IRJEMS International Research Journal of Economics and Management Studies
Published by Eternal Scientific Publications
ISSN: 2583 – 5238 / Volume 4 Issue 8 August 2025 / Pg. No: 23-33
Paper Id: IRJEMS-V4I8P104, Doi: 10.56472/25835238/IRJEMS-V4I8P104

Original Article

Security Token Standards for Institutional Adoption of Tokenized Funds

[1]Vittal Jadhav
[1]Akkodis, Inc Department: Technical Delivery Management.

Received Date: 06 July 2025 Revised Date: 23 July 2025 Accepted Date: 26 July 2025 Published Date: 03 August 2025

***Abstract**: The future of asset management, Tokenized funds, is an emerging digital analog of conventional types of investment instruments represented on a blockchain. The effectiveness of its success, particularly in institutional settings, depends largely on the maturity and core stability of the underlying cleansing token standards that ensure compliance, governance, and operational integrity. In this paper, the dynamic nature of standards such as ERC-1400, ERC-3643, CMTAT, and new protocols in the ecosystem is discussed. We examine how these standards address the primary institutional needs of KYC/AML compliance, including restrictions related to asset transfer, identity management, and auditability, both in terms of financial instrument structuring and governance. In addition to the technical one, the paper explores barriers institutions have to using tokenized funds, including regulatory uncertainty and cross-border compliance, as well as custody infrastructure and examines how the modern standards solve or fail to solve these aspects. We review each of the standards using a structured comparison matrix, with a focus on fundamental institutional standards. We also point out how future development can proceed, such as through central banks, the development of new cryptographic technologies such as zero-knowledge proofs, and harmonization between frameworks in jurisdictions and chains. According to our observations, none of the existing standards fully meet the institutional requirements at present, but the alignment of new protocols, regulatory guidance, and solutions to interoperability may trigger the broad-based implementation of tokenized finance. Such a transformation will be anchored in security token standards, which will become the linking tissue between legal compliance and programmable financial infrastructure.*

***Keywords**: Security tokens, tokenized funds, ERC-1400, ERC-3643, CMTAT, KYC/AML.*

I. INTRODUCTION

Blockchain technology and digitalizing traditional assets have produced a massive turnaround in the financial industry. One of the most potential is the tokenization of investment funds, whose ownership rights are expressed in the form of programmable digital tokens that operate on a distributed ledger. Tokenized funds have a range of benefits, such as making it possible to have fractional ownership, achieve settlement, lower management expenses, and greater liquidity via immediate secondary markets. [1-3] These advantages have opened the interests of diverse market players, such as fintech startups, to large financial institutions. However, despite the promising technology, institutional adoption is rather sluggish. Among the most important of them is the absence of generally accepted standards that guarantee compliance, interoperability, and legal status of tokenized securities.

Security tokens are digital pieces of classic financial instruments (equity, debt, or fund units) and under regulations, they have to be compliant with the standards and regulations, and they should follow strict compliance protocols. Security tokens, unlike utility tokens or cryptocurrencies, need to integrate identity verification and limit the transferability with lockup periods and record keeping, complying with securities legislation. This has prompted the introduction of specialized token standards designed to serve institutional applications. ERC-1400 and ERC-3643 (previously known as T-REX) standards have been developed, which enable the integration of compliance logic into the smart contract layer of the token. The standards allow functions inherent in whitelisting, role-based access control, partitioned ownership, and audit trails, all features that are essential to institutional-level digital assets.

The significance of security token specifications cannot be overestimated. Without standardized procedures, issuers, custodians, exchanges, and regulators encounter a fragmented network of infrastructures, not those that can drive scale, but riddled with legal and operational risks. To enable tokenized funds to take off in the mainstream, there needs to be a unified framework to support cross-platform compatibility, regulatory adherence and risk protection of investors. In this paper, we will examine the existing security token standards and relate technical and regulatory characteristics and investigate how they can enable tokenized funds to be adopted on an institutional basis. In analyzing both current implementations and future advances, it would be prudent to first note the underlying importance of standards in facilitating the next generation of compliant, efficient, scalable financial instruments.

II. FUNDAMENTALS OF TOKENIZED FUNDS AND SECURITY TOKENS

A) Understanding Tokenization in Asset Management

Tokenization is the presentation of an actual asset, e.g. real estate, equities, or units of an investment fund, in digital form in a blockchain or distributed ledger system. The issuance of security tokens representing the shares of digital funds would be possible through tokenization in a context of asset management; the investors would be able to store digital securities and transfer the right to possession with the help of the blockchain infrastructure. [4-7] The process has great gains, about transparency, efficiencies in transactions and the cost. Conventional portfolio frameworks are typically subject to intermediaries, have slow settlement times, and incur cumbersome administrative costs. In contrast, using tokenized funds provides settling the balance in a matter of seconds, automatized AML checks and availability worldwide. Fractional ownership also makes available cash that was fragmented in the hands of wealthy individuals or entities. Notably, it is not a tokenization which alters the legal or economic identity of the asset: it is the improvement in representation and management of such an asset provided by programmable, blockchain-based technologies.

B) Institutional Perspectives on Security Tokens

From an institutional standpoint, security tokens offer a significant value opportunity, but also present questions regarding regulatory compliance, custodianship, and integration. Institutional investors, such as banks, asset managers, and pension funds, require security tokens to meet the stringent criteria of legal enforceability, identity management, and risk control. Institutions cannot purchase tokens that would be subject to the securities laws as retail investors can, insofar as institutions need to make sure that the tokens they deal with are subject to recognized securities laws and can be combined with existing back-office infrastructure, including custodians, transfer agents, and compliance systems. Security tokens may also offer programmable functionalities, such as automatic dividend payments, continuous cap table updates, and built-in barriers to transferability. However, institutions are wary of non-standardized or inadequately governed token formats that may create regulatory risks or interoperability issues. Therefore, the use of security tokens by structures is directly connected to the maturity of token standards, regulation and custodianship services.

C) Compliance-By-Design: Embedding Legal Rules in Tokens

The ability to integrate legal and regulatory demands directly into the token smart contract is one of the defining features of security tokens. It is a concept (compliance-by-design) that enables issuers and regulators to impose rules such as KYC (Know Your Customer), AML (Anti-Money Laundering), accredited investor status, and jurisdictional restrictions in a programmatic manner. Standards such as ERC-1400 and ERC-3643 have been established based on this principle. Such standards can enable tokens to incorporate a layer of role-based permissions, transfer validation, and partitioned ownership, allowing issuers to choose with whom the token is allowed to be held or traded and under what compliance standards. Such functionality not only minimizes the middleman but also allows real-time regulatory monitoring and auditing. Compliance by design is crucial to ensure that the tokenized securities are not void in terms of their legality and that institutions are confident in the quality and authenticity of the financial instruments based on the tokens. As regulations continue to change, the institution of digital assets will centre on tokens that natively offer flexible and transparent compliance structures.

D) Custody and Settlement in Tokenized Asset Ecosystems

Custody and settlement are both important elements of any financial infrastructure, and the transfer of tokenized assets ecosystems, these operations are redefining themselves with the help of blockchain technology. Traditional finance has centralized institutions that offer custody of assets to clients, such as banks and custodians that manage client assets, settle transactions and are compliant with regulations. In the tokenized world, custody is handled by the custodians of digital assets, who can be centralized custodians, or they can use decentralized self-custody means such as wallets with control of the key of said wallet. To facilitate institutional adoption, digital asset custodians regulated to acceptable standards are necessary, including, but not exclusive: secure storage, insurance, and integration with compliance products. Tokenized ecosystems can settle almost instantly, and atomically, i.e., transfer of property and payment occurs on-chain simultaneously, often in a single transaction, lowering counterparty risk and operational latency. Nevertheless, connecting legacy settlement systems with blockchain networks remains a challenge; however, strong interoperability models and regulatory direction are necessary. Ultimately, the future of tokenized funds hinges on the advancement of institutional-grade custody and settlement infrastructure that meets the security, legal, and operational requirements demanded by the financial sector.

E) Jurisdictional Compliance and Cross-Border Challenges

The digital assets which are tokenized operate on the global digital platform and are subject to the domestic security regulations and laws. This creates a complex landscape as far as cross boundary issuance, trading and holding tokenized funds is concerned. Jurisdictional compliances deal with the issue of compliance with laws and regulations of every jurisdiction where the token is issued or sold. Differences in the definitions of securities, investors who are allowed to participate and conditions of disclosure of requirements and taxation are some of the major aspects that raise serious legal concerns to international acceptance. As an example, a SEC compliant tokenized fund in Reg D could not be permitted to make a public offer under either the EU MiFID II or the UK FCA. Also, the regulations that assist in data privacy may interfere with processing of data and storing of the data by investors on the chain e.g., GDPR. The international questions of this sort brought up the significance of the token standards that would enable the jurisdiction-specific differing rules, and regulatory convergence and the concertation of countries to provide international facilities of the tokenized instruments.

F) Risks and Limitations of Tokenized Instruments

Although there are possible advantages of tokenized instruments, there are also multiple risks and drawbacks that should be overcome to be trusted by institutions. Technological risks encompass aspects such as weaknesses in smart contracts, the stability of the blockchain network, and security threats to wallets and custodians. Legal ambiguities persist regarding the enforceability of smart contracts, proprietary rights, and remedies in the event of. Investor confidence can also be influenced by market risks, including low liquidity, transparency in valuations and exposure to counterparty risks. In addition, an unstable presence of universal standards might lead to incompatibility and disintegrated ecosystems. Regulatory arbitrage can undermine the long-term stability and credibility of tokenized markets, particularly when issuers exploit weak jurisdictions. Compliance breaches and damage to reputation can result from operational risks, such as mistakes in the token issuance process, governance issues, or flawed KYC/AML protocols. Although many of these issues are addressed by improvements in token standards, institutional uptake will require a sufficiently elaborate legal, technical, and operational framework that guarantees security, compliance, and investor protection on a large scale.

III. SECURITY TOKEN STANDARDS: A COMPARATIVE REVIEW

Security token standards are a requirement in the secure, compliant and interoperable issuance and management of tokenized assets. They represent the standards that determine the logic of the smart contract, which dictates how tokens behave, how they can be transferred, and under which regulatory conditions. [8-11] With increased institutional interest in the use of tokenized securities, their strength and their alignment with legal systems and other existing financial infrastructure have become critical. This section provides a comparison of the three well-known security token standards over various blockchain platforms: ERC-1400 (Ethereum), ST-20 (Polymath), and FA1.2/FA2 (Tezos).

A) ERC-1400: Ethereum Security Token Standard

ERC-1400 introduces an overall security token standard in the Ethereum blockchain platform, specifically focused on meeting the needs of regulated digital securities. It is modular, and it compounds what already exists in terms of previously developed token standards like the ERC-20 (fungible tokens) and the ERC-721 (non-fungible tokens), but incorporates compliance-related mechanisms. ERC-1400 implements the concept of partitioned ownership, allowing various tranches of securities to be followed individually, all within a single token. This is especially intended in the management of investment limitations, voting rights, and eligibility for dividends.

Some of its most significant innovations include the provision of transfer validation facilities, which impose identity, jurisdiction, and accreditation constraints. The standard also facilitates off-chain data connectivity using document references, allowing them to match with traditional legal documentation. Ethereum has an enormous developer ecosystem, and ERC-1400 is well-positioned to gain exposure to interoperability with wallets, exchanges, and custodians. Nonetheless, it is a relatively complex system and would be subject to Ethereum gas pricing, which can affect its scalability and attractiveness to some internal institutional applications.

B) ST-20 (Polymath Standard)

ST-20 Polymath ST-20 is a security token standard created by Polymath, a business facilitating the easy issuance of regulated tokens. Designed as an addition to the ERC-20 standard, ST-20 presents a new capability, identity whitelisting, which allows the transferring of tokens to other addresses that have gone through KYC/AML checks. In contrast to the modular approach of ERC-1400, ST-20 is more of a guiding hand, offering the issuer a regulatory-friendly structure that is easily approachable, regardless of their technical knowledge.

The ecosystem consists of polymath-built tools that allow identity control, investor onboarding, and transfer restrictions, all incorporated with its smart contracts. Although ST-20 has high compliance capabilities, it may be closely related to the Polymath platform, potentially reducing its flexibility and cross-platform capabilities. However, ST-20 has helped to popularize compliance-focused tokenization and exerted an impact on larger Ethereum standardization efforts.

C) FA1.2/FA2 (Tezos-based Standards)

FA1.2 and FA2 are the main token standards on the Tezos blockchain with which asset tokenization (also security tokens) is performed. The FA1.2 share similar functionality with Ethereum ERC-20 and basic fungible token operations. FA2, however, is more modern and adaptable, and can support the notion of a variety of asset types, e.g., fungible, non-fungible, and even hybrid tokens, in a single contract architecture. Such flexibility is especially attractive to tokenized funds, which could contain multiple classes of shares or instruments.

FA2 enables permissioned transfers, operator roles and metadata integration, which enables us to adapt it to compliance. Tezos also provides formal verification and on-chain governance benefits that may be attractive to institutions that value security and protocol updates. Tezos, however, has a small ecosystem and developer base relative to Ethereum, which may lead to unsolvable integration and third-party assistance problems. Nonetheless, the FA2 standard makes Tezos a potential alternative for institutions with a strong compliance feature and a more energy-efficient blockchain framework.

D) Other Emerging Standards (e.g., R-Token, ERC-3643)

Newer, more limited token systems are also emerging as alternatives to older standards such as ERC-1400 and ST-20 to support new regulatory and institutional requirements. An example of these is R-Token by Harbor (acquired by BitGo). R-Token is an ERC-20-compatible asset governed by an additional layer of regulatory compliance, which requires checks off-chain before any transfer can be executed. This is through tethering the token contract to a compliance service that will check the eligibility of both sender and receiver according to certain rules. This model proposes a modular-flexible way of compliance to the extent that an issuer may renew its rules without having to redeploy its token contract.

A further notable development is ERC-3643 (previously known as the Tokeny T-REX protocol). ERC-3643 is based on the principles of ERC-1400 and focuses on identity-based permissioning. Wallet addresses are connected to on-chain identities, over which identity contracts allow issuers to enforce jurisdiction-specific regulations, lockups, and investor type categorization (e.g., accredited, retail). ERC-3643 is compatible with transparent communication with a tokenized security, introducing options such as modular compliance modules, revocable tokens, and corporate action support. This standard is also rising in popularity, especially in Europe, because of its convergence with regulatory needs and its coordination with identity and compliance service providers. These new standards represent the latest evolution of security token infrastructure, focusing on flexibility, composability, and integrating institutions into the ecosystem. They are indicative of a wider industry movement toward dynamic compliance enforcement and integration with identity management systems, aspects that are key enablers of secure and legally sound digital capital markets.

E) Interoperability and Cross-Chain Considerations

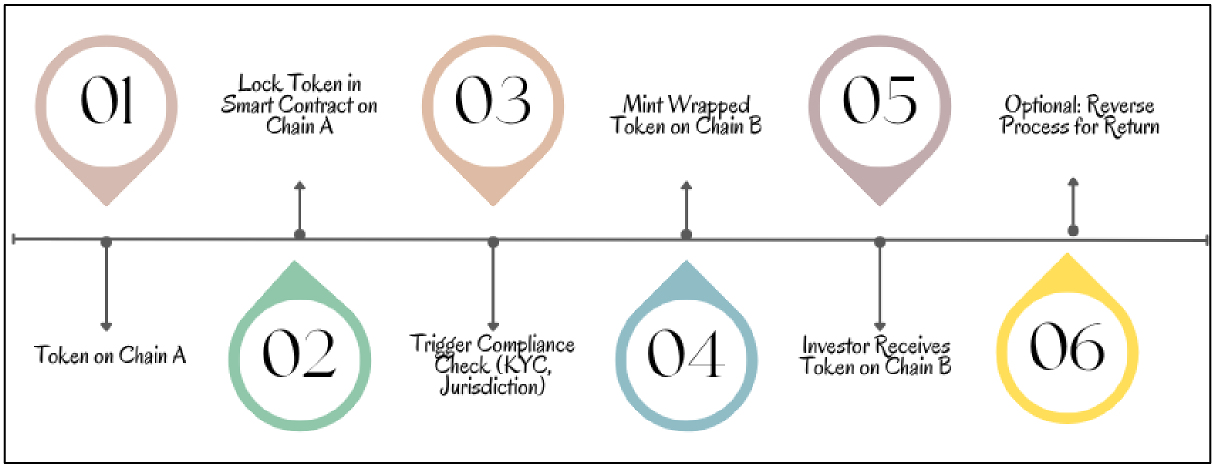

01
Lock Token in Smart Contract on Chain A
03
Mint Wrapped Token on Chain B
05
Optional: Reverse Process for Return
Token on Chain A
02
Trigger Compliance Check (KYC, Jurisdiction)
04
Investor Receives Token on Chain B
06

Figure 1: Interoperability and Cross-Chain Transfer of Security Tokens

With the changes in the concept of tokenization among various blockchain ecosystems, interoperability has emerged as a major issue of interest amongst institutions that need to tokenize and trade assets in a combined and streamlined manner across multiple networks. Security tokens have been kept within silos to date, either within Ethereum, Tezos, or Polymesh blockchains, with limited capability to transfer assets or data across blockchains. This generates inefficiencies and fragmentation, particularly for global institutions that must meet the varied regulatory regimes and manage diversified portfolios.

Several efforts are being made to facilitate cross-chain compatibility. These include Polkadot, Cosmos, and LayerZero, which attempt to offer interoperability layers to connect disparate blockchains, so that tokenized assets can be transferred or mirrored between blockchains, leaving their compliance logic intact. Inter-network communication is also facilitated through the use of token bridges, sidechains, and models based on wrapped assets. These methods, however, bring security threats and complexity of operation, especially in the maintenance of compliance mechanisms across chains.

Standardization of metadata and identity systems is another important point, as those systems should be portable over networks to allow smooth authentication and transfer limitations. New standards Emerging frameworks such as ERC-5564 (of off-chain identity attestations) and Decentralized Identity (DID) standards are working towards this direction. Ultimately, delivering reliable cross-chain security token functionality will not be possible without both technical innovation and cooperation among industry stakeholders and regulatory alignment. The complete potential of tokenized capital markets (and, particularly, in institutional settings) will essentially be left underexploited without interoperability.

IV. INSTITUTIONAL REQUIREMENTS FOR TOKENIZATION

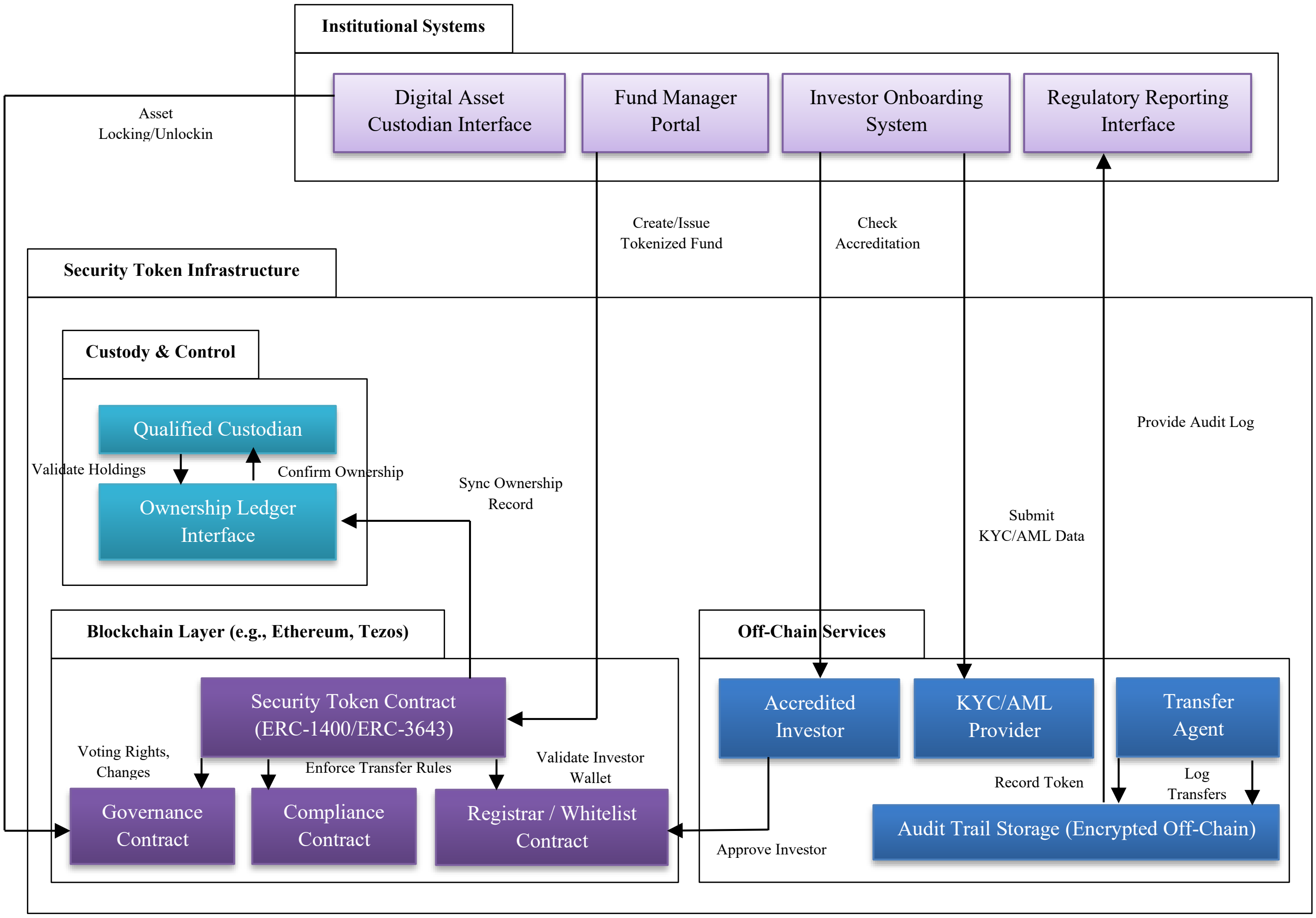


Figure 2: Architecture: Security Token Standards for Institutional Adoption of Tokenized Funds

The Security Token Infrastructure is the core component of this system, used to combine blockchain-based smart contracts, accredited custodians, off-chain compliance services, and institutional platforms. These parts work synergistically to deliver [12-16] secure issuance of assets and constraints imposed by regulation and to enable sophisticated business processes such as KYC/AML procedures, investor onboarding and audit ledger. At the blockchain layer, smart contracts (e.g. ERC-1400 or ERC-3643) are used prominently to encode compliance rules, oversee investor privileges, and the real-time application of transfer limitations. Such smart contracts communicate with various other contracts, including governance contracts, compliance contracts, and registrars or whitelisting modules. As an example, the requirements of validating the wallet with which an investor wishes to buy an asset and transferring the asset tokens are programmatically enforced, so that only fulfilled accredited and authorized investors can store or trade security tokens.

The custody and control segment indicates the extreme importance of qualified custodians, who can provide the safety of tokenized assets to institutional clients. These custodians attest to ownership of assets and match them with blockchain chain property records to ensure correctly reconciled records. Another notable architecture is the ownership ledger interface that serves as an interface between the custodial systems and decentralized registries and maintains the integrity of ownership records. Another significant aspect of the ecosystem lies in off-chain services, which facilitate compliance and operational efficiency. KYC/AML providers (typically referred to as accredited investor validators), transfer agents, and other third-party service providers are also outside the blockchain but closely coupled to it through API invocations and event-driven interactions. For example, the data required to onboard investors is provided off-chain and used to whitelist genuine wallets that can interact with the chain. All token movements and transfer events are fully captured and available in an audit trail storage, which is secured and off-chain and fully auditable by the regulators. Finally, the front-end is represented by institutional platforms, including fund manager portals, investor onboarding interfaces, digital asset custodians, and regulatory reporting tools, which financial institutions use to exchange with tokens. They integrate with the low-level blockchain and compliance layers, allowing for end-to-end workflows (including investor onboarding, fund issuance, transaction execution, and reporting) with full regulatory compliance and security enabled.

A) Compliance and KYC/AML Integration

To accommodate institutional tokenized funds, compliance procedures, especially Know Your Customer (KYC) and Anti-Money-Laundering (AML) services, must be strongly integrated. Securities that are tokenized should also comply with the existing frameworks of traditional financial tools. As the architecture diagram reveals, compliance functionality is usually managed using other off-chain services that can communicate directly with the smart contracts based on the blockchain. Identity documents and personal information are provided during investor onboarding using institutional systems, i.e. investor onboarding platforms. The providers of KYC/AML and validators of accredited investors then certify such.

After verification with a whitelisting contract, their wallet address is whitelisted; anyone can then access the security token contract if the investor's wallet address has been acknowledged. This process allows ensuring only a certain number of acceptable individuals can transfer or take tokens. The rules impacting the investment, such as regional restriction, investor qualification or limited areas, are dynamically enforced using the compliance contract embedded in the blockchain layer. This close integration of off-chain data concerning compliance and on-chain enforcement can promote real-time, full-automation compliance, lowering the manual work overhead and fund manager compliance risk.

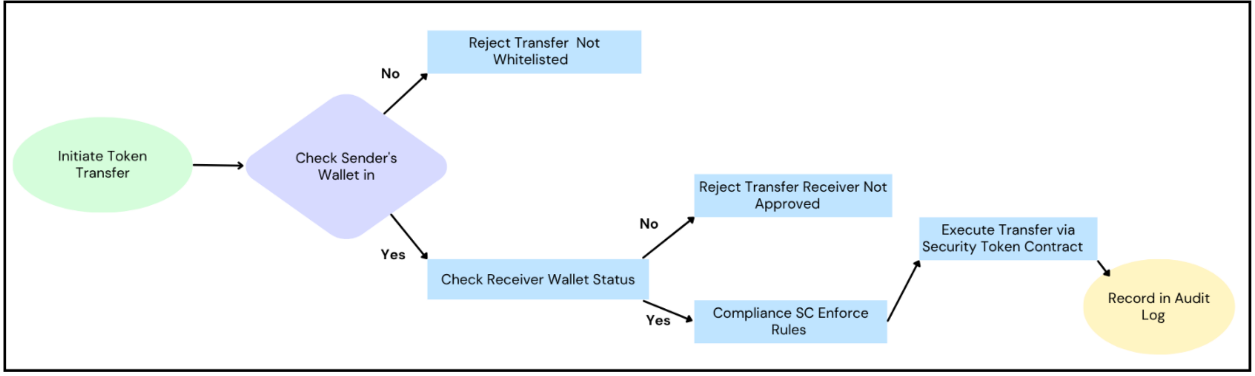
B) Custody and Ownership Tracking

Institutional investors need to know that they can entrust their tokenized assets to a safe store and maintain their legal status. Institutions are likely to use the services of qualified custodians to hold assets, unlike retail investors who can access wallets for self-custody assets. These custodians authorize holdings, prove possession, and update them against blockchain-based ownership records via the ownership ledger interface, as shown in the architecture. By having this hybrid structure, institutional grade custody will be able to match regulatory demands concerning asset separation and fiduciary responsibility.

The blockchain of this architecture provides real-time copy of a blockchain that stores the file of each ownership to the tokens, however, custodians provide an interface to make the assets available as well as reports and reconciliation. It is important to note that this dual-layered involvement does not only facilitate the integration of this system with other financial systems but also reduces operational risks such as key management, or transfer fraud. The custody control also enables affordability of features like locking and unlocking of assets, compliance and operation checks before any transfer can be approved. Transparency and control in a controlled environment is very critical in terms of such a mechanism.

C) Transfer Restrictions and Whitelisting

Figure 3: Compliance-Driven Token Transfer Approval Process


Initiate Token Transfer
Check Sender's Wallet in
No
Reject Transfer Not Whitelisted
Yes
Check Receiver Wallet Status
No
Reject Transfer Receiver Not Approved
Yes
Compliance SC Enforce Rules
Execute Transfer via Security Token Contract
Record in Audit Log

One of the most crucial institutional requirements of tokenized finance is the feature of eye-catching flexibility to control by token transfer in accordance with the regulatory terms. This is ensured through the whitelisting and management of token transfer by the logic of the token smart contract. Checking elements of compliance standards such as ERC-1400 or ERC-3643 are entrenched in an attempt to certify that a transfer is in-compliance with jurisdiction and identity-based approvals prior to finalization. A move of some token, i.e. between wallets that passed a KYC process and are registered in a complaint jurisdiction can be a bounded transfer.

Once applied, whitelisting would be managed by a registrar or a whitelist contract which will interact with an external identity checker and compliance providers. When a wallet is added to the whitelist, it will accept the wallet so that the wallet can send or receive security tokens. They are automatically self-enforced on the chain level and do not require a manual intrusion. No third-party brokers are also necessary. This does a lot in avoiding the risk of compliance and can increase the efficiency in the transaction. Moreover, smarter contracts may be set to contain additional parameters, e.g., lockups, investment caps or transaction approval protocols. Such degree of programmability and transparency is one of the key distinguishing features of tokenized instruments and involves dispersion of institutional requirements relating to regulatory certainty, audibility, and operational governance.

D) Auditability and Transparency

Transparency and auditability are anchor stones in institutional belief about tokenized financial assets. Tokenized assets, unlike those within traditional finance, are carried on blockchain ledgers, which provide permanent and time-stamped data on every movement and programme. All issuance, transfer, or compliance verification occurrences are recorded either on-chain or in related off-chain audit systems, e.g., encrypted audit trail storage, as shown in the system architecture. This enables regulators, custodians, and auditors to have a verifiable and tamper-protected history of asset transactions.

The institutions gain real-time transparency concerning holdings, changes in ownership, and history of transfers, which promotes internal risk management, as well as simplifying external reporting. Furthermore, audit logs may be published via regulatory reporting interfaces, allowing for easy integration with compliance monitoring tools. This end-to-end automated traceability with a full audit trail becomes orders of magnitude more efficient than the time and cost of using a traditional audit system, while allowing the institution to demonstrate its compliance with regulatory requirements, such as MiFID II, SEC Rule 17a-4(f), or FATF recommendations. In addition, as compliance-related data will be stored off-chain and encrypted, the architecture will both ensure data privacy and maintain the transparency required by audit and regulatory authorities.

E) Governance and Voting Mechanisms

Institutional asset management encompasses crucial aspects of governance, especially those funds and securities that provide voting rights, shareholder voice, or participatory control, which appear to be a governance dimension. Traditional governance mechanisms may be time-consuming as processes, like paintings of proxies or running shareholder meetings may be performed manually. On the other hand, tokenized money will enable the inclusion of advanced automatized governance in smart contracts and will make the process easier and increase their involvement. The system has a certain system or governance contract which takes charge of voting rights, captures resolutions as well as vote counting in an on-chain manner.

These types of governance contracts can be associated with specific wallet addresses or digital identities to where only approved investors will be able to propose or vote on modifications. The votes in the token-weighted models can also be in proportions in terms of the number of tokens that a participant holds and this ensures some sense of equity among the participants. Further, it can be achieved with smart contracts to automatize quorum checks, enforce voting periods as well as to make proposals executable upon passing. This reduces chances of manipulation that is followed by instantaneous and transparent decision making. Among institutional actors, programmable governance manages life-critical fund parameters, such as fee levels, redemption rights, and investment mandates, without sacrificing investing involvement, as done by fund managers or custodians. It also reveals the potential of livelier and decentralized frameworks of governance in the event that the regulatory environment modifies to reflect the same. Overall, on-chain governance tools could be conceptualized in the context of the institutional environment of accountability, responsiveness, and fiducial control in the modern-day capital markets.

V. EVALUATION OF STANDARDS AGAINST INSTITUTIONAL CRITERIA

Security token standards must reach high regulatory compliance, security and operational functionality standards to justify institutional adoption of tokenized funds. The assessment of the three most widely used security token standards, including ERC-1400, ERC-3643, and CMTAT, touches upon the compatibility of the given standards with the requirements and limitations of the financial sector. [17-20] The next analysis targets major institutional standards: regulatory conformity, security and auditing facility, financial device capacities, functionality of the operations and governance capabilities. All the standards are discussed on several dimensions, and the information is synthesized based on technical papers, industry security audits, and specialists' analysis. The table below provides a side-by-side comparison of the performance of each of these standards against core institutional requirements that institutions may reference when evaluating the suitability of a solution for managing tokenised assets.

A) Methodology for Evaluation

The process of assessing standards of security tokens is multi-purpose as it focuses on five main institutional requirements:

- **Regulatory Compliance**: Debuts the standard capacity to aid in transfer restraint, KYC/whitelisting, and flexibility across jurisdictions. These features are essential since they help to be legally and regulatory-compliant in different jurisdictions.
- **Security & Auditing**: Reviews suffer cryptographic integrity of the token contract, inclusion of third-party audits; role-based access controls are in place, to enable security and transparency in transactions.
- **Financial Instrument Support**: Evaluates the capability of the standard in accommodating diverse financial instruments, like debt instruments, tranche-based ownership, and forced transfers essential in the management of complicated assets by institutions.
- **Operational Efficiency**: Concentrates on the modularity of the token contract, its optimization of transaction costs (i.e. gas optimization), interoperability with other systems, on-chain and off-chain.
- **Governance**: Reviews the traits regarding the management of the document, the capability to freeze a contract in the event of a problem, and the future upgradability of the contract to enhance it to the requirements of the market.

The analysis is performed based on a sophisticated comparison of the technical characteristics and features described in official documents, auditing reports, and industry analyst reviews.

B) Comparison Matrix

The table below sums up the institutional requirements of the three securities token standards, namely, ERC-1400, ERC-3643, and CMTAT. Comparatively, this analysis highlights the advantages and disadvantages of the two standards in major areas.

Table 1: Comparative Evaluation of Security Token Standards Against Institutional Criteria

Criterion	ERC-1400	ERC-3643	CMTAT
Transfer Restrictions	Yes	Yes	Yes
KYC/Whitelisting	Yes	Yes	Yes
On-Chain Identity Mgmt	No	Yes	Yes
Document Management	Yes	No	Yes
Token Contract Pause	Yes	Yes	Yes
Debt Instrument Support	No	No	Yes
Tranche Ownership	Yes	No	No
Forced Transfers	Yes	Yes	Partial (burn/mint)
3rd-Party Audits	Yes	Yes	Yes
Role-Based Access	Yes	Partial (Agent-only)	Yes
Modular Design	Yes	No	Yes
Gasless Support	No	No	Yes (ERC-2771)
License	Apache 2.0	GPL 3.0	MPL 2.0

C) Evaluation Discussion

a. Transfer Restrictions & KYC/Whitelisting

Transfer restrictions and KYC/whitelisting are also strongly supported in all three standards, ERC-1400, ERC-3643, and CMTAT. It is necessary to adhere to a regulatory regime, especially in jurisdictions such as the U.S. or Europe, where investors must pass certain tests before they can access financial products. Such structures entail the sole discretions to acquire, own and trade in terms of security tokens under the restrictions of limited rules of different governments.

b. On-Chain Identity Management

The on-chain identity management entitlement is one of the major distinct features of the standards. The ERC-3643 and integrated CMTAT aids in the management of identity on-chain through the dynamically proven identity of investors, a factor that investors need to present to have some compliance and trackability. On the other hand, ERC-1400 lacks this and the verification of identity has to be carried out on off-chain systems.

c. Document Management and Governance

Document management is supported with the help of ERC-1400 and CMTAT and is needed in the case of working with legal agreements, financial accounting, and other regulatory documentation provided with tokenized assets. ERC-3643 lacks the feature, however. In addition to existing governance properties which allows ERC-1400 and CMTAT to pause contracts as well as upgrade token contracts, it is more flexible in changing any rules and regulations or staying with the market trend.

d. Financial Instrument Support

One of the biggest advantages of CMTAT over ERC-1400 and ERC-3643 is that it does support debt-based tokens and forced trades. They are needed in places where complex financial products such as bonds or structured finance are operated. ERC-1400 and ERC-3643 are both more appropriate to backing with equity based instruments, without having built-in support to more rudimentary financial investment instruments, like debt, or tranche based ownership.

e. Gasless Support and Modular Design

The other noteworthy distinction is the possibility of gasless support that CMTAT can offer through the employment of ERC-2771. This attribute allows executing transactions without any gas payment by the user, further improving the user experience, especially in case of working at the scale and involving institutional transactions. It is also aimed that CMTAT and ERC-1400 are modular, and more flexibility can be achieved when adapting and extending tokens. In relation, ERC-3643 lacks this modularity and is therefore not so flexible to the specificities of organization.

VI. CHALLENGES AND LIMITATIONS

Using the tokenized funds and security tokens in institutions is an idea that can be quite productive, but it has a complicated set of barriers. These limitations do not only rely on the imprecision of regulations but also on the technical, infrastructural, and market-level complexities of introducing blockchain-based assets to the capital systems. The challenges established in this section indicate structural and emergent challenges that still define the widespread implementation.

A) Regulatory Uncertainty

The situation with security tokens regulations remains fragmented and fragmented across jurisdictions. Regulatory approaches Countries: Switzerland, Singapore, and Liechtenstein have published progressive regulations that can accommodate tokens securities. Other countries have adopted a more conservative/cautious view. This kind of ambiguity complicates cross-border activities, and fails to induce even institutional actors to embark on a tokenized asset approach with full force. A lack of connection also exists with the failure to provide a common international legal platform that governs digital securities. Therefore, the inability to implement universally regulatory-compliant functions into security token contracts is problematic. Institutions, therefore, are forced to operate in a constantly changing maze of regulatory requirements, which adds to legal risk and costly compliance requirements.

B) Technology Fragmentation

The security token marketplace is extremely fragmented with many competing standards (e.g., ERC-1400, ERC-3643, CMTAT), blockchain platforms (Ethereum, Tezos, Polygon) and custody designs. This multiplicity introduces inefficiencies and integration complexities, especially for institutions planning to implement a multi-platform strategy or establish ecosystem-transformed reporting. Institutions will have strong switching costs and interoperability challenges to adopt or upgrade tokenized fund infrastructures unless they converge on a very small number of well-established, highly supported standards.

C) Market and Liquidity Constraints

Security token markets are relatively illiquid, even though much interest is surging towards tokenized assets. The tokens have narrow secondary-market trading platforms, which can be small in terms of volume and/or unregulated and/or not involving many investors. This generates a liquidity premium, which hinders the involvement of institutions, especially by such funds that are less restrictive in their entry and exit strategies. Furthermore, the quality of price discovery suffers due to fragmented order books and the absence of a standardised trading infrastructure, which means that the markets are currently not characterised by efficient price discovery and cannot yet demonstrate the potential advantages of tokenisation.

D) Interoperability Barriers

Security token systems will have to fit into an array of institutional platforms such as custodians, fund administrators, regulatory reporting systems and onboarding tools. This also reduces data sharing and transfer of transactions across the domains because there is no interoperability standard in those dimensions. For example, a security token published on Ethereum can be difficult to transfer or identify by applications deployed on Tezos or Hyperledger. This fragmented environment creates duplicate procedures, inconsistent data formats, and a high operational overhead. Work is being done towards cross-chain bridges and universal token registries, and complete interoperability is a desirable goal, but has not been achieved.

VII. FUTURE DIRECTIONS

With the industry of digital securities and tokenized funds coming to maturity, several foresighted projects are defining the future of the industry. These included compatibility at the basic harmonization level, incorporation of central banks, and use of sophisticated cryptography technology in order to accommodate existing shortcomings and tap into new capabilities of institutional adoption. The next sections will cover some of the main fronts where steps should and are likely to be made in the direction of a globally interconnected and compliant tokenized financial system.

A) Standard Harmonization Initiatives

The standardization is one of the most relevant future directions of security token development. Currently, standards such as ERC-1400, ERC-3643, and CMTAT all offer overlapping, though slightly different functionalities, which contribute to ecosystem fragmentation and interoperability issues. Blockchain industry consortia and alliances, including the International Token Standardisation Association (ITSA) and the InterWork Alliance (IWA), are collaborating to coordinate these efforts, which involve the dissemination of standard taxonomies, metadata syntaxes, and compliance standards. Harmonization both promotes an easy integration across platforms and increases investor confidence since it demystifies technical ambiguity. Multi-standard frameworks or abstraction layers may also enable issuers and platforms to transition the underlying protocols of the token, thereby avoiding the need to re-implement core logic, which can support long-term scalability.

B) Role of Central Banks and Regulators

In the future, central banks and financial regulators will play a defining role in the security token market. More and more regulators are exploring regulatory sandboxes, pilot schemes, and changes to legislation that are friendly to securities based on the blockchain. An example is MiCA (Markets in Crypto-Assets Regulation), an initiative proposed by the European Union, and the Digital Securities Sandbox by the United Kingdom, which are preparing the legal framework that would enable the tokenization of assets. Meanwhile, central banks around the globe are considering issuing a Central Bank Digital Currency (CBDC) that may be used as a native settlement asset by security tokens. The interaction between the CBDCs and the tokenized securities can lead to a coherent digital financial infrastructure with the use of the fully integrated payment and asset rails, which considerably minimizes counterparty risk as well as settlement latency.

C) Emerging Technologies (e.g., Zero-Knowledge Proofs, MPC)

The future of privacy, security, and efficiency of the security tokens will be rewritten with advanced cryptographic tools. Zero-Knowledge Proofs (ZKPs) can enable an institution to confirm the eligibility of investors (e.g., KYC or AML compliance) or the legitimacy of transactions without exposing any sensitive personal or business data on-chain. This does not sacrifice privacy and becomes regulatorily aligned. Along the same vein, Multi-Party Computation (MPC) enables the safe handling and custody of digital assets that are not based on a single point of failure in key management. These technologies are also at an early stage of maturity; they will tend to be used in institutional tokenization platforms and are expected to provide a mix of confidentiality, auditability, and security that is not possible within traditional smart contract infrastructure.

D) Towards Global Institutional Adoption

In the end, the future direction of tokenized finance is pointing to the institutionalization of development on a global scale. This vision will also necessitate technical innovation, as well as legal recognition across jurisdictions, enhanced liquidity models, and wider involvement of actors in the capital markets. Tokenized assets need to be completely intertwined into institutional practices, including fund formation and asset servicing, compliance, and secondary trading. Using interoperable ecosystems, uniform protocols, reliable regulatory control, and scalable systems will be the foundation on which global adoption will be based. Such a future will not mean that security is a niche offering, but rather the broad adoption of security tokens across investment banks, asset managers, pension funds, and sovereigns.

VIII. CONCLUSION

The security tokens standards will serve as an excellent firewall against institutional penetration to tokenized funds. They can be used to model existing financial instruments on blockchain infrastructure where the most important features such as transfer restrictions, KYC/AML compliance, as well as ownership tracking and governance logic are built in them. Standards, including ERC-1400, ERC-3643, and CMTAT, allow issuing and processing digital securities within an institution in a form reflecting both the regulatory requirements and the business operations. However, the issues regarding fragmentation, lack of regulations certainty, and interoperability are also major blockers on the path to mass implementation. Then, there will be a convergence of novel technologies, such as zero-knowledge proofs and MPC, with more vibrant regulatory systems and alignment of standards. Regulators and central banks are starting to get involved in this sector and have already begun to actively influence it, this indicates that tokenized finance is no longer an experiment but has become part of a structure. Security tokens are combinations of technical, legal, and institutional platforms with the ability to change the capital markets, freeing more efficiencies, transparency, and access to international opportunities.

IX. REFERENCES

[1] Hines, B. (2020). Digital finance: Security tokens and unlocking the real potential of blockchain. John Wiley & Sons.

[2] Zhang, D. (2019). Security Tokens: Complying with Security Laws and Regulations Provides More than Token Rewards. UMKC L. Rev., 88, 323.

[3] Frolov, V. N., Vatolin, A. A., & Romanchuk, A. P. (2023). Asset tokenization and related problems. Proceedings of the Steklov Institute of Mathematics, 323(Suppl 1), S98-S112.

[4] Ahmed, H. (2024). Security tokens, ecosystems and financial inclusion: Islamic perspectives. International Journal of Islamic and Middle Eastern Finance and Management, 17(4), 730-745.

[5] Momtaz, P. P. (2023). Security tokens. In The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges (pp. 61-78). Emerald Publishing Limited.

[6] Casanovas Romeu, P., Gonzalez-Conejero, J., & de Koker, L. (2017). Legal Compliance by Design (LCbD) and through Design (LCtD): Preliminary Survey.

[7] Donoghue, S. (2024). Custody in the age of digital assets: The path to building market infrastructure fit for a tokenized economy. Journal of Securities Operations & Custody, 16(2), 168-179.

[8] Leckow, R., & Emre, E. (2019). Cross-Border Resolution: Progress and Challenges in Cross-Border Enforcement. List of IMF Member Countries with Delays in Completion of Article IV Consultations or Mandatory Financial Stability Assessments over 18 Months, 69.

[9] Budnik, R. A. (2023). Risks and prospects of creativity tokenization. Journal of digital technologies and law, 1(3).

[10] Di Angelo, M., & Salzer, G. (2023). Identification of token contracts on Ethereum: standard compliance and beyond. International Journal of Data Science and Analytics, 16(3), 333-352.

[11] Harris, C. G. (2023, July). Cross-chain technologies: Challenges and opportunities for blockchain interoperability. In 2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS) (pp. 1-6). IEEE.

[12] Goodhart, C. A. (2011). The changing role of central banks. Financial History Review, 18(2), 135-154.

[13] Tian, Y., Lu, Z., Adriaens, P., Minchin, R. E., Caithness, A., & Woo, J. (2020). Finance infrastructure through blockchain-based tokenization. Frontiers of Engineering Management, 7(4), 485-499.

[14] Dutta, S. K. (2020). Tokenization. In The definitive guide to blockchain for accounting and business: Understanding the revolutionary technology (pp. 79-105). Emerald Publishing Limited.

[15] Silva, R., Marques, R. P., & Inácio, H. (2024). A design for tokenization in governmental investment. International Journal of Accounting & Information Management, 32(1), 19-39.

[16] Buldas, A., Draheim, D., Gault, M., Laanoja, R., Nagumo, T., Saarepera, M., ... & Truu, A. (2022). An ultra-scalable blockchain platform for universal asset tokenization: Design and implementation. IEEE Access, 10, 77284-77322.

[17] Glass, G. V. (1978). Standards and criteria. Journal of Educational Measurement, 15(4), 237-261.

[18] Ciriello, R. F. (2021). Tokenized index funds: A blockchain-based concept and a multidisciplinary research framework. International Journal of Information Management, 61, 102400.

[19] Layr, A. K. (2021). Tokenization of assets: security tokens in Liechtenstein and Switzerland. Milan Law Review, 2(1), 45-72.

[20] Ford, M. W. (2022). Management standards and institutional influence: An exploratory study using the Baldrige criteria. Quality Management Journal, 29(1), 18-33.