



GBBC
Global Blockchain
Business Council

DIGITAL IDENTITY AND PRIVACY REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 6.0

DIGITAL IDENTITY AND PRIVACY: SETTING THE
FOUNDATION FOR RESPONSIBLE WEB3



GBBCGSMI 6.0

ACKNOWLEDGEMENTS

Diana Oreto (Barrero Zalles)
Head of GSMI & Research, GBBC

ShihYun Chia - CO-CHAIR
CEO, VerifyVASP

Karen Ottoni - CO-CHAIR
Sr. Director of Ecosystem & Strategic Initiatives,
LF Decentralized Trust

Thank you to our working group participants and
review committee for your inputs.

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland



PURPOSE

The objective of this paper is to discuss the role of digital identity in fostering the responsible growth of Web3 without compromising on data privacy. As decentralized applications, tokenized assets, and blockchain-based solutions scale without jurisdictional boundaries, the need for trusted identity frameworks becomes critical. Responsible growth in Web3 encompasses regulatory compliance, risk minimization, scalability, and user autonomy. Rather than increasing surveillance or centralized control, Web3 solutions are meant to enable secure interactions, reduce fraud, and support regulatory compliance in a way that aligns with the values and benefits that blockchain technology is built on. Digital identity, especially when designed with decentralized and privacy-preserving architectures, can provide a verifiable assurance about users, devices, and organizations, while minimizing the amount of personal and sensitive information revealed.

We emphasize that privacy is meant to safeguard user-centered control over what data users wish to reveal about themselves. This goes beyond minimizing the disclosure of personal and sensitive information, as users can also choose to reveal additional information as it may be beneficial to them. Web3 points to a future where individuals can have the opportunity to both protect themselves against unwanted disclosure of personal data and also project data about themselves to their advantage (e.g., building a personal digital brand). Decentralization, on which Web3 ecosystems operate, is a tool to accomplish this dual goal.

This paper covers the foundations of identity, the importance of privacy, and how identity and privacy are both essential for Web3 ecosystem scalability. Next, we offer a landscape of basic privacy-preserving tools used to support the Web3 economy, protocols built on those tools, and both industry examples and broader initiatives that can utilize those tools and protocols to further promote widespread adoption of Web3. This assessment highlights the challenges and opportunities of privacy-preserving identity tools, ultimately focusing on the importance of common standards and best practices.

1) FOUNDATIONS OF IDENTITY & PRIVACY FOR WEB3

1.1) WHAT IS IDENTITY AND WHAT IS ITS FUNCTION?

Identity encompasses a collection of attributes, attestations, and credentials that together prove something about an individual or entity. Specifically, identity is the conceptual underpinning, while attributes are the properties, credentials are signed statements to support these, and identifiers are tools to reference identities. This is far more than a name or a passport number. These attributes may include age, legal status, financial background, risk ratings, or other characteristics that enable one's participation in a wide range of services and approve one to carry out transactions.

WHAT IS DECENTRALIZED IDENTITY (DID)?

Decentralized identity, which is closely related to self-sovereign identity (SSI), is a digital identity model that gives individuals and organizations control over their own credentials and personal data, without relying on a single central authority (like a government, platform, or company) to manage or store that identity. Decentralized identity is built on a technical architecture in where identifiers and verifiable credentials are not controlled by a single centralized authority. Decentralized technologies, namely blockchains and distributed ledgers, can anchor those identifiers and verification methods

Not all decentralized identities, however, are SSI-based. Decentralized identity, often aligned with self-sovereign identity (SSI) principles, is a digital identity model that can give individuals and organizations control over their own credentials and personal data through cryptographic mechanisms, without requiring a single central authority.

- Decentralized identity is a technical specification (i.e., a W3C technical standard for self-generated, cryptographically controlled identifiers.
- Self-sovereign identity is a “philosophical/governance” model emphasizing user control, portability, and minimalism.:

WHAT IS PERSONALLY IDENTIFIABLE INFORMATION (PIII)?

PII often refers to any data that can be used to identify, contact, or trace an individual. While PII is often associated with obvious identifiers (e.g., an individual's name, address, email, passport number, or biometric data), PII can constitute anything attributable to an individual (e.g., date of birth, IP address, wallet address), even indirectly attributable, as long as the data can be reasonably be linked back to a specific individual. For technical precision and building solutions, is important, to adhere to harmonized standards and definitions – namely those provided in the privacy framework under ISO/IEC 29100 – as well as making a distinction between PII, quasi-identifiers, and inference-derived identity elements. PII can be categorized into three tiers:

1. direct identifiers (e.g., name, SSN, passport number)
2. quasi-identifiers (e.g., age, postal code, occupation) that can identify an individual when combined with other data
3. inference-derived identity elements derived through data mining or correlation analysis.

For technical precision and building solutions, is important, to adhere to harmonized standards and definitions, namely those provided in the privacy framework under ISO/IEC 29100, as well as making a distinction between PII, quasi-identifiers, and inference-derived identity elements.



1.1.1) IDEAL SOURCE OF IDENTITY DATA

The golden source for identity data, both for individuals and organizations, would be an authoritative foundation that underpins trusted identity systems where available, noting that certain jurisdictions may lack high-assurance national identity systems or deliberately avoid centralized registries. This trusted foundation is a primary reference point that allows other platforms, verifiers, and digital services to rely on identity knowing that it is accurate and high-quality. A 'golden source' for identity data is a trusted, authoritative foundation that stakeholders in a particular context agree serves as the highest-assurance reference point.

1. For government-issued credentials, this aligns with national identity systems.
2. For organizational affiliation, GLEIF (for legal entities) or professional bodies (for certifications) serve as golden sources.
3. In decentralized contexts, multiple golden sources with different assurance levels may coexist.

→ *For individuals*, this trusted origin of identity data would point to government-backed digital identities (e.g., national identity systems, digital passports, driver's licenses, and other government-issued credentials). Governments have the legal authority to verify an individual's citizenship, residency, age, and other core identity attributes, from which identities can be digitized through various schemes (e.g., eID in the EU, mobile driver's licenses) and continue to serve as authoritative identity anchors.

→ *For legal entities*, the Global Legal Entity Identifier Foundation (GLEIF) has taken the role of overseeing a global system of standardized and globally recognized Legal Entity Identifiers (LEIs), which can be issued to a wide array of legal entities (e.g., companies, funds, financial institutions, etc.). While LEI coverage is still not fully complete globally and may not yet extend to all legal entity forms, and vLEI has yet to expand, GLEIF's verified, regulated system with strict validation procedures is meant to make LEIs a trusted reference point that serves as a golden source for organizational identity data.

1.1.2) WHAT IS PRIVACY?

Privacy safeguards individuals' and entities' ability to prove specific claims about their own identities (e.g., age, role, organizational affiliation) without revealing unnecessary or excessive information. For example, entering a bar requires only proof of being over 21, not disclosure of one's exact birth date and age. Modern digital attestations support this principle by allowing individuals to share only the minimum data needed to access a certain service or perform a transaction.

Proper handling of Personally Identifiable Information (PII) is essential to prevent data leakage. The most effective privacy frameworks pair user control with selective audit and disclosure mechanisms. This way, privacy may be interpreted to a certain extent as "anonymity with accountability": safeguarding personal data over digital and blockchain environments while ensuring that data owners' rights, such as those granted under GDPR (e.g., the ability to update, delete, or control data sharing), are respected. These rights place obligations on data controllers and support a broader framework for responsible data stewardship.

One important distinction in the context of privacy is anonymity vs. pseudonymity:

Anonymity

Full anonymity can obscure identities to the point that neither party in a transaction knows who the other party is.

Pseudonymity

Under pseudonymity, PII is concealed but can be accessed by authorized parties through established processes when necessary (e.g., government authorities investigating illicit activity).

DIDs and VCs enable pseudonymous yet verifiable interactions, where users interact with Web3 protocols through a wallet address (a pseudonym), attaching verifiable proofs when needed (e.g., proof of not being on sanctions lists, residence of a specific jurisdiction, eligibility requirements for a tokenized asset offering). Moreover, as zero-knowledge proofs (ZKPs) become integrated into verifiable credentials, it is essential to understand their implications for privacy, verification, and regulatory compliance.



Privacy is not a synonym for anonymity; privacy is selective and contextual disclosure. Anonymity comes inherently with unlinkability. These distinctions are foundational. While privacy still assumes data can be disclosed; anonymity refers to the full obfuscation of data. From the standpoint of normative policy more than a technical conclusion, anonymity offers an approach that is incompatible with the needs of a mature financial system due to the opportunity for bad actors to take part in the system and create harm. However, there do exist regulated contexts requiring anonymity (e.g., protected disclosures, health access logs).

With privacy at the core, PII is considered highly sensitive because misuse or unauthorized exposure can lead to harms (e.g., identity theft, fraud, surveillance, discrimination). Protecting PII requires a combination of legal, technical, and design safeguards.

Privacy Laws

Data privacy laws and regulatory frameworks globally (e.g., GDPR, CCPA) establish clear parameters for how personal data should be collected, stored, and shared, in addition to placing obligations on organizations to protect the rights of individuals who own and control their data. The growing realm of privacy laws and national data protection frameworks impose strict rules on how PII is collected, stored, shared, and processed.

Technical and design safeguards

Selective disclosure mechanisms can be enabled in traditional ecosystems, but today's overall reliance on centralized identity mechanisms may limit their use.



1.2) HOW DOES IDENTITY FUNCTION IN WEB3?

While traditional systems rely on platform-owned digital identity systems, Web3 shifts the control over identity to the owner, generally the individual, through decentralized and cryptographic mechanisms. Web3 presents a new model where users can manage their own identifiers and credentials, decide what data to share, and interact across applications without needing a single, persistent login provider. Therefore, Web3 identity in the future may no longer rely on centralized providers like governments (or even centralized technology players) to store and validate identity information in the same way as traditional systems. Today, existing market and KYC/AML practices, custodial flows, recovery mechanisms, and off-chain verification still depend heavily on centralized identity proofing and regulated entities.

Two central tools on which this identity system operates are decentralized identifiers and verifiable credentials:

Decentralized Identifier (DID)

A DID is a self-generated, cryptographic identifier owned by the user, which does not need to be issued by a centralized authority.

Verifiable Credential (VC)

A VC is a digitally signed attestation (e.g., proof of membership, accreditation, age, employment, residency, or organizational status) that the user stores in a wallet and presents only when needed. Using cryptographic proofs and decentralized public key registries anchored on blockchains or distributed ledgers, applications and smart contracts can verify these credentials without retrieving the underlying personal data or contacting the issuer.

DIDs and VCs enable pseudonymous yet verifiable interactions, where users interact with Web3 protocols through a wallet address (a pseudonym), attaching verifiable proofs when needed (e.g., proof of not being on sanctions lists, residence of a specific jurisdiction, eligibility requirements for a tokenized asset offering). DIDs and VCs facilitate selective disclosure and enhance privacy by allowing users to disclose the minimum information required. Yet correlation exposure and metadata leakage can still compromise pseudonymity. Hence linkability risks raise the need for anti-correlation techniques (e.g., VCs, DIDs, and ZKPs paired with unlinkability guarantees).

Web3 also enables a decentralized identity model that supports portability and interoperability. Once a user has obtained a set of credentials, they can be used across different blockchains, applications, and ecosystems, just like a physical identity card can be used in multiple contexts. In this way, Web3 identity also preserves user sovereignty, where credentials remain with the user, not locked inside a platform, and no central entity can revoke or monitor all activity.

Ultimately, the shift from platform-owned identity to user-centric identity reduces data collection risks, eliminating centralized honeypots and creating a scalable foundation for trustworthy Web3 ecosystems. When implemented responsibly, identity in Web3 can become an underlying pillar supporting digital ecosystems and markets with greater safety, compliance, inclusion, and more resilient digital economies, all without sacrificing privacy protections or user control.

1.2.1) PRIVACY & PROTECTING PII IN WEB3 ECOSYSTEMS

Privacy is a critical factor enabling trusted and scalable Web3 ecosystems, particularly as largescale companies like financial institutions explore how to responsibly adopt emerging technologies. Banks, asset managers, and regulated entities evaluating the use of blockchain and decentralized systems must ensure that customer information, transaction data, and compliance-related attributes are handled securely and in alignment with legal and regulatory requirements. For instance, while biometrics can strengthen assurance, they also carry significant risks - most notably, that biometric traits cannot be changed if compromised. This underscores the importance of careful system design, especially in Web3 and decentralized systems, where sensitive information should never be stored on-chain. The need for strong privacy protections, combined with selective disclosure, auditability, and user control, drives growing interest in privacy-preserving decentralized technologies capable of supporting both innovation and trust at scale.

Protecting personally identifiable information (PII) in Web3 ecosystems, as in traditional ecosystems, also requires a combination of legal, technical, and design safeguards.

Laws: Web3 is still subject to data privacy laws and regulatory frameworks mandating how data should be collected, stored, and shared. Yet the global and decentralized nature of Web3 ecosystems may raise questions on what specific rules users may be subject to, and enforcement of those rules may also be met with a series of challenges.

Technology Solutions: Privacy-preserving digital identity tools allow individuals to control their own data and selectively disclose only what is necessary to access a service or carry out a transaction. These tools help verify information without exposing underlying data.

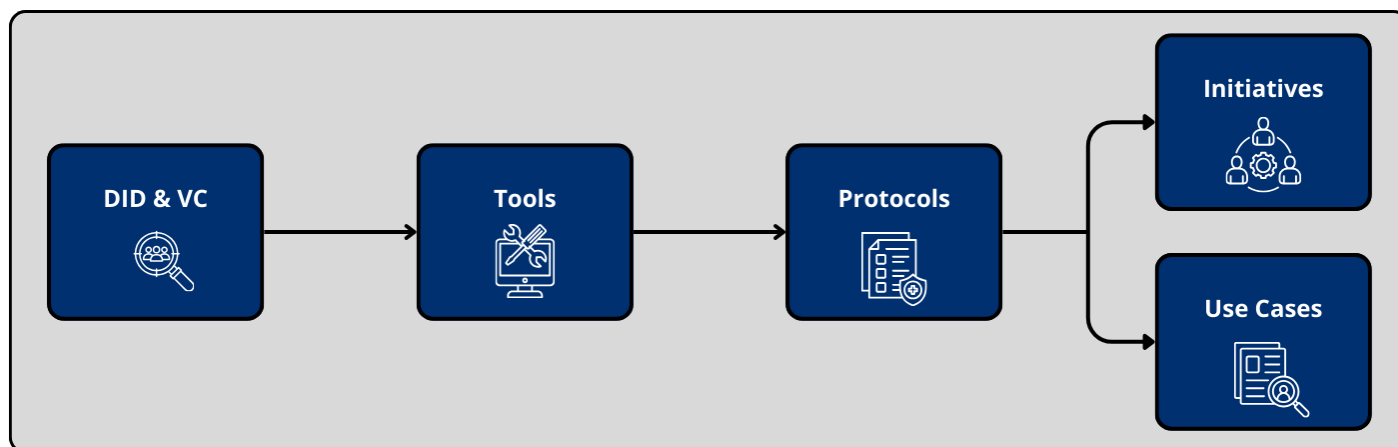
Consent-Based Practices: Best practices support a consent-based model for data sharing. These include:

- Never publishing PII in a public domain, while avoiding any collection and storage of PII on a blockchain, even in encrypted form. Once information is written on-chain, depending on how the blockchain is structured, it can become extremely difficult, if not impossible, to modify or remove it.
- Blockchain systems should rely on on-chain attestations, often structured as binary yes/no confirmations (e.g., verifying accredited investor status), in addition to information about the trusted issuer generating the attestation.

These principles align closely with Self-Sovereign Identity (SSI) principles, which hold that data should be disclosed only by its rightful owner and handled privately, securely, and with full user control over when and how it exits the system. By following these practices and respecting legal obligations, decentralized identity frameworks can protect PII while enabling trusted, privacy-preserving digital interactions.

2) LANDSCAPE OF PRIVACY PRESERVING TOOLS

At the core of the Web3 identity model, Decentralized Identifiers (DID) & Verifiable Credentials (VCs) are modular basic tools that allow users to control their digital identity and selectively disclose personal information through. Building on these tools, below is a landscape of privacy-preserving technologies using on blockchain technology, advancing privacy solutions for the Web3 ecosystem. These are granular solutions that can be combined across privacy-preserving protocols, which in turn form the basis of broader global initiatives and industry use cases focused on privacy.



Moreover, many of these basic tools and protocols, particularly with open-source models, have the potential to become foundational digital public goods (DPGs) and digital public infrastructures (DPIs).

Digital Public Goods (DPGs)

Open-source software, standards, or datasets that are freely reusable and meet privacy, transparency, and ethical-use criteria.

Digital Public Infrastructure (DPIs)

Large-scale national or regional digital systems that enable essential public and private services (identity, payments, data exchange).

DPGs support digital identity systems without vendor lock-in, with transparent code, interoperability, and strong privacy protections – noting that they DPGs alone do not guarantee openness but only reduce vendor lock-in if governance, maintenance, and certification frameworks are also open.

DPIs enable universal access to essential services (e.g., healthcare, finance, social benefits) by providing a secure, interoperable identity layer. DPGs are essentially the building blocks for largescale implementations offering open-source components, and DPIs are made of those building blocks to offer government-scale systems for widespread adoption.

DPI then can provide trusted and authoritative identity sources, which can be integrated into Web3 applications for KYC, compliance, and credentialing across all areas of economic activity, spanning public and private sectors.

DPGs and DPIs together facilitate transparency, trust, interoperability, and long-term sustainability. For instance, open-source frameworks allow governments and organizations to inspect the code, verify security mechanisms, and adapt systems to specific or local needs without vendor lock-ins. This is crucial for largescale adoption of privacy-preserving and interoperable digital identity solutions, which in turn advances interoperability and global inclusion for underrepresented communities.

The landscape of privacy-preserving tools below identifies their benefits, limitations and risks that that can prevent these solutions from achieving their intended goals, and mitigating controls, ultimately highlighting examples.

2.1) LANDSCAPE OF PRIVACY-PRESERVING IDENTITY TOOLS, PROTOCOLS, AND TECHNIQUES

Below is a landscape of privacy-preserving identity tools, protocols, and techniques that highlights their benefits, limitations and risks that that can prevent these solutions from achieving their intended goals, and mitigating controls.

- 1. Tools:** Intended as primitive mechanisms or components (software or hardware) that protocols and techniques are built from. These tools can be used alone or in different combinations to build sets of protocols and techniques for adoption in different contexts and objectives.
- 2. Protocols:** Intended as specified interaction schemes between entities (e.g., issuer–holder–verifier, client–server, parties in MPC, etc.) that use tools to provide security and privacy properties
- 3. Techniques:** Intended as design patterns or ways of combining tools and protocols to achieve specific privacy properties (e.g., unlinkability, minimal disclosure, anonymity sets, etc.).

The categorization of cryptographic and security components into tools, protocols, and techniques is not absolute but rather context-dependent and hierarchically determined. This is because of the layered abstraction model that characterizes modern cryptographic systems architecture, where a component’s classification depends on the level of abstraction being examined and the role it plays within a larger system.

The key principle underlying this flexibility is the concept of vertical composition—the use of lower-level abstractions as building blocks for higher-level abstractions. In this paradigm, a component classified as a “protocol” at one architectural level can function as a “tool” at a higher level of abstraction. Similarly, established techniques can become formalized as protocols when they are standardized and deployed at scale.

TABLE 1: TOOLS

Tool	Description & Function	Benefits for Digital Identity	Limitations & Risks	Suggested Mitigating Controls	Real-World Examples
Symmetric Encryption	Cryptographic technique to make data unreadable without a key, with the purpose to protect data confidentiality so it can be read only by authorized parties. Data can be decrypted back into original form. Encrypts data with a single, shared secret key (e.g., AES).	- Secure storage and transmission of identity data - Encrypted databases - Allowing end-to-end encrypted messaging between authorized parties (e.g., Financial Institutions, governments) - Data confidentiality at rest and in transit	- Key management and distribution; insider threats - PII data sharing constraints - No selective disclosure or computation over encrypted data	- Need to define applicable use cases (e.g., securing sensitive data of certain kinds), as some use cases are not a good fit (e.g., password storage, data integrity checks) - Use Hardware Security Models/ TEEs for key storage; KMS rotation.	<i>HTTPS</i>: Used in browser address bars, indicating that connection between browser and website is encrypted, protecting sensitive information like login credentials and payment details Encrypted biometric data stores (e.g., Aadhaar, India) <i>Virtual Private Networks (VPNs)</i>: encrypt data traveling between one's device and a remote server, making one's online activity private and secure, especially when using public Wi-Fi
Public-Key Encryption	Asymmetric encryption using public/private key pairs (e.g., RSA, ECC).	Secure communication, authentication, message origin.	Computational cost; vulnerable to quantum attacks (RSA/ECC).	Use strong key policies, quantum-safe algorithms.	PKI, SSL/TLS in eIDAS (EU eID).
Fully Homomorphic Encryption (FHE)	Type of encryption that allows computations to be performed directly on encrypted data without needing to decrypt it Enables computation on encrypted data without decryption.	- Processing biometric or credential data privately. - Allowing anyone to verify encrypted computations without seeing the underlying data - Verifying identity attributes (age, residency, accreditation) on encrypted data without decrypting sensitive information - Comparing encrypted identity records (e.g., passport number or national ID) across institutions to detect duplicates or fraud without exposing raw data - Running AML/CFT or sanctions list screening on encrypted identity data	- High computational overhead, complex implementation. - Currently limited by computation cost and speed - No production ready technology - Mostly at proof-of-concept stage, with few production grade solutions that are not yet at ready to scale, especially for enterprise use - There are still unknown unknowns regarding risks and limitations given this is a young technology	- Use for limited fields, hybrid with MPC/TEE. - Need for more testing and proof-of-concepts - Need for more pilots with tech providers - Engagement with enterprise including financial institutions - Need for feedback from actual and potential users	<i>Zama.ai</i> – FHE infrastructure for private computation on the blockchain Privacy-preserving authentication research models.

Tool	Description & Function	Benefits for Digital Identity	Limitations & Risks	Suggested Mitigating Controls	Real-World Examples
Hash Functions	Selected Definition: ""The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data."" - National Institute of Standards and Technology (NIST) One-way functions mapping data to fixed size output (e.g., SHA-2) Hashing is a cryptographic technique comprising of a one-way function that converts data into a fixed-size output. The purpose is to verify integrity or uniqueness, not necessarily confidentiality	- Not reversible or verifiable - One can't perform computations on hashed data - Susceptible to collisions or brute-force attacks if not implemented properly - Hashing is still in its early days of use, being very efficient and working perfectly for certain use cases, while not working for others - Data integrity, biometric template protection	- Need to define applicable use cases (e.g., solutions that require quick data lookup or integrity verification, digital signatures, password storage), as some use cases are not a good fit (e.g., where original data needs to be retrieved, encrypting sensitive data, reversible processes) - Implement hashing wisely, with secure passwords (e.g., using "salt and pepper" techniques), secure algorithms, and staying updated on latest developments - Weak hash choice enables collisions/ reversibility	- Use modern hash functions, salt inputs - Apply salting and peppering for password hashing - Implement rate limiting against brute-force attacks	<i>Secure Hash Algorithm (SHA)</i> - cryptographic hashing family, commonly used in various security protocols and applications <i>Argon2</i> - Secure hashing algorithm designed for password hashing <i>CRC32</i> - Non-cryptographic hash function commonly used for error detection, such as checking data integrity within a data stream Password storage (hashed/salted); biometric matching
Digital Signature Schemes	Cryptographically verifies sender identity & message integrity	- Selected Definition: "The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data." - National Institute of Standards and Technology (NIST) - One-way functions mapping data to fixed size output (e.g., SHA-2) - Hashing is a cryptographic technique comprising of a one-way function that converts data into a fixed-size output. The purpose is to verify integrity or uniqueness, not necessarily+B8	Key compromise enables forgery; algorithm aging	Implement key lifecycle controls, algorithm updates	Document signing (UN, EU diplomas); eIDAS-legal eSignatures
Commitment Schemes	Digital signature allowing any member of a group to sign a message, revealing only the message and the group, without disclosing the identity of the specific signer.	Enabling anonymous communication	Early stage solution with limited adoption	Education and engagement with key stakeholders	<i>Blockchain Transactions</i> - Ring signatures can combine several users' public keys to prove a transaction came from someone within that group, without revealing the specific sender

Tool	Description & Function	Benefits for Digital Identity	Limitations & Risks	Suggested Mitigating Controls	Real-World Examples
Zero-Knowledge Proofs (ZKP)	Selected Definition: “A cryptographic scheme where a prover is able to convince a verifier that a statement is true, without providing any more information than that single bit (that is, that the statement is true rather than false)” - National Institute of Standards and Technology (NIST) ZKPs enable one party to prove knowledge of information, without revealing the actual data Proves possession/ quality of data without revealing the data itself	• Relevant for validation and authentication, providing the minimum data needed to access a service, carry out a transaction, or obtain any given benefit • Verifying identity attributes (e.g., age, nationality, accreditation, sanction check) without exposing personal data • These attributes can be used by other applications during onboarding processes • Enabling compliant DeFi where attested users can only interact with other attested users and applications • Enhancing AML/KYC systems • Selective disclosure, anonymous/age proofs	• Generating ZKPs still requires serious computations and is time consuming, which slows down adoption and limits scalability • There is no regulatory framework for using and trusting ZK-proofs • ZKPs can't replace AML/KYC systems today • Usability, computational burden; weak math opens attacks	• Tech solutions are progressive, with greater efficiencies being improved • Developing guidance on legislative changes and updates • Developing guidance on legislative changes and updates • Engaging regulators is key • Use audited, standardized libraries	<i>Zero-Knowledge Succinct Non-interactive Argument of Knowledge (zk-SNARKs) & Zero-Knowledge Scalable Transparent Argument of Knowledge (zk-STARKs)</i> – Cryptographic techniques used for scalable, verifiable privacy <i>Zcash</i> – A privacy-focused cryptocurrency that uses zk-SNARKs to enable shielded transactions <i>Polygon zero-knowledge Ethereum Virtual Machine (zkEVM)</i> – A zero-knowledge Ethereum Virtual Machine supporting private smart contracts <i>Aztec Network</i> - Privacy layer for Ethereum using ZK rollups to enable confidential transactions <i>Zero-Knowledge Rollups (ZK Rollups)</i> - Layer 2 scaling solution that moves majority of computation and state storage off-chain, using cryptographic proofs to ensure integrity of off-chain transactions. This greatly increases transaction speed, while reducing costs and maintaining security of the underlying Layer 1 mainnet Age verification (zk-SNARKs), privacy pools, UNJSPF
Ring Signature Schemes	Digital signature allowing any member of a group to sign a message, revealing only the message and the group, without disclosing the identity of the specific signer. Provides signer ambiguity among group (anyone in group could have signed).	• Enabling anonymous communication • Transaction unlinkability and anonymity	• Early stage solution with limited adoption • Quantum risks, provable linkability flaws if handled incorrectly	• Education and engagement with key stakeholders • Update with post-quantum designs, review size	<i>Blockchain Transactions</i> - Ring signatures can combine several users' public keys to prove a transaction came from someone within that group, without revealing the specific sender Monero, CryptoNote blockchains, private e-voting
Attribute-Based Encryption (ABE)	Grants decryption rights based on attributes, not identities.	Granular access policies in identity data systems.	Complexity in key distribution and revocation.	Key management standards, attribute audits.	Medical record systems in privacy-focused hospitals.
Multi-Party Computation (MPC)	Cryptographic technique that enables collaborative processing of data without revealing it. Multiple parties can jointly compute a function on their private inputs without revealing those inputs to each other Multiple parties compute together on secret inputs, without revealing them	• Risk modeling • Key management, where MPC allows generating, storing, and using cryptographic keys across multiple servers without having a complete key exist on any single server • Custody, creating wallets where the private key is split into shares across multiple devices, allowing secure signing of transactions without any single device holding the complete key	• Limited mainstream adoption despite robust production implementations (Fireblocks, ZenGo, institutional wallets); requires technical expertise for setup and coordinated multi-party protocols” • High bandwidth, communication rounds, error-prone implementations	• Need for more testing and proof-of-concepts • Need for more pilots with tech providers • Engagement with enterprise including financial institutions • Need for feedback from actual and potential users • Formal verification, TEEs for hybrid use	<i>Partisia Blockchain</i> – Combines blockchain and MPC for privacy-preserving applications. Fireblocks; ZenGo; BitGo Bank KYC, EU digital identity pilots, UN biometric verification

Tool	Description & Function	Benefits for Digital Identity	Limitations & Risks	Suggested Mitigating Controls	Real-World Examples
Trusted Execution Environment (TEE) ¹²	Secure enclave within hardware that isolates code execution and data from the rest of the system, adding protections by securely processing sensitive computations. This is especially useful when sensitive data is kept in individuals' devices and under their control. Enclaved CPU area to process sensitive data in isolation from host OS	- Performing identity verification and compliance screening within a secure enclave, where raw identity data is never exposed outside - Matching biometric data (fingerprint, facial scan) in a TEE to authenticate user - Generating and signing identity credentials inside a TEE - Running logic on sensitive identity data within the TEE and returning only the boolean result, hash, zk-proof, etc. - Device-level hardware root of trust, secure matching	- Trust assumptions in hosting hardware vendors, which may not be as trustworthy as expected - Potential vulnerabilities in side-channel attacks - Hardware bugs (e.g. Spectre, Foreshadow), limited memory, vendor lock-in	- Due diligence/requirements on how to select vendors and ensure their trustworthiness - Robust defense strategy for side-channel attacks, including software and hardware countermeasures - Code attestation, patching, TEEs + SW proofs	TEE for mobile devices can secure biometric data for digital wallets (e.g., Apple Pay), and Digital Rights Management (DRM) content TEE for cloud computing can protect sensitive workloads and data from cloud providers and unauthorized processes TEE for IoT devices can ensure secure processing and storage of data from devices like home security systems TEE for financial services can ensure secure online banking transactions, digital signature verification, and fraud prevention Intel SGX used for biometric match; Apple Secure Enclave
Hardware Security Module (HSM)	Physical appliance to generate, manage, and protect cryptographic keys.	Hardware-level key storage and cryptography.	Expensive, risk of physical attack, supply chain attacks.	Tamper-evidence, geo-dispersed HSM backup.	Root CAs, national eID infrastructure (Estonia's SK HSM).
Differential Privacy Libraries	Mechanisms to add carefully-calibrated noise to statistics and queries to protect individuals.	Analytics/reporting on identity data	Utility/privacy tradeoff, parameter misconfiguration, lack of auditability	DP budget accounting, algorithm openness	US Census data, COVID mobility studies, Apple, Google
Pseudonymization Engines	Replaces real identities with pseudonyms, unlinking data from individuals.	Reduces risk of identity exposure in analytics.	Possible re-identification via auxiliary data.	Regular rotation, k-anonymity checks.	Healthcare research, GDPR compliance reports.
Tokenization Engines	Substitute tokens for sensitive values in transaction streams and storage.	Protects data in transit, simplifies compliance.	Token mapping breach can reveal identities, system dependency	Strong token/key isolation, audit logs	Payment cards (PCI DSS), EU payment identity networks
Biometric Template Protection	Transforms and protects stored biometric templates (e.g., cancelable biometrics, encrypted matching)	Mitigates biometric database theft risk	False accept/reject rates, template irreversibility not guaranteed	Fuzziness calibration, template rotation	UNJSPF facial template protection, passport eGates

TABLE 2: PROTOCOLS

Protocol	Description & Function	Benefits for Digital Identity	Limitations & Risks	Suggested Mitigating Controls	Real-World Examples
Verifiable Credential (VC) Protocols	Issue, present, and verify cryptographic claims with proof mechanisms, using open data models (W3C).	Enables trust-minimized, privacy-preserving credentials.	Relies on secure holder devices, standard adoption slow.	Open standards, credential expiration, pairing w/ TEEs.	<i>W3C VC in Sovrin/Indy, EU EBSI pilots, UNJSPF PoL.</i>
Decentralized Identifier (DID) Protocols	Resolves public key material of peer or org via decentralized registry (not PII by design).	User-controlled, revocable, no central registry.	DID methods need interoperability, registry security.	Peer-reviewed DID methods, registry governance.	<i>Hyperledger Indy, EU EBSI, W3C DID.</i>
Anonymous Credential Protocols (Idemix)	Issue and prove claims with cryptographically unlinkable presentations & multi-show proofs.	User anonymity, selective disclosure.	Large credential size, key revocation, verification cost.	Storage hardening, key rotation, selective proof.	<i>Idemix, AnonCreds (Hyperledger), eIDAS pilots.</i>
SSI Protocols	Schemes for self-sovereign identity: issuer-holder-verifier models using VCs/ DIDs	Holder autonomy; no central storage of digital ID	Usability/key recovery, presentation policy ambiguity	Key backups, policy registries, human factors research	<i>ToIP, Sovrin, Kiva pilot, EU EBSI, UNJSPF/UN pilots</i>
Remote Attestation Protocols (TEE/ TPM)	TEE generates cryptographic proof of executing specific code in secure hardware environment.	Trust in device, not host OS; detects node tampering.	TEE bugs/breaches; attestation log management.	Combined ZKP/TEE proofs, attestation transparency.	Intel SGX attestation (Microsoft Azure Confidential Ledger)
Privacy Tokens	Tokens designed to protect user anonymity by obscuring transaction details (e.g., sender, receiver, amount) and making them untraceable Privacy tokens may serve legitimate purposes including financial privacy for businesses (salary payments, commercial transactions), protection from surveillance in authoritarian regimes, prevention of front-running in DeFi, and confidential commercial transactions. Users obtain anonymous tokens from providers and later redeem them anonymously (rate limits without tracking)	- Ensuring privacy on an entity or individual's activities on chain - It is possible to disclose certain data or trigger market movement because of a certain activity or transaction (similar to financial services privacy motives) - Anonymous authentication/ access control	- Use by bad actors for illicit activities like money laundering and terrorist financing, leading to a bad reputation in the industry - Some jurisdictions are banning privacy tokens fully, leading to limited uses - Replay attacks, token theft, cross-origin leakage	- Unlike pseudonymous cryptocurrencies such as Bitcoin, which show transaction details publicly while hiding the user's real-world identity, privacy tokens use advanced cryptography to fully mask this information - Short-lived tokens, origin binding	<i>Monero (XMR)</i> - Uses ring signatures, stealth addresses, and RingCT to obscure sender, receiver, and amount in all transactions by default <i>Zcash (ZEC)</i> - Allows users to choose between transparent or shielded transactions, which use zero-knowledge proofs to hide transaction details <i>Dash (DASH)</i> - Offers optional privacy feature PrivateSend, which mixes transactions from different users. IETF Privacy Pass; Cloudflare

Protocol	Description & Function	Benefits for Digital Identity	Limitations & Risks	Suggested Mitigating Controls	Real-World Examples
Confidential Transaction Protocols (CT)	Hides transaction amount (and optionally sender/receiver) while allowing correct balance verification.	Protects financial privacy; auditability.	Performance hit, trace analysis attacks, compliance.	On-chain auditing, bulletproof range proofs.	Monero, Zcash, Elements Project, Incognito chain
Mixing/Tumbling Protocols (CoinJoin)	Aim to obfuscate transaction trails to make it difficult to trace users and their activities Multi-party protocol to mix funds/transactions to obfuscate original participants.	- Allowing anonymous transactions and activities - Transaction unlinkability	- Regulatory challenges due to misuse for illicit purposes - Production use cases involve largely illicit activities - Centralization risks, blacklists, service bans	- Education, especially the need to articulate legitimate use cases prior to controls - Identifying, standardizing, and implementing controls - Decentralized, open-source implementations	<i>Tornado Cash</i> – Ethereum-based mixer using zero-knowledge proofs to anonymize ETH and ERC-20 tokens <i>Wasabi Wallet</i> – Bitcoin wallet with built-in coinjoin features for privacy <i>Samourai Wallet + Whirlpool</i> – Bitcoin mixing focused on financial privacy Monero, Ethereum Tornado.
Privacy Pools Protocol¹³	Smart contract-based protocols, allowing the creation of an association set of legitimate users with legitimate source of funds without revealing individuals' transaction history. A privacy pool functions as a mixing service using zk proofs for groups of legitimate users, balancing privacy with regulatory compliance. Authorized entities can verify the funds are legitimate by checking against the approved "association set." ZK-based pools allow selective, accountable mixing, including compliance-oriented proofs (association sets).	- Anonymous yet "compliant" transactions - Demonstrating source-of-funds legitimacy in DeFi - Users can deposit and withdraw cryptocurrency privately while proving their funds are legitimate - Privacy with regulatory/Audit compliance	- Regulatory uncertainty - Require user education, onboarding training, and interface improvements for adoption - Complicated proofs, user misconfiguration	- Education for users and regulators - Develop selective disclosure mechanisms for audits (view keys, compliance proofs) - Clearer UI/UX for ease of use - Fail safe approaches and adequate risk warnings - Standards for association proofs, DAO audits	<i>Tornado Cash</i> - uses early privacy pool anonymizing transactions on platforms like Ethereum, requiring users to provide cryptographic proof to withdraw funds <i>Aztec Network</i> - Built privacy-enhancing layers and private execution environments on blockchains <i>Penumbra</i> - Built privacy-enhancing layers and private execution environments on blockchains Latest Ethereum privacy pools, research pilots
Shielded Transfer Protocols (Zcash, etc.)	ZKP protocol for sender/receiver and amounts; enables confidential value transfers.	Transaction recipient privacy at protocol level.	Trusted setup risk (early zk-SNARKs), high gas cost.	Open setup ceremonies, key rotation, circuit updates.	Zcash Sapling, Panther Protocol.
Privacy-Preserving Smart Contract Protocols	Smart contracts with privacy preserving tools embedded Enables contract logic to run privately (using TEE, ZKP, MPC, or hybrids)	- Allowing transactions and logic to remain encrypted or hidden from public view while still being verified - User/computation privacy on public blockchains	- What is encrypted can be decrypted - Cost, complexity, TEE vulnerabilities, ZKP scaling	- On/off ramps - to extent there's a cefi regulated entity where can onboard client under regulatory requirements. Even if they use privacy enabled tokens/tools, they're vetted - Audit contract bytecode, runtime proofing	<i>Secret Network</i> – Uses Trusted Execution Environments (TEEs) to execute smart contracts privately <i>Oasis Network</i> – Supports confidential smart contracts with on-chain/off-chain data separation <i>Phala Network</i> – A privacy-preserving cloud computing platform using TEEs and blockchain <i>Enigma (SCRT)</i> – A privacy protocol for secure computation Oasis, Chainlink Confidential Compute

Protocol	Description & Function	Benefits for Digital Identity	Limitations & Risks	Suggested Mitigating Controls	Real-World Examples
MPC Key Management/ Sig Protocols	MPC or threshold protocols for shared control/creation of keys or signatures.	No single point of compromise for signing/auth.	Key share loss/neglect, communication attack.	Redundant share backup, formal analysis.	Fireblocks, ZenGo, institutional wallets.
"DATA MARKETPLACES Privacy-Preserving Data Market Protocols"	Enable controlled data sharing while preserving user consent and privacy Secure buying/selling/evaluating of data/ML models without revealing originals (MPC/FHE/TEE based)	• Providing easier and faster access to diverse, high-quality data • Confidential computation on personal/biometric data	• Possibility of uncontrolled and unexpected data disclosures and data sharing • Data leakage via outputs/pricing, collusion	• Implementing best practice of keeping data within an individual or organization's system • Safeguarding of data • Data sovereignty • Audited outputs, price fairness mechanisms	<i>Ocean Protocol</i> – Allows data providers to share data while maintaining control and privacy <i>Numeraire (Numerai)</i> – Crowdsourced hedge fund where encrypted data science models are shared privately Sterling Demo, Partisia Data Markets
Federated Learning with MPC/DP	Multi-organization model training without sharing raw data, often with DP noise for aggregate privacy.	Global scaling, cross-org fraud/AML detection.	Model inversion, DP utility tradeoff, poisoning.	Minimum batch size, outlier filtering, DP monitoring.	COVID-19 risk models, banking consortia risk engines.



TABLE 3: TECHNIQUES

Technique	Description & Function	Benefits for Digital Identity	Limitations & Risks	Suggested Mitigating Controls	Real-World Examples
Selective Disclosure	Revealing only requested attributes/claims from a credential (e.g., "over 18").	Data minimization, personal privacy.	Side-channel inference, protocol divergence.	Standardized proof templates, minimized sets.	W3C VC presentations, UNJSPF PoL age proof.
Unlinkability	Ensuring repeated interaction or credential showings can't be linked to a user.	Prevents tracking, aggregated profiling.	Re-linking via metadata, device/browser fingerprinting.	Fresh identifiers, session rotation, network privacy.	Monero transaction outputs, rotating DID in VC apps.
Anonymity Set Enlargement (Mixing/Pools)	Using protocol structures to increase the privacy set (e.g., CoinJoin, privacy pools).	Hides "needle" in a larger haystack.	Small set size risks traceability, external correlation attacks.	Large default set sizes, encourage pooling.	Wasabi/Tornado wallets, Ethereum compliance pools.
Association Set Compliance	Proving one's activity is outside a "bad actor" set while being privacy protected.	Regulatory compliance with strong privacy.	Complexity in proving, user opt-out/in errors.	DAO/standards oversight, interface guidance.	Privacy Pools for DeFi, ZK-KYC logs (Polygon).
Compute-on-Encrypted-Data	Using FHE/SHE/MPC/TEE to process identity data privately (matching, scoring).	Outsourcing and cross-jurisdiction verification.	Costly/failure offloading, side channel in execution logs.	Use for critical ops, combine with audit logs.	UNJSPF secure on-chain PoL, secure international KYC.
Pseudonymization	Replacing identifiers with revocable tokens/pseudonyms for internal processing.	Reduces re-identification risk, enables research.	Re-linking via auxiliary info, token leaks.	Token/class rotation, isolated mapping stores.	GDPR compliance in EU, medical research databases.
Tokenization	Substituting opaque tokens for sensitive values in public/partner systems.	Data breach protection, easier compliance.	Mapping service compromise, aggregated linkage.	Segregation, monitoring, periodic remapping.	Payment processing in ID-linked finance.
Differential Privacy	Introducing noise to summary statistics to hide individual's effect on result.	National/social research, audit logs, analytics.	Over-noising (loss of utility), under-noising (privacy breach).	Budget transparency, audit DP config.	US Census, identity analytics reports.
Data Minimization by Design	Limiting collected data to what is strictly necessary for service.	Compliance, risk minimization by default.	Over-collection due to poor requirement definition.	Regular privacy audits, engineering review.	UNJSPF PoL: only proof-of-life
Biometric Template Protection Techniques	Making biometric templates revocable, encrypted, and non-linkable between uses.	Prevents biometrics from being lifelong "password".	Reduced matching accuracy, template collision attacks.	Regular revocation, template version audits.	UNJSPF facial template encryption, ePassports.

2.2) INDUSTRY USE CASES

Privacy preserving solutions envisioned for Web3 can be fundamental for several industries as Web3 is becoming a fundamental part of the digital transformation journey. Privacy preservation goes hand in hand with responsible growth. These solutions are reducing frictions and costs for processes ranging from onboarding, AMK/KYC, risk modeling (e.g., scenarios for investment, market, credit, operational), accounting and reporting, and transaction operations (e.g., payments, clearing & settlement, treasury management), and various services (e.g., investments, asset allocations).

Below we illustrate ways that entire industries can benefit from privacy preserving digital identity as they prepare for the advent of Web3. Major sectors we highlight are financial services (both traditional and decentralized finance), healthcare, and government can benefit from privacy preserving digital identity.

Industry Use Case	Benefits of Privacy Preserving Digital Identity
Financial Services (TradFi)	• Facilitating compliance with data protection laws to which financial services companies are bound • Allowing customers to participate in open blockchain ecosystems, facilitating customer acquisition and growth of Web3 marketplaces • Making technology accessible to a wider range of users while protecting customers. • Cutting onboarding costs and facilitating accelerated onboarding onto various platforms, with solutions like shared KYC models, noting that shared KYC models require detailed trust and liability frameworks to ensure interoperability without legal or regulatory constraints. • Removing intermediaries and frictions because trust is based on cryptography, requiring less human verifications that can be costly and time consuming
Financial Services (DeFi)	• Facilitating meeting requirements for TradFi adoption, as solutions can be conceptualized to address issues raised by TradFi • Many privacy tools are already used in DeFi, providing benchmarks, lessons learned, and use cases for scale, especially for TradFi and integrations
Healthcare	• Facilitates safeguarding privacy of patient data, making it accessible agnostic to healthcare provider • Reducing costs and intermediation with shared data models • Enhancing use of AI solutions and predictive models by providing high quality data while safeguarding patient privacy (e.g., better risk screenings, multiple conditions can be analyzed in conjunction to better assess correlations, etc.)
Government	• Enhancing government controls • Enabling government authorities to access digital versions of public services • Providing more functional national digital identity systems (e.g., identity issued on individuals' digital wallets or devices) • Better identity delivery, improving broader access to basic services to benefit users • Facilitating onboarding for public and private institutions • Enabling better derived identity systems, with greater recognition of identity by various providers (e.g., grandfathering identity, linking financial and health identities to national identities) • Open-source models enable robust, scalable, and cost-effective infrastructure for DPIs, government-scale platforms like national digital identity systems, payment rails, and data-exchange layers • Transparent and widely vetted codebases allow building identity systems that citizens trust, especially when sensitive components such as authentication, cryptography, and data-sharing protocols require verifiability



2.3) GLOBAL PRIVACY PRESERVING IDENTITY INITIATIVES

The initiatives below are tangible examples of solutions built on blockchain-based and privacy preserving digital identity solutions, with a wide range of applications:

2.3.1) CHAINLINK CROSS-CHAIN IDENTITY (CCID) FRAMEWORK

As part of Chainlink's broader Automated Compliance Engine (ACE), the CCID framework is designed to bring institutional grade identity and compliance functionality into blockchain ecosystems. CCID provides a standard framework to put identity data on chain and share it cross-chain, acting as a reusable identity model for representing on-chain identities of entities, both individuals and institutions, by anchoring cryptographic proofs of verified credentials while keeping sensitive data (e.g., PII or non-public information) off-chain. CCID provides a container that stores attestations about any entity, which can take the form of proofs of certain things (e.g., KYC and accredited investor status for individuals, beneficial accounts for corporates, proof of funds, AML, etc.). Those attestations can be stored on chain and provided to off chain entities. CCID can also provide identity verification for wallets and identify users across public blockchains. CCID does not store PII but just the cryptographic proof of the attestations.

With the CCID model, once a user or entity completes verification through a trusted issuer (e.g., an ID verification provider, financial institution, or regulatory agent), the resulting attestations (e.g., "this wallet belongs to a KYC-verified individual", "this legal entity holds LEI/vLEI") are represented on-chain. These attestations can be referenced across different blockchain networks and tokenized ecosystems without the need for repeated onboarding. This way, CCID supports multiple trust-models. For example:

Model 1: Asset issuers themselves provide attestations and other market participants trust those issuers.

Model 2: Specialized identity verification platforms issue attestations and are trusted by asset issuers and ecosystems.

Model 3: Governments or official bodies issue primary identity attestations, while financial institutions or IDVs verify and attest further claims.

With CCID enabling identity verification for wallets and digital assets in a privacy-preserving manner, for instance, a wallet can prove to a smart contract or token issuance platform that the holder has passed KYC or meets accreditation criteria without exposing sensitive personal information. This design addresses a critical need for Web3 ecosystems that must balance decentralization, privacy, and regulatory compliance. Moreover, with identity infrastructure and compliance rules that can work across multiple chains and jurisdictions, institutional capital and compliant digital assets can operate on chain with less friction.





2.3.2) GLOBAL LEGAL ENTITY IDENTIFIER FOUNDATION (GLEIF) VLEI

The Verifiable Legal Entity Identifier (vLEI) is the next evolution of the traditional Legal Entity Identifier (LEI), created to meet the needs of a rapidly digitizing global economy. While the LEI was established after the 2008 financial crisis, to provide a unique identifier for organizations participating in financial transactions and improve transparency in the financial sector, accelerating digital transformation brought the need for more robust, verifiable digital identities. The Global Legal Entity Identifier Foundation (GLEIF), founded by the Financial Stability Board in 2014, initiated the shift from LEI to vLEI. This new system enhances the LEI by embedding it into cryptographically verifiable credentials, enabling automated, tamper-resistant, and globally interoperable identity verification.

Unlike the original LEI, which can only identify organizations, the vLEI also extends identity solutions to individuals affiliated with those organizations. It allows verification of not only an entity's identity but also the identity, role, and authority of people acting on its behalf. KERI/AID-based architecture, a decentralized identity management system built on Key Event Receipt Infrastructure (KERI) using Autonomic Identifiers (AIDs) for self-verifiable, portable, and long-lived digital identities, is the basis for vLEI, which relies on key-evolving infrastructures. Because of these expanded capabilities, vLEI supports use cases such as KYC processes, sanctions checks, role verification, and automated onboarding across jurisdictions. GLEIF plays a central role in this ecosystem, establishing the standards, governance structures, and trust frameworks behind vLEI, and serving as the root of trust to ensure global reliability and acceptance.

Moreover, KERI, which backs the vLEI issued by GLEIF, has its technical specifications hosted on Trust Over IP (ToIP) described below. The GLEIF ecosystem governance framework also is directly based on the ToIP metamodel and governance principles. LEI (and vLEI thereby) also have their own ISO standards – ISO 17442.¹ This is an example of connections between seemingly separate players in the ecosystem.

Overall, the vLEI provides a digital-first identity solution designed to strengthen trust, security, and automation across industries. By enabling verifiable credentials for organizations and individuals alike, it brings identity into the digital era and lays the foundation for more seamless, secure digital interactions across borders.

2.3.3) UNITED NATIONS JOINT STAFF PENSION FUND (UNJSPF) DIGITAL CERTIFICATE OF ENTITLEMENT (DCE)

Developed out of a strategic partnership between UNJSPF and United Nations International Computing Centre (UNICC), the DCE² is UNJSPF's revolutionary blockchain-powered digital identity solution. Using blockchain, biometrics (facial recognition to verify beneficiaries), AI, and geo-location technologies, the DCE is a secure and inclusive digital identity solution that has transformed pension verification for over 70,000 pension beneficiaries across 190 countries, modernizing a 70+ year old paper-based verification process. The results have shown a 40% reduction in paper-based processing, 95% decrease in archiving costs, 76.5% decrease in overtime costs, and a user loyalty with a 99.96% retention rate.

As security measures, biometric risk containment, template protection, or anti-replay measures are essential in addition to operating under globally recognized standards – namely ISO/IEC 24745 on “Information security, cybersecurity and privacy protection — Biometric information protection.”³

Given the impact and scale of pension beneficiaries and UNJSPF's global operations, the DCE importantly adheres to best practices that dictate keeping PII (including biometric data) on the user's device, while using blockchain only to anchor proofs and support verification. Understanding the relationship between identity, identifiers, and the potential risks they introduce is essential for building secure, privacy-preserving identity solutions. Accordingly, the DCE solution enhances security, efficiency, and fraud prevention, while aligning with the UN's broader digital transformation agenda. Looking to expand the DCE solution beyond the pension fund, the DCE Consortium Initiative offers a DCE-as-a-Service model to other UN entities and international organizations. This would promote shared governance, cost reductions, and stakeholder cooperation, in alignment with the Global Digital Compact and the Pact for the Future that drive major UN initiatives globally.

2.3.4) BLOCKCHAIN GOVERNANCE INITIATIVE NETWORK (BGIN)

BGIN is a global, multi-stakeholder network dedicated to advancing open and responsible blockchain governance practices worldwide as a neutral governance body. The Accountable Wallet framework is a protocol to balance the need for AML/KYC controls with privacy protections. This framework is meant to bridge the adoption gap for privacy preserving tools, ensuring broad adaptability and extensibility to mitigate AML risks and other risks. It presents an approach to constructing a compliance scoring system for wallet addresses that minimizes single points of failure (SPOF) and eliminates the need for a trusted centralized authority.

The core objective of this system is to leverage verifiable credentials issued by reliable providers and non-membership proofs to propagate compliance scores off-chain, forming a chain of credentials. The framework draws on several privacy-preserving building blocks beyond verifiable credentials: on-chain and off-chain attestations of wallet behavior and asset provenance (e.g., chain certificates, witness data, reputation systems) and privacy-preserving proof mechanisms (e.g., zero-knowledge proofs) allowing wallet holders to prove compliance or legitimacy without exposing unnecessary personal or transactional details. The Accountable Wallet framework also complements privacy pools, ultimately enhancing the balance between on-chain privacy and regulatory compliance.

This framework is intended to create a wallet model that enables users to prove their legitimacy in blockchain ecosystems, not just in terms of identity, but also in terms of historic behavior and asset provenance. In this system, wallets score or demonstrate trustworthiness, and transactions between accountable wallets can take place with reduced counter-party risk.

Three core dimensions of legitimacy, which together form the foundation of an “Accountable Economy” are:

- (1)** ownership legitimacy - who controls the wallet, and whether that controller is subject to sanctions or other disqualifying status
- (2)** transactional history legitimacy - whether the wallet has been involved in illicit or suspect flows
- (3)** asset origin legitimacy - whether the funds or tokens held / received by the wallet can be traced to legitimate sources



2.3.5) SINGAPORE GOVERNMENT DIGITAL IDENTITY SOLUTION

Singapore's SingPass⁴ system is the country's foundational government-backed digital identity solution based on a federated login solution that allows users to access multiple applications with a single set of credentials provided by an external entity. SingPass is designed to let individuals securely authenticate themselves and access both public and private sector services. Today, SingPass primarily enables financial institutions and other organizations to verify a user's identity for login or onboarding and to retrieve "golden-sourced" personal information directly from government records. This allows, for example, the opening of a bank account entirely through a mobile device, with financial institutions downloading the necessary personal data to complete KYC checks. Yet while effective and widely adopted, the current system exposes raw personal data rather than providing hashed, privacy-preserving credentials. SingPass represents Singapore's initial phase in building a trusted national digital identity infrastructure.

In addition to SingPass, Singapore is taking further steps toward a more sophisticated, credential-based digital identity model. The government recently launched a verified credentials sandbox, currently limited to organizational participants, in which entities are issued a hashed, blockchain-anchored credential tied to verifiable background information. This marks Singapore's early move into decentralized and verifiable digital identity. The next evolution of the system is expected to shift from directly sharing personal information to offering APIs that return verification results against authoritative sources, similar to how GLEIF's vLEI framework provides cryptographically verifiable organizational identity. Such an approach would allow organizations to confirm attributes (e.g., eligibility, authorization, signatory rights) without retrieving full personal data.

Ultimately, these initiatives pave way toward the potential of a future decentralized wallet ecosystem. To fully achieve digital trust across all economic activity, future developments need to expand beyond individuals and incorporate legal entities and organizational roles, aligning with global trends toward verifiable credentials and privacy-preserving identity frameworks.



2.3.6) TRUST OVER IP (TOIP)

Trust Over IP (ToIP) provides a comprehensive, layered model for establishing digital trust that aligns closely with the needs of Web3 identity systems. Built on open standards such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) as specified by W3C, ToIP defines a four-layer architecture that separates cryptographic trust from human, legal, and organizational trust. The lower layers establish decentralized roots of trust and secure communication protocols, enabling entities such as wallets, applications, or smart contracts to authenticate each other and exchange data securely. The upper layers provide the governance, policies, and credential-exchange frameworks needed for real-world accountability and interoperability across different platforms, jurisdictions, and ecosystems. Ultimately, the root of trust may be decentralized, hierarchical, or jurisdiction specific. ToIP allows multiple trust models, and we highlight the example below:

Layer 1 (Bottom) Trust Support (Cryptographic Roots): Foundational infrastructure where identifiers and verifiable roots of identity are established, with decentralized key material, DIDs, basic cryptographic operations, and registries or roots of trust.

Layer 2 Trust Spanning (Secure, Peered Communication): Defines protocols and connection mechanisms for transport-agnostic trustworthy communication (e.g., DIDComm as a “Trust Spanning Protocol”), allowing 2 entities to connect securely and verifiably, ensuring authenticity, integrity, and confidentiality.

Layer 3 Trust Tasks (Credential Exchange & Issuance): Protocols to issue, exchange, verify and revoke VCs, allowing issuers, holders, and verifiers to manage claims and credentials in a standardized and interoperable way.

Layer 4 (Top) Application Ecosystems & Governance: Provides the final applications that rely on credentials and identities, handling business, legal and social frameworks, and providing ecosystem governance, compliance, policies, trust frameworks, and liability structures. This layer ensures digital identity implementations remain rooted in real-world accountability and interoperability.

By bridging technical trust with governance-based trust, ToIP enables Web3 ecosystems to support privacy-preserving and interoperable digital identity. This model allows individuals and organizations to control their identifiers, present verifiable claims selectively, and interact across decentralized platforms without revealing unnecessary personal information. For Web3 applications, ranging from DeFi and DAOs to identity-enabled wallets, ToIP offers a scalable blueprint for trusted onboarding, cross-chain identity exchange, and regulatory-ready verification. In doing so, it helps create a consistent trust layer for the decentralized internet, reducing fragmentation and enabling secure, accountable digital interactions ready for global scale.

2.2.7 ZERO-KNOWLEDGE-PROOF (ZKP) AND SELECTIVE DISCLOSURE IN COMPLIANCE CONTEXTS

Zero-knowledge proofs enable proof of claims without revealing the underlying data. While powerful for privacy, ZKP integration with identity credentials raises challenges:

- **Auditability Gap:** Authorities cannot directly verify ZKP inputs, requiring trust in issuer integrity
- **Computational Burden:** Generating and verifying ZKPs remains expensive; scalable implementations are nascent (15% of AML procedures use blockchain as of 2025)
- **False Proof Risk:** A zero-knowledge proof can only verify what the prover knows; it cannot verify accuracy of source data

Effective Web3 identity frameworks must clarify which compliance activities require ZKP privacy, and which require full auditability.

2.4) HURDLES TO PRIVACY SOLUTIONS' SCALABILITY

Finding the right balance between privacy and security controls is essential for Web3, especially as the space approaches institutional scale. There is a tradeoff where obfuscation of sensitive data at a certain level may not make it available for compliance purposes. While privacy is ideologically good, when it reaches the bounds of anonymity it brings risks, where bad actors can conduct illicit practices within a platform.

AML/KYC is a particular area of longstanding challenges, especially when it comes to financial transactions, which form the backbone for business models across industries. In traditional financial systems, AML often lacks sufficient privacy safeguards, as acknowledged by FATF guidance⁵ and known AML high false positive statistics.⁶ Moreover, while financial institutions are legally required to perform KYC, yet they may not trust one another's KYC processes, even when operating under the same regulations. This lack of mutual trust complicates information sharing and carries over into blockchain environments, where interoperability depends on consistent and reliable attestations. Moreover, incentive structures are set up in such a way that financial institutions prefer funds to be "sticky" and remain within a given institution rather than moving quickly across platforms in a streamlined way. Additionally, if one institution flags an individual for AML risk, whether it is done accurately or not, it creates a friction can propagate across the ecosystem, creating systemic barriers. High rates of false positives in AML processes intensify this issue. On the blockchain, if incorrect risk attributes are written onto the ledger, they can introduce new and persistent transaction obstacles. In such cases, the cost of dealing with erroneous or overly rigid data may outweigh the intended efficiency and transparency benefits of blockchain technology.

The regulatory focus of Web3 initially started with AML concerns, due to the anonymous nature of Web3 participation. The stance of many AML approaches with respect to Web3 has taken into account these regulatory concerns. Tumblers and mixers, for instance, have been widely disapproved by regulators for obfuscating user data. This has been a red flag at the level of FATF forums. A series of recent court actions have targeted the Tornado Cash mixing service, with initial OFAC sanctions⁷ that were later removed⁸, while the privacy coin Monero has faced regulatory scrutiny⁹ and delistings from exchanges.

2.5) WEB3 GROWTH OPPORTUNITIES THROUGH PRIVACY SOLUTIONS

As institutions must balance compliance with privacy, decentralized identity solutions offer a path to meeting both goals simultaneously in ways that don't contradict each other. Solutions to strengthen privacy in Web3 increasingly focus on enabling verification without compromising user data and control. There is also a strong commercial demand for privacy-preserving identity systems, as they enable safer user onboarding, reduce friction in financial interactions, and support scalable, interoperable Web3 ecosystems. Effective approaches involve using nonfungible, unique identities paired with systems that keep sensitive information on an individual's device, ensuring data never leaves the user's control.

Regarding financial transactions and onboarding users for any platform, especially in the financial sector, KYC processes function most effectively when supported by decentralized data storage mechanisms, allowing verified credentials to be referenced without exposing underlying personal information. In this model, identity becomes the necessary layer driving financial transactions, where other factors like creditworthiness, risk scoring, asset class restrictions, and liquidity access play parallel roles.

For instance, if a bank or other trusted financial institution has verified a user, that verification can authorize that user to transact across different platforms. This approach also aligns with existing regulatory frameworks, where AML rules, customer due diligence (CDD) requirements, and broader legislative obligations intersect with data protection laws like GDPR.

In the context of the digital economy, identity functions as a foundation for trust and compliance. For instance, a financial institution, or any platform that onboards users, may rely on identity-related information to determine whether a user is a sanctioned entity, resides in a high-risk jurisdiction, or is acting as an individual or a legal entity. In this sense, identity is not a single data point but a structured set of claims that allow individuals and organizations to interact securely and meet both regulatory and operational requirements.

3) STANDARDS

Commonly agreed upon standards, ideally open-source standards, are fundamental for privacy-preserving digital identity solutions in the Web3 economy to ensure interoperability across borders and sectors, eventually taking the role of DPIs and DPGs. This way, identity solutions built in one sector or jurisdiction can integrate seamlessly with services offered in other sectors and jurisdictions, contributing to the truly global nature of the Web3 economy. Common standards promote openness, accountability, resilience, and innovation: essential qualities for scalable and digital identity infrastructure to underpin a Web3 ecosystem that respects the rights of data owners.

Standards for digital identity to preserve privacy and respect rights of data owners are essential for the maturation, safety, and global adoption of Web3 because they create a shared foundation for how identity, security, interoperability, and trust are implemented across decentralized systems. Web3 ecosystems are inherently multi-party and cross-border, involving wallets, dApps, exchanges, custodians, regulators, infrastructure providers, enterprises, and end users. Without common standards, each participant may build on proprietary or incompatible approaches, resulting in fragmentation, security gaps, and siloed identity systems that undermine the very promise of decentralization. Standards help ensure that identities can be verified across platforms, that credentials can be trusted universally, and that interactions, whether signing a transaction, proving authorization, or onboarding users, are consistent, secure, and legally meaningful. For instance, trust models based on cryptographic security, legal recognition, governance-backed mechanisms, or multi-party verifiability lead to different architecture choices. Standards are necessary to determine harmonized approaches for Web3.

Digital-identity standards are critical because Web3 replaces centralized account models with decentralized identity and key-based authentication. This increases both opportunity and risk. Moreover, by grounding Web3 identity in globally recognized standards, Web3 ecosystems gain interoperability with the existing digital economy infrastructure and satisfy regulatory expectations. Standards also provide clarity for developers, reduce duplication of effort, and create stable interfaces for innovation. They help protect users from fraud and privacy violations, define acceptable levels of security, and ensure that organizations interacting through Web3 systems can trust each other's credentials and data. While many standards are in early stages with respect to Web3 relevance, and some are still in production, they can be key to address risks.

The reference table below is therefore valuable for all stakeholders in the Web3 space, providing single consolidated view of the diverse standards landscape that Web3 builders must navigate. Ecosystem participants often come from different industries with different compliance requirements, so having a unified resource helps ensure consistent understanding of which standards matter and why. For developers, it highlights which technical specifications to build against. For enterprises and institutions, it clarifies the regulatory and assurance frameworks needed for adoption. For policymakers, it illuminates the global best practices that can guide national or sectoral digital-asset frameworks. As Web3 evolves, such reference points enable coordinated progress, reduce fragmentation, and accelerate the development of trustworthy, interoperable, and future-proof digital-identity infrastructures.

Standard / Framework	Region	Description & Relevance for Web3
AICPA SOC 2 (Type I & II) – Trust Services Criteria	Primarily US, used globally	- Assurance reporting framework evaluating controls over security, availability, processing integrity, confidentiality, and privacy at service organizations.¹⁴ Web3 relevance: common expectation for exchanges, custodians, ID providers, and infrastructure platforms to demonstrate operational security and privacy controls to institutions.
eIDAS & eIDAS 2.0 (EU Digital Identity Wallet Regulation)	EU	- EU regulation establishing a framework for electronic identification, authentication, and trust services; eIDAS 2.0 adds the European Digital Identity Wallet, requiring member states to offer at least one wallet for citizens and businesses.¹⁵ Web3 relevance: sets regulatory expectations for digital identity, signing, and credentials in the EU; Web3 wallets and DID/VC ecosystems will increasingly need to interoperate with or align to EU Digital Identity Wallets.
eIDAS 2.0 — Architecture Reference Framework (ARF) for EU Digital Identity Wallet Interoperability	EU	- Defines the architecture and interoperability rules for the EU Digital Identity Wallet, ensuring cross-border functionality, which enable verifiable credentials, digital attestations, signatures, and authentication processes to be exchanged uniformly across member states. Web3 relevance: alignment with decentralized identity principles, with a government-backed, verifiable credential framework, supporting regulated applications built on identity (e.g., DeFi, RWA tokenization).
ETSI Trust Services Standards (e.g., ETSI EN 319 411, 319 412, 319 421)	Europe, but globally influential	- Requirements for trust service providers (TSPs) (e.g., identity verification, issuance of qualified certificates, electronic signatures, seals, timestamps, and secure authentication mechanisms), providing a foundation for legally recognized eID, eSignatures, and trust services under eIDAS (Electronic Identification, Authentication, and Trust Services). Web3 relevance: technical and regulatory blueprint for legally binding signature and authentication services that can anchor decentralized systems to legal identity and accountability, as a compliance layer.
FIDO2 (FIDO Alliance)	Global	- Set of standards (WebAuthn + CTAP) enabling phishing-resistant, public-key based authentication using passkeys.¹⁶ Web3 relevance: provides strong MFA and hardware-bound keys that can be combined with Web3 wallets or used for account-abstraction schemes and custodial access.
ICAO Doc 9303 – Machine-Readable Travel Documents (MRTD/ ePassport)	Global	- Specifies formats, security features, and use of biometrics for machine-readable pass-ports and travel documents, including ePassports with embedded chips.¹⁷ Web3 relevance: authoritative source for government-issued identity credentials; can be a high-assurance input into Web3 identity proofing or VC issuance (e.g., passport-derived credentials).
IETF OAuth 2.0 (RFC 6749)	Global	- Authorization framework that lets third-party apps obtain delegated, limited access to resources via tokens.¹⁸ Web3 relevance: used by many Web3 frontends, custody platforms and APIs for access delegation; can be bridged with DIDs/VCs for hybrid Web2+Web3 access control.
ISO 17442 - Legal Entity Identifier (LEI) & vLEI	Global	20-character, globally unique identifier used to unambiguously identify legal entities participating in financial transactions. The LEI system helps improve transparency, risk management, and regulatory reporting by ensuring each firm has a standard, interoperable identifier recognized worldwide.¹⁹ Web3 relevance: Trusted anchor for legal entities interacting with decentralized finance, tokenization platforms, and institutional-level smart contracts, enabling clear entity identification, compliance and auditability. LEI alongside decentralized identity tools facilitate institutional adoption and cross-jurisdiction trust.
ISO 18013-5 — Mobile Driver's License (mDL)	Global	- Technical and security framework for mobile driver's licenses, enabling cryptographically secure and selectively disclosable digital identities on mobile devices. Web3 relevance: Globally recognized model for selective disclosure and holder-controlled identity, aligned with the way VCs are utilized in decentralized identity ecosystems, with high-assurance, government-issued credentials.
ISO/TR 23244 – Blockchain and DLT: Privacy & PII Protection Considerations	Global	- Technical report giving an overview of privacy and PII protection considerations in blockchain and DLT systems.²⁰ Web3 relevance: addresses how to handle PII in DLT designs (e.g., off-chain storage, pseudonymity, linkability), key for privacy-by-design in Web3 identity and credential systems.
ISO/TR 24760-1 – Identity Management - concepts and terminology	Global	- Establishes core concepts and terminology for identity management, providing a foundation for other standards. This includes a core set of concepts and relationships (e.g., what constitutes “identity,” “identifier,” “attribute,” and how identity management systems should handle identity information across contexts). This standard is applicable to any information system that processes identity information.²¹ Web3 relevance: In context where identity came more fluid, decentralized, and privacy-focused, this standard provides a shared language for identity across traditional and decentralized systems. This standard also supports privacy-aware and rights-respecting identity systems.
ISO/IEC 27701 – Privacy Information Management System (PIMS)	Global	- Extension to ISO/IEC 27001/27002 that specifies requirements and guidance for a Privacy Information Management System, helping controllers and processors manage PII privacy risks.²² Web3 relevance: foundational privacy and governance layer for dApps, custodians, and infrastructure providers that process off-chain PII linked to on-chain identifiers or wallets.
ISO/IEC 29100 – Privacy Framework	Global	- High level privacy framework defining actors, PII processing, and privacy principles; forms a foundation for more specific privacy and identity standards.²³ Web3 relevance: supports privacy-by-design analysis in token, credential, and DAO designs where PII may be linked (directly or indirectly) to on-chain activity.

Standard / Framework	Region	Description & Relevance for Web3
ITU-T X.1254 – Entity Authentication Assurance Framework	Global	- Specifies authentication assurance levels (AALs) and a framework for managing them, including mapping to other schemes.²⁴ Web3 relevance: provides a conceptual model for “assurance levels” of Web3 identities and credentials, useful when mapping DID/VC-based authentication to regulated assurance frameworks.
NIST Privacy Framework (PF 1.1)	US (NIST; globally used)	- Voluntary framework to help organizations identify, assess, and manage privacy risk in products and services.²⁵ Web3 relevance: useful for designing privacy-preserving dApps and identity services, especially where on-chain data can create long-lived privacy risk.
NIST SP 800-63-3 – Digital Identity Guidelines	US (NIST, but widely referenced)	- Suite of documents (63-3, 63A, 63B, 63C) specifying identity proofing, authentication, and federation assurance levels and technical requirements.²⁶ Web3 relevance: provides a well-understood assurance model for mapping wallet/DID-based identities and credential issuers to traditional assurance levels (IAL, AAL, FAL).
PCI DSS 4.0 – Payment Card Industry Data Security Standard	Global	- Industry standard defining security requirements for environments where payment card data is stored, processed, or transmitted.²⁷ Web3 relevance: applies to card-based on/off-ramps, custodians, and payment processors that bridge Web3 tokens with card rails. Strong overlap with wallet KYC, tokenization of card data, and exchange infrastructure security.
OpenID Connect (OIDC)	Global (OpenID Foundation)	- Authentication layer built on top of OAuth 2.0; defines ID tokens, user info, discovery, and client registration for interoperable federated login.²⁸ Web3 relevance: critical for “sign-in with X” flows that complement wallet-based auth; can issue VCs or bridge Web2 identities into Web3 ecosystems.
OpenID for Verifiable Presentation 1.0	Global	- Mechanism to request and present Verifiable Credentials (VCs), allowing wallets or identity agents to securely deliver cryptographic proofs using a familiar, interoperable web- and mobile-based interaction model.²⁹ Web3 relevance: The standard supports selective disclosure, privacy preservation, and secure verification without requiring issuers to be online at the time of presentation. Provides interoperability bridge between decentralized identity systems and existing web authentication frameworks, enabling Web3 wallets, dApps, and smart-contract-based services to accept verifiable identity proofs in a standardized, privacy-preserving way.
OpenID for Verifiable Credential Issuance 1.0	Global	- Defines how digital wallets or identity agents can obtain Verifiable Credentials from issuers using secure, interoperable, OAuth-based protocols, while supporting multiple credential formats, dynamic credential requests, and strong user consent flows.³⁰ Web3 relevance: Enables Web3 wallets and decentralized applications to receive trusted, portable credentials (e.g., KYC attestations, domain ownership proofs, or role-based permissions) from authoritative issuers, bridging traditional identity systems and decentralized ecosystems.
OpenID High Assurance Interoperability Profile 1.0	Global	- Requirements for existing specifications to enable interoperability among issuers, wallets, and verifiers of credentials where a high level of security and privacy is required. Provides an interoperability profile that can be used by implementations in various contexts (e.g., industry, regulatory environment). Aimed at high assurance use-cases, and can also be used for lower assurance use-cases.³¹ Web3 relevance: Enables Web3 platforms to incorporate high-assurance, verifiable real-world identities (e.g., regulated financial identities, enterprise credentials, or government-backed digital identities) into decentralized applications, allowing for stronger compliance, reduced fraud, and secure participation without centralizing user data.
Trust Over IP (ToIP) Stack	Global	- Four-layer architecture for decentralized digital trust combining cryptographic infrastructure with governance and legal layers to define “Internet-scale digital trust.”³² Web3 relevance: provides an architectural blueprint for layering DIDs, VCs, governance frameworks, and trust registries over Web3 networks, aligning them with enterprise and regulatory expectations.
W3C Decentralized Identifiers (DID) Core	Global	- Defines the syntax, data model, and operations for Decentralized Identifiers (DIDs), URIs that can be resolved to DID Documents controlled by cryptographic keys rather than a central registry.³³ Web3 relevance: core identity primitive in Web3, used to represent wallets, organizations, smart contracts, and agents in a chain-agnostic way.
W3C / FIDO – Passkeys & WebAuthn (Levels 2 & 3)	Global	- WebAuthn Level 2 & 3 and FIDO passkeys specify strong, cryptographic, phishing-resistant credentials for web authentication.³⁴ Web3 relevance: essential for securing access to Web3 accounts, signing portals, and identity wallets with high-assurance device-bound keys instead of passwords.
W3C Verifiable Credentials Data Model 2.0	Global	- Data model for expressing verifiable credentials—digitally signed statements about a subject (e.g., KYC status, accreditation, membership). It defines how credentials can be made tamper-evident and privacy-preserving.³⁵ Web3 relevance: de-facto standard for off-chain attestations that can be presented by Web3 identities (wallets/DIDs) to dApps, exchanges, and DeFi protocols.
W3C Web Authentication (WebAuthn) – FIDO2 Web API	Global	- WebAuthn defines a browser API for strong public-key-based authentication with hardware or platform authenticators (passkeys).³⁶ Web3 relevance: passwordless, phishing-resistant login for wallets, exchanges, and Web3 gateways; can secure key-management UX and access to custodial/non-custodial accounts.

While there is yet no unilateral consensus in the identity community to a single architecture, there is overall an increasing global adoption of wallet standards, alongside efforts toward interoperability. As standards adoption continues by a wide range of stakeholders, this raises questions on how they can become “relying parties” consuming many freely available, high assurance credentials to meet their business objectives. For those with KYC obligations, the OpenID Foundation (OIDF) reports on KYC may be especially useful to understand how to comply with law using these credentials. Those experiencing deep fake compromises benefit especially from these standards’ adoption trends as acceptance of high assurance credentials are the best possible tool to counter deep fake fraud.

3.1) CASE STUDY: OPEN ID FOUNDATION (OIDF) SPECIFICATIONS

The three standards listed above from OIDF already underpin the verifiable credential and wallet architecture of 38 jurisdictions globally. 22 US states are supporting mobile drivers’ licenses specification (mDL/mdocs) issuance, and 38 countries are issuing and accepting VCs from OIDF, with the California DMV as the first jurisdiction globally state to be live with both OpenID4VP and VCI.

Moreover, these OIDF specifications interoperate with:

- ISO/IEC 18013-7 (Annex D and E)
- W3C DC API for cross device online presentation, which in turn works with OpenID4VP 1.0 and ISO18013-7 (Annex D)
- ISO/IEC 18013-5 for mobile Drivers License (mDL) in person presentation.
- Various complementary specs from ETSI, CSC, FIDO, with additional collaborations to be announced

These standards also underpin the core of interoperability and security for the EU Digital Wallet. The OIDF specifications will be pointed to by the EU implementing acts, and all 27 member states will need to conform to them by end of 2026. They are credential type agnostic. ETSI is under a mandate from European Commission to further profile these OIDF specifications, and there is tripartite work underway on test requirements for further conformance and launches. The UK and Switzerland have also selected the OpenID4VP and OpenID4VCI specifications for their national wallet programs, in addition to 6 Western Balkan states for their jurisdiction wallet programs to ensure interoperability with Europe.

NIST NCCOE Mobile Driving License also cohosted 9 of the 11 OIDF interoperability events in 2025, including the release of their own “NIST bank” and “NIST verifier” to show how mDL / mdoc from a state issuer can be used via OpenID4VP on a browser or in app to open a bank account. That work led to a suite of NIST deliverables and further collaborations between OIDF and NIST, including reports to show how exactly financial institutions (including crypto wallets with CIP/KYC obligations) can comply with the law using these credentials. This work is being deepened to prove it out in the US live in production, as well as other jurisdictions (e.g., EU, Australia, New Zealand, Taiwan, Indonesia and India).

Moreover, major global private corporations are also affirming their plans to deploy these specifications. Many have taken part in the interop events on the record , such as the public hybrid demo of OpenId4VP in Germany.

In the Global South, OIDF channel partners are driving global open standards through country relationships. MOSIP is offering OpenID4VP and VCI modules to their client countries, and OIDF is partnering with the World Bank to highlight how their clients can leverage wallets and VC in a series of webinars and workshops.

Ultimately, with respect to conformance status, the conversation in most of the jurisdictions above is starting to shift from selection of specifications and build to conformance. OIDF has open-source tests available on all three core specifications, which are expected to form the foundations of nearly all wallet conformance programs, especially as they are proven to deliver interoperability and security assurance by default.



3.2) CASE STUDY: BGIN CYBERSECURITY VULNERABILITY & THREAT INFORMATION SHARING FRAMEWORK

A comprehensive framework for sharing cybersecurity information in blockchain ecosystems is essential for enabling secure, coordinated responses across decentralized and semi-decentralized stakeholders. This framework provides requirements and guidance for exchanging threat intelligence, indicators of compromise, vulnerability disclosures and proofs of concept, incident reports, and legal or regulatory notifications such as sanctions or subpoenas.

Given the high volume and cross-border nature of security incidents affecting blockchain networks, a standardized model for cybersecurity information sharing is urgently needed. This framework offers a common structure tailored specifically to blockchain and cryptocurrency environments, facilitating international interoperability and enabling cross-organizational and cross-governmental collaboration to counter increasingly sophisticated adversaries, including nation-state actors. By enabling global yet privacy-preserving information sharing, it helps eliminate weakest links across the ecosystem and supports faster, more coordinated incident response.

The model is built on guiding principles such as trust, reciprocity, timeliness, and data minimization, supported by trust mechanisms like the Traffic Light Protocol (TLP) and pseudonymous attribution to balance transparency and confidentiality. It defines clear stakeholder roles and a lifecycle that progresses from discovery to remediation, disclosure, and post-incident learning. To ensure broader applicability and adoption, the framework aligns with existing standards including ISO and NIST, bridging traditional cybersecurity practices with blockchain-specific realities. Ultimately, the objective is to promote trusted, structured, and verifiable information sharing that enhances system-wide resilience, accountability, and interoperability across the global blockchain ecosystem.

3.3) CASE STUDY: CONTENT AUTHENTICITY INITIATIVE (CAI)

The Content Authenticity Initiative (CAI)¹⁰, founded by Adobe, The New York Times, and Twitter, is an effort to bring transparency and trust to digital media globally through open standards for content provenance and authenticity. In partnership with the Coalition for Content Provenance and Authenticity (C2PA), CAI released Content Credentials, an interoperable framework for creators, publishers, and platforms to attach cryptographically verifiable metadata to images, video, audio, and text. CAI maintains open source tools, SDKs, and a conformance program for organizations to generate and verify provenance information. Metadata records origin, authorship, edit history, and tool usage. CAI ultimately provides a secure and tamper-proof “digital nutrition label” for consumers and systems to better distinguish authentic content from forgeries, deepfakes, or manipulated media.

For Web3, trust, provenance, and identity are fundamental for decentralized applications and digital asset ecosystems. Content Credentials offer a standardized way to provide digital media with a cryptographic proof of source and authorship, which reinforcing key Web3 principles such as verifiable identity, accountability, and traceability. Aligning with decentralized identity models (e.g., VCs and DIDs), CAI enables creators, DAOs, institutions, and platforms to reliably assert attribution without exposing unnecessary personal data.

CAI therefore becomes a tool to address concerns about data provenance, in a digital world where NFTs, generative AI content, tokenized media, and decentralized publishing demand robust verification of origin and integrity. CAI’s tools provide building blocks for a trust architecture compatible with Web3. While it does not certify the factual accuracy of content, it establishes a reliable provenance layer to mitigate fraud, strengthen compliance, and support more transparent information flows across decentralized networks.

3.4) CASE STUDY: STATE ENDORSED DIGITAL IDENTITY (SEDI)

SEDI¹¹ is a framework, rooted in state law (originally passed as SB 260 in Utah), establishing a “rights-first” model for government-endorsed digital identity. In this model, digital identity belongs to the individual, not to a government or corporation. Hence the role of the state is not to create identity, but to endorse a digital identifier that the individual already controls. Under SEDI, individuals generate their own cryptographic identifiers, while the state verifies real-world identity and then issues a signed credential endorsing it. This means the identifier remains under the sole control of the individual, ensuring sovereignty, privacy, and self-determination. SEDI allows selective disclosure, privacy, and decentralized control, making it compatible with self-sovereign identity (SSI) principles.

Ultimately, SEDI offers a blueprint for a digital identity infrastructure that finds a balance between public sector endorsement and trust, with individual privacy and autonomy. By embedding governance principles (e.g., legal protection of rights, transparency, decentralization, and cryptographic assurance), SEDI aims to deliver secure, privacy-preserving, and portable identity. This state-endorsed identity layer, which is built to coexist with decentralized, user-controlled identity architectures, aligns with Web3 ecosystems in a way that can offer legitimacy and self-sovereignty simultaneously.

3.5) BEST PRACTICES AND PRINCIPLES ACROSS STANDARDS

Best Practices & Principles	Description
Transparency	Informing individuals about how their data is used
Consent	Getting permission before collecting or processing data
Purpose Limitation	Using data only for specified, legitimate purposes
Data Minimization	Collecting only the data necessary
Security	Protecting data with appropriate technical and organizational measures
Accountability	Organizations must demonstrate compliance with privacy obligations
User Rights	Allowing users to access, correct, delete, or transfer their data
Self-Sovereign Identity (SSI)	Users own and control their personal data and digital identity
Minimal Disclosure	Systems support selective disclosure and zero-knowledge proofs to reduce data exposure
Consent-driven data sharing	Data sharing is based on explicit user consent and purpose limitation
Decentralization	Reduces reliance on central authorities that could exploit or leak personal data
Interoperability	Enables trust and data exchange without compromising privacy
Governance Frameworks	Define roles, responsibilities, and compliance requirements for data privacy and protection.

4) CONCLUSION

A user-controlled Web3 identity model, enabled through Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), offers a clear path toward secure, privacy-preserving digital interactions that also respect the rights of data owners. These tools allow individuals and organizations to prove what is necessary while minimizing data exposure, supporting trusted, human-centered, and portable identity across blockchain ecosystems. As zero-knowledge proofs become integrated into verifiable credentials, it is essential to understand their implications for privacy, verification, and regulatory compliance.

Responsible growth requires acknowledging regulators' AML concerns, particularly around systems that obscure financial provenance. However, when privacy-preserving identity solutions that are rights-respecting and standards-aligned, they can provide the right balance to meet both privacy and compliance goals. Regulations, governance frameworks, and dedicated resources will be crucial for driving adoption, while privacy must remain a core principle rather than an afterthought. Collaboration across stakeholders (e.g., banks, identity providers, developers, and policymakers) is essential to ensure that new tools meet real institutional requirements. Global references such as the World Bank's ID4D initiative and leading digital-identity frameworks illustrate the importance of interoperability, strong governance, and user-centric design.

Together, these efforts form the foundation of a trustworthy Web3 ecosystem: one that enhances inclusion, reduces fraud, strengthens compliance, and preserves the user's right to control their own identity.

6.1) RECOMMENDATIONS

1. Build on Open Standards for Identity, Privacy, and Interoperability
2. Prioritize User Control, Minimal Disclosure, and Privacy-by-Design
3. Address AML/KYC Requirements Through Cryptographic Verification
4. Use DID + VC as the Foundation for Cross-Platform Trust
5. Encourage Multi-Stakeholder Collaboration and Ecosystem Governance
6. Develop Transparent Trust-Scoring and Attestation Models
7. Invest in Digital Public Goods and Digital Public Infrastructure (DPG + DPI) Development
8. Prepare for Regulatory Integration and Compliance Alignment
9. Ensure Systems Support Both Individuals and Legal Entities



6.2) OPEN QUESTIONS TO ADDRESS

1. **How should Web3 define trust, assurance levels, and credential reliability across jurisdictions, while there is no global consensus?**
2. **What governance model ensures credential issuers are trustworthy, non-centralized, and globally interoperable?**
3. **How can zero-knowledge proofs scale efficiently while remaining verifiable, affordable, and user-friendly?**
 - ZK systems remain computationally heavy and complex. How can decentralized identity frameworks ensure performance at a global scale?
4. **What is the appropriate balance between pseudonymity and regulatory visibility?**
 - If pseudonymity is too strong, regulators may view systems as a risk; if too weak, privacy becomes compromised. How can Web3 implement “anonymity with accountability”?
5. **How can AML-risk propagation be managed without writing irreversible, potentially inaccurate risk attributes on-chain?**
 - How should redress, correction pathways, issuer liability, and the governance of attestation revocation be assessed?
 - Incorrect AML flags can permanently harm users and create systemic frictions. What privacy-preserving redress mechanisms are needed - specifying data structures (e.g., Merkle trees, persistent state registries, smart contract mappings) that introduce irreversibility?
6. **How can decentralized identity avoid fragmentation across chains, countries, and industries?**
 - Multiple identity frameworks already exist. What strategy ensures interoperability across public chains, enterprise blockchains, national ID schemes, and regulatory systems?
7. **How can wallets incorporate trust-scoring without creating “reputation prisons” that limit user mobility?**
 - Web3 needs ways to reward trustworthy behavior without creating systems that permanently stigmatize users.
8. **How should long-term credential validity, revocation, and recovery be managed?**
 - Identity credentials can expire, associations change, and keys get lost. What decentralized solutions support lifecycle management without central fallbacks?
9. **How can identity systems protect biometric data while supporting accessibility and inclusion?**
 - Biometrics can strengthen assurance but introduce irreversible privacy risks. What architectural safeguards ensure they are only used safely and consensually?
10. **Who bears liability when decentralized identity components fail—issuers, verifiers, wallet providers, or protocols?**

ENDNOTES

DIGITAL IDENTITY AND PRIVACY

- 1 <https://committee.iso.org/sites/tc68/home/news/content-left-area/news-and-updates/iso-17442-3-verifiable-leis-vlei.html>
- 2 <https://www.unjspf.org/for-clients/digital-certificate-of-entitlement/>
- 3 <https://www.iso.org/standard/75302.html>
- 4 <https://www.singpass.gov.sg/main/>
- 5 <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>
- 6 <https://finance.yahoo.com/news/hidden-cost-aml-95-false-134601048.html>
- 7 <https://home.treasury.gov/news/press-releases/jy0916>
- 8 <https://home.treasury.gov/news/press-releases/sb0057>
- 9 <https://www.dlnews.com/articles/defi/regulators-turn-on-privacy-coin-monero-after-bitcoin-booms>
- 10 <https://contentauthenticity.org>
- 11 <https://rufftimo.medium.com/sedi-details-for-identity-nerds-e1949af5cc30>
- 12 https://people.csail.mit.edu/mengyuanli/files/asiaccs_sok.pdf
- 13 <https://privacypools.com/>
- 14 <https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2>
- 15 <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>
- 16 <https://fidoalliance.org/specifications/>
- 17 https://www.icao.int/sites/default/files/publications/DocSeries/9303_p1_cons_en.pdf
- 18 <https://datatracker.ietf.org/doc/html/rfc6749>
- 19 <https://www.iso.org/standard/85628.html>
- 20 <https://www.iso.org/standard/75061.html>
- 21 <https://www.iso.org/standard/24760-1>
- 22 <https://www.iso.org/standard/71670.html>
- 23 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>
- 24 <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14260>
- 25 <https://www.nist.gov/privacy-framework>
- 26 <https://pages.nist.gov/800-63-3/>
- 27 <https://www.pcisecuritystandards.org/standards/>
- 28 <https://openid.net/developers/how-connect-works/>
- 29 https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#name-introduction
- 30 https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
- 31 https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0-05.html
- 32 <https://trustoverip.org/our-work/technical-architecture/>
- 33 <https://www.w3.org/TR/did-1.0/>
- 34 <https://www.w3.org/TR/webauthn-2/>
- 35 <https://www.w3.org/TR/vc-data-model-2.0>
- 36 <https://www.w3.org/TR/webauthn-2>



GBBC

© 2025 Global Blockchain Business Council - Without permission, anyone may use, reproduce or distribute any material provided for noncommercial and educational use (i.e., other than for a fee or for commercial purposes) provided that the original source and the applicable copyright notice are cited. Systematic electronic or print reproduction, duplication or distribution of any material in this paper or modification of the content thereof are prohibited.