETH	€2,600/ETH	€2,800/ETH	€0

Lot 2 has no impairment because FMV exceeds its cost basis.

Integrations

CryptaCount integrates with accounting platforms and supports centralized exchange (CEX) connections for trade data import. Manage integrations under **Settings → Integrations**.

Accounting Platform Connections

CryptaCount connects to accounting platforms for both sign-in and data synchronization:

Provider	Sign-In	Data Sync
Google	✓	—
Microsoft	✓	—
Xero	✓	✓ Accounting data sync
Intuit (QuickBooks)	✓	✓ Accounting data sync
Zoho	✓	✓ Accounting data sync

Connecting an Accounting Platform

1. Navigate to **Settings → Integrations**

2. Click **Connect** next to the desired platform

3. You'll be redirected to the platform's authorization screen

4. Authorize CryptaCount to access your accounting data

5. Select which organization/company to connect (if applicable)

6. Done — the integration is active

> *Note: CryptaCount requests read and write access for journal synchronization. It does not access bank accounts, payment methods, or payroll data.*

What Accounting Integrations Do

Once connected, you can:

- **Push journal entries** — Send generated journal entries directly to your general ledger
- **Sync chart of accounts** — Import your existing chart of accounts
- **Reconcile** — Compare CryptaCount's data against your existing general ledger
- **Disconnect** — Revoke access without deleting data

Zoho Export Support

For Zoho Books users, dedicated export functionality under **Exports → Zoho** provides:

- CSV exports formatted for Zoho Books import
- Account mapping between CryptaCount and Zoho chart of accounts

CEX Connections

Centralized exchange connections under **CEX** in the sidebar import trade data from major exchanges:

Sidebar Label	Purpose
CEX	CEX account management — connect and manage exchange connections
CEX Transactions	View CEX transactions — trades, deposits, withdrawals
CEX Import	Import CEX data — via API, CSV, XLS, PDF, or generic import
CEX GL Mappings	Map CEX transaction types to GL accounts
CEX Transfer Matching	Match CEX transfers with on-chain transactions

Setting Up a CEX Connection

1. Go to **CEX** in the sidebar
2. Click **Add Exchange** and select your exchange
3. **API connection:** Generate a read-only API key on the exchange and enter it in CryptaCount
4. **CSV import:** Upload trade history exports from the exchange

5. Start sync

> *Tip:* *Always use read-only API keys. CryptaCount never needs write access to your exchange account.*

CEX Import Options

The import tool supports multiple methods:

- **Exchange-specific API** — Direct integration per exchange
- **Exchange-specific CSV** — Pre-formatted CSV templates per exchange
- **Generic CSV** — Flexible CSV import with column mapping
- **XLS import** — Excel file import
- **PDF import** — Statement PDF parsing
- **Preview** — Review imported data before committing

CEX GL Mappings

Configure under **CEX GL Mappings** how CEX transactions map to your chart of accounts:

- Set default GL accounts per transaction type
- Override mappings for specific exchanges
- Automatically post CEX transactions as journal entries

Fiat Ramp Tracking

Fiat on/off ramp tracking under **Fiat Ramp** in the sidebar:

- Track fiat deposits and withdrawals through crypto exchanges
- Manual entry for OTC transactions
- Match unreconciled fiat movements with on-chain transactions

Disconnecting

To disconnect an integration, navigate to **Settings → Integrations**, click the connected platform, and select **Disconnect**. This revokes CryptaCount's access token. No data is deleted from either platform.

Journal Entries & Generation

Journal entries are the atomic records of CryptaCount's double-entry bookkeeping system. Every balance change — whether from an on-chain transaction, a CEX trade, or a manual adjustment — is expressed as a journal entry with balanced debits and credits.

Viewing Journal Entries

Navigate to **Accounting → Journal Entries** to browse the full journal ledger.

Ledger View

The journal ledger displays entries in reverse chronological order with:

- **Entry date** — When the economic event occurred
- **Posted date** — When the entry was posted to the ledger
- **Reference** — Source transaction hash, CEX trade ID, or manual reference
- **Description** — Auto-generated or user-provided narrative
- **Accounts** — Debit and credit GL accounts with amounts
- **Status** — Draft, Posted, or Reversed
- **Hash** — Truncated hash for chain verification

Filtering & Search

Filter journal entries by:

Filter	Options
Date range	Custom start/end dates
GL account	Specific account or account type
Status	Draft, Posted, Reversed
Transaction type	Source transaction classification
Amount range	Min/max amounts

| Reference | Free-text search on reference field |

Search supports partial matching on descriptions and references. Results can be exported to CSV or Excel.

Journal Entry Detail

Click any entry to view its full detail:

Each entry shows:

- **Header** — Date, reference, description, status, created-by user
- **Lines** — Each debit and credit line with GL account, amount, and optional memo
- **Source** — Link to the originating transaction (if auto-generated)
- **Hash chain** — Current entry hash plus link to predecessor
- **Audit trail** — Who created, posted, or reversed the entry and when
- **Attachments** — Any supporting documents linked via audit attachments

Creating Manual Entries

To create a journal entry manually:

1. Click **New Entry**
2. Set the entry date and description
3. Add debit lines — select GL account, enter amount, optional memo
4. Add credit lines — total credits must equal total debits
5. Save as **Draft** or **Post** immediately

Example: *Acme Digital Holdings* records a year-end accrual:

Account	Debit	Credit
Accrued Expenses — Audit Fees	€15,000	
Accounts Payable		€15,000

Posting Draft Entries

Draft entries do not affect account balances until posted. To post:

1. Open the draft entry

2. Review the lines

3. Click **Post**

4. The entry is assigned a hash, linked into the hash chain, and account balances update

Posting is irreversible in the sense that the entry cannot be edited after posting. To correct a posted entry, reverse it and create a new entry.

Reversing Entries

Reverse a posted entry to undo its effect:

1. Open the posted entry

2. Click **Reverse**

3. CryptaCount creates a new entry with all debits and credits swapped

4. Both the original and reversal entries are linked for audit trail

The reversal entry carries a reference to the original entry (e.g., "Reversal of JE-00412"). Both entries remain in the ledger — nothing is deleted.

Reassigning GL Accounts

If journal entries were posted to incorrect GL accounts:

1. Navigate to **Balances → Reassign GL**

2. Select the entries to reassign

3. Choose the correct GL accounts

4. CryptaCount generates reversal and re-posting entries automatically

Tamper-Evident Journal Hashing

CryptaCount implements a cryptographic hash chain across journal entries to ensure ledger integrity.

How It Works

Each journal entry's hash is computed from:

- The entry's date, lines (accounts, amounts), description, and metadata

- The hash of the **previous** journal entry in the chain

This creates a linked chain: modifying any historical entry changes its hash, which breaks the chain for all subsequent entries.

Verification

The hash chain is verified during:

- **Period close checks** — The close workflow includes a hash chain integrity check
- **On-demand verification** — Run hash chain verification from the accounting pipeline
- **Reconciliation** — The full reconciliation suite includes ledger replay with hash verification

A broken hash chain indicates that an entry was modified outside the normal workflow — a critical audit finding.

> *Tip:* The hash chain provides tamper evidence, not tamper prevention. It ensures that any unauthorized change is immediately detectable during the next verification cycle.

Generate & Migrate Journals

The journal generation tool under **Accounting → Generate Journals** handles batch processing for scenarios where journals need to be created or recreated in bulk.

Use Cases

Scenario	Description
Historical migration	Generate journals for transactions that predate the accounting pipeline setup
Rule changes	Regenerate journals after modifying accounting rules to apply new classifications
Bulk re-posting	Reprocess a date range after correcting GL mappings or cost basis settings
System migration	Generate CryptaCount journals from data imported from another platform

Running a Generation

1. Navigate to **Accounting → Generate Journals**

2. Select the scope:

- **Date range** — Process all transactions within the specified dates

- **Wallet** — Process only transactions for specific wallets

- **Transaction type** — Limit to specific transaction classifications

3. Click **Start Generation**

4. Monitor progress in the status panel:

- Transactions processed / total

- Journals created

- Errors encountered

5. Review any errors before completing

Controls

Action	Description
Start	Begin journal generation for the selected scope
Cancel	Stop an in-progress generation (already-created journals are retained)
Cleanup	Remove journals created by a cancelled or failed generation run
Purge	Remove all generated journals for the selected scope (use before re-running)

Status Tracking

The generation tool tracks:

- Total transactions in scope

- Transactions processed

- Journals successfully created

- Transactions skipped (already have journals)

- Errors with details

Generation runs are recorded with start/end timestamps and can be reviewed in the activity log.

Caution: Journal generation for large date ranges can take significant time. The process runs in the background — you can navigate away and return to check progress. Do not close the period

being processed while generation is in progress.

Practice Mode (Audit Firms)

Practice mode transforms CryptaCount from a single-company tool into a multi-client platform for audit firms, accounting practices, and tax advisory firms. Practice users manage multiple client workspaces from a centralized dashboard with dedicated billing and sharing controls.

Who Uses Practice Mode

Practice mode is for organizations that manage crypto accounting or auditing for multiple external clients:

User Type	Typical Activities
Accounting firms	Bookkeeping, period close, financial reporting for clients
Audit firms	Reviewing client records, running reconciliations, verifying balances
Tax advisory firms	Preparing tax calculations and filings for client entities
Managed service providers	Full-service crypto accounting outsourcing

Account Type

Practice mode is activated during registration by selecting the **Practice** account type. This grants access to the practice dashboard and multi-client management features.

Client Management

Manage clients under **Practice → Clients**.

Adding Clients

There are two paths to adding a client workspace:

Client creates their own account:

1. The client registers on CryptaCount with a Business account
2. The client navigates to **Settings → External Access**

3. The client invites the practice by email

4. The practice accepts the invitation — the client's workspace appears under **Practice →
Clients**

Practice creates a workspace for the client:

1. Navigate to **Practice → Clients**

2. Click **New Client**

3. Enter the client company name and details

4. A new workspace is created under the practice's management

5. Optionally invite the client to view their own workspace

Client Dashboard

The client list shows:

Column	Description
Client name	Company name
Workspaces	Number of workspaces managed
Status	Active, onboarding, archived
Last activity	Most recent action in any workspace
Period status	Current accounting period state (open/closing/closed)
Subscription	Client's billing plan

Switching Between Clients

Click any client row to enter their workspace. The sidebar and all features operate within that client's context. The practice banner at the top confirms which client workspace is active and provides a quick-switch dropdown.

Client Access Levels

Practice users have configurable access to each client workspace:

Access Level	Capabilities

Full access	All features including settings, user management, and billing
Accounting access	Transactions, journals, balances, reports, period close
View-only	Read-only access to all data — no modifications
Audit access	Read-only plus reconciliation and attestation tools

Practice Billing

Manage practice-level billing under **Practice → Billing**.

Billing Model

Practice accounts have a different billing structure from standard business accounts:

Feature	Business Account	Practice Account
Billing unit	Per workspace	Per client workspace (volume pricing)
Plan selection	Self-service	Practice admin assigns plans per client
Invoicing	Auto-billing	Consolidated invoice or per-client
Payment	Client pays directly	Practice pays for clients (pass-through optional)

Managing Client Subscriptions

1. Navigate to **Practice → Billing**

2. View the billing overview:
   - Total monthly cost across all clients
   - Per-client billing breakdown
   - Feature usage by client

3. Assign or change plans per client

4. View invoices and payment history

Volume Pricing

Practice accounts qualify for volume discounts based on total managed workspaces:

Tier	Workspaces	Discount
Starter	1–5	—
Growth	6–20	10%
Professional	21–50	20%
Enterprise	51+	Custom

Pass-Through Billing

Practices can optionally enable pass-through billing, where CryptaCount bills each client directly. The practice retains administrative control but the client sees and pays their own invoice.

Shared Workspaces

View workspaces shared with the practice under **Practice → Shared**.

How Sharing Works

When a client shares their workspace with a practice:

1. The workspace appears under **Practice → Shared**
2. The practice gains access at the level specified by the client (view-only, accounting, full)
3. All actions performed by practice users are logged in the client's audit trail with the practice user's identity
4. The client can revoke access at any time from **Settings → External Access**

Shared vs. Managed

Aspect	Shared Workspace	Managed Workspace
Owner	Client	Practice
Billing	Client pays	Practice pays
Access control	Client grants/revokes	Practice controls
Workspace creation	Client created	Practice created

Auditor vs. Accountant Workflow

Practice mode supports two primary workflow patterns:

Accountant Workflow (Ongoing Bookkeeping)

Typical monthly cycle for an accounting firm managing a client:

1. **Week 1** — Sync wallets, import CEX transactions, reconcile fiat
2. **Week 2** — Review and classify transactions, resolve manual review items
3. **Week 3** — Calculate balances, run impairment tests, create manual adjustments
4. **Week 4** — Period close workflow, generate financial reports, deliver to client

Example: *Acme Digital Holdings* outsources monthly bookkeeping to Baker & Associates, a crypto accounting practice. Baker & Associates logs into their practice dashboard, switches to the Acme workspace, runs the monthly close workflow, and delivers the trial balance and income statement by the 15th of each month.

Auditor Workflow (Periodic Audit)

Typical engagement for an audit firm:

1. **Planning** — Review client's accounting policies, assess risk areas
2. **Fieldwork:**
   - Run proof of reserves attestation
   - Verify address screening results
   - Replay reconciliation checks
   - Review journal hash chain integrity
   - Sample test manual adjustments and their approvals
   - Verify period close check results and waivers
3. **Reporting** — Export supporting evidence, document findings
4. **Follow-up** — Track remediation of findings

Audit workflows use **view-only** or **audit access** levels to ensure the auditor cannot modify client data.

Separation of Duties

Practice mode enforces separation:

- Practice users are identified separately from client users in the audit trail

- Practice user actions carry the practice organization's identity

- Permission changes are logged

- Access grants and revocations are timestamped

Settings for Practice Users

Some settings behave differently for practice accounts:

Setting	Behavior
Billing	Hidden from Settings sidebar — use **Practice → Billing** instead
External Access	Manages which clients have shared their workspace
Workspace Accounting	Accessible per-client workspace
Profile	Practice user's own profile

Partner Referral Program

Practice accounts have access to a partner referral dashboard for tracking referrals and earning rewards.

Reconciliation

Reconciliation is the process of verifying that your accounting data is complete, consistent, and matches external sources. CryptaCount provides 12 automated workspace checks that cover everything from address mappings to double-entry integrity.

Reconciliation Dashboard

The dashboard under **Reconciliation** in the sidebar shows the current state of all workspace checks.

Each check displays:

- **Check name** — What is being verified
- **Status** — Pass, Fail, Warning, or Not Run
- **Last run** — When this check was most recently executed
- **Findings count** — Number of issues found (if any)

The 12 Workspace Checks

1. Unmapped Addresses

What it checks: Finds transaction addresses that don't have a GL account mapping.

Why it matters: Unmapped addresses mean transactions can't be properly journalized. If an address appears in your transaction data but has no GL mapping, journal entries for those transactions will be incomplete or missing.

Resolution: Add the address as an internal or external wallet with a GL mapping, or assign a GL account to the existing wallet.

2. Transaction Counts

What it checks: Compares expected transaction counts (from blockchain data and CEX imports) against actual recorded transactions.

Why it matters: A mismatch indicates missing data — transactions that should have been imported but weren't. This can happen due to sync failures, import errors, or incomplete pulls.

Resolution: Re-sync affected wallets or re-import CEX data for the missing periods.

3. Opening / Closing Balances

What it checks: Verifies that the closing balance of one period equals the opening balance of the next.

Why it matters: A break in the opening/closing chain means something changed between period boundaries — a late-arriving transaction, a recalculation, or a manual adjustment that wasn't properly propagated.

Resolution: Recalculate balances for the affected periods. If the discrepancy persists, check for transactions with timestamps that fall between period boundaries.

4. Internal Transfers

What it checks: Verifies that internal transfers between your own wallets are properly matched and net to zero.

Why it matters: An unmatched internal transfer inflates both outflows and inflows, distorting your financial statements. Every TRANSFER_OUT from one of your wallets to another of your wallets should have a corresponding TRANSFER_IN.

Resolution: Use the CEX Transfer Matching tool for CEX-to-wallet transfers, or classify matched pairs as INTERNAL_TRANSFER.

5. Fees

What it checks: Validates that gas fees and trading fees are properly recorded and classified.

Why it matters: Missing fee transactions understate expenses. Misclassified fees (e.g., a gas fee recorded as a transfer) distort reporting categories.

Resolution: Review flagged fee transactions and correct their classification.

6. Price Availability

What it checks: Identifies transactions and balance dates where price data is missing.

Why it matters: Without a price, CryptaCount cannot compute fair market value for the transaction or balance. This affects FMV calculations, realized gain/loss, and impairment testing.

Resolution: Missing prices may resolve with a price backfill. For obscure or low-liquidity tokens, manual price entry may be required.

7. CEX Matching

What it checks: Verifies that CEX deposits and withdrawals are matched with on-chain wallet movements.

Why it matters: Unmatched CEX transfers cause double-counting — the same economic event appears as both an exchange transaction and a wallet transaction.

Resolution: Use the Transfer Matching tool to link unmatched pairs.

8. Double Entry

What it checks: Validates that every journal entry has balanced debits and credits.

Why it matters: An unbalanced journal entry violates the fundamental accounting equation. This check catches corrupted or partially-posted entries.

Resolution: Review and correct the flagged journal entries. Re-post from the source transaction if needed.

9. Ledger Replay

What it checks: Replays the journal entry sequence and verifies that the resulting balances match the computed balances.

Why it matters: This is a comprehensive integrity check. If replaying journals from scratch produces different balances than the stored calculations, something in the data pipeline is inconsistent.

Resolution: This typically indicates a data issue. Export the findings and investigate the specific assets and periods where replay differs from stored values.

10. Integrity

What it checks: Runs data integrity validation across the full workspace — referential integrity, hash chain verification on the general ledger, and consistency between related entities.

Why it matters: Catches low-level data issues that other checks miss — orphaned records, broken references, and tampered ledger entries.

Resolution: Integrity failures should be investigated promptly. The findings detail which specific records failed validation.

11. Balance vs. Blockchain

This check compares your computed on-chain balances against live blockchain data.

What it checks: Queries current on-chain balances for each wallet and compares against CryptaCount's calculated holdings.

Why it matters: A mismatch means either transactions are missing from your data (sync gap) or transactions are incorrectly classified (e.g., a TRANSFER_IN that should be a SWAP).

Resolution: Re-sync the affected wallet. If the discrepancy persists after sync, investigate individual transactions during the mismatched period.

12. Hierarchy Reconciliation

What it checks: Verifies that balances roll up correctly through the GL account hierarchy — sub-accounts sum to their parent accounts.

Why it matters: Ensures report totals are consistent. A broken hierarchy means your balance sheet or trial balance totals don't match the sum of their line items.

Resolution: Review the GL account tree and correct any misconfigured parent/child relationships.

Running Reconciliation

Individual Checks

Run any single check from the reconciliation dashboard by clicking **Run** next to the check name. Results appear within seconds for most checks; ledger replay and integrity checks may take longer for large workspaces.

Full Reconciliation

Click **Run Full Reconciliation** to execute all 12 checks in sequence. This produces a comprehensive reconciliation report that is saved for audit trail purposes.

A full reconciliation is recommended:

- At the end of each accounting period before closing
- After importing large batches of new data
- After making bulk classification or GL mapping changes
- Before generating financial statements for external use

Reconciliation Reports

View completed reports under **Reconciliation** → **Reports**.

Each report shows:

- **Run date** — When the reconciliation was executed
- **Type** — Full reconciliation or individual check
- **Status** — Pass (all checks passed), Warning (some issues), or Fail (critical issues found)
- **Findings** — Total number of issues across all checks

Report Details

Click a report to view its full findings:

- **Summary** — Pass/fail status for each check with finding counts
- **Findings list** — Individual issues with description, affected entity, and severity
- **Recommendations** — Suggested resolution for each finding

Exporting Reports

Reconciliation reports can be exported for external audit use. The export includes:

- Full findings detail
- Check methodology descriptions
- Resolution status for previously addressed findings

- Timestamp and workspace identification

This export is essential for audit documentation — it provides evidence that reconciliation procedures were performed and their results.

:::tip[Period-End Workflow] The recommended period-end sequence for Acme Digital Holdings (or any workspace) is:

1. **Sync** all wallets and import latest CEX data

2. **Classify** any transactions in the review queue

3. **Match** CEX transfers with on-chain movements

4. **Calculate** balances for the period

5. **Reconcile** — run full reconciliation and resolve all findings

6. **Report** — generate financial statements

7. **Close** the accounting period

Reporting & Exports

CryptaCount's reporting engine produces structured financial outputs from your accounting data. All reports are generated on demand from live data — there are no stale cached reports.

Financial Reports

Five financial reports are available from the **Reports** section in the sidebar:

Report	Purpose
General Ledger	Complete journal entry record with hash chain verification
Trial Balance	Debit/credit balances for all GL accounts at a point in time
Balance Sheet	Assets, liabilities, and equity at a specific date
Income Statement	Revenue, expenses, gains/losses, and net income for a period
Cash Flow	Cash and crypto flow categorized by operating, investing, and financing activities

General Ledger

Balance Sheet

Cash Flow

Report Configuration

All reports share common configuration options:

- **Date range** — Predefined period (this month, this quarter, YTD, last year) or custom dates

- **Wallets** — All wallets or a selected subset

- **Assets** — All assets or filtered to specific ones

- **Cost basis method** — Defaults to workspace setting; override for comparison

- **Currency** — Reports display in your base currency with USD also shown

Additional Report Capabilities

- **Inventory Valuation** — Asset inventory with cost and FMV comparison
- **Gas Fee Report** — Per-workspace gas fee analysis
- **Annual Report** — Excel export combining all financial statements

Reconciliation

The reconciliation module under **Reconciliation** in the sidebar provides comprehensive data verification:

Sidebar Label	Purpose
Reconciliation	Dashboard — overview of all checks
Reconciliation → Reports	Reconciliation report list and detailed findings

Reconciliation checks include:

- **Balance vs. blockchain** — Compare computed balances against on-chain data
- **Hierarchy reconciliation** — Verify rollup consistency across the account hierarchy
- **Unmapped addresses** — Find transaction addresses without GL mappings
- **Transaction counts** — Verify expected vs. actual transaction volumes
- **Opening/closing balance** — Validate period transitions
- **Internal transfers** — Match internal transfer pairs
- **Fee verification** — Verify fee calculations
- **Price availability** — Check for missing price data
- **CEX matching** — Verify CEX transaction matching
- **Double-entry validation** — Ensure all journals balance
- **Ledger replay** — Replay transactions to verify journal integrity
- **Data integrity** — Hash chain and data consistency checks

Full reconciliation runs produce exportable reports with difference details.

Exports

The **Exports** section in the sidebar provides:

- **Generate exports** — Create CSV, Excel, or PDF exports of any report
- **Export history** — View previously generated exports
- **Download** — Download generated export files

Zoho Export

For Zoho Books users, dedicated Zoho export functionality under **Exports → Zoho** provides:

- CSV exports formatted for Zoho Books import
- Account mapping between CryptaCount and Zoho chart of accounts

Export Formats

Format	Best For
CSV	Importing into other tools, data analysis, ERP integration
Excel (.xlsx)	Client delivery, formatted workbooks with summary rows
PDF	Formal deliverables, audit documentation, filing

Tip: For clients who use Excel-based workflows, the .xlsx export includes formatted headers, column widths, and summary rows — ready for client delivery without additional formatting.

Revenue Contract Rules

Revenue contract rules under **Revenue Rules** in the sidebar define how CryptaCount classifies incoming transactions as revenue. These rules automate the distinction between different revenue streams — staking rewards, validator fees, protocol income, service revenue — so transactions are posted to the correct GL accounts without manual review.

Why Revenue Rules Matter

Crypto entities often receive multiple types of income through the same wallet addresses:

- **Staking rewards** from validator operations
- **Protocol fees** from DeFi protocol ownership
- **Service revenue** from SaaS or infrastructure services paid in crypto
- **Airdrops** which may or may not constitute revenue depending on jurisdiction
- **Yield** from lending or liquidity provision

Without rules, all incoming tokens default to a generic classification. Revenue rules apply business logic to distinguish these categories automatically, ensuring:

- Correct GL account posting (different revenue types → different accounts)
- Accurate income statement categorization
- Proper tax treatment (revenue recognition timing may differ by category)
- Audit-ready classification with documented rules

Creating a Rule

To create a new revenue classification rule:

1. Navigate to **Revenue Rules**
2. Click **Create Rule**
3. Configure the rule criteria:

Rule Criteria

Field	Description
Name	Descriptive label (e.g., "Ethereum Staking Rewards — Acme Digital Holdings")
Asset	Which token or coin this rule applies to (e.g., ETH)
Transaction type	Match specific types (STAKING_REWARD, CLAIM_REWARD, etc.)
Source address	Match transactions from specific sender addresses (e.g., a known staking contract)
Amount range	Optional minimum/maximum amount filter
Wallet	Optionally restrict to specific wallets

Rule Action

When a transaction matches the criteria, the rule assigns:

- **Revenue classification** — The specific revenue category (operating revenue, staking income, protocol fees, etc.)
- **GL account** — Which ledger account to post to
- **Economic intent** — INCOME, OPERATIONAL, INVESTMENT, etc.

4. **Save** the rule

Testing Rules

Before activating a rule, test it against your existing transaction data:

1. From the rule detail view, click **Test Rule**
2. The system evaluates the rule criteria against all workspace transactions
3. Results show:
   - **Matched transactions** — How many existing transactions would be classified by this rule
   - **Sample matches** — A preview of matched transactions with their proposed classification
   - **Conflicts** — Transactions that match this rule AND another existing rule

Test Before Activate

Testing is strongly recommended before enabling a new rule. A rule with overly broad criteria can misclassify transactions at scale. Review the test results to verify:

- The match count is reasonable (not unexpectedly high or low)
- Sample transactions are genuinely the type you intend to classify
- No conflicts with higher-priority rules

Toggling Rules On/Off

Each rule has an active/inactive toggle:

- **Active** — The rule is applied during classification. New and reclassified transactions will be evaluated against this rule.
- **Inactive** — The rule exists but is not applied. Use this to temporarily disable a rule without deleting it.

Toggle a rule from the rule list or detail view. Deactivating a rule does not undo classifications already made — it only stops future transactions from being matched.

Rule Priority and Conflicts

When multiple rules could match the same transaction, CryptaCount applies rules in priority order. The first matching rule wins.

Managing Priority

Rules are evaluated in list order. Drag rules to reorder them and set priority. Place more specific rules above broader ones:

1. **Specific contract + specific asset + specific wallet** — Highest priority
2. **Specific contract + specific asset** — Medium priority
3. **Asset-only or type-only rules** — Lower priority, broader catch-all

Conflict Resolution

If the test feature shows conflicts between rules, resolve by:

- **Narrowing criteria** — Add more conditions to the conflicting rule so it doesn't overlap

- **Reordering** — Place the more specific rule higher in the priority list

- **Merging** — Combine overlapping rules into a single rule with the correct classification

Workspace and Global Rules

Revenue classification operates at two levels:

- **Workspace rules** — Created by workspace users, apply to one workspace only

- **Global rules** — Platform-level rules that apply across all workspaces

Workspace rules take precedence over global rules for the same transaction type.

Integration with Accounting Pipeline

Revenue rules feed into the accounting pipeline:

1. **Transaction arrives** (from wallet sync or CEX import)

2. **Auto-classification** runs, including revenue rule evaluation

3. **Matched rule** assigns the revenue category and GL account

4. **Journal generation** uses the assigned GL account for the credit entry

5. **Financial reports** reflect the classified revenue in the correct income statement line

If no rule matches an income transaction, it falls to the default classification logic or enters the manual review queue.

> *Tip: Start with rules for your highest-volume revenue streams. For Acme Digital Holdings, this might be staking rewards and protocol fees. Add rules for edge cases as they appear in the review queue — this way, you build a comprehensive rule set incrementally without over-engineering upfront.*

Rollforward & Balances

The rollforward is the central reconciliation artifact in CryptaCount. Together with balance calculation, monthly snapshots, and lot-level detail, the Balances section provides complete position tracking.

What Is a Rollforward?

A rollforward (also called a "roll-forward schedule" or "movement schedule") answers the question: *How did we get from the opening balance to the closing balance?*

For each asset, it shows:

```
Opening Balance
+ Additions (purchases, transfers in, rewards, airdrops)
− Disposals (sales, transfers out, fees)
± Revaluations (FMV changes, FX translation)
= Closing Balance
```

This is the standard format expected by auditors for verifying digital asset positions.

Five-Column Structure

CryptaCount's rollforward tracks five dimensions simultaneously:

Column	What It Measures	How It's Calculated
Quantity	Number of units held	Sum of in/out transactions
Cost (USD)	Historical acquisition cost in USD	Purchase price × quantity at each acquisition
FMV (USD)	Current fair market value in USD	Market price × quantity at period end
Cost (EUR)	Historical cost translated to EUR	Cost USD × FX rate at each acquisition date
FMV (EUR)	Fair market value in EUR	FMV USD × closing FX rate at period end

All five columns must reconcile independently: opening + additions − disposals ± adjustments = closing.

Balance Calculation

Trigger balance calculations under **Balances → Calculate**:

- **Synchronous calculation** — For smaller workspaces, computes immediately
- **Asynchronous calculation** — For larger workspaces, runs in the background with progress tracking
- **In-progress tracking** — Monitor currently running calculations
- **Retry** — Re-run failed calculations
- **Diagnostics** — Investigate stuck or failed balance computations
- **Validation** — Verify calculated balances against on-chain data

Monthly Balances

Monthly snapshots under **Balances → Monthly** provide:

- Balance state at each month-end
- Month-over-month comparison
- Trend analysis across periods
- Export for external reporting

Lot Viewer

The lot viewer under **Balances → Lots** provides granular visibility into individual lots:

- View each acquisition lot with date, quantity, and cost basis
- See which lots have been partially or fully disposed
- Select specific lots for Specific Identification disposals
- Track lot-level holding periods for tax classification

FX Translation Components

For workspaces reporting in EUR (or any non-USD currency), three components reconcile the FMV column:

FMV Revaluation

The change in fair market value, translated using the **monthly average exchange rate** (per IAS 21). This isolates the asset's price movement from FX fluctuations.

FX Translation

The impact of exchange rate changes on the balance, calculated using the **closing rate** (the rate on the last day of the period). This captures the pure FX effect.

FX on Revaluation

The **balancing difference** — the amount needed to make the columns reconcile after FMV Revaluation and FX Translation. This arises from the interaction between asset price changes and FX rate changes.

> *Note: FX on Revaluation is derived as a residual. This is standard practice in multi-currency accounting and ensures the rollforward always balances.*

Audit Use Cases

The rollforward is the primary document auditors use to verify digital asset positions:

- **Completeness:** All transactions are accounted for (opening + movements = closing)
- **Accuracy:** Cost basis and FMV calculations are correct
- **Classification:** Each movement is properly categorized
- **FX treatment:** Translation methodology is consistent and IAS 21-compliant
- **Reconciliation:** Closing quantity matches on-chain balance; FMV matches market data

Settings & Preferences

The Settings area provides 11 tabs for configuring your profile, workspace, appearance, and connected services. Additional workspace-level settings are available at dedicated locations.

Settings Tabs

Navigate to **Settings** in the sidebar to access the following tabs:

Tab	Description
Profile	Name, email, personal information (default tab)
Security	2FA setup, session management, password
Activity Log	User activity history and audit trail
Asset Registry	Manage token/coin catalog, spam, classification
Notifications	Email notification preferences
API Keys	Generate and manage API access keys
Integrations	Connections to accounting platforms
Appearance	Theme selection, light/dark mode
Billing	Subscription, usage, payment (hidden for Practice users)
External Access	Workspace sharing with external parties (hidden for Practice users)

Profile

Under **Settings → Profile**:

- **Personal information** — Name and email address
- **Avatar** — Profile picture
- Your email is used for login and notifications

Security

Under **Settings → Security**:

- **Two-Factor Authentication (2FA)** — TOTP-based 2FA with setup wizard, backup codes

- **Active sessions** — View all active sessions with device info

- **Session management** — Revoke individual sessions or all sessions

- **Password** — Change password (for accounts with password auth)

Activity Log

Under **Settings → Activity Log**:

- User activity history organized by workspace and entity

- Authentication events (logins, failed attempts)

- Action-level audit trail

- Statistics and cleanup

Asset Registry

Under **Settings → Asset Registry** — see Asset Management for full details on the asset registry, spam management, and per-asset configuration.

Notifications

Under **Settings → Notifications**:

- Control which events trigger email notifications

- Sync completions and errors

- Team invitations

- Billing alerts

- Security events

API Keys

Under **Settings → API Keys**:

- Generate API keys for programmatic access

- View and revoke existing keys

- Key-level access control

Integrations

Under **Settings → Integrations** — see Integrations for full details on connections and accounting platform connectivity.

Appearance

Under **Settings → Appearance**:

Themes

CryptaCount includes four themes, each available in light and dark modes:

Theme	Character	Best For
Nexus	Violet-forward, modern	The default brand experience
Forge	Warm, earthy tones	Extended working sessions
Arctic	Cool blues and whites	High-contrast readability
Classic	Neutral, professional	Conservative/formal environments

Light / Dark Mode

Toggle between light and dark mode using the sun/moon icon in the top bar, or set to follow your system preference (auto mode). Your choice is saved per-device.

Billing

Under **Settings → Billing** — see Billing & Plans for full details on subscription management and payment.

> *Note: The Billing tab is hidden from Practice users, who have their own billing under **Practice → Billing**.*

External Access

Under **Settings → External Access**:

- Share workspace access with external parties (auditors, accountants, regulators)
- Manage sharing permissions
- The external party accesses the shared workspace through their own account

> *Note: External Access is hidden from Practice users.*

Additional Settings

Beyond the 11 settings tabs, additional configuration is available:

Sidebar Location	Purpose
Settings → Workspace Accounting	Workspace-level accounting settings — default cost basis method, base currency, fiscal year
Settings → Rules	Accounting rules — define, test, and manage classification and journal rules
rnal rules	
les	
rnal rules	

Tax Compliance

CryptaCount's tax module provides multi-jurisdiction tax support with 73 jurisdictions, automated tax calculations, form generation, and export capabilities. The module includes features available to all users and advanced features available on qualifying plans.

Jurisdiction Comparison (All Users)

The jurisdiction comparison tool under **Tax → Jurisdiction Compare** is available to all users.

It provides:

- Side-by-side comparison of tax rules across jurisdictions

- Holding period rules and exemptions

- Tax rate references

- Permitted cost basis methods

- Anti-avoidance provisions

- Reporting requirements

This covers 73 jurisdictions organized into five tax tiers:

Tier	Description	Examples
TIER_1	Tax follows accounting	Luxembourg, Singapore
TIER_2	Tax differs from accounting (parallel calculation)	US, UK
TIER_3	Unique regime (share pooling, ACB, VDA)	UK (S104), Canada, India
TIER_4	No CIT / exempt	UAE, Cayman Islands
TIER_5	Unclear / no formal crypto framework	Various

Tax Settings (Qualifying Plans)

Business entity tax settings under **Tax → Settings** configure:

- Corporate tax rates on crypto gains

- Permitted cost basis methods for the jurisdiction

- VAT treatment of crypto transactions

- Depreciation and impairment rules

- Book-to-tax differences

Tax Calculations

The tax calculation engine under **Tax → Calculations** provides:

- Create and manage tax calculation configurations

- Run tax calculations for specific periods

- Set active calculation for the workspace

- Track jurisdiction-specific usage and rules

Corporate Tax Center

The corporate tax center under **Tax → Corporate** provides:

- **Tax summary** — Overall tax position for the entity

- **Calculate** — Run corporate tax calculations

- **Jurisdiction rules** — Applied rules for the entity's jurisdiction

- **Book-tax differences** — Reconciliation between accounting and tax treatment

Tax Disposals

The disposal schedule under **Tax → Disposals** shows:

- Every disposal event with calculated gain/loss

- Cost basis lot matching

- Holding period classification (short-term vs. long-term)

- Summary totals and export

Tax Forms

Tax form generation under **Tax → Forms** supports multiple jurisdictions and form types:

US Forms:

- Form 8949 — Sales and Other Dispositions of Capital Assets
- Schedule D — Capital Gains and Losses
- 1099-DA — Digital Asset Broker Reporting
- Wash Sale reporting
- FBAR (FinCEN 114)
- Form 8938 — FATCA Statement of Foreign Financial Assets
- Form 8283 — Noncash Charitable Contributions
- Form 1120 — Corporate Income Tax
- Form 1065 K-1 — Partner's Share of Income
- Form 1120S K-1 — S Corp Shareholder's Share
- Form 1099-NEC — Nonemployee Compensation
- Form 4797 — Sales of Business Property
- Distribution declarations

International Forms:

- Jurisdiction-specific forms accessed via **Tax → Forms** with the relevant jurisdiction selected

Tax Exports

Tax exports under **Tax → Exports** support multiple formats:

Format	Description
Generic CSV	Universal CSV format
TXF	Tax Exchange Format (for tax software)
Form 8949 PDF	IRS Form 8949 as PDF
Schedule D 1120	Schedule D for corporate filers
SA108 CSV	UK Self Assessment capital gains

DAC8 XML	EU DAC8 reporting format
CoinTracker CSV	CoinTracker import format
Koinly CSV	Koinly import format

1099-DA Reconciliation (US Only)

The 1099-DA reconciliation tool under **Tax → Reconciliation** helps US entities:

- Match 1099-DA forms received from exchanges against CryptaCount's records

- Identify discrepancies between broker reporting and your calculations

- Prepare documentation for potential IRS inquiries

Regulatory Framework Alignment

The platform's data outputs align with regulatory frameworks:

- **DAC8** — Transaction and holding data structured for EU tax information exchange

- **MiCA** — Financial reporting for licensed crypto-asset service providers

- **CARF** — Cross-border information exchange requirements

> *Caution:* CryptaCount provides tax-relevant data and calculations. It does not provide tax advice, prepare tax returns, or make filing decisions. All tax classifications should be reviewed by a qualified tax professional.

Team & Permissions

CryptaCount's role-based access control provides granular permissions across three role tiers plus 42 workspace-level permissions, designed for the workflows of accounting practices and audit teams.

Team Management

Navigate to **Team** in the sidebar (visible only to Owner and Manager roles). From here you can invite members, assign roles, and manage access.

Click **Invite Member**, enter the person's email address, and assign their roles. They'll receive an invitation email with a link to join.

Role System

CryptaCount uses a three-tier role system. Each tier controls a different dimension of access:

Tier 1: Platform Role (Staff Only)

System-level access for platform operations. Most users don't have a platform role — these are for CryptaCount staff only.

Tier 2: Company Role

Permissions within a specific company:

Role	Can do
OWNER	Everything — billing, deletion, all settings, ownership transfer
MANAGER	Manage workspaces, team members, settings. Cannot delete company or manage billing.
MEMBER	Work with data — transactions, reports, assets. Cannot invite team or change settings.
VIEWER	Read-only access to all company data

Tier 3: Workspace Role

Permissions within a specific workspace:

Role	Can do
OWNER	Everything — workspace deletion, ownership transfer
MANAGER	Manage wallets, team, integrations, settings
MEMBER	Work with transactions, reports, assets, journal entries
VIEWER	Read-only access to all workspace data

Granular Workspace Permissions

Beyond workspace roles, CryptaCount supports 42 granular permissions that provide fine-grained control over specific actions. Permissions cover these resource types:

Resource	Available Permissions
workspace	view, edit, delete
users	view, invite, edit, delete
wallets	view, create, edit, delete, sync
transactions	view, create, edit, delete, categorize
accounts	view, create, edit, delete
journals	view, create, post, reverse
reports	view, generate, export
settings	view, edit
integrations	view, create, edit, delete
api_keys	view, create, delete
audit	view
rules	view, create, edit, delete
assets	view, create, edit, delete

These permissions can be assigned individually to workspace members, allowing you to create custom access profiles. For example, a junior accountant might have `transactions:view`, `transactions:categorize`, and `reports:view` but not `journals:post` or `settings:edit`.

Account Types

Set during registration, the account type determines the user's primary workflow:

Account Type	Purpose
Business	Companies managing their own crypto accounting
Practice	Audit firms and accounting practices managing client books
Tax Adviser	Tax-focused advisory work
Individual	Solo users managing personal crypto

Practice Mode

Practice users (audit firms, accounting practices) have a dedicated portal for managing client relationships:

- **Practice → Clients** — Manage client companies and workspaces
- **Practice → Billing** — Practice-specific billing (separate from standard billing)
- **Practice → Shared** — View workspaces shared with the practice

Practice users can access client workspaces without the client incurring additional charges ("no double billing" principle).

Workspace Sharing for External Access

When a business grants access to an external party (auditor, accountant, regulator):

1. Navigate to **Settings → External Access**
2. Invite the external party by email
3. Assign appropriate roles and granular permissions

4. The external party sees the shared workspace alongside their own workspaces

> *Note:* *External access is managed at the workspace level. The business's existing subscription covers the workspace — the external party is not billed separately for access.*

How Roles Combine

A team member's effective permissions are the intersection of all applicable role tiers:

- **Jane** has Company Role: OWNER, Workspace Role: MANAGER on "DeFi Ops" and VIEWER on "Treasury"

    - Jane can fully manage the DeFi Ops workspace but only view Treasury data

- **Bob** has Company Role: VIEWER

    - Bob has read-only access to everything in the company, regardless of workspace roles

Transactions

Transactions are the fundamental data unit in CryptaCount. Every wallet sync, CEX import, and manual entry feeds transaction data that drives classification, journal generation, and reporting.

Transaction List

The main transaction list under **Transactions** in the sidebar shows all events across all connected wallets and CEX accounts, sorted by date (newest first).

Each row displays:

- **Date/Time** — UTC timestamp of the on-chain event
- **Type** — Classified transaction type (TRANSFER_IN, SWAP, STAKING_REWARD, etc.)
- **Asset** — The primary asset involved
- **Amount** — Quantity of the asset
- **FMV** — Fair market value at the time of the transaction
- **Wallet** — Which wallet this transaction belongs to
- **Status** — Processing status (classified, pending review, manually overridden)

Transaction Types (100+)

CryptaCount supports over 100 transaction types organized by category:

Category	Types
Transfers	TRANSFER_IN, TRANSFER_OUT, INTERNAL_TRANSFER
Trading	BUY, SELL, SWAP
DeFi	LP_ADD, LP_REMOVE, STAKE, UNSTAKE, BORROW, REPAY, LIQUIDATION, LENDING_DEPOSIT, LENDING_WITHDRAW, BRIDGE_OUT, BRIDGE_IN, WRAP, UNWRAP, CLAIM_REWARD, YIELD_CLAIM
Income	INCOME, AIRDROP, MINING_REWARD, STAKING_REWARD, VALIDATOR_REWARD

Expense	EXPENSE, FEE, PROTOCOL_FEE
Fiat	FIAT_DEPOSIT, FIAT_WITHDRAWAL
NFT	NFT_MINT, NFT_BUY, NFT_SELL, NFT_TRANSFER
Margin	MARGIN_OPEN, MARGIN_CLOSE, MARGIN_COLLATERAL_IN/OUT, MARGIN_INTEREST, MARGIN_LIQUIDATION
Futures	FUTURES_OPEN, FUTURES_CLOSE, FUTURES_FUNDING, FUTURES_SETTLEMENT
Options	OPTIONS_BUY, OPTIONS_SELL, OPTIONS_EXERCISE, OPTIONS_EXPIRE, OPTIONS_ASSIGN
Restaking	RESTAKE_DEPOSIT, RESTAKE_WITHDRAW, AVS_REWARD, RESTAKE_SLASH
Token Migration	TOKEN_MIGRATE_OUT, TOKEN_MIGRATE_IN
Loss/Theft	ASSET_LOST, ASSET_STOLEN, ASSET_RECOVERED
IBC/Cosmos	IBC_TRANSFER_OUT, IBC_TRANSFER_IN, IBC_TIMEOUT_REFUND, IBC_RELAYER_FEE
Layer 2	L2_DEPOSIT, L2_WITHDRAW
Governance	GOVERNANCE_LOCK, GOVERNANCE_UNLOCK, GOVERNANCE_REWARD, GOVERNANCE_BRIBE, GOVERNANCE_DELEGATE
Privacy	PRIVACY_SHIELD, PRIVACY_UNSHIELD
Insurance	INSURANCE_PURCHASE, INSURANCE_CLAIM, INSURANCE_PREMIUM, INSURANCE_EXPIRE
Other	CONTRACT_INTERACTION, APPROVAL, UNKNOWN

Filtering

Filter transactions by any combination of:

- **Date range** — Custom start/end dates
- **Wallet** — One or more specific wallets
- **Chain** — Filter by blockchain network
- **Asset** — Filter by specific token or coin

- **Transaction type** — Filter by classification category

- **Status** — Classified, pending review, manually overridden

- **Search** — Free-text search across transaction hashes, addresses, and notes

Transaction Detail View

Click any transaction to open the full detail view:

Transaction data: Transaction hash (links to block explorer), block number, timestamp (UTC), from/to addresses, gas/network fee, counterparty address.

Accounting data: Classified transaction type (with override option), FMV at transaction time, cost basis impact, generated journal entry (debit/credit table), notes/memo field.

Audit trail: Classification history, who changed it and when.

Transaction Review Queue

The review queue under **Transactions → Review** surfaces transactions that need manual attention:

- Transactions classified as UNKNOWN

- Transactions flagged by rules that couldn't auto-resolve

- Transactions with missing price data

- Transactions with potential misclassification

Transaction Groups

Under **Transaction Groups** in the sidebar, you can group related transactions together. This is useful for:

- Multi-step DeFi operations that span multiple transactions

- Related transfers across chains (bridge out + bridge in)

- Batch operations that should be viewed as a unit

Groups can be expanded, collapsed, and archived.

Bulk Operations

For high-volume wallets, bulk operations help manage transactions efficiently:

- **Bulk reclassify** — Select multiple transactions and change their type at once

- **Bulk export** — Export a filtered set of transactions to CSV or Excel

- **Bulk action** — Apply actions to selected transactions (classify, archive, add to group)

Transaction Classification

Every transaction synced or imported into CryptaCount is assigned a type by the classification engine. This type determines how the transaction is journaled, whether it triggers a gain/loss calculation, and how it appears in reports.

Automatic Classification Engine

The classification engine analyzes each transaction's on-chain data to assign a type:

- **Direction analysis** — Is the wallet the sender, receiver, or both?
- **Contract interaction** — Is this a simple transfer or a smart contract call?
- **Function classification** — Over 70 function categories map on-chain function signatures to classification hints (TRANSFER, SWAP, BRIDGE, STAKING, LENDING, etc.)
- **Event parsing** — For contract interactions, which events were emitted?
- **Counter-asset detection** — Did the wallet receive a different asset in the same transaction (indicating a swap)?
- **Known contract matching** — Is the contract a recognized DeFi protocol, DEX router, staking contract, or bridge?
- **Economic intent** — The engine assigns an economic intent (INVESTMENT, TRADING, OPERATIONAL, INCOME, EXPENSE, FINANCING, HEDGING, TRANSFER, UNKNOWN) to guide accounting treatment.

The classification is deterministic — the same transaction data always produces the same type.

Manual Override

If the automatic classification is incorrect, you can override it from the transaction detail view:

1. Open the transaction detail

2. Click the current type label

3. Select the correct type from the dropdown

4. Optionally add a note explaining the override

5. Save

The override is recorded in the audit trail. The original automatic classification remains visible for reference.

> *Note:* *Overriding a transaction type triggers recalculation of the affected journal entry and any downstream cost basis or gain/loss calculations.*

Classification Rules

Define rules under **Settings → Rules** that automatically override the classification for transactions matching specific criteria:

- **Contract address** — All interactions with a specific contract get a specific type
- **Token** — Transactions involving a specific token are classified a certain way
- **Direction and amount** — Combine direction, asset, and amount thresholds

Rules support versioning — you can test rules against existing transactions before activating them.

AI Classification

The AI classification feature under **AI Classification** in the sidebar is available on qualifying plans. It provides:

- **AI-powered suggestions** — Machine learning model analyzes transaction patterns and suggests classifications
- **Accept/reject workflow** — Review AI suggestions individually or in bulk
- **Bulk accept/reject** — Process multiple AI suggestions at once
- **Generate suggestions** — Trigger AI analysis for unclassified transactions

AI classification supplements the rule-based engine — it catches patterns that static rules miss, especially for novel DeFi protocols.

Revenue Classification Rules

Revenue classification rules under **Revenue Rules** in the sidebar provide specialized handling for revenue-generating transactions:

- **Revenue contract rules** — Define rules for recognizing revenue from specific token flows or contract interactions
- **Registry levels** — Rules can be defined at global level, workspace level, or per-token level
- **Test matching** — Validate rules against sample transactions before activating
- **Toggle** — Enable/disable rules without deleting them

This is particularly useful for businesses that receive crypto as payment — rules can automatically classify incoming transfers from known customer addresses as revenue.

Bulk Reclassification

For recurring misclassifications:

1. Filter the transaction list to show affected transactions
2. Select all matching transactions
3. Use **Bulk Reclassify** and choose the correct type
4. Review and confirm

Common Misclassifications

Symptom	Likely Cause	Fix
Staking rewards shown as TRANSFER_IN	Contract not recognized as staking	Override to STAKING_REWARD or add a rule
DEX swap shown as two separate transfers	Complex routing not detected	Override to SWAP
Bridge shown as TRANSFER_OUT with no BRIDGE_IN	Destination chain wallet not connected	Connect destination wallet, or manually add BRIDGE_IN
All token transfers showing as TRANSFER_OUT	Address comparison issue	Check wallet address format

Wallets & Sources

Wallets are the primary data source for CryptaCount. The platform distinguishes between internal wallets (owned by the entity) and external wallets (counterparties), and supports grouping and GL mapping per wallet.

Internal Wallets

Manage internal wallets under **Wallets** in the sidebar. These are wallets owned or controlled by the entity being accounted for.

Each wallet shows:

- Wallet label (your custom name)
- Chain identifier and address type
- Address (truncated with copy button)
- Sync status and last sync timestamp
- GL account mapping
- Wallet group membership

Adding a Wallet

See the Connect a Wallet guide for the step-by-step walkthrough.

Supported Address Types (21 Types)

Address Type	Format	Examples
EVM	`0x...`	Ethereum, Polygon, BSC, Arbitrum, Optimism, Base, Avalanche C-Chain, etc.
BITCOIN_LEGACY	`1...`	Bitcoin P2PKH
BITCOIN_P2SH	`3...`	Bitcoin Pay-to-Script-Hash
BITCOIN_SEGWIT	`bc1q...`	Bitcoin native SegWit

BITCOIN_TAPROOT	`bc1p...`	Bitcoin Taproot
SOLANA	Base58	Solana
TRON	`T...`	TRON
XRP	`r...`	XRP Ledger
CARDANO	`addr1...`	Cardano
COSMOS	`cosmos1...`	Cosmos Hub, IBC chains
TON	Various	The Open Network
POLKADOT	SS58	Polkadot relay chain + parachains
STELLAR	`G...`	Stellar
NEAR	`account.near`	NEAR Protocol
APTOS	`0x...`	Aptos
SUI	`0x...`	SUI
STARKNET	`0x...`	StarkNet L2
HEDERA	`0.0.xxxxx`	Hedera
AVALANCHE_X	`X-avax1...`	Avalanche X-Chain
AVALANCHE_P	`P-avax1...`	Avalanche P-Chain
UNKNOWN	Various	Unrecognized format

GL Mapping Per Wallet

Each wallet can be mapped to a GL account, controlling where its transactions post in the chart of accounts. Configure this from the wallet detail view or in bulk from the wallet list.

External Wallets

Manage external wallets under **Wallets → External**. These represent counterparty addresses — wallets not owned by the entity but that appear in transaction data (e.g., exchange deposit addresses, vendor wallets, client addresses).

External wallets help with:

- **Transaction classification** — Knowing a counterparty address helps classify transfers correctly
- **Reconciliation** — Match incoming/outgoing transfers to known external parties
- **Reporting** — Label counterparties in reports instead of showing raw addresses

External wallets can be imported in bulk, assigned GL accounts, and organized into groups. You can also convert an external wallet to an internal wallet if ownership changes.

Scan Wallets

The **Scan Wallets** feature discovers wallet addresses that appear in your transaction data but haven't been explicitly added. This helps ensure completeness — you won't miss a wallet that should be tracked.

Additionally, **Balances → Scan External** scans for external addresses that should be added as external wallets for proper reconciliation.

Wallet Groups

Wallet groups let you organize wallets into logical categories for reporting and management:

- **By purpose:** "Treasury", "DeFi Operations", "Staking"
- **By entity:** "TechCorp Wallets", "InvestCo Wallets"
- **By chain:** "Ethereum Wallets", "Bitcoin Wallets"

Groups can be reordered, and each group can be mapped to a GL account. Manage groups from the wallet list interface.

Wallet Detail View

Click any wallet to see its detail view:

- **Summary:** Balance overview, sync status, last sync details, chain assets
- **Transactions:** All transactions for this wallet with filtering and classification tools
- **Sync:** Sync details including last processed block, sync progress per stream, and error logs
- **GL Mapping:** Which GL account this wallet's transactions post to
- **Initial Balances:** Set opening balances for wallets that had existing positions before connecting

Removing a Wallet

To remove a wallet, open the wallet detail view and use the **Remove Wallet** option.

Caution: Removing a wallet deletes all its transaction data, journal entries, and calculated cost basis from the workspace. This action is irreversible. Export any needed reports before removing a wallet.

Workspaces & Companies

Workspaces and companies form the organizational hierarchy of CryptaCount. Understanding this structure is essential for setting up your accounting workflow correctly.

Organizational Hierarchy

CryptaCount uses a three-level hierarchy:

```
Company → Workspace → Entities (Wallets, GL Accounts, Accounting
Periods, Transactions, External Wallets, etc.)
```

A **company** is the top-level legal entity. Each company contains one or more **workspaces**, and each workspace contains the actual accounting data — wallets, transactions, journal entries, reports, and settings. Most entities are workspace-scoped.

Companies

Manage companies under **Companies** in the sidebar. Each company represents a legal entity in the system.

Creating a Company

Click **Add Company** and provide:

- **Company name** — The legal entity name
- **Jurisdiction** — Determines which tax profile rules apply. Select from 73 available jurisdictions.
- **Registration number** — Optional, for reference and reporting
- **Accounting defaults** — Set default cost basis method, base reporting currency, and reporting period

Company Roles

Access within a company is controlled by company-level roles:

Role	Can do
OWNER	Everything — billing, deletion, all settings
MANAGER	Manage workspaces, team members, and settings. Cannot delete the company or manage billing.
MEMBER	Work with data — transactions, reports, assets. Cannot invite team or change settings.
VIEWER	Read-only access to all company data

Company Tree

Companies support a parent-child structure via the company tree. Sub-companies can be created for group structures where multiple legal entities roll up to a parent.

Workspaces

Manage workspaces under **Workspaces** in the sidebar. A workspace is the primary container for accounting data within a company.

Creating a Workspace

Each workspace belongs to a company. When creating a workspace, you specify:

- **Workspace name** — Descriptive label for this set of books
- **Company** — Which company this workspace belongs to
- **Accounting settings** — Can inherit from the company or override:
  - Default cost basis method (Historic FIFO, Historic Weighted Average, FMV, NRV + FIFO, NRV + Weighted Average, LIFO, HIFO, Specific Identification)
  - Base reporting currency (EUR, USD, GBP, CHF, etc.)
  - Reporting period (calendar year or custom fiscal year)

Workspaces can be duplicated for creating similar setups quickly.

Workspace Accounting Settings

Configure workspace-level accounting under **Settings → Workspace Accounting**:

- Default cost basis method
- Base currency
- Fiscal year settings
- Accounting rules and policies

Workspace Roles

Access within a workspace is controlled by workspace-level roles:

Role	Can do
OWNER	Everything — workspace deletion, ownership transfer
MANAGER	Manage wallets, team, settings. Cannot delete workspace.
MEMBER	Work with transactions, reports, assets
VIEWER	Read-only access

When to Create Multiple Workspaces

Accounting firms (Practice users): One workspace per client engagement provides complete data isolation between clients. Manage all clients from **Practice → Clients**.

Multi-entity businesses: One workspace per business unit or entity. Different jurisdictions and accounting methods per workspace.

Separate books: Different workspaces for DeFi operations vs. treasury vs. trading — then consolidated at the company level.

Practical Setup Examples

Example 1: Accounting Firm with Three Clients

```
Company: "Smith & Partners Crypto Practice"
├── Workspace: "Client A — TechCorp GmbH" (Germany, Historic FIFO)
├── Workspace: "Client B — InvestCo SAS" (France, Historic
Weighted Average)
└── Workspace: "Client C — NodeOps Ltd" (Luxembourg, Historic
FIFO)
```

Each workspace has its own wallets, transactions, and reports. The firm manages all clients from the Practice portal.

Example 2: Corporate Group

```
Company: "Acme Holdings Ltd" (Luxembourg)
├── Workspace: "Acme Trading" (Delaware, USA — Historic FIFO)
├── Workspace: "Acme DeFi Operations" (Luxembourg — FMV)
└── Workspace: "Acme Asia Treasury" (Singapore — Historic Weighted
Average)
```

Different jurisdictions, potentially different cost basis methods, unified at the company level.

Example 3: Solo Business

```
Company: "MyCompany Ltd" (UK)
└── Workspace: "Main Books" (Historic FIFO)
```

Simple structure for a single-entity business managing its own crypto accounting.

CryptaCount

Thank you for reading

Product

app.cryptacount.com

Documentation

docs.cryptacount.com

Website

www.cryptacount.com