JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

# Virtual Currency Exposure and Wallet Safekeeping Training Course

27 – 31 December 2026
Muscat

# Virtual Currency Exposure and Wallet Safekeeping Training Course

**Ref:** 2410_90729 **Date:** 27 – 31 December 2026 **Location:** Muscat **Fees:** 5500 GBP

Virtual Currency Exposure and Wallet Safekeeping is a 1-week training course for bank treasury, risk and product staff who must judge how cryptoassets, stablecoins and central bank digital currency reach the balance sheet, with a digital asset risk assessment as the work product. Clients and payment partners now use tokens daily, so unseen exposure grows. Jupiter Prime Training sets the subject in its banking context.

## Why Virtual Currency Exposure and Wallet Safekeeping Matters Now

Three forces shape the subject today. Corporate clients and fintech partners settle more value in tokens, pulling banks into flows they did not design. Supervisors expect a clear view of holdings, borrower links and key safekeeping. Central banks are testing their own digital money, which may change deposit behaviour and payment rails. Banks that map these links early serve token-active clients well; others risk frozen funds, lost keys and reputational damage. The course rests on widely used risk taxonomy, key custody practice and token classification logic, described in general terms.

## Who Gains Most from Virtual Currency Exposure and Wallet Safekeeping

- Treasury staff who handle liquidity, settlement accounts and stablecoin-linked client balances
- Market and credit risk staff who rate counterparties with token activity
- Product staff who shape payment, custody or tokenised deposit offers
- Operational risk and control staff who test wallet procedures and key ceremonies
- Financial crime staff who screen wallet addresses and on-chain flows

Banks that send treasury, risk and product colleagues together gain most, as each sees the same exposure from a different seat.

## Virtual Currency Exposure and Wallet Safekeeping Capabilities

Participants trace a token from client request to ledger entry and rate what could fail at each point.

- Classify a token by its backing, issuer and redemption rights — product approval committees
- Map direct, indirect and contingent token exposure across the book — treasury and credit limits
- Assess stablecoin reserve quality and redemption mechanics — counterparty and liquidity decisions
- Compare hot, warm and cold wallet set-ups with multi-party key schemes — custody design choices
- Weigh how central bank digital currency could shift deposits and payment flows — strategy and funding teams

- Build a scored exposure register with controls and owners — the board risk committee

## Key Virtual Currency Exposure and Wallet Safekeeping Terms

- Cryptoasset — a digital token recorded on a distributed ledger, with value set by the market rather than by an issuer promise.
- Stablecoin — a token designed to hold a steady value against a reference asset, usually backed by a reserve pool.
- Central bank digital currency — a digital form of money issued directly by a central bank.
- Private key — the secret code that authorises movement of tokens; whoever holds it controls the assets.
- Cold wallet — a key store kept offline, used to protect larger balances from network attack.
- Depeg event — a period when a stablecoin trades away from its target value, often triggering redemption pressure.

## Virtual Currency Exposure and Wallet Safekeeping Day by Day

### Day 1: The Token Landscape for Banks

- Token Classification Grid — Which Products Fall Inside Bank Appetite
- Public and Permissioned Ledgers — Settlement Finality and Reversal Limits
- Stablecoin Backing Models — Reserve, Collateral and Algorithmic Design Trade-Offs
- Retail and Wholesale Central Bank Digital Currency — Deposit and Payment Impact
- Client Token Activity Survey — Where Hidden Exposure Already Sits

### Day 2: Measuring Token Exposure

- Direct Holdings Ledger — Treasury Positions and Concentration Limits
- Indirect Borrower Exposure Mapping — Credit Ratings for Token-Active Clients
- Stablecoin Issuer Due Diligence File — Reserve Attestation and Redemption Queues
- Price Shock and Depeg Scenarios — Liquidity Buffers and Margin Calls
- Exposure Heat Map — Prioritising Business Lines for Control Work

### Day 3: Wallet Safekeeping and Key Control

- Hot, Warm and Cold Wallet Tiers — Balance Limits per Tier
- Multi-Signature and Multi-Party Computation Schemes — Who Can Approve Transfers
- Key Generation Ceremony Script — Segregation of Duties and Witness Roles
- Sub-Custodian Selection Checklist — Outsourcing Choices and Exit Clauses
- Key Loss and Theft Playbook — Recovery Steps and Client Notice

### Day 4: Controls, Screening and Product Decisions

- Wallet Address Screening Rules — Onboarding Token-Active Clients Safely
- On-Chain Flow Monitoring — Alert Thresholds and Escalation Paths
- Tokenised Deposit Product Sheet — Pricing, Disclosure and Redemption Terms
- Smart Contract Risk Review — Code Audit Evidence and Upgrade Rights
- New Product Approval Pack — Committee Questions for Token Offers

## Day 5: Practising the Digital Asset Risk Assessment

- Token Inventory Walk-Through — Applying the Classification Grid to Live Cases
- Exposure Scoring Exercise — Combining Direct, Indirect and Issuer Ratings
- Safekeeping Control Test — Checking Wallet Tiers Against Balance Limits
- Peer Challenge Panel — Defending Ratings Before Treasury and Product
- Digital Asset Risk Assessment — Final Register, Owners and Escalation Triggers

## Applying Virtual Currency Exposure and Wallet Safekeeping After the Course

- Run a client token activity survey across two business lines and feed the results into the exposure heat map.
- Test the wallet tier limits and key ceremony script with operations, then record gaps and owners in the register.

## Virtual Currency Exposure and Wallet Safekeeping Questions FAQ

### What is virtual currency exposure and wallet safekeeping, and why does it matter now?

It is the practice of measuring how tokens reach a bank and protecting the keys that control them. It matters now because token use is rising and weak links can freeze funds.

### Which roles gain most from virtual currency exposure and wallet safekeeping skills?

Treasury, risk and product staff gain most. Each sees a different side: liquidity, counterparty ratings or product terms.

### How does virtual currency exposure and wallet safekeeping differ from a crypto trading or token accounting course?

It looks at a bank's exposure and safekeeping rather than trading strategy or bookkeeping. You rate client, issuer and custody links and set controls rather than forecast prices.

### What do you bring back from virtual currency exposure and wallet safekeeping training?

You bring back a scored register of token exposure with named controls and owners. It supports limit setting, product approval and onboarding.

## Virtual Currency Exposure and Wallet Safekeeping: The Way Forward

The digital asset risk assessment first informs whether the bank widens or narrows its appetite for token-active clients. Treasury uses it to set limits, risk staff to plan tests and product staff to shape offers. After first use, revisit the safekeeping section as wallet technology and central bank digital currency pilots mature.