ERC-3643 Tokens for Derivative Collateralization

Enabling Compliant On-Chain Smart Derivatives

September 2025

Contributors

Anaïs Ofranc - QualitaX
Samuel Edoumou - QualitaX
Stefan Haupt - QualitaX
Joachim Lebrun - Tokeny
Robin Jelin - Tokeny
Pat Hourigan - Frictionless Markets
Jaspreet Khaira - Frictionless Markets
George Gledhill - CMS
Charles Kerrigan - CMS
Ghazi Ben Amor - Zama
Olivia Vande Woude - Ava Labs
Ash Nathan - Chainlink

Table of contents

Summary

The uncleared OTC derivatives market faces significant inefficiencies:

- **Reliance on Manual Processes:** 38% of operational resources consumed by manual Business-As-Usual tasks. Heavy reliance on manual processes for trade capture, portfolio reconciliation, and collateral management.
- **High Dispute Rates:** 45% of margin calls disputed, indicating high reconciliation complexity.
- **High operational costs:** price out smaller market participants.

Exploring a Solution: ERC-3643 + Smart Derivatives

- **ERC-3643:** Compliant security token standard with embedded KYC/AML and regulatory compliance.
- **Smart derivative contracts:** Automated, self-executing derivative contracts.
- **Automated Trade Lifecycle:** a) Identity & Compliance Verification: All participants must have a verified on-chain identity (OnchainID) before trading, ensuring adherence to KYC/AML and jurisdiction rules. b) Trade Inception & Collateralization: A factory contract deploys a unique smart contract for each bilateral trade, which locks in ERC-3643 tokens as initial margin and termination fees. c) Ongoing Management: The smart contract uses oracle data for daily mark-to-market calculations and automates margin calls, with transfers automatically checked for compliance. d) Final Settlement: At maturity, the contract automatically settles based on pre-agreed rates and facilitates the withdrawal of remaining collateral.

Key Benefits of This Approach

- **Operational Efficiency**: Automated settlement and reconciliation eliminate manual overhead, deterministic smart contract execution could reduce dispute rates, real-time mark-to-market calculations and automated margining
- **Capital Efficiency:** Tokenized collateral (like tokenized money market funds) can generate yield while posted as margin, enhanced netting arrangements across multiple contracts could eventually lead to double digit basis points in annual cost savings
- **Risk Management:** Automated daily settle-to-market mechanisms reduce counterparty risk, and automatic contract termination for non-compliance.

Introduction

The global financial system relies heavily on the Over-The-Counter (OTC) derivatives market, a vast ecosystem with a notional value of around $700 trillion[1] (as per the end of December 2024). This massive scale underscores the critical role derivatives play in risk management, portfolio optimization, and facilitating financial stability.

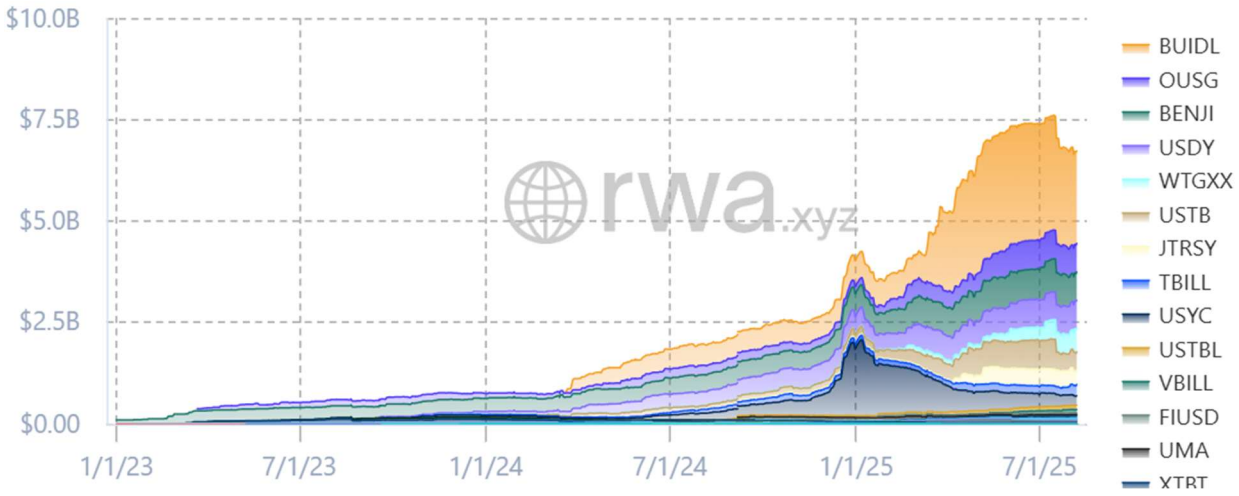
Within this enormous derivatives landscape, non-cleared derivatives represent a substantial portion that continues to operate outside centralized clearing mechanisms. Unlike cleared derivatives that pass through central counterparties (CCPs) and benefit from standardized margining and risk management protocols, non-cleared derivatives are bilaterally negotiated contracts between counterparties who must independently manage their credit risk exposures. These bilateral arrangements, while offering greater customization and flexibility to meet specific hedging or investment needs, require sophisticated collateral management frameworks and robust margining practices to mitigate counterparty credit risk.

The ISDA Margin Survey Year-End 2024[2] shows that initial margin (IM) and variation margin (VM) collected by leading derivatives market participants for their non-cleared derivatives exposures increased by 6.4% to $1.5 trillion at the end of 2024.

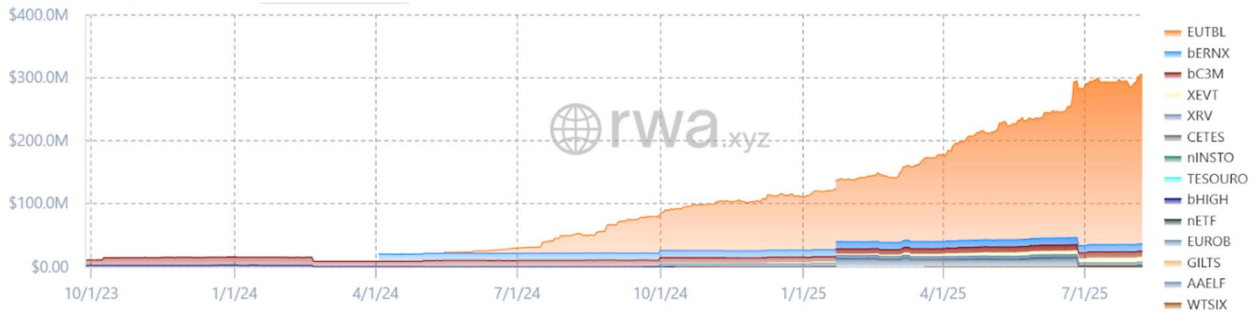
Uncleared OTC derivatives, including Non-deliverable Forwards (NDFs), Physical FX Forwards, are utilized by key market participants (financial institutions) acting as market-makers, to hedge their own risks, and for proprietary trading and are essential tools for achieving precise risk-return profiles that standardized cleared products cannot adequately address.

In parallel, over the last 18 months, the landscape of digital assets has seen a pivotal development with the significant growth in tokenized treasuries and global government bonds, collectively reaching nearly $7.5 billion in USD value[3]. Institutional stakeholders, including prominent digital asset hedge funds, have begun actively leveraging these tokenized assets—such as BlackRock's BUIDL tokenized money market fund—as collateral for their trading activities. And, market makers and liquidity providers like Wintermute have stepped in to offer crucial 24/7 secondary OTC liquidity for BUIDL and similar tokenized assets, further legitimizing their use. This evolution underscores a key driver for continued growth: **the ability to seamlessly and compliantly use these tokenized assets as collateral presents a compelling new opportunity for both capital and operational efficiency** for uncleared OTC bilateral trading.

[1] https://www.isda.org/a/1rjgE/Key-Trends-in-the-Size-and-Composition-of-OTC-Derivatives-Markets-in-the-Second-Half-of-2024.pdf (p.2)
[2] https://www.isda.org/a/EyfgE/ISDA-Margin-Survey-Year-end-2024.pdf
[3] https://app.rwa.xyz/treasuries



Tokenized US treasuries, bonds and cash-equivalents as of 08 August 2025
Source: https://app.rwa.xyz/treasuries



Tokenized bonds backed by public debt issued by governments and companies as of 08 August 2025 - Source: https://app.rwa.xyz/global-bonds

However, to date, uncleared OTC bilateral derivatives remain burdened by deep-seated inefficiencies that hinder capital optimization and elevate operational costs. These challenges stem from a reliance on manual processes, complex reconciliation, and burdensome collateral management. For an enterprise-grade trading system, the manual effort involved in managing breaks, disputes, and settlement failures for OTC bilateral trades is notoriously inefficient, consuming substantial resources and creating dependencies on counterparty automation.

While smart derivatives contracts executed on DLT ledgers/blockchain networks are still emerging, promising solutions are surfacing to tackle those challenges. This report aims to provide a deep dive into how ERC-3643 tokens can be used for derivative collateralization, enabling compliant smart derivatives contract execution. We will explore:

- Uncleared OTC Bilateral Derivatives: Challenges & Opportunities
- Bridging Compliant RWAs with Smart Derivatives Contracts
- Practical Use Cases: Illustrated through USDC Yield Index Cash-Settled Forward and FX EURUSD Forward with Delivery
- Emerging Best Practices/Learnings
- Ongoing Development & Future Outlook

Our goal is to explore a viable path for institutional stakeholders to unlock new levels of capital efficiency, operational agility, and regulatory compliance within the uncleared OTC bilateral derivatives landscape.

Uncleared OTC Bilateral Derivatives: Challenges & Opportunities

The primary characteristic of uncleared OTC bilateral derivatives is their bespoke nature, allowing for highly customized contracts tailored to the specific needs of counterparties. However, this flexibility introduces significant operational, credit, and legal complexities. OTC bilateral trading allows for:

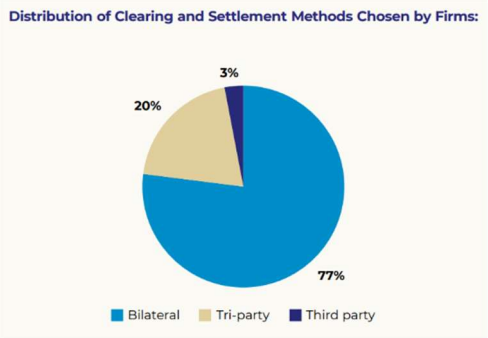
- **Customizability:** Ability to negotiate nearly all terms allowing for highly specific risk management solutions.
- **Product Availability:** Broader diversity of derivative products beyond standardized exchange-traded instruments.
- **Access Limitations**: Counterparties may not be members of a Central Counterparty (CCP) or the product itself may not be eligible for central clearing. Even when clearing is an option, firms might choose not to clear to maintain direct ownership and control over the risk management of their positions.

However, this bespoke nature creates significant challenges:

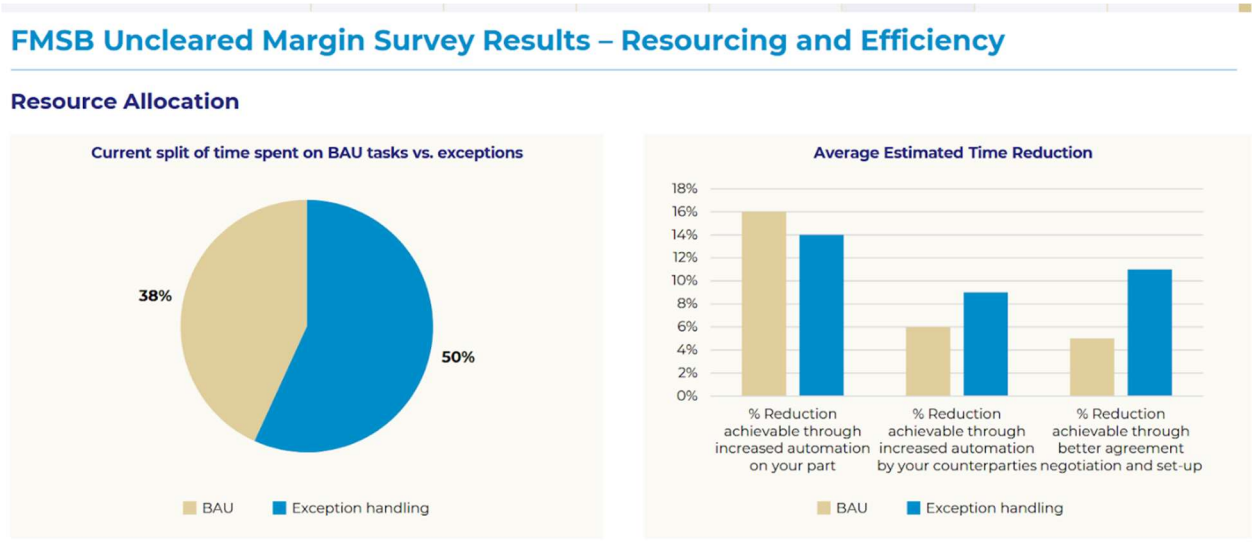
- **Trade Processing:** Lack of standardized trade formats and processes leads to manual trade capture and reconciliation.
- **Legal Documentation:** Bespoke ISDA agreements and CSAs require extensive negotiation and maintenance.
- **Collateral Management:** Without a CCP, collateral is exchanged bilaterally. The lack of netting across relationships can significantly reduce collateral efficiency, resulting in fragmented pools and complex margining.

Quantifying the Challenges with Uncleared OTC Derivatives

The operational challenges associated with uncleared OTC derivatives are notably quantified by the significant manual effort required and the high dispute rates. According to the recent report ‘Uncleared Margin for OTC Derivatives’ (May 2025) by the Financial Market Standards Board (https://fmsb.com/wp-content/uploads/2025/05/Uncleared-Margin-Spotlight-Review_May-2025_FINAL.pdf) , the overwhelming majority of time and resources—specifically 38% for Business As Usual (BAU) tasks, with a substantial portion dedicated to manual processes—are consumed by managing these derivatives. Furthermore, exception handling (breaks in Straight-Through Processing, disputes, settlement failures, and reconciliations) consumes a large proportion of time within BAU activities, highlighting a pervasive lack of automation.

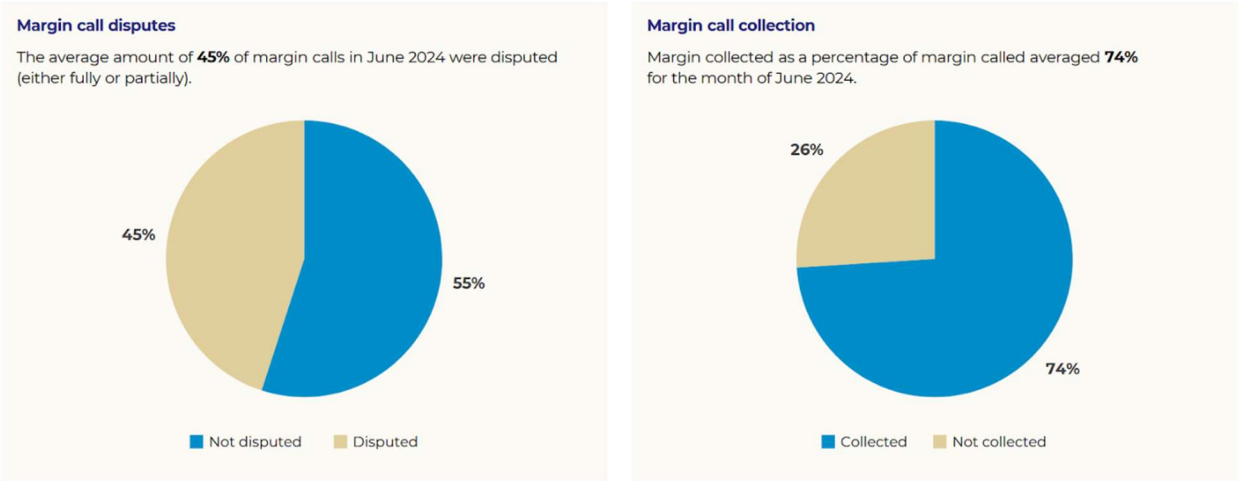


Distribution of Clearing and Settlement Methods Chosen by Firms (p.12)



Resource Allocation - Uncleared margin process activity & Anticipated time reductions (p.14)

A significant 45% of all margin calls were disputed (either fully or partially), indicating the high level of disagreement and complexity surrounding collateral valuation and reconciliation.



Margin call disputes and Margin call collection (p.18)

The most problematic areas for manual effort include trade capture and portfolio reconciliation, where counterparty non-automation is the biggest obstacle (27% high, 53% medium, 20% low manual effort). Across the trade lifecycle, the reliance on manual processes increases the potential for errors and delays, which can have significant financial and operational consequences, underscoring the pressing need for increased automation and standardization across these critical functions.

	Manual Effort to manage STP Breaks			
Trade Lifecycle	**High**	**Medium**	**Low**	**Most problematic area**
Trade Capture & Portfolio Reconciliation	27%	53%	20%	Counterparty non-automation
Exposure & Margin Calculation	0%	13%	87%	Counterparty non-automation
Call Issuance	0%	13%	87%	Counterparty non-automation
Call Matching /Agreement	13%	33%	53%	Counterparty non-automation
Collateral Asset Selection	7%	29%	64%	Own non-automation
Collateral Move Booking	7%	27%	67%	Own non-automation
Settlement /Fails Management	13%	27%	60%	Own non-automation

Manual effort required & Causes of manual handling (p.15)

Opportunities for Modernization

Modernization efforts must address these inefficiencies without sacrificing the inherent flexibility of uncleared OTC derivatives. Emerging technologies, particularly RWA tokenization and smart contract automation, offer a promising pathway to automate processes and reduce operational overhead.

These efforts could aim to dramatically reduce the operational overhead and capital intensity currently pricing out smaller entities. Automation and cost reduction can broaden market access, allowing a more diverse range of participants to engage in essential risk management and capital optimization strategies that were previously exclusive due to the high barriers to entry.

- Tokenization and Digital assets
- Smart Contract Automation

Problem statement:

Given these current challenges, a critical question emerges: can tokenized assets and smart derivatives unlock a viable solution to the capital and operational inefficiencies that currently plague uncleared bilateral OTC derivatives?

ERC-3643 Tokens as Collateral for Smart Derivative Contracts

In this section, we will demonstrate how using tokenized assets and smart contracts for sophisticated OTC bilateral trading can help address the challenges of executing complex financial derivatives like FX Forward with Delivery or NDFs.
We will first provide an overview of ERC-3643, compliant security token standard, as well as a step-by-step walkthrough of a typical trade lifecycle, highlighting the use of ERC-3643 tokens and on-chain identity verification to ensure regulatory compliance.

Overview of ERC-3643: The Compliant Security Token Standard

ERC-3643 is an open-source, ERC-20-compliant suite of smart contracts that enables issuing, managing, and transferring permissioned tokens on public networks. It is designed to address the limitations of previous ERC proposals, focusing on compliance and regulatory adherence.
The ERC-3643 token standard embeds regulatory compliance directly into a token's smart contract framework:

Integrated Compliance Mechanisms: ERC-3643 facilitates compliance with KYC/AML and specific securities regulations through a consistent framework built into the token's architecture. This integration facilitates the efficient management of security tokens, ensuring a token’s adherence to its offering terms and other legal mandates throughout its lifecycle.

Automated On-Chain Validator System: Leveraging on-chain identities for eligibility checks, ERC-3643 introduces an automated validator system. This system streamlines the process of validating transactions and investor identities, enhancing the security and legal conformity of tokenized assets. This structure may enable compliance with certain regulated securities applications in certain jurisdictions.

Advanced Token Lifecycle Management: The standard provides a robust and consistent framework for managing the complete lifecycle of security tokens. That includes issuance, transfer between eligible investors, and enforcement of certain compliance rules, with additional features like token pausing and freezing in response to regulatory needs.

Enhanced Security and Flexibility: ERC-3643 builds upon the ERC-20 structure while introducing additional functions for compliance and security. It includes conditional transfer mechanisms, recovery systems for lost access, and functionalities for freezing and managing tokens, reflecting a comprehensive approach to regulated token management.

For further information about ERC-3643 please refer to the report ‘Demystifying ERC-3643: A Deep Dive into Compliant RWA Tokenization’ (March 2024) published by QualitaX : https://www.qualitax.io/erc3643

Financial Derivatives as Smart Contracts

As previously mentioned, managing and settling derivatives contracts in the traditional OTC derivatives market is complex, manual, and inefficient, leading to high operational costs for market participants. Counterparty credit risk is a major concern for both parties in a derivatives contract. This risk is typically managed through several mechanisms: a) Credit Valuation Adjustment (CVA), a pricing adjustment that reflects the market value of counterparty credit risk. This adjustment results in higher costs for the parties having higher credit risk, b) Regulatory capital charges imposed on financial institutions to cover potential losses from counterparty defaults. These requirements tie up significant capital, reducing overall market efficiency and increasing costs, c) Netting agreements, which allow for the offsetting of positive and negative exposures between counterparties, reducing overall credit risk exposure, d) Collateral requirements, where parties post liquid assets against their positions to mitigate potential losses in case of default. These operational requirements and risk management practices contribute to the complexity and cost of OTC derivatives trading.

To help address those challenges, a proposed standard for smart derivative contracts, ERC-6123, has been proposed by DZ Bank. ERC-6123 offers an open-source standard for creating and managing derivative contracts on blockchain platforms. ERC-6123, titled "Smart Derivative Contract" (SDC), is an Ethereum Improvement Proposal (EIP) to create a deterministic, decentralized trade process protocol for financial derivative contracts, removing counterparty credit risk by design.

ERC-6123 has versatile applications across traditional finance (TradFi) and decentralized finance (DeFi). In traditional finance, it can be used for non-cleared interbank OTC derivatives trading, enabling automated settlements and risk mitigation without central counterparty novation. It can also facilitate cost-efficient derivative transactions for non-bank entities. In DeFi, ERC-6123 can enable the creation of native on-chain derivatives and structured products using DeFi yield indices as settlement rates.

Its key benefits include

- **Automation**: Self-executing contracts with predefined rules reduce the need for intermediaries and manual processes
- **Standardization**: A uniform interface and set of functions promote interoperability and composability between different derivative contracts
- **Enhanced Security:** Blockchain technology ensures immutability, and real-time settlement
- **Risk Reduction:** Automated and instantaneous settlement via a pre-agreed valuation model mitigates operational burdens, reduces the duration of credit risk exposure, and removes the risk of disagreeing on the valuation
- **Efficiency Gains:** Streamlined processes and reduced counterparty risk contribute to overall market efficiency. By leveraging ERC- 6123, market participants can benefit from a more streamlined, secure, and efficient approach to derivatives management, addressing many of the challenges present in traditional OTC markets.

Those benefits are achieved through several mechanisms inherent to the ERC-6123 specification:

1. **Settle-to-Market Mechanism (STM)**

Description: ERC-6123 utilizes a settle-to-market mechanism where the positions are marked to market and settled daily. This means the value of the contracts is recalculated each trading day based on the current market price, and the resulting profit or loss is credited or debited to the counterparties' accounts accordingly.

Benefit: The STM mechanism reduces counterparty risk by ensuring that gains and losses are settled daily. This continuous revaluation and settlement prevent the accumulation of large obligations and ensure that counterparties maintain their financial positions, thereby minimizing the risk of significant defaults.

2. **Automated Settlement and Margining:**

Description: The ERC-6123 smart contract automates calculating and transferring margin and settlement amounts. This includes real- time adjustments based on market conditions and predefined rules.

Benefit: Automated settlement processes reduce the likelihood of human error and delay, ensuring that obligations are met promptly and accurately. This reliability further diminishes the risk of counterparty default.

3. **Deterministic Valuation and Settlement:**

Description: ERC-6123 incorporates a deterministic valuation model contractually agreed upon by both parties. The smart contract uses this model to calculate net present value of the reference derivative and enforce settlements automatically. This model is contractually agreed upon and is part of the OTC contract.

Benefit: This deterministic approach ensures that both parties clearly and consistently understand their obligations, reducing contract risk, resulting disputes and the associated counterparty risks.

4. **Automatic Contract Termination:**

Description: ERC-6123 includes provisions for automatic contract termination if a counterparty fails to meet its margin or settlement obligations. In such cases, the smart contract will enforce the transfer of any pre-funded amounts to cover losses.

Benefit: Automatic termination reduces prolonged exposure to defaulting counterparties, ensuring that losses are contained and managed swiftly.

By incorporating these elements, ERC-6123 aims to address the complexities and inefficiencies in traditional non-cleared OTC derivative post-trade processing. Its goal is to eliminate the need for separate collateral processes, reduce settlement risks by netting

product cash flows and market value changes, and enforce consistent valuation and automatic termination independently of the counterparties.

For further information about ERC-6123, please refer to the report ‘Deep Dive into ERC-6123: Rethinking Financial Derivatives’ (August 2024) published by QualitaX: https://www.qualitax.io/erc6123

Use Cases

The proofs-of-concept (PoCs) below feature use cases where smart contracts hold ERC-3643 collateral directly on-chain, rather than relying on custodians. While this design is technically functional for demonstration purposes, custodian integration for secure, off-chain fund management is critical for institutional adoption. These early PoCs focus on two distinct types of forward contracts: USDC Yield Index Cash-Settled Forward and EURUSD Forward with Delivery . It is also important to note that while this ERC-6123 has served as a source of inspiration, the smart derivative contracts used in our use cases are not ERC-6123 compliant.

Use Case 1: USDC Yield Index NDF

For this first use case, we are proposing to explore the USDC Yield Index Cash-Settled Forward as a tool for speculation and risk management. For speculators, it provides a capital-efficient way to take a directional view on the future of DeFi lending rates. They can bet on whether the USDC Yield Index will rise or fall relative to the forward rate, with profits or losses settled in cash. For market participants like DeFi protocols such as liquidity providers, the index forward can serve as a crucial hedging instrument. It allows them to lock in a fixed return, protecting their revenue streams from the volatility of variable DeFi yields. Furthermore, for firms that trade only on CEX such as some hedge funds or market makers, it offers a sophisticated arbitrage opportunity, bridging the gap between centralized and decentralized markets.

In a nutshell, as market participants increasingly engage with digital assets, particularly stablecoins like Circle’s USDC, they face exposure to the fluctuating yields offered by DeFi lending and borrowing protocols. Traditional interest rate derivatives often rely on off-chain interbank rates (e.g., SOFR). However, for on-chain stablecoin holdings, a benchmark that reflects the actual cost or return of capital within the digital asset ecosystem is crucial to accurately hedge or speculate on these specific exposures. A USDC Yield Index Cash-Settled Forward bridges this gap, providing a relevant, transparent, and auditable tool for managing on-chain interest rate risk, addressing basis risk between TradFi and DeFi benchmarks.

Illustrative Example

A hedge fund has been gradually increasing its digital asset allocation over the past 18 months. The fund currently holds millions in USDC across various DeFi lending protocols including Aave, Morpho and Maple Finance. While these positions generate attractive yields, the fund's risk management team has grown concerned about the volatility in DeFi lending rates.

Due to market events, USDC lending yields have dropped over six weeks due to reduced borrowing demand in DeFi markets. This decline directly impacts the fund's income projections and creates uncertainty around their strategy. Traditional interest rate derivatives

tied to SOFR do not provide effective hedging since DeFi rates often move independently of traditional banking rates, creating significant basis risk.

Working with a counterparty, the hedge fund decided to implement a hedging strategy using USDC Yield Index Cash-Settled Forward.

Transaction Overview

To demonstrate how this hedging solution works, the following transaction details illustrate the implementation and execution of the USDC Yield Index Cash-Settled Forward as a smart derivative.

Transaction Details

Parties: Counterparty A (Reference Yield Index Buyer) and Counterparty B (Reference Yield Index Seller).
Trade Date: September 10, 2025.
Trade Type: USDC Yield Index Cash-Settled Forward.
Direction: Counterparty A buys the forward yield index, and Counterparty B sells it. The settlement is in cash, based on the difference between the fixed and variable rates.
Maturity: September 15, 2025.
Notional Amount: $ 5,000,000 USD.
Collateral: ERC-3643 Tokenized Assets (e.g., regulated stablecoin).
Forward Rate: 4.8% (fixed rate).
Reference Rate: Chainlink CDY USDC Yield index

Financial Instruments in the transaction

- An ERC-3643 Token representing a regulated stablecoin.
- A USDC Yield Index Cash-Settled Forward deployed as a smart contract.

Technical Setup

Compliance Infrastructure

Integrates with Tokeny ERC-3643 compliance modules to ensure all collateral movements are compliant:

- Identity Verification: All derivative parties must have verified ONCHAINID
- Transfer Compliance: Compliance checked before collateral deposit/withdrawal
- Ongoing Monitoring: Ongoing verification throughout the derivative lifecycle
- Cross-Border Support: Automatic jurisdiction checking and regulatory compliance

Collateral Infrastructure

`IdentityRegistry` (OnchainID): The foundational contract that maps wallet addresses to verified on-chain identities and their associated claims (e.g., KYC/AML status, accredited investor status, jurisdiction).

`ERC-3643 Token Contract` (e.g. Tokenized MMFs or regulated stablecoins): Specific ERC-3643 token contract is deployed. It is configured to point to the `IdentityRegistry` and embed transfer restrictions, ensuring only compliant entities can hold or transfer these bonds. ERC-3643 tokens to be used as collateral for derivative contracts.

Derivative Infrastructure

`ParticipantRegistry` (Compliance Gateway) : A dedicated `ParticipantRegistry` smart contract is deployed. It handles all identity and compliance verification using the ERC-3643/OnchainID framework. All other contracts in the ecosystem query this single registry for compliance checks. This contract is configured to interact with the `IdentityRegistry` to perform compliance checks (e.g., its `isCompliant(address _participant)` function queries the `IdentityRegistry` for specific claims or whitelisted status).

`A Factory Contract:` A single smart contract responsible for deploying new instances of the USDC Yield Index Cash-Settled Forward contracts. It is configured to store the address of the `ParticipantRegistry` contract (or receives it as a constructor argument during deployment), making it aware of the compliance authority. It contains the logic to deploy new instances of the index forward contracts.

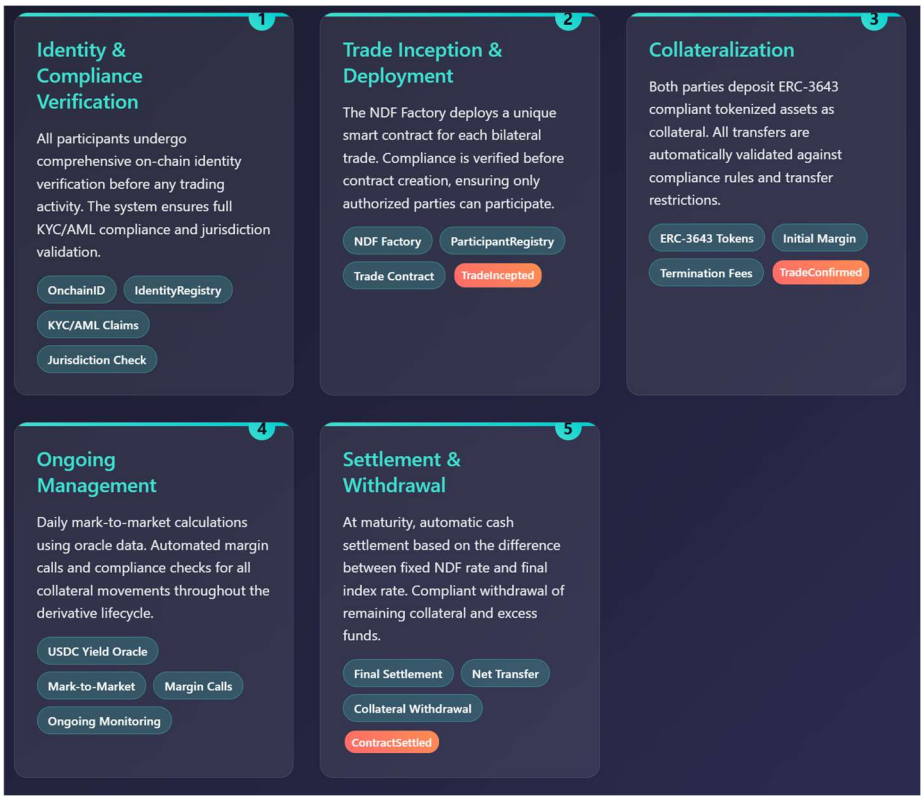
`Derivative Contract:` A separate smart contract deployed for each individual bilateral USDC Yield Index Cash-Settled Forward trade.

Test Trade

Network	Polygon Amoy
ERC-3643 Token Contract	https://amoy.polygonscan.com/address/0x97d66cb700D69F3059F2ad482A49A5429F67b7f7
Factory Contract	https://amoy.polygonscan.com/address/0xA7644267cf9cb2dba93Ef831157aF9e7F07c4381
Derivative Contract (on-chain trade)	https://amoy.polygonscan.com/address/0x830A4382B70c9E02C27B5e99cA66bCE685c36A18

The source code for this use case is available in this GitHub repository: https://github.com/QualitaX/ERC-3643-Tokens-for-Derivatives

Overview of Trade Lifecycle using a Derivative Smart Contract



1. **On-Chain Identity & Compliance Verification**: Before a trade can even be initiated, both parties must be verified. This involves two core components:
    - **IdentityRegistry (OnchainID)**: This foundational contract maps a participant's wallet address to their verified identity, including claims like KYC/KYB/AML status, jurisdiction, and accredited investor status.
    - **ParticipantRegistry**: A dedicated compliance gateway that queries the `IdentityRegistry` to perform real-time verification. It ensures that only compliant entities can engage in the OTC bilateral trade.
2. **Trade Inception and Collateralization**: With compliance verified, the trade begins:
    - A **Factory Contract** is used to deploy a unique **Index Forward Contract** for the specific bilateral trade. This factory contract is aware of the `ParticipantRegistry` and ensures the parties are compliant before creating the new derivative contract.
    - One counterparty then calls the `inceptTrade` function on the newly deployed Index Forward Contract to incept the trade. This function locks the ERC-3643 assets into the Index Forward smart contract, which acts as the initial margin and termination fee. The smart contract then emits a `TradeIncepted` event.

3. **Confirmation and Collateral**: The second counterparty then confirms the trade by calling the `confirmTrade` function and also posts their initial margin and termination fee into the contract. This step triggers the `TradeConfirmed` event. All collateral movements, both for the initial deposit and for any future margin calls, are

checked by the `ParticipantRegistry` to ensure they meet the `ERC-3643` transfer compliance rules.

4. **Ongoing Mark-to-Market and Margin Calls**: The Index forward contract is designed to get the USDC Yield Index, through an oracle. This data is used to perform daily mark-to-market calculations, which determine any potential margin calls. The `CheckMarginCall` evaluates the required margin. If a counterparty needs to post additional collateral, the transfer is automatically checked for compliance by querying the `ParticipantRegistry` before being accepted. The contract includes functions for collateral management, such as `postCollateral` to add more funds to meet a margin call. If a party fails to post the required margin, the trade can be automatically terminated.The `TradeTerminated` event would be emitted in this scenario.
5. **Final Settlement**: At maturity, the contract facilitates the final cash settlement based on the difference between the fixed forward Rate and the final Yield Index Rate. The `performSettlement` and `settle` functions handle this process, and a `ContractSettled` event is emitted upon completion. The USDC Yield Index Cash-Settled Forward Contract executes the settlement by transferring the net amount between the parties' collateralized funds.
6. **Collateral Withdrawal**: Once the trade is fully settled or terminated, the counterparties can withdraw their remaining ERC-3643 collateral and any excess funds using functions `withdraw` or `withdrawInitialMarginAndTerminationFees`, with the withdrawal also being subject to a final compliance check by the `ParticipantRegistry` to ensure all rules are followed.

Overview of the USDC Yield Index Cash-Settled Forward Smart Contract

Key Functions:

- **inceptTrade**: Initiates a new trade with a counterparty, specifying the trade data, position, payment amount, and initial settlement data. This function returns a unique `tradeID`.
- **confirmTrade**: The other party to the trade confirms the terms of the initiated trade.
- **performSettlement**: This is a core function for the cash settlement. It takes a `_settlementAmount` and `_settlementData` to finalize the exchange of funds.
- **CheckMarginCall**: This function is used to evaluate margin requirements for the contract. The `getMarginRequirement` function can also be used to query the current margin buffer and termination fees.
- **requestTradeTermination / confirmTradeTermination**: These functions allow one or both parties to propose and agree on an early termination of the contract.
- **balanceOf**: A standard function for tokens that checks the balance of a specific account.

Key Events: Events are emitted by the contract to log important actions and can be monitored off-chain.

- **0x858f0e93 - TradeIncepted**
  - Event signature:TradeIncepted(address,address,string,string,int256,int256,string)
  - Parameters: initiator, withParty, tradeId, tradeData, position, paymentAmount, initialSettlementData
- **`0x8d71833e - TradeConfirmed`**
  - Event signature: TradeConfirmed(address,string)
  - Parameters: confirmer, tradeId
- **`0xec11c4e9 - CollateralUpdated`**
  - Event signature: CollateralUpdated(string,address,uint256)
  - Parameters: tradeID, updater, collateralAmount
- **`0x0b6f20cc - ContractSettled`**
  - Event signature: ContractSettled(string,address,address,uint256,uint256,uint256)
  - Parameters: tradeID, payer, receiver, netSettlementAmount, fixedRatePayment, floatingRatePayment
- **`0x21c3cbc2 - TradeTerminated`**
  - Event signature: TradeTerminated(string,string)
  - Parameters: tradeId, cause

Use Case 2: EURUSD Forward with Delivery

In 2024, FX derivatives grew by a rapid 10% yoy to reach $130 trillion[4]. For this second use case, we will explore a Physical FX Forward. For a market-making bank, it is a foundational service that provides liquidity and risk management solutions to its institutional clients. For an asset manager or hedge fund, it is a critical tool for locking in a future exchange rate, protecting the value of foreign currency-denominated assets and income streams from adverse currency movements. The "delivery" aspect ensures the contract is tied to a genuine, physical cash flow, which is fundamental to managing real-world, cross-border investment risk.

In a nutshell, as financial institutions engage in complex, multi-currency strategies, they face inherent foreign exchange risk. While standardized exchange-traded futures exist, they often do not match the specific dates or notional amounts required for a perfect hedge, creating basis risk. A Physical FX Forward provides a bespoke, over-the-counter (OTC) solution that bridges this gap, offering a transparent and legally binding mechanism to manage precise on-balance-sheet currency exposures.

[4] https://www.bis.org/publ/otc_hy2411.htm

Illustrative Example

A European-based hedge fund has a significant portfolio of investments in publicly listed US companies. As part of its strategy, the fund anticipates receiving a substantial dividend payment of USD 500 million in six months' time. The fund's base currency is the Euro (EUR), and its risk management policy requires that all significant foreign currency exposure be hedged back to its base currency. The fund's risk management team is concerned about the potential for the US Dollar (USD) to weaken against the Euro (EUR) over the next six months. If the USD depreciates, the value of the USD 500 million dividend would be worth less in EUR when the fund repatriates the funds. This creates an unacceptable exchange rate risk that could erode the fund's returns.

To eliminate this risk, the hedge fund enters into a Physical FX Forward contract with its prime broker. They agree to a forward rate today to exchange $500 million USD for EUR in six months. This forward rate locks in the exact exchange rate for the future conversion, regardless of how the market rate changes.

In six months, when the fund receives a USD 500 million dividend, it will physically deliver the funds to the bank. In return, the bank will deliver the pre-agreed amount of EUR to the fund. This process ensures the fund receives the expected EUR value of its dividend, completely removing the currency risk from the transaction.

Transaction Overview

To demonstrate how this would work in practice, the following transaction details illustrate the key mechanics of a physical FX forward contract implemented as a smart derivative contract and relying on Frictionless Markets FX Swap infrastructure.

Transaction Details

Parties: Counterparty A and Counterparty B.
Trade Date: Monday, Day 1
Trade Type: EUR/USD forward with delivery
Direction: Counterparty A buys 10,000,000 fsEUR and sells fsUSD.
Notional:
Maturity: 5 business days from the trade date (end of the day on Friday, Day 5).
Initial Forward Rate: 1.0500 EUR/USD (meaning €1 = $1.0500).
Total fsUSD to be Delivered: 10,000,000 fsEUR x 1.0500 = 10,500,000 fsUSD.
Collateral: Both parties post an initial margin of 50,000 fsUSD + 10,000 fsUSD Termination fees.

Financial Instruments in the transaction

- **fsUSD:** Fiat-backed Institutional Deposit Token (USD) as primary collateral and settlement asset
- **fsEUR:** Fiat-backed Institutional Deposit Token (EUR) as reference currency and hedge notional.

Technical Setup

Orchestration Infrastructure

The Chainlink Runtime Environment (CRE) provides the decentralized execution layer that automates and secures workflow orchestration. Each derivative trade lifecycle triggered by events such as oracle price updates, compliance checks, or settlement milestones can be codified as a CRE Workflow. These workflows run across Workflow DONs, which coordinate triggers and callbacks, and invoke Capability DONs (e.g., data fetch, onchain write). This ensures consistent, verifiable execution of trade processes, reduces manual intervention, and enables modular integration of compliance, collateral, and settlement logic

Compliance Infrastructure

Integrates with Frictionless Markets ERC-3643 compliance modules on Avalanche Fuji to ensure all collateral movements are compliant:

- Identity Verification: All derivative parties must have verified ONCHAINID along with a verified risk-based assessment, KYC/AML file, a verified off-chain identity.
- Transfer Compliance: Compliance checked before collateral deposit/withdrawal
- Ongoing Monitoring: Ongoing verification throughout the derivative lifecycle
- Cross-Border Support: Automatic jurisdiction checking and regulatory compliance

Collateral Infrastructure

`IdentityRegistry` (OnchainID): The foundational contract that maps wallet addresses to verified on-chain identities and their associated claims (e.g., KYC/AML status, accredited investor status, jurisdiction).

`ERC-3643 Token Contract`: Specific ERC-3643 token contract is deployed. It is configured to point to the `IdentityRegistry` and embed transfer restrictions, ensuring only compliant entities can hold or transfer these bonds. ERC-3643 tokens to be used as collateral for derivative contracts.

Derivative Infrastructure

`ParticipantRegistry` (Compliance Gateway) : A dedicated `ParticipantRegistry` smart contract is deployed. It handles all identity and compliance verification using the ERC-3643/OnchainID framework. All other contracts in the ecosystem query this single registry for compliance checks. This contract is configured to interact with the `IdentityRegistry` to perform compliance checks (e.g., its `isCompliant(address _participant)` function queries the `IdentityRegistry` for specific claims or whitelisted status).

`An FX Forward Factory Contract:` A single smart contract responsible for deploying new instances of the FX Forward contracts. It is configured to store the address of the `ParticipantRegistry` contract (or receives it as a constructor argument during

deployment), making it aware of the compliance authority. It contains the logic to deploy new instances of ERC-6123 contracts.

FX Forward Smart Contract: A separate FX forward smart contract deployed for each individual bilateral FX Forward with Delivery trade.

Test Trade

Network	Avalanche Fuji
fsUSD Token Contract	https://testnet.snowtrace.io/address/0xdB783ea7C0534dc7A0edb9De735C063bd02e4322
fsEUR Token Contract	https://testnet.snowtrace.io/address/0x580FAC15FFE9b2DF937bCe58f686233e911e53D4
Factory Contract	https://testnet.snowtrace.io/address/0x060d46f1Cdb2Ee0Ecf8407E3344e35e6eE0453EA
FX Forward Contract (on-chain trade)	https://testnet.snowtrace.io/address/0x56b78E1092FAE562A6d2C18CeEdB17859f75C64a
Frictionless FXSwap Contract	https://testnet.snowtrace.io/address/0xe3a39a11066eD8e0c233c24959943ab30c7Aeb11

The source code for this use case is available in the GitHub repository below:
https://github.com/QualitaX/ERC-3643-Tokens-for-Derivatives-FX

In addition,

- Frictionless Markets - Frictionless Protocol
  https://gitlab.com/dfyclabs/protocol/dfyclabs-tokens
- Frictionless Markets - Frictionless Protocol Documentation
  - Institutional Deposit Tokens: https://docs.frictionless.markets/legal/legal-notices/terms-of-service/institutional-deposit-token-holders
  - FXSwaps Contracts: https://docs.frictionless.markets/developer/smart-contracts/smart-contract-docs/frictionless-fx-swaps

These two use cases demonstrate how the ERC-3643 standard can provide the foundation for smart derivative infrastructure. By combining regulatory compliance with automation, these smart derivative contracts can offer institutional participants sophisticated risk management capabilities while maintaining the efficiency and accessibility advantages of decentralised finance.

The Physical FX Forward with Delivery showcases how smart contracts can provide bespoke, transparent hedging solutions for cross-border currency exposures. Meanwhile, the USDC Yield Index Cash-Settled Forward illustrates how DeFi-native benchmarks can bridge the basis risk between traditional finance and decentralized markets, offering sophisticated risk management tools for the growing digital asset ecosystem.

Legal & Regulatory Considerations

From a legal perspective, we consider there to be an in-principle workable path for UK and EU counterparties to implement the OTC bilateral trades (described in the Use Cases above) via a smart contract, using the International Swaps and Derivatives Association ("ISDA") documentation framework and with non-regulatory driven collateral arrangements. The smart contract code itself shall have no independent legal effect – it is intended only to automate certain transactional functions with respect to the OTC bilateral trades as further described above (i.e. trade execution, collateral management, valuation and settlement). As such, the legal relationship between the parties with respect to each OTC bilateral trade would remain solely governed by the underlying ISDA documentation.

The underlying ISDA documentation (comprising an ISDA Master Agreement, related Confirmation(s) and ISDA published Definition(s), and a 1995 Credit Support Annex) will provide the legal framework for the smart contract, and the smart contract code shall be structured to give effect to the relevant provisions of that underlying documentation. Similarly, bespoke amendments will be required to the underlying ISDA documentation to ensure the underlying legal framework aligns with the functionality of the smart contract (i.e. automated settlement, valuation using oracles etc.).

We have set out a number of key considerations below. However, this list is not exhaustive, and there are several other factors to consider. Please also note that these considerations will not be implemented in the Proof-of-Concept smart derivative contracts, but will need to be resolved/implemented when developing the final model.

- **Smart Contract Disruption:** A key consideration is how disruptions at the smart contract level (e.g. technical faults) are treated. This is an important point - for example, if a technical fault causes one party not to make a payment when due, that failure would constitute an Event of Default (subject to the applicable grace period) under the ISDA Master Agreement, entitling the other party to close-out all outstanding transactions under the ISDA Master Agreement at its side of the market. One potential solution would be to, in the event of a smart contract disruption, allow parties to suspend or override the automated settlement provisions of the smart contract and revert to off-chain settlement until the disruption ceases.

- **Conditions Precedent:** Under the ISDA Master Agreement, a party's payment obligations are subject to the condition precedent that no Event of Default or Potential Event of Default has occurred with respect to its counterparty. Where such an event has occurred and is continuing, the non-defaulting party can suspend its payment obligations with respect to transactions under the ISDA Master Agreement. This needs careful consideration when automating settlement via the smart contract.

- **Payment Netting:** The ISDA Master Agreement provides that payment obligations due on the same day and in the same currency in respect of a single transaction (or, if agreed between the parties, across multiple transactions) will be netted against each other to produce a single payable amount. The smart contract will therefore need to distinguish between different payment streams and calculate the net amount payable. The smart contract will also need to ensure that there are no gaps between on-chain and off-chain payment streams (i.e. if some amounts are

determined/settled off-chain, consideration will need to be given to how those calculations feed into the on-chain system to ensure they are appropriately netted).

· **Discretion**: There are various provisions in the ISDA documentation that rely on the exercise of discretion by one of the counterparties (or by the calculation agent), either in respect of a single transaction or more generally across transactions. Key areas include (but are not limited to):

o the determination of Events of Default and/or Termination Events, and the calculation of the relevant close-out amount; and

o the determination of adjustment or disruption events at the transaction level, and the application of the relevant fallbacks. These determinations are typically made by the calculation agent.

In our view, discretionary determinations (such as those as described above) are less well suited to automation and should be dealt with off-chain, meaning that the smart contract will need to allow the flexibility for the parties to take the relevant transaction off-chain in certain circumstances. Furthermore, any actions/determinations resulting from the exercise of such discretion off-chain must be accurately reflected in the smart contract to avoid any mismatch.

- **Business Days**: The ISDA framework uses several "Business Day" definitions, which are central to determining the days on which parties are required to make payments. These definitions are generally tied to days on which commercial banks and/or the relevant settlement systems are open in the applicable location, and the smart contract should adhere to these "Business Day" definitions.

- **Collateral:** Where using ERC-3643 Tokens as collateral, the following should be considered:

o ISDA's 1995 Credit Support Annex does not contemplate digital assets as collateral, so bespoke amendments will be required to the 1995 Credit Support Annex underlying the smart contract to accommodate ERC-3643 Tokens as collateral. These include (but are not limited to) (i) incorporating transfer and valuation provisions for E-3643 Tokens and (ii) including provisions to deal with forks and/or airdrops (if applicable).

o The 1995 Credit Support Annex's notice-and-demand framework for collateral calls and transfers will need to be amended to reflect that collateral will be transferred automatically via the smart contract.

o To automate collateral transfers, the smart contract must be able to replicate the calculation of **"**Exposure**"** under the 1995 Credit Support Annex, which is used to determine whether a collateral transfer is required. The calculation of "Exposure" requires a degree of discretion, which is exercised by the party acting as the valuation agent. As such, careful consideration must be given as to whether such discretion can be translated into objective, rule-based logic within the smart contract, or whether "Exposure" should in-fact be calculated differently to accommodate automatic collateral transfers

via the smart contract (in which case the definition of “Exposure” in the underlying 1995 Credit Support Annex would need to be revised accordingly).

- Collateral transfers under the 1995 Credit Support Annex are effected by title transfer, meaning the receiving party obtains full rehypothecation rights in respect of the transferred collateral. Accordingly, the smart contract will need to ensure that parties are afforded full rehypothecation rights in relation to the ERC-3643 Tokens transferred as collateral. This is important to mitigate the risk of any potential re-characterisation of the arrangement as creating a security interest.

- Furthermore, due to these rehypothecation rights, the transferee may not retain the exact same collateral originally received. As such, where the transferee is required to effectively “return” collateral, the transferee is obliged to return “equivalent” (meaning fungible) collateral. The smart contract must therefore be able to clearly identify what constitutes fungible collateral for return purposes.

- **ISDA Common Domain Model (CDM):** When building the smart contract, it could be relevant to leverage ISDA’s CDM. It is a model developed by ISDA providing a standardised, machine-readable, and machine-executable blueprint for how derivatives are traded and managed throughout their entire lifecycle, offering a single and common digital representation of trade events and actions.

Ongoing Development & Future Outlook

The integration of ERC-3643 compliant tokens with smart derivative contracts represents a significant opportunity to address the systemic inefficiencies that plague the uncleared Over-The-Counter (OTC) derivatives market. This approach delivers benefits across multiple dimensions of capital and operational efficiency.

- **Yield Enhancement:** Tokenized collateral, such as tokenized money market funds, can generate returns while posted as margin. This is a sharp contrast to traditional cash collateral, which often earns minimal interest.
- **Operational Efficiency:** Automating settlement and reconciliation eliminates the manual effort that currently consumes 38% of operational resources. Deterministic smart contract execution can also dramatically reduce the 45% dispute rate on margin calls.
- **Enhanced Risk Management:** The system allows for mark-to-market calculations and automated margining. This can lead to more sophisticated netting arrangements across multiple contracts and counterparties, all within a single compliance framework.

While the technical foundation and regulatory path are being established through these proofs-of-concept, the next crucial phase is to quantify the precise economic advantages. Preliminary analysis suggests that settlement and reconciliation efficiencies could yield double digit basis points in annual cost savings from reduced operational overhead and dispute resolution. Capital efficiency improvements, from yield-generating collateral to enhanced netting, could deliver an additional double digit basis points annually. However, rigorous modeling is essential to substantiate these estimates across different market conditions and counterparty profiles. This quantification is vital to building a compelling business case for institutional adoption.

Furthermore, while our proofs-of-concept demonstrate direct on-chain collateral management for technical validation, institutional adoption requires robust custodian integration to meet fiduciary standards and regulatory requirements. Simultaneously, smart contract confidentiality is critical for competitive OTC trading, where sensitive transaction details, pricing models, and counterparty positions must remain private. Technologies like Fully Homomorphic Encryption (FHE) such as those developed by Zama and Zero-Knowledge Proofs (ZKPs), will be key to enabling computations and verification on encrypted data without revealing sensitive information. This ensures both compliance and privacy, bridging the gap between traditional finance and the digital asset ecosystem.

www.qualitax.io
contact@qualitax.io