CryptaCount Whitepaper

Crypto Accounting Methodology, Compliance Framework & Platform Overview

CryptaCount, Inc.
docs.cryptacount.com
March 2026

Accounting Methodology

The accounting engine is CryptaCount's core differentiator. It transforms classified blockchain transactions into proper double-entry journal entries, calculates cost basis under eight internationally recognized methods, and produces rollforward schedules that reconcile period-over-period — the fundamental requirement for audit-ready financial reporting.

Double-Entry Bookkeeping

Every transaction processed by CryptaCount generates one or more journal entries following double-entry accounting principles. Debits always equal credits. There are no single-sided entries, no unexplained balance adjustments, and no opaque calculations.

For a simple ETH purchase at €2,100:

Account	Debit (EUR)	Credit (EUR)
Digital Assets — ETH	2,100.00	
Cash / Bank		2,100.00

For a more complex DeFi staking reward claim (0.5 LINK at FMV €7.25):

Account	Debit (EUR)	Credit (EUR)
Digital Assets — LINK	7.25	
Staking Income		7.25

The journal structure supports a full chart of accounts, allowing businesses to map crypto transactions into their existing accounting framework.

Tamper-Evident Journal Integrity

Each journal entry is cryptographically hashed upon creation. The hash chain links each entry to its predecessor, creating a tamper-evident ledger. Any modification to a historical journal entry breaks the hash chain, making unauthorized changes immediately detectable.

This mechanism provides the audit evidence that the ledger has not been retroactively modified — a fundamental requirement for financial statement audits. Corrections are still possible but must be transparent and traceable, consistent with accepted accounting practice.

Cost Basis Methods

CryptaCount implements eight cost basis methods, covering the full range of internationally recognized approaches:

Method	Description	Common Jurisdictions
FIFO	First In, First Out — oldest lots disposed first	US (default), UK, many EU states
LIFO	Last In, First Out — newest lots disposed first	Permitted in some jurisdictions
HIFO	Highest In, First Out — highest-cost lots disposed first	Tax optimization where permitted
WAVG	Weighted Average Cost — single blended cost per asset	France (mandatory), IFRS common
FMV	Fair Market Value — mark-to-market	Trading firms, certain fund structures
NRV + FIFO	Net Realizable Value (FIFO basis)	IAS 2 inventory valuation
NRV + Weighted Average	Net Realizable Value (WAVG basis)	IAS 2 inventory valuation
Specific Identification	Specific Identification — user selects lots	Permitted in US, others

Three-Level Resolution Hierarchy

The cost basis method resolves through a three-level hierarchy:

1. **Asset-specific override** — A method set on a particular asset (e.g., "use HIFO for LINK") takes highest precedence
2. **Asset class level** — A method set for an asset class (e.g., "use WAVG for all stablecoins") applies to all assets in that class unless overridden at level 1

3. **Workspace default** — The workspace-level default (e.g., "FIFO") applies to everything not overridden at levels 1 or 2

This hierarchy accommodates the real-world requirement where a portfolio may need different methods for different asset categories within the same jurisdiction, or where a specific asset has a regulatory carve-out.

For example, an accounting firm managing a Luxembourg client might set FIFO as the workspace default, WAVG for stablecoins (asset class level), and Specific Identification for a particular large ETH position where lot selection matters for tax optimization (asset-specific level).

Fair Market Value (FMV)

The platform sources fair market value data for pricing transactions and positions. FMV is captured at three granularities:

- **Transaction-time FMV** — The market price at the exact timestamp of each transaction, used for cost basis and income recognition
- **Daily closing rate** — End-of-day prices used for reporting and position valuation
- **Monthly average rate** — Used for FMV Revaluation per IAS 21 methodology

All FMV data is stored in both USD (primary pricing currency) and translated to the workspace's reporting currency (typically EUR) using the applicable exchange rate.

Five-Column Rollforward

The rollforward is the central reconciliation artifact. It tracks each asset position across a reporting period in five columns:

Column	Description	Source
Quantity	Number of units held	Transaction in/out aggregation
Cost (USD)	Historical cost in USD	Acquisition price at purchase
FMV (USD)	Fair market value in USD	Current market price × quantity
Cost (EUR)	Historical cost in EUR	Cost USD × FX rate at acquisition
FMV (EUR)	Fair market value in EUR	FMV USD × FX closing rate

The rollforward reconciles: **Opening Balance + Additions − Disposals ± Revaluations = Closing Balance**, verified across all five columns.

FX Translation Methodology

For workspaces reporting in EUR (or any non-USD currency), the platform applies IAS 21-aligned translation:

- **FMV Revaluation (EUR)** uses the **monthly average exchange rate** — this smooths daily FX volatility in revaluation gains/losses, consistent with IAS 21 guidance for income and expense items
- **FX Translation** uses the **closing rate** — the balance sheet date exchange rate applied to monetary items
- **FX on Revaluation** is the **balancing difference** — the residual that arises from the interaction between FMV changes and FX rate changes. This is not independently calculated; it is derived as the amount needed to balance the rollforward after FMV Revaluation and FX Translation are applied

This three-component approach (FMV Revaluation, FX Translation, FX on Revaluation) ensures that the EUR rollforward columns always reconcile while properly attributing value changes to their economic sources.

Realized and Unrealized Gains

Realized gains/losses are calculated at disposal (sale, trade, transfer out) as the difference between proceeds and cost basis under the selected method. The gain or loss is denominated in both USD and the reporting currency.

Unrealized gains/losses represent the mark-to-market difference between current FMV and historical cost for assets still held. These are computed at any point-in-time for reporting purposes without affecting the underlying cost basis.

For jurisdictions that distinguish short-term and long-term capital gains (based on holding period), the platform tracks acquisition dates at the lot level. The holding period classification is jurisdiction-dependent and resolved through the tax profile system.

Transaction Classification

The platform automatically assigns transaction types based on on-chain event analysis:

Category	Transaction Types
Transfers	Transfer in, Transfer out
Trading	Trade, Swap
Fees	Gas and network fees
Income	Staking reward, Mining reward, Airdrop, Other income
Expense	Expense
DeFi	Liquidity add/remove, Stake/unstake, Borrow/repay, Reward claim, Wrap/unwrap, Bridge in/out
NFT	NFT mint, NFT trade

Classification is automatic but overridable. Users can reclassify individual transactions or define bulk reclassification rules. Every classification change is logged in the audit trail, ensuring full traceability of any professional judgment applied.

Solution Design

CryptaCount is structured as a three-layer system: a blockchain data ingestion layer, an accounting computation engine, and a reporting and compliance output layer. Each layer is designed to be independently verifiable and auditable.

Three-Layer Design

Layer	Function	Capabilities
Data Ingestion	Multi-chain blockchain data normalization and sync	131+ chain coverage, real-time wallet sync, automated transaction parsing, spam detection
Accounting Engine	Cost basis calculation, journal generation, fair market value pricing	Eight cost methods, double-entry bookkeeping, five-column rollforward, automated classification
Compliance Output	Reporting, tax computation, regulatory mapping	73-jurisdiction profiles, DAC8/CARF/MiCA alignment, multi-format export

This separation ensures that raw blockchain data is never directly coupled to reporting logic. The accounting engine operates on normalized, classified transaction data — meaning the same underlying data can produce different outputs depending on the selected cost basis method, reporting currency, or jurisdictional rules without re-fetching or re-processing blockchain data.

Multi-Tenant Design

The platform implements a full multi-tenant model designed for the workflows of accounting practices, audit firms, and multi-entity businesses.

Account Types

Four account types define the primary use case and available features:

Account Type	Primary Use Case	Key Capabilities

Accountant	Accounting firms managing client crypto books	Multi-client workspaces, journal generation, reporting
Auditor	Audit firms verifying client crypto positions	Read-only workspace access, reconciliation tools, audit trail
Tax Adviser	Tax advisory practices	Jurisdiction-specific reporting, multi-method comparison
Individual	Businesses managing their own crypto accounting	Full workspace control, self-service reporting

Workspace and Company Hierarchy

Each account contains one or more **workspaces**, which serve as the primary organizational unit. Within a workspace, **companies** represent distinct legal entities — one level of hierarchy. This maps to the real-world structure where an accounting firm (workspace) manages multiple client companies, or a corporate group (workspace) contains several entities.

Workspace-level settings (default cost basis method, reporting currency, reporting period) cascade to all companies within, with company-level overrides available.

Four-Tier Role System

Access control operates through four independent role dimensions:

- **Platform Role** — System-level access (platform administration)
- **Account Type** — Determines available features and interface (Accountant, Auditor, Tax Adviser, Individual)
- **Workspace Role** — Permissions within a workspace (owner, admin, member, viewer)
- **Company Role** — Permissions within a company (manager, contributor, viewer)

This separation allows fine-grained control. An auditor can be granted read-only access to a specific company within a client's workspace without gaining access to other companies in the same workspace or any write permissions.

Segregation of Administrative and User Functions

The platform maintains separate interfaces for administrative functions versus standard user functions. Administrative operations (user management, system monitoring, data management) are

isolated from the accounting workflow. This prevents accidental administrative actions and simplifies the day-to-day experience for accounting professionals.

Consent-Based Workspace Sharing

When a business grants workspace access to their auditor or accountant, the sharing model operates on a **"no double billing" principle**: the business's existing subscription covers the workspace. The professional (auditor or accountant) accesses the shared workspace through their own account without incurring duplicate charges for the same data.

This mirrors the real-world engagement model where a business pays for their accounting system and grants access to their external accountant or auditor — the accountant doesn't pay separately for access to each client's books.

Transparent Plan Enforcement

Subscription plan limits are enforced transparently. When a workspace reaches its plan allocation (wallets, transactions, companies, team members), the platform clearly communicates which limit has been reached and what upgrade resolves it — rather than silently degrading functionality.

Dual-Entity Billing

The dual-entity corporate structure (CryptaCount Inc. for US, CryptaCount S.à r.l. for EU/ROW) is reflected in the billing system:

- EU customers are billed through the Luxembourg entity with EU VAT handling via Luxembourg's One-Stop-Shop (OSS) mechanism
- Payments are processed through a PCI-compliant payment platform for both entities

Entity assignment is automatic based on customer jurisdiction and transparent to the end user.

Data Infrastructure

The data infrastructure layer is responsible for ingesting blockchain data from 131+ networks, normalizing it into a consistent transaction format, and delivering accounting-grade data to the computation engine. This layer handles the fundamental heterogeneity of blockchain architectures while maintaining the data quality and completeness that financial reporting demands.

Blockchain Coverage

EVM-Compatible Networks

CryptaCount covers the full spectrum of EVM-compatible chains, including Ethereum, Polygon, BSC, Arbitrum, Optimism, Avalanche, Base, and dozens of additional networks. For each chain, the platform captures:

- **Native asset transfers** — Primary on-chain transfers involving the chain's native currency
- **Token transfer events** — All token movements (fungible and non-fungible)
- **Contract interactions** — Including DeFi protocol events, liquidity operations, and staking
- **Transaction fees** — Per-transaction cost attribution in the native asset

Non-EVM Networks

Eleven distinct blockchain architectures are fully supported, each with dedicated data normalization:

Chain	Architecture	Key Characteristics
Bitcoin	UTXO	Input/output model, multi-signature support
NEAR	Sharded account model	Receipts-based execution, named accounts
Cosmos	IBC message passing	Multi-chain IBC transfers, staking and delegation
Stellar	Custom consensus (SCP)	Operations within transactions, built-in DEX
Cardano	Extended UTXO	Multi-asset native tokens
Polkadot	Relay chain + parachains	Cross-chain messaging, nomination staking

Hedera	Hashgraph	Account-based with native token service
TRON	DPoS	TRC-20 tokens, energy and bandwidth model
StarkNet	ZK-rollup	Layer 2 on Ethereum
Aptos	Move VM	Resource-oriented parallel execution
SUI	Move VM (object-centric)	Object model with unique ownership semantics

Each network's data is normalized into CryptaCount's universal transaction format before it reaches the accounting engine. The normalization layer handles differences in timestamp formats, address formats, fee structures, and event semantics — presenting a consistent data model regardless of the underlying chain.

Data Quality Assurance

Continuous Sync and Smart Resume

Wallet synchronization is continuous and incremental. Once a wallet is connected, the platform tracks the latest synchronized point for each data category independently. Subsequent syncs resume from where they left off rather than re-fetching entire histories — critical for high-volume wallets that may involve millions of historical events.

Deduplication

Token transfer events are deduplicated using unique on-chain identifiers. This prevents double-counting when the same event appears in multiple data responses, which can occur at pagination boundaries or during data provider replication.

Category-Separated Synchronization

Blockchain data is synchronized in distinct categories — native currency transactions and token transfer events are tracked independently. This separation ensures that each data stream maintains its own synchronization state, preventing interference between different event types and enabling more reliable incremental updates.

Spam Token Detection

The blockchain ecosystem is saturated with spam tokens — worthless tokens distributed to wallets for phishing, advertising, or scam purposes. Including these in accounting records creates noise and potential misclassification risks.

CryptaCount employs multi-factor spam detection:

- **Heuristic scoring** — Tokens are evaluated based on contract age, holder count, liquidity, transfer patterns, and metadata quality. Tokens below a confidence threshold are flagged as potential spam.
- **Homoglyph detection** — Token names and symbols are checked for Unicode lookalike attacks (e.g., visually similar characters used to impersonate legitimate tokens).
- **Manual override** — Users can mark any asset as spam or not-spam, overriding the automatic detection based on their professional judgment.

Spam-flagged assets are hidden from default views but retained in the underlying data for completeness and auditability. They can be restored at any time.

Balance Reconciliation

The platform reconciles computed balances against on-chain source data. For each wallet and asset, the system compares:

- **Computed balance** — Derived from processing all ingested transactions (inflows minus outflows)
- **On-chain balance** — Current balance as reported directly by the blockchain

Discrepancies indicate missing transactions, synchronization gaps, or classification errors. This reconciliation provides independent verification of data completeness — a critical assurance for audit-ready financial reporting.

Data Reliability Principles

The data infrastructure is built on three reliability principles:

1. **Completeness** — Every on-chain event relevant to a connected wallet is captured. Balance reconciliation against live blockchain data validates this continuously.

2. **Accuracy** — Transaction amounts, timestamps, fee attributions, and token identities are verified against on-chain source data. No estimates or approximations are used for on-chain values.
3. **Timeliness** — New transactions are captured during each synchronization cycle. The platform manages provider rate limits and pagination automatically to ensure steady data ingestion without gaps.

These principles ensure that the accounting engine operates on a data foundation that meets the evidential standards required for professional financial reporting and audit engagements.

Executive Summary

CryptaCount is an institutional-grade crypto accounting and tax compliance platform built to serve accounting firms, auditors, and businesses operating with digital assets. The platform transforms raw blockchain data into structured, auditable financial records that comply with IFRS, EU regulatory frameworks (DAC8, MiCA, CARF), and 73 national tax jurisdictions.

What Makes CryptaCount Different

Unlike consumer-oriented crypto tax calculators, CryptaCount is purpose-built for professional use. The platform provides:

Double-entry bookkeeping with tamper evidence. Every transaction generates proper journal entries. Journals are cryptographically hashed to provide tamper-evident audit trails — a requirement for institutional accounting that no consumer tool addresses.

Eight cost basis methods with hierarchical resolution. The platform supports FIFO, LIFO, HIFO, Weighted Average, Fair Market Value, NRV (FIFO), NRV (WAVG), and Specific Identification. Methods resolve through a three-level hierarchy: asset-specific overrides take precedence over asset class settings, which take precedence over workspace defaults. This accommodates the real-world complexity where a single portfolio may require different methods for different asset categories.

Multi-entity workspace management. Built for accounting practices managing multiple clients, with four account types (Accountant, Auditor, Tax Adviser, Individual), hierarchical company structures, and four-tier role-based access control.

131+ blockchain networks. The data infrastructure covers both EVM-compatible chains (Ethereum, Polygon, BSC, Arbitrum, Optimism, Avalanche, Base, and others) and non-EVM chains (Bitcoin, NEAR, Cosmos, Stellar, Cardano, Polkadot, Hedera, TRON, StarkNet, Aptos, SUI). Transaction classification handles the full spectrum of on-chain activity — from simple transfers through complex DeFi interactions including liquidity provision, yield farming, staking, lending, and cross-chain bridges.

73 tax jurisdictions. Each jurisdiction's crypto-specific rules are modeled as structured data covering reporting obligations, business tax treatment, and individual tax treatment. This includes jurisdiction-specific cost basis requirements, holding period rules, staking and mining income recognition, and DeFi event treatment.

Core Principle

CryptaCount operates under a fundamental design principle: **it calculates, but does not decide.** The platform provides accounting data infrastructure and computational tools. Tax classification, regulatory interpretation, and advisory decisions remain with the qualified professionals who use it. This is not a disclaimer — it is an architectural decision that shapes every product feature.

Company

CryptaCount is incorporated as CryptaCount Luxembourg S.à r.l. (RCS Luxembourg B286141), headquartered in Luxembourg. A US entity (CryptaCount Inc.) provides US market access.

The platform targets two B2B audience segments: **Businesses** (companies holding or transacting in digital assets) and **Practice** (accounting firms and auditors providing crypto accounting services to their own clients).

CryptaCount Whitepaper

Version 1.0 — March 2026

This whitepaper describes the methodology, regulatory framework, and value proposition behind CryptaCount — an institutional-grade crypto accounting and tax compliance platform built for accounting firms, auditors, and businesses operating with digital assets.

Contents

> ***Note:*** *CryptaCount provides accounting data infrastructure and computational tools. It does not provide tax, legal, or financial advice. Tax classification, regulatory interpretation, and advisory decisions remain with qualified professionals.*

Download as PDF

The Problem: Crypto Accounting at Scale

Digital asset accounting presents challenges that existing financial software was never designed to address. The intersection of blockchain technology, evolving regulation, and traditional accounting standards creates a complexity gap that manual processes and spreadsheets cannot reliably bridge.

Data Fragmentation

A single business may operate across dozens of blockchain networks, multiple centralized exchanges, custodial wallets, and DeFi protocols — each with its own data format and transaction semantics.

Aggregating this data into a unified ledger requires chain-specific normalization, cross-chain reconciliation, and consistent taxonomy mapping across fundamentally different blockchain architectures. Account-model chains, UTXO chains, message-passing chains, and object-centric chains each produce structurally different transaction data that must be harmonized before any accounting logic can apply.

The problem compounds with scale. A Chainlink node operator, for example, may generate thousands of token transfer events per month across multiple chains — each requiring fair market value pricing, gas fee attribution, and income recognition. Manual reconciliation at this volume is not just inefficient; it is unreliable.

Transaction Complexity

On-chain transactions are not simple debits and credits. A single DeFi interaction may involve multiple token transfers, gas fees denominated in different assets, liquidity pool token minting, reward accruals, and slippage — all within one transaction hash.

Consider a typical yield farming interaction: a user deposits ETH and USDC into a liquidity pool, receives LP tokens, stakes those LP tokens in a farming contract, and periodically claims reward tokens. Properly accounting for this requires tracking cost basis across four assets, recognizing income events at claim time, handling impermanent loss on withdrawal, and maintaining the LP token's proportional claim on underlying assets — all with fair market value pricing at each event's timestamp.

Consumer crypto tax tools typically flatten this complexity into "trade" events. For an accounting firm producing audit-ready financials, this level of abstraction is insufficient. Every component of a complex transaction must be decomposable into proper journal entries.

Regulatory Fragmentation

There is no global consensus on crypto tax treatment. Each jurisdiction maintains its own rules for asset classification (property, currency, financial instrument, or other), holding period benefits, permitted cost basis methods, staking and mining income recognition, DeFi event treatment, and reporting obligations.

The European Union alone is implementing three overlapping frameworks: DAC8 for tax reporting between member states, MiCA for market regulation of crypto-asset service providers, and CARF (via OECD adoption) for cross-border information exchange. A Luxembourg-based accounting firm with clients across the EU must navigate all three simultaneously.

Specific jurisdictional examples illustrate the fragmentation: the US does not apply wash sale rules to crypto (as of 2025), Germany abolished the extended holding period for staking income in 2022, France requires a portfolio-wide weighted average cost formula, Italy increased its crypto tax rate to 33% from January 2026, South Korea deferred its crypto tax implementation to 2027, the Czech Republic enacted a 3-year holding period exemption in February 2025, and Portugal introduced a 1-year exemption in January 2023. A platform serving multiple jurisdictions must model all of these rules as structured, queryable data — not as hardcoded assumptions.

The Audit Gap

Accounting firms and auditors require verifiable data trails, not just summary numbers. Every calculated value must trace back to on-chain source data through a documented, reproducible methodology.

Existing crypto tax tools are designed for the individual consumer use case: upload transactions, pick a cost basis method, export a tax report. They lack the journal structure, tamper evidence, role-based access controls, and multi-entity management that professional accounting practice demands.

The gap is particularly acute for auditors. An audit engagement requires independent verification of balances, reconciliation against on-chain source data, review of classification decisions, and assessment of methodology consistency. No consumer tool provides the infrastructure for this workflow.

Cost Basis Complexity

Different jurisdictions mandate or recommend different cost basis methods. Some require FIFO. Others allow weighted average only. Some permit taxpayer choice among several options. Within a single portfolio, different asset classes may require different methods — a jurisdiction might mandate FIFO for short-term trading assets while allowing weighted average for long-term holdings.

Furthermore, professional accounting often requires running multiple methods simultaneously for comparison, sensitivity analysis, or dual-reporting purposes. A platform that hardcodes a single method per portfolio cannot serve this need. The method resolution must be hierarchical: asset-specific overrides must coexist with asset-class defaults and workspace-level fallbacks.

The eight methods CryptaCount implements (FIFO, LIFO, HIFO, WAVG, FMV, NRV + FIFO, NRV + Weighted Average, Specific Identification) cover the full range of internationally recognized cost basis approaches. The three-level resolution hierarchy (asset → asset class → workspace) provides the flexibility that multi-jurisdictional practice requires.

Regulatory Compliance Framework

CryptaCount is designed to produce data that satisfies three overlapping EU regulatory frameworks while remaining useful globally. The platform does not itself perform regulated activities — it provides the computational infrastructure that regulated entities (accounting firms, audit practices, licensed tax advisers) use to meet their obligations.

EU Regulatory Landscape

DAC8 — Directive on Administrative Cooperation

DAC8 extends the EU's tax information exchange framework to crypto-assets. It requires crypto-asset service providers (CASPs) and intermediaries to report transaction and holding data to national tax authorities, who then exchange it across member states.

For CryptaCount's users, DAC8 means their clients face new reporting obligations. The platform structures its data outputs to align with DAC8 reporting schemas, ensuring that the transaction data, holding periods, cost basis calculations, and gain/loss reports can be mapped to the required reporting formats.

MiCA — Markets in Crypto-Assets Regulation

MiCA establishes a licensing and operational framework for crypto-asset service providers operating in the EU. While CryptaCount itself is not a CASP (it does not custody, trade, or transfer crypto-assets), its users often are — or serve clients who are.

The platform's accounting outputs align with MiCA's financial reporting requirements for licensed entities, including balance sheet treatment of crypto-assets, revenue recognition for crypto services, and regulatory capital calculations.

CARF — Crypto-Asset Reporting Framework

CARF is an OECD standard for cross-border information exchange related to crypto-assets, analogous to CRS (Common Reporting Standard) for traditional financial accounts. It requires intermediaries to collect and report information on crypto-asset transactions to participating jurisdictions.

CryptaCount's multi-jurisdiction tax profile system models CARF reporting requirements alongside domestic tax rules, enabling users to identify which transactions and holdings trigger CARF reporting obligations.

IFRS Alignment

For institutional users (businesses, funds, publicly reporting entities), the platform's accounting methodology aligns with International Financial Reporting Standards:

- **IAS 2 (Inventories)** — Applied where crypto-assets are held as inventory (mining operations, market-making). NRV methods (NRV + FIFO, NRV + Weighted Average) implement IAS 2's "lower of cost and net realizable value" principle.
- **IAS 21 (Foreign Currency)** — The FX translation methodology for non-USD reporting currencies follows IAS 21 guidance: monthly average rates for income/expense items, closing rates for balance sheet items.
- **IAS 38 (Intangible Assets)** — Relevant classification framework for crypto-assets held as intangible assets (the default IFRS treatment for most crypto-assets as of 2026).
- **IFRS 13 (Fair Value Measurement)** — Fair market value sourcing and hierarchy follows IFRS 13 principles for determining fair value of crypto-assets.

Luxembourg GAAP

For Luxembourg private companies (which are not required to use IFRS), the platform supports Luxembourg GAAP treatment. This is relevant because CryptaCount is Luxembourg-based and many of its initial clients are Luxembourg entities. Luxembourg GAAP treatment of crypto-assets differs from IFRS in several respects, particularly around revaluation reserves and impairment testing.

"Calculates but Doesn't Decide"

This principle is not a legal disclaimer — it is a foundational design decision that shapes every product feature.

The platform computes numbers: cost basis, fair market value, gains/losses, journal entries, rollforward schedules, tax-relevant amounts by jurisdiction. It does not make classification decisions that require professional judgment: whether a particular DeFi interaction constitutes a taxable event in a specific jurisdiction, whether a particular token should be classified as a security, or whether a specific holding period exemption applies.

This boundary is maintained throughout the product:

- Transaction types are automatically classified but always overridable by the user
- Jurisdiction tax profiles provide data (rates, rules, thresholds) but do not automatically generate final tax returns
- Reports are labeled as computational outputs, not as tax filings or regulatory submissions
- The platform explicitly surfaces areas where professional judgment is required rather than making silent assumptions

For the B2B audience (accountants, auditors, tax advisers), this is not a limitation — it is a feature. Professionals need tools that provide reliable data and computation, not tools that substitute their judgment. The platform enhances their efficiency without overstepping into their domain of expertise.

Vision

The digital asset accounting landscape is undergoing a structural transformation. What began as a niche concern for early cryptocurrency adopters has become a systemic challenge for the global accounting profession. CryptaCount's vision is shaped by three converging forces that will define this space over the coming years.

The Regulatory Convergence

The era of regulatory ambiguity around digital assets is ending. The EU's implementation of DAC8, MiCA, and CARF — alongside the OECD's Crypto-Asset Reporting Framework — signals a global shift toward formalized crypto reporting and compliance obligations. Jurisdictions that once had no position on digital asset taxation are rapidly establishing comprehensive frameworks.

This convergence creates both urgency and opportunity. Accounting firms that previously deferred crypto capabilities will need institutional-grade tooling as their clients face mandatory reporting obligations. The firms that build this capability early will capture a structural advantage in an expanding market.

CryptaCount is positioned at this intersection: providing the computational infrastructure that enables accounting professionals to meet emerging obligations with the same rigor and auditability they apply to traditional financial reporting.

The Complexity Escalation

Blockchain technology is not simplifying. The proliferation of Layer 2 networks, cross-chain bridges, novel DeFi mechanisms, real-world asset tokenization, and institutional custody solutions means that the transaction complexity facing accountants will continue to increase.

Each new blockchain architecture, each new DeFi primitive, and each new cross-chain interaction pattern introduces accounting questions that existing tools were not designed to answer. The gap between what consumer crypto tax tools can handle and what professional accounting engagements require will continue to widen.

CryptaCount's multi-chain data infrastructure — currently covering 131+ blockchain networks — is designed to expand alongside this evolving landscape. The platform's normalized data model and

extensible classification system are built to accommodate new transaction types and blockchain architectures as they emerge, without requiring fundamental redesign.

The Institutional Adoption Curve

Digital assets are moving from the periphery to the core of institutional finance. Corporate treasuries hold Bitcoin. Tokenized bonds trade on regulated exchanges. Stablecoin payment volumes rival traditional payment networks. Central bank digital currencies are in active development across major economies.

As institutional adoption deepens, the demand shifts from basic tax reporting to full accounting integration: general ledger connectivity, multi-entity consolidation, regulatory reporting, and audit-ready documentation. The tooling that serves this market must meet the same standards as enterprise financial software — not the standards of consumer tax calculators.

CryptaCount's "calculates but doesn't decide" principle is designed for this institutional reality. As digital assets become a routine component of corporate balance sheets, accounting firms need infrastructure that provides reliable, verifiable computation while preserving the professional judgment that defines their role. The platform enhances the accountant's capability without attempting to replace it.

The Market Opportunity

Three audience segments define CryptaCount's addressable market:

Accounting Practices

Accounting firms are force multipliers. A single firm adoption brings all of their crypto-holding clients onto the platform. CryptaCount's consent-based sharing model — where the business's subscription covers workspace access for their accountant or auditor — removes the economic friction from this adoption path.

The firm-first strategy is amplified by CryptaCount's Luxembourg base. As a Luxembourg-registered entity, CryptaCount has direct access to the Luxembourg financial services ecosystem, including the accounting community, and the broader EU regulatory landscape.

Businesses

Companies holding or transacting in digital assets need more than a tax calculator. They need ongoing accounting infrastructure that integrates with their financial workflows, supports multi-entity structures, and produces the documentation required by their auditors and regulators. CryptaCount provides this as a self-service platform with full workspace control.

Auditors

The audit profession faces a unique challenge with digital assets: verifying positions and transactions that exist on public but technically complex ledgers. CryptaCount's reconciliation capabilities, tamper-evident journal records, and complete audit trails provide the infrastructure that audit engagements require — independent verification, traceable methodology, and documented evidence.

A Consumer Path

Beyond the B2B market, the same accounting methodology and multi-chain data infrastructure can serve individual taxpayers through a simplified, consumer-facing experience. This path — operating under a distinct brand and pricing model — becomes viable once the core platform demonstrates product-market fit in the professional segment. The consumer product reuses the same computational foundation while providing an interface optimized for individual tax reporting rather than professional accounting practice.

The Enduring Thesis

CryptaCount's long-term thesis is straightforward: as digital assets become a permanent feature of the global financial system, the accounting profession will require purpose-built infrastructure to serve this market. That infrastructure must be as rigorous, auditable, and professionally-oriented as the tools accountants use for traditional financial reporting.

The firms and platforms that establish this infrastructure early — with genuine depth in accounting methodology, broad blockchain coverage, and multi-jurisdictional tax knowledge — will define the standard for how digital assets are accounted for in the decades ahead.

CryptaCount is building that infrastructure.

Security and Data Integrity

For a platform handling financial data, security is not a feature — it is a prerequisite. CryptaCount implements security across three domains: data integrity (ensuring accounting records are trustworthy), access control (ensuring only authorized users see and modify data), and operational security (ensuring the platform itself is resilient and compliant).

Data Integrity

Tamper-Evident Ledger

Every journal entry created by the accounting engine is cryptographically hashed. Each hash incorporates the entry's content and the hash of the preceding entry, forming a chain. This provides tamper evidence: if any historical journal entry is modified, the chain breaks from that point forward, making unauthorized changes immediately detectable.

This mechanism does not prevent modification — it makes modification visible. This is the appropriate guarantee for accounting records, where corrections are sometimes necessary but must always be transparent and traceable.

Double-Entry Enforcement

The platform enforces double-entry accounting as an invariant. Every journal entry must balance — total debits must equal total credits. Entries that fail this validation are rejected before they are persisted. This eliminates the category of errors where one-sided adjustments create unexplained balance discrepancies.

On-Chain Reconciliation

Computed balances (derived from processing all ingested transactions) are reconciled against actual on-chain balances. For each wallet and asset, the platform compares what the transaction history says the balance should be against what the blockchain reports it actually is.

Discrepancies indicate missing transactions, synchronization gaps, or classification errors. This independent reconciliation has been validated against block explorers for multiple chains with exact matching, establishing that the data pipeline produces complete and accurate records.

Access Control

Role-Based Permissions

The platform's four-tier role system (Platform Role, Account Type, Workspace Role, Company Role) ensures that every action is authorized across all applicable permission dimensions before it is executed.

This prevents both horizontal privilege escalation (accessing another user's data) and vertical privilege escalation (performing administrative actions without appropriate authorization). Permission checks are enforced consistently across all platform interactions, regardless of access method.

Administrative Segregation

Administrative functions (user management, system monitoring, data management) are fully segregated from standard accounting operations. Users without administrative privileges cannot access administrative functions through any means. This separation reduces the surface area for accidental or unauthorized administrative actions.

Authentication and Session Security

Bot and Abuse Prevention

All authentication flows are protected by invisible risk-scoring that evaluates each request's likelihood of being automated. Requests that score below the confidence threshold are blocked, protecting against credential stuffing, brute force attacks, and automated account creation.

Session Management

User sessions employ industry-standard protections:

- **Encrypted, tamper-resistant session tokens** — Session credentials cannot be intercepted or modified in transit
- **CSRF protection** — Cross-site request forgery attacks are mitigated
- **Automatic session expiry** — Inactive sessions are terminated after a defined period
- **Concurrent session controls** — Limits on simultaneous active sessions per account

Privacy and GDPR Compliance

Cookie Consent

The platform implements a two-layer GDPR-compliant cookie consent mechanism. The first layer presents a clear consent banner; the second layer provides granular control over cookie categories. No tracking technologies are activated before explicit consent is granted.

Data Handling Principles

- **Lawful basis** — Core accounting functions operate under contractual necessity (GDPR Article 6(1)(b)). Analytics operate only under explicit consent (Article 6(1)(a)).
- **Data subject rights** — Users can exercise access, rectification, erasure, and portability rights through their account settings and through a dedicated opt-out page for non-authenticated requests.
- **Blockchain data** — Publicly available blockchain data is processed under the legitimate interest of providing the accounting service.

Operational Security

Data Encryption

All data is encrypted in transit and at rest. Customer data at rest is protected using industry-standard encryption. Network communications between all platform components use TLS encryption.

Data Residency

All customer data is hosted within EU data centers, ensuring compliance with GDPR data transfer requirements and providing data sovereignty assurance for EU customers.

Automated Backups

Database backups are performed automatically on a continuous schedule. Backups are encrypted and stored in geographically separate locations from primary data to ensure recoverability in disaster scenarios.

Secrets Management

All platform credentials and sensitive configuration are stored in dedicated, access-controlled secrets infrastructure — never in source code, configuration files, or application logs.

Deployment Integrity

All platform updates are deployed through an automated, auditable pipeline. Every deployment is traceable to a specific, reviewed change. No manual server access is required or permitted for production deployments.

SOC 2 Readiness

The platform's security controls — access management, encryption, audit logging, change management, and data handling — are designed to align with SOC 2 Type II trust service criteria (Security, Availability, Confidentiality, Processing Integrity, Privacy). Formal certification is on the compliance roadmap.

Audit Trail

Every significant action on the platform is logged in an immutable audit trail:

- Transaction classification changes
- Cost basis method modifications
- Journal entry creation and any corrections
- User access grants and revocations
- Data export events
- Workspace and company configuration changes

This audit trail provides the evidentiary foundation that auditors require to assess the integrity and consistency of accounting records produced by the platform.

Multi-Jurisdiction Tax Coverage

CryptaCount maintains structured tax profile data for 73 jurisdictions, covering the majority of global crypto markets. Each profile models jurisdiction-specific rules across three domains: reporting obligations, business (B2B) tax treatment, and individual (B2C) tax treatment.

Tax Profile Structure

Each jurisdiction's profile is organized as structured data across three domains:

Domain	Coverage	Example Data Points
REPORTING	Filing obligations, reporting thresholds, disclosure requirements	Reporting deadlines, de minimis thresholds, required forms
TAX_B2B	Business entity tax treatment of crypto-assets	Corporate tax rates, permitted cost basis methods, depreciation rules, VAT treatment
TAX_B2C	Individual tax treatment of crypto-assets	Capital gains rates, holding period exemptions, income classification, loss offset rules

This structured approach allows the platform to present jurisdiction-specific guidance alongside computed accounting data without making the tax determination itself. An accountant working on a German client's crypto portfolio sees Germany's specific rules (staking holding period abolished in 2022, 1-year holding period exemption for capital gains on other disposals) alongside the calculated gains and losses.

Regional Coverage

European Union

All 27 EU member states are covered, plus the EEA states (Norway, Iceland, Liechtenstein) and Switzerland. EU coverage includes DAC8 reporting alignment, MiCA-relevant treatment, and each member state's domestic crypto tax rules, which vary significantly despite the common framework.

Key EU jurisdictional variations:

- **Germany** — 1-year holding period exemption for capital gains; staking holding period extension was abolished in 2022; €600 annual exemption threshold
- **France** — Mandatory portfolio-wide weighted average cost formula for individuals; flat 30% prélèvement forfaitaire unique (PFU) for occasional traders
- **Italy** — Tax rate increased to 33% from January 2026; 14% substitute tax option available
- **Portugal** — 1-year holding period exemption enacted January 2023; 28% rate for short-term gains
- **Luxembourg** — Private companies use Luxembourg GAAP (not IFRS); 6-month holding period exemption for individuals
- **Czech Republic** — 3-year holding period exemption enacted February 2025

North America

United States and Canada are fully covered, including state/provincial variations where materially different.

- **United States** — Capital asset treatment (property, not currency); no wash sale rule applicable to crypto (as of 2025); FIFO default; cost basis reporting requirements per broker; Form 8949 / Schedule D alignment
- **Canada** — 50% capital gains inclusion rate; business income vs capital gains distinction; mining/staking treated as business income or capital depending on activity level

Asia-Pacific

Coverage includes major crypto markets: Japan, South Korea, Australia, Singapore, Hong Kong, India, and others.

- **South Korea** — Crypto tax implementation deferred to 2027; 20% rate on gains above ₩2.5M when enacted
- **Japan** — Miscellaneous income classification; up to 55% marginal rate; total average method required
- **Australia** — Capital gains tax with 50% CGT discount for assets held >12 months; crypto-to-crypto is a taxable event
- **Singapore** — No capital gains tax; trading income taxable for businesses
- **India** — 30% flat rate on gains, 1% TDS on transfers above ₹10,000

Middle East and Africa

Coverage includes UAE, Israel, South Africa, and other jurisdictions with emerging crypto regulatory frameworks.

- **UAE** — No personal income tax; corporate tax (9%) applies to crypto business income above AED 375,000; free zones may provide exemptions

Latin America

Brazil, Argentina, Mexico, and other major markets in the region.

- **Brazil** — Progressive rates 15–22.5% on monthly gains; mandatory exchange reporting for offshore holdings

Data Accuracy and Corrections

The tax profile dataset undergoes continuous verification to ensure accuracy. Notable corrections in the current dataset include:

Jurisdiction	Correction	Impact
United States	Wash sale rule confirmed as inapplicable to crypto	Cost basis calculations do not account for wash sale adjustments
Germany	Staking holding period extension removed (abolished 2022)	1-year standard exemption applies regardless of staking activity
France	Portfolio-wide weighted average formula specified	Mandatory individual method for French taxpayers
Italy	Tax rate updated to 33% from January 2026	Rate tables updated with effective date
Denmark	Inventory method noted as proposed only, not enacted	Flagged as pending legislation
South Korea	Tax implementation deferred to 2027	No active tax computation required
Czech Republic	3-year holding period exemption added (Feb 2025)	Exemption logic included in tax profile

Portugal	1-year holding period exemption added (Jan 2023)	Exemption logic included in tax profile
Luxembourg	Private company GAAP noted as Lux GAAP, not IFRS	Treatment distinction surfaces in business profile

Jurisdiction Data Maintenance

Tax rules change frequently. The platform's jurisdiction profiles are maintained as versioned, structured data. Updates to tax rates, thresholds, holding period rules, or method requirements are applied as data changes — they do not require platform updates.

Each profile record carries an effective date, allowing the platform to apply the correct rules for historical periods (e.g., using Italy's pre-2026 rate for transactions in 2025 while using the 33% rate for 2026 transactions). This temporal versioning ensures that retrospective reporting remains accurate even as rules evolve.

Platform Overview

CryptaCount's platform is built around three operational principles: reliability, security, and auditability. Every design decision prioritizes the evidential standards required by accounting professionals and the data protection requirements of handling sensitive financial information.

Operational Principles

Reliability

The platform is designed for continuous availability with automatic scaling to handle peak workloads — particularly during high-volume blockchain synchronization periods. The infrastructure scales efficiently to accommodate growing client portfolios and increasing transaction volumes without degradation in performance or data quality.

ACID-Compliant Data Operations

All accounting operations — journal generation, cost basis calculation, balance updates — execute atomically. There are no partial writes and no race conditions. If any step in a multi-part accounting operation fails, the entire operation is rolled back to maintain data consistency. This is non-negotiable for financial data integrity.

Data Isolation

Each workspace's data is logically isolated. Cross-tenant data access is prevented at every layer of the platform. A user with access to one workspace cannot access, query, or infer the existence of another workspace's data.

Security Posture

Encryption

- **In transit** — All communications between users and the platform, and between platform components, are encrypted using current industry-standard protocols

- **At rest** — All persisted data, including database contents and backup archives, is encrypted

Access Controls

- **Four-tier role-based access** — Permissions are evaluated across platform, account, workspace, and company dimensions before any action is authorized
- **Administrative segregation** — Administrative functions are isolated from standard accounting workflows
- **Audit logging** — Every significant action is recorded in an immutable audit trail

Compliance Posture

- **GDPR compliant** — EU data residency, lawful processing basis, full data subject rights, two-layer cookie consent
- **SOC 2 aligned** — Controls designed to trust service criteria standards (Security, Availability, Confidentiality, Processing Integrity, Privacy)
- **PCI-compliant payments** — Payment processing handled through certified payment infrastructure

Data Handling

What We Store

- **Blockchain transaction data** — Publicly available on-chain data, normalized and classified for accounting purposes
- **Accounting records** — Journal entries, cost basis calculations, rollforward schedules, and classification decisions generated by the platform
- **User account data** — Authentication credentials (hashed, never stored in cleartext), profile information, and workspace configuration
- **Pricing data** — Fair market value and foreign exchange rates used for transaction valuation and reporting

What We Do Not Store

- **Private keys** — CryptaCount never requests, receives, or stores private keys or seed phrases. The platform is read-only with respect to blockchain data; it cannot initiate, sign, or execute transactions on any blockchain.
- **Raw credentials** — Passwords and sensitive tokens are stored only in irreversible hashed form
- **Unnecessary personal data** — Data collection follows the GDPR principle of data minimization

Data Retention

Accounting data is retained for the duration of the customer relationship plus the legally required retention period for financial records in the applicable jurisdiction. Users can exercise data erasure rights subject to these legal retention obligations.

Availability and Disaster Recovery

- **Automated backups** — Continuous, encrypted, geographically distributed
- **Automatic scaling** — Platform scales dynamically based on demand, from periods of low activity through peak synchronization loads
- **EU data residency** — All primary data and backups hosted within EU data centers

Intellectual Property

CryptaCount operates under a proprietary license. The platform's competitive differentiation lies in the depth and correctness of its accounting methodology, the breadth of its multi-chain data coverage, and the comprehensiveness of its jurisdictional tax dataset — reflecting years of domain-specific research and implementation in the intersection of blockchain technology and professional accounting.

Four-Theme User Experience

The platform provides a four-theme visual system (Nexus, Forge, Arctic, Classic) with light and dark modes, allowing accounting professionals to customize their working environment to their preference.

The interface is designed for extended use during accounting engagements, with attention to readability, information density, and workflow efficiency.

Thank you for reading

Product

app.cryptacount.com

Documentation

docs.cryptacount.com

Website

www.cryptacount.com
