

(12) STANDARD PATENT APPLICATION (11) Application No. AU 2026201945 A1
(19) AUSTRALIAN PATENT OFFICE

(54) Title
System and Method for Entity-Controlled Permissioning of Compliance Metadata in Blockchain-Based Credential Systems.

(51) International Patent Classification(s)
H04L 9/32 (2006.01) **G06Q 30/018** (2023.01)
G06Q 20/06 (2012.01) **H04L 9/00** (2022.01)
G06Q 20/22 (2012.01) **G06Q 20/40** (2012.01)
G06Q 20/38 (2012.01)

(21) Application No: **2026201945** (22) Date of Filing: **2026.03.13**

(43) Publication Date: **2026.04.02**

(43) Publication Journal Date: **2026.04.02**

(62) Divisional of:
2025202797

(71) Applicant(s)
Dominic Thaddeus Tayco

(72) Inventor(s)
Tayco, Dominic

(74) Agent / Attorney
Darren Martin Conlon, 74-76 Campbell St, Surry Hills, NSW, 2010, AU

Abstract

With this invention, a computer-implemented system and method are provided for controlling disclosure of compliance metadata associated with a blockchain-based entity credential. A compliance credential issued to an entity is linked to encrypted metadata containing regulatory compliance information. A permissioning module enables the entity to selectively grant, revoke, or limit access to portions of the compliance metadata. Authorised parties may request verification of specific compliance attributes through a verification interface that provides access only to metadata permitted by the entity. The system enables privacy preserving verification of entity compliance information while allowing regulated platforms to confirm eligibility for participation in restricted regulated offerings.

TITLE OF YOUR INVENTION

System and Method for Entity-Controlled Permissioning of Compliance Metadata in Blockchain-Based Credential Systems.

TECHNICAL FIELD

This invention relates to systems and methods for issuing, managing, and verifying cross-jurisdictional regulatory compliance credentials for wholesale investors using blockchain or distributed ledger technologies.

BACKGROUND OF THE INVENTION

This invention relates to financial services regulation, specifically the onboarding and compliance assessment and management of investors who participate in restricted investment offerings. Such offerings, including private placements, tokenised financial products, and alternative investment vehicles, are generally limited to investors who meet jurisdiction-specific eligibility criteria. These investors may be referred to by various terms, for example and without limitation: as *accredited investors* (United States), *professional investors* (Hong Kong), *eligible counterparties* (European Union), or *wholesale investors* (Australia). For consistency, the term *wholesale investor* is used throughout this document to refer collectively to these financially sophisticated market participants.

Regulatory frameworks typically require these wholesale investors be identified and verified before gaining access to restricted products, because accurate identification and classification of wholesale investors is critical to protecting the integrity of financial markets. Regulators impose these requirements to prevent market abuse, ensure fair access, and reduce the risk of financial crime, including fraud, money laundering, and terrorism financing. As a result, wholesale investors are required to undergo extensive identity and compliance verification processes including:

- **Know Your Customer/Client (KYC)** requirements, which compel institutions to verify an investor's identity and assess their risk profile;
- **Anti-Money Laundering (AML)** obligations, which aim to prevent the integration of illicit funds into the financial system;
- **Counter-Terrorism Financing (CTF)** measures, which require screening and reporting of transactions potentially linked to terrorist activities; and
- **Tax Residency and Investor Classification Checks**, such as compliance with the Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standard (CRS), or determination as a "wholesale" or "accredited" investor.

Another critical market trend is the rise of **Environmental, Social, and Governance (ESG)**-aligned investing. ESG refers to a framework used to assess the sustainability, ethical impact, and long-term value alignment of investors or capital recipients. Wholesale investors are increasingly required to present ESG-related declarations or certifications. However, there is no standardised, reusable method for investors to present verified ESG credentials during onboarding. Consequently, ESG preferences are either manually collected or omitted entirely from the verification process, undermining transparency and sustainability mandates.

Failure to properly screen and classify investors can result in unauthorised access to restricted offerings, misuse of financial products, or circumvention of jurisdictional restrictions. In decentralised or cross-border investment environments, such as tokenised asset platforms or digital fund ecosystems, these risks are heightened by automation, anonymity, and fragmented regulatory oversight. Therefore, a reliable, verifiable credentialing system for wholesale investors is essential to uphold legal obligations, preserve investor confidence, and enforce participation rules in real time.

In recent years, the digitisation of capital markets and the emergence of tokenised investment vehicles have introduced new opportunities for wholesale investors. Despite these technological advances, the regulatory compliance infrastructure underpinning investor onboarding has remained largely manual, repetitive, and jurisdictionally fragmented. Additionally, each investment or platform currently requires repeat verification, increasing

cost, delay, and friction. Regulators globally are tightening expectations for real-time, verifiable, and auditable compliance. Consequently, manual processes are no longer sustainable.

Several digital identity and compliance products have emerged to address aspects of this problem. Examples include Bloom Protocol, Civic/Identity.com, Tokeny's InvestorID, and IBM's Digital Credential Framework. These systems support self-sovereign identity and selective disclosure, but none provide a purpose-built, programmable compliance token architecture capable of:

- Mapping investor classifications across jurisdictions;
- Embedding lifecycle management (expiry, renewal, revocation);
- Supporting third-party ESG attestations; and
- Integrating directly with smart contracts for automated eligibility checks.

Therefore, the market lacks a reusable, investor-controlled compliance credential that supports cross-border interoperability, aligns with existing legal classifications, and is capable of securely interfacing with decentralised investment platforms. This gap has created a compliance bottleneck in tokenised capital markets, where speed, security, and automation are essential. There is a need for a system that transforms paper-based, static verification processes into a verifiable, digital, and reusable credential that is privacy-preserving, regulator-aligned, and programmable across jurisdictions, and this invention provides a credential-based system to streamline, enforce, and manage these requirements in real time across platforms and jurisdictions.

Statement of problem to solve

Current compliance frameworks for wholesale investors are fragmented, manual, and jurisdictionally siloed. As a result, verifying KYC, AML, licensing status, ESG-alignment, and investor classification typically involves duplicative processes, static document exchange, and centralised data silos. These systems lack interoperability across jurisdictions,

are not user-controlled, and do not support secure, real-time verification in decentralised environments.

This invention addresses this by introducing a secure blockchain-based system for issuing, managing, and verifying investor credentials using non-transferable tokens, cross-jurisdictional mapping, and privacy-preserving verification mechanisms.

SUMMARY OF THE INVENTION

This invention provides a system and method for issuing and managing non-transferable, blockchain-based compliance credentials (Single Onboarding Lodgement Online Tokens referred to as “SOLO Tokens” throughout this specification) that enable wholesale investors to present verified eligibility status across multiple jurisdictions.

These credentials are embedded with programmable metadata, including accreditation status, ESG declarations, expiry information, and jurisdictional classification. A credential issuance engine verifies attestations from compliant validators (e.g., Australian Transaction Reports and Analysis Centre [AUSTRAC]-registered KYC providers), then mints tokens to investor wallets using smart contracts.

Credential metadata is stored off-chain and accessed via cryptographic links, enabling selective disclosure and privacy preservation. A jurisdictional equivalence engine maps investor categories across regions (e.g., Australia ↔ Singapore ↔ United States), while a lifecycle module manages expiration, renewal, and revocation.

Investment platforms query these tokens via Application Programming Interface (API) or smart contracts to validate investor eligibility in real time. This eliminates redundant onboarding, enhances cross-border compliance, and supports ESG-aligned capital flows.

This invention thereby improves upon fragmented manual compliance systems by offering a reusable, verifiable, regulator-aligned infrastructure for investor onboarding and credential validation.

Advantages of this invention

This invention offers several advantages over existing compliance verification systems.

It provides a secure single-stop decentralised blockchain-based method and system that enables ongoing real-time issuance, storage, and verification of compliance credentials for wholesale investors. These credentials may include, but are not limited to, investor type, regulatory licenses held, participation rights in regulated offerings, and other compliance attributes encoded in secure, tokenised formats.

It enables faster and more reliable onboarding of wholesale investors by automating the issuance and validation of credentials via smart contracts. Investor-controlled tokens ensure greater privacy and flexibility, while the use of distributed ledger technology increases auditability, reduces fraud, and removes reliance on centralised intermediaries. The cross-jurisdictional equivalence engine eliminates the need for repeated verification across borders, improving efficiency for global asset managers and regulatory platforms alike. The modular structure also allows integration with both traditional and decentralised financial infrastructure.

Similar products and their operations

1. Securrency's Compliance Aware Token® Framework (CATF)

How the Product Operates:

- **Embedded Compliance:** The product integrates regulatory rules directly into the token's architecture, so that compliance checks are enforced automatically at the time of transaction without needing external validation layers.
- **Compliance Oracle:** It uses an off-chain oracle service to validate the compliance status of transaction participants, ensuring they meet specific jurisdictional regulations before a transaction is approved.
- **Ledger Agnostic:** The system is built to operate across various blockchain platforms, meaning it does not depend on a specific distributed ledger and can interoperate with multiple ecosystems.
- **Recovery Mechanisms:** It includes identity-based asset recovery tools, which allow verified users to regain access to their assets in the event of private key loss or theft.

Differentiation of the Product from this Invention:

- **Scope of Compliance:** Securrency's CATF focuses on embedding regulatory compliance directly within tokens to govern their movement, whereas this invention emphasises managing the entire lifecycle of compliance credentials separately from asset tokens.
- **Target Audience:** CATF is designed for general-purpose digital asset compliance, while this invention is purpose-built for wholesale investors who require ongoing, auditable compliance credentials.
- **Credential Management:** CATF lacks a comprehensive system for issuing, updating, or revoking compliance credentials over time, whereas this invention delivers a credential-specific management framework independent of tokenised assets.

Shortcomings of the Product:

- **Compliance logic is embedded in tokens:** Compliance logic is hardcoded into each token, so any updates to regulations or user status require the token itself to be reissued or updated, which is inefficient and inflexible.
- **Reliance on external oracles introduces off-chain vulnerabilities:** Since compliance decisions rely on oracles that operate outside the blockchain, the system is exposed to potential data integrity and availability risks, undermining the trust model of decentralised verification.
- **Focus is on transactional compliance, not on the broader lifecycle of regulatory credential issuance and management:** The product ensures compliance at the time of asset transfer but does not manage long-term credential attributes such as expiration, renewal, jurisdictional updates, or revocation, which are essential for regulated investors.

Why the Shortcomings are Problematic for Clients:

- **Asset-level compliance rules do not solve onboarding standardisation:** Embedding compliance rules into individual tokens ensures enforcement at the point of transaction, but it fails to establish a consistent and repeatable onboarding process across different platforms and jurisdictions, which leads to inefficiencies and inconsistency.

- **Requires expensive custom integration for each fund or issuer:** Since each fund must embed its own specific compliance logic into its tokens, there is a high development cost and integration burden for issuers trying to scale across multiple jurisdictions or offerings.
- **Credential reusability across platforms is functionally limited:** Credentials embedded in token smart contracts cannot be extracted or reused on other platforms, forcing investors to undergo duplicative verification processes and increasing overall friction and compliance costs.

How this Invention Addresses these Shortcomings:

- **This invention separates credential management from token logic, allowing dynamic updates without reissuing tokens:** Compliance data is managed independently of the token, so credentials can be updated, renewed, or revoked without the need to destroy or replace the token, making it far more flexible and adaptable to changing regulatory conditions.
- **Compliance is linked to verified credentials, not hardcoded into token movement:** The system verifies compliance status using verifiable credentials that are separate from the asset transaction logic, allowing platforms to check investor eligibility in real time without embedding rigid rules in the token itself.
- **This invention focuses on the governance, issuance, revocation, and portability of regulatory credentials themselves, independent of asset structure:** It offers a modular and interoperable framework for managing investor credentials throughout their lifecycle, ensuring they can be reused across platforms and jurisdictions without being tied to any single asset or transaction type

2. DTCC's ComposerX Suite

How the Product Operates:

- **Capital Markets Platform:** ComposerX provides a digital infrastructure that manages the lifecycle of tokenised assets, from issuance and trading to corporate actions, making it a platform for asset management.
- **Factory:** It includes a tokenisation engine referred to as "Factory," which automates the creation and management of digital assets by enhancing tokens with structured data schemas for better transparency and functionality.

- **LedgerScan:** The system features an oversight tool called LedgerScan, which monitors token activity across blockchain ecosystems and integrates with traditional systems to support regulatory compliance and reporting.

Differentiation of the Product from this Invention:

- **Infrastructure Level:** ComposerX functions as an infrastructure solution for managing tokenised assets, whilst this invention is focused on managing compliance credentials for wholesale investors.
- **Regulatory Focus:** ComposerX enforces compliance within the transactional flow of assets, whereas this invention targets the upstream regulatory need for validating and verifying investor credentials before transactions occur.
- **Integration:** Unlike ComposerX, which handles tokens and their mechanics, this invention provides credential-level compliance validation of investors.

Shortcomings of the Product:

- **Broad infrastructure offering; not purpose-built for regulatory credential management:** ComposerX is designed to handle a wide range of digital asset processes but lacks specialised tools for issuing, verifying, or managing compliance credentials associated with the investors themselves.
- **Heavy focus on asset lifecycle, not the credentialing of investors or participants:** The platform concentrates on the movement and structure of tokenised assets, offering limited support for managing the regulatory status or classification of the users who interact with those assets
- **Relies on external integrations for compliance verification:** ComposerX does not offer native, end-to-end compliance credential verification; instead, it depends on third-party tools or services to validate whether users meet eligibility or jurisdictional requirements

Why the Shortcomings are Problematic for Clients:

- **Institutions must implement their own credentialing frameworks externally:** ComposerX does not offer built-in investor compliance credentialing, so fund managers and platforms must build and maintain separate systems to verify and track investor eligibility, increasing operational complexity and regulatory exposure.
- **No portable investor credentials for reuse across platforms:** The platform does not support reusable credentials, which means investors must undergo a fresh compliance process each time they use a new platform or investment product, reducing efficiency and scalability.
- **Onboarding logic is fragmented, increasing integration overhead and regulatory exposure:** Without a unified compliance layer, onboarding procedures are often disconnected from token operations, which results in duplicated work, inconsistent compliance enforcement, and increased regulatory risk for financial institutions.

How this Invention Addresses these Shortcomings:

- **This invention fills the credential-specific compliance layer ComposerX lacks:** It introduces a dedicated credentialing framework that enables wholesale investors to present verified, dynamic compliance tokens, addressing the gap in ComposerX's infrastructure for investor eligibility verification
- **This invention provides real-time, credential-based compliance verification, which is especially valuable for onboarding and risk-based segmentation:** This invention enables platforms to instantly validate investor credentials, allowing for segmented access based on jurisdiction, investor type, or ESG status without duplicating KYC or onboarding processes.
- **This invention complements platforms like ComposerX by handling eligibility and authorisation at the identity level:** It integrates seamlessly into platforms focused on asset flows by providing real-time investor verification, allowing fund managers to control access based on dynamically updated credentials rather than static preconditions.

3. Redbelly Network

How the Product Operates:

- **Compliant Asset Tokenisation:** Redbelly allows issuers of real-world assets (RWAs) to create compliant on-chain financial products by converting traditional assets into tokenised forms that follow legal and regulatory frameworks.

- **Identity Verification:** The platform integrates user identity checks at the transaction layer, using privacy-preserving tools like zero-knowledge proofs and verifiable credentials to protect personally identifiable information while maintaining regulatory integrity.
- **High Performance:** Redbelly achieves high throughput and transaction scalability through a leaderless consensus protocol called Deterministic Byzantine Fault Tolerance (DBFT), enabling fast, secure, and efficient blockchain operations.
- **Use Cases:** Redbelly has partnered with various organisations to tokenise assets such as private equity holdings and carbon credits, demonstrating its adaptability to different sectors and asset classes.

Differentiation of the Product from this Invention:

- **Asset Focus:** Redbelly primarily focuses on the issuance and structuring of compliant digital assets, whereas this invention centres on the creation and lifecycle management of investor compliance credentials.
- **Compliance Approach:** Redbelly enforces compliance at the point of transaction execution, while this invention offers a credential-based model that verifies compliance status independently of any single transaction.
- **Target Audience:** Redbelly serves a broad user base of asset issuers and ecosystem participants, whereas this invention is purpose-built for wholesale investors needing portable, multi-jurisdictional compliance verification.

Shortcomings of the Product:

- **Designed for compliant asset issuance, not credential issuance:** Redbelly's compliance architecture is embedded in its asset tokenisation process and does not include a system for managing investor credentials or compliance profiles across platforms
- **Compliance is enforced at the transaction layer, but lacks robust credential lifecycle management:** While compliance checks are conducted during transactions, the platform does not offer tools to manage the ongoing status of investor credentials, such as updates, renewals, or revocations

- **Focus is more on performance/scalability and consensus innovation:** The platform's technical strengths lie in its scalable consensus mechanism and transaction speed, rather than its capacity to manage investor compliance workflows over time.

Why the Shortcomings are Problematic for Clients:

- **Compliance enforced per transaction, not sustained over time:** By validating compliance only at the time of each transaction, Redbelly does not support long-term regulatory obligations like periodic re-verification or credential monitoring, creating risk for ongoing investment relationships.
- **Credential lifecycle not tracked or revocable across platforms:** In the absence of support for revocation, expiry, or jurisdictional reassessment, investors may use outdated or invalid credentials, exposing platforms to non-compliance with evolving legal standards.
- **Asset-tokenisation centricity means investor compliance remains secondary:** The Redbelly system is designed around asset structuring not investor verification, so compliance controls for the investor side of transactions are limited, leading to increased reliance on manual processes and parallel systems.

How this Invention Addresses these Shortcomings:

- **This invention provides institution-level compliance tooling—credential registration, verification, expiration, and revalidation:** It delivers a full lifecycle management framework for investor compliance, enabling institutions to issue, update, revoke, and revalidate credentials across jurisdictions in line with regulatory requirements
- **Works independently of a specific architecture, allowing credential portability across chains.** This invention's credentialing system is blockchain-agnostic and can integrate with other products like Redbelly or function independently of them, enabling investors to reuse their credentials across multiple platforms.
- **Focuses on the trusted verification process itself, not just transaction validation:** This invention is designed to ensure investor eligibility is verified and traceable at the identity level, beyond just moment-of-transaction checks, offering sustained compliance over time

4. Hyland Credentials

How the Product Operates:

- **Digital Credentialing:** Hyland Credentials uses blockchain technology to issue and verify digital records in a secure and tamper-proof manner, ensuring the authenticity of credentials.
- **Blockcerts Standard:** It adopts the open-source Blockcerts framework for credential issuance, which is widely used for academic and professional certification standards.
- **User Ownership:** The platform ensures that users retain full ownership and control of their credentials, allowing them to independently verify and present their records through API-enabled platforms.
- **Integration:** Hyland offers integration APIs that enable third-party applications to add features such as digital signatures, time-stamping, and credential validation, making the system extensible.

Differentiation of the Product from this Invention:

- **Sector Focus:** Hyland is primarily focused on issuing digital records for the education and public sectors, whereas this invention is purpose-built for issuing compliance credentials within the financial services industry.
- **Credential Types:** Hyland Credentials is designed to handle academic and government-related documents, while this invention supports highly specialised regulatory credentials for wholesale investors.
- **Compliance Integration:** This invention directly integrates compliance logic and verification workflows into the credentialing process, whereas compliance functionality is not a core feature of the Hyland system.

Shortcomings of the Product:

- **Primarily designed for education and government certifications:** Hyland's platform lacks support for use cases involving financial regulatory compliance or investor onboarding, making it unsuitable for capital markets.

- **No embedded compliance logic or linkage to transactional use cases:** Credentials issued by Hyland are passive and cannot be used for automated enforcement of compliance or eligibility in transactional environments.
- **Relies on static credentials, often verified manually:** Hyland's system does not support dynamic credentialing features such as expiration, revocation, jurisdictional layering, or programmable access conditions.

Why the Shortcomings are Problematic for Clients:

- **Not suited to investment onboarding or regulated capital markets:** Hyland's use in regulated onboarding workflows is impractical or non-compliant, because it does not provide features required for financial services compliance.
- **Credentials lack dynamic attributes like jurisdictional layering or ESG tagging:** Investors cannot use Hyland-issued credentials to reflect changing compliance statuses, regulatory alignment across jurisdictions, or ESG declarations, which are common onboarding requirements.
- **Manual verification requirements limit automation and scale:** In the absence of support for smart contract interaction or real-time validation, the system depends on manual or semi-automated processes, which limits its suitability for large-scale or real-time investor onboarding.

How this Invention Addresses these Shortcomings:

- **This invention is designed for real-time credential validation, suitable for automated financial compliance checks:** It provides instant, verifiable confirmation of investor status and eligibility through smart contracts or APIs, enabling seamless integration with onboarding systems.
- **Includes compliance triggers, expiry mechanisms, and revocation flows:** This invention supports full credential lifecycle management, allowing credentials to be updated, suspended, or retired based on changing investor status or regulatory needs.
- **Integrates with transaction systems, enabling enforcement of participation rules via credential validity:** This invention ensures only verified investors can access regulated products because compliance data is linked to programmable credentials, reducing risk and manual intervention.

5. TruScholar

How the Product Operates:

- **Blockchain Credentials:** TruScholar issues credentials secured by blockchain technology, ensuring that each certificate is tamper-proof and verifiable, providing an immutable record of educational achievement.
- **Verification:** The system allows employers and institutions to verify the authenticity of credentials using quick response (QR) codes embedded in digital certificates, which link directly to the blockchain-stored verification data.
- **Integration:** TruScholar supports integration with third-party automation platforms such as Zapier, enabling credential verification and issuance to be streamlined across workflows and services.
- **Compliance:** TruScholar ensures alignment with educational regulatory standards, including those set by bodies such as the National Academic Depository (NAD) and Academic Bank of Credits (ABC) under India's National Education Policy (NEP) 2020.

Differentiation of the Product from this Invention:

- **Educational Focus:** TruScholar is tailored to educational institutions issuing academic credentials, whereas this invention serves financial institutions that require investor compliance credentials for regulated onboarding.
- **Credential Purpose:** TruScholar's primary use case is academic certification, while this invention is focused on verifying compliance status for wholesale investors in financial markets.
- **Compliance Standards:** TruScholar aligns with national education frameworks and standards, whereas this invention is designed to meet the requirements of financial regulatory regimes such as KYC/AML, FATCA, and investor accreditation rules.

Shortcomings of the Product:

- **Limited to academic use cases, not financial institutions or regulators:** TruScholar's system is not designed for compliance-driven industries such as finance, where credentials must reflect regulatory eligibility and evolve over time.
- **Certificates are largely static and intended for proof of attendance/degree:** TruScholar issues credentials that confirm past events (e.g. graduation) but do not support dynamic attributes like investor status, jurisdictional classification, or risk scoring.
- **Does not support risk-based credentialing or periodic re-validation:** TruScholar lacks features to assess investor risk levels or mandate recurring validation, both of which are essential for meeting financial compliance obligations.

Why the Shortcomings are Problematic for Clients:

- **Static academic-style credentials not viable in compliance-sensitive markets:** Credentials that cannot change over time or reflect regulatory status are unsuitable for institutions that must meet ongoing obligations for KYC, AML, and investor classification.
- **Inflexible structure prevents smart contract enforcement:** TruScholar credentials are not programmable or machine-readable via smart contracts, so they cannot be used in automated onboarding or eligibility enforcement systems.
- **No linkage to investment onboarding, investor classification, or real-time revocation:** TruScholar's platform does not provide any mechanism to assess, update, or revoke credentials based on financial regulation, investor residency, or compliance changes, leaving platforms exposed to risk.

How this Invention Addresses these Shortcomings:

- **This invention issues compliance-grade credentials that can expire, be revoked, or dynamically validated:** It provides regulatory-compliant credentials that reflect up-to-date investor status, include expiry dates, and support revocation events, which are all managed through a secure, verifiable infrastructure.
- **Designed for regulated financial use, including AML/KYC, wholesale eligibility, and cross-jurisdiction validation:** This invention meets complex requirements for financial onboarding, including jurisdiction-specific rules and investor classification logic that evolves over time.

- **This invention supports ongoing compliance checks, not one-off credential verification:** Unlike static education certificates, credentials are monitored and updated throughout their lifecycle, ensuring compliance remains active and auditable at all times.

6. Bloom Protocol

How the Product Operates:

- **Blockchain-based identity system using third-party attestations:** Bloom provides a decentralised identity framework in which users collect and present identity attestations issued by third-party validators, stored and verified via blockchain technology.
- **Users retain control of credentials and selectively share them:** The system is designed with user privacy in mind, allowing individuals to hold their identity data locally and share only specific credentials as needed with requesting parties.
- **Focused on credit scoring, identity access, and general-purpose ID use cases:** Bloom is primarily used for personal identity verification and credit profiling, with applications in lending, account access, and basic user authentication.

Differentiation of the Product from this Invention:

- **No investment credentialing or jurisdictional mapping:** Bloom does not support classification of investors according to regulatory requirements or map those classifications across different legal systems, which are essential functions of this invention.
- **Does not support lifecycle controls or real-time validation:** Credentials issued through Bloom are not designed to expire, be renewed, or be automatically revoked based on regulatory triggers, whereas this invention is specifically structured to manage such events.
- **Limited metadata structure and no smart contract compatibility:** Bloom's credential framework lacks the rich, programmable metadata required for regulatory onboarding and does not natively support interaction with smart contracts for automated access control.

Shortcomings of the Product:

- **Lacks financial compliance structure (e.g. KYC/AML, accredited investor checks):** Bloom is not designed to verify or store financial compliance attributes such as AML status, investor accreditation, or FATCA/CRS classification, which are essential for capital markets.
- **No ESG metadata or regulated onboarding alignment:** The platform does not incorporate environmental, social, and governance (ESG) declarations or support compliance workflows that align with regulated financial onboarding procedures.
- **Not usable as a plug-and-play credential in regulated financial environments:** Bloom's credentials cannot be readily integrated into institutional financial platforms or investment offerings, because it lacks regulatory awareness and validation features.

Why the Shortcomings are Problematic for Clients:

- **Manual re-verification still required by platforms:** Investors must undergo separate, manual compliance checks on each platform they use, as Bloom credentials cannot satisfy regulatory onboarding requirements, leading to increased inefficiencies and delays.
- **Slows onboarding, increases legal risk for cross-border investors:** Platforms using Bloom risk admitting unverified or ineligible investors because it lacks regulatory mapping or jurisdictional controls, which increases the chances of non-compliance and associated penalties.
- **No unified structure for lifecycle management or platform interoperability:** The absence of expiry, revocation, or renewal functionality limits Bloom's use in long-term investor workflows, and its credentials cannot be reliably reused across different platforms or regulatory systems.

How this Invention Addresses these Shortcomings:

- **Offers jurisdiction-aware, lifecycle-managed credentials:** This invention manages compliance credentials through structured lifecycle events, including issuance, expiration, renewal, and revocation, ensuring credentials remain valid and regulatorily aligned over time.
- **Integrates ESG flags and investor class validation:** Credentials can carry ESG declarations and investor classification statuses, enabling platforms to assess suitability for participation in ESG-aligned or jurisdiction-specific investment products.
- **Fully reusable across platforms with smart contract compatibility:** This invention supports verifiable, machine-readable credentials that can be used across multiple financial platforms

and jurisdictions, integrating directly with smart contracts for real-time access control and compliance checks.

7. Tokeny (InvestorID)

How the Product Operates:

- **Links investor identity to wallet address:** InvestorID ties a user's verified identity to their blockchain wallet address, enabling platforms to associate real-world identities with wallet-based interactions for digital securities.
- **Used primarily for digital securities issuance in Europe:** The system is widely implemented in European jurisdictions to satisfy regulatory requirements for investor identification during the issuance phase of tokenised securities.
- **Credentials verify identity and basic jurisdictional eligibility:** The platform provides verification that an investor meets jurisdiction-specific eligibility criteria, but only at a basic level and primarily during the onboarding phase.

Differentiation of the Product from this Invention:

- **Narrow scope, focused on issuance phase, not full lifecycle:** InvestorID is designed mainly to support identity verification at the point of asset issuance, whereas this invention manages credentials throughout the entire investor relationship, including renewal, expiration, and revocation.
- **No embedded compliance logic, ESG tagging, or jurisdictional mapping:** The platform does not include deeper compliance structures such as investor classification across jurisdictions, support for ESG indicators, or programmable regulatory logic within credentials.
- **Limited support for expiry, revalidation, or investor classification:** InvestorID credentials do not dynamically evolve based on regulatory changes or investor status updates, making it difficult to maintain up-to-date compliance over time.

Shortcomings of the Product:

- **Static credentials that don't evolve with regulation or investor status:** InvestorID lacks mechanisms to update or expire credentials, meaning changes in an investor's eligibility or compliance standing are not reflected in real time.
- **Limited to certain jurisdictions; no cross-border portability:** The platform does not support jurisdictional equivalence rules or multi-region investor onboarding, restricting its usefulness in global financial markets.
- **Requires manual policy mapping on each platform:** Each investment platform must independently interpret and map compliance criteria to the credential structure, increasing duplication and inconsistency in enforcement.

Why the Shortcomings are Problematic for Clients:

- **Limits scaling for global offerings:** Absent cross-jurisdictional support or reusable credential architecture, financial institutions must repeat onboarding processes for each region, increasing time and cost.
- **Requires additional KYC checks across platforms:** Credentials are static and platform-specific, so investors must undergo redundant KYC and compliance verification each time they engage with a new platform, leading to inefficiencies and frustration.
- **Slows onboarding and increases cost per investor:** The lack of lifecycle management and automation features raises onboarding friction and costs, especially for platforms that onboard wholesale clients across multiple funds and geographies.

How this Invention Addresses these Shortcomings:

- **Credentials are dynamic, regulator-aligned, and reusable:** This invention enables credential updates in response to regulatory changes and ensures alignment with jurisdictional and investor-type rules, while supporting reuse across multiple compliant platforms.
- **Investor status, expiry, and jurisdiction encoded directly in token:** Each credential includes machine-readable metadata about the investor's current classification, jurisdictional eligibility, and expiration status, enabling automated access control and compliance assurance.
- **Enables one-time onboarding for multi-market use:** Investors undergo verification once and then use their credentials across multiple jurisdictions and platforms, reducing repetition, increasing efficiency, and ensuring consistent regulatory compliance.

8. Civic (CVC) / Identity.com

How the Product Operates:

- **Decentralised ID platform using mobile wallet and blockchain attestations:** Civic provides a decentralised identity system where users manage their identity credentials via a mobile wallet, with attestations stored and validated through blockchain infrastructure.
- **Users receive KYC verifications and can present proof without sharing data:** The system enables users to obtain verified KYC status and prove their compliance without disclosing personal information, leveraging cryptographic proofs for privacy preservation.
- **CVC token is primarily used for settling identity transactions between ecosystem participants:** The CVC token is used within a closed-loop identity marketplace to compensate validators and service providers for identity verification activities.

Differentiation of the Product from this Invention:

- **No investor classification or regulated onboarding framework:** Civic's system is designed for general-purpose identity verification, and does not support financial investor categories such as accredited or wholesale investor classifications required for regulatory onboarding.
- **No metadata standard for compliance or ESG alignment:** Unlike this invention, Civic does not include structured metadata that reflects regulatory attributes, jurisdictional mappings, or ESG indicators, limiting its use in wholesale finance.
- **Credentials are general-purpose, not tailored to regulated transactions:** The Civic platform is primarily intended for broad identity use cases (e.g., account access), not for complex financial workflows where compliance status must be verified across multiple jurisdictions.

Shortcomings of the Product:

- **Not designed for financial service use cases:** The platform lacks support for regulatory frameworks specific to capital markets, including KYC layering, FATCA, CRS, investor class validation, or multi-jurisdictional credentialing.

- **Offers no revocation, expiry, or validator lineage tracking:** Credentials issued through Civic cannot be expired, revoked, or traced back to a certified validator, making them unsuitable for environments that require auditable compliance trails.
- **Credentials lack specificity for regulatory onboarding:** Civic's credentials do not encode regulatory attributes such as jurisdictional eligibility, accreditation status, or ESG alignment, which are increasingly required in investor onboarding.

Why the Shortcomings are Problematic for Clients:

- **Verification cannot be trusted alone in regulated environments:** Civic credentials lack standardised regulatory metadata, so financial institutions cannot rely on them to satisfy compliance obligations, requiring additional layers of verification and documentation.
- **Increases overhead and legal exposure for fund managers:** Civic is absent regulator-aligned verification, so fund managers must implement manual screening processes and redundant KYC systems, exposing them to increased costs and legal liability.
- **Fragmented compliance leaves platforms vulnerable to misclassification:** Platforms risk admitting ineligible participants, leading to compliance breaches and enforcement actions, because they are relying on general-purpose credentials without investor classification or jurisdictional mapping.

How this Invention Addresses these Shortcomings:

- **Purpose-built for investment onboarding and regulatory validation:** This invention supports the specific needs of financial institutions by issuing credentials that reflect investor type, jurisdictional status, and regulatory requirements for onboarding and participation.
- **Smart contract-readable, expiry-controlled, and traceable:** Credentials are structured for automated enforcement via smart contracts, include expiration dates and revocation mechanisms, and maintain validator lineage for full auditability.
- **Supports ESG and investor class modules for complex fund requirements:** Credentialing using this invention allows for tagging ESG alignment and investor classifications, ensuring platforms can filter participants according to fund mandates and regulatory conditions.

9. IBM Blockchain Identity

How the Product Operates

- **Enterprise-focused digital identity built on Hyperledger Fabric:** IBM Blockchain Identity is designed for use within permissioned enterprise blockchain environments, leveraging Hyperledger Fabric to support secure identity management across business networks.
- **Enables organisations to issue and verify credentials across ecosystems:** The platform allows corporate and government entities to create, manage, and validate digital credentials, enabling secure information exchange within and between institutional ecosystems.
- **Often tied to enterprise workflows (supply chain, government, health):** IBM's identity system is primarily applied in non-financial use cases such as supply chain provenance, health records, and government credentialing, rather than regulated financial onboarding.

Differentiation of the Product from this Invention

- **Operates on permissioned infrastructure with limited Web3 portability:** IBM's platform is closed to public networks and does not natively support interaction with decentralised finance (DeFi) systems or public smart contracts, which limits its flexibility.
- **Lacks features for regulatory onboarding or investment fund access:** It does not support investor accreditation, jurisdictional equivalence, or ESG integration, which are core to this invention's utility in capital markets.
- **No jurisdictional compliance logic or ESG credentialing:** The IBM system lacks mechanisms to classify users according to financial regulations or associate credentials with ESG-related attributes or restrictions.

Shortcomings of the Product

- **Incompatible with public blockchain and token-based platforms:** Credentials issued within IBM's closed infrastructure cannot be ported to or verified within open blockchain ecosystems, limiting their usefulness in decentralised markets.
- **No support for smart contract verification of credentials:** IBM's system does not offer credentials that can be programmatically checked by smart contracts, making it unsuitable for automated access control in tokenised financial systems.

- **Not built for investor lifecycle compliance or cross-border use:** The platform does not support features such as expiration, revocation, jurisdictional mapping, or reusable credentials that are essential for regulated investor workflows.

Why the Shortcomings are Problematic for Clients

- **Cannot integrate into decentralised or permissionless environments:** Institutions operating in decentralised markets cannot use IBM's credentials for onboarding or compliance, forcing them to maintain separate identity systems for public blockchain engagement.
- **Fund managers must build parallel systems for compliance:** IBM's solution lacks investor-specific regulatory features, so asset managers are required to build separate compliance infrastructures to meet onboarding and regulatory obligations.
- **Limits interoperability and introduces vendor lock-in:** Credentials issued through IBM's network are tightly coupled with its proprietary stack, making it difficult for organisations to integrate with third-party platforms or exit the ecosystem without major redevelopment.

How this Invention Addresses these Shortcomings

- **Blockchain-native, smart contract-verifiable credentials:** This invention is designed to operate on public and private blockchains, issuing credentials that are readable by smart contracts and usable in decentralised platforms for automated access decisions.
- **Designed for financial compliance use across jurisdictions:** This invention supports multi-jurisdictional regulatory requirements, including KYC/AML, investor accreditation, and ESG verification, making it ideal for global wholesale onboarding.
- **Portable across public and private ecosystems with verifiable metadata:** Credentials are structured to operate across different platforms, combining decentralised portability with standardised, verifiable metadata for regulatory and operational alignment.

Similar patents and their operations

1. US20220058636A1 – Tokenization Platform

How the Patent Operates:

- **Smart Contracts:** The patent facilitates token-based transactions using smart contracts, which are used to represent and manage both physical and digital assets on a blockchain.
- **Asset Representation:** It allows for the digital representation of physical assets on-chain, enabling ownership and transaction tracking within a decentralised ledger environment.

Differentiation of the Patent from this Invention:

- **Functionality:** The patent focuses on the tokenisation of assets and their associated transactions, while this invention is centred on the issuance and ongoing management of compliance credentials tied to investor eligibility.
- **Use Case:** This invention is intended to verify and manage institutional compliance of wholesale investors across jurisdictions, not to facilitate the creation or trading of tokenised assets as the patent does.

Shortcomings of the Patent:

- **Centers on asset tokenisation, not on participant or credential compliance:** The patent's core innovation lies in asset creation and representation, with no native functionality for verifying the regulatory status or compliance standing of transaction participants.
- **Lacks a modular system for credential issuance, expiration, or jurisdictional adaptation:** It does not provide a framework to issue, revoke, or map compliance credentials to different regulatory regimes or update them dynamically.
- **Does not enable credential-based access control or compliance enforcement:** Access to tokenised assets is not governed by credential states or real-time compliance checks, leaving enforcement responsibilities to external systems.

Why the Shortcomings are Problematic for Clients:

- **Tokenisation of assets without participant compliance tools leads to regulatory blind spots:** Platforms may allow ineligible or unverified users to interact with regulated assets,

creating legal and operational risks due to the lack of built-in compliance mechanisms for user access control.

- **Clients must bolt on external systems to screen users, resulting in fragmented workflows and compliance gaps:** Without integrated compliance credentialing, firms must manually screen and manage investor eligibility through separate tools, increasing administrative burden and potential for inconsistency.
- **No ability to tailor access based on verified credentials leaves firms unable to automate participation controls:** This shortcoming prevents real-time validation of investor eligibility, slowing onboarding, and increasing the risk of regulatory violations in sensitive markets.

How this Invention Addresses these Shortcomings:

- **This invention introduces a participant-layer compliance system that plugs into asset/token ecosystems:** It enables platforms to check investor eligibility via dynamic credentials at the identity level, adding a regulatory filter before token interaction.
- **Shifts focus from asset issuance to who can participate and why, based on live credential states:** This invention ensures that access to regulated assets is controlled through real-time, updatable credentials that reflect current investor classification and jurisdictional eligibility.
- **Enables cross-jurisdiction compliance enforcement via verifiable credential metadata:** Credentials issued by this system include structured metadata that supports jurisdictional mapping and validation logic, allowing platforms to comply with multiple regulatory regimes through a unified framework.

2. WO2019067603A1 – Compliance Aware Tokenization

How the Patent Operates:

- **Attribute-Based Access Control (ABAC):** The patent implements a system of attribute-based access control to govern asset transfers. Users must meet specific compliance-related attributes, such as identity verification or jurisdictional eligibility, to execute token transactions.

- **Smart Contracts:** Compliance rules are enforced via smart contracts, which automatically apply regulatory conditions to transactions and may also assist in generating compliance-related audit logs or regulatory reports.

Differentiation of the Patent from this Invention:

- **Compliance Enforcement:** The patent enforces compliance by embedding access rules into transactions using ABAC, while this invention manages dynamic, modular compliance credentials that can be verified across platforms and evolve independently of the tokens or smart contracts.
- **Application:** The patent focuses on applying rules at the transactional level, whereas this invention provides a full credential lifecycle management system that allows institutions to issue, renew, revoke, and validate investor credentials for multiple regulatory use cases.

Shortcomings of the Patent:

- **Relies heavily on static, hardcoded ABAC:** Compliance rules must be programmed into the smart contract at the time of deployment, making it difficult to adapt to regulatory changes without reengineering or redeploying contract logic.
- **Embeds compliance logic in tokens without modular or portable credentialing:** Compliance is tied to the asset rather than the user, which limits the ability to apply the same credential across different platforms or investment types.
- **Poorly suited to environments where regulatory conditions or user status change frequently:** The system does not support automatic updates to user status or investor credentials, which are essential in jurisdictions requiring periodic revalidation or renewal of compliance data.

Why the Shortcomings are Problematic for Clients:

- **Hardcoded access controls do not allow for quick adaptation to new regulations, forcing costly system changes:** Organisations must update or redeploy smart contracts to reflect new rules when compliance conditions evolve, incurring significant development and audit overheads.

- **Lack of modular credentialing complicates updates, credential renewal, or multi-jurisdictional compliance:** Institutions cannot issue or update credentials independently from the tokens or contracts, making compliance management cumbersome, especially when dealing with multiple regulatory regimes.
- **Clients cannot issue reusable or cross-platform credentials, limiting interoperability and scaling across ecosystems:** Absent portable credentials, platforms are isolated and cannot benefit from shared compliance verification, increasing friction and reducing the ability to expand across jurisdictions.

How this Invention Addresses these Shortcomings:

- **This invention treats credentials as dynamic, verifiable, and portable digital assets:** Compliance credentials can be updated, revoked, or renewed in real time and are designed to be interoperable across platforms, supporting both public and private blockchain environments.
- **Maintains a full credential lifecycle: issuance, attestation, expiration, revocation, and jurisdictional scoping:** The system enables comprehensive lifecycle management, ensuring credentials remain valid, accurate, and aligned with current regulatory conditions.
- **Makes compliance adaptive, so credentials can evolve independently of the token or asset structure:** Compliance decisions are based on verifiable off-chain metadata linked to on-chain tokens, allowing for responsive, real-time compliance without altering the core logic of the asset or its associated smart contract.

3. US Patent Application US20210350343A1 – Blockchain-Based AML/KYC Compliance Network

How the Patent Operates:

- **Describes a blockchain-based compliance verification network:** The patent outlines a system where AML and KYC checks are conducted within a blockchain-based infrastructure to validate user identities before transactions.
- **Performs AML and KYC screenings:** The system screens participants against regulatory requirements for AML and KYC, storing verification data in the blockchain to serve as a persistent proof of compliance.

- **Embeds compliance data directly into the blockchain as proof of verification:** Once a user passes screening, the verification data is stored immutably on-chain, acting as a permanent record of compliance status.
- **Allows users to transact only after passing screening:** Access to transactions is conditional upon having a verified compliance status, with unauthorised users being automatically excluded from participation.

Differentiation of the Patent from this Invention:

- **This invention does not embed compliance data directly into the blockchain:** Instead, it uses cryptographic references to encrypted off-chain metadata to preserve user privacy and ensure compliance data can be updated, revoked, or scoped according to jurisdiction.
- **This invention uses portable, verifiable credentials that are managed off-chain but referenced on-chain:** Unlike the patent, which stores static verification data on-chain, this invention allows credentials to be managed off-chain, enabling greater adaptability and privacy.
- **This invention focuses on credential lifecycle management, not just proof-of-screening:** It includes tools to issue, renew, expire, and revoke credentials, providing a full compliance lifecycle that goes beyond one-time screening.
- **This invention's system is designed for wholesale investors, while this application is user-centric:** The patent targets individual users in consumer or retail scenarios, whereas this invention serves regulated financial institutions that require wholesale-grade investor onboarding and verification.

Shortcomings of the Patent:

- **Embeds compliance data directly on-chain, raising privacy and regulatory concerns:** Storing personally identifiable or sensitive data directly on a public blockchain creates potential conflicts with data protection laws, such as the European Union General Data Protection Regulation (GDPR), and reduces the ability to manage, modify, or delete such information.
- **Does not support credential expiration, revocation, or jurisdiction-specific variation:** Once compliance data is written on-chain, it cannot easily reflect changes in regulatory classification or investor eligibility, making it unsuitable for dynamic compliance requirements.

- **Designed for one-time compliance checks with no revalidation mechanism:** The system verifies users at a single point in time, without ongoing monitoring or re-screening, which is inconsistent with regulatory obligations that require periodic re-verification.
- **Focused on individual user screening, not scalable institutional compliance management:** The architecture lacks features to support complex institutional workflows, such as managing multi-jurisdictional investor classes or performing large-scale credential operations.

Why the Shortcomings are Problematic for Clients:

- **Clients risk breaching data privacy laws by embedding sensitive compliance data on-chain without recourse to modify or delete it:** Permanently storing sensitive information on a public ledger may violate global privacy regulations and creates irreversible records that could expose users to identity theft or misuse.
- **Without credential expiration or jurisdictional scope, firms may allow ineligible participants into restricted offerings:** Static credentials do not reflect time-bound or geography-based compliance rules, meaning investors may retain access to offerings they are no longer eligible for.
- **One-time verification does not meet the needs of ongoing regulatory obligations (e.g. annual KYC refresh):** Regulatory frameworks typically require regular updates to investor information, and systems that lack lifecycle tracking force firms to re-onboard users manually or risk non-compliance.
- **Institutions managing large investor pools need flexible, real-time credential validation, not just a yes/no screen:** Scalable financial operations require sophisticated credential states (e.g., “expired,” “under review,” “revoked”) rather than binary access logic, which the patent does not support.

How this Invention Addresses these Shortcomings:

- **Uses verifiable credentials that can be updated, revoked, or scoped to specific regulatory needs:** This invention enables compliance credentials to reflect real-time changes in investor status, regulatory frameworks, or jurisdictional requirements through structured lifecycle governance.

- **Keeps sensitive compliance data off-chain, improving privacy and adaptability:** This invention allows for secure, privacy-preserving verification without compromising auditability, by storing data off-chain and referencing it cryptographically on-chain.
- **Designed for regulated markets, enabling dynamic compliance enforcement for institutional roles and jurisdictions:** It supports advanced regulatory use cases such as jurisdictional equivalence, multi-role investor types, and ESG integration, all of which are critical in global institutional finance.

4. US Patent Application US20220188836A1 - Blockchain-Verified AML/KYC Identity

How the Patent Operates:

- **Embeds AML-compliant user data into the blockchain:** The patent proposes a system in which compliance-related user data, AML and KYC information, is stored directly on the blockchain as part of the verification process.
- **Issues public/private keys to verified users:** Once users are verified, they are assigned cryptographic key pairs that allow them to interact with the system and access services gated by compliance verification.
- **Only verified users can participate in transactions:** The system restricts access to blockchain-based transactions to those users whose compliance status has been previously verified and encoded on-chain.

Differentiation of the Patent from this Invention:

- **This invention allows credential-based access control across systems—not just a gatekeeping mechanism:** Unlike the binary access approach in the patent, this invention uses structured credentials that define scope, jurisdiction, and investor classification, enabling nuanced access logic.
- **This invention provides layered and scoped credentials (e.g., for different asset types or jurisdictions):** The system supports complex regulatory layering, such as being a “wholesale

investor” in Australia and an “accredited investor” in the U.S., all within a single credential framework.

- **Supports a broader range of regulatory credentials, not just KYC/AML:** In addition to basic compliance checks, this invention enables integration of ESG attestations, jurisdictional eligibility, and investor classification, offering end-to-end onboarding solutions for financial institutions.

Shortcomings of the Patent:

- **Offers a binary, static verification model (verified/unverified) with no credential granularity:** The system determines user eligibility with a simple yes/no flag and lacks the ability to represent complex compliance statuses or role-based permissions.
- **Lacks support for credential lifecycle management such as expiry, renewal, or revocation:** Once issued, compliance data cannot be updated or revoked, meaning users may retain verified status even when their regulatory position has changed.
- **Cannot adapt to changes in participant status (e.g. residency, accreditation):** If a user’s residency or financial status changes, the system does not accommodate those shifts without manual re-entry or a new identity being created.
- **Credentials are tied to one blockchain, limiting portability and interoperability:** The design confines credentials to a specific chain or system, making them difficult to use across platforms or jurisdictions that rely on different blockchain technologies.

Why the Shortcomings are Problematic for Clients:

- **A binary verification system provides insufficient granularity to meet different regulatory thresholds (e.g. accredited vs. wholesale investor):** Fund managers and platforms often need to distinguish among multiple investor types and risk profiles, which binary systems cannot support, resulting in blunt access decisions and regulatory gaps.
- **Changes in participant status (residency, license, sanctions) cannot be reflected without re-verification or renewal tools:** When a user’s compliance standing evolves, the absence of a credential lifecycle leads to outdated permissions remaining active, increasing compliance risk.
- **Lack of credential portability locks clients into single ecosystems, reducing operational flexibility across platforms:** Institutions are forced to maintain multiple systems or re-onboard users when switching platforms, leading to inefficiency, fragmentation, and elevated costs.

- **Financial institutions must demonstrate adaptive compliance programs, which this static model cannot support:** Regulators expect institutions to respond dynamically to compliance changes; static credentials prevent this and may result in audit failures or penalties.

How this Invention Addresses these Shortcomings:

- **Enables real-time credential status checks with expiry, renewal, and revocation flows:** This invention continuously manages investor credentials across their lifecycle, ensuring that only up-to-date, verified investors can access regulated offerings.
- **Allows granular and dynamic credentials (e.g. wholesale investor, accredited status, FATCA alignment):** Each credential encodes structured metadata to represent investor classification, jurisdictional eligibility, and optional ESG factors, enabling fine-tuned access logic.
- **Credentials are portable and interoperable, working across chains and compliance systems:** The design supports seamless use of credentials on multiple blockchain platforms and traditional systems, reducing onboarding friction and supporting cross-border scalability.

5. US Patent US11483154B2 – Blockchain Supplier Attestation

How the Patent Operates:

- **Uses blockchain to validate supplier information using certificates of attestation:** The patent describes a system for verifying supplier-provided information—such as company details, certifications, or compliance documents—by issuing certificates of attestation stored on a blockchain.
- **Certificates are issued to verify the integrity of factsheets or documents:** Third-party verifiers issue blockchain-based certificates that confirm the authenticity of documents like supplier profiles, contracts, or technical sheets.
- **Focused on supply chains and supplier documentation, not identity or compliance status:** The patent is intended for verifying the legitimacy of suppliers and the accuracy of business records, rather than for verifying an individual's or institution's regulatory compliance status.

Differentiation of the Patent from this Invention:

- **This invention issues credentials to wholesale participants, not factsheet attestations:** This invention provides regulated investors with credentials that reflect their compliance status, investor classification, and jurisdictional eligibility, whereas the patent deals with document verification in the supply chain domain.
- **The credentials are live, dynamic, and use case-specific—e.g. investor eligibility or onboarding compliance:** Unlike static attestations, this invention's credentials evolve over time to reflect changes in regulatory status, enabling dynamic enforcement of access and participation in financial ecosystems.
- **This invention is designed for financial regulatory infrastructure, not general-purpose document attestation:** This invention is tailored specifically for onboarding and compliance workflows in capital markets and institutional finance, rather than general business-to-business documentation.

Shortcomings of the Patent:

- **Designed for document validation, not participant compliance or regulatory enforcement:** The patent ensures the authenticity of documents, but it does not offer tools for verifying or managing the compliance status of individuals or institutions involved in regulated financial activities.
- **Attestations are passive and not tied to user roles or regulatory status:** The blockchain certificates confirm that a document exists and is genuine, but they do not indicate whether the holder is eligible or authorised to engage in a regulated activity.
- **No support for credential lifecycle features like expiry, jurisdictional scope, or revocation:** Once issued, the attestations do not expire or adapt to changing regulatory conditions, and cannot be revoked if a supplier or user becomes non-compliant.
- **Not built for real-time compliance or eligibility enforcement in regulated financial settings:** The system lacks integration with smart contracts or transaction logic, meaning it cannot be used to automatically gate access based on up-to-date compliance checks.

Why the Shortcomings are Problematic for Clients:

- **Clients need active and enforceable credentials tied to investor eligibility—not static attestations of passive data:** In regulated financial environments, institutions must be able to verify that a participant remains compliant at the time of each transaction, which static document attestations cannot support.
- **Absent role-specific or time-sensitive credentialing, institutions face compliance failures during audits or transactions:** If a user’s eligibility changes but there’s no mechanism to reflect that in real time, firms risk engaging with ineligible participants and breaching regulatory requirements.
- **This model cannot support regulatory workflows like onboarding risk scoring or jurisdiction-based limitations:** The lack of programmable compliance logic means firms must use manual processes to enforce jurisdictional access restrictions, increasing the risk of inconsistency or oversight.
- **Lacks enforcement mechanisms needed for real-time transaction gating based on credential status:** Platforms cannot enforce rules such as “only verified investors from X jurisdiction may participate”, because the attestation system does not integrate with smart contracts or validation APIs.

How this Invention Addresses these Shortcomings:

- **Introduces dynamic, reusable credentials for regulatory compliance:** Credentials issued by this invention evolve over time and are verifiable by third parties, allowing platforms to rely on them for real-time compliance decisions.
- **Enables automated verification, expiration, revocation, and multi-jurisdictional use:** Each credential includes built-in logic for lifecycle management, including expiry and revocation, and supports cross-border equivalence to meet jurisdiction-specific rules.
- **Tailored to support financial institutions and regulated markets:** This invention’s credentialing architecture is designed specifically for use in highly regulated industries, such as wholesale investing, where eligibility and auditability are critical.

6. AU2018243625 – Advanced New Technologies Co., Ltd.

How the Patent Operates:

- **Processes transaction requests using a decentralised blockchain:** The patent describes a blockchain-based system that handles transaction requests in a decentralised manner, allowing changes to be processed and validated by a network of distributed nodes.
- **Ensures replicated changes across nodes for consensus:** The system achieves consensus by ensuring that any changes to the ledger are synchronised and replicated across all participating nodes in the network, preserving data integrity.
- **Enhances privacy and integrity in blockchain-based transactions:** The system aims to maintain the confidentiality of sensitive information while ensuring the accuracy and trustworthiness of blockchain data, by using distributed consensus and encrypted messaging.
- **Nodes can validate and initiate changes, increasing security:** The architecture allows trusted nodes to participate in both the validation and initiation of transactions, which enhances overall system resilience and mitigates the risk of centralised failure.

Differentiation of the Patent from this Invention:

- **Focuses on transaction processing within a blockchain network, whereas this invention emphasises the issuance and management of compliance credentials:** The patent is centred on how data is processed and validated on-chain, while this invention is concerned with issuing verifiable compliance credentials that govern access to regulated financial activities.
- **Addresses privacy and security at the transaction level, while this invention manages compliance verification and credential lifecycle:** The patent and this invention value privacy. However, this invention offers credential-level compliance verification tools that support issuance, renewal, and revocation over time, rather than focusing solely on data transmission integrity.
- **Operates within the blockchain's transaction validation process, unlike this invention, which functions as an external compliance layer:** The patent's functionality is embedded in the core infrastructure of the blockchain, whereas this invention integrates with blockchain platforms as a credentialing and compliance overlay.

Shortcomings of the Patent:

- **Focuses on transaction integrity, not participant compliance:** The system of the patent ensures transactions are securely processed, but does not provide a mechanism to verify whether the participants themselves meet legal or regulatory eligibility requirements.
- **Lacks a system for issuing, managing, or verifying compliance credentials:** There is no provision for creating verifiable credentials for investors or institutions, nor any process for updating, revoking, or validating those credentials in regulated environments.
- **Offers no support for jurisdictional compliance variation or dynamic regulatory adaptation:** The patent lacks features that allow it to adapt to different legal frameworks or respond to changes in participant compliance status across regions.

Why the Shortcomings are Problematic for Clients:

- **Financial service providers must screen participants, not just protect transactions; the patent overlooks that need entirely:** In regulated markets, institutions must ensure that only eligible, verified investors can participate—something this system cannot do because it validates data but not users.
- **No way to issue or revoke credentials leaves clients unable to meet “know your investor” obligations:** Absent tools to issue or manage compliance credentials, financial institutions cannot demonstrate adherence to onboarding and due diligence requirements.
- **Jurisdictional non-compliance could result from admitting parties whose credentials don’t meet local regulatory standards:** The lack of jurisdictional mapping or credential validation exposes platforms to the risk of allowing ineligible users to transact, leading to potential legal violations and enforcement actions.

How this Invention Addresses these Shortcomings:

- **Introduces a system for issuing portable, verifiable compliance credentials separate from the blockchain’s transaction process:** This invention creates a distinct layer for compliance, ensuring credentials can be independently managed and validated across platforms and jurisdictions.

- **Supports dynamic credential management, including expiration and revocation, adaptable to various jurisdictions:** This invention includes lifecycle logic to handle regulatory changes, allowing credentials to expire, renew, or be revoked as investor circumstances or laws evolve.
- **Enhances compliance verification by focusing on participant credentials rather than solely on transaction integrity:** This invention adds a regulatory eligibility layer to blockchain ecosystems, ensuring that only credentialed, compliant participants can access and interact with sensitive financial products.

7. AU2018202562 – Identitii Ltd

How the Patent Operates:

- **Securely attaches detailed compliance info to financial messages:** The patent provides a method for embedding compliance-related data into financial messages, enabling institutions to transmit supplementary regulatory information alongside standard transaction details.
- **Allows institutions to exchange AML/KYC information:** The system supports the secure exchange of AML and KYC data between parties, facilitating regulatory compliance without altering core messaging infrastructure.
- **Facilitates regulatory compliance without changing core financial messaging systems:** It integrates with existing Society for Worldwide Interbank Financial Telecommunications (SWIFT) or International Organization for Standardization (ISO) 20022 financial information formats, allowing compliance metadata to be sent without requiring system-wide upgrades or replacements.
- **Ensures integrity of messages using blockchain anchoring:** Financial messages are anchored to a blockchain ledger to guarantee message authenticity, providing an immutable audit trail that enhances transparency and accountability.

Differentiation of the Patent from this Invention:

- **Emphasises the secure sharing of transaction-related information, whereas this invention focuses on the issuance and management of compliance credentials:** Identitii's solution deals with embedding supplemental data into transaction messages, while this invention governs investor eligibility and access via independent credential structures.

- **Operates within the context of financial messaging systems, unlike this invention, which functions as a standalone compliance credentialing system:** This invention is designed to issue credentials to investors that persist across platforms, rather than piggybacking compliance metadata onto financial messages.
- **Aims to enhance transparency in financial transactions, while this invention provides a framework for verifying participant compliance status:** The patent helps ensure message-level integrity; this invention helps ensure only verified participants are permitted to engage with regulated investment opportunities.

Shortcomings of the Patent:

- **Designed for secure message annotation, not credential issuance or management:** The system supports attaching data to messages but lacks any mechanism to create, manage, or revoke investor credentials or classifications.
- **Compliance logic is passive and not enforceable via credential status:** Institutions must still rely on manual or external systems to evaluate the compliance status of message recipients or senders.
- **Does not support dynamic credential lifecycle management or role-based verification:** The platform does not accommodate expiration, revalidation, or jurisdictional mapping of credentials, nor does it enable role-specific access control.
- **Not designed for regulated identity verification at scale:** The system does not scale to handle onboarding or ongoing compliance verification for large investor populations across jurisdictions.

Why the Shortcomings are Problematic for Clients:

- **Messaging-level compliance metadata is not enforceable or dynamic, which leaves gaps in transaction eligibility enforcement:** Institutions cannot rely solely on annotated financial messages to determine whether a participant is currently compliant, making enforcement inconsistent and unreliable.
- **Clients cannot rely on message-based attachments to manage credential updates or revocation over time:** Firms must maintain separate processes to monitor eligibility, creating inefficiencies, because compliance status is not managed through dynamic credentials.

- **Without centralised credential logic, firms must duplicate compliance checks across systems, raising cost and risk:** Every platform must perform its own due diligence, increasing overhead and introducing the potential for inconsistent application of regulatory requirements.

How this Invention Addresses these Shortcomings:

- **Offers a dedicated system for issuing and managing compliance credentials, independent of transaction information sharing:** This invention decouples compliance verification from financial messaging, allowing institutions to manage eligibility at the participant level through verifiable, portable credentials.
- **Includes comprehensive credential lifecycle management features, adaptable to regulatory changes:** It supports expiration, revocation, renewal, and jurisdictional scoping to ensure that investor credentials remain accurate and up to date.
- **Enhances compliance verification by providing verifiable credentials for participants, ensuring adherence to regulatory requirements:** Credentials are structured to reflect investor class, jurisdictional status, and ESG alignment, enabling platforms to enforce participation rules programmatically and in real time.

8. AU2018202563 – Bloxian Technology Pty Ltd

How the Patent Operates:

- **Manages digital identity via blockchain:** The patent outlines a system for creating and managing digital identities using blockchain technology, offering a decentralised and tamper-resistant method of identity storage.
- **Creates immutable identity records for individuals or entities:** The system generates blockchain-based identity profiles that cannot be altered retroactively, ensuring trust and traceability across applications.
- **Allows individuals to control access to their data:** Users retain ownership of their personal information and can selectively disclose data to third parties, enhancing privacy and user autonomy.
- **Enables third-party verification of identity data:** External parties can verify the authenticity of an individual's identity data without direct access to sensitive information, using cryptographic proofs anchored on-chain.

Differentiation of the Patent from this Invention:

- **Concentrates on digital identity management, whereas this invention specialises in compliance credential issuance and verification:** Bloxian's solution provides foundational identity infrastructure, while this invention builds on identity to manage investor eligibility and regulatory compliance across jurisdictions.
- **Provides a framework for identity control and verification, unlike this invention, which focuses on compliance status and regulatory adherence:** This invention extends beyond identity to include structured compliance elements like investor classification, jurisdictional mapping, and ESG declarations.
- **Operates within the realm of digital identity ecosystems, while this invention is tailored for financial compliance contexts:** The use case for this invention is specifically targeted at onboarding and verifying institutional and wholesale investors under financial regulations.

Shortcomings of the Patent:

- **Emphasises generic digital identity control, not regulatory compliance status:**
- The system supports identity sovereignty, but it does not provide information about whether an individual or institution meets specific regulatory criteria for financial participation.
- **No mechanism for issuing, adapting, or verifying compliance-specific credentials:** The patent lacks tools to issue credentials that reflect investor class, regulatory standing, or eligibility in specific jurisdictions.
- **Lacks lifecycle control such as revalidation or jurisdictional scoping:** Once issued, identity records remain static; the system does not support renewal, expiration, or compliance changes over time.
- **Not optimised for financial regulation or wholesale compliance workflows:** The architecture is not designed to handle multi-step, regulator-mandated onboarding processes or jurisdiction-specific validation rules required in financial services.

Why the Shortcomings are Problematic for Clients:

- **Digital identity management alone is insufficient for compliance with financial regulations requiring dynamic eligibility checks:** Institutions cannot rely on identity alone to determine

whether an investor qualifies under current financial laws, especially when jurisdiction, risk class, or ESG factors are relevant.

- **Lack of role-based or regulation-specific credentialing forces institutions to manually assess investor eligibility:** Absent automated compliance layering, firms must conduct manual reviews, increasing costs and the chance of human error.
- **No lifecycle control means clients may act on outdated identity data, exposing them to breach or fraud risks:** Static credentials may remain valid even after an investor becomes ineligible, creating potential regulatory violations or reputational harm.

How this Invention Addresses these Shortcomings:

- **Provides a specialised system for issuing compliance credentials, ensuring participants meet regulatory requirements:** This invention creates and manages credentials that reflect whether an investor satisfies specific legal definitions, such as “wholesale investor” or “accredited investor.”
- **Supports credential adaptation to various jurisdictions and regulatory frameworks:** This invention maps investor classifications across global regulatory systems, allowing a single credential to validate eligibility in multiple countries based on encoded equivalence rules.
- **Enhances compliance processes by focusing on verifiable compliance status rather than general identity verification:** This invention goes beyond who someone is—it establishes whether they are currently allowed to participate in a given investment, based on dynamic, verified credentials.

In Summary: Distinguishing this invention from existing products and patents

This invention distinguishes itself from existing products and patents through the use of:

- Non-transferable, investor-controlled compliance tokens that embed jurisdiction-specific credentials

- A cross-jurisdictional equivalence engine that maps investor eligibility across multiple regulatory regimes (e.g. Australia, United States, European Union)
- Integration of privacy-preserving mechanisms, including selective disclosure and support for zero-knowledge proofs
- A token lifecycle management system for real-time revocation, attestation updates, and audit trails
- Compatibility with both traditional financial institutions and DeFi platforms, enabling flexible deployment in hybrid environments

In addition to its technical distinctions, this invention is also **more comprehensive in scope** than prior products and patents. It provides a unified framework that encompasses credential issuance, multi-jurisdictional compliance mapping, selective disclosure, and lifecycle governance, all integrated within a blockchain environment. Existing products and patents typically address isolated functions (such as embedding KYC data or AML verification), whereas this invention offers a **full-stack compliance infrastructure** that is modular, interoperable, and also adaptable across traditional and decentralised financial systems. Its architecture supports seamless onboarding, cross-border validation, and privacy-aware auditing in a manner that is scalable and regulatory-aligned, positioning it as a **next-generation compliance layer** for wholesale finance.

BRIEF DESCRIPTION OF THE DRAWINGS

- **Figure 1: System architecture overview of the SOLO Credentialing Framework:** FIG. 1 is a system architecture diagram of the SOLO Credentialing Framework, showing the interactions between the validator, credential issuance engine, blockchain infrastructure, off-chain metadata storage, jurisdictional equivalence engine, and investment platforms. It illustrates how non-transferable compliance tokens are issued and used for real-time investor eligibility validation.

- **Figure 2: Jurisdictional equivalence engine mapping investor status across multiple regions:** FIG. 2 illustrates the Jurisdictional Equivalence Engine, which maps investor classification statuses across different regulatory regimes. It shows how equivalent investor statuses (e.g., “wholesale investor” in Australia, “accredited investor” in the United States) are aligned and encoded into the token’s metadata for cross-border compliance.
- **Figure 3: Metadata structure and token linkage using hash references:** FIG. 3 depicts the structure and flow of compliance metadata linked to a SOLO Token. It shows how encrypted off-chain metadata, privacy-preserving mechanisms (e.g., zero-knowledge proofs), and a permissioning module interact to support selective disclosure and access control by the investor.
- **Figure 4: Credential issuance flow for lifecycle management:** FIG. 4 illustrates the credential issuance and lifecycle management process. It highlights how SOLO Tokens are minted following validator attestation, and how lifecycle events such as issuance, revocation, and renewal are logged and managed on-chain for sustained compliance.
- **Figure 5: Token lifecycle events including expiry, revocation, and renewal triggers:** FIG. 5 shows token state transitions across various lifecycle triggers. It depicts how SOLO Tokens may become inactive upon expiry, be revalidated through renewal, or be revoked by validators, with all status changes recorded on-chain to ensure real-time platform synchronisation.
- **Figure 6: ESG credential integration and use in onboarding filters:** FIG. 6 presents the ESG credential integration flow. It demonstrates how third-party ESG attestations are linked to the investor’s credential, enabling platforms to filter participants based on sustainability criteria and allowing investors to present ESG-aligned credentials during onboarding.

DETAILED DESCRIPTION OF EMBODIMENTS

Introduction: Abbreviated Overview of the Functional Flow of this invention

1. Validator Stage

- Investor submits identity and compliance documents to an authorised validator.
- Validator performs checks:
 - KYC/AML
 - Accreditation (e.g., wholesale or professional investor)
 - Tax residency (FATCA/CRS)
 - ESG credentials (optional)
- Validator digitally signs an attestation using their private key.

2. Credential Issuance

- The Credential Issuance Engine receives the signed attestation.
- Mints a **non-transferable ERC-721 token** to investor's wallet.
- Token includes:
 - Link (cryptographic hash) to **off-chain encrypted metadata**
 - Issuer ID, timestamp, jurisdictional status, ESG status

3. Metadata Management

- Metadata stored in IPFS/S3, encrypted using investor's public key.
- Structured using interoperable JSON schema.
- Supports Merkle roots and zero-knowledge-proof-ready design.

4. Permissioning (Investor-Controlled Disclosure)

- Investor uses smart contract interface to:
 - Grant field-level access (e.g., accreditation only)
 - Define expiry on access rights
 - Revoke or renew access at will
 - Audit logs of access events may be written on-chain.

5. Jurisdictional Equivalence Mapping

- Engine compares and maps investor classifications across jurisdictions (e.g., AU ↔ SG ↔ US).
- Encodes equivalence in registry smart contract.
- Adapts token metadata to reflect cross-border recognition logic.

6. ESG Credentialing (Optional)

- ESG auditors certify sustainability credentials.
- Their attestations are linked cryptographically to the token.
- Investors can present ESG-aligned status to participating funds.

7. Lifecycle Management

- Tokens include expiration logic (e.g., 12–24 months).
- Lifecycle events:
 - Expiry trigger → status set to inactive
 - Renewal → triggers new validation
 - Revocation → triggered by validator/system on status change

8. Investment Platform Integration

- Funds or platforms query via:
 - Smart contract confirms token validity, jurisdiction, ESG filters.
 - If valid, the platform permits participation

Preferred embodiment / Comprehensive Overview of how this Invention Works

In a preferred embodiment, this invention is implemented as a system for issuing and managing non-transferable blockchain-based compliance credentials, referred to as “SOLO Tokens,” for use by wholesale investors. The system is designed to enhance regulatory onboarding, ensure credential portability across jurisdictions, and reduce duplicative compliance workflows.

The system comprises the following functional modules:

- (a) **Validator Interface:** A secure API gateway and identity processing layer that enables authorised validators (e.g., [AUSTRAC]-registered KYC/AML providers, licensed compliance bodies) to submit verified attestations. The system accepts signed attestations verifying an investor's identity, status under s.708 of the *Corporations Act 2001* (Cth), AML/CTF obligations, and optionally, ESG profile data.
- (b) **Credential Issuance Engine:** Upon receiving a valid attestation, the engine cryptographically verifies the validator's signature using its public key. It then generates a SOLO Token, encoded as a non-transferable Ethereum Request for Comments (ERC)-721 or equivalent Non-Fungible Token (NFT). Each token is minted to the investor's self-custodied blockchain wallet address. The token cannot be transferred, ensuring only the verified investor can use it.
- (c) **Metadata Generation Module:** Compliance metadata is embedded in or linked to the token via secure hash pointers. Off-chain metadata includes:
- Jurisdictional accreditation matrix (e.g., meets "wholesale" status in Australia, "accredited" in United States)
 - Validator ID and timestamp
 - Expiry date and renewal trigger
 - Optional ESG attestations (e.g., Sustainable Development Goals [SDG] alignment, sector exclusions)

Metadata is encrypted and stored on a decentralised file system such as Interplanetary File System (IPFS) or Arweave, with access permissions managed by the investor via smart contract.

- (d) **Jurisdictional Equivalence Engine:** This component matches regulatory definitions across different financial systems. For example, an investor verified as a "sophisticated investor" in Singapore may be automatically mapped to "wholesale investor" status under the *Corporations Regulations 2001* (Cth) via an equivalence rule encoded in the smart contract or oracle network.
- (e) **Lifecycle Management Module:** The system monitors token status and supports revocation and renewal flows. Validators or platforms may request revocation if the investor becomes non-compliant. Expiry may be enforced after a fixed time interval (e.g., 12 months), prompting re-verification. The status change triggers an on-chain event, ensuring dependent platforms update in real time.
- (f) **Platform Validation Logic:** Investment platforms (both centralised and DeFi-based) may query a validation API or directly integrate a validation smart contract. The system returns compliance status, permitted jurisdictions, and ESG filters (if applicable), allowing access control based on current credential state. These calls are read-only and privacy-preserving.

- (g) **ESG Integration:** If enabled, investors may request ESG tags or credentials from an approved attestor (e.g., ESG rating agency, sustainability auditor). These are encoded in the token metadata and made available to ESG-aligned fund managers during onboarding or portfolio allocation. Examples include climate alignment (e.g., Paris Agreement-compliant), sector exclusions (e.g., no fossil fuels), or values-based investment criteria.
- (h) **Portability and Interoperability:** SOLO Tokens are interoperable across multiple platforms, enabling “verify once, use many times” onboarding. Tokens issued on Platform A (e.g., an Australian [Private Equity] PE fund) may be used on Platform B (e.g., a Singaporean infrastructure fund) if jurisdictional equivalence rules match and validator status is recognised.

Example use Case 1: Australian Wholesale Investor Workflow

In one embodiment, this invention is implemented by an Australian financial services licensee (AFSL holder) offering investment products to wholesale investors. A wholesale investor domiciled in Australia initiates onboarding by submitting credentials to a validation service.

The validator—a third-party KYC/AML provider registered with AUSTRAC—verifies the investor’s identity, accreditation status under s708 of the Corporations Act, and compliance with AML/CTF obligations. The validator produces a cryptographic attestation, which is submitted to the Credential Issuance Engine.

The Credential Issuance Engine:

- Confirms attestation authenticity using the validator’s public key;
- Cross-references jurisdictional equivalence mappings to verify that the investor satisfies onboarding requirements in Australia and additional permitted jurisdictions (e.g., Singapore, Hong Kong, United States);
- Generates a SOLO Token as a non-transferable ERC-721-compliant asset with embedded metadata including:
 - Unique investor identifier (hashed),
 - Status and expiry timestamp,
 - Jurisdictional compliance matrix,
 - Cryptographic hash of off-chain verification data.

The token is minted to the investor's non-custodial wallet. When the investor accesses a third-party investment platform via a dApp or smart contract, the platform queries the SOLO Token via a validation API. The API returns:

- Confirmation of token authenticity and currency;
- A list of permitted investment jurisdictions;
- Any expiry constraints.

Access is granted or denied automatically by the smart contract based on the token state. The investor's SOLO Token is renewable upon periodic revalidation.

Example use Case 2: Singaporean Investor Accessing an Australian Platform

In another embodiment, the system supports cross-border verification and onboarding for a Singaporean investor accessing an Australian private equity platform.

The investor, domiciled in Singapore, undergoes verification with a validator licensed under the Monetary Authority of Singapore (MAS). This validator conducts identity verification, AML/CTF compliance, and certifies that the investor meets Singapore's accredited investor criteria.

The validator transmits an attestation to the Credential Issuance Engine. The engine:

- Validates the input against known MAS schema;
- References the jurisdictional mapping engine to verify equivalence with Australia's wholesale investor requirements;
- Issues a SOLO Token with jurisdictional scope ["Singapore", "Australia"] and a reference to the validator's MAS license metadata.

When the investor connects to the Australian investment platform, the platform's smart contract:

- Requests a token scan via the SOLO Token API;
- Receives a positive jurisdictional match and validity flag;
- Grants the investor access to eligible investment products.

Example use Case 3: Token Revocation and Expiry Management

In this embodiment, this invention supports both automatic and manual revocation of compliance tokens based on expiry or risk flags raised by validators or platform rules.

A wholesale investor in Australia has been verified through an authorised validator and issued a SOLO Token with a 12-month expiry. The token includes metadata defining jurisdictional compliance for Australia and Hong Kong.

After six months, the validator detects non-compliance with updated AML obligations. The validator submits a revocation request to the Credential Revocation Engine. The system verifies the request origin, checks the cryptographic signature, and updates the token metadata with a “revoked” flag and a reason code.

A downstream platform running a token validation smart contract calls the SOLO Token API to evaluate access rights. The API detects the “revoked” flag and denies access to the investment product.

Separately, if the token reaches its expiry without renewal, the system automatically flags the token as invalid on its next use attempt. Smart contract logic ensures expired tokens cannot be used to access regulated services.

Example use Case 4: Platform Interoperability and Portability

In this embodiment, this invention supports decentralised token portability between onboarding platforms.

An investor is initially verified and onboarded by Platform A, an ESG-aligned private equity platform based in Australia. A SOLO Token is minted with verification metadata that includes Platform A’s validator signature, jurisdictional tags, and ESG filter conformance.

The investor subsequently accesses Platform B, an infrastructure investment platform registered in Singapore. Platform B does not replicate onboarding, but instead calls the SOLO Token API using smart contract logic.

The API returns a confirmation that:

- The token is still valid,
- The issuing validator meets Singapore's licensing equivalence requirements,
- The investor's profile satisfies Platform B's ESG criteria based on SOLO Token metadata.

Platform B then authorises the investor to view and engage with eligible deals.

CLAIMS

1. A computer-implemented system for controlling disclosure of compliance information associated with a blockchain-based compliance credential, the system comprising:
 - (a) a compliance token associated with an entity wallet;
 - (b) encrypted compliance metadata linked to the compliance token;
 - (c) a permissioning module configured to allow the entity to grant, revoke, or limit access to portions of the compliance metadata; and
 - (d) a verification interface configured to provide authorised third parties with access to permitted metadata fields based on permissions granted by the entity.
2. The system of claim 1 wherein the permissioning module enables field-level disclosure of individual metadata components.
3. The system of claim 1 wherein permissions include time-limited access rights.
4. The system of claim 1 wherein permission grants and revocations are recorded on a blockchain.
5. The system of claim 1 wherein authorised third parties include investment platforms performing compliance verification.
6. The system of claim 1 wherein the verification interface supports zero-knowledge proof mechanisms that enable authorised third parties to confirm entity compliance status without accessing the underlying compliance metadata.
7. A computer-implemented method for controlling disclosure of compliance information associated with a blockchain-based compliance credential, the method comprising:
 - (a) associating a compliance token with an entity wallet;

- (b) linking encrypted compliance metadata to the compliance token;
 - (c) allowing the entity to grant, revoke, or limit access to portions of the compliance metadata via a permissioning module; and
 - (d) providing authorised third parties with access to permitted metadata fields based on permissions granted by the entity.
8. A non-transitory computer-readable medium storing instructions that, when executed by one or more processors, cause the one or more processors to perform the method of claim 7.

THE DRAWINGS

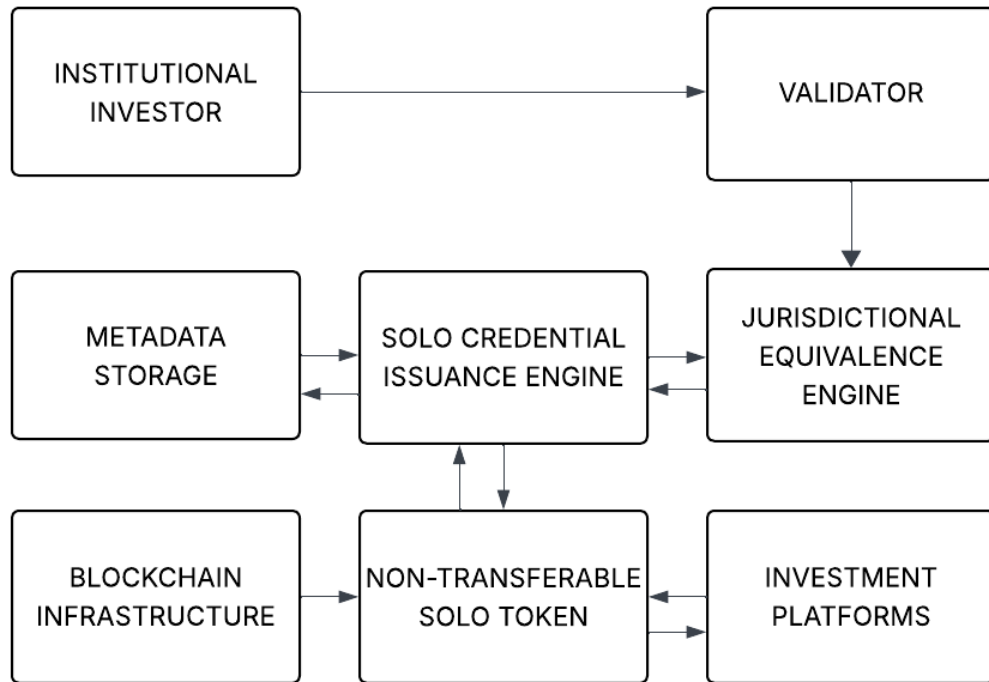


FIG 1

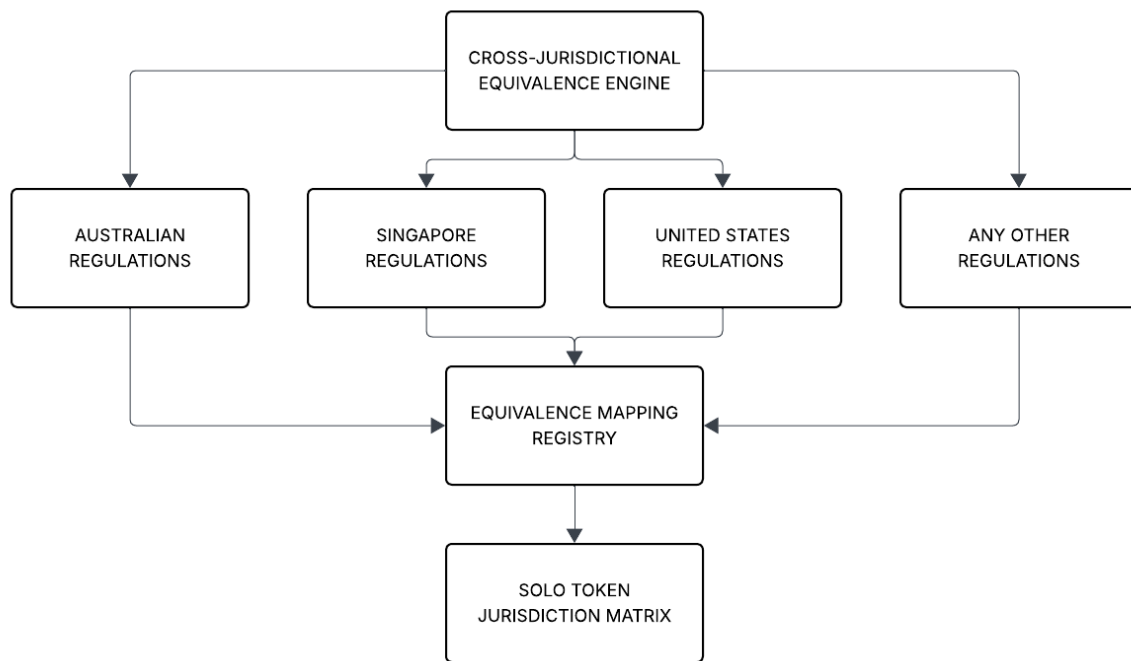


FIG 2

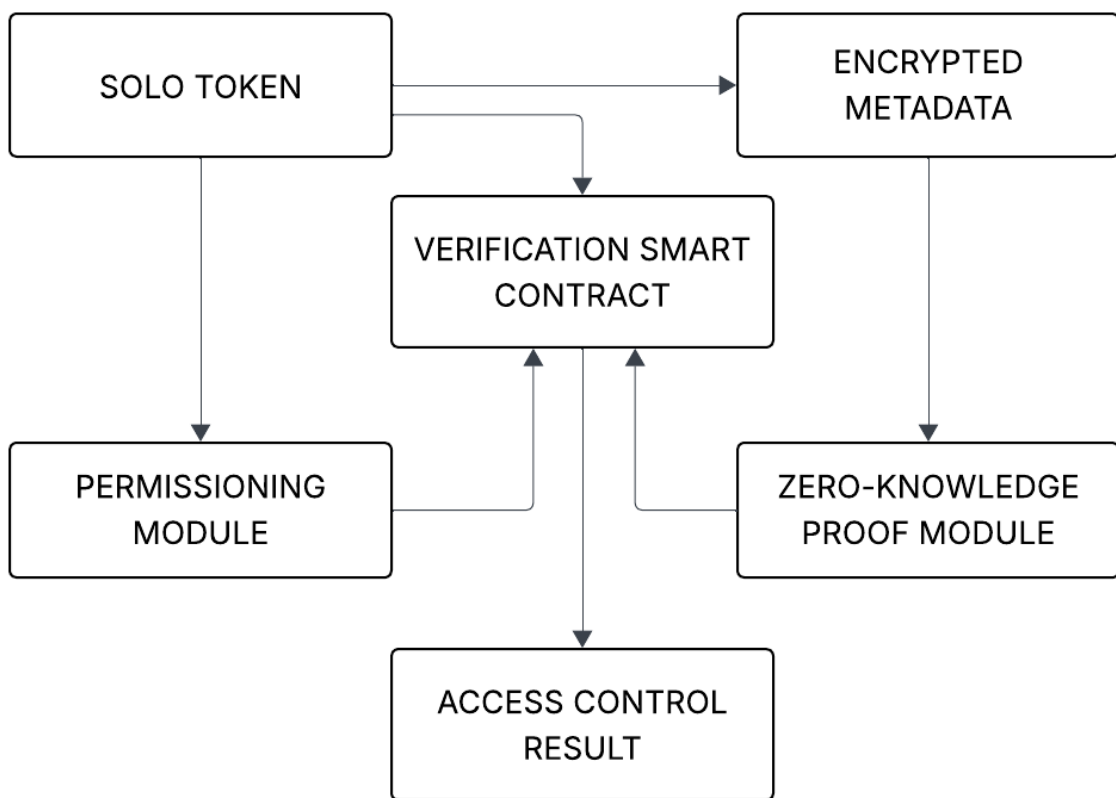


FIG 3

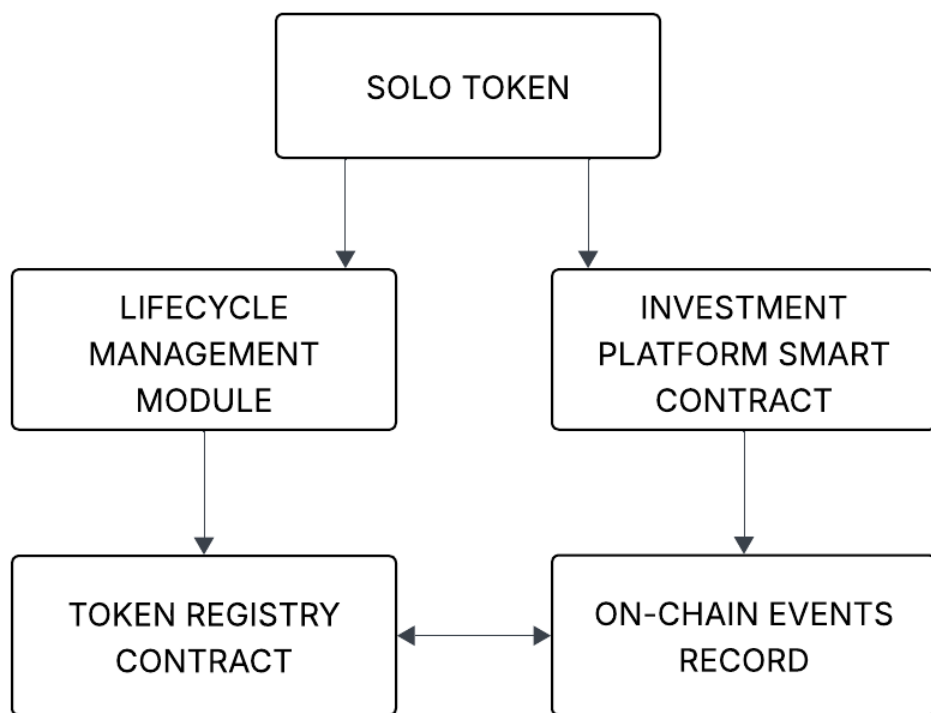


FIG 4

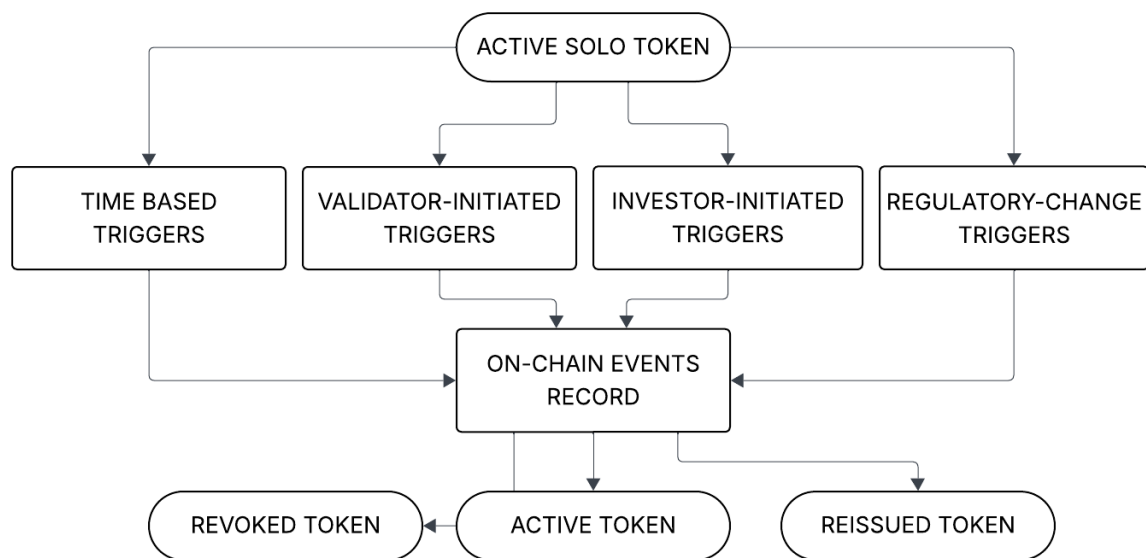


FIG 5

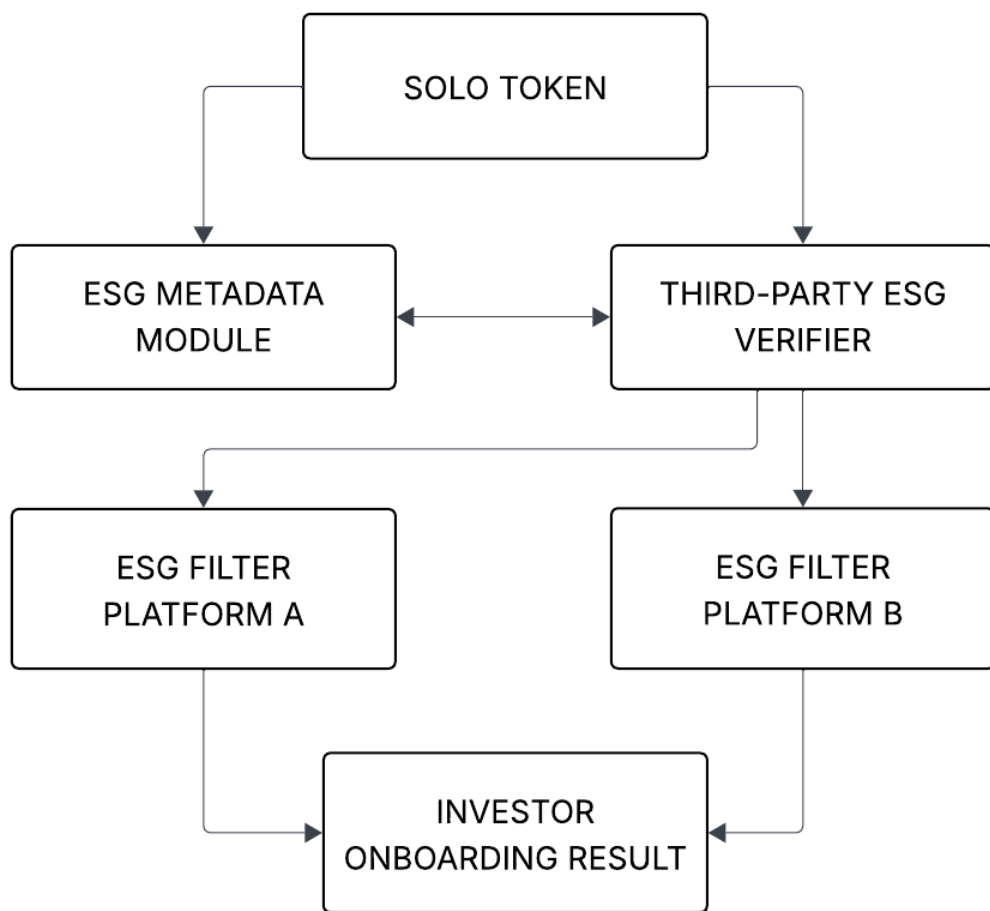


FIG 6