Research Report

Tokenization Standards: Taming the Regulatory Menagerie

Nethermind & PwC Germany

February 2025

NETHERMIND

pwc

Executive Summary

Tokenization is revolutionizing the financial landscape by enabling efficient, transparent, and programmable digital assets. As the market is projected to reach $16.1 trillion by 2030, tokenization offers significant opportunities across various industries. However, regulatory uncertainty and fragmented token standards remain key challenges.

This report, produced by Nethermind and PwC Germany, explores the intersection of tokenization standards and regulatory compliance in the European Union (EU), particularly in relation to MiCAR and MiFID II. It provides a deep dive into token standards such as ERC-20, ERC-721, ERC-1155, ERC-1400, ERC-3643, and CMTAT, evaluating their role in ensuring compliance, security, and interoperability.

As regulators and industry participants work toward standardization, the adoption of compliance-aware token standards will be crucial for enabling secure, regulated, and scalable tokenized financial products.

Key Takeaways

1. Tokenization is Transforming Financial Markets
- The tokenized asset market is expected to reach $16.1 trillion by 2030 with a 50.1% CAGR from 2022 to 2026.
- Tokenization streamlines processes, reduces costs, enhances liquidity, and enables fractional ownership of real-world assets (RWAs).

2. Regulation is the Biggest Challenge & Opportunity for Tokenization
- MiCAR (Markets in Crypto-Assets Regulation) provides a comprehensive framework for crypto assets in the EU, but it does not apply to financial instruments.
- MiFID II (Markets in Financial Instruments Directive) governs tokenized financial instruments, creating a complex compliance landscape.
- Regulatory clarity is increasing, but jurisdictional differences remain an obstacle for global adoption.

3. Token Standards Play a Crucial Role in Compliance & Adoption
- ERC-20 remains the dominant fungible token standard but lacks built-in compliance features.
- ERC-1400 and ERC-3643 are tailored for security tokens, embedding compliance mechanisms such as KYC, AML, and transfer restrictions.
- CMTAT (Swiss-compliant standard) is optimized for Swiss financial regulations but may require adaptation for other jurisdictions.

4. Compliance-Aware Token Standards are Gaining Adoption

- ERC-3643 (T-REX) integrates identity management and regulatory controls directly into token operations, ensuring on-chain compliance.
- ERC-1400 enables document management and investor protections, making it suitable for tokenized securities and regulated assets.
- Hybrid approaches will likely dominate, combining off-chain compliance processes with on-chain automation.

5. The Road Ahead: Standardization & Cross-Chain Interoperability

- Industry-wide collaboration is needed to establish universal tokenization standards aligned with regulatory frameworks like MiCAR.
- Cross-chain interoperability remains a challenge, as token standards must adapt to different blockchain environments.
- The adoption of zero-knowledge proofs (ZKPs) and privacy-enhancing technologies will be key for institutional adoption of tokenized financial assets.

Final Thought

For tokenization to reach its full potential, issuers, service providers, and regulators must align on scalable, compliance-friendly token standards. The future of digital assets will depend on the harmonization of regulatory frameworks, interoperability solutions, and the continued evolution of blockchain-based compliance mechanisms.

Table of Content

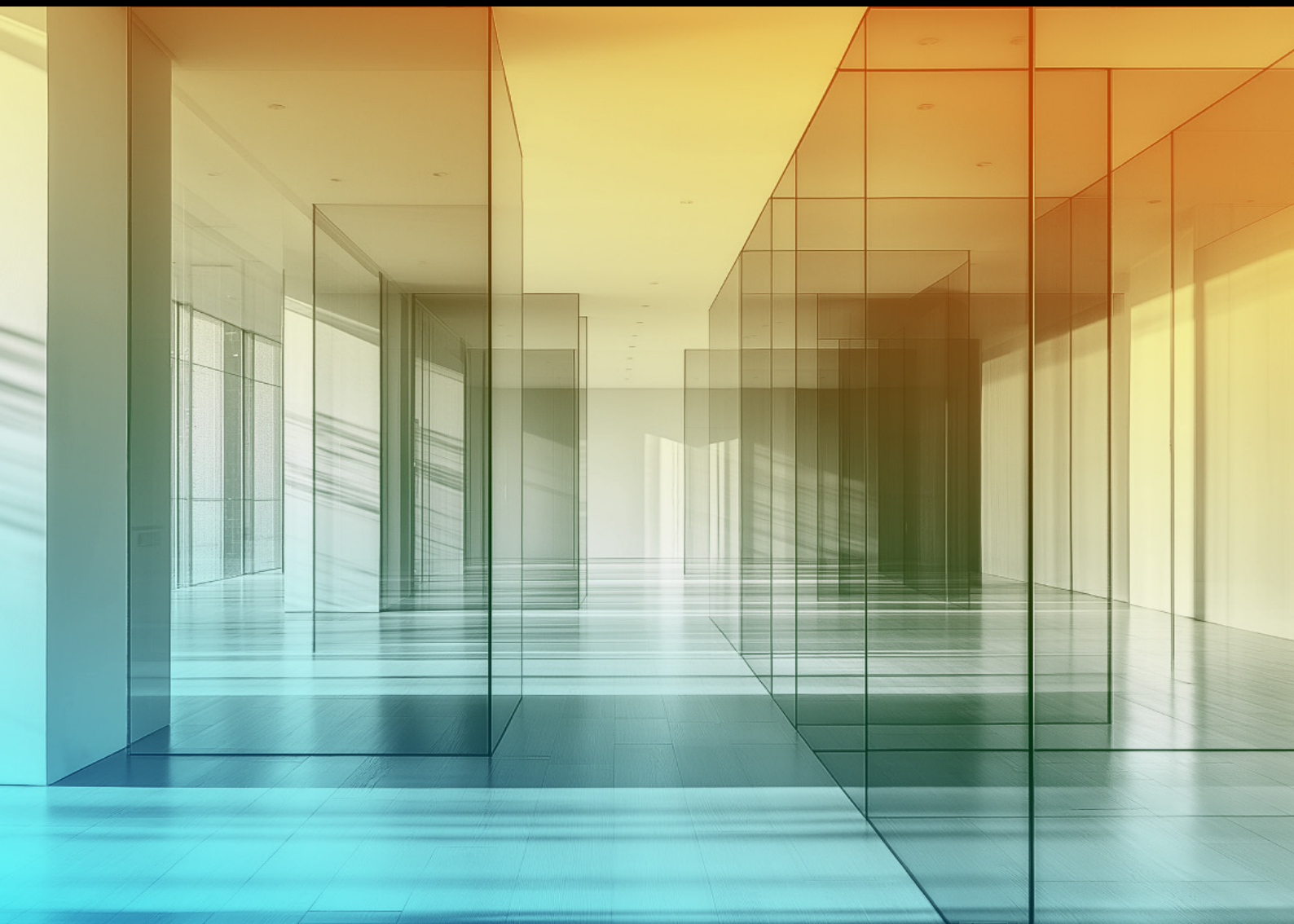
Introduction

Tokenization—the process of converting rights or assets into digital tokens on blockchain networks—is transforming industries through enhanced efficiency, transparency, and composability. By creating digital representations of real-world assets (RWAs), issuers streamline processes, reduce costs, and expand market access. This transformation is particularly evident in financial instruments, where tokenization eliminates manual compliance checks and enables transparent, flexible transaction rules. A prime example is BlackRock, the world's largest asset manager, which launched a tokenized fund on the Ethereum blockchain in 2023 to give institutional investors streamlined access to short-term US Treasury bills. Such innovations demonstrate tokenization's transformative potential in traditional finance and beyond.

The tokenized asset market shows remarkable growth potential, with projections reaching $16.1 trillion by 2030 and a compound annual growth rate of 50.1% from 2022 to 2026. Currently, over $91 billion worth of RWAs are tokenized across various blockchain networks, with Ethereum leading the space [1]. However, tokenization faces two significant challenges: regulation and standardization. The complex regulatory landscape across jurisdictions poses a major hurdle, while the need for universal token standards that support compliance, enhance composability, and simplify development remains crucial. Overcoming these challenges is essential to unlock tokenization's full potential and achieve its projected growth.

01

Shaping the future: Token Standards and Regulatory Compliance in the EU



01 The Crucial Role of Token Standards in Navigating Regulatory Waters

Implementing standards plays a pivotal role in unifying data handling across various industries and use cases. It acts as a driver of efficiency and the foundation for seamless integration and communication between different systems and platforms. Within the landscape of crypto and digital assets, the implementation of standards has been a large benchmark in scaling adoption as well as ensuring interoperability.

A major regulatory adoption of token standards can be observed in transaction reporting for tokenized financial instruments. Token standards enable regulators to monitor market activities more effectively. The high level of transparency makes it easier to detect anomalies and mitigate fraudulent activities, aiming at a safer and more secure market environment.

From a regulatory perspective, the unification brought about by standards simplifies the oversight of the market and the execution of regulatory policies. For instance, functionalities within the ERC-20 token standard, such as burning and minting, help external stakeholders understand its structure and see how the underlying tokenized financial instrument executes its functions. As a result, standards enable regulatory frameworks and pay into clear guidelines for existing as well as future digital asset regulations.

The following chapters will introduce the current regulatory landscape and explain how token standards play a role in it.

---

02 Mapping the Rules - Understanding MiCAR and MiFID II

This section seeks to explore and clarify the regulatory framework for crypto assets within the European Union (EU). It focuses on the Markets in Crypto Assets Regulation (MiCAR) and its interplay with the Markets in Financial Instruments Directive (MiFID II) - the two most significant regulatory frameworks, as they encompass most tokenized assets.

The regulation of tokenized assets in the EU is primarily shaped by the Regulation 2023/1114, known as the Markets in Crypto Assets Regulation and adopted by the EU on May 16, 2023. MiCAR aims to create a harmonized legal framework for crypto assets across the EU, fostering investor protection, market integrity, and financial stability while setting out comprehensive rules for the issuance and trading of crypto assets. It stands out globally as the most progressive legislation on crypto assets to date. The regulation introduces an extensive range of requirements for the prudential and conduct regulation of issuers of crypto assets, as well as providers of crypto-asset services. Under MiCAR, three types of crypto assets can be distinguished:

Figure 1: Classification of crypto assets under MiCAR

1. Asset-referenced tokens (ARTs)
2. E-Money tokens (EMTs)

3. Crypto assets other than ARTs or EMTs

An asset, represented on-chain using a certain token standard, can therefore be classified into one of these three categories based its characteristics. However, MiCAR does not cover all distributed ledger technology (DLT) based tokens and excludes assets already regulated by other EU legislation like the Payment Services Directive (PSD II) (Directive 2015/2366/EU), the EU Directive on Deposit Guarantee Schemes (Directive 2014/49/EU) or the Securitization Regulation (Regulation (EU) 2017/2402).

Most pertinently however, MiCAR does not apply to financial instruments (including security tokens) and structured deposits which instead fall within the scope of MiFID II (Directive 2014/65/EU). Therefore, MiFID II is the second most significant regulatory framework for crypto assets, as it governs the trading of financial instruments within the EU, and thus applies to all crypto assets that are classified as such instruments. This directive includes requirements for transparency, reporting, investor protection, and the regulation of trading platforms and intermediaries. The applicable regulatory regime depends on the specific characteristics of the individual underlying asset or financial instrument.

Figure 2: Distinction between the scope of MiCAR and MiFID II

The legal classification of crypto assets is vital in determining the applicable regulations and identifying the categories of market participants permitted to engage with them. Although a token standard's design can facilitate regulatory compliance and support the implementation of certain compliance features directly on-chain, it is not the token standard itself that determines regulation. Instead, it is the underlying asset or financial instrument represented on-chain through the token standard that is subject to regulation. As mentioned before, in the European regulatory landscape, this distinction often places crypto assets under the scope of either MiCAR or MiFID II.

However, drawing a clear line between blockchain-based financial instruments and other crypto assets can be challenging. It is the responsibility of the crypto-asset issuer to clearly outline in the white paper the type of asset being offered to the public and justify its classification. The following sections will provide a concise explanation, highlighting how the underlying asset, rather than the token standard, determines the regulatory classification and the framework under which the asset falls.

03 Breaking the Link - Why Token Standards and Regulations Stand Apart

While tokenized instruments are subject to regulatory requirements, it's important to note that these requirements are not tied to any specific token standard. Instead, the regulatory framework is linked to the nature and structure of the underlying asset, i.e., the underlying financial instrument. This distinction is crucial as it emphasizes that the regulations focus on what the token represents rather than the technology, the token standard or blockchain protocol

used to create the token. Understanding this point helps in navigating the complex regulatory landscape and sets the stage for a deeper dive into specific regulations, such as those outlined in MiCAR and MiFID II.

04 MiCAR – A Framework for Digital Assets Compliance

MiCAR, as the major crypto-asset regulatory framework within the European Economic Area (EEA), is structured to regulate the issuance and servicing of crypto assets by focusing on the roles of key market participants, such as issuers and service providers. The regulation primarily addresses the classification of underlying assets, assigning them to specific regulatory categories such as EMTs, ARTs, or other types of crypto assets. Once the asset is classified, MiCAR outlines the specific requirements for the issuer or service provider involved.

In relation to token standards like ERC-20 or ERC-721, MiCAR does not directly regulate the technical structure of these standards. Instead, it uses the nature of the underlying asset as the basis for determining regulatory compliance. The token standard becomes relevant in ensuring that the processes and mechanisms required by MiCAR, such as transparency, consumer protection, and governance, can be effectively implemented by issuers and service providers. In other words, the design of the token standard can facilitate compliance with MiCAR by supporting the necessary controls and protocols that meet the regulation's requirements.

MiCAR specifically targets crypto assets issued by various actors and sets regulatory obligations for both the issuers of these tokens and the Crypto Asset Service Providers (CASPs) that manage their trading, storage, and other services. This framework ensures that token issuance and service provisioning are conducted within a compliant and transparent environment but leaves the technical design of token standards to support, rather than dictate, regulatory compliance. MiCAR specifically sets forth regulatory requirements for issuers of EMTs, ARTs, utility tokens, and other crypto assets as well as CASPs.

Table 1: Regulatory obligations for issuers of crypto asset

Issuers of other crypto assets	A key distinction is made between "issuers of ARTs and EMTs" and "issuers of other crypto assets." For issuers of crypto assets other than EMTs and ARTs, public offerings or the listing of tokens on a trading platform must comply with certain conditions, which include publishing a white paper, adhering to conduct regulations, and meeting transparency requirements in advertising. Issuers must also give retail holders the right to withdraw from their holdings within a specified timeframe, act in the best interest of retail holders, and implement governance measures to prevent conflicts of interest.
Issuers of ARTs and EMTs	Issuers of ARTs and EMTs, however, face more stringent requirements. They must typically obtain prior authorization from national supervisory authorities. In addition to general obligations like publishing a white paper, they are also required to provide monthly disclosures on the number of tokens in circulation and the composition of reserve assets. Furthermore, they must maintain strong governance structures, including clear organizational management and a business continuity plan, while keeping authorities informed of any management changes.
Issuers of EMTs	Issuers of ARTs and EMTs, however, face more stringent requirements. They must typically obtain prior authorization from national supervisory authorities. In addition to general obligations like publishing a white paper, they are also required to provide monthly disclosures on the number of tokens in circulation and the composition of reserve assets. Furthermore, they must maintain strong governance structures, including clear organizational management and a business continuity plan, while keeping authorities informed of any management changes. Since EMTs are classified as electronic money under the Electronic Money Directive (EMD) and fall within its scope, MiCAR imposes additional requirements on EMT issuers. They must be authorized as either a CRR credit institution or an electronic money institution and funds received in exchange for EMTs must be invested in secure, low-risk assets or deposited in a separate account with a credit institution, with at least 30% of the funds held as deposits. EMTs must also be issued at par value, and holders must be able to redeem them at any time and free of charge.

Significant ARTs and EMTs as classified by the EBA

The European Banking Authority (EBA) is a regulatory agency of the European Union responsible for ensuring a harmonized and effective regulatory framework for financial institutions across the EU. Its role includes developing technical standards, guidelines, and recommendations to enhance the stability and integrity of the financial system. The EBA can designate ARTs or EMTs as significant based on certain criteria, such as the number of token holders or the value of the tokens issued. In such case, the issuers of significant ARTs or EMTs will be subject to additional

of a remuneration policy promoting effective risk management, the guarantee that tokens can be held in custody by different CASPs and enhanced supervision by the EBA and national competent authorities.

Crypto Asset Service Providers (CASPs)

CASPs are required to provide detailed information about their business operations and internal structures as part of the authorization process. This includes disclosing internal risk control mechanisms, compliance with anti-money laundering (AML) regulations, and other critical operational details. CASPs must also maintain thorough records of all activities, orders, and transactions, ensuring this information is accessible to both clients and regulatory authorities. In addition, they are required to disclose any legal entities holding significant stakes in the company, along with their IT security protocols and business continuity plans. To ensure the integrity of their operations, CASPs must also maintain appropriate financial safeguards, establish a robust governance framework, and properly manage outsourcing agreements.

CASPs with at least 15 million active users in the EU within a calendar year are classified as significant and must notify their competent authorities within two months of reaching this user threshold. Once classified as such, MiCAR grants competent authorities enhanced powers of investigation and supervision over significant CASPs.

Specifications by the EBA

Issuers of significant asset-referenced tokens (≥ €5 billion in reserves or ≥ 10 million users) must maintain sufficient liquidity to fulfill redemption requests, holding at least 60% of reserves in highly liquid assets with banks, thus mitigating the risk of broader financial instability through ties to traditional banking systems. Additionally, the RTS mandates over-collateralization for tokens to ensure sufficient backing. This applies to both asset-referenced and e-money tokens, with requirements for quarterly reporting on reserves for tokens exceeding EUR 100 million in issue value.

Stablecoins are further subject to liquidity rules, ensuring the maturity of their underlying assets and redemption capabilities, with exposure limits on single issuers for both bank deposits and liquid assets.

Token standards' features for assets under MiCAR

A leading example of how token standard features can facilitate regulatory compliance is USDC - a US dollar stablecoin issued by Circle, built on the widely adopted ERC-20 standard. ERC-20's interoperability and token management features make it a common choice for crypto assets that aim to be compliant with existing regulations while still offering a high degree of flexibility.

The USDC functionality is explained as follows: *"For every USDC issued by Circle and remaining in circulation in the European Economic Area ("EEA"), Circle holds either one U.S. Dollar ("USD") or an equivalent amount of USD-denominated assets on behalf of holders, in order to facilitate the frictionless movement of the e-money tokens, utilizing blockchain technology. As a fully reserved*

e-money token, USDC is backed by an equivalent amount of U.S. Dollar-denominated assets held by Circle SAS and redeemable 1:1 for U.S. dollars." [2].

Circle and its USDC make use of the core functionalities of the ERC-20, including minting (issuance), burning (redemption), and the transfer of tokens between parties, which align closely with MiCAR's regulatory requirements. These functions ensure that token management is transparent, auditable, and easily trackable, helping meet the demands for transparency and accountability in both the issuance and trading of tokenized assets. USDC's use of a minting and burning system allows Circle to maintain reserves that match the value of tokens in circulation, ensuring compliance with MiCAR's liquidity and redemption requirements for e-money tokens (EMTs). ERC-20's support for tracking the total supply of tokens, verifying balances with the balanceOf function, and facilitating transfers through transfer and approve methods further strengthens its ability to comply with MiCAR's requirements. These features enable issuers like Circle to maintain transparency and provide seamless reporting on token activity, which is mandatory for significant issuers under this regulatory framework. Events such as transfer and approval help automate transaction tracking, ensuring that all token movements are fully auditable, while the built-in programmability of ERC-20 tokens simplifies the implementation of governance structures aligned with MiCAR's liquidity and over-collateralization requirements. For instance, by burning USDC tokens, Circle can maintain parity between the total token supply and the underlying USD reserves, ensuring compliance with requirements for redeemability and transparency.

In addition to these ERC-20 standard features, Circle extends the existing ERC-20 token standard with additional functionalities. USDC includes a blacklist functionality, enabling Circle to freeze funds in certain accounts. This capability helps complying with regulatory mandates, such as sanctions and fraud prevention, and demonstrates how token standards can be tailored to meet specific obligations like anti-money laundering and security measures. For non-EVM compatible blockchains, that are not capable of using the ERC-20 token standard (e.g. Solana or Stellar), Circle refactored available token standards per blockchain to the required specification.

Of course, other token standards, such as ERC-1400, may provide additional features aimed at easing regulatory compliance as well. For instance, ERC-1400, specifically designed for security tokens, includes compliance mechanisms like KYC/AML-based transfer restrictions, document management, and granular control over token transfers. This further emphasizes how various token standards can be designed to help meet the requirements of the regulatory frameworks. However, ERC-20 remains the most widely used standard for tokenized assets due to its flexibility and interoperability, making it easy to implement and adaptable to various use cases.

Limitations

While token standards like ERC-20 and ERC-1400 provide functionalities that can support compliance with MiCAR, many regulatory requirements are still largely fulfilled off-chain. The key reason is that regulatory frameworks do not specify whether compliance must occur on-chain or off-chain, as long as the necessary obligations are fulfilled. As a result, while the token standards' individual features may be beneficial for certain compliance requirements, they are not yet widely applied in areas such as anti-money laundering checks or corporate governance.

These areas continue to depend on well-established, off-chain processes that are recognized as

effective and secure under current regulations. Therefore, the use of token standards' compliance features only makes sense where they can make the existing compliance process more efficient or effective.

Consequently, although token standards can improve certain aspects of regulatory compliance - such as enabling transparent transactions and ensuring traceability - many core functions vital to meeting MiCAR's requirements, including governance structures, auditing, and KYC/AML compliance mostly remain off-chain. This hybrid approach ensures compliance is met in an efficient and battle-tested way while still allowing for flexibility in creating and incorporating on-chain compliance features, such as blacklisting or whitelisting features, where they provide added value.

05 MiFID II - Laying Down the Rules for Tokenized Financial Instruments

Although MiCAR covers various types of assets such as EMTs, ARTs or utility tokens, crypto assets may also be classified as financial instruments, in which case they fall under the scope of MiFID II rather than MiCAR. In light of the distinction between financial instruments and crypto assets under MiCAR, this issue becomes challenging, as MiFID II does not provide a universal definition for all types of financial instruments. Instead, the term "financial instrument" is outlined through a list of instruments in Annex I of MiFID II [3], rather than being defined by a specific set of conditions and criteria. Additionally, unlike the U.S., where the Howey test is applied, EU jurisprudence has yet to fully address the nature and defining characteristics of financial instruments.

To provide further clarity on which assets are considered financial instruments and which are not, the European Securities and Markets Authority (ESMA) published a Consultation Paper on January 29, 2024, with Draft Guidelines for distinguishing crypto assets from financial instruments under MiFID II (European Securities and Markets Authority) [4]. This distinction is important, given that MiCAR clearly stipulates that crypto assets qualifying as financial instruments are not subject to MiCAR, but to the regulation of financial instruments. The consultation paper highlights several key points and distinguishes between specific categories of financial instruments, including (i) transferable securities, (ii) money-market instruments, (iii) units in collective investment undertakings, (iv) derivatives, and (v) emission allowances.

1. **Transferable Securities:** Crypto assets may be classified as transferable securities if they grant rights like shares, bonds, or other securities, are part of a negotiable class of securities, and are not payment instruments.
2. **Money-market Instruments:** Crypto assets are unlikely to be classified as such, unless they embed a monetary obligation with a set maturity or redemption date within 397 days and have a stable value.
3. **Units in Collective Investment Undertakings:** These are crypto assets that represent investor rights in pooled funds aimed at generating returns, provided investors do not control the investment vehicle.
4. **Derivatives:** Crypto assets can act as underlying instruments for derivatives or be considered derivatives if they represent a contract with an underlying asset that determines value.

5. **Emission Allowances:** These represent rights to emit greenhouse gases. While theoretically possible, it's unlikely for crypto assets to be classified as emission allowances.

If a crypto-asset is classified as financial instrument under MiFID II, subsequently it is subject to the spectrum of regulatory obligations defined by the framework, which are designed to ensure transparency, investor protection, and market integrity.

One of its key objectives is to move trading activities to regulated platforms, reducing the use of over-the-counter (OTC) trading. MiFID II also creates the Organized Trading Facility (OTF) to bring previously unregulated trades under supervision, and it requires investment firms executing client orders to operate through a Multilateral Trading Facility (MTF).

In terms of transparency, MiFID II requires regulated markets and MTFs to continuously publish bid and offer prices, ensuring that market participants have access to more detailed and real-time pricing information. Additionally, it mandates the unbundling of research costs from transaction fees, allowing investors to see the distinct charges for these services, providing clarity on costs and promoting fair competition.

Investor protection is further strengthened by limiting inducements from third parties to financial advisors and investment firms. These restrictions aim to ensure that services and advice are provided in the best interests of clients, free from conflicts of interest. Furthermore, investment firms are required to take all necessary steps to achieve the best possible outcomes for their clients, including clear disclosures regarding fees and commissions.

MiFID II also imposes strict reporting requirements. Firms must report all transactions to regulators by the next business day and must keep records of communications to support regulatory oversight and reduce the risk of market abuse.

Further requirements imposed by MiFID II include:

- **Best Execution:** Firms must ensure the best possible outcome for client orders, considering factors such as price, costs, speed, and likelihood of execution.
- **Suitability and Appropriateness:** Firms are required to assess whether a product or service is suitable for the client's needs and financial situation. This includes evaluating the client's knowledge, experience, financial background, and investment objectives to ensure that offerings are appropriate.
- **Conflicts of Interest:** Firms must identify and manage conflicts of interest to ensure they do not adversely affect the interests of clients. This involves implementing policies and procedures to detect, prevent, and disclose any potential conflicts that could influence the firm's decisions.
- **Product Governance:** Proper procedures must be established for the creation and distribution of financial instruments.
- **Investor Protection:** Firms must implement measures to safeguard clients' investments and ensure fair treatment. This includes providing clear and accurate information, offering secure investment environments, and addressing client complaints effectively.
- **Risk Management:** Effective risk management policies and procedures must be implemented to identify, monitor, and manage risks related to the firm's activities. This involves regular risk assessments, mitigation strategies, and continuous monitoring to ensure stability and compliance.

Features of token standards can contribute to meeting some of these regulatory requirements, particularly in areas such as transparency, reporting, and investor protection. For instance, they can facilitate transparent and verifiable transactions on the blockchain, providing a clear audit trail for all token transfers, as all transactions can be automatically recorded and accessed in real time, therefore reducing the risk of market abuse and supporting regulatory oversight.

While blockchain-based transactions themselves do not directly ensure best execution, the immutability and transparency of token transfers can support firms in monitoring execution quality. Similarly, the programmability of ERC-20 tokens can be used to integrate conflict of interest policies, ensuring that certain transactions are blocked or flagged if they violate compliance rules.

Token standards also offer a way to enforce rules about who can hold or trade a token, supporting efforts to design and distribute financial instruments that align with clients' needs. Furthermore, the transparency provided contributes to investor protection by enabling firms to disclose transaction costs and other relevant details clearly and in a verifiable manner.

One example of a financial institution developing MiFID II-compliant tokenized financial products is Société Générale, which has created a variety of offerings [5].

Smart cash for example aims to be a secure alternative for money market investors, designed as an alternative to traditional certificates of deposit [6]. SGIS Smart Cash is tokenized on Ethereum and Tezos and classified as a debt security under MiFID II. Issued by SG Issuer, a member of Société Générale, and collateralized by BNY Mellon, it offers daily liquidity with a T+2 settlement cycle. The collateral is monitored independently by BNY Mellon to ensure that its value exceeds the pre-agreed percentage of the notes' accrued value. Investors benefit from greater transparency, efficiency in capital markets, and improved security through blockchain-based registration. All transactions and redemptions are automatically recorded, facilitating compliance with reporting requirements and offering investors flexibility through early redemption options.

Société Générale also offers structured products for professional investors [7]. These products are classified as debt securities under MiFID II and are designed to enable faster settlement times and enhanced transparency. By utilizing blockchain, they provide real-time traceability and security, fulfilling the transparency and governance requirements of MiFID II, while ensuring that investors have clear visibility into their transactions and holdings.

The above-mentioned example shows that tokenizing financial products collateral still largely rely on off-chain processes like the collateral monitoring by banks, which highlights that blockchain hasn't fully eliminated off-chain processes. While token standards can facilitate features like automated reporting, these don't inherently improve efficiency over traditional off-chain mechanisms. Ultimately, MiFID II's framework doesn't consider the nuances of blockchain technology, which often results in the need for ongoing human oversight and reliance on off-chain infrastructure for areas like collateral monitoring and risk management.

Furthermore, MiFID II doesn't offer a clear, universal definition for financial instruments that accounts for distributed ledger technology. The list of instruments under Annex I Section C did not cover DLT-issued assets fully, creating regulatory ambiguity. Since MiFID II is a directive, its transposition into national law across EU member states has resulted in differing interpretations of what constitutes a financial instrument, leading to a lack of full harmonization. This creates

uncertainty for digital assets, making compliance more complex for cross-border activities. This often creates a hybrid approach to compliance where DLT contributes to transparency but falls short of replacing the off-chain systems entirely.

06 Token Standards and Regulation – The Road Ahead

In summary, the regulatory landscape for tokenized assets in the EU, primarily shaped by the MiCAR, offers a comprehensive and forward-thinking framework for the issuance, trading, and governance of crypto assets, aiming to ensure investor protection, market integrity, and financial stability. By establishing guidelines for the classification and requirements of various types of crypto assets, MiCAR provides much-needed clarity and consistency across the European Union. However, the interaction between MiCAR and other EU regulations, such as MiFID II, also creates a complex compliance environment for issuers and service providers. These regulations require careful evaluation of each tokenized asset to determine the applicable regulatory requirements.

At the same time, regulatory focus remains on the underlying product rather than the specific token standard used, targeting token issuers more directly than the technological implementation, thus rendering regulation largely standard agnostic. This environment demands that token issuers prioritize compliance irrespective of the token standard they employ.

Certain token standards, such as CMTAT, ERC-1400, and T-REX, are specifically designed to support regulatory compliance by embedding essential information directly on-chain. For example, T-REX provides a robust framework for the compliant management and transfer of security tokens, earning recognition from major regulators like CSSF, BaFin, DFSA, FSRA, and MAS. It has also been referenced in reports by authorities such as ESMA, institutions like Citi, and blockchain industry leaders including Polygon [8].

However, while compliance-focused token standards offer advanced features that can simplify adherence processes, they must be carefully evaluated to ensure alignment with the specific regulatory requirements of each jurisdiction. In contrast, widely adopted standards like ERC-20 provide greater flexibility and interoperability, benefiting from broad adoption, extensive developer support, and a strong foundation for innovation and integration.

Additionally, the evolving nature of regulatory frameworks demands regular updates and audits of token standards to maintain compliance. Token issuers must stay proactive and informed about regulatory changes across jurisdictions to effectively address these challenges.

As blockchain technology progresses, new token standards are likely to emerge, offering enhanced compliance features and improved efficiencies. Collaboration between regulators and blockchain developers will play a crucial role in establishing robust and compliant token standards. As regulatory frameworks and token standards continue to evolve, the emphasis should remain on ensuring that token issuers and their underlying products meet compliance requirements, rather than prioritizing the specific token standards used.

07 Unlocking Success in Token Compliance

As we conclude this comprehensive exploration of the regulatory framework for tokenized assets in the European Union, the Markets in Crypto assets Regulation emerges as a global benchmark for crypto-asset legislation. Especially the interplay between MiCAR and other EU regulations, such as MiFID II, PSD II, and local laws like Germany's eWpG, highlights the need for thorough compliance, careful evaluation of each tokenized asset, and the opportunity for financial institutions to establish their business models with a clear and consistent approach.

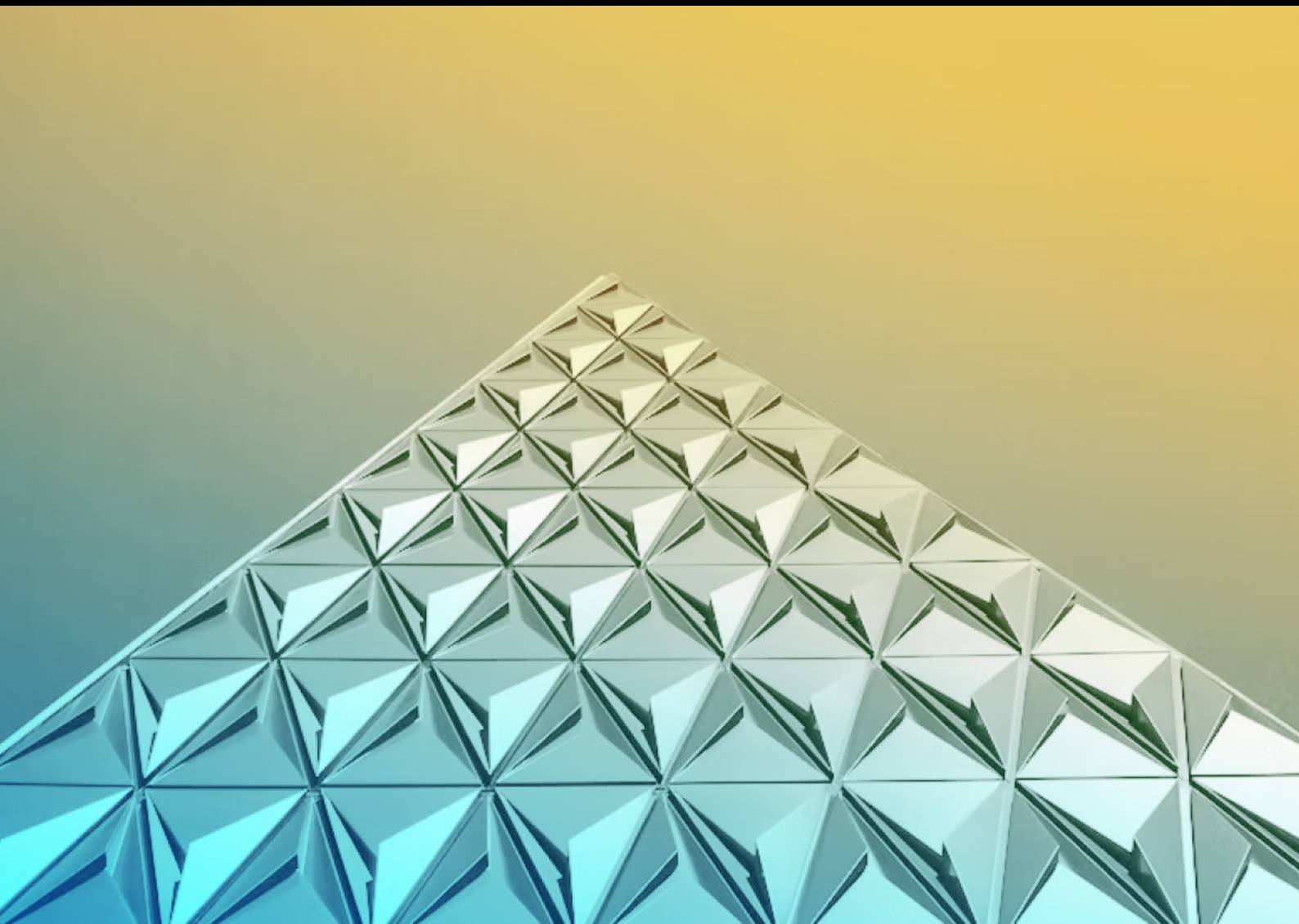
Now, more than ever, issuers, offerors, and crypto-asset service providers must prioritize regulatory compliance to navigate in this evolving sector effectively:

- **Stay Informed and Updated:** Regulatory landscapes are dynamic. Ensure you are always up to date with the latest developments, guidelines and consultation papers from regulatory bodies like ESMA and EBA.
- **Evaluate and Adapt:** Carefully assess your tokenized assets to determine the specific regulatory requirements they fall under. Experiment with compliance-focused token standards like T-REX or ERC-1400 to streamline adherence processes or leverage widely adopted standards like ERC-20 for greater flexibility and interoperability while carefully evaluating the balance between on-chain and off-chain service capabilities.
- **Engage with Experts:** Consult with professional services such as legal and compliance experts to ensure your white papers, marketing communications, and business operations meet the regulatory requirements.
- **Implement Robust Compliance Measures:** Develop strong internal controls, governance structures, and a risk management framework to align with MiCAR and other relevant regulations.
- **Collaborate and Innovate:** Work closely with blockchain developers, web3 native companies and regulatory bodies to create and adopt token standards that facilitate regulatory compliance while driving innovation.

By taking these proactive steps, you can ensure your operations not only comply with the current regulatory framework but also adapt to future changes, thereby fostering trust, integrity, and stability in the crypto-asset market.

02

Tokenization Standards



Tokenization standards are protocols and guidelines that govern how tokens are created and managed on blockchain platforms. These standards ensure tokens work together seamlessly and securely. They allow tokens from different projects to work smoothly with wallets, exchanges, and DeFi protocols without extra modifications. ERC-20 tokens exemplify this, having become fundamental to many blockchain ecosystems through their universal compatibility.

Using established standards makes tokens more secure, as these frameworks have undergone extensive testing and refinement by the blockchain community. This provides a robust foundation for development. Additionally, building on existing standards lets teams concentrate on creating innovative features while meeting industry best practices and regulatory requirements, instead of building everything from scratch.

In the next sections, we examine key token standards and their roles in blockchain ecosystems. The following sections deep dive into various popular token standards used for tokenization, and analyzes their unique contributions towards the creation of tokenized assets and their integration with DeFi and real-world applications.

ERC-20 The Fungible Token Standard	**ERC-721** The Non-Fungible Token Standard		**ERC-1155** Multi-Token Standard
	ERC-1400 Security Token Standard	**ERC-3643** The Compliance-Aware Token Standard	
CMTAT The Swiss-Compliant Standard		**ERC-1450** Issuing and trading SEC-compliant securities	**ERC-2980** Swiss Compliant Asset Token

ERC-20: The Fungible Token Standard

Ethereum Improvement Proposals: ERC-20

ERC-20 is the most widely used token standard on the Ethereum blockchain and other EVM chains. It defines a set of rules that all fungible tokens must follow, ensuring seamless interaction with wallets, exchanges, and other smart contracts. Originally proposed by Vitalik Buterin and Fabian Vogelsteller in 2015, it was first intended as a standard for currency, but was later made more general to serve any kind of fungible token. The ERC-20 standard has been fundamental to the growth and development of both Decentralized Finance and the broader Ethereum ecosystem, providing a clear and consistent framework for creating fungible tokens.

Key Features

The ERC-20 standard focuses on the most basic aspects of a token, such as transferring and keeping balances. Standardized functions such as **`transfer`** and **`getBalance`** allow ERC-20 tokens to integrate with various platforms effortlessly. ERC-20 defines a set of six mandatory functions, and three optional ones, ensuring that all tokens implementing the standard adhere to the same basic functionality.

Mandatory Functions:

- **`totalSupply`**: Returns the total existing supply of the tokens.
- **`balanceOf`**: Returns the balance of tokens held by a specified address.
- **`transfer`**: Transfers a specified number of tokens from the caller to a specified address.
- **`transferFrom`**: Transfers tokens from one address to another on behalf of the token holder.
- **`approve`**: Allows an address to spend a specified number of tokens on behalf of the token holder.
- **`allowance`**: Returns the number of tokens that a token holder has allowed an address to spend on their behalf.

Optional Functions:

- **`name`**: `Returns the name of the token.`
- **`symbol`**: Returns the symbol of the token.
- **`decimals`**: Returns number of decimal places the token uses for precision.

In addition to these functions, ERC-20 tokens include two events that enable tracking of token transactions and approvals, which is critical for transparency and auditability.

Events:

- **`Transfer`**: Emitted when tokens are transferred from one address to another.
- **`Approval`**: Emitted when a token holder approves another address to spend tokens on their behalf.

While any token contract properly implementing these functions and events follows the standard, OpenZeppelin's ERC20.sol implementation has become the conventional choice when creating an ERC-20 token. This implementation allows for specifying the token name and symbol at deployment, while allowing inheriting contracts to specify their own token minting logic. It also contains some additional features that are not present in the standard, such as reverting on failed function calls, and having a default decimal value of 18.

The uniformity and simplicity created by the standard allows ERC-20 tokens to be easily integrated with various Ethereum-based applications, including wallets and DeFi platforms. The standardization of its events and functions facilitates interoperability and composability within the ecosystem, and combined with a first mover advantage, results in the ERC-20 standard benefitting from widespread adoption and use.

Advantages

ERC-20 has become the de facto standard for creating fungible tokens on Ethereum, leading to a vast ecosystem of tokens, tools, and services. This broad adoption provides network effects that benefit new token projects by leveraging existing infrastructure and community support, from wallets to block explorers.

In addition to this broad adoption, the rise of decentralized finance (DeFi) has benefited ERC-20 tokens even further. DeFi platforms often use the composability of ERC-20 tokens for lending, borrowing, staking, and yield farming, further enhancing their utility and value.

Furthermore, the ERC-20 standard simplifies the process of creating new tokens. Developers can deploy an ERC-20 token with minimal or no code, reducing the barrier to entry for asset tokenization. This ease of creation has led to a proliferation of tokenized assets, from cryptocurrencies to real-world assets like real estate and commodities.

While most ERC-20 tokens only need to implement the basic functionality, it is possible to enhance or alter this functionality to suit specific use cases. This flexibility makes the standard very powerful, and very suitable for tokenizing assets that require bespoke logic.

Lastly, liquidity is enhanced by the fact that ERC-20 tokens can be traded on a plethora of decentralized and centralized exchanges. This liquidity is essential for asset tokenization, as it allows token holders to easily buy and sell their tokens, increasing market efficiency and accessibility.

Disadvantages

While ERC-20 tokens allow for easily interacting with DeFi applications and other smart contracts trough it's allowance system, this has also enabled scams. Since decentralized smart contracts often ask for high allowances to avoid the gas expense of repeated approvals, users get accustomed to allowing their entire balance of tokens. This is a problematic practice, as it makes it more likely for users to be scammed by giving an allowance to the wrong contract, often by accessing malicious phishing sites. Another attack vector is the intended smart contract being compromised, and an attacker using the contracts allowance to steal user tokens. Despite the token standard not being directly vulnerable, its design has fostered an environment where users need to be extremely careful when carrying out approvals.

Another downside stemming from the design decisions of ERC-20 is due to the simplicity of the standard. While this simplicity makes it flexible and easy to implement, it also leaves a lot of decisions up to the token creator. One such example is the number of decimals. While 18 decimals are used for most tokens, some have a different amount, such as USDC having 6

decimals. Other tokens might have more significant changes, such as burn on transfer or rebasing mechanisms. This can lead to integration issues with infrastructure and DeFi protocols, or making smart contracts more complex in order to deal with these edge cases.

The simplicity and neutrality of the standard also means the standard does not have tokenization specific features. This functionality can be added on top of the standard, and while it's a powerful approach, it still contains tradeoffs. Like previously mentioned, custom functionality can dampen composability within the DeFi ecosystem. Not only that, but implementing common tokenization features takes time and effort that could be avoided by using a different standard better tailored to tokenization.

Real-World Applications

- **CitaDao [Real Estate]**: CitaDAO makes use of the ERC-20 standard to tokenize real estate properties. By tokenizing real estate assets, property ownership can be divided into smaller, tradeable units. This fractional ownership model makes real estate investment accessible to a broader audience, reduces entry barriers, and increases liquidity in the market. ERC-20 tokens can be issued to represent shares in individual properties. Additional benefits of this tokenization model are reduced middlemen fees and paperwork. While not the case for CitaDAO, with real estate tokenization it's also possible for token holders to receive rental income proportional to their holdings.
- **XAUt [Commodities]**: Commodities such as gold, silver, and oil can be tokenized using ERC-20 tokens, allowing these assets to be traded on blockchain platforms, providing greater transparency while reducing transaction costs and enhancing liquidity. Tether's XAUt token is an example of tokenized gold, with each token representing one ounce of the asset, providing a bridge between traditional commodities and digital assets.
- **USDC [Stablecoins]**: Arguably the most successful example of blockchain tokenized assets are stablecoins, especially US dollar equivalents like USDC. US dollar stablecoins are a popular application of ERC-20 tokens, as they allow token holders to use them as a store of value in volatile markets while also benefitting from high liquidity and the ability to use the asset in DeFi applications. The UDSC ERC-20 token makes use of a minting/burning system in order to issue and redeem USDC for US dollars. It also contains a custom blacklist functionality which allows the issuer Circle to freeze balances for certain addresses, usually applied as a result of sanctions or malicious exploits.
- **OUSG [Bills]**: Traditional financial instruments such as bills and bonds and equities can also be tokenized using ERC-20 tokens, facilitating more efficient and transparent trading while reduces settlement times, lowering costs, and enabling fractional ownership. An example of this is *Ondo Short-Term US Government Treasuries*, also known as OUSG. This ERC-20 is a token representation of USD invested into funds that are themselves invested in US Treasury bills.
- **Tokenize.it [Equities]**: Tokenize.it is an example of a Germany-based business that aims to facilitate company participation by allowing their customers to create their own platform-independent security tokens. The use of the ERC-20 standard on the Ethereum network provides a simple, fast and standardized way for investors to participate without the need for a notary, tokenizing the rights to the asset.

ERC-721: The Non-Fungible Token (NFT) Standard

Ethereum Improvement Proposals: ERC-721

The ERC-721 standard was introduced in January 2018 by William Entriken, Dieter Shirley, Jacob Evans, and Nastassia Sachs to enable the creation of tokens that represent ownership of unique items. Unlike ERC-20 tokens, which are fungible and identical to each other, ERC-721 are non-fungible tokens, each having a unique identifier and can represent distinct assets with individual properties and values.

ERC-721 tokens provide a framework for developers to create and manage NFTs on Ethereum and other EVM blockchains, ensuring interoperability and ease of integration across different platforms and marketplaces. This has led to an explosion of innovation in the digital economy, creating new opportunities for artists, creators, and investors.

Key Features

Like ERC-20, the ERC-721 standard focuses on the most basic aspects of a token, with a few additions. With each token being unique, these basic functions act over individual tokens, with a few related to approvals applying to all assets belonging to an owner. Additions to these basic operations serve to make using the standard convenient and safe to use. Safe transfers with `safeTransferFrom` ensure the recipient can receive and use the token in the case of it being a smart contract, while the `tokenURI` function points to the metadata of the token.

Mandatory Functions:

- `balanceOf`: Returns the number of NFTs owned by a specified address.
- `ownerOf`: Returns the owner of a specified NFT.
- `safeTransferFrom`: Safely transfers the ownership of a specified NFT from one address to another, ensuring that the recipient is capable of receiving NFTs.
- `transferFrom`: Transfers the ownership of a specified NFT from one address to another.
- `approve`: Grants or revokes permission to a specified address to transfer a specified NFT on behalf of the token holder.
- `getApproved`: Returns the address approved to transfer a specified NFT.
- `setApprovalForAll`: Enables or disables approval for a third party to manage all of the caller's NFTs.
- `isApprovedForAll`: Returns whether a specified operator is approved to manage all of the assets of a specified owner.

Optional Functions:

- `name`: Returns the name of the token collection.
- `symbol`: Returns the symbol of the token collection.
- `tokenURI`: Returns a URI pointing to metadata about a specified token.
- `totalSupply`: Returns the total number of tokens stored by the contract.
- `tokenByIndex`: Returns a token ID at a given index of all the tokens stored by the contract.

Events:

- `Transfer`: Emitted when an NFT is transferred from one address to another.

- `Approval`: Emitted when the approval status of an NFT is changed.
- `ApprovalForAll`: Emitted when an operator is enabled or disabled for an owner.

The ERC-721 standard has made it easy to integrate non-fungible assets across the wider Ethereum ecosystem. While the most popular use case revolves around collectible NFTs and markets around them, financial use cases are also present, such as being used to tokenize Uniswap V3 liquidity provider positions.

Advantages

ERC-721 has become the de facto standard for creating non-fungible tokens on Ethereum, in a similar way to how ERC-20 is used for fungible tokens. The standard is used to represent unique assets, such as real estate, collectibles, or intellectual property, tracking ownership and provenance in a transparent fashion. The standard benefits from wide adoption, with many platforms integration and supporting it.

While not as used in DeFi as ERC-20 tokens, it has gained some adoption there too, such as mentioned previously with Uniswap V3. Since liquidity can be provided in a custom range, the "position" of each liquidity provider will be unique. Instead of being issued ERC-20 tokens like with Uniswap V2, Uniswap V3 liquidity providers are issued a single ERC-721 token representing their custom range.

ERC-721 tokens are also simple to create using minimal or no code solutions, allowing for an easy path to unique asset tokenization. The standard is also extensible, allowing for custom logic. Certain assets require this flexibility and customization to be properly tokenized, especially when taking regulations into account.

While very similar to ERC-20 in these aspects, ERC-721 supports safe transfers, making it much less likely to accidentally make tokens unrecoverable by sending them to a wrong contract address, since contracts have to explicitly allow incoming ERC-721 transfers.

Disadvantages

While safer with transfers than ERC-20, ERC-721 tokens are still problematic with their allowance system. To avoid repeated allowances and increased gas expenses, applications often ask for approvals of an entire ERC-721 collection rather than an individual token. This makes the damage significantly worse whenever a user is phished or a smart contract they've approved is compromised, draining their entire collection. Users need to be extremely cautious of which contracts they approve, especially for entire collections.

As a non-fungible tokens, ERC-721 tokens suffer from liquidity and valuation challenges. Each token being unique makes it difficult to efficiently trade them in financial markets. Tools like liquidity pools are not really suitable, and thus order books are often used. Because of this lack of liquidity, these tokens usually take longer to trade, or require a steep discount to be traded readily. Valuation is also a challenge, since assessing the worth of non-fungible tokens is complicated by their uniqueness. Some have gotten around these issues by fractionalizing each unique ERC-721 token using ERC-20

tokens, but this could be improved by just using ERC-20 tokens from the start instead.

Like with ERC-20, the simplicity of the standard is what makes it so widely used, but it lacks tokenization specific features. While the standards flexibility makes it possible to implement them, again this could worsen composability with existing tools, and take too much time and effort when compared with readily available existing tokenization specific standards.

Real-World Applications

- **Project Guardian [Identity]**: Project Guardian aims to create infrastructure for that enables digital assets to be traded across platforms and liquidity pools across open, interoperable networks. Particularly they focus on securities in the form of digital bearer assets and tokenized deposits issued by deposit-taking institutions. ERC-20 tokens are being used for these assets, while ERC-721 tokens are being used as verifiable credentials for the investor's identity.
- **Finka Building [Real Estate]**: The Finka Building, a residential property in New York City, was tokenized using ERC-721 tokens. Ownership of each specific unit within the building was represented with a unique token. Investors could buy and trade these tokens, gaining fractional ownership and the potential for rental income from the respective units.

ERC-1155: Multi-Token Standard

Ethereum Improvement Proposals: ERC-155

ERC-1155 is a versatile standard that allows for the creation of both fungible and non-fungible tokens within a single smart contract. Introduced by Enjin in June 2018, ERC-1155 was designed to address some of the limitations of previous token standards like ERC-20 and ERC-721, combining the best of both worlds. Issuers can create multiple types of assets, whether fungible or non-fungible, under a single contract, greatly increasing of the flexibility of the standard, while still being compatible with existing infrastructure.

Key Features

ERC-1155 implements all the basic features of the ERC-20 and ERC-721 standards, while combining and extending them. One of the unique features of the standard is its efficiency in handling batch operations. For instance, a single transaction can involve the transfer of multiple token types, which drastically reduces the number of required blockchain operations and, consequently, the associated costs. ERC-1155 also introduces the concept of semi-fungibility, where a token can start as fungible and later become non-fungible based on its usage or context. This added versatility can make the standard suitable for assets with complex or unique lifecycles. Furthermore, the ERC-1155 standard retains compatibility with existing infrastructure like wallets and exchanges, that can interacts with it as they would with ERC-20 or ERC-721 tokens.

Mandatory Functions:

- `balanceOf`: Returns the balance of a specified token ID for a given address.

- `balanceOfBatch`: Returns the balances of multiple token IDs for multiple addresses in a single call.
- `safeTransferFrom`: Transfers a specified amount of a specified token ID from one address to another, ensuring the recipient is capable of receiving tokens.
- `safeBatchTransferFrom`: Transfers specified amounts of multiple token IDs from one address to another in a single transaction.
- `setApprovalForAll`: Enables or disables approval for a third party to manage all of the caller's tokens.
- `isApprovedForAll`: Returns whether a specified operator is approved to manage all of the assets of a specified owner.

Optional Functions:

- `uri`: Returns a URI pointing to metadata about a specified token ID. This URI can be used to provide details about the token, such as its name, symbol, and other attributes.

Events:

- `TransferSingle`: Emitted when a single token transfer occurs.
- `TransferBatch`: Emitted when multiple tokens are transferred in a batch.
- `ApprovalForAll`: Emitted when an operator is enabled or disabled for an owner.
- `URI`: Emitted when the URI for a token ID is set or updated.

Advantages

ERC-1155 has become a versatile standard for creating both fungible and non-fungible tokens on Ethereum, offering a hybrid approach that simplifies token management. The standard enables developers to represent a variety of assets, such as in-game items, fractionalized real-world assets, or financial instruments, all within a single smart contract. This versatility reduces complexity and improves efficiency.

The standard has also seen adoption in DeFi applications, where its ability to batch transfer tokens and handle multiple token types in one transaction brings significant gas savings. For instance, liquidity pool tokens or collateralized debt positions can be represented using ERC-1155, optimizing operational costs and management.

ERC-1155 tokens are simple to create, with user-friendly tools available to deploy fungible or non-fungible tokens. This ease of use lowers barriers to entry for developers and projects, facilitating rapid adoption and innovation. Additionally, ERC-1155's extensible nature allows for custom logic, making it adaptable to a wide range of use cases, including regulatory compliance or dynamic metadata for evolving assets.

Finally, ERC-1155 supports batch operations and safe transfers. Batch operations enable users to transfer multiple tokens of different types in a single transaction, reducing costs and improving efficiency. The standard also includes safeguards for safe transfers, minimizing the risk of accidentally losing tokens by sending them to incompatible addresses.

Disadvantages

Despite its versatility, ERC-1155 faces challenges that can impact its broader adoption and usability. One major drawback is its relative complexity compared to simpler standards like ERC-20 or ERC-721. The multi-token functionality and batch operations require a deeper understanding of the standard, which may deter some developers and projects.

Another limitation is the adoption rate. While ERC-1155 offers significant advantages, it hasn't yet achieved the widespread adoption and compatibility seen with ERC-20 and ERC-721. This limited adoption can result in reduced support from wallets, marketplaces, and DeFi protocols, restricting the utility of tokens created using the standard.

Interoperability can also be a challenge. Many existing platforms are built primarily for ERC-20 or ERC-721 tokens, which may result in incompatibilities or require additional development effort to properly integrate ERC-1155 tokens into those ecosystems. This can hinder seamless user experiences and discourage experimentation.

Finally, while ERC-1155 provides batch operations and cost savings, it may not always be the most efficient choice for applications that only require a single token type. In such cases, the added complexity of the standard may outweigh its benefits, making simpler standards like ERC-20 or ERC-721 more suitable.

Real-World Applications

- **Polytrade's RWA Marketplace [Invoices]:** Polytrade's RWA Marketplace was developed as a platform where investors can buy, sell, and manage real-world assets in a secure and user-friendly setting. The marketplace offers fractionalized assets, and thus benefits from increased liquidity and flexibility. Multiple asset classes are available, with the focus being on invoice financing. An expanded version of the ERC-1155 standard is used to tokenize the assets, incorporating a sub-entry to track ownership and facilitate their fractionalization. This sub-entry also enables additional features such as dividend distribution, voting rights, or access to asset-related information and updates.

ERC-1400: Security Token Standard

Ethereum Improvement Proposals: ERC-1400

ERC-1400 is a comprehensive token standard specifically designed for security tokens on the Ethereum blockchain and other EVM-compatible chains. It was introduced to address the unique needs of security tokens, combining various existing standards into a unified framework. The development of ERC-1400 was primarily driven by the recognition that traditional financial assets and securities could benefit significantly from blockchain technology, particularly in terms of transparency, efficiency, and regulatory compliance.

The standard was proposed by Polymath, a company focused on bringing traditional financial securities to the blockchain. Polymath's team, including notable contributors like Adam Dossa and Pablo Ruiz as well as the creator of the ERC-20 standard, Fabian Vogelsteller, played a pivotal role in the development and promotion of ERC-1400. Their aim was to create a token standard that could support the complex regulatory requirements of security tokens while maintaining the flexibility and interoperability of blockchain technology.

Key Features

While ERC-20 focuses on fungible tokens, ERC-1400 caters to non-fungible tokens representing securities. It introduces several new concepts on top of the ERC-20 standard:

- **Granular Control over Transfers**: ERC-1400 allows for enforcing compliance rules and investor restrictions on token transfers. This can be achieved through a system of certificates attached to the tokens, specifying ownership rights and transfer limitations. Imagine a scenario where only accredited investors can purchase a specific security token. ERC-1400 facilitates implementing such restrictions by embedding accreditation requirements within the token itself.
- **Document Management**: Facilitates associating legal and other relevant documents with the tokenized security. This improves transparency and simplifies regulatory compliance. For instance, an offering memorandum outlining the terms and conditions of a security token can be linked directly to the token, readily accessible to potential investors.
- **Gatekeeper Control**: Enables the implementation of access control mechanisms. Gatekeepers, typically designated third-party entities like brokerage firms or transfer agents, can approve or reject token transfers based on predefined rules. This adds an extra layer of security and ensures compliance with regulations.
- **Forced Transfers**: ERC-1400 allows for the forced transfer of tokens in specific situations, such as corporate actions like mergers or stock splits. This ensures a smooth process for corporate events that may involve changes in ownership.
- **Partial Fungibility**: While ERC-1400 primarily deals with non-fungible security tokens, it can also accommodate partially fungible tokens where specific classes or tranches of tokens may have different rights or restrictions. For instance, a company might issue different classes of security tokens with varying voting rights or dividend payouts. ERC-1400 can represent these distinctions within the token itself.

These features enhance the suitability of ERC-1400 for representing traditional financial instruments like stocks, bonds, and funds on the blockchain.

Mandatory Functions and Features:

- `Transfer Validity`: Ensures that a transfer is valid before it occurs and provides a reason for any failed transfer, crucial for compliance with regulatory requirements.
- `Forced Transfers:` Allows for forced transfers to comply with legal actions or recover lost funds.
- `Standard Events`: Issues and redemptions are tracked through standardized events, enhancing transparency.
- `Metadata Attachment`: Attaches metadata to token balances, such as shareholder rights or transfer restrictions.

- `Document Management`: Supports attaching and querying documents relevant to the security token, such as offering memorandums.

The complete interface with Mandatory Functions and Events is quite extensive, it can be found here: ERC-1400 Interface

Sub-Standards Under ERC-1400

- **ERC-1594: Core Security Token Standard**: Focuses on the essential functions for any security token, including transfer validity and off-chain data injection for regulatory compliance.
- **ERC-1410: Partially Fungible Token Standard**: Allows tokens to be divided into partitions with attached metadata, enabling functionalities like vesting and lock-up periods for different token segments.
- **ERC-1643: Document Management Standard**: Manages documents associated with the security tokens, such as legal agreements and investor communications, and ensures updates are accessible to token holders.
- **ERC-1644: Controller Token Operation Standard**: Grants controllers the ability to force transfers of tokens to comply with legal requirements or address security issues.

Advantages

ERC-1400 is a specialized token standard designed for security tokens that ensures compliance with legal and regulatory standards. It offers flexibility across different regulatory environments, allowing issuers to meet various jurisdictional requirements. A key feature is its robust investor protection mechanisms—including transfer restrictions and gatekeeper controls—which prevent unauthorized or non-compliant transactions. These safeguards are essential for security tokens where compliance and investor protection are crucial.

The standard streamlines compliance through built-in features that align with securities regulations, making it an attractive option for issuers looking to integrate security tokens into traditional financial systems. It also enhances liquidity through the Ethereum ecosystem—unlike tokens on private blockchains, ERC-1400 tokens can leverage Ethereum's established infrastructure for easier trading on compatible exchanges and wallets.

Beyond compliance and liquidity, ERC-1400 enables composability by allowing tokens to interact with other ERC-1400-compliant smart contracts, fostering innovative DeFi applications for security tokens. The standard also includes comprehensive document management features, enabling efficient handling and sharing of documentation for improved investor relations and regulatory reporting. These combined capabilities—compliance, liquidity, composability, and document management—make ERC-1400 an effective framework for security token issuance.

Disadvantages

ERC-1400, while designed to address the complexities of security token issuance and compliance, presents several challenges that can hinder its broader adoption. One significant drawback is its inherent complexity. The standard's extensive feature set, including transfer restrictions

and document management, often translates into higher development costs and extended implementation timelines. This complexity can be particularly burdensome for smaller projects or teams with limited technical resources, making ERC-1400 less accessible than simpler standards like ERC-20. This could deter the widespread adoption within the Ethereum ecosystem.

Additionally, ERC-1400 introduces off-chain dependencies for certain compliance features, such as transaction validation. This reliance on external processes and keys creates potential security vulnerabilities, as off-chain components may be more susceptible to breaches. These dependencies can undermine the security assurances that blockchain-based solutions typically provide.

Lastly, the partial fungibility of ERC-1400 tokens, which allows them to be divided into partitions with distinct rules, can complicate token management and user understanding. For investors and users accustomed to the simplicity of fully fungible tokens, this added complexity may act as a deterrent. These challenges collectively highlight the trade-offs involved in adopting ERC-1400 for security token offerings.

Real-World Applications

- **Polymath [Securities]**: Polymath uses ERC-1400 to tokenize equity and debt instruments. By issuing security tokens for equities and bonds, Polymath enables more efficient and transparent trading and management of these financial instruments. ERC-1400's features, such as forced transfers and metadata attachment, ensure regulatory compliance and facilitate corporate actions like dividends and interest payments.
- **Consensys Codefi [Securities]**: Consensys Codefi leverages ERC-1400 for issuance and management of tokenized financial assets that meet regulatory requirements. Their platform utilizes the standard's compliance features to tokenize traditional financial instruments while maintaining regulatory oversight. The granular control over transfers and document management capabilities of ERC-1400 enable Codefi to implement sophisticated compliance rules and automate corporate actions.

ERC-3643: The Compliance-Aware Token Standard

Ethereum Improvement Proposals: ERC-3643

ERC-3643, also known as T-Rex, is a token standard for Ethereum and other EVM-compatible blockchains that meets the strict requirements of compliance-driven industries. Created by Tokeny, it embeds regulatory compliance, identity management, and access control directly into token operations, offering a comprehensive framework for regulated digital assets like security tokens. Jean-Marc Seigneur and Olinga Taeed conceptualized this standard in 2021 to address the growing need for on-chain compliance in an evolving regulatory landscape.

The standard's significance is evident in its adoption—Tokeny has tokenized over $28 billion in assets using ERC-3643, demonstrating its effectiveness in high-stakes financial operations. As the first tokenization standard to complete the ERC process with community validation, its compliance-focused design makes it ideal for regulated industries.

ERC-3643 involves two primary entities: issuers and investors. Issuers deploy tokens and play a crucial role in managing compliance through identity systems like ONCHAINID, linking real-world identities to wallet addresses with KYC/AML verification. They may also administer smart contracts independently or via tokenization platforms. Investors maintain the system's integrity through their onchain identity, which safeguards privacy by controlling access to private off-chain data required for smart contract executions. This framework ensures secure and compliant token issuance and trading while addressing the needs of regulated industries.

Key Features

ERC-3643 focuses on embedding compliance and identity management into token operations, ensuring that tokens can only be held and transferred by verified entities. The standard introduces a set of core functions and capabilities that cater to regulatory and business requirements, making it ideal for use cases where compliance is complex and of paramount importance.

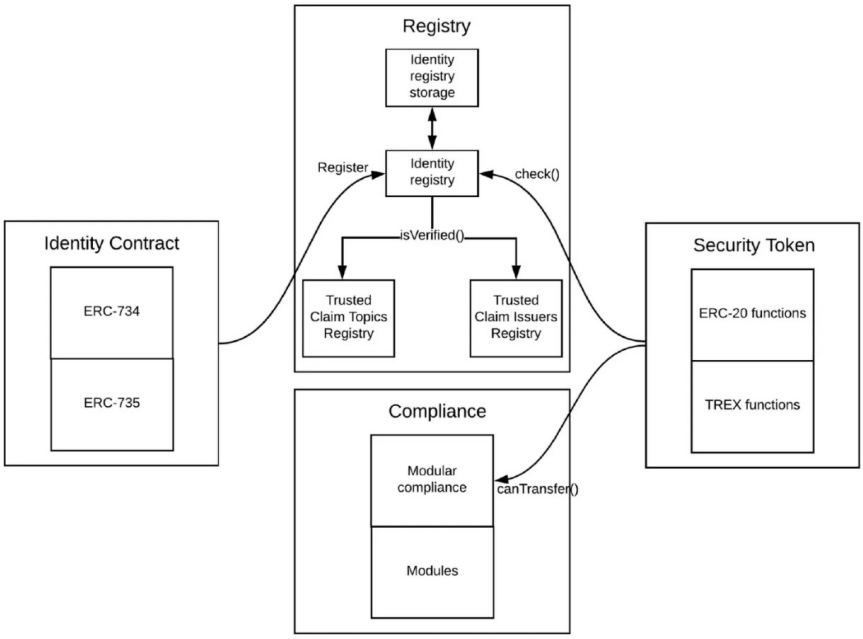


Figure 1: T-REX Components (Smart Contracts Library)
(Source: Tokeny, 2023, p. 13) [9]

ERC-3643's security tokens are extensions to the ERC-20 standard, with additional custom logic. This custom logic interacts with a variety of periphery contracts, that enables the standard's more advanced functionality:

- **Identities**: Identities are created using the ERC-734 and ERC-735 standards, creating a pseudo anonymous ONCHAINID, linked to the offchain identity of a user. This identity is then stored in an identity registry, where claims by trusted issuers can be used to verify the identity is valid. Valid identities can be used by the security token to limit transfers to allowed parties.
- **Compliance**: Compliance is managed through a set of optional modules, which limit transfers to certain conditions, such as users in certain countries or maximum token balances that can be held. This modular approach is flexible enough to accommodate a wide range of use cases, with

custom modules allowing for any custom restriction to be applied on security token transfers.

Mandatory Functions and Features:

- `Core token logic`: Apart from the core logic belonging to ERC-20, ERC-3463 contains logic for freezing addresses, pausing the token contract, performing forced transfers, and recovering tokens from lost wallets. The standard also contains functions for interacting with the periphery contracts, such as compliance modules or the identity registry. The core logic also contains batch functions for most functionality, allowing for more efficient operations.
- `Identity`: The Identity registry, as it's name implies, is used for verifying and managing the identities of investors, and their countries. Identities are associated to claims made for them by trusted issuers, which can include any necessary custom information. Claims and trusted issuers are each managed by their respective registries.
- `Compliance`: Compliance is managed through optional compliance modules, which implement logic restricting token transfers. This is done through a read-only function that checks if a transfer is compliant, with any custom checks needed. Compliance contracts can be bound or unbounded to tokens as needed.

Optional Modules:

Modules are custom and optional restrictions that can be applied to security token transfers. Some existing examples are as follows:

- `CountryAllowModule`: This module allows for explicit allowance user's countries by the compliance entities, restricting interactions to only permissioned ones. The associated country for a given investor is stored in the identity registry.
- `ExchangeMonthlyLimitsModule`: This module is designed to set a monthly limit for token transfers.
- `TimeTransfersLimitsModule`: This modules limits token transfers to specific timeframes, often replicating restrictions imposed by traditional finance.
- `TransferRestrictModule`: This module defines an allow list to be implemented, allowing for granular control of which users can transfer tokens.

Advantages

ERC-3643 stands out as a pivotal standard for compliance-aware digital assets, offering distinct advantages for regulated industries. Its core functionality embeds compliance mechanisms directly into the token architecture, enforcing regulatory requirements like identity verification and transfer restrictions. This design makes it ideal for security tokens and other regulated assets that require strict legal compliance.

The standard's integrated identity management system is a key differentiator. Through mandatory verification processes, only authorized participants can interact with the tokens, preventing unauthorized transactions and fraud. This level of control creates increased trust and security in tokenized ecosystems—setting ERC-3643 apart from general-purpose tokenization standards.

The standard's programmable compliance rules offer crucial adaptability, letting developers customize it for different regulatory frameworks. This flexibility is essential for global asset tokenization, where legal requirements vary across markets. ERC-3643 maintains compliance

across jurisdictions, making it uniquely suited for international trading.

Disadvantages

While ERC-3643 offers strong compliance mechanisms, it also introduces notable technical challenges. Implementing ERC-3643 demands a comprehensive understanding of regulatory frameworks, which can increase development complexity and associated costs. This requirement may deter smaller projects or developers without expertise in legal and compliance domains.

The need for continuous updates to remain compliant with evolving regulations adds operational overhead. Tokens deployed under ERC-3643 must be adaptable to shifting legal requirements, which can create ongoing maintenance burdens, especially for multi-jurisdictional projects with diverse regulatory landscapes.

Finally, the strict regulatory alignment of ERC-3643 can limit its interoperability with decentralized applications and platforms that prioritize composability. The standard's compliance-centric architecture may restrict its integration into broader DeFi ecosystems, limiting its applicability for projects seeking high flexibility and seamless interactions with the secondary market.

Real-World Applications

- **Tokeny Solutions [Security Tokens]**: Tokeny Solutions implements ERC-3643 to issue compliant security tokens for enterprises tokenizing equity and debt assets. The standard's built-in compliance features ensure adherence to regulations across multiple jurisdictions, facilitating seamless cross-border investments. Through token-level identity verification, Tokeny limits ownership and transfers to verified investors, protecting against unauthorized access and regulatory violations.
- **Defactor [Asset-Backed Financing Tokens]**: Defactor employs ERC-3643 to tokenize real-world assets, transforming traditional asset-backed financing into a transparent and efficient blockchain-based process. By incorporating compliance mechanisms within the token architecture, Defactor ensures alignment with regulatory requirements across different jurisdictions. The standard's identity verification feature restricts token interactions to verified participants, reducing risks related to fraud and unauthorized transactions.

CMTAT: The Swiss-Compliant Standard

CMTAT: Functional specifications for the Swiss law compliant tokenization of securities.

The CMTA token standard, also know as CMTAT, is a financial instrument tokenization standard designed specifically to comply with Swiss law. It is a framework that defines the logic required for tokenizing debt, equity, structured products, and other financial instruments. CMTAT was initially developed by a working group of CMTA's Technical Committee. The Capital Markets and Technology Association is an independent association formed by members from Switzerland's financial, technological and legal sectors with the objective to create common standards around operating securities using blockchain technology. The CMTAT standard is blockchain agnostic,

meaning it defines a set of functionalities a token should follow without specifying the network it should operate on. Reference implementations of this specification currently exist for the Ethereum and Tezos blockchains.

Key Features

CMTAT is designed as a set of modules that can be combined to enable specific functionality, with a mandatory base module. This base module contains the logic for the core fungible token logic, while the optional modules define more specialized logic for snapshots, validation, and authorization. While all the functions in the modules are mandatory to implement for included modules, some attributes in the base module are optional, a majority of them revolving around debt securities. While not part of the standard, it's also possible to add custom modules to a CMTAT token. This might make sense when tokenizing assets which require additional functionality.

Base Module:
The CMTAT's base module is mandatory, and contains all the essential functionalities that enable the token to be fungible and issued on a blockchain network, in addition to some administrative functionalities.

- `TotalSupply`: Returns the current total number of tokens in circulation.
- `BalanceOf`: Returns the balance of tokens held by a specified address.
- `Transfer`: Transfers a specified number of tokens for a user to a specified address.
- `Mint`: Issues a specified number of tokens to a given address.
- `Burn`: Destroys a specified number of tokens from a given address.
- `Pause`: Prevents all token transfers until `UnPause` is called.
- `UnPause`: Restores the token transfer functionality previously blocked by `Pause`.
- `Kill`: Permanently prevents any token transfers or any other operation from being carried out, effectively destroying the token itself.

Snapshot Module:
This mandatory modules allows for taking snapshots, keeping track of balances at a certain point in time. These snapshots can then be used to carry out corporate actions onchain, such as dividend or interest payments.

- `ScheduleSnapshot`: Schedules a snapshot to be taken at a point in time in the future, which cannot be set before any already pending scheduled snapshots.
- `RescheduleSnapshot`: Reschedules a snapshot to be taken at a point in time in the future. It cannot be reschedule to happen before or after any other pending snapshot.
- `UnscheduleSnapshot`: Cancels a snapshot that was to be taken at a point in time in the future. Only the latest pending snapshot can be canceled.
- `SnapshotTime`: Returns the time a scheduled snapshot will occur.
- `SnapshotTotalSupply`: Returns the total number of tokens in circulation for a given snapshot at creation time.
- `SnapshotBalanceOf`: Returns the balance of tokens held by a specified address for a given snapshot at creation time.

Validation Module:
This optional module provides functionality to apply legal restrictions to the transfers of the token, limiting the scope of entities that may hold them.

- `ValidateTransfer`: Sends a request for validation for a particular token transfer, given the sender and recipient addresses, and the amount to be transferred.
- `SetRuleEngine`: Designates a set of rules to be enforced by the **`ValidateTransfer`** function, defined in a separate contract.

Authorization Module:
This optional module allows for implementing a role-based access control system for the token, instead of only having issuers and users. The issuer can use this module to assign responsibilities and authorizations in the way they prefer.
- `GrantRole`: Grants a role to a specified address.
- `RevokeRole`: Revokes a role from a specified address.
- `HasRole`: Returns whether a given address has been granted a specified role.

Advantages

When compared to other tokenization standards, CMTAT has some unique advantages. The main one is how it is tailored and optimized for Swiss law. Legal requirements have been carefully translated into the technical requirements of the standard, making it incredibly easy to use when tokenizing assets within Switzerland. Furthermore, while not tailored to other jurisdictions, CMTAT is flexible and extensible enough to be able to accommodate the requirements of other legal systems, using custom modules.

Modules can be used to extend the functionality of CMTAT tokens, better adapting them to specific use cases. This flexibility allows for tokenizing all kinds of different assets. That being said the flexibility does not rely solely on modules, it also stems from the standard only defining functional requirements. Not being bound to a technical specification, the CMTAT standard can be implemented using different approaches or technologies that are suitable for the intended use case.

The standard lacking a technical specification means it is not tied to a blockchain network or technology, such as Ethereum. While an Ethereum reference implementation of CMTAT for Ethereum and EVM networks exists, it based on the standard, not part of it. This implementation is based on the ERC-20 standard and extends it, leveraging the existing infrastructure and composability present in EVM networks. Another reference implementation exists for Tezos, and more can be developed for different blockchains in the future as long as they follow the functional requirements of the standard. The standard can be implemented differently for each network, taking advantage of their unique strengths.

CMTAT is managed by CMTA, which is not a single company, but a not-for-profit association with multiple contributors, including Lenz & Staehelin, Swissquote Bank, Temenos Group, and others. This shared participation make it unlikely the standard will be abandoned or tied to the interests of a single company.

Disadvantages

While CMTAT has very clear advantages for some use cases, some of it's features might make

alternative tokenization standards preferable in some situations. It's focus on Switzerland and Swiss law might limit adoption in other jurisdictions. While it can be extended and made compliant with other regulatory environments, this can take custom modules and a significant effort, while still having "leftovers" that are only applicable or relevant to Swiss law. Other less opinionated or neutral standards might be preferred for such cases.

Other token standards include functionalities such as forced transfers, onchain identity management, or even partial fungible token support. While CMTAT can potentially support these features making use of custom modules, other token standards support them natively, not requiring any extra work to implement. Not having these included natively in the standard also means if such features are developed for CMTAT, different entities might develop and use them differently, breaking standardization and composability for such features. This could be mitigated if CMTA adds these modules to the standard as optional, similar to the current validation and authorization modules.

In a similar manner, the standard not being limited to EVM chains like other ERC token standards can also be a disadvantage. Not being limited by a specific technology is generally a good thing, but that flexibility comes at a cost. Other token standards generally have gone through the Ethereum Request for Comments (ERC) process, which involves the Ethereum community for feedback and improvements. This helps find issues the original authors might have missed, and tweaks standards to be the most compatible with the wider Ethereum ecosystem. The CMTA includes actors with knowledge and experience in the ecosystem, especially in relation to Swiss regulation, but the resulting EVM implementation has not been vetted by the Ethereum community.

Real-World Applications

- **Magic Tomato SA** [Bons de Participation]: Magic Tomato SA, an online grocery platform, used CMTAT to offer non-voting shares to it's community. By opening up their governance, they allowed customers, suppliers and supporters to participate financially in the development of the company.
- **Cité Gestion SA** [Equities]: CMTAT was used by Cité Gestion SA, a Swiss bank and wealth manager, in order to offer their shares to investors. One of the benefits of the offering was having a real-time and accurate view of their shareholder base online. Investors also benefited from legal certainty for share transfers, due to the evidence of ownership provided by the blockchain.
- **UBS** [Bonds]: Multinational investment bank and financial services company UBS used CMTAT in order to issue a digital bond. This is notable since the bond was natively-issued instead of tokenized, and as such it was the first of its kind to be issued on a public blockchain (Ethereum).
- **Credit Suisse, Pictet and Vontobel** [Investment Products]: Credit Suisse, Pictet and Vontobel issued tokenized investment products, which were then traded against Swiss francs on BX Swiss, a FINMA regulated Swiss securities exchange. This proof of concept transaction, which was carried out in a matter of hours as opposed to days, highlights the efficiency of issuing, trading, and settling tokenized assets on public blockchains.

Honorable mentions: ERC-1450 & ERC-2980

Not all token standards are successfully adopted, like in the case of the ERC-1450 and ERC-2980. Both of these proposed token standards have been abandoned and marked as stagnant in the Ethereum Request for Comment process (ERC). While not currently in use, these standards are interesting because of their similarity with CMTAT's jurisdiction specific philosophy, and regulator-first approach. ERC-1450 and ERC-2980 were proposed to appeal to US and Swiss regulators respectively, with the objective of standardizing the tokenized assets to be compliant with the laws in their jurisdiction.

ERC-1450: A compatible security token for issuing and trading SEC-compliant securities

Ethereum Improvement Proposals: ERC-1450

ERC-1450 was proposed in 2018 by Start Engine as the "LDGRToken", a standard for creating digital stock certificates. It facilitates the recording of ownership and transfer of securities sold in compliance with the US Securities Act Regulations CF, D and A. This standard made use of SEC registered transfer agents to act as record keepers, with an Issuer role. The Issuer was the only role allowed to mint, burn, or transfer tokens. The standard did not receive traction, perhaps due to it's limited utility due to disabled token transfers, acting more as an onchain visualization.

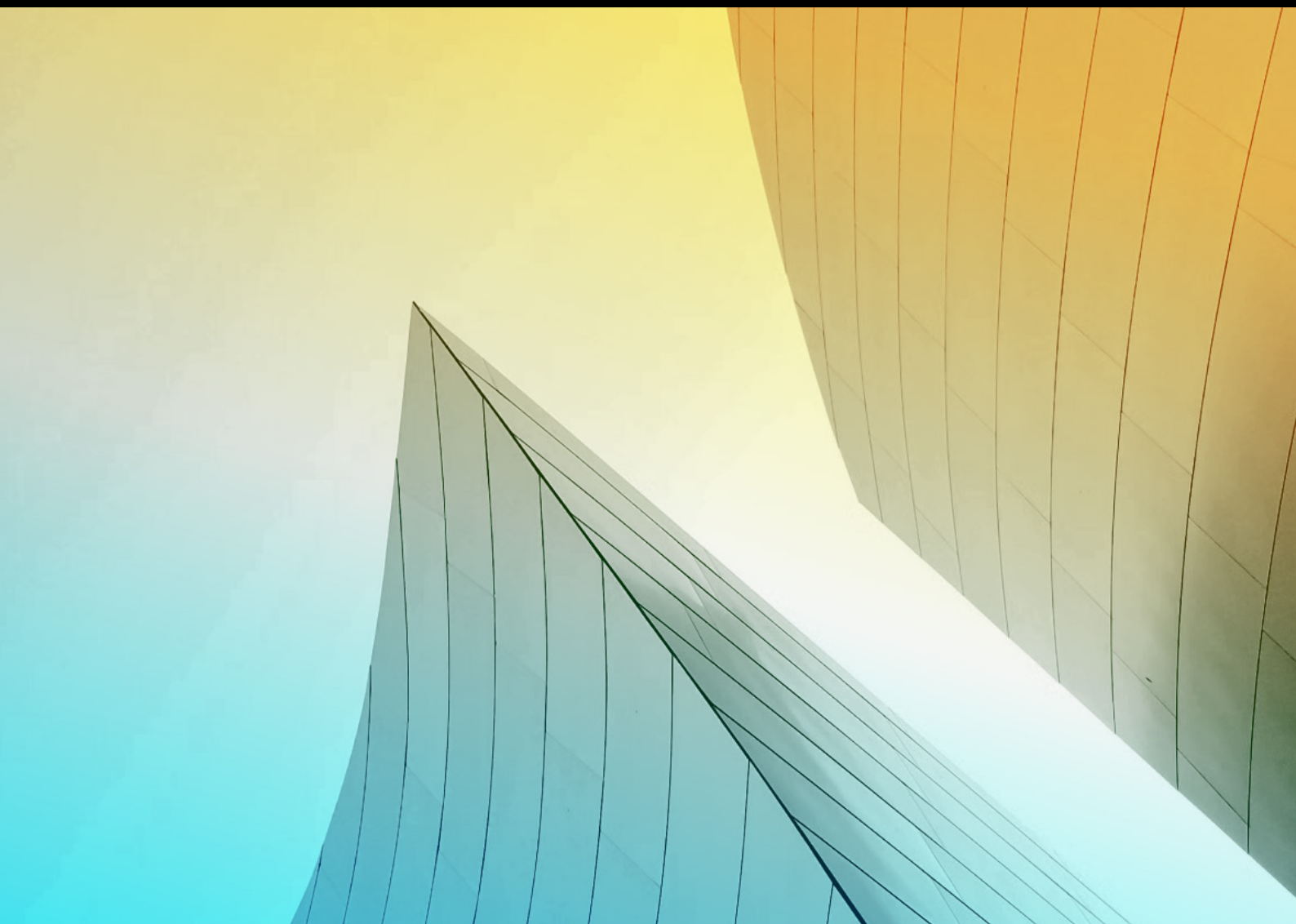
ERC-2980: Swiss Compliant Asset Token

Ethereum Improvement Proposals: ERC-2980

ERC-2980 was proposed in 2020, motivated by FINMA (Swiss Financial Market Supervisory Authority) explicitly stating in its 2018 ICO guidance that asset tokens are analogous to and can economically represent shares, bonds, or derivatives. This standard attempted to follow all relevant Swiss laws, while also being compatible with the EU's European Jurisdiction. It did so by implementing Whitelists and Frozenlists, Revoke and Reassign functionality, and an Issuer role. While the standard did not gain traction, it feels like CMTAT is its spiritual successor, incorporating many of the same ideas and goals.

03

Conclusion



Tokenization of RWAs is revolutionizing the financial landscape, unlocking efficiency, liquidity, and global accessibility. However, its growth is hindered by several challenges, primarily around regulatory environments, but also interoperability, and privacy. Standards like ERC-1400 and ERC-3643 provide foundational frameworks for tokenizing regulated assets, embedding compliance mechanisms and identity verification directly into token operations. They face limitations such as the complexity of integrating with existing systems, insufficient interoperability between protocols and blockchains, and the challenge of adapting to evolving regulatory demands. These factors can hinder seamless implementation, reduce efficiency, and restrict scalability by increasing the time and resources required to deploy and manage tokenized assets effectively.

The Markets in Crypto-Assets Regulation (MiCAR) establishes a comprehensive regulatory framework for crypto assets within the European Economic Area (EEA). It focuses on regulating the roles of issuers and Crypto Asset Service Providers (CASPs) by classifying assets into categories like e-money tokens (EMTs), asset-referenced tokens (ARTs), and other crypto assets. MiCAR defines specific requirements for each category, ensuring transparency, consumer protection, and governance. While the regulation does not seek to directly govern technical token standards like ERC-20 or ERC-721, these standards play a critical role in enabling issuers and service providers to implement the processes and mechanisms required for regulatory compliance, such as identity verification, transaction tracking, and adherence to governance protocols. There is a growing alignment between token standards and regulatory frameworks, particularly within European markets. This is seen with the development of the CMTAT standard, which ensures compliance with Swiss government regulations, defining the logic required for tokenizing debt, equity, structured products and other financial products.

Key challenges in tokenizing RWAs persist, particularly in the areas of regulation, interoperability and privacy. Regulations are crucial to study for token standards as they directly influence the design, adoption, and interoperability of these standards, ensuring legal compliance has become the need of the hour for the development of an efficient digital assets ecosystem. It is vital for regulations to focus on the nature and structure of the underlying asset rather than the token standard or blockchain protocol, emphasizing compliance with what the token represents rather than the technology used to create it. On the other hand, fragmented blockchain networks and isolated permissioned systems complicate cross-chain asset transfers and the creation of secondary markets, limiting liquidity. On the privacy front, institutional adoption of public blockchains is gaining traction due to advancements like zero-knowledge proofs (ZKPs) and programmable privacy frameworks, ensuring data confidentiality while maintaining compliance. Addressing these challenges is essential to unlock tokenization's potential fully.

Looking ahead, the development of universal token standards that align with regulatory frameworks like MiCAR while supporting interoperability and privacy is critical. Collaborative industry efforts, innovative cross-chain protocols, and privacy-enhancing technologies can pave the way for broader adoption, fostering a more efficient, transparent, and inclusive digital asset ecosystem in general and tokenized real world assets in particular.

04

References

[1] Boston Consulting Group & ADDX. (2022). Relevance of on-chain asset tokenization in 'crypto winter.' Boston Consulting Group.

[2] Circle Internet Financial LLC. (2024). USDC White Paper 2024. Circle.

[3] European Securities and Markets Authority (ESMA). (2024). MiFID II ANNEX I, Section C. European Commission.

[4] European Securities and Markets Authority (ESMA). (2024). Consultation paper on the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments. ESMA.

[5] Boston Consulting Group. (2024). Bridging the gap between capital markets and digital assets. BCG.

[6] Société Générale Insurance Solutions (SGIS). (2024). SGIS Smart Cash: A liquid and secured solution providing an attractive yield. Société Générale.

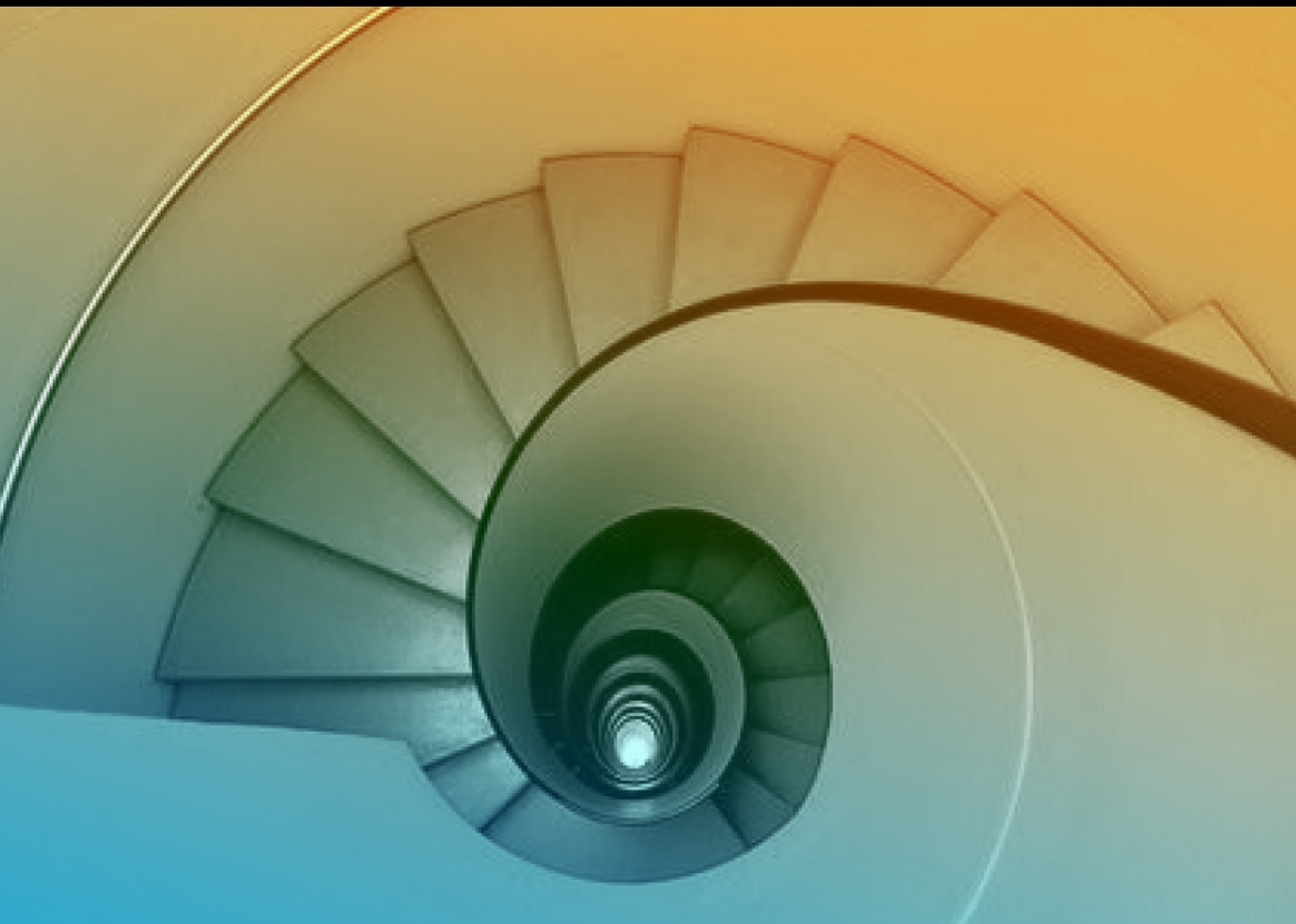
[7] SG Forge. (2024). Structured Products: Professional investors can now invest in structured products registered on public blockchains. Société Générale.

[8] ERC3643 Association. (2024). ERC3643 Association leads RWA tokenization standardization with 78 industry leaders. ERC3643.

[9] Tokeny. (2023). ERC-3643: T-REX - The Institutional-Grade Token Standard for Permissioned Tokens (Version 4).

05

Glossary



AML (Anti-Money Laundering): Regulations and procedures designed to prevent the conversion of illegally obtained money into legitimate assets.

ARTs (Asset-referenced tokens): Tokens that maintain their value by referring to multiple currencies, commodities, or other crypto-assets.

Batch Transactions: A mechanism that allows multiple token transfers or operations to occur within a single transaction, improving efficiency and reducing gas costs.

Blockchain Explorer: A web tool that allows users to view and analyze blockchain transactions, addresses, and other network data.

Burning: The process of permanently removing tokens from circulation.

CASPs (Crypto Asset Service Providers): Entities that provide services related to crypto assets, such as trading, custody, or exchange services.

Cold Storage: A method of keeping cryptocurrency offline to reduce the risk of hacking or theft.

Cross-chain: Referring to interactions or transfers between different blockchain networks.

Custody Solution: Services or systems that securely store and manage digital assets on behalf of users.

DAO (Decentralized Autonomous Organization): Organizations represented by rules encoded as computer programs, transparent and controlled by network participants.

DeFi (Decentralized Finance): Financial services and products built on blockchain technology that operate without traditional intermediaries.

EMTs (E-money tokens): Digital tokens that aim to maintain a stable value by referring to a single fiat currency.

ERC-1400: A security token standard designed for compliance with regulatory requirements, incorporating features like transfer restrictions and document management.

ERC-20: A widely used Ethereum standard for fungible tokens, defining functions like transfer, approve, and balanceOf for interoperability.

ERC-3643 (T-Rex): A compliance-focused token standard enabling identity management and regulatory adherence for digital assets.

ERC-721: A standard for non-fungible tokens (NFTs) representing unique assets, such as art, real estate, or collectibles.

ERC-1155: A multi-token standard supporting fungible and non-fungible tokens within a single smart contract.

EVM (Ethereum Virtual Machine): The runtime environment for smart contracts on Ethereum.

Fungible Tokens: Digital tokens that are interchangeable with each other, like cryptocurrencies

where each unit has the same value.

Gas Fees: Transaction fees paid to network validators for processing and validating blockchain transactions.

Hard Fork: A radical change to a blockchain's protocol that makes previously invalid blocks/transactions valid (or vice-versa).

Interoperability: The ability of different blockchain systems and tokens to work together and exchange information.

KYC (Know Your Customer): The process of verifying the identity of customers, often required for regulatory compliance in financial services.

Layer 2: Scaling solutions built on top of existing blockchains to improve transaction speed and reduce costs.

Minting: The process of creating new tokens on a blockchain.

NFT (Non-Fungible Token): Unique digital tokens that represent ownership of specific assets or items.

Oracle: Systems that enable blockchain networks to access external data for smart contract execution.

Permissioned Systems: Blockchain networks where only approved participants can validate transactions or access the network.

Programmability: The capability of blockchain tokens to execute custom logic or enforce rules through smart contracts.

Secondary Markets: Trading venues where previously issued tokens can be bought and sold between parties.

Smart Contracts: Self-executing contracts with terms directly written into code that automatically enforce and execute agreements.

Stablecoins: Cryptocurrencies designed to maintain a stable value, usually pegged to a fiat currency or other assets.

Tokenization: The process of converting real-world rights or assets into digital tokens on blockchain networks.

Wallet: Software or hardware that stores private keys and allows users to send and receive cryptocurrency.

Whitelist: A list of approved addresses or entities that are permitted to interact with a smart contract or token.

Zero-Knowledge Proofs (ZKPs): Cryptographic methods that allow one party to prove to another that a statement is true without revealing any specific information about the proof.

06

About us

Nethermind

Nethermind is a blockchain research and software engineering company empowering enterprises and developers worldwide to work with and build on decentralized systems.

Our work touches every part of the blockchain ecosystem, from fundamental cryptography research through security to application-layer protocol development. As a core contributor to the development of Ethereum and active builders of the Starknet ecosystem, we leverage our expertise to provide strategic support to our institutional and enterprise partners in blockchain, digital assets, and DeFi.

PwC Germany

Build trust in society, solve important problems.

When it comes to auditing and advisory, PwC supports clients of all industry fields to reach their goals. We advise corporations as well as family-owned companies, industry- and service companies, global players and local heroes, the public sector, organizations and NGOs. With our know-how and our expertise, around 600 partners and more than 13,000 experts in 21 locations in Germany support our clients in terms of finding solutions for complex questions in a world changing rapidly – in line with our purpose statement “Build trust in society, solve important problems”.

Authors

Philipp Gretz
Manager - Financial Services Transformation, Digital Assets & Crypto
philipp.gretz@pwc.com

Dimitri Gross
Director - Financial Services Transformation, Digital Assets & Crypto
dimitri.gross@pwc.com

Eric Marti Haynes
Blockchain Engineer & Tokenization Tech Lead
eric@nethermind.io

Yehia Tarek
Blockchain & Tokenization Engineer
yehia@nethermind.io

Andrei Toma
Blockchain & Tokenization Engineer
andrei@nethermind.io

Aneesha Chitgupi
Tokenization Research Intern
aneesha.chitgupi@nethermind.io

Tomasz Kurowski
Head of DeFi & Enterprise Business
tomasz.kurowski@nethermind.io

Acknowledgements:
The authors extend their sincere appreciation to Jonas Müller, Constantin Schreiber, Ilham El Bouloumi, Melannie Manrique, and Julia Laganowska for their significant contributions to this work.

Let's build a compliant and innovative future **together.**

www.nethermind.io

www.pwc.de