Deep Dive into ERC-6123: Rethinking Financial Derivatives.

August 2024

AUTHOR

Bradley Stone - Research Lead, QualitaX

REVIEWERS

Peter Kohl-Landgraf - Co-author ERC-6123, DZ BANK AG

Prof. Dr Christian Fries - Co-author ERC-6123, DZ BANK AG

CONTRIBUTORS

Chaals Neville - Enterprise Ethereum Alliance

Ciarán McGonagle - Tokenovate

Richard Baker - Tokenovate

Wilfried Schütte - DZ BANK AG

Yevheniia Broshevan - Hacken

Valeriia Skorik - Hacken

Andrew Richardson - Kaleido

Brindrajsinh Chauhan – Kaleido

Anaïs Ofranc - QualitaX

Samuel Edoumou - QualitaX

Malcolm Moreno

Stefan Haupt

QX

Table of Contents

ERC-6123 Overview 4
Summary 5
Introduction 7
Tokenized Financial Instruments vs Native On-Chain Financial Instruments 9
Derivatives Market 13
Introducing ERC-6123 21
Overview 21
Use Cases 23
Reference Implementations 26
ERC-6123 Contemporaries 27
ERC-7586 27
ERC-3643 28
ERC-1400 28
ERC-1155 29
CMTAT 29
ERC-6123 Technical Breakdown 31
Key Methods 31
Trade and Settlement Events 32
State Machine Implementation for a Single Trade 33
Rationale for ERC-6123 Design Patterns 34
Implementation Sequence 35
ERC-6123 Trade Initiation and Settlement Lifecycle 36
Comparing Traditional vs. ERC-6123 Non-Cleared Interbank OTC Derivatives.. 41
'As-Is' Non-cleared interbank OTC interest rate cap trade 41
'To-Be' Non-cleared interbank OTC interest rate cap trade 48
Summary of key differences 51
Literature and References 54

ERC-6123 Overview

- **Smart Derivative Contracts:** ERC-6123 is an Ethereum Virtual Machine (EVM)-based standard for creating Smart Derivative Contracts (SDCs).
- **Immutable:** ERC-6123 enables the creation of self-executing, transparent, and immutable derivative contracts on EVM-compatible networks.
- **Full Contract Lifecycle:** ERC-6123 provides a standardized interface and functions for initiating, confirming, and settling derivative trades.
- **Automation and Efficiency in Derivatives Lifecycle:** Utilizes smart contract technology to automate key aspects of the derivatives lifecycle, reducing counterparty risk and increasing efficiency.
- **Eliminating Counterparty Credit Risk:** ERC-6123 is designed to remove counterparty credit risk, a significant concern in traditional over-the-counter (OTC) derivatives trading, and aims to bring the benefits of decentralization to the traditional derivatives market.

Summary

Problem: 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.

Solution: ERC-6123 offers an open-source standard for creating and managing derivative contracts on blockchain platforms. Key benefits include 1) Automation: Self-executing contracts with predefined rules reduce the need for intermediaries and manual processes 2) Standardization: A uniform interface and set of functions promote interoperability and composability between different derivative contracts 3) Enhanced Security: Blockchain technology ensures transparency, immutability, and real-time settlement 4) 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 5) 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.

Summary

Technical level: ERC-6123 is a smart contract interface written in Solidity that standardizes the creation, management, and settlement of decentralized derivative contracts on EVM-compatible networks. The core contract, ISDC.sol, defines the interface and method signatures for the Smart Derivative Contract (SDC), which is implemented as a finite state machine with strict transition rules. Key methods include inceptTrade(address,string,int,int256,string) and confirmTrade(address,string,int,int256,string) for initiating and confirming trades, cancelTrade(address, string memory, int, int256, string memory)for one counterparty to unilaterally cancel a trade, for example, in the case where the trade is not confirmed in a timely manner, initiateSettlement() and performSettlement(int256,string) for triggering and processing settlements, and requestTradeTermination(string,int256,string memory), confirmTradeTermination(string,int256, string memory) for mutually terminating contracts and cancelTradeTermination(string,int256, string)to allow the requesting party to cancel its trade termination request. The proposed specification comes with a reference implementation. The reference implementation of the SDC integrates with external components through a pull-based callback mechanism, using an ERC-20 compatible settlement token for transferring value and an off-chain valuation service for providing settlement data. Events are emitted at key stages of the contract lifecycle, allowing off-chain systems to monitor and respond to state changes.

Practical applications: 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.

Introduction

Managing and settling derivative contracts on-chain presents several challenges. ERC-20 and ERC-721 are popular Ethereum token standards designed for fungible and non-fungible tokens, respectively. Derivatives and other complex financial instruments require support for their entire lifecycle, including initial setup, ongoing management, and final settlement. For instance, product data needs to be confirmed on-chain between both parties to mitigate inconsistencies in contract terms right at the beginning. ERC-6123[1] captures the entire lifecycle of a financial product, such as an OTC derivative, not just the final transfer of value. While ERC-20 and ERC-721 have been successful for many use cases, they fall short when it comes to the complex requirements of the processing of financial instruments as derivatives contracts:

Lack of built-in time dependency: Derivatives often have specific time-based conditions and expiration dates, which are not natively supported in ERC-20 or ERC-721.

Limited state management: Derivatives have complex lifecycles involving margin calls, rollovers, and early terminations, which are not supported by basic token standards. These standards do not provide mechanisms for managing the evolving states of a derivative contract throughout its lifecycle.

Inadequate support for multi-party interactions: Many derivatives involve multiple parties with different roles and permissions. This is not easily implemented using existing token standards with a simple token ownership model.

Conditional settlements: Unlike simple token transfers, derivative settlements may depend on external market conditions or specific contract terms.

Counterparty risk management: ERC-20 and ERC-721 lack built-in mechanisms for managing and mitigating counterparty risk, which is crucial for derivatives.

Collateral management: Fundamental Ethereum standards ERC-20 and ERC-721 do not provide native functionality for handling collateral posting, monitoring, and fallback processes in case of failed transfers.

---

[1] https://eips.ethereum.org/EIPS/eip-6123

ERC-6123, the Smart Derivative Contract (SDC) standard, seeks to address these challenges by providing a framework for creating, managing, and settling derivative contracts on EVM-based networks.

To understand its significance, we must compare ERC-6123 with existing standards:

Figure 1: Comparison of ERC Standards

FEATURES	ERC-20	ERC-721	ERC-6123
CONTRACT TYPE	Fungible Tokens	Non-Fungible Tokens (NFTs)	Smart Derivative Contract (SDC)
REGULATORY COMPLIANCE	External to protocol	External to protocol	Partial - designed to facilitate compliance
COMPLIANCE RESPONSIBILITY	Token issuers and validators	Token issuers and validators	Smart contract, oracles, and counterparties
USER EXPERIENCE (UX) CHALLENGE	Due diligence process is inefficient and prone to error	Similar to ERC-20, complex due diligence	Improved, but requires blockchain familiarity
ADOPTION BARRIER	Compliance separated from token standard leads to inefficiencies	Similar to ERC-20, complex legal requirements	Integration with existing systems and regulatory adaptation
PRIMARY USE CASE	General digital assets	Unique digital assets, collectibles	OTC derivatives.

The following sections will examine the current state of the derivatives market and its challenges, setting the stage for understanding why a standard like ERC-6123 is beneficial. We will then explore the technical specifications and potential implications of ERC-6123 in detail.

This report explains how ERC-6123 can improve the trading and settlement of OTC derivatives, both traditional and native on-chain derivatives.

Tokenized Financial Instruments vs Native On-Chain Financial Instruments

Tokenization of financial instruments involves creating digital representations of traditional assets like stocks, bonds, and derivatives on a blockchain network. This process involves the establishment of some legal mechanism intended to attach enforceable rights to digital entries (i.e., the token) on the system. Advantages include streamlined operations, reduced costs, and enhanced security through blockchain's immutable data and smart contract capabilities.

Figure 2: Comparison of Traditional, Tokenized, and On-chain Financial Instruments.

CHARACTERISTIC	Traditional Financial Instrument	Tokenized Financial Instrument	Native On-Chain Financial Instrument
Definition	A traditional financial contract or security representing	Digital representation of a traditional financial	Financial instrument native to and existing entirely within a

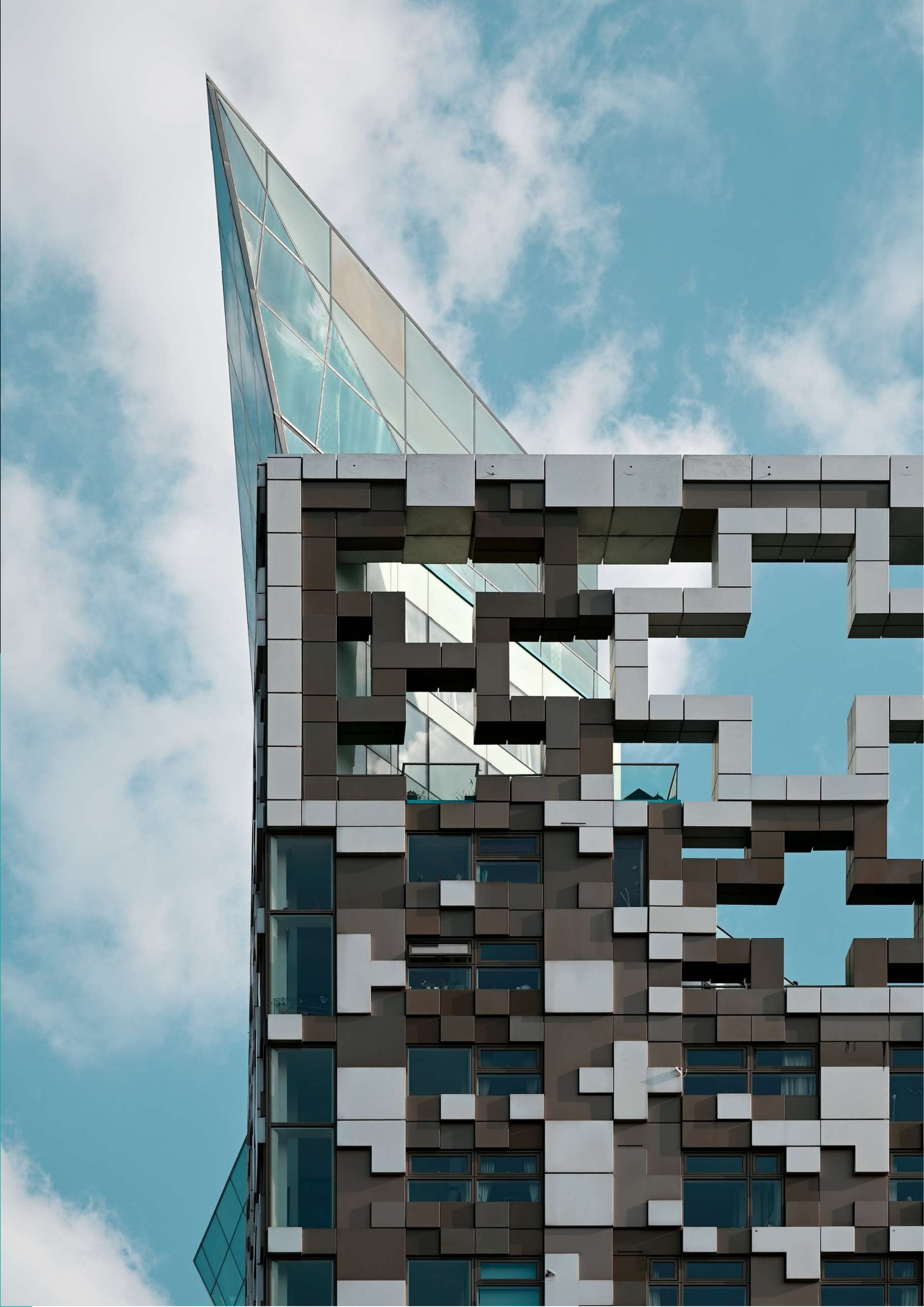
	financial value or claim.	instrument on a blockchain.	blockchain ecosystem.
Examples	Stocks, bonds, derivatives, commodities, currencies.	Security tokens (tokenized stocks/bonds), tokenized real estate, tokenized commodities.	Cryptocurrency, DeFi tokens, smart contract-based derivatives.
Underlying Asset	Real-world assets or financial claims.	Represents real-world assets in digital token form	May not have any underlying real-world asset.
Regulatory Framework	Well-established financial regulations.	Subject to both traditional and emerging digital assets regulations.	Regulatory framework still evolving, often in a gray area.
Intermediation	Relies heavily on financial intermediaries.	May reduce but not eliminate intermediaries.	Can operate with minimal or no intermediaries.
Technology	Centralized databases and traditional IT systems.	Uses DLT/blockchain for representation and transfers.	Entirely DLT/ blockchain-based.
Settlement Time	Can vary from instant to several days.	Faster than traditional, but may still involve off-chain processes.	Instant to near-instantaneous settlement.

Programmability	Limited, mostly static terms.	Some programmability through smart contracts.	Highly programmable with complex, automated functions.

While tokenized financial instruments bridge the gap between traditional finance and blockchain technology, native on-chain financial instruments exist entirely within blockchain ecosystems. The key distinction lies in their underlying nature:

1. Tokenized instruments represent digital forms of traditional assets.
2. Native on-chain instruments exist solely within the blockchain environments, not tied to off-chain assets.

With that crucial distinction between tokenized and native on-chain financial instruments covered, we will explore the broader derivatives market, setting the stage for understanding ERC-6123’s approach and value proposition.



Derivatives Market

Derivatives are financial contracts whose value is derived from an underlying asset or benchmark. They allow parties to mitigate market risk—hedging against adverse price movements or speculation—by entering into agreements based on future outcomes.

The primary function of derivatives is to transfer risk from a party seeking to hedge (limit) risk to a party willing to assume that risk. These risks can be related to commodity prices, interest rates, exchange rates, or even the creditworthiness of a third party[2]. While the primary function of the derivative is to manage a specific type of risk (e.g., market risk), it may itself introduce unwanted counterparty risk against the derivative counterparty.

Derivatives primarily fall into two main categories: over-the-counter (OTC) and exchange-traded. OTC derivatives are customized contracts negotiated directly between two parties, offering flexibility in terms and conditions but typically with less transparency and regulation. These instruments are often used for specific risk management needs, including swaps, forwards, and certain options. On the other hand, exchange-traded derivatives are standardized contracts traded on regulated exchanges, such as futures and many options. These derivatives offer greater liquidity, transparency, and reduced counterparty risk due to the involvement of clearinghouses. Clearinghouses, or Central Counterparties (CCPs), mitigate the unwanted counterparty risks by acting as intermediaries between buyers and sellers, ensuring the fulfillment of contract terms and managing default risks. Additionally, some types of OTC derivative trades, especially interest rate derivatives, are now required to be cleared through CCPs, further enhancing market stability and reducing systemic risk. While both types serve essential roles in financial markets, they differ significantly in structure, regulation, and typical use cases.

Exchange-traded derivatives (ETD)

The exchange-traded derivatives (ETD) market has experienced substantial growth, with global trading volume reaching 15.19 billion contracts in April 2024, marking an 89.9% increase from the previous year[3]. This surge was primarily driven by options trading, which saw a remarkable 109% year-over-year increase to 12.57 billion contracts, with the Asia-Pacific region leading in activity. Futures trading also grew, albeit slower, rising 30.3% to 2.62 billion contracts. The market's expansion is

---

2 https://academic.oup.com/jfr/article/6/2/159/5917276

3 https://www.fia.org/fia/articles/etd-volume-april-2024

further evident in the year-to-date figures, with total volume for the first four months of 2024 reaching 63.1 billion contracts, a 77.5% increase from the same period in 2023.

2024 April ETD Volume

	Futures	Options	Total	M/M	Y/Y
Asia-Pacific	942,821,005	10,948,242,268	11,891,063,273	-0.4%	106.2%
North America	509,160,978	1,162,148,944	1,671,309,922	11.8%	40.6%
Latin America	615,497,113	340,878,293	956,375,406	38.3%	60.9%
Europe	404,272,920	101,707,303	505,980,223	-3.9%	57.3%
Other	144,541,739	21,647,330	166,189,069	-10.7%	30.1%
Grand Total	2,616,293,755	12,574,624,138	15,190,917,893	2.4%	89.9%
M/M	8.6%	1.2%	2.4%		
Y/Y	30.3%	109.9%	89.9%		

Figure 3 – 2024 April ETD Volume Source: FIA

Over-the-counter (OTC) derivatives

The over-the-counter (OTC) derivative markets experienced significant growth in 2023, with outstanding derivatives increasing by 8% to reach $667 trillion[4]. This expansion was primarily driven by interest rate derivatives, which grew by 8% year-over-year, and foreign exchange derivatives, which saw a 10% increase. However, the market also exhibited a notable seasonal pattern, with growth concentrated in the year's first half followed by a contraction in the second half. This trend reflects the global OTC derivative markets' complex dynamics and evolving landscape.

---

4 https://www.bis.org/publ/otc_hy2405.htm#:~:text=Across%20risk%20categories%2C%20growth%20rates,the%20first%20half%20of%202023.

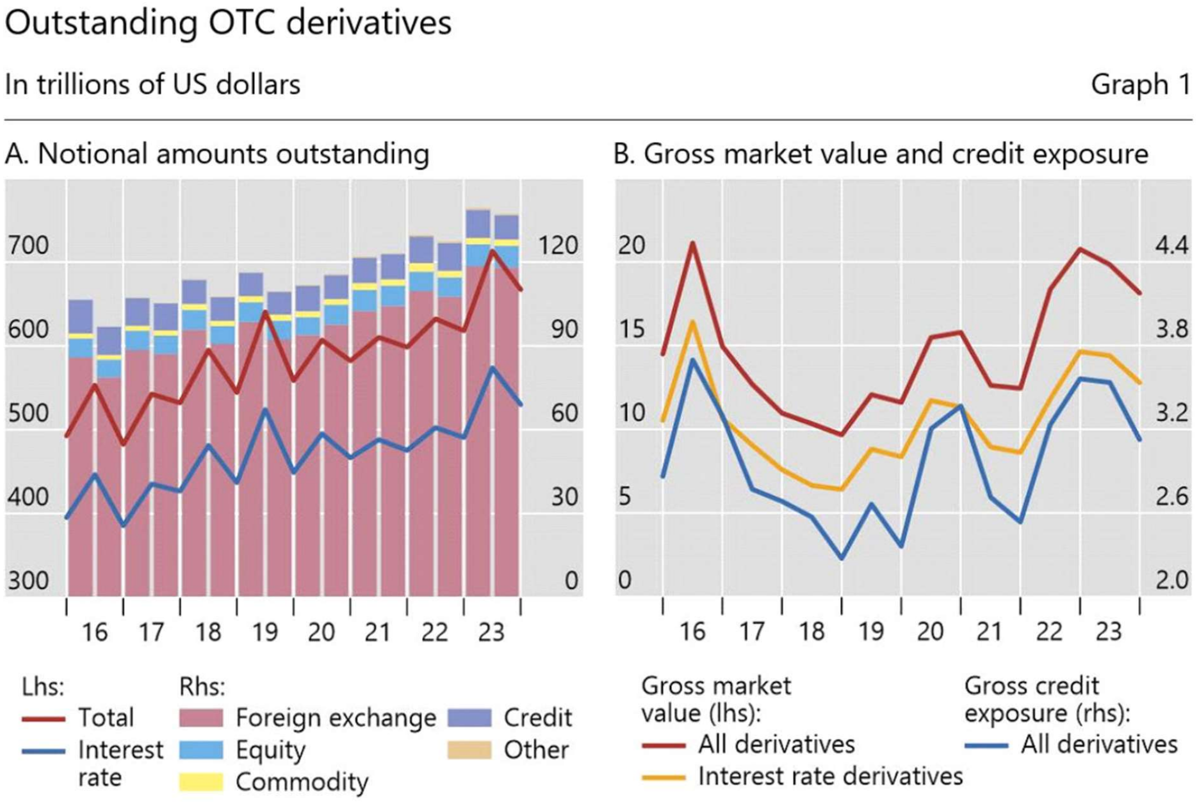


Figure 4 - OTC Derivatives Trends – Source: BIS

Centrally Cleared VS Non-Cleared OTC Derivatives

Centrally cleared and non-cleared OTC derivatives differ primarily in processing and risk management approaches.

- **Centrally Cleared Derivatives:** Trades are bilaterally negotiated between the counterparties using standardized contract terms. These are processed through a central clearinghouse, an intermediary between trading parties. Centralized clearing through CCPs mitigates counterparty risk by acting as an intermediary between trading parties. The CCP becomes the counterparty to both sides of the trade, effectively guaranteeing performance even if one party defaults. The clearinghouse requires margin payments and monitors positions, enhancing market stability and transparency.

- **Non-Cleared Derivatives:** Trades are bilaterally negotiated between the counterparties using customized contract terms. These transactions are conducted directly between two parties without the involvement of a central clearinghouse. Non-cleared derivatives offer more flexibility in terms and conditions but carry higher counterparty risk. They are typically less standardized and may be more complex, but they are often used for highly customized risk management solutions. Depending on the agreement between the parties and regulatory requirements, they can be either collateralized or uncollateralized. However, following the introduction of new post-financial crisis regulations (e.g., Dodd-Frank, EMIR), most non-cleared OTC derivatives are subject to both initial and variation margin requirements. Most non-cleared OTC derivatives are collateralized to mitigate credit risk.

According to ISDA, "non-cleared OTC derivatives play a vital role in risk management and in business decision-making that cannot be filled by clearable instruments." [5]

And, while the market for non-cleared OTC derivatives has been significantly shrinking in developed markets in response to regulatory pressures and increased costs, the need for non-standard, bespoke derivatives will persist. These instruments provide essential flexibility, customization, and innovation that standardized derivatives cannot offer. They play a crucial role in risk management, financial innovation, and meeting the specific needs of various market participants. Therefore, despite the trend toward central clearing and standardization, non-cleared OTC derivatives will remain a vital component of the financial system.

Also, emerging markets might experience different trends. In these markets, the demand for non-cleared OTC derivatives can be stable or even increasing due to less stringent regulations, specific local needs, and the lack of advanced clearing infrastructure. The global landscape could thus be quite diverse, with varying dynamics influencing the use and volume of non-cleared OTC derivatives across different regions. The paper 'ISDA Survey on OTC Derivatives in Emerging and Developing Markets' (July 2023) indicates that 88% of the emerging markets jurisdictions have no requirements to execute OTC derivatives on trading venues, and only 13% have mandatory clearing requirements.[6]

Non-cleared OTC Derivatives Challenges

While intended to manage market risk, OTC derivatives have complex processes and frictions. As bilateral contracts, they inherently carry counterparty credit risk. To mitigate this, market participants use several mechanisms 1) standardized contractual frameworks (published by ISDA) providing contractual protections against default 2) collateral processes 3) netting agreements, which allow offsetting of exposures between counterparties, reducing overall credit risk. However, these introduce their own complications. While the absence of payment netting can lead to settlement risk, it is important to note that uncleared derivatives can be netted under the ISDA Master Agreement framework, which helps

[5] https://www.isda.org/a/gPDDE/non-cleared-otc-derivatives-paper.pdf

[6] https://www.isda.org/a/qfogE/ISDA-Survey-on-OTC-Derivatives-in-Emerging-and-Developing-Markets.pdf

mitigate some of this risk. Differing valuation models between counterparties can result in collateral disputes.

Over-collateralization and initial margin (IM) requirements are implemented to address counterparty risk of collateral. IM acts as a buffer against (i) sudden intraday increases in credit exposure and/or (ii) a decline in the value of posted Variation Margin, helping protect against potential losses during the time between a counterparty's default and the closing out of positions. As previously mentioned, for certain derivatives like interest rate swaps, there's a clearing obligation through Central Counterparties (CCPs). While reducing bilateral risk, this introduces liquidity risk due to CCP requirements. CCPs demand high-quality, liquid assets for margin, which can strain participants' liquidity, especially during market stress. Additionally, the need to meet potential margin calls quickly can create short-term liquidity pressures for clearing members.

CCPs have complex default resolution processes involving non-deterministic auction procedures. All these factors make the OTC derivatives market a challenging and complex environment for participants.

Specifically, non-cleared OTC derivatives have been subject to increased costs associated with margin requirements, capital charges, and regulatory compliance. These factors make it less attractive for many market participants in traditional finance to engage in non-cleared derivatives trading.

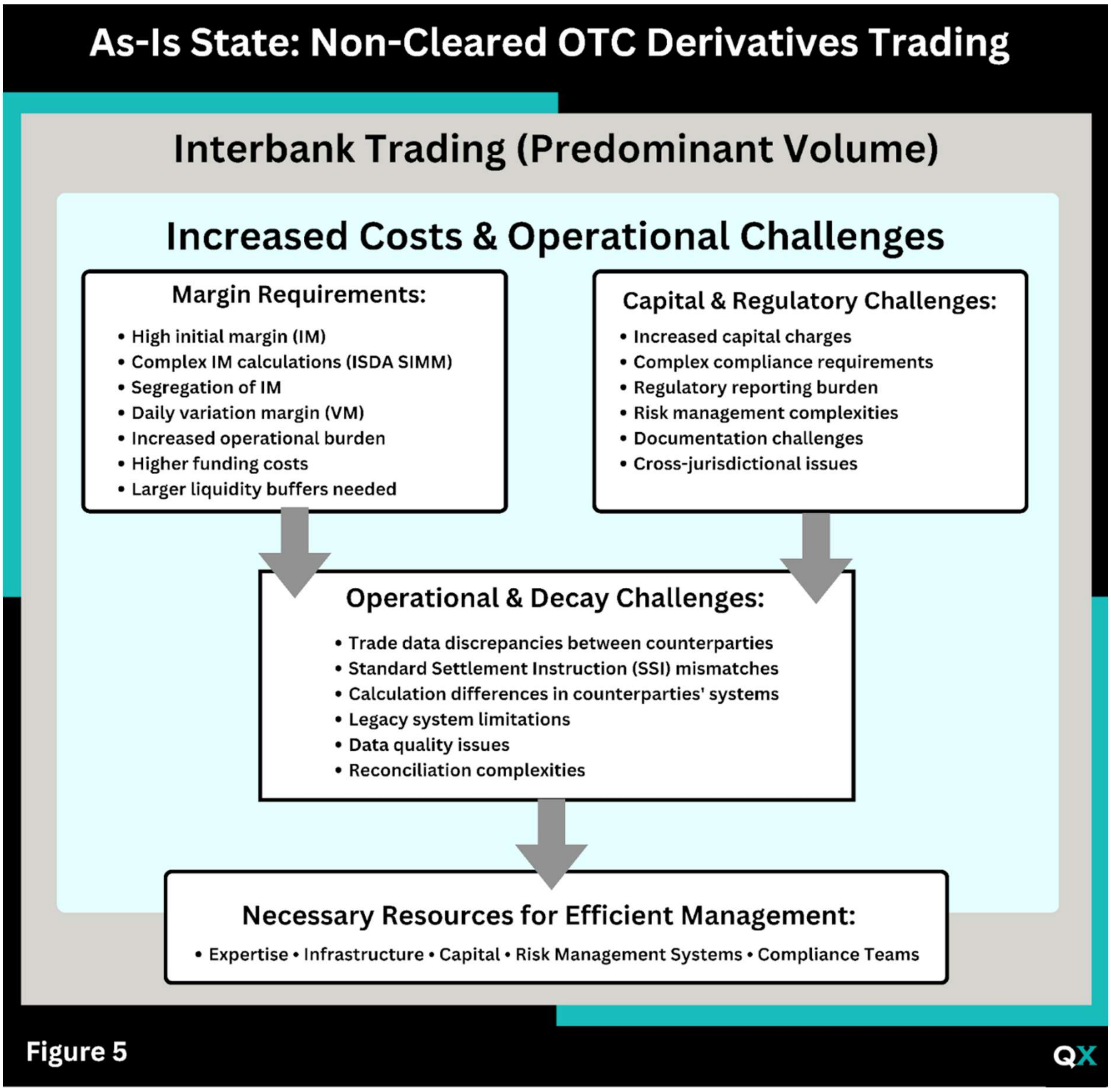


Figure 5 - 'As-Is' State: Non-Cleared OTC Derivatives Trading

Margin & Counterparty Default Risk Management

Banks must post significant upfront collateral to cover potential future exposure. Initial margin (IM) calculations often require complex models (e.g., ISDA SIMM), leading to additional operational costs. Segregation of IM increases custody costs and reduces the ability to rehypothecate assets. Regarding variation margin (VM), daily mark-to-market valuations and margin calls increase operational burden. Higher margin requirements also tie up more capital, increasing overall funding costs. Maintaining larger liquidity buffers to meet potential margin calls affects profitability.

Decay challenges

Other operational and decay challenges include both counterparties being unaware of the same trade with the same data, discrepancies in standard settlement instructions (SSIs) between counterparties, and calculations not matching in both counterparties' systems.

The ERC-6123 standard offers an approach that partially addresses these challenges by leveraging smart contracts and blockchain technology. This standard can help automate many aspects of non-cleared OTC derivative processing, from margin calculations to settlement instructions, thereby reducing operational costs, improving data consistency, and enhancing overall efficiency.

Introducing ERC-6123

Overview

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.

This is achieved through several mechanisms inherent to the ERC-6123 framework:

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. **Prefunding Mechanism:**

- **Description**: ERC-6123 requires both counterparties to pre-fund the settlement amounts before executing the trade. This ensures that the funds needed for settlement are available at the outset, reducing the risk that one party will default on its obligations.
- **Benefit:** The combination of prefunding and daily settlement offers a balanced approach between strong risk mitigation and capital efficiency. While some capital is locked initially, daily settlements prevent the accumulation of large obligations over time, so overall, it appears better for liquidity management of the participants in comparison to the traditional collateral processes.

3. **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.

4. **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.

5. **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.

6. **Transparent and Immutable Record-Keeping:**

- **Description:** Implemented as a finite state machine, all transactions and state changes within an ERC-6123 smart contract are recorded on the blockchain, providing an immutable and transparent audit trail.
- **Benefit:** This transparency enhances trust between counterparties and allows for real-time monitoring and verification of obligations.

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.

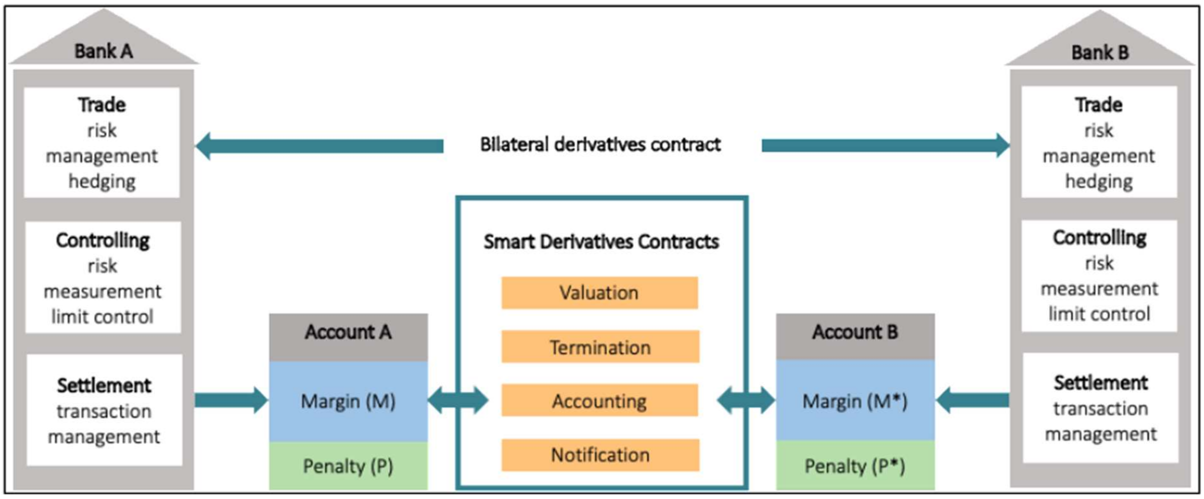


Figure 6 – ERC-6123 Mechanisms - Source: Rethinking derivative financial products - DZ Bank Innovation Lab (2018)

Use Cases

ERC-6123 is a standard designed for the creation and management of on-chain derivatives. It can cater to a variety of use cases, including tokenized derivatives such as collateralized OTC derivatives and uncollateralized OTC derivatives, Smart Bond Contracts, the creation of native on-chain derivatives, structured products like principal-protected notes or yield-enhanced products, and the creation of decentralized insurance products, where payouts are triggered automatically based on predefined conditions.

It has seen active development and involvement from institutional players and experts in the financial technology sector, highlighting the interest in its potential for delivering significant operational and cost efficiencies in trading complex OTC financial instruments.

TradFi Derivatives

Non-Cleared Interbank

In 2021, DZ Bank and Bayern LB successfully executed an Smart Derivative based on an interest rate swap leveraging ERC-6123 . The implementation involved several key players: DZ BANK and BayernLB acted as trading partners, while Eurex Clearing, Deutsche Börse's central counterparty (CCP), served as a neutral account manager for exposures from this OTC transaction.

The ERC-6123 smart derivative contract (SDC) process logic that automated key processes throughout the derivative's lifecycle was reflected in thea legally binding OTC agreement. As interest rates fluctuate, the contract autonomously calculates and processes daily payments for the uncleared derivative via Deutsche Börse. A crucial feature of this system was its ability to automatically terminate the contract if a party failed to meet the agreed terms, thereby substantially reducing exposure to counterparty risks whereby mututal termination with an agreed termination fee is also part of the legal contract[7].

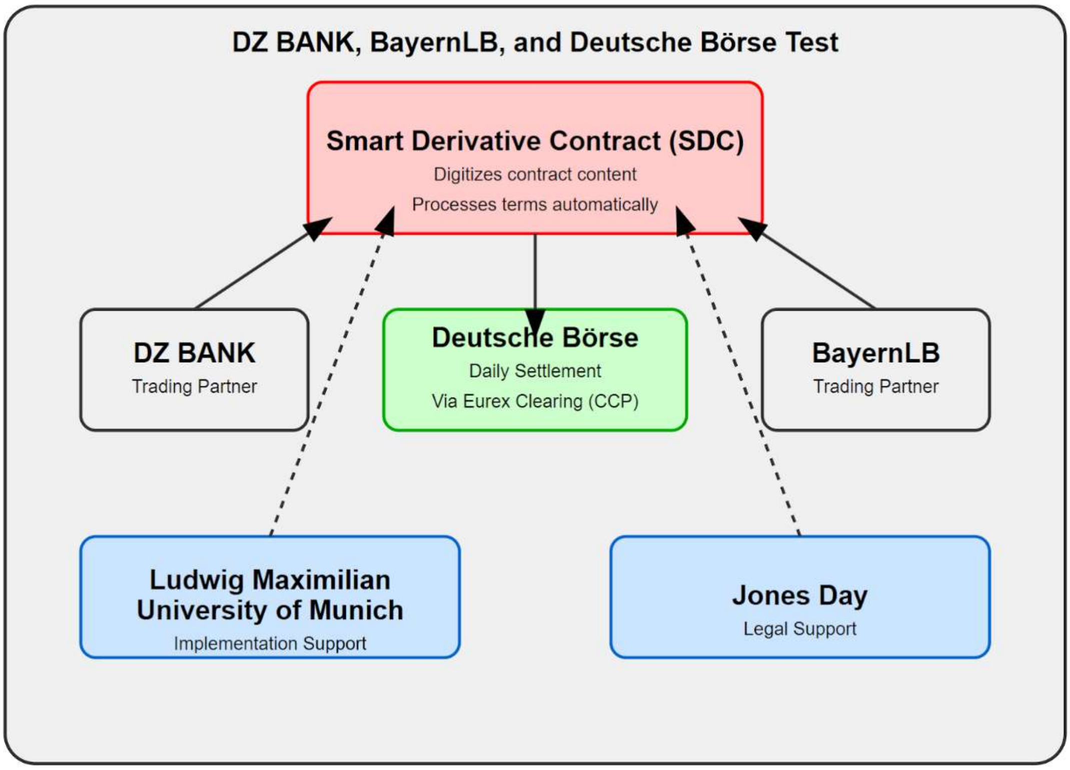


Figure 7 - DZ Bank and Bayern LB test.

[7] https://www.bayernlb.com/internet/en/blb/resp/bayernlb_2/news_273346.jsp

It is important to highlight that while Deutsche Börse and Eurex Clearing are involved, they do not act as central counterparties (CCP), taking on the trade risk. i.e., there is no novation. DZ BANK and BayernLB traded directly via the Smart Derivative Contract (SDC) as a bilateral OTC contract. Due to its economics this is an OTC derivative not subject to clearing.

This test showcased:

- Uniform valuation: Market value is calculated using a contractually agreed uniform model.
- Automated settlement: Outstanding receivables and liabilities are settled daily through automated booking (settled-to-market).
- Efficient payment processing: Daily pre-financing ensures smooth transactions.
- Risk mitigation: Automatic contract termination activates if partners fail to meet agreed terms.
- Transparent record-keeping: DLT is a digital accounting system for recording and verifying transaction data and automating exposure settlement.

Cost-Efficient Derivative Transactions for Non-Bank Entities

In 2022, DZ BANK and Union Investment successfully executed a legally binding over-the-counter (OTC) derivative as a smart derivative contract (SDC). Based on an interest rate swap, the transaction was settled automatically over several days using a settlement token and linked SEPA payments facilitated by DZ BANK's trigger solution "TrAP". This implementation, built on an EVM-based private permissioned blockchain and operated on interconnected cloud environments, allowed for transactions without a central entity, potentially reducing costs and risks[8].

Wholesale Central Bank Digital Currencies (wCBDCs)

The European Central Bank (ECB) has shown interest in exploring the potential of ERC-6123 in the context of its ongoing work on central bank digital currencies (CBDCs)[9]. In a document outlining potential use cases for its 2024 exploratory phase, the ECB mentioned the Smart Derivative Contract (SDC) concept, designed to reduce counterparty credit risk and frictions in OTC derivatives post-trade processing.

---

[8] https://www.dzbank.de/content/dzbank/en/home/we-are-dz-bank/press/news_archive/2023/new-digital-standarddzbankandunioninvestmenttradeotcderivativeas.html

[9] https://www.ecb.europa.eu/paym/groups/ntwcg/pdf/ecb.ntwdocs240125_business_cases_6th_ntwcg_meeting.en.pdf

The document suggests that an "SDC-Trade as Experiment" could be conducted involving a SDC-based OTC trade with another counterparty over a limited time period. This experiment would consider one of the provided CBDC solutions for settlement, and the open-source SDC code (ERC-6123) could be used.

This potential application of ERC-6123 in CBDC experiments highlights the growing interest from central banks and other stakeholders in utilizing digital standards to enhance the efficiency, transparency, and security of financial transactions in a digital currency environment.

DeFi Derivatives

The emergence of DeFi Yield Indices, capable of providing settlement rates for derivative contracts, has opened up new possibilities for on-chain financial instruments. By leveraging the ERC-6123 standard, new native on-chain financial instruments for OTC markets can be created.

Examples of such instruments could include native on-chain swaps with settlement terms based on a given DeFi yield index, allowing for transparent, reliable, and standardized financial contracts.

Reference Implementations

Reference implementations are available under the Finmath Smart Derivative Contract project, which offers open-source implementations in Java and Solidity for smart derivative contracts. It includes extensive documentation, schema definitions, demo code, and a valuation oracle. The project supports ERC-6123 and ERC-7573 protocols and provides a visualization tool, a valuation service via Docker, and interfaces for settlement amounts and valuation oracles. It uses the Finmath library for underlying valuation and follows Eclipse coding conventions. The code is distributed under the Apache License 2.0.

Please note that the code has not been audited and as such it is not recommended for usage in production.

For more details, visit Finmath Smart Derivative Contract: https://www.finmath.net/finmath-smart-derivative-contract/.

ERC-6123 Contemporaries

To develop a broad view of the landscape ERC-6123 occupies, it is important to acknowledge and explore other token standards that have emerged alongside ERC-6123, each aiming to address specific challenges and requirements associated with (though not always directly addressing) tokenized securities.

ERC-7586

ERC-7586 is a proposed interest rate swaps (IRS) standard on EVM-compatible networks. It aims to provide a standardized framework for on-chain IRS, enabling the seamless exchange of fixed and floating interest rate cash flows between parties. This standard is designed to facilitate DeFi applications and improve the efficiency of financial derivatives trading[10].

The ERC-7586 standard defines several key functions and events:

1. **Swap Event**: This event is triggered when interest rates are swapped between parties. It includes the interest difference to be transferred and the recipient account address.
2. **Terminate Swap Event**: This event is triggered when the contract is terminated. It includes the payer and receiver addresses.
3. **Payer Function**: This function returns the IRS payer account address, which is the party that agreed to pay the fixed interest rate.
4. **Receiver Function**: This function returns the IRS receiver account address, which is the party that agreed to pay the floating interest rate.
5. **Swap Rate Function**: This function returns the fixed interest rate, which is recommended to be expressed in basis points (1 basis point = 0.01%).
6. **Spread Function**: This function returns the floating rate spread, the fixed part of the floating interest rate, also expressed in basis points.
7. **Oracle Contract for Benchmark Function**: This function returns the contract address of the asset to be transferred when swapping IRS. This allows for the use of different oracles for different swap agreements.

[10] https://eips.ethereum.org/EIPS/eip-7586

8. **IsActive Function**: This function returns a boolean indicating whether the swap is active (not matured or not terminated).
9. **Agree to Swap Function**: This function gives agreement to swap IRS, which must be done before initiating the first swap.

The standard also includes a tokenization process for swap cash flows. Tokens are issued to both the buyer and the payer, and each time a swap happens, one token is burned from each counterparty wallet. This ensures that the total supply of tokens remains constant and that the swap cash flows are accurately tracked.

ERC-7586 is designed to provide a robust foundation for decentralized finance applications, enabling the creation of complex financial instruments and improving the efficiency of trading and settlement processes.

ERC-3643

ERC-3643 is a standard for security tokens on the Ethereum blockchain and EVM-compatible networks. It provides a framework for issuing, transferring, and managing security tokens while ensuring compliance with regulatory requirements.

ERC-3643 emphasizes compliance through embedded transfer rules in tokens and rigorous identity verification using ERC-734 and ERC-735 standards and via identity solutions such as ONCHAINID (ONCHAINID is an open-source, decentralized identity system for compliant digital assets).

For a comprehensive review of the ERC-3643 standard, refer to the report "Demystifying ERC-3643: A Deep Dive Into Compliant RWA Tokenization" published in March 2024 and accessible here: https://www.qualitax.io/erc3643.

ERC-1400

ERC-1400 was created to address the lack of standardization in creating, issuing and managing security tokens on Ethereum and EVM-compatible networks. It has evolved into an umbrella for ERC-1410 (Partially Fungible Token Standard), ERC-1594 (Core Security Token Standard), ERC-1643 (Document Management Standard), and ERC-1644 (Controller Token Operation Standard) to improve adoption by decomposing the security token standard into a library of related and interoperable standards, making the implementation more flexible and adaptable to different use cases.

For a comprehensive review of the ERC-1400 standard, refer to the report "Deep Dive into ERC-1400: Enabling Secure and Compliant Digital Securities," published in May 2024 and accessible here: https://www.qualitax.io/erc1400.

ERC-1155

ERC-1155 is a token standard in the EVM-based ecosystem that allows for creating fungible and non-fungible tokens within a single smart contract. It is a multi-token standard that combines the functionality of previous standards like ERC-20 and ERC-721.

ERC-1155 enables the efficient transfer of fungible and non-fungible tokens within a single contract, thus reducing the transaction costs and the complexity of deploying and managing multiple contracts for each new token the system needs. Its unique features include support for infinite tokens, semi-fungible tokens, safe transfer functions, batch transfer and approvals, and metadata storage capabilities.

CMTAT

The Capital Markets and Technology Association (CMTA) standard token for securities (CMTAT) is a digital token framework that enables the creation of "ledger-based securities" in compliance with Swiss law[11]. CMTAT is designed to enhance regulatory compliance within the Ethereum ecosystem by building on the ERC-20 standard and introducing mechanisms for identity verification, anti-money laundering (AML) protocols, and Know Your Customer (KYC) compliance directly within the token transfer framework. The standard is licensed under the permissive Mozilla Public License 2.0 (MPL 2.0).

CMTAT aims to streamline the compliance process for tokenized assets, making it an essential tool for issuers and investors dealing with securities, real estate, and other regulated financial products.

This standard is particularly significant for projects seeking to navigate the complex regulatory landscape of tokenized assets, providing a clear pathway for compliance with local and international regulations.

[11] https://cmta.ch/content/15de282276334fc837b9687a13726ab9/cmtat-functional-specifications-jan-2022-final.pdf

ERC-6123 Technical Breakdown

The ERC-6123 standard is implemented as a set of smart contract methods and events defining the parties' interactions in a derivative contract. The key components include:

- **Counterparties:** The parties engaging in the derivative contract
- **Smart Derivative Contract (SDC):** The on-chain contract implementing the ERC-6123 interface
- **Settlement Token:** An ERC-20 compatible token used for transferring value between parties. Multiple transfers can be batched.
- **Event Handler:** An off-chain system that listens for emitted events to trigger actions
- **Valuation Service:** An off-chain system for providing market data for settlement calculations

Key Methods

- inceptTrade(address,string,int,int256,string): Allows a party to initiate a trade by specifying the counterparty (address), trade data (string), position (int), payment amount (int256), and initial settlement data (string)
- confirmTrade(address,string,int,int256,string): Allows the other (non-incepting) counterparty to confirm the trade with their corresponding parameters, activating the contract if parameters match
- cancelTrade(address,string,int,int256,string): Allows the incepting counterparty to confirm the trade with their corresponding parameters, activating the contract if parameters match
- initiateSettlement(): Allows eligible participants to trigger a settlement process
- performSettlement(int256,string): Callback from an oracle service with the settlement amount (int256) and settlement data (string)
- afterTransfer(uint256,bool): Callback to complete the settlement transfer, moving to the next phase or termination based on success, called with a transaction hash (uint256) and a boolean indicating success (bool)
- requestTradeTermination(string, int256, string): Allows a party to request a termination with given trade id (string), termination amount (int256), termination terms (string)

- confirmTradeTermination(string,int256, string): Allows the other party to confirm the termination of the specific contract
- cancelTradeTermination(string,int256, string): Allows the requesting party to cancel its trade termination request

Trade and Settlement Events

An implementation for the interface may allow to incept/confirm multiple trades, then perform a common and netted settlement of these trades. Hence, the standard distinguishes between trade related events and settlement related events.

Trade Events

- TradeIncepted: Emitted when a trade is incepted. Will generated a unique trade id.
- TradeConfirmed: Emitted when a trade inception has been confirmed.
- TradeCanceled: Emitted when a trade inception has been canceled.
- TradeActivated: Emitted when a trade has been activated.
- TradeTerminated: Emitted when a trade inception has been terminated.
- TradeTerminationRequest: Emitted when a trade termination has been requested.
- TradeTerminationConfirmed: Emitted when a trade termination has been confirmed.
- TradeTerminationCanceled: Emitted when a trade termination has been canceled.

Settlement Events

- SettlementRequested: Emitted when a settlement is requested.
- SettlementEvaluated: Emitted when the settlement value has been determined/received.
- SettlementTransferred: Emitted when the settlement transfer is completed successfully.
- SettlementFailed: Emitted when the settlement failed.

QX

State Machine Implementation for a Single Trade

The SDC reference implementation SDCSingleTrade.sol considers the special case of an SDC for a single trade (i.e., there is only one incept/confirm per SDC instance). Nevertheless, in this case, the “trade” can also be a portfolio of trades. The implementation is based on a state machine pattern, where the contract's state transitions are clearly defined and controlled. The states also serve as guards (via modifiers) to restrict which functions can be called at each stage of the contract's lifecycle.

The main states in the SDCSingleTrade lifecycle are:

- Incepted: One counterparty has initiated the trade and awaits confirmation from the other.
- Confirmed: Both counterparties have agreed to the trade terms, and the trade is ready to proceed.
- Valuation: The contract is awaiting valuation data from an external oracle to calculate settlement amounts.
- InTransfer: The contract is in the process of transferring margin buffers or settlement amounts between parties.
- Settled: The settlement process for the current cycle has been completed successfully.
- Terminated: The trade has been terminated through mutual agreement or due to a failure condition.

The state machine approach provides several benefits:

- **Clarity:** The contract's behavior is clearly defined for each state, making the code easier to understand and audit.
- **Security:** State transition rules prevent unauthorized or unexpected actions from being taken at the wrong time.
- **Modularity:** The state machine logic is separated from other contract functionality, making it easier to update or replace if needed.

By leveraging the state machine pattern, the SDC implementation ensures that the contract behaves predictably and securely throughout its lifecycle, from trade inception to termination.

For full technical details, refer to the ERC-6123 specification and the reference implementation code[12].

[12] https://github.com/ethereum/ERCs/blob/master/assets/erc-6123/contracts/SDCSingleTrade.sol

Rationale for ERC-6123 Design Patterns

The ERC-6123 standard incorporates several key design patterns and best practices to ensure that derivative contracts built on the standard are secure, efficient, and modular. Let's explore some of these design choices in more detail.

Callback Pattern for External Interactions

The ERC-6123 standard uses a callback pattern for interacting with external components such as off-chain valuation services. This allows the contract to request data from these services without blocking execution or relying on a specific implementation. It is important to note that this approach is particularly useful for complex financial instruments like interest rate derivatives, whose valuation methodologies often cannot be brought entirely "on-chain" due to their complexity. The initiateSettlement and performSettlement functions demonstrate this pattern, with performSettlement serving as the callback that receives the settlement amount and data from the valuation service. This approach provides flexibility and modularity, as the valuation service can be changed or updated without modifying the core contract code. Additionally, for more native settlement values on-chain, oracles could also be used when appropriate.

Separation of Token Logic

The ERC-6123 standard separates the settlement token logic from the core derivative contract. This allows for greater flexibility and reusability, as different settlement tokens can be used with the same derivative contract. The settlement token is assumed to be ERC-20 compatible, allowing for seamless integration with existing token standards and wallets.

Finite State Machine

As mentioned, the SDC reference implementation utilizes a finite state machine pattern to manage the contract's lifecycle and enforce strict transition rules between states. This pattern helps to ensure the contract behaves predictably and securely, preventing unauthorized or unexpected actions from being taken at the wrong stage of the lifecycle.

By incorporating these design patterns, the ERC-6123 standard aims to provide a robust and flexible framework for building decentralized derivative contracts on EVM-compatible networks. The standard's modular architecture, callback-based interactions, and state machine approach contribute to its security, efficiency, and extensibility.

Implementation Sequence

Deploying and interacting with an ERC-6123 derivative contract involves the following high-level steps:

1. The counterparties allocate balances of the settlement token and approve the SDC to transfer tokens on their behalf.
2. One counterparty initiates the trade by calling inceptTrade and providing the trade parameters and initial settlement data. The SDC collects the initial valuation from an off-chain service via a callback.
3. The other counterparty confirms the trade by calling confirmTrade with matching parameters. This moves the contract to the Confirmed state.
4. The SDC transfers margin buffers and any upfront fees from the parties, moving the trade to the Active state.
5. At each settlement cycle, a settlement is initiated via initiateSettlement, and the valuation service provides the settlement amount by invoking the performSettlement callback. The SDC transfers the settlement amount and moves to the next cycle if successful or to Terminated if the transfer fails.
6. If either party requests a termination using requestTradeTermination and the counterparty confirms with confirmTradeTermination, the SDC moves to the Terminated state and returns any remaining balances.

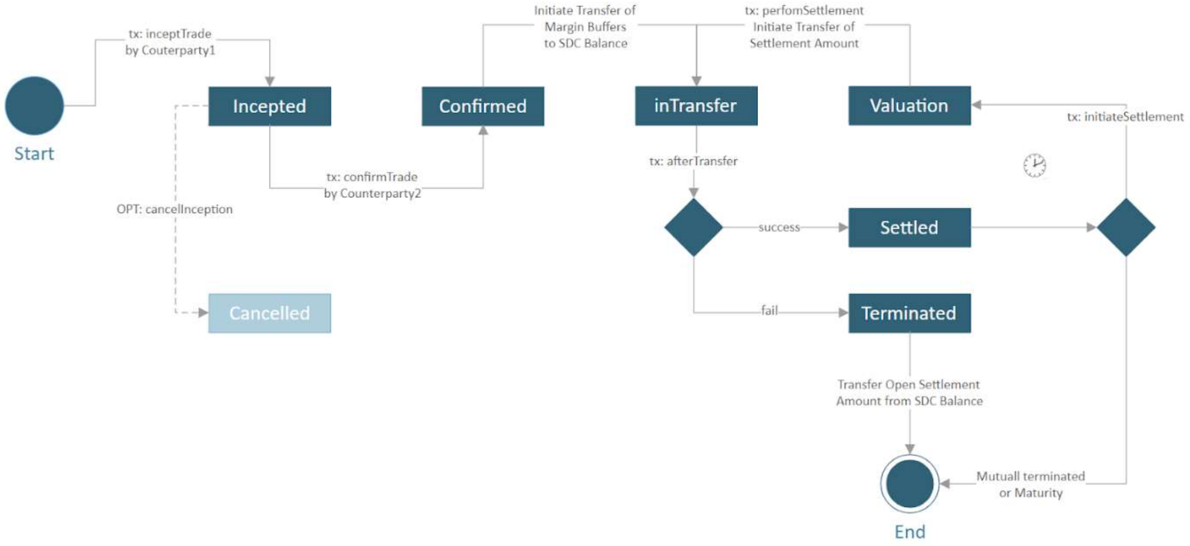


Figure 8: ERC-6123 State diagram of trade and process states
Source: https://eips.ethereum.org/EIPS/eip-6123

This sequence demonstrates how the various components of the ERC-6123 ecosystem, including the SDC, settlement token, and off-chain valuation service, interact to facilitate the decentralized creation, management, and settlement of derivative contracts.

The next section will cover the entire trade initiation and settlement lifecycle of an SDC. While some parts are redundant with what we've already covered, repeating all of the steps in a complete sequence will help with comprehension.

ERC-6123 Trade Initiation and Settlement Lifecycle

An ERC-6123 derivative contract progresses through the following interaction sequence:

1. **Setup:**
    - The counterparties (CP1 and CP2) allocate balances of the settlement token (ERC-20 token).
    - They approve the SDC transferring tokens on their behalf by calling to approve on the token contract.
2. **Trade Initiation:**
    - One counterparty (CP1) initiates the trade by calling inceptTrade on the SDC, providing the trade parameters, their position, payment amount, and initial settlement data.
    - The SDC emits the TradeIncepted event.
    - The SDC requests initial valuation data from the off-chain (or on-chain) ValuationService.
    - The SDC receives the valuation data through a call to performSettlement and stores the initial valuation, moving the trade to the Incepted state.

3. **Trade Confirmation:**
    - The other counterparty (CP2) confirms the trade by calling confirmTrade with matching parameters.
    - The SDC validates the trade data and emits the TradeConfirmed event.
    - The trade moves to the Confirmed state.

4. **Funding:**
    - The SDC transfers margin buffers and termination fees from CP1 and CP2 to its own balance.
    - If applicable, the SDC transfers any upfront fees from the paying party to the receiving party.
    - The trade moves to the InTransfer state during these transfers.
    - Once the transfers are complete, afterTransfer is called to move the trade to the Settled state.

5. **Settlement Cycle** (repeated for each settlement period):
    - An authorized party calls initiateSettlement to start the settlement process, moving the trade to the Valuation state.
    - The SDC emits the SettlementRequested event.
    - The ValuationService is requested to provide the current valuation data.
    - The ValuationService invokes the performSettlement callback with the settlement amount and data. The trade emits the SettlementEvaluated event.
    - The SDC caps the settlement amount at the margin buffer level and transfers the amount from the paying party to the receiving party's balance and moves to the InTransfer state during the transfer.
    - If afterTransfer is called, the SDC will check the transfer status:
        - If successful, the trade returns to the Settled state, ready for the next settlement cycle.
        - If failed, the SDC transfers the settlement amount and termination fee from its own balance to the receiving

party, unlocks the remaining balances, and moves the trade to the Terminated state.

6. Trade Termination:

- Either counterparty can request trade termination by calling requestTradeTermination, providing the termination amount and further termination terms.
- The SDC emits the TradeTerminationRequest event.
- The other counterparty confirms the termination by calling confirmTradeTermination.
- The SDC emits the TradeTerminationConfirmed event and transfers the termination amount and remaining balances as per the termination terms.
- The trade moves to the Terminated state, and the SDC emits the TradeTerminated event.

The sequence diagram below portrays the lifecycle of an ERC-6123 derivative contract, from setup and initiation to settlement cycles and termination.

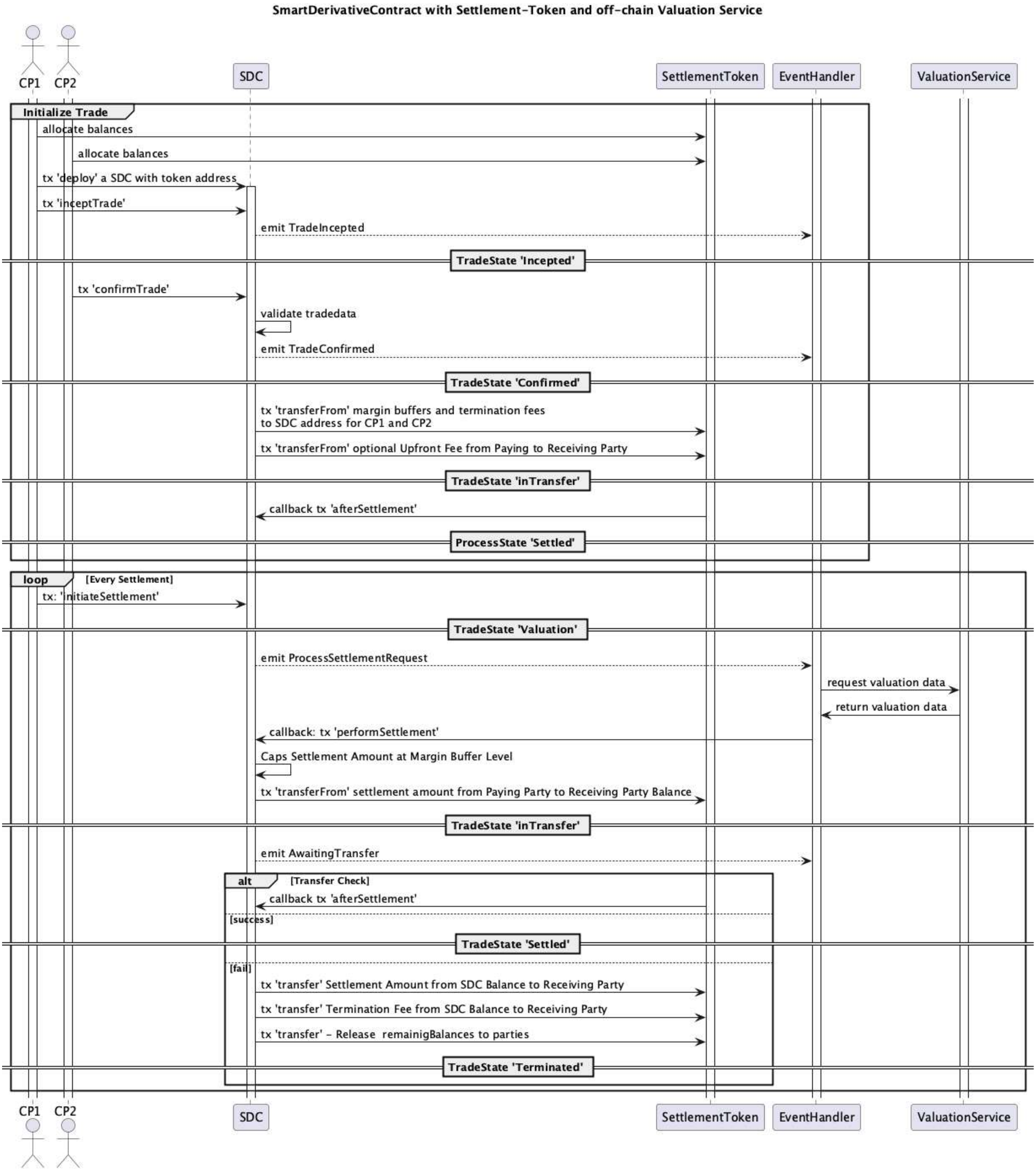


Figure 9: Sequence diagram of reference implementation 'SDCPledgedBalance.sol'. Source: https://eips.ethereum.org/EIPS/eip-6123

Comparing Traditional vs. ERC-6123 Non-Cleared Interbank OTC Derivatives

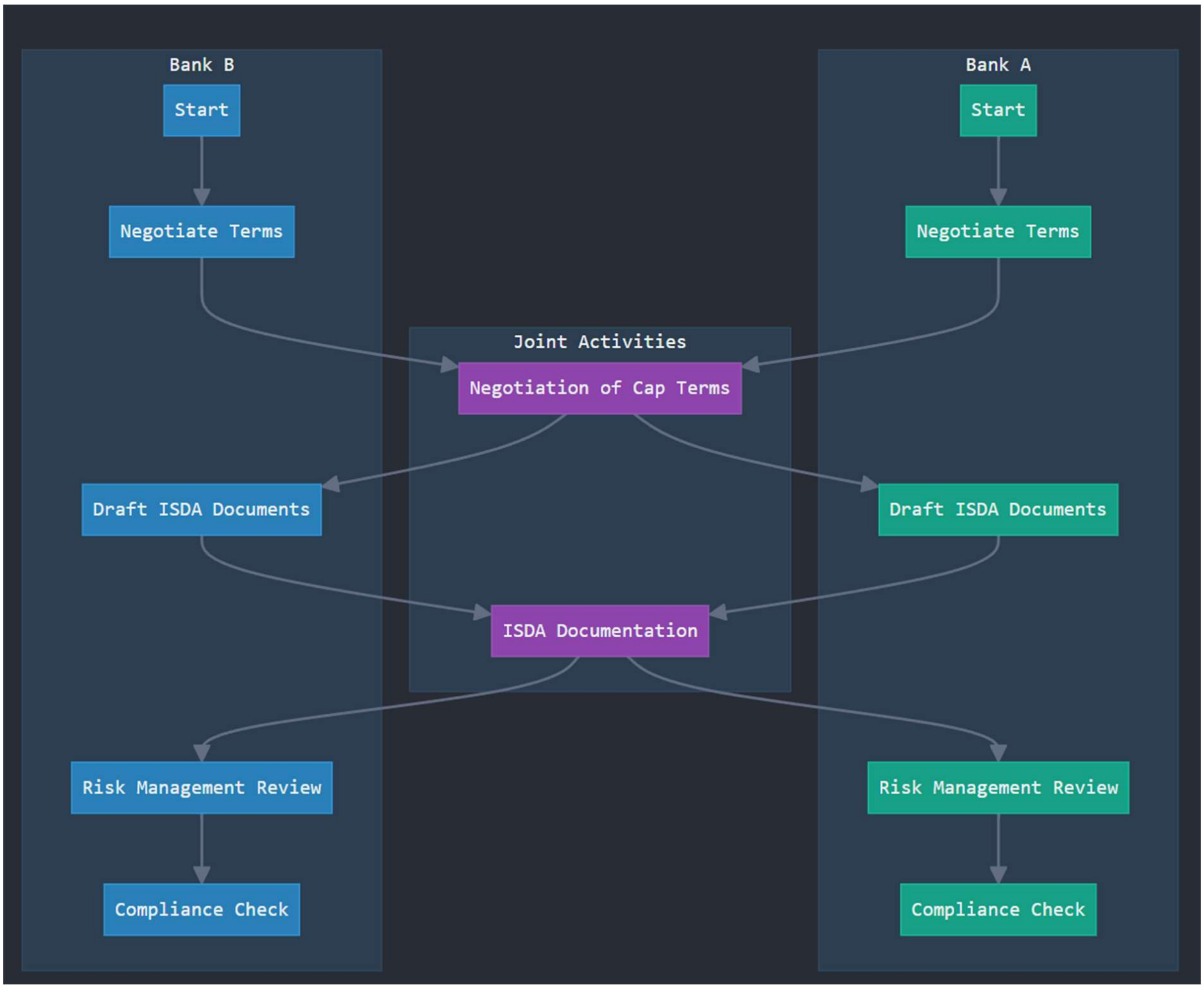
To understand the differences between traditional and ERC-6123 processes, we will examine the steps involved in executing a non-cleared interbank OTC interest rate cap trade between two counterparties. This comparison will highlight how ERC-6123 can enhance efficiency, reduce risks, and automate various aspects of the trade lifecycle.

'As-Is' Non-cleared interbank OTC interest rate cap trade

An interest rate cap is a financial derivative that sets a maximum limit (strike) to protect against rising interest rates (the underlying money market rate). Settlements occur with the frequency of the money market rate (e.g. quarter-annually for the 3-month LIBOR). A cap with a maturity of 3 years would thus have 12 settlements.

The traditional process for a non-cleared interbank OTC interest rate cap trade involves multiple manual steps, including negotiation, documentation, margin posting, regular settlements, and compliance with regulatory requirements. Each step requires coordination between different departments within each bank, such as trading desks, risk management, compliance, and treasury. The process is often time-consuming and resource-intensive due to the reliance on manual processes and the need for continuous monitoring and margin management.

1. **Initial Setup**



1.1 **Agreement and Documentation:**

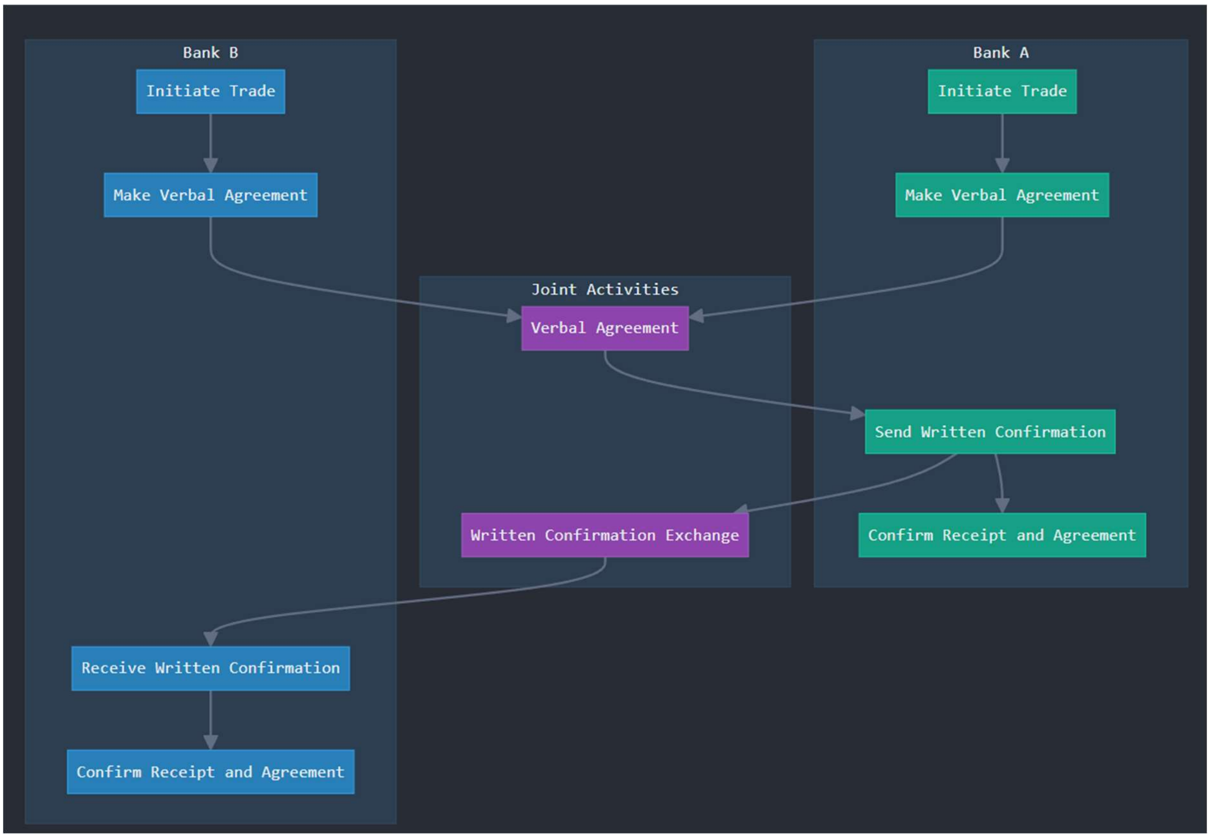
- **Negotiation:** The two counterparties, typically Bank A and Bank B, negotiate the terms of the interest rate cap, including the notional amount, cap rate strike, maturity date, premium, and settlement terms.
- **Legal Agreement:** They draft and sign an International Swaps and Derivatives Association (ISDA) Master Agreement, a Schedule, and a Confirmation outlining the specific interest rate cap trade terms.

1.2 **Internal Approvals:**

- **Risk Management:** Each bank's risk management team reviews the trade terms to ensure they align with its risk policies and the counterparty risk limits.

- **Compliance Check:** Both banks conduct compliance checks to ensure the trade meets relevant regulations.

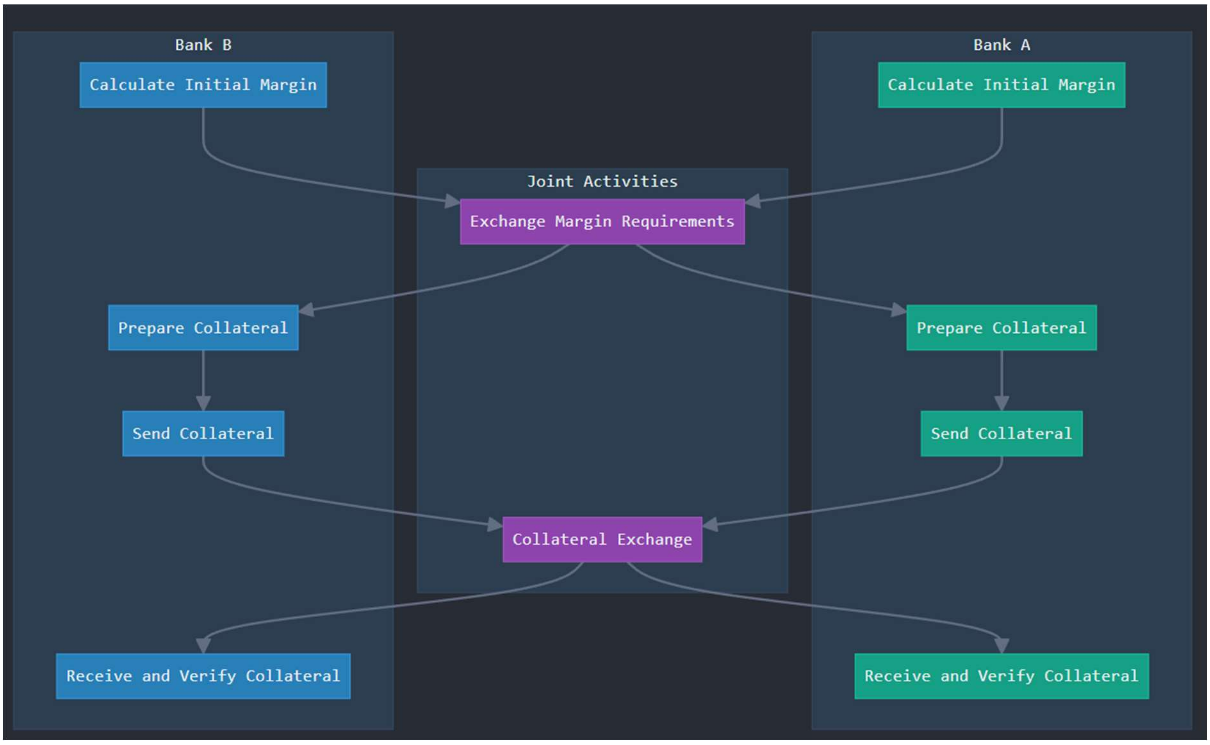
2. **Trade Execution**



2.1 **Trade Confirmation:**

- **Verbal Agreement:** Initially, the trading desks of Bank A and Bank B made a verbal agreement.
- **Written Confirmation:** This is followed by a written confirmation sent via email or an electronic trading platform, which includes all the trade details. Both parties confirm receipt and agreement of the terms.

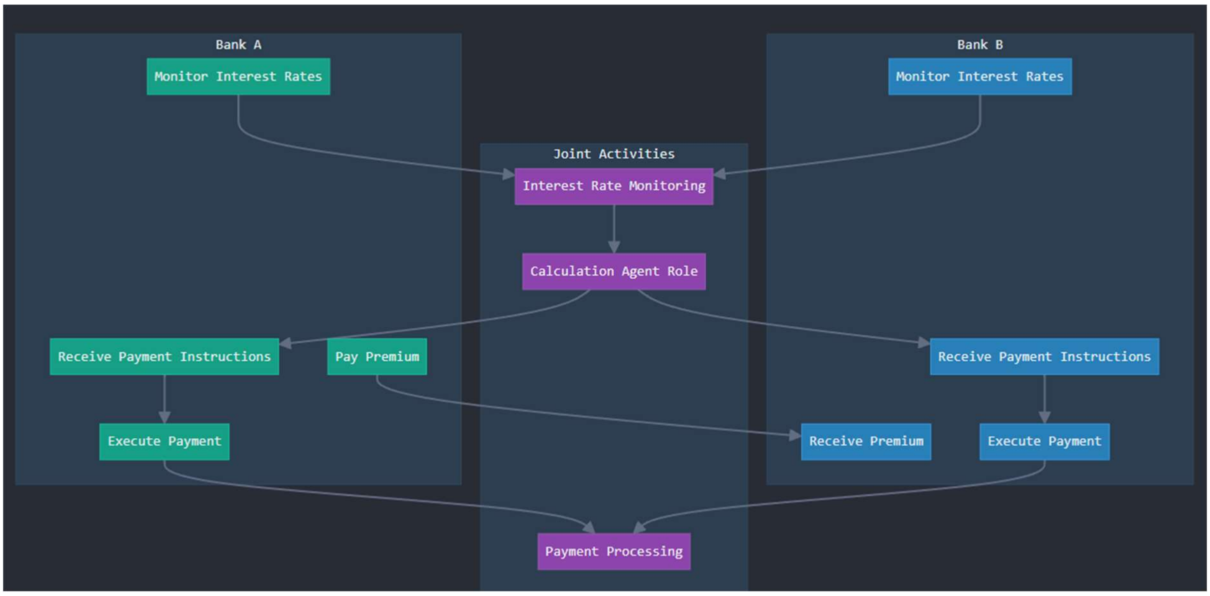
3. **Funding and Margin Posting**



3.1 **Initial Margin Posting:**

- **Margin Requirements:** Both banks calculate the initial margin required based on the trade terms and each bank's internal risk models.
- **Collateral Exchange:** The required margin is exchanged, often using cash or high-quality securities, and held in a segregated account. This is typically managed by the banks' treasury or collateral management departments.

4. Lifecycle Management



4.1 **Regular Payments and Settlements:**

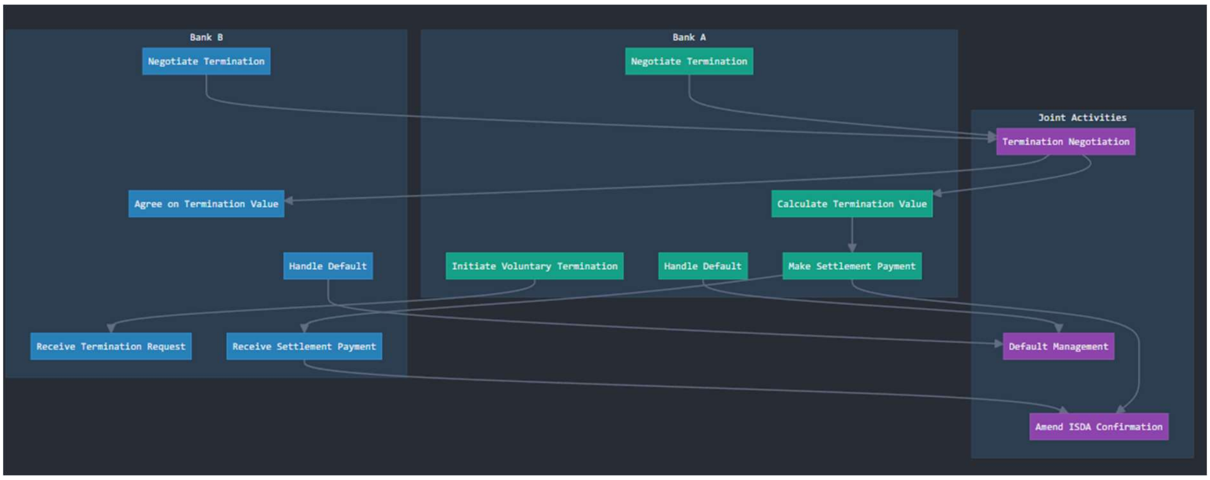
- **Premium Payment:** The buyer of the cap (the bank seeking protection) pays a premium to the seller (the bank providing the cap) upfront or periodically.
- **Interest Rate Monitoring:** The banks continuously monitor the relevant interest rates (e.g., LIBOR, SOFR) to determine if the cap rate strike is exceeded.

4.2 **Settlement of Payments:**

- **Calculation Agent Role:** If the reference rate exceeds the cap rate, a designated calculation agent (either one of the banks or a third party) calculates the settlement amounts.
- **Payment Instructions:** Based on these calculations, payment instructions are sent to the treasury departments of both banks.
- **Funds Transfer:** Payments are made through standard interbank payment systems such as SWIFT or Fedwire, typically monthly or quarterly.

QX

5. Trade Termination



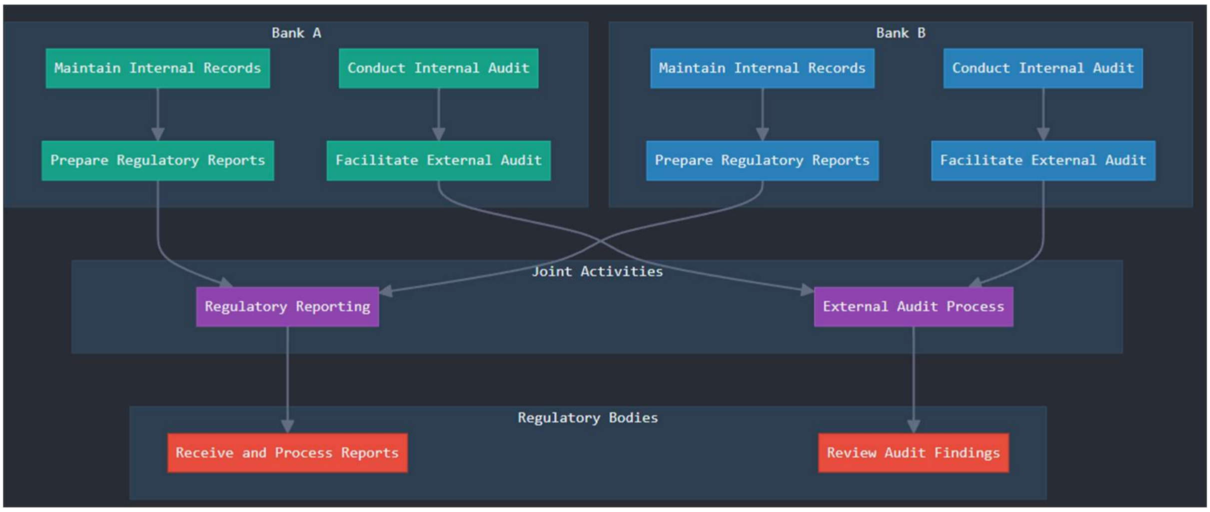
5.1 **Voluntary Termination:**

- **Negotiation:** If either bank wishes to terminate the trade early, they negotiate an early termination agreement, which includes calculating the termination value.
- **Settlement Payment:** The terminating party makes a settlement payment to compensate for the early termination, and the ISDA Confirmation is amended accordingly.

5.2 **Automatic Termination:**

- **Default Management:** If one party defaults (e.g., fails to make a margin call), the non-defaulting party follows the procedures outlined in the ISDA Master Agreement, which may include terminating the trade and calculating the close-out amount.

6. **Post-Trade Reporting and Audit**



6.1 **Record-Keeping:**

- **Internal Records:** Both banks maintain detailed internal trade records, including all confirmations, margin calls, payments, and settlements.
- **Regulatory Reporting:** The banks report the trade details to relevant regulatory bodies, such as the US Commodity Futures Trading Commission (CFTC) or the European Securities and Markets Authority (ESMA) in the EU.

6.2 **Audits and Reviews:**

- **Internal Audits:** Internal audit teams periodically review the trade records to ensure compliance with internal policies and regulatory requirements.
- **External Audits:** External auditors may also review the trade documentation and processes as part of their annual audits.

‘To-Be’ Non-cleared interbank OTC interest rate cap trade

1. **Initial Setup**

1.1 **Agreement and Documentation:**

- **Negotiation:** The two counterparties, Bank A and Bank B, negotiate the terms of the interest rate cap, including the notional amount, cap rate, maturity date, premium, and settlement terms. They also agree on the valuation model.
- **Legal Agreement:** They draft and sign a legal agreement outlining the terms and conditions of the trade. The valuation model is part of the contractual agreement.

1.2 **Smart Contract Deployment:**

- **ERC-6123 Smart Derivative Contract (SDC):** Deploy an instance of the ERC-6123 compliant smart derivative contract on an EVM-compatible blockchain.
- **Settlement Token:** Both parties agree on an ERC-20 compatible settlement token to transfer value between them.

2. **Trade Inception**

2.1 **Contract Inception:**

- **Initiation by Bank A:** Bank A calls the inceptTrade method on the ERC-6123 SDC, providing the trade parameters (counterparty address, trade data, position, payment amount, and initial settlement data).
- **Initial Valuation:** The SDC requests initial valuation data from an off-chain valuation service and stores it upon callback, emitting the TradeIncepted event.

2.2 **Trade Confirmation:**

- **Confirmation by Bank B:** Bank B reviews the trade details and confirms the trade by calling the confirmTrade method, which provides matching parameters.
- **Activation:** The SDC validates the data, emits the TradeConfirmed event, and transitions to the Confirmed state.

3. **Funding and Margin Posting**

3.1 **Initial Funding:**

- **Margin Requirements:** The SDC calculates initial margin requirements based on the agreed terms.
- **Transfer of Funds:** Both banks transfer the required margin amounts to the SDC's balance by approving the SDC to transfer tokens on their behalf.
- **State Transition:** The contract moves to the InTransfer state during these transfers.

3.2 **Confirmation of Funding:**

- **Verification:** The SDC verifies the receipt of funds and calls the afterSettlement method to transition the trade to the Settled state.

4. **Lifecycle Management**

4.1 **Regular Settlements:**

- **Settlement Initiation:** At each settlement period (e.g., monthly), an authorized party (either Bank A or B) calls initiateSettlement to start the process.
- **Valuation Callback:** The off-chain valuation service provides current market data, invoking the performSettlement callback with settlement amounts.
- **Fund Transfer:** The SDC transfers the required settlement amounts between the parties, ensuring the cap rate is respected if the market rate exceeds it.
- **State Update:** The contract transitions back to the Settled state if successful or to Terminated if the transfer fails.

4.2 **Interest Rate Monitoring:**

- **Interest Rate Cap Activation:** If the floating rate exceeds the cap rate, the SDC ensures payments are adjusted to reflect the cap, automatically calculating and transferring any difference above the cap rate to the protected party.

5. **Trade Termination**

5.1 **Voluntary Termination:**

- **Request Termination:** Either bank can request to terminate the trade by calling requestTradeTermination with the termination amount and terms.
- **Confirmation:** The other bank confirms the termination by calling confirmTradeTermination.
- **Final Settlement:** The SDC transfers any remaining balances and emits the TradeTerminated event.

5.2 **Automatic Termination:**

- **Insufficient Funds:** If a party fails to meet margin requirements or settlement obligations, the SDC can automatically terminate the contract.
- **Penalty Enforcement:** The contract ensures the automatic transfer of termination fees from the defaulting party to the other party.

6. **Post-Trade Reporting and Audit**

6.1 **Record-Keeping:**

- **Blockchain Ledger:** All transactions and state changes are recorded on the blockchain, ensuring an immutable audit trail.
- **Event Monitoring:** Off-chain systems monitor emitted events to maintain synchronized records.

6.2 **Regulatory Compliance:**

- **Reporting:** Both banks ensure compliance with regulatory reporting requirements by leveraging blockchain records' transparent and verifiable nature.
- **Audits:** Regular audits are facilitated by the clear and immutable record of all trade-related activities on the blockchain.

Summary of key differences

Figure 11 - OTC Derivatives Process Comparison

PROCESS STAGE	PROCESS STEP	As-Is	To-Be (using ERC-6123)	Key Benefits/Improvements
INITIAL SETUP	AGREEMENT AND DOCUMENTATION	Negotiation and signing of ISDA Master Agreement, Schedule, and Confirmation	Negotiation and signing of ISDA Master Agreement, Schedule, Valuation model part of the OTC contract, agreement on settlement token. Deployment of ERC-6123 smart contract.	Streamlined agreement process, Automated contract terms and deployment, reducing setup time
	INTERNAL APPROVALS	Risk management and compliance reviews	Compliance reviews and initial configuration of smart contract parameters.	Faster and streamlined approval process with predefined parameters
TRADE EXECUTION	TRADE CONFIRMATION	Verbal agreement followed by written confirmation via email or electronic platform	Bank A calls inceptTrade and Bank B calls confirmTrade on SDC	Reduced risk of miscommunication and discrepancies between counterparties, Automated confirmation process*, Instant and immutable trade confirmation
FUNDING AND MARGIN POSTING	INITIAL MARGIN POSTING	Exchange of initial margin through cash or securities	Transfer of margin amounts using ERC-20 tokens to SDC	Increased efficiency and speed of margin transfers, Reduced counter party risk and operational risk
LIFECYCLE MANAGEMENT	REGULAR PAYMENTS AND SETTLEMENTS	Premium payment upfront or periodically, monitoring interest rates	Automated settlement via smart contract based on predefined conditions	Automated, consistent and timely settlements, Reduced manual monitoring, Increased accuracy in calculations
	SETTLEMENT OF PAYMENTS	Calculation by designated agent, payment via SWIFT or Fedwire	Automatic calculation and transfer by smart contract using blockchain	Reduced calculation errors, Instant settlements, Reduced settlement risk, Faster settlement process, Elimination of intermediaries
TRADE TERMINATION	VOLUNTARY TERMINATION	Negotiation of early termination, settlement payment, amendment of ISDA Confirmation	Request and confirm termination via smart contract methods	Simplified termination process, Reduced negotiation time, Reduced disputes in termination values
	AUTOMATIC TERMINATION	Procedures outlined in ISDA Master Agreement in case of default	Automatic termination by smart contract if margin requirements not met	Immediate response to default, Reduced credit and counterparty risks, Elimination of manual intervention in defaults
POST-TRADE REPORTING AND AUDIT	RECORD-KEEPING	Detailed internal records, regulatory reporting	Integration of blockchain originating data in regulatory reporting tool (immutable records on blockchain, transparent and real-time reporting).	Enhanced transparency, Reduced risk of record discrepancies, Real-time accessibility of trade data
	AUDITS AND REVIEWS	Internal and external audits	Real-time monitoring and automated reporting leveraging blockchain technology	Continuous real-time auditing capabilities, Increased transparency for regulators, Reduced cost and time for audit processes

Impact on Pricing and Regulatory Capital Charges

- **Credit Valuation Adjustment (CVA):**
  - **Traditional Approach:** In traditional OTC derivatives, CVA is used to adjust the pricing of a derivative to account for the counterparty credit risk. This adjustment increases the cost of the derivative to compensate for the potential risk of default.
  - **With ERC-6123:** ERC-6123 significantly reduces counterparty credit risk through its automated and pre-funded mechanisms, so the need for a substantial CVA is diminished. This can result in more favorable pricing for both counterparties.
- **Regulatory Capital Charges:**
  - **Traditional Approach:** Financial institutions are required to hold regulatory capital to cover potential counterparty credit risk exposures. This capital is often calculated based on the potential future exposure (PFE) and other risk metrics.
  - **With ERC-6123:** The reduced counterparty credit risk achieved through ERC-6123's pre-funding and settle-to-market mechanisms that automated risk management and that can lead to lower PFE. Consequently, institutions may be able to reduce the amount of regulatory capital they are required to hold, freeing up capital for other uses and potentially improving their overall financial efficiency.

The ERC-6123 specification offers a technical framework for Smart Derivative Contracts, focusing on the automation OTC derivatives lifecycle through blockchain technology. However, developing a compliant implementation in practice necessitates a thorough examination of the regulatory landscape. This is particularly important when considering the use of tokenized assets for prefunding transactions. Implementers must ensure that their use of blockchain and tokenized assets aligns with regulations, which may vary significantly across different jurisdictions. This includes understanding legal recognition, compliance requirements, and the implications of using digital assets as a means of securing or settling transactions.

QX

Literature and References

1. Ethereum.org. (n.d.). EIP-6123: Smart derivative contract. Retrieved from https://eips.ethereum.org/EIPS/eip-6123
2. Singh, M., & Aitken, J. (2020). Counterparty credit risk and the credit default swap market. Journal of Financial Regulation, 6(2), 159-180. https://doi.org/10.1093/jfr/fjaa006
3. Futures Industry Association. (2024). ETD volume - April 2024. Retrieved from https://www.fia.org/fia/articles/etd-volume-april-2024
4. Bank for International Settlements. (2024, May). OTC derivatives statistics at end-December 2023. Retrieved from https://www.bis.org/publ/otc_hy2405.htm
5. International Swaps and Derivatives Association. (2020, October). The importance of non-cleared OTC derivatives. Retrieved from https://www.isda.org/a/gPDDE/non-cleared-otc-derivatives-paper.pdf
6. International Swaps and Derivatives Association. (2023, July). ISDA survey on OTC derivatives in emerging and developing markets. Retrieved from https://www.isda.org/a/qfogE/ISDA-Survey-on-OTC-Derivatives-in-Emerging-and-Developing-Markets.pdf
7. BayernLB. (2021, September 29). DZ BANK and BayernLB trade OTC derivative as a smart derivative contract for the first time. Retrieved from https://www.bayernlb.com/internet/en/blb/resp/bayernlb_2/news_273346.jsp
8. DZ BANK. (2023). New digital standard: DZ BANK and Union Investment trade OTC derivative as a smart derivative contract. Retrieved from https://www.dzbank.de/content/dzbank/en/home/we-are-dz-bank/press/news_archive/2023/new-digital-standarddzbankandunioninvestmenttradeotcderivativeas.html
9. European Central Bank. (2024, January 25). Business cases for the 6th NTWCG meeting. Retrieved from https://www.ecb.europa.eu/paym/groups/ntwcg/pdf/ecb.ntwdocs240125_business_cases_6th_ntwcg_meeting.en.pdf

10. Ethereum.org. (n.d.). EIP-7586: Interest rate swaps standard. Retrieved from https://eips.ethereum.org/EIPS/eip-7586

11. Capital Markets and Technology Association. (2022, January). CMTAT functional specifications. Retrieved from https://cmta.ch/content/15de282276334fc837b9687a13726ab9/cmtat-functional-specifications-jan-2022-final.pdf

12. Fries, C., & Kohl-Landgraf, P, & Korpis, A. SDCSingleTrade.sol. GitHub. Retrieved from https://github.com/ethereum/ERCs/blob/master/assets/erc-6123/contracts/SDCSingleTrade.sol

13. Fries, C., & Kohl-Landgraf, P. (2018, April 15). Smart Derivative Contracts (Detaching Transactions from Counterparty Credit Risk: Specification, Parametrisation, Valuation). SSRN. http://dx.doi.org/10.2139/ssrn.3163074

14. PwC. (2022, December 19). PwC Global Crypto Regulation Report 2023. https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf

15. Fries, C., & Kohl-Landgraf, P. (2020, August 3). Smart derivative contracts: detaching transactions from counterparty credit risk. Risk.net. https://www.risk.net/cutting-edge/banking/7487946/smart-derivative-contracts-detaching-transactions-from-counterparty-credit-risk

16. Outsmarting counterparty risk with smart contracts. (2020, August 3). Risk.net. https://www.risk.net/cutting-edge/views/7494071/outsmarting-counterparty-risk-with-smart-contracts

17. PwC (2023, October 25) . Funding cost reduction through derivative life cycle automation and risk limitation – Can smart derivative contracts be the game changer? https://blogs.pwc.de/de/risk/article/240055/transforming-finance-a-deep-dive-into-smart-derivatives-whitepaper/

MEDIA CREDITS

Frontpage:

Photo by Danijel Durkovic on Unsplash

Source: https://unsplash.com/photos/high-rise-building-m7pEg9F17iE

Description: High-rise building.

Page 12:

Photo by Paulina Milde-Jachowska on Unsplash

Source: https://unsplash.com/photos/a-tall-building-with-many-windows-_-b88sATOe0

Description: A tall building with many windows.

Page 20:

Photo by Maarten Deckers on Unsplash

Source: https://unsplash.com/photos/low-angle-photo-of-white-building-yWO5xD-JFAM

Description: Low-angle photo of a white building.

Page 30:

Photo by Yukon Haughton on Unsplash

Source: https://unsplash.com/photos/a-large-tall-tower-with-a-sky-background-0UBiwg3d6YQ

Description: A large tall tower with a sky background.

Page 40:

Photo by Joel Filipe on Unsplash

Source: https://unsplash.com/photos/high-rise-gray-concrete-building-during-daytime-QrpQ2M0Mb1U

Description: Glass panel high-rise building under blue sky with the sunrise.

Page 53:

Photo by Simone Hutsch on Unsplash

Source: https://unsplash.com/photos/gray-and-white-digital-wallpaper-g9-R1PprzVw

Description: Gray and white digital wallpaper.

www.qualitax.io

contact@qualitax.io

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.