ERC-3643 Tokens as Collateral for Institutional OTC Derivatives

February 2026

Contributors

Anaïs Ofranc - QualitaX
Stefan Haupt - QualitaX
Joachim Lebrun - Apex/Tokeny
Robin Jelin - T-REX.network
Nicolas Lebrun - T-REX.network
George Gledhill - CMS
Charles Kerrigan - CMS
Dylan Walter - CMS
Ghazi Ben Amor - Zama
Ash Nathan - Chainlink
De Clercq Wentzel - Chainlink
Sahil Sood - Zodia Custody
Steven Taylor - Zodia Custody
Olivia Vande Woude - Ava Labs
Pat Hourigan - Frictionless Markets

QX

Table of contents

Introduction 5
Case Study: USD/BRL NDF Portfolio 6
Business Context 6
Key Considerations 8
Scope 12
High-Level Overview 14
Approach 14
Data Confidentiality 15
Custody Integration 15
ERC-3643 Standard 15
CRE Workflows 17
Key Smart Contract 20
PoC Test Data 23
Conclusion 24

Overview

This paper explores whether ERC-3643 compliant stablecoins can serve as eligible collateral for non-regulatory variation margin in institutional OTC derivative operations. We present a proof of concept ("PoC") that tests the integration of blockchain-based settlement infrastructure with traditional OTC derivatives workflows, using USD/BRL non-deliverable forwards ("USD/BRLNDFs") as the reference instrument. The proof of concept addresses three requirements critical to institutional adoption: maintaining confidentiality of commercial data, providing regulators with independently verifiable compliance records, and minimizing trust dependencies between counterparties. Our findings demonstrate that a USD-pegged stablecoin leveraging ERC-3643's embedded compliance architecture offers material advantages for regulated financial institutions, while introducing manageable new risks that can be mitigated through appropriate haircuts, circuit breakers, and fallback mechanisms considerations.

Introduction

Daily variation margin (VM) for Over-the-Counter (OTC) bilateral derivative transactions involves counterparties exchanging collateral daily to cover changes in the value (i.e. mark-to-market) of such transactions. The daily exchange of variation margin is one of the most operationally intensive functions in bilateral OTC derivatives trading. Each exchange of collateral triggers wire transfers constrained by banking hours, correspondent networks, and manual reconciliation workflows. For a business that prices and trades around the clock, the infrastructure supporting collateral movement remains stubbornly tethered to the limitations of traditional payment rails.

Digital assets such as stablecoins present a compelling alternative. A dollar-denominated token that settles in minutes, operates continuously, and executes programmatically could fundamentally change how margin flows between counterparties. Yet the appeal comes with meaningful risks: stablecoins can and do deviate from their pegs, smart contracts can fail, and regulatory frameworks remain unsettled in key jurisdictions.

This document describes a proof of concept designed to explore how a financial institution bound by prudential requirements and fiduciary obligations can leverage a USD stablecoin based on the ERC-3643 standard. Our case study aims at testing whether an ERC-3643 USD stablecoin can serve as eligible collateral for non-regulatory variation margin on USD/BRL non-deliverable forwards. The proof of concept architecture addresses three imperatives that any institutional deployment must satisfy: maintaining strict confidentiality of commercial data, providing regulators with independently verifiable compliance records, and minimizing trust dependencies through neutral third-party infrastructure.

We cover the operational workflows to be implemented, the risks to be monitored, and the success criteria against which results should be evaluated. Our goal is to help assess whether an ERC-3643 USD stablecoin can work within the constraints that govern institutional derivatives operations.

It is important to note that while this proof of concept uses USD/BRL NDFs as the reference instrument, the settlement architecture is instrument-agnostic. The same infrastructure could support variation margin settlement for any bilateral, cash-settled OTC derivative denominated in USD—including interest rate swaps, credit derivatives, and equity swaps. The choice of NDF serves to illustrate specific operational pain points, not to constrain applicability.

Please note that this proof of concept contemplates only the transfer of non-regulatory variation margin and does not cover variation margin required to be transferred by parties that are in scope of any applicable regulatory margin regime.

Case Study: USD/BRL NDF Portfolio

The selected case study explores how an investment bank and a hedge fund can operationalize daily margin settlement using blockchain infrastructure while maintaining the confidentiality, regulatory verifiability, and risk controls that institutional finance demands. The proof of concept focuses on USD/BRL NDFs, considers automatic fallback mechanisms for depeg scenarios, and leverages Chainlink's CRE infrastructure. For the daily margin calls, we created an ERC-3643 USD stablecoin on testnet ("CTT Token").

Why focusing on daily variation margin (VM): Appropriate fit for a USD-pegged stablecoin because it is bilateral, frequent, and reversible. The operational pain points an ERC-3643 stablecoin solves are real:

- **Settlement speed**: USD wires via traditional rails have cutoff times (typically 5-6pm ET). An ERC-3643 token can settle in ~seconds. This eliminates the timezone arbitrage problem for counterparties in different regions.
- **Reduced nostro/vostro friction**: Banks currently pre-fund accounts at correspondent banks to ensure same-day settlement. An ERC-3643 USD-pegged token could remove the need for this trapped liquidity.
- **Weekend/holiday coverage**: Brazil is notorious for local holidays (Carnival, Corpus Christi) that create settlement mismatches. An ERC-3643 token can move 24/7/365.

Why USD/BRL NDF as an example? In the BRL market, "Onshore" (BMF) and "Offshore" (NDF) rates often diverge because of the difficulty in moving USD in and out of Brazil. If the Bank can settle the offshore NDF in ERC-3643 token instantly, they can more efficiently hedge their risk against other digital liquidity providers, potentially narrowing the bid-ask spread they offer their counterparties. By using an ERC-3643 USD stablecoin, the Bank might actually improve the pricing of the NDF for the Hedge Fund.

Business Context

The Problem

Traditional variation margin settlement via traditional transfer faces several friction points:

Challenge	Impact
Banking hours constraint	If margin calls generated after hours wait until next day
Weekend/holiday gaps	No settlement Friday evening through Monday morning
Cross-border delays	International wires can take 1-2 days
Correspondent banking fees	Additional cost adds up across frequent margin calls
Operational overhead	Often manual initiation, reconciliation, and confirmation

The Opportunity

A USD-pegged stablecoin offers potential advantages for margin settlement:

Benefit	Mechanism
24/7/365 availability	Blockchain Infrastructure operates continuously
Near-instant settlement	Transfer confirms in seconds/minutes, not hours/days
Programmable logic	Smart contracts can enforce certain terms of the CSA (as defined below) automatically
Lower transaction costs	Gas fees typically significantly cheaper than wire fees
Real-time transparency	Both parties see transfer immediately on-chain

While recognizing the benefits, we also acknowledge the new risks introduced that require careful evaluation:

- **Depeg risk**: A ERC-3643 USD-pegged stablecoin could trade below $1.00
- **Smart contract risk**: Vulnerabilities in token contract or custody infrastructure
- **Operational risk**: New workflows, wallet/onchainID management, key security
- **Regulatory uncertainty**: Evolving guidance on stablecoin use in regulated finance
- **Counterparty readiness**: Not all counterparties have digital assets operational capability. Ideal counterparties would be digital asset-focused macro hedge funds, prop trading firms with digital asset desks or corporate treasury of a crypto-native company hedging USD/BRL exposure (exchange, mining operation with Brazil presence).

The Actors

Role	Entity	Responsibilities
Dealer	Investment Bank	Calculate VM, manage collateral ledger, custody integration
Counterparty	Digital Asset Native Hedge Fund	Post/receive stablecoin margin, maintain wallet infrastructure
Custody Provider	Zodia Custody	Secure key management, transaction signing
Orchestration	QualitaX leveraging Chainlink CRE	Depeg monitoring, settlement attestation
Stablecoin Issuance	Stablecoin Issuer	Stablecoin issuance, redemption
Tokenization	Tokeny	Platform used to create CTT Token

Key Considerations

Integrating stablecoin-based settlement into existing OTC derivatives infrastructure requires careful attention to legal, risk management, and regulatory dimensions. The established frameworks governing bilateral margin arrangements were designed for traditional assets and fiat currencies, meaning that novel digital assets require explicit accommodation within these structures. Three areas demand particular focus: contractual amendments to existing credit support arrangements, management of risks unique to stablecoin collateral, and clarity on prudential capital treatment.

Legal Documentation

For an ERC-3643 USD-pegged stablecoin to serve as effective collateral for variation margin in OTC derivative transactions, as contemplated by this PoC, the underlying legal documentation (which constitutes the legal framework on which counterparties rely) must accurately reflect how the PoC is intended to operate in practice.

For this PoC, the legal documentation would follow the established International Swaps and Derivatives Association's ("ISDA") framework and consist of the following:

- 2002 ISDA Master Agreement;
- Confirmations (incorporating, where applicable, ISDA published Definitions), which would document the relevant USD/BRL NDFs; and
- 1995 Credit Support Annex (English law) (the "CSA"), which would govern the transfer of ERC-3643 USD-pegged stablecoin as collateral

For the purposes of this report, we focus solely on the CSA. There are, however, additional considerations in relation to the underlying legal documentation. By way of example, careful attention would need to be given to the drafting of any Confirmation for a USD/BRL non-deliverable forward to ensure that it accurately reflects the agreed commercial terms of the transaction. Such matters are outside the scope of this report.

<u>Overview of the 1995 Credit Support Annex</u>

The CSA operates as an annex to the relevant ISDA Master Agreement. It governs the transfer of collateral between the parties to ensure that a party's net exposure across all outstanding OTC derivative transactions under the relevant ISDA Master Agreement is appropriately collateralised.

Two key overarching principles of the CSA are that:

- collateral is transferred by way of title transfer; and
- the receiving party has full rehypothecation rights in respect of the transferred collateral.

The use of ERC-3643 USD-pegged stablecoin as collateral, as contemplated by this PoC, must therefore be structured so as not to impinge upon these fundamental principles.

Amendments to the 1995 Credit Support Annex

As mentioned above, the CSA used by eligible counterparties must accurately reflect the operational reality of this PoC, as, in the event of any misalignment or dispute, the provisions of the CSA would ultimately govern.

Accordingly, the following amendments would be required to the CSA. Please note that this is not intended to be an exhaustive list.

Eligible Collateral

Only assets specified in the CSA as "Eligible Credit Support" can be transferred as collateral thereunder. The CSA would therefore need to specify ERC-3643 USD-pegged stablecoins as Eligible Credit Support.

Valuation

The CSA contemplates only cash and securities as eligible collateral and, accordingly, includes valuation provisions solely for those asset types. As a result, the CSA will need to be amended to include valuation provisions for ERC-3643 USD-pegged stablecoins, in order to determine, among other things, the quantity of such stablecoins required to satisfy a margin call and the value of any such stablecoins posted as collateral. It is important that these valuation provisions are drafted with sufficient clarity and transparency to reduce the risk of dispute.

Any haircuts applied to the ERC-3643 USD-pegged stablecoins (as further discussed in "De-pegging risk management" below) will need to be reflected in the CSA. This would be achieved by specifying a Valuation Percentage for such stablecoins of less than 100%.

Transfers

The CSA includes transfer provisions only for cash and securities. Accordingly, it would need to be amended to incorporate provisions governing the transfer of ERC-3643 USD-pegged stablecoins.

ISDA has published tokenised collateral model provisions intended for use where parties transfer tokenised securities or stablecoins as collateral. Although these provisions were developed primarily for use with ISDA's Credit Support Annexes for Variation Margin (VM), they could also be used as a basis to expand the transfer mechanics in the CSA to accommodate transfers of ERC-3643 USD-pegged stablecoins.

For the avoidance of doubt, ISDA's Credit Support Annexes for Variation Margin (VM) were introduced to enable parties to comply with regulatory variation margin requirements. As noted above, this report considers only the transfer of non-regulatory variation margin (for which the 1995 Credit Support Annex is more commonly used).

Furthermore, the "Transfer Mechanics" section below sets out when settlement finality is achieved in respect of a transfer of ERC-3643 USD-pegged stablecoins and confirms that any associated gas fees are payable by the transferor. These points will need to be reflected in the CSA.

In addition, this PoC contemplates that, in the event of a failed transfer of ERC-3643 USD-pegged stablecoins (for example, as a result of a technical fault in the underlying blockchain), USD could potentially be transferred as collateral as a fallback. Any such fallback arrangement would need to be appropriately documented in the CSA.

An alternative approach to addressing settlement disruption would be to include a grace period to cover any failure to transfer, so that a purely technical failure does not immediately constitute an Event of Default and give the "non-defaulting" party the right to terminate and close out all USD/BRL NDFs between the parties.

Transfer timing

The CSA uses a notice-and-demand framework, and the timing of the relevant collateral transfer depends on when the demand for collateral is made. Generally speaking under the CSA, if the demand is made by the notification time, the transfer must be made by close of business on the next business day (i.e. T+1) and if the demand is made after the notification time, the transfer must be made by close of business on the second business day following the date of such demand (i.e. T+2).
However, under this PoC, the transfer of ERC-3643 USD-pegged stablecoins as collateral differs materially from the CSA's standard notice-and-demand framework (for example, including a significantly shorter settlement window). The CSA will therefore need to be amended to reflect this.

De-peg checks

As noted in the "De-peg checks" section below, this PoC considers a number of specific checks in the event of a de-peg affecting the ERC-3643 USD-pegged stablecoins, including (without limitation) the inclusion of an Additional Termination Event (exercisable by either party) where such stablecoins deviate materially from USD for sustained period.
The CSA (together with the other underlying legal documentation) will therefore need to include provisions to give effect to the "De-peg checks" described in this report.

Other Considerations

In addition to the above, there are a number of other considerations when using the CSA for this PoC. These include (without limitation) the following:

On-chain vs off-chain

Whilst certain provisions of the CSA (and the 2002 ISDA Master Agreement) can be effected or automated on-chain, a number of important provisions require off-chain discretion and determination. These include, without limitation, the calculation of a counterparty's mark-to-market exposure, dispute resolution, the determination of market or underlying disruption events, and the determination of whether an Event of Default or Termination Event has occurred (together with the subsequent calculation of any early termination amount).

This PoC will therefore need to ensure that any action taken, or determination made, off-chain is accurately and promptly reflected at the smart-contract level, so as to avoid any misalignment between the legal position and the on-chain mechanics.

What happens upon enforcement?

There is no concept of “enforcement” of collateral under the CSA, as collateral is transferred outright by way of title transfer. Accordingly, if a party defaults and all OTC derivative transactions are terminated under the relevant ISDA Master Agreement, equivalent collateral is not returned to the transferor in those circumstances.

Instead, the CSA constitutes a terminated “Transaction” under the ISDA Master Agreement for determining the close-out. The value of the transferred collateral is treated as an “Unpaid Amount” payable by the transferee to the transferor and forms part of the calculation of the single early termination amount.

Therefore, if this PoC were to contemplate the return of ERC-3643 USD-pegged stablecoins following a counterparty default, the underlying legal documentation would need to be amended to reflect this outcome.

Legal enforceability

There is also a broader question around the enforceability of collateral arrangements involving the transfer or exchange of digital assets in particular jurisdictions. This will need to be considered on a case-by-case basis depending on the eligible counterparties.

It should however be noted that ISDA is actively exploring the use of tokenized collateral (including stablecoins) in the OTC derivatives market, working with market participants and experts to address the legal, regulatory and operational challenges to effective adoption. A central focus is the development of clear and consistent legal and regulatory frameworks, supported by robust documentation and legal opinions, so that OTC derivatives transactions collateralised by tokenised assets can be managed with the same confidence as those secured by traditional instruments.

De-pegging risk management

While stablecoin settlement eliminates traditional settlement lag, it introduces a risk factor absent from the traditional USD cash model: the basis risk of the stablecoin itself.

The core concern is the potential valuation gap between the stablecoin and its USD peg. An NDF is a contract referencing USD/BRL, and if a stablecoin held as collateral experiences a depeg event, the portfolio becomes under-collateralized not because the BRL moved adversely, but because the collateral itself lost value. Although the ERC-3643 token issuer may maintain full 1:1 backing with underlying reserves, market price deviations can still occur. The March 2023 USDC depeg event, when Circle's stablecoin temporarily traded below par during the Silicon Valley Bank crisis, demonstrated that even well-backed stablecoins can experience intraday price disruption.

The standard mechanism for addressing this risk is the application of a haircut to stablecoin collateral. This means that such stablecoins would be valued below their nominal value for the purposes of determining margin calls, with the result that a party would need to transfer a nominal amount of stablecoins in excess of its counterparty’s overall OTC derivatives exposure in order to ensure that its counterparty is fully collateralised under the CSA. A

haircut in the range of 2% to 5% would provide a buffer against depeg events while still preserving much of the operational efficiency benefit.

The haircut compensates the collateral receiver for several risk components that the collateral poster introduces by delivering ERC-3643 tokens instead of USD. These include redemption delay risk arising from the issuer's settlement service level agreement, typically ranging from same-day to next-day, which creates opportunity cost during the waiting period. Depeg tail risk must also be considered, informed by historical maximum deviation data for the specific stablecoin. Smart contract risk, while mitigated through audits, remains non-zero for any blockchain-based system. Finally, operational risks including wallet errors, gas price spikes, and network congestion introduce additional uncertainty that the haircut must accommodate.

Clarify capital treatment

A critical question for bank adoption concerns the prudential treatment of stablecoin collateral. If a USD-pegged stablecoin is held as collateral, what risk weight applies for capital adequacy purposes?

Under Basel III, cash receives a 0% risk weight, reflecting its status as the ultimate risk-free asset. An ERC-3643 stablecoin, however, may receive different treatment depending on regulatory interpretation. It could be classified as a corporate exposure to the issuer, carrying a corresponding risk weight based on the issuer's credit rating. Alternatively, under the Basel Committee's framework for cryptoasset exposures finalized in 2022, it might be treated as a crypto-asset unless it qualifies for the more favorable stablecoin classification, which requires meeting specific criteria around redemption rights, reserve backing, and governance. Banks considering stablecoin adoption for margin purposes should engage with their prudential regulators to obtain clarity on applicable capital treatment before implementation.

Scope

This proof of concept covers USD/BRL Non-Deliverable Forwards executed bilaterally, meaning either party may owe variation margin depending on market movements. We assume here that eligible counterparties have the required legal documentation (as further described in the section “Legal Documentation Considerations” above) in place with the bank (i.e. the foundational legal documentation exists) which contain the necessary provisions to support implementation of a smart contract and that both parties have established operational connectivity for trade execution and lifecycle management.

Scenario Parameters

The proof of concept defines parameters designed to balance meaningful operational testing against prudent risk limits.

Parameter	Value	Rationale
Haircut	2%	Compensates for redemption delay, depeg tail risk
Settlement Window	2 hours from margin call	This would need to be reflected in CSA terms
Minimum Transfer	$100,000	Avoid gas cost inefficiency on small amounts
Blockchain	Ethereum (sepolia testnet)	Proven infrastructure

Transfer Mechanics

Stablecoin transfers operate under three governing principles. First,1) a transfer is considered complete when settlement attestation event is emitted, at which point settlement finality is achieved for purposes of the CSA. Second, 2) the transferor bears responsibility for all gas fees associated with the transaction, ensuring that the receiving party's margin position is not diminished by transaction costs. Third, 3) failed stablecoin transfers must be retried by the transferor, or alternatively substituted with USD wire transfer, before the settlement deadline expires. This fallback mechanism ensures that technical failures do not result in breaches of the underlying legal documentation (provided that the relevant CSA in place includes the relevant fallback provisions).
Please note that only 1) and 2) have been implemented as part of this PoC.

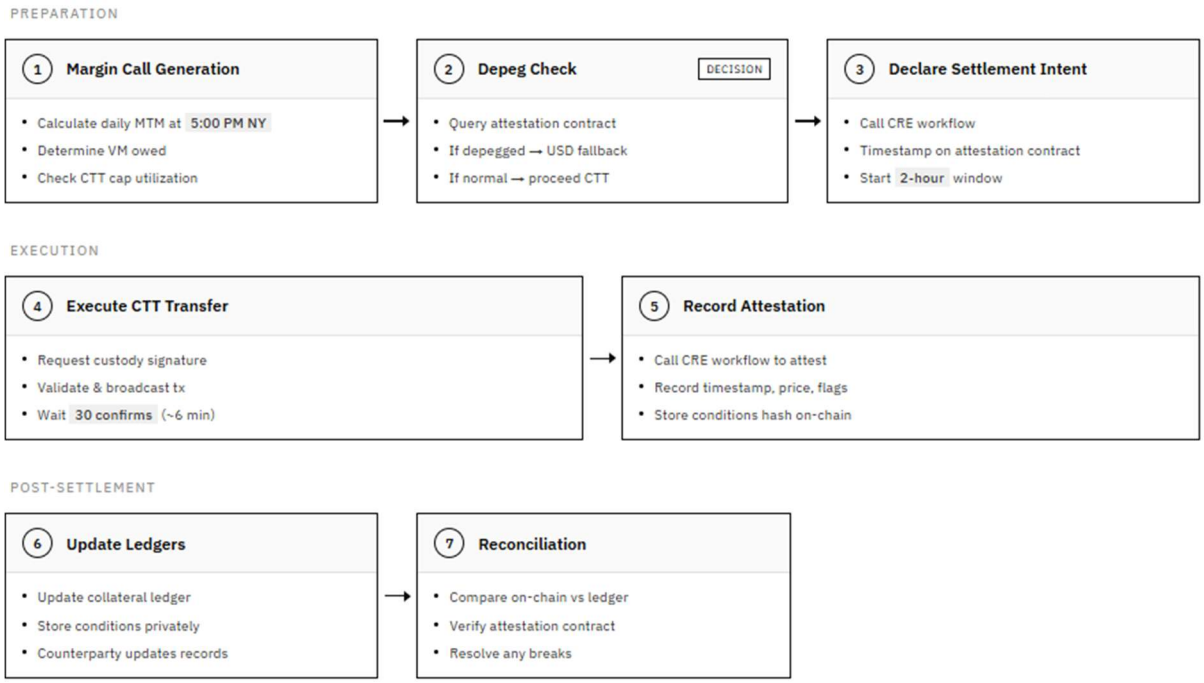
Depeg Checks

The PoC incorporates specific checks triggered upon a depeg event, defined as the stablecoin trading outside the 0.98 to 1.02 band against USD.
Upon occurrence of a depeg event, three protective measures activate. First, 1) no new stablecoin transfers are permitted until the event clears, ensuring that neither party is required to accept collateral of uncertain value during periods of market stress. Second, 2) existing stablecoin collateral held by either party is revalued at the prevailing market rate rather than par, ensuring that margin calculations accurately reflect actual collateral value. Third, 3) a severe depeg below $0.95 triggers an Additional Termination Event under the ISDA Master Agreement, providing either party the right to terminate affected transactions and close out positions if the stablecoin experiences sustained material deviation from its peg.

High-Level Overview

The proof of concept delivers a Daily Variation Margin (VM) Settlement System as a blockchain-based collateral management solution for financial derivatives combining:

- A test ERC-3643 Token (CTT Token) for regulatory-compliant transfers
- Chainlink Compute Runtime Environment (CRE) workflows for trustless automation
- Simulated Real-time price monitoring for depeg detection and risk management



Approach

Our approach prioritizes three foundational design principles. First, confidentiality ensures that no trade details, counterparty identities, or sensitive commercial information are stored on-chain or exposed to third parties. Second, regulatory verifiability provides independent, tamper-proof attestations that enable regulators and auditors to verify compliance without relying solely on bank self-reporting. Third, trust minimization ensures that critical functions—including depeg detection, settlement timing, and compliance attestation—are handled by a neutral third party leveraging Chainlink CRE that neither the bank nor counterparty controls.

Data Confidentiality

The architecture strictly separates sensitive commercial data from public blockchain and third-party systems through a three-tier model.

Tier 1 - Bank Private Infrastructure (All Sensitive Data)

Tier 1 encompasses the bank's private infrastructure, which retains all sensitive data. This includes counterparty identity and LEI information, trade details such as notional amounts, tenor, and strike prices, portfolio mark-to-market and variation margin calculations, stablecoin cap utilization per counterparty, wallet-to-counterparty mappings, and historical settlement records.

Tier 2 - Orchestration Infrastructure (Transient Processing + Attestations)

Tier 2 leverages Chainlink CRE, which handles transient processing and attestations. This tier processes data in-flight during workflow execution and stores only depeg events, settlement timestamps, compliance flags, and condition hashes. Critically, no counterparty identifiers, amounts, or trade details are retained at this level.

Tier 3 - Blockchain Infrastructure (Minimal Footprint)

Tier 3 represents the blockchain network, which maintains a minimal footprint. On-chain data is limited to stablecoin transfer transactions showing amounts and wallet addresses, attestation contract state containing only hashes and timestamps, and publicly available price feed data.

The total on-chain data exposure is limited to depeg events which reflect publicly available price data, settlement timestamps with no counterparty information, condition hashes that are opaque and reveal nothing about underlying transactions, and compliance flags expressed as simple boolean values with no amounts. No counterparty names, transfer amounts, or trade details are ever recorded on-chain.

Custody Integration

The bank utilizes an institutional custody provider for all blockchain operations. The custody provider enforces comprehensive policy controls including destination address whitelisting restricted to approved counterparty wallets, per-transaction and daily transfer limits, multi-approval requirements for large transfers, and time-based restrictions where applicable.

ERC-3643 Standard

A major hurdle for adoption in regulated capital markets is the requirement for mandatory Know Your Customer (KYC), Anti-Money Laundering (AML), and transfer restriction checks. Standard ERC-20 tokens cannot enforce these restrictions at token-level. The ERC-3643

token standard addresses those challenges. This standard transforms the token layer into a compliance-enforcement layer by embedding regulatory logic directly into the asset:

Modular Compliance Rules and Atomic compliance verification — ERC-3643 supports configurable compliance modules that can enforce jurisdiction-specific requirements, transaction limits, holding periods, or any other rule expressible in smart contract logic. For bilateral derivative collateral, relevant modules might include: Counterparty eligibility verification ensuring both parties maintain required regulatory authorizations. Jurisdiction controls preventing transfers to or from wallets in prohibited jurisdictions. Transaction limits enforcing minimum transfer amounts aligned with the CSA terms. Time-based restrictions supporting settlement window requirements.

These modules can be updated as regulations evolve, without requiring token migration or contract redeployment. The compliance framework adapts to changing requirements while maintaining continuity of the underlying collateral positions.

With ERC-3643, every single transfer re-validates that both sender and receiver are in the identity registry and that all associated required claims are valid. If a counterparty gets sanctioned or blacklisted between margin calls, the next transfer automatically fails. For VM where moving collateral happens daily, this continuous verification matters.

Transfer failure > transfer success to wrong party — With an ERC-20 stablecoins, a fat-finger error or compromised wallet means funds go to an unintended recipient and recovery is very challenging, even impossible. With ERC-3643, transfers to non-verified addresses simply revert. For institutional ops teams, "transaction failed" is vastly preferable to "transaction succeeded to an unknown party.

Regulator-verifiable compliance without disclosure — As ERC-3643 settlements carry compliance context on-chain, regulators can independently verify that the counterparty held required credentials at settlement time, that the token contract enforced eligibility requirements, and that the transaction completed under the compliance rules encoded in the token's modules. This shifts regulatory verification from trust-based (relying on the institution's internal records) to cryptographically-verifiable (confirming on-chain state). With ERC-3643, the identity registry is on-chain—regulators can independently verify that all collateral movements occurred between registered entities without the bank disclosing counterparty identities or amounts.

CSA-enforceable transfer restrictions at token level — The CSA governs margin arrangements for bilateral derivatives. Provisions from the CSA that ERC-3643 can enforce natively include ‘Threshold’ and ‘Minimum Transfer Amounts’, which can be encoded in compliance modules, preventing transfers that violate agreed terms. Custody policy controls are a second layer, not the only layer. When eligible counterparties enter into a CSA, both parties must have verified identities registered in the relevant token's Identity Registry facilitating the CSA onboarding and identity verification.

Recovery mechanisms for institutional edge cases — ERC-3643 includes provisions for token recovery in cases of lost keys, wallet compromise, or legal requirements (court orders, regulatory seizure). Designated recovery agents can facilitate token transfers under defined circumstances, providing institutional-grade asset protection that ERC-20 cannot offer.

For margin collateral, this addresses a critical operational risk: the possibility that a counterparty loses access to posted collateral due to key management failure. Rather than requiring costly legal proceedings to establish ownership and create workarounds, ERC-3643's recovery mechanisms provide a native solution.

For institutional derivative collateral, the choice of ERC-3643 is not a matter of technical preference—it reflects fundamentally different approaches to compliance. ERC-20 treats compliance as an external concern, addressed through wrapper infrastructure that exists alongside but separate from the settlement mechanism. ERC-3643 treats compliance as intrinsic, embedded in every transfer and verifiable by any party.

For bilateral OTC derivatives, where counterparty relationships persist over extended periods and regulatory obligations are extensive, ERC-3643's architecture can provide material advantages: continuous eligibility verification, protocol-enforced transfer restrictions, recoverable assets, and on-chain audit trails. These capabilities help address the core concerns that compliance officers, risk managers, and regulators raise when evaluating blockchain-based settlement infrastructure.

CRE Workflows

Chainlink CRE is used to orchestrate depeg monitoring, settlement window enforcement, and compliance attestation addresses the key trust and verification challenges without exposing sensitive commercial data. This architecture provides a model for how traditional financial institutions can leverage blockchain infrastructure selectively - using it where decentralization and verifiability add clear value, while keeping sensitive operations in private systems.

Trust Challenges in Bilateral Settlement

Traditional bilateral arrangements present inherent trust asymmetries that blockchain-based attestation can resolve.
The first challenge concerns depeg determination. Whilst a provision can be included in the CSA to suspend stablecoin margin transfers during depeg events, the question as to who decides whether a depeg has occurred creates potential conflicts. If the bank decides, the counterparty must trust the bank's monitoring systems, and the bank could theoretically claim a false depeg to force USD settlement. If the counterparty decides, the bank must trust the counterparty's monitoring, and the counterparty could ignore a genuine depeg to avoid USD conversion. If each party decides independently, disputes inevitably arise when determinations diverge.

The solution leverages a CRE workflow to monitor the price feed and maintain authoritative depeg status on-chain. Neither party controls the determination, and both can independently verify the status by reading the attestation contract.

The second challenge involves settlement timing verification. The CSA requires variation margin to be settled within a specified window agreed between the parties – for example, two hours from the margin call. Proving timeliness matters for determining whether an Event

of Default or Termination Event has occurred under the ISDA Master Agreement, for regulatory compliance reporting, and for dispute resolution.

The solution leverages a CRE workflow to timestamp both the settlement intent when the margin call is generated and the execution when the transfer is confirmed. These timestamps are recorded on-chain and cannot be backdated.

In addition, the solution leverages a CRE workflow that records a hash of the settlement conditions on-chain at execution time. The bank retains the full conditions privately but can prove that the hash matches, providing cryptographic assurance without disclosure.
The proof of concept runs three distinct CRE workflows that collectively provide comprehensive verification while maintaining strict data confidentiality.

Depeg circuit breaker

Monitors CTT/USD price and maintains authoritative depeg status. Neither bank nor counterparty controls this.

Mechanism:

- CRE workflow runs every two minutes for testing purposes
- Reads latest price from oracle
- If price crosses depeg threshold (0.98 or 1.02), updates on-chain status
- Emits event that both parties' systems can monitor
- When price recovers, clears the depeg status

Value: Eliminates trust dependency and potential disputes about depeg status.
Note: An alternative approach could be to use the NAV (assetID) of the stablecoin asset rather than an oracle (susceptible to temporary market spikes) and use a CRE workflow to monitor NAV update events and trigger the same mechanism if it crosses the depeg threshold.

VM Settlement Intent
Timestamps settlement intents and enforces relevant settlement deadlines. Provides verifiable proof that settlements met timing requirements.

Mechanism:

1. When bank generates margin call, it calls the CRE workflow to "declare settlement intent"
2. The workflow records the current timestamp and deadline on the attestation contract
3. After transfer executes, bank calls the workflow to "attest settlement"
4. The workflow records execution timestamp and whether deadline was met
5. Both parties can verify the timeline on-chain

Value: Creates indisputable proof of settlement timing that neither party can manipulate.

Input Parameters:

```
{
  "settlementId": "----------------------------------------------",
  "receiverAddress": "----------------------------------------------",
  "requestTimestamp": ----------------------------------------------,
  "windowDurationSeconds": ----------------------------------------------
}
```

Field Descriptions:

- settlementId (string): Unique identifier for the settlement
- receiverAddress (string): Ethereum address of the party receiving the CTT tokens
- requestTimestamp (number): Unix timestamp when intent is declared
- windowDurationSeconds (number): Time window for execution

VM Settlement Attestation

Mechanism:

1. Bank computes hash of full settlement conditions (counterparty, amount, prices, cap status, etc.)
2. The CRE workflow records this hash on attestation contract along with compliance flags
3. Hash is immutable once recorded
4. Bank can later disclose full conditions to regulator
5. Regulator can verify hash matches on-chain attestation

What the attestation contains:

- Settlement ID (opaque identifier)
- Intent timestamp and execution timestamp
- Price at execution
- Depeg status at execution
- Window compliance flag (met deadline or not)
- Conditions hash

What the attestation does NOT contain:

- Counterparty name or identifier
- Transfer amount
- Trade details
- Cap utilization

Value: Provides cryptographic proof of compliance without exposing sensitive data publicly.

Input Parameters:

```
{
  "settlementId": "----------------------------------------------",
  "conditionsHash": "----------------------------------------------",
  "transferTxHash": "----------------------------------------------",
```

```
  "transferFrom": "----------------------------------------------",
  "transferTo": "----------------------------------------------",
  "transferAmount": "----------------------------------------------",
  "requestTimestamp": ----------------------------------------------
}
```

Field Descriptions:

- settlementId (string): Same settlement ID from intent declaration
- conditionsHash (string): SHA256 hash of settlement conditions (includes amount, timestamp, parties)
- transferTxHash (string): Ethereum transaction hash of the token transfer
- transferFrom (string): Sender address
- transferTo (string): Receiver address
- transferAmount (string): Amount of tokens transferred
- requestTimestamp (number): Unix timestamp when attestation is submitted

Key Smart Contract

Attestation Contract

The attestation contract serves as a neutral record-keeper for settlement events. It provides third-party verification without third-party data exposure
It serves as the immutable ledger for daily variation margin settlements using CTT tokens. It performs three critical functions:

1. Depeg Monitoring: Tracks CTT/USD price deviations from the $1.00 peg
2. Settlement Intent Recording: Records when a settlement obligation is declared
3. Settlement Attestation: Permanently records settlement execution with market conditions

It acts as a “trustless notary” that:
- Witnesses and records settlement commitments
- Captures market conditions at critical moments
- Provides an immutable audit trail for all parties
- Enables external verification of all settlements

Trust Minimization: Neither party can manipulate depeg determinations or backdate settlement records.

Regulatory Verifiability: Auditors get cryptographic proof of compliance rather than relying solely on bank self-reporting. They can independently verify on-chain that a hash matches disclosed conditions.

Confidentiality Preservation: Sensitive commercial data (counterparty identity, amounts, trade details) never touches the public blockchain—only opaque hashes and timestamps.

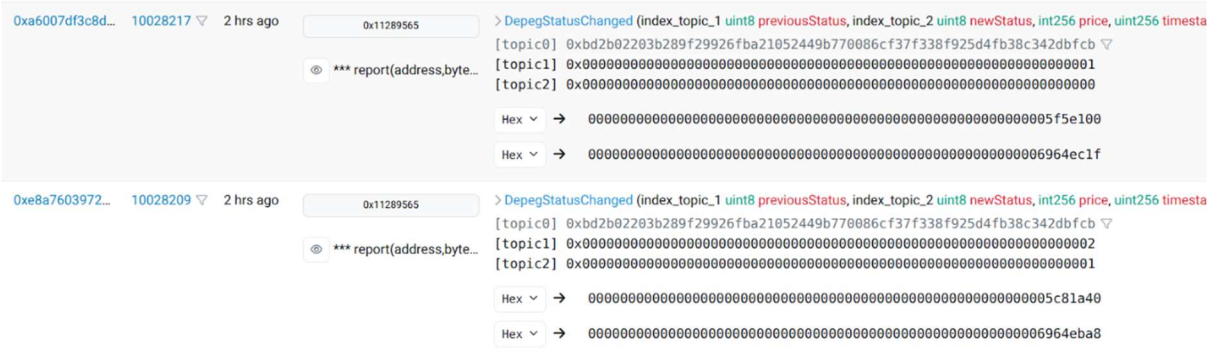
Dispute Resolution: Creates indisputable evidence for timing and conditions, useful if CSA breach claims arise.

It is integrated with the three CRE workflows.

```
                    CRE WORKFLOW EXECUTION
                              |
                              ↓
    1. Workflow generates report data
    2. DON signs report (consensus)
    3. DON submits to Keystone Forwarder
                              |
                              ↓
                 CHAINLINK KEYSTONE FORWARDER
                  (Authorized CRE Infrastructure)
                              |
                              ↓
    1. Validates DON signatures
    2. Packages report with metadata
    3. Calls contract.onReport(metadata, report)
                              |
                              ↓
              CTT VARIATION MARGIN ATTESTATION
                        (This Contract)
                              |
                              ↓
    1. Validates msg.sender == allowedForwarder
    2. Decodes report type
    3. Routes to appropriate handler
    4. Updates state
    5. Emits event
```

1. Depeg Monitor Integration

The depeg-monitor workflow operates on a cycle, continuously monitoring CTT Token price stability through Chainlink's price feed infrastructure. When the DON reads the current price data, it calculates the depeg status and generates a DepegUpdate report. The contract updates the currentDepegStatus state variable and, if the status has changed from the previous reading, emits a DepegStatusChanged event to notify interested parties.



2.Settlement Intent Integration

The settlement-intent workflow is triggered on-demand variation margins obligations are declared for counterparties. The variation margin amount is calculated offchain and an API

calls the settlement-intent workflow. The workflow first validates that all compliance requirements are met, then generates a SettlementIntentReport containing the declared settlement details. The contract emits a SettlementIntentDeclared event to signal that a counterparty has committed to a specific settlement amount.

```
0xba65cd1d29...   10029457   6 mins ago   0x11289565   SettlementIntentDeclared (index_topic_1 bytes32 settlementId, uint256 intentTimestamp, uint256 deadline)
                                                        [topic0] 0xb02e687b559db3c7b4bea0242518e95b9f7287348a233b0de048fc3632a330b5
                                           *** report(address,byte...   [topic1] 0x2bff82d05cc15f771343cad6609d350eee75438b9bf978e80a4f1bf0c8c6a276
                                                        Hex → 0000000000000000000000000000000000000000000000000000000000063ffe700
                                                        Hex → 0000000000000000000000000000000000000000000000000000000000064000320
```

If the counterparty is not verified, the compliance check fails and the settlement intent report is not generated/declared.

```
2026-01-12T15:04:38Z [USER LOG] msg="Step 2: Validating receiver address format..."
2026-01-12T15:04:38Z [USER LOG] msg="Receiver address validated" receiverAddress=0x0000000000000000000000000000000000000001
2026-01-12T15:04:38Z [USER LOG] msg="Step 2a: Checking receiver compliance with Identity Registry..."
2026-01-12T15:04:38Z [USER LOG] msg="Creating EVM client for Identity Registry" chainSelector=16015286601757825753
2026-01-12T15:04:38Z [USER LOG] msg="Creating Identity Registry contract binding" registryAddress=0x838d4f2bCC2a3df9e90cbA05f53B550F6eeeac56
2026-01-12T15:04:38Z [USER LOG] msg="Calling isVerified() on Identity Registry..." userAddress=0x0000000000000000000000000000000000000001
2026-01-12T15:04:38Z [USER LOG] msg="Awaiting isVerified() response..."
2026-01-12T15:04:39Z [USER LOG] msg="Receiver verification status retrieved" isVerified=false
2026-01-12T15:04:39Z [USER LOG] msg="❌ COMPLIANCE CHECK FAILED: Receiver is not verified in Identity Registry" receiverAddress=0x0000000000000000000000000000000000000001
```

3. Settlement Attestation Integration

The settlement-attestation workflow is also triggered on-demand after a counterparty has completed a CTT transfer. Once the transfer occurs, the counterparty calls the settlement-attestation workflow, which performs verification of the transfer details against the declared intent. The workflow also captures current market conditions at the time of attestation for audit purposes. The contract stores the Attestation record and emits a SettlementAttested event, completing the settlement lifecycle for that margin call.

```
0x1c3e0e4662...   10029479   1 min ago   0x11289565   SettlementAttested (index_topic_1 bytes32 settlementId, uint256 executionTimestamp, bool windowCompliance, bytes3
                                                       [topic0] 0x8f6da3a8552ce67fe5a8bbf7fef9924d3c29566192848058a1a557dcdaad33eb
                                          *** report(address,byte...   [topic1] 0x2bff82d05cc15f771343cad6609d350eee75438b9bf978e80a4f1bf0c8c6a276
                                                       Hex → 0000000000000000000000000000000000000000000000000000000000063ffe700
                                                       Hex → 0000000000000000000000000000000000000000000000000000000000000001
                                                       Hex → 0c9cd35590781632a2da14045426d1f64e2faa7e4f794aa8cbd0f904ce232d06
```

PoC Test Data

Contract	Etherscan link
CTT Token Contract	https://sepolia.etherscan.io/token/0x93d625c8e9e74bc22e18a3da7dc0d3c64ce96086
CTT/USD Price Feed Contract	https://sepolia.etherscan.io/address/0xd0CC39fA6BF672ed5B3Ebb0cbC98510E344b5B6E
Attestation Contract:	https://sepolia.etherscan.io/address/0xb611024c01c6a6472ddba15e3af0427c0ca4383a

Attestation Contracts Event	Etherscan link
Depeg Status Changes	https://sepolia.etherscan.io/tx/0xa6007df3c8d24a665736f5d9d1b1b26efba6f674473cb14ee88345f9cd55acd4
Settlement Intent Declared	https://sepolia.etherscan.io/tx/0xba65cd1d29d94444622070a0b5efdbf877e3fd519a8f901c483ecdc85eda6cc6
Settlement Attested	https://sepolia.etherscan.io/tx/0x1c3e0e4662630c65384970790a497b47b0186763ba4634ceaf84beb044400641

Results

Criterion	Status	Evidence
ERC-3643 transfers execute with compliance validation	✅ Achieved	CTT Token Contract
Depeg monitoring triggers correctly	✅ Achieved	DepegStatusChanged event
Settlement intent recorded on-chain	✅ Achieved	SettlementIntentDeclared event
Settlement attestation immutably stored	✅ Achieved	SettlementAttested event
Sub-10-minute settlement	✅ Achieved	Block timestamp delta

Transfers to non-registered addresses rejected	✅ Achieved	Compliance check-failed. Settlement-intent not generated.

The PoC validates depeg detection and transfer blocking, but does not yet demonstrate automated fallback to wire settlement. In production, this would require integration with the bank's payment rails and operational workflows to ensure seamless handoff when stablecoin settlement is suspended in case of depeg events.

Conclusion

This proof of concept explored how an ERC-3643 USD-pegged stablecoin can serve as effective collateral for variation margin on bilateral OTC derivatives, delivering measurable operational benefits while introducing manageable new risks. The core value proposition is clear: eliminating the settlement gap between when margin is calculated and when it actually moves. For USD/BRL NDFs specifically, this means no more trapped liquidity over Brazilian holidays, no more timezone arbitrage disadvantaging one party, and no more next-day settlement for margin calls generated after banking hours. The transition from settlement by message to settlement by value fundamentally changes what is operationally possible.

While this proof of concept uses USD/BRL NDFs as the reference instrument, the settlement architecture is instrument-agnostic. The same infrastructure can support variation margin settlement for any bilateral, cash-settled OTC derivatives denominated in USD—including interest rate swaps, credit derivatives, and equity swaps - . The choice of NDF serves to illustrate specific operational pain points, not to constrain applicability.

Stablecoin collateral introduces issuer credit risk and smart contract risk that USD cash does not carry. However, these risks can be quantified and mitigated through appropriate haircuts, depeg circuit breakers, and fallback mechanisms to traditional settlement rails. For a sophisticated derivatives desk already comfortable with counterparty credit assessment, adding stablecoin issuer risk to the evaluation framework is an incremental complexity rather than a categorical barrier. In addition, smart contract infrastructure and risk rating claim on the assetID of ERC-3643 based collaterals could enable dynamic haircut methodologies—adjusting valuations in real-time—which would be harder to effect when using traditional securities as collateral under ISDA’s current collateral documentation.
What distinguishes ERC-3643 is its compliance embedded at the token layer. Every transfer automatically validates that both parties remain eligible—a critical safeguard for institutions operating under prudential supervision. The identity registry, transfer restrictions, and recovery mechanisms address key institutional requirements. For institutions evaluating blockchain-based settlement infrastructure, ERC-3643 offers a path that works with existing compliance frameworks rather than around them.

www.qualitax.io
contact@qualitax.io

©2025 Consianimis Consulting Ltd.
All rights reserved.
QualitaX.io is owned and operated by Consianimis Consulting Ltd.
A private limited company registered in England and Wales under registration number 09006129.
Registered address: 167-169 Great Portland Street, 5th Floor, London, England, W1W 5PF, UK.