GLOBAL BLOCKCHAIN BUSINESS COUNCIL

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

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland

TABLE OF CONTENTS

SECTION I

INTRODUCTION TO GSMI 6.0

Since 2020, Global Blockchain Business Council (GBBC) has kept the industry up to date with the Global Standards Mapping Initiative (GSMI), the most comprehensive industry-focused effort to map and analyze the blockchain and digital assets community across six key areas:

1. **Legislation & Regulatory Developments**
2. **Taxonomy**
3. **Technical Standards**
4. **Blockchain & Digital Assets Landscape**
5. **Courses & Degree Programs from Accredited Educational Institutions**
6. **In-Depth Reports & Visuals on Key Themes**

GSMI reports and resources are crowd-sourced, open access, and intended to serve as a baseline for thoughtful and workable frameworks. This body of work supports the advancement of common standards to enable adoption, incentivize continued innovation, and advance collaboration.

GSMI content is referenced and utilized by corporations, regulators, government agencies, and academia globally, seeking a holistic view of critical topics for the blockchain and digital assets community.

With the release of GSMI 6.0, GBBC is profoundly grateful for the active participation of 110+ entities spanning government, corporates, startups, nonprofits, and academia, who also took part in 8 specialized working groups that continue to produce the most meaningful discussions on the most crucial issues in the space:

1. **Blockchain & AI Convergence**
2. **Decentralized Finance (DeFi) & Governance**
3. **Digital Identity & Privacy**
4. **Digital Money & Payments**
5. **Supply Chains & Critical Minerals**
6. **Taxonomy**
7. **Technical Standards**
8. **Tokenization & Custody**

The value of our dedicated network of members, partners, and collaborators is manifested in the quality and breadth of the final content. These individuals, as well as the journey of active dialogue, debate, and reflection that it takes to collectively produce this body of work, are fundamental. GBBC continues to advance meaningful collaboration in support of responsible innovation to meet the world's most pressing challenges, and the attitude and effort that these contributors bring is the reason for the remarkable progression of GSMI with every launch.

With this sixth annual release of GSMI comes an updated website with improved user friendliness, more robust content, and 5 landscapes that are more interactive than in previous versions. These improvements cumulatively build upon each other, making GSMI 6.0 the most robust and comprehensive release to date.

ACCESS GSMI 6.0

GSMI KEY FINDINGS

1.0 (2020)

- Global Regulatory Developments from 185 Jurisdictions
- Taxonomy with 10 Key Terms & Definitions
- 30 Technical Standards Bodies Advancing Blockchain Developments
- 2 In-Depth Reports & Visuals on Global Regulation and Crypto Derivatives
- Analysis of 50 Industry Consortia
- 8 Brief Country Spotlights on Switzerland, United States, China, Bermuda,
- Singapore, United Arab Emirates, Mauritius, and Kazakhstan

2.0 (2021)

- Global Regulatory Developments from 187 Jurisdictions
- Taxonomy with 182 Terms & Definitions
- 38 Technical Standards Bodies Advancing Blockchain Developments
- 300+ Courses from Accredited Educational Institutions
- 5 In-Depth Reports & Visuals on the Crypto Derivatives, Digital Identity, Global
- Taxation, Green Economy, and Policy
- Country Spotlight on South Korea

3.0 (2022)

- Global Regulatory Developments from 210 Jurisdictions
- Taxonomy with 182 Terms & Definitions
- 50 Technical Standards Bodies Advancing Blockchain Developments
- Landscape with 2,000+ Stakeholders
- 700+ Courses from Accredited Educational Institutions
- 5 Visual Fact Cards on, Crypto Markets, Central Bank Digital Currencies, Green
- Economy, and Blockchain for Taxation, and Stablecoins
- Country Spotlight on China

4.0 (2023)

- Global Regulatory Developments from 230 Jurisdictions & 6 International Bodies
- Taxonomy with 350 Terms & Definitions
- 63 Technical Standards Bodies Advancing Blockchain Developments
- Landscape with 2,000+ Stakeholders
- 1,500+ Courses from Accredited Educational Institutions
- 4 In-Depth Reports & Visuals on AI Convergence, Digital Identity, Supply Chain & Sustainability
- Country Spotlight on Brazil

5.0 (2024)

- Global Regulatory Developments from 230 Jurisdictions & 6 International Bodies
- Taxonomy with 391 Terms & Definitions
- 67 Technical Standards Bodies Advancing Blockchain Developments
- Landscape with 2,000+ Stakeholders
- 1,500+ Courses from Accredited Educational Institutions
- 5 In-Depth Reports & Visuals on AI Convergence, Decentralized Finance (DeFi),
- Digital Identity, Supply Chain & Sustainability
- Country Spotlight on India

6.0 (2025)

- Global Regulatory Developments from **230 Jurisdictions & 6 International Bodies**
- Taxonomy with **400+ Terms & Definitions**
- **100+ Technical Standards Bodies** Advancing Blockchain Developments
- Landscape with **2,000+ Stakeholders**
- **1,500+ Courses** from Accredited Educational Institutions
- **130+ Degree Programs** from Accredited Educational Institutions
- **5 Landscapes:** Regulatory Map, Taxonomy, Technical Standards, Educational Programs, Stakeholders
- **7 Reports:** AI & Blockchain Convergence, DeFi Governance, Digital Identity & Privacy, Digital Money & Payments, Supply Chains & Critical Minerals, Technical Standards, Tokenization & Custody

In the fast-changing environment in which blockchain technology and digital assets are developing, new themes and new key stakeholders arise with each launch of GSMI, as the GBBC community remains relevant on the importance of fundamental principles and standards for harmonized global scale for these solutions.

For the interactive regulatory map, the team expanded the content and user-friendliness, covering over 4,000 individual regulatory developments across 230 jurisdictions & 6 international regulatory bodies, while enhancing filtering features.

GSMI 6.0 also expanded the taxonomy to include 400+ terms, including multiple definitions for blockchain and digital assets terms, from globally recognized standards setters and selected major global regulators. The taxonomy also introduced a suggested "Top Definition" most relevant for certain stakeholders (e.g., regulators, financial institutions, decentralized finance players, technical standards setters, technology companies, educators).

The technical standards section continues to become more comprehensive, this time including 100+ bodies advancing standards, categorized by their role in the standards setting process. GSMI 6.0 also illustrates the main interactions and roles of the different standards setting bodies, as well as the process to develop and comply with globally recognized technical standards – namely the International Organization for Standardization (ISO) Technical Committee 307 on blockchain and distributed ledger technologies.

GSMI 6.0 also continues to update the blockchain and digital assets landscape mapping of over 2,000 stakeholders, categorized across essential functions (e.g., data providers, exchanges, wallets and custodians, decentralized finance applications, supporting infrastructure), while the mapping of 1,500+courses from accredited educational institutions is also expanded to include 130+ full degree programs, as the blockchain and digital assets space evolves.

With this comprehensive body of resources, we hope to serve our community with meaningful resources to support continued growth.

CONTRIBUTORS

Thank you to our team of contributors representing over 110+ entities including:

1inch
Accenture
Africa Blockchain Association
AI MIND Systems
AI2030
Aleo
Alliance Block
Animoca Brands
Askari Bank
Association of National Numbering Agencies (ANNA)
Ava Labs
Banca d'Italia
Banco Central do Brasil
BC Public Service
BGIN
Buenos Aires Government
Cahill Gordon & Reindel LLP
Capital Market Authority Kenya
Central Bank of Jordan
Chainlink
CUNY
Deusche Bank
DFM Data
Dhiway
Digital Euro Association
DTIF
EC-Council University
Eichner Advisory
Environmental Carbon Offset Allliance (ECOTA)
EUBOF
FedEx
Florida International University
Florida Tech
Fmr. State Dept
GBBC Ambassadors
George Washington University
GLEIF
GMC
Gosai Law
HBAR Fund
Hearts of Change
IDB Lab
Impera Strategy
IOTA Foundation
JFSA
Jitterbits
Kadena
Kenyan State Department for Investment promotion
Key State Capital
Kinexys by JP Morkgan
Kintsugi
LF Decentralized Trust
Linux Foundation
Media Luna
Mercy Corps Ventures
Mississippi House of Representatives
Moody's Ratings
Neural Fabric
Nigerian Bar Association-Section on Business Law
Nirmata-ai Ventures
NorthStar DAO
Open ID Foundation
Paravela
PayPal
Perkins Coie
Polymesh
RecycleGo
RFI Foundation
Ripple
SEC Zambia
Shinhan Securities
SMU
Standard Chartered
Sumsub
Suremark Digital
The Provenance Blockchain
The- EPE
United Nations Joint Staff Pension Fund
United Nations Pension Fund
University of Arkansas
U.S. Blockchain Coalition (USBC)
VerifyVASP
Wave Digital Assets
World Bank
Zodia Custody

Special thanks to the GBBC team for their contributions:

Diana Oreto (Barrero Zalles) – *Head of GSMI & Research*

Adrian Matak
Alfredo Oballos Diaz
Amina Turgulova
Emma Joyce
Jackson Ross
Justin Legesse
Patrick Bruckwick
Philip Gant
Riley Fay
Sandra Ro
Sierra Lewis
Tristen Dague

SECTION II

LEGISLATION & REGULATORY DEVELOPMENTS

What does Brazil's legal framework for digital assets look like?

Which agencies in Nigeria are shaping digital-asset regulation?

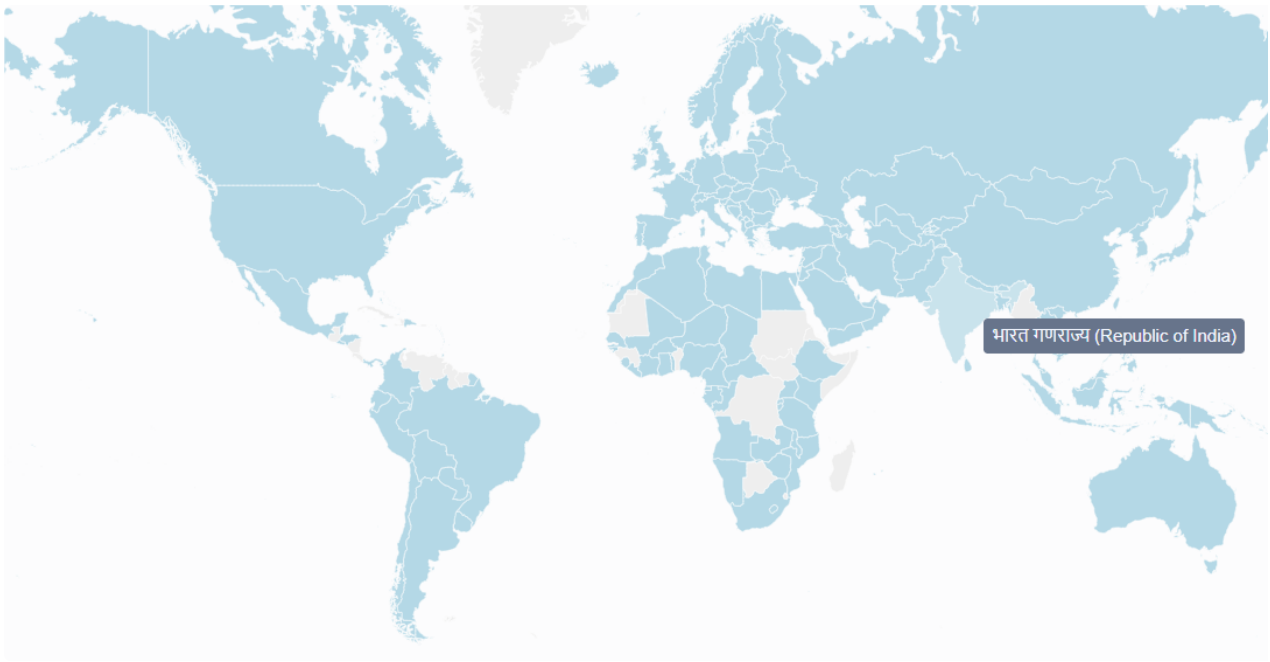
How is Japan structuring its licensing and consumer-protection rules?

How is the European Union regulating crypto and tokenized assets?

These questions—and many others—can be answered using GBBC's updated interactive map of digital-asset legislation and regulatory developments, published as part of GSMI 6.0.

A huge thank you to GBBC's 2025 IFC-Milken Institute Capital Markets Program Scholar, Chika Phiri, for applying her regulatory expertise to track the digital asset regulatory developments across more than 230 jurisdictions.

ACCESS THE INTERACTIVE MAP



SECTION III

TAXONOMY

As the blockchain and digital assets space develops at lightning speed, definitions are evolving with new applications being launched. Common understanding has become both increasingly critical and progressively complex. The need for clear and consistent communication is more important than ever, underscored by universally accepted definitions. Shared language creates the foundation for collaborative understanding and progress, bringing together stakeholders with shared interests to advance common goals and standards. Blockchain, often in combination with other emerging technologies, is already breaking silos and progressing substantive solutions to move our world in a positive direction and meet the most pressing challenges of our time.

The GSMI 6.0 Taxonomy includes 403 total terms specific to blockchain and digital assets and sector-specific terms relevant for key applications in AI convergence, supply chain, sustainability, and digital identity. At the core, 217 essential blockchain and digital assets terms are further categorized into main subject areas, drawing on academic approaches to categorization. Each term has been cross-checked against definitions from multiple globally respected standards setting bodies and industry-specific glossaries.

Notably, this taxonomy includes multiple definitions for blockchain and digital assets terms, developed by a range of globally recognized standards setting bodies, industry bodies, and regulatory entities, in order to reflect the fact that the space is still developing and that the definitions are continuously evolving. GSMI 6.0 introduces a "top definition" selection for each key term, based on the desired usability (e.g., legal, regulatory compliance, financial (traditional and DeFi), technical standards, technology, industry). Ultimately, this landscape of terms and definitions is meant to capture the full meaning of each concept as it is utilized in the industry today. Certain definitions are also inherently related based on common concepts, for which we have also provided visuals to illustrate major clusters of definitions.

METHODOLOGY

GBBC provides a taxonomy landscape, which includes multiple existing definitions for key terms in the space, as a way to document the state of common language and understanding. The foundational piece of this taxonomy consists in blockchain and digital assets, with additional sector-specific terms.

ACCESS THE INTERACTIVE LIST OF TAXONOMY AND DEFINITIONS

Blockchain and Digital Assets

Selection of Key Terms
- Foundational industry concepts
- Current developments being built
- Terms must fit technical, financial, and regulatory compliance objectives

Selection of Sources of Definitions
- Globally recognized international bodies
- Industry recognized sources of educational content
- Regulatory developments outlining terms

Categorization of Key Terms
- Taxonomy of blockchain and digital assets based on key concepts and activities

Populating Landscape
- Filling terms with definitions
- Revising sources of definitions against key terms and drawing all relevant definitions into a landscape

Selection of Top Definition Per Term
- Defining top definition as that with greatest usability for a specific purpose:
  - » Legal/Regulatory Compliance
  - » Financial (Traditional)
  - » Financial (DeFi)
  - » Technical Standards
  - » Technology
  - » General Education (this is relevant for non-blockchain native industries)

Sector-Specific Terms

Selection of Key Sectors
- In coordination with other relevant GSMI working groups

Selection of Key Terms
- In coordination with other relevant GSMI working groups

Selection of Sources of Definitions
- In coordination with other relevant GSMI working groups

Populating Landscape
- Fill top terms with top selected definition

Addition to Taxonomy
- Append sector-specific terms to taxonomy landscape for blockchain & digital assets

SECTION IV

COURSES FROM ACCREDITED EDUCATIONAL INSTITUTIONS

UPDATES ON COURSES FROM ACCREDITED EDUCATIONAL INSTITUTIONS

We have compiled this repository of over 1,500 courses spanning multiple academic disciplines, as well as over 130 full degree programs focused on blockchain technology. We hope that by compiling this repository of education related to blockchain, we will make it easier for those looking to get a more formal education to access the training they want. We also hope this resource can also help educators and researchers connect with each other to promote knowledge sharing and other collaborations such as research on common topics.

Since GSMI began documenting blockchain-related courses from accredited institutions, we have seen a year-over-year increase in the number of courses being offered across all regions globally. This reflects the fact that blockchain has become more mainstream over the same period and that there is significant demand for formalized education and skills-development around blockchain and blockchain-adjacent topics such as DeFi, decentralized systems, tokenization, and more. GSMI's mapping of individual university courses served as both a way for individuals interested in formal education on blockchain to find venues to satisfy that interest and for professors and others in the industry to connect with other professors and university departments on common areas of focus or interest.

With this in mind, we decided to shift the focus for GSMI 6.0 to examine full degree programs, minors, and professional certificates offered by accredited institutions. This shift in focus coincides with the proliferation of blockchain-related courses and aims to provide those seeking a deeper understanding of blockchain with more complete educational opportunities that will set them up for either a future career in blockchain or augment their existing education credentials with professional certificates to broaden their career opportunities and deepen their knowledge on specific topics within blockchain technology.

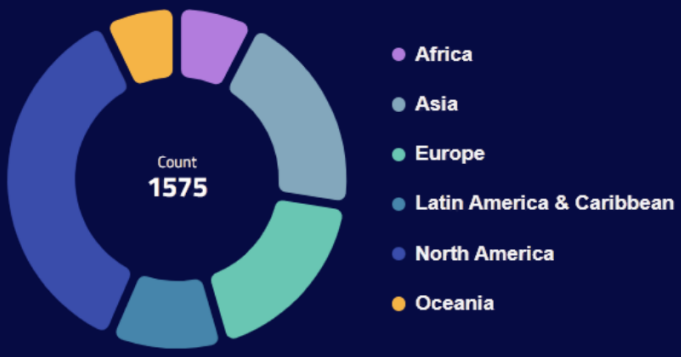
Through this mapping exercise, we discovered that many universities offer blockchain-related courses, but not full degree programs. Instead, we found that many existing degree programs have begun to integrate blockchain topics into their existing degree programs in lieu of having standalone blockchain degrees. In recognition of this, we will continue to host the GSMI 5.0 list of accredited university courses for those interested in course-specific educational opportunities.

If you are aware of any blockchain-related majors, minors, or certificate programs that are not shown on this list, please email gsmi@gbbc.io.

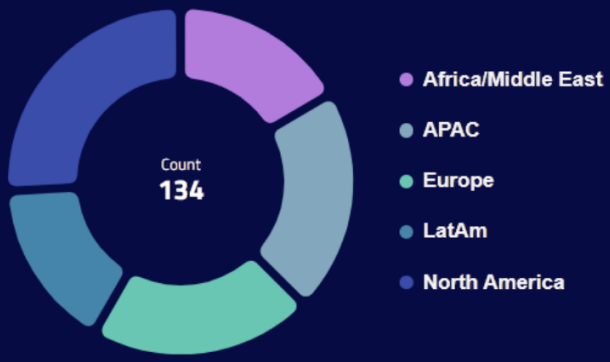
In parallel, there are several efforts to expand the actual credentialing process to digitally represent educational outcomes and give ownership of those credentials directly to learners. Several of these efforts are leveraging blockchain technology and tokenization concepts to track learning outcomes and provide ownership of educational data to students.

KEY ANALYTICS

Course Statistics



Degree Program Statistics



ACCESS THE FULL LIST

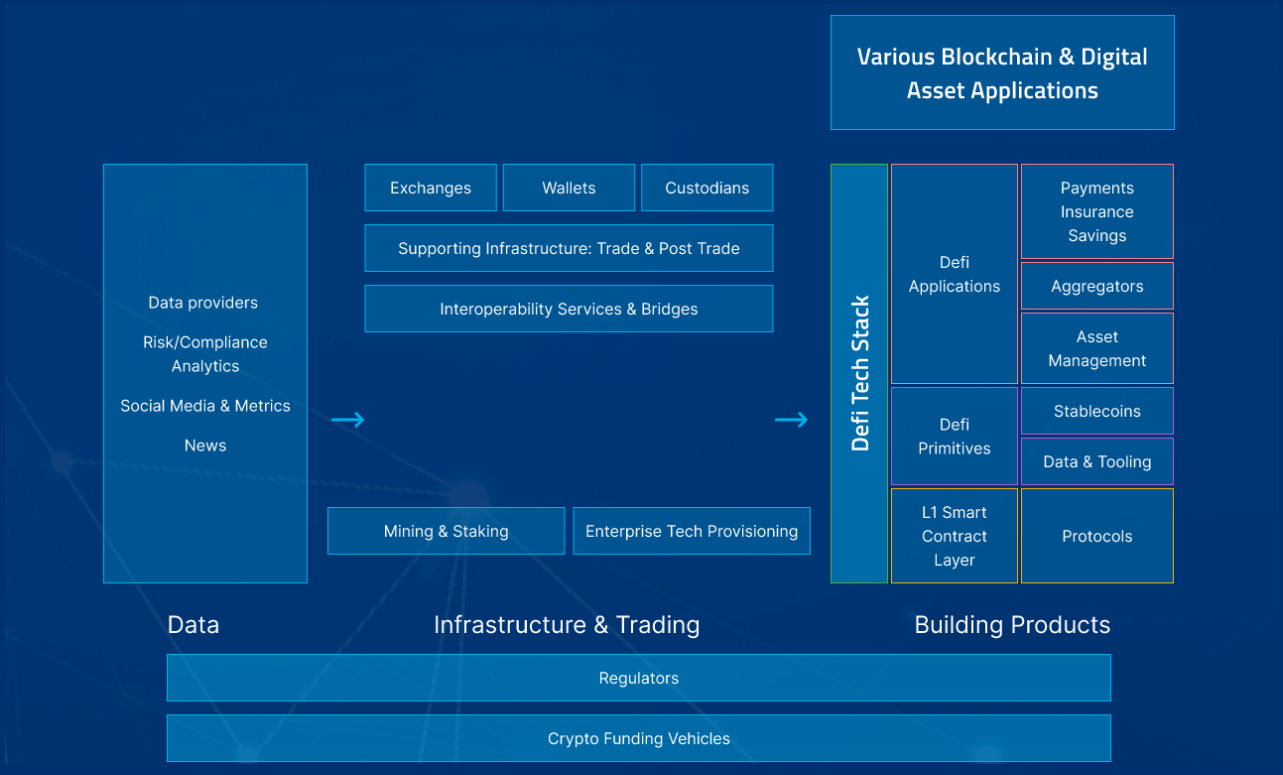
SECTION V

BLOCKCHAIN & DIGITAL ASSETS LANDSCAPE

GSMI offers a continually updated global mapping of key stakeholders and their roles in the blockchain and digital assets ecosystem, with their interactions summarized in the diagram below. GSMI 6.0 provides access to the full list of 2,000+ stakeholders and welcomes further suggestions from the community.

Use cases and infrastructure developments are continuing to unfold across all industry verticals, bringing a new generation of decentralized business models that rely heavily on communities of users and participants in order to make decisions and scale. The industry is continuing to mature and institutionalize into a multi-trillion dollar sector, with many more developments underway and innovations to come.

Key Stakeholders in the Blockchain & Digital Assets Landscape



ACCESS THE LIST

SECTION VI

IN-DEPTH REPORTS

Pages 13-255 include in-depth reports that were produced by our GSMI 6.0 Working Groups

GBBC
Global Blockchain
Business Council

AI CONVERGENCE REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 6.0

TOWARD DECENTRALIZED & OPEN-SOURCE AI: TRANSPARENCY, PRIVACY, SECURITY, AND RELIABILITY

GBBC GSMI 6.0

ACKNOWLEDGEMENTS

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

John deVadoss - CHAIR
Co-Founder, Providentia Capital

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

EXECUTIVE SUMMARY

AI deployment has moved from pilot to production – across content, decision support, and domain copilots. The upside is material; so are the risks. In the face of this trend, and the opportunities and risks it represents, this paper takes a position that is pragmatic: evaluating the use of blockchain strategically to make AI verifiable. For instance, blockchain technology can facilitate provenance of data and models, event-driven audit, and machine-readable attestations that third parties can test without exposing sensitive content. Building on prior GSMI reports on Blockchain & AI Convergence,[1] which established foundational topics on how blockchain can enhance AI deployments, this report comments specifically on recent developments toward decentralized and open-source AI, distinguishing hype from reality in light of existing challenges toward trustworthy AI, and ultimately offering an approach toward AI transparency, privacy, security, and reliability that is more attainable in the short term.

Better solutions & worse problems? AI can amplify value and, just as easily, scale existing bias and perpetuate system societal challenges. Blockchain technology can advance provenance and auditability, as levers to guide toward better solutions. Putting the AI explosion into perspective, consumer tools have reset expectations, and enterprises are weaving copilots into core workflows. Yet velocity has outpaced assurance. The goal is not to rush into maximal function in ways that can increase compliance issues, governance failures, and other risks; instead, the goal is to ensure responsible functions that can be trusted in the long term — with provable inputs, accountable execution, and verifiable outcomes.

The goals of AI transparency, privacy, security, and reliability are aligned with privacy goals, emerging governance scaffolds including standards and regulatory developments (e.g., ISO/IEC 42001, NIST AI, RMF, GenAI Profile, EU AI Act GPAI/Code), and illustrated through operating models that enterprises can adopt now.

FAST AI ADOPTION, FASTER THAN ASSURANCE

Increasingly in the recent months and years, AI adoption has accelerated across all firm sizes, from startups to major enterprises, and in all economic sectors, with tools ranging from content generation and decision support to domain-specific copilots embedded in enterprise workflows. In the EU, for instance, over 40% of large enterprises used AI in 2024.[2] This growth is not merely experimental; it is tied to revenue ambitions, cost containment, and competitive differentiation. Yet the velocity of deployment has outpaced the maturation of AI assurance, with much to be developed in areas like robust governance, run-time observability, auditable provenance, and defensible accountability. Leaders face three recurring questions:

- **What data went in and how was it processed to reach an outcome?**
- **What exactly happened at inference time?**
- **Who is accountable when outcomes drift or other unintended functions cause harm?**

At the same time, the regulatory and standards landscape is continuing to evolve around aspects like lifecycle governance—specifying what to document, what to prove, and how to verify it. Notably, ISO/IEC 42001 introduces a certifiable AI management system framework[3]; the NIST AI Risk Management Framework[4] and Generative AI Profile[5] translate risk concepts into operational controls; and EU obligations for general-purpose AI (GPAI)[6] begin phasing in, supported by a GPAI Code of Practice[7] with obligations and a Code of Practice.

Ultimately, in order for AI to scale business outcomes responsibly, assurance can no longer an ethics add-on; it becomes an operational requirement. The case for blockchain in AI is therefore not ideological but instrumental. To make claims verifiable—provenance of data and models, tamper-evident audit trails, and machine-readable attestations that external parties can test without exposure of sensitive content. In other words: transparency, privacy, security, and reliability. As many of the most tangible AI & Blockchain Convergence wins still flow through use cases and foundation models, this paper's emphasis is on the assurance fabric that makes those wins sustainable.

THE IDEAL OF OPEN-SOURCE AND DECENTRALIZED AI

In late 2004 and early 2005, DeepSeek took off as an open-weight AI company with a revolutionary approach where anyone can modify and deploy models. Worth noting is that while DeepSeek quickly brought attention to open-source AI, its own model is technically open-weight, not fully open-source. For readability purposes, the rest of this document will mean "open-weights" when referring to "open-source."

Releasing a series of powerful AI models that were significantly cheaper to train and run than existing competitors, DeepSeek sent shockwaves across the AI market, having found a way to optimize algorithms and hardware to enabling high performance at a fraction of the cost of existing models out of Silicon Valley. The draw of DeepSeek's open-source approach goes hand in hand with its decentralized AI capability where anyone can download, modify, and deploy AI models without centralized oversight. This characteristic is unlike that of proprietary, SaaS-based models and opens access to AI tools at a broader level, democratizing access to advanced AI tools for developers and researchers around the world. DeepSeek therefore allows community-driven deployment and usage without the need for a single controlling entity, and often relying on decentralized storage networks to reduce dependence on centralized servers. It is worth noting, however, that only DeepSeek could create newer versions of models, having the source code for pre-training and training, as well as the lineage of data. Other participants could 'distill' DeepSeek (e.g., fine-tune, RAG, etc).

Within policy and technical communities, open-source AI and decentralized AI are often presented as remedies to opacity and concentration concerns, leading toward greater reliability. The ideal is attractive: **models whose code and weights are inspectable; datasets with declared provenance and licenses; contributions recognized via verifiable credentials; and execution spread across diverse nodes to avoid single points of failure**.

In this vision, AI becomes more explainable, reproducible, and inclusive, with community governance mitigating monopolistic control. Moreover, privacy can be preserved with self-hosting solutions and users' control over their data use and processing.

Decentralization extends the ideal by distributing compute, storage, and decision rights, aligning incentives through tokenized or reputation-based systems, and enabling federated and privacy-preserving training that respects data sovereignty. Together, open and decentralized approaches promise to widen participation, increase resilience, and ground model behavior in provable contributions. New business models can arise from decentralized AI marketplaces, open models, and cooperative ownership structures.

Open-source and decentralized AI models can reveal exactly how models were trained and where the data was sourced, providing full visibility and certainty rather than a “black box” of unknown data provenance and processing leading to a result. In “black box” scenarios, it is difficult to understand why models may hallucinate or perpetuate biases, and leaving these concerns unaddressed can risk the compounding of even more problematic behavior with each new version of a model. Without accurate data provenance, it is impossible to predict how much AI can deviate in different directions from the expected outcome if access to data is not sourced in a quality manner.

If open source and decentralized AI can allow concerns to be more effectively identified, there can also be mechanisms of economic incentives (e.g., credits, points) to reward participants globally for contributing to address these concerns, which can lead to greater clarity on who and how sources come from. Finaly, more open-source and decentralized approaches to AI will allow a broader view of lived experiences globally that is beneficial to all – from embracing transparency and accountability for training data, to provenance of data sets.

In short, open-source AI could level the playing field by democratizing access to technology solutions, in ways that lower the entropy of coordination, while decentralized AI spreads rights and responsibilities. A primary benefit of open-source AI may be that it is the optimal ethos, and best cultural and technical fit for decentralized AI. This combination increases traceability, which enterprises need to trust and scale AI.

BENEFITS OF OPEN-SOURCE AI

Open-source models provide an alternative to major concerns around AI being controlled with monopoly power. Open-source AI is attractive for the following characteristics:

TRANSPARENCY & INSPECTABILITY

Public code, model cards, and—where feasible—training declarations allow independent scrutiny, in ways that reduce information asymmetries and increase verifiability. Anyone can inspect a model's code, data, and model architecture. This can reduce risks of hidden biases, unethical practices, or backdoors.

REPRODUCIBILITY & SUPPLY-CHAIN INTEGRITY

When artifacts (e.g., weights, tokenizers, loaders) are signed, hashed, and anchored, participants can independently rebuild and replay pipelines. This can enhance education and research, as an excellent resource for learning and experimentation that encourages academic collaboration (e.g., artifact signing solutions standard and tooling).

CUSTOMIZABILITY & SELF-HOSTING

Organizations can tailor, fine-tune, and deploy locally to preserve confidentiality and enforce policy. Developers can tailor models for specific tasks or environments. Customizability also facilitates experimenting with modifications and fine-tuning.

DEMOCRATIZATION

Democratization: Lower barriers to entry can facilitate free access to individuals, startups, and researchers, especially in the Global South and traditionally underrepresented populations, seeking to build and experiment with AI solutions, without the need for substantial budgets.

COLLABORATION

Open contributions from community-driven innovation foster rapid developments, where bugs or other concerns may be found and fixed more quickly by a global community.

ATTRIBUTION & INCENTIVES

Verifiable credentials and on-chain attestations enable granular credit for data, compute, and evaluation—foundations for sustainable contribution markets.

BENEFITS OF DECENTRALIZING AI

As an ideal, many of the benefits of decentralized AI overlap with the benefits of open-source AI, which yet again supports the fact that these two attributes are a natural fit to be deployed together. The attributes and value added by decentralization in AI can be summarized as the following:

SECURITY & PRIVACY

By avoiding central data lakes, decentralized approaches reduce single-point compromise risk, as there is no central database to hack or manipulate. In addition, rather than centralized platforms owning user data, individuals and organizations can better control their own data in a model that provides greater data sovereignty. With confidential computation, sensitive data may be used for training purposes or inference, without being exposed. This enables privacy-enhancing computation (e.g., TEEs, MPC, ZK proof systems) that performs learning or inference without exposing raw data.

FAIRNESS & INCLUSIVITY

Broader participation—both in data contribution and in governance—can improve representativeness and reduce geographic or cultural bias. Diversity in nodes and datasets expands the model's "lived experience" beyond a handful of players or synthetic data which can become unrealistic over iterations of reprocessing. Diverse data sources, by including data from many nodes and communities, also improves representation and reduces bias. With democratized access, any participant can also contribute to, train, and utilize AI models without the need to rely on a few large tech players. Moreover, models and updates can be managed collectively, which leads to reduced monopoly power.

RESILIENCE & RELIABILITY

Distributed topologies mitigate outages and censorship, while consensus-anchored events provide tamper-evident histories of model changes and policy updates. Decentralization creates an environment of no single point of failure, where even if some nodes may fail or go offline, continued AI services remain. This also results in censorship resistance, where it becomes more difficult for a single entity (e.g., government or corporation) to shut down or censor AI models.

INNOVATION & EFFICIENCY

Shared compute marketplaces and cooperative training enable resource pooling and resource sharing, where idle compute power can be pooled together (e.g., edge devices, GPUs). Fine-tuning can propagate through verifiable release channels that preserve lineage and licensing, in a model of collaborative building involving several parties contributing to building models. In this context, training can become scalable, with federated learning and swarm intelligence training models across nodes distributed globally.

ECONOMIC ALIGNMENT ACROSS THE ECOSYSTEM

Tokenized and credential-based systems reward data providers, validators and nodes, red-teamers, and evaluators, creating a more complete AI supply chain with accountable roles. Shared infrastructure also reduces dependence on otherwise expensive compute (e.g., centralized cloud services).

REALITY CHECK: NEITHER OPEN-SOURCE NOR DECENTRALIZED AI ARE A REALITY AT SCALE

While AI delivered in an open-source and decentralized format has much promise, this has yet to materialize. As both consumer-facing and enterprise-focused AI solutions are expected to alter how human work is performed, the pace of AI adoption today has far exceeded the ability to manage risks and enforce governance. Estimates suggest that 82%[8] of open-source software components are considered risky due to factors like poor maintenance, outdated code, and security flaws. Moreover, many open-source projects are run by small teams or individual volunteers with limited resources, leaving them vulnerable to attacks. Threats are becoming more sophisticated, with the potential for supply chain interference in ways that can have significant ripple effects.[9]

For instance, despite the excitement created around a model like DeepSeek, users expressed concerns around data privacy, leading a portion of them to run the model in their own devices as a way to avoid making their data openly available. In the current geopolitical context, concerns around sending data to China, where DeepSeek originated and where its servers may store data, also raised questions, especially in the event of vulnerabilities that could allow sensitive data to be sent over unencrypted channels. Certain governments (e.g., Australia, Italy, Taiwan) have even blocked or restricted access to DeepSeek on government devices, due to national security and privacy concerns, while regulators have raised concerns over lack of transparency and potential user data exposure. It is worth noting, however, that it is possible to download and run DeepSeek (and other models from China) on one's own infrastructure, which would minimize these concerns.

These concerns are an indication that today's AI ecosystem, which has yet to mature, falls short of both ideals of open-source and decentralized AI. "Open" models are often open-weights with incomplete training transparency. Replication is possible in part, but end-to-end reproducibility is theoretical. Decentralized networks grapple with coordination overhead, uneven quality, poisoning and backdoor risks, and fragmented governance. Meanwhile, enterprises gravitate to centralized API providers because they deliver performance, tooling, and support agreements—features that are still maturing in the open and decentralized stack. It becomes evident that open-source and decentralized AI systems have their associated risks that would need to be addressed in order to scale.

Because we haven't yet realized yet true open-source AI or decentralized AI today, and there are still multiple technical and related challenges to get there, it may be deceptive to utilize these terms in a context where nobody has truly released an AI model that is as open and decentralized as to allow truly replicating results.

LIMITATIONS AND RISKS OF OPEN-SOURCE AI

Open-source ecosystems carry specific trade-offs:

Security & Misuse: Functional models can be repurposed for deception, intrusion, or automated abuse without central chokepoints. Because open models pose no restrictions over who uses them and how, bad actors can propagate deepfakes, misinformation, spam, and even repurpose open models for harmful purposes if there are no controls, oversight, or accountability.

Cybersecurity: Because models depend on vast community-managed supply chains, there is no guarantee of legitimate training data, and attackers can analyze and exploit architecture-level weaknesses. Bad actors can inject malicious code, copy or modify weights and redistribute them with hidden backdoors, or re-release "trojaned" versions of models. Compromised model weights or poisoned training scripts can propagate before being detected. Sensitive data can also be leaked and misused.

Quality Control & Maintenance: Documentation, testing, and security hardening vary widely, such that sustainability may depend on contributor bandwidth. Open-source does not guarantee that all projects would uphold high standards, and some may indeed lack adequate governance. Moreover, as many open-source projects rely on unpaid contributors, long-term maintenance, support, and sustainability may be unpredictable.

Fragmentation & Incompatibility: As forks multiply; governance can diverge and standardization would lag, which would ultimately hinder interoperability. This poses challenges for standardizing and regulating a growing ecosystem.

Reproducibility Gaps: Without full data lineage and environment capture, "open" does not equal "replicable."

LIMITATIONS AND RISKS OF DECENTRALIZED AI

Decentralizing AI is currently an evolving process and can be viewed as a moving target, to be achieved at some point in the future, with several challenges if we are to eventually get there at all. Due to the concerns over AI holding hidden biases and obscurity on sources of data, many projects have sought to brand themselves as decentralized AI. Yet centralized approaches still have distinct advantages that are clearly beneficial today, especially as decentralized AI continues to mature. Decentralized approaches to AI also face specific tradeoffs, with the following considerations:

Technical Coordination: Synchronizing many nodes reduces efficiency and complicates versioning and rollbacks because it requires several resources, and it may also be difficult to ensure all nodes contribute clean, high-quality data or compute. Performance inefficiencies may also arise, with slower training and inference (e.g., limits of distrubuted training and federation). Fragmentation may occur, with multiple and inconsistent model versions may also arise across the network.

Security & Trust: Data poisoning and adversarial updates demand robust verification (e.g., cryptographic proofs, attested execution) that are still costly to operate. Bad actors may also insert backdoors. If not designed carefully, even decentralized, federated and peer-to-peer learning models can leak sensitive patterns.

Governance & Accountability: Disputes over upgrades, licensing, and ethical bounds, stemming from a lack of clear authority, can stall progress, such that it may be unclear who is accountable when harm occurs. Ensuring legitimate model updates and results requires robust cryptographic proofs and consensus mechanisms – pointing to the need for effective governance models. Governance, moreover, can become fragmented if different communities adopt divergent rules or protocols, which may ultimately lead to lack of standardization. Community-driven governance brings risks of decision-making being misaligned with broader societal values, leading to potential ethical drift.

Jurisdiction-specific Compliance: Especially when it comes to specific requirements on issues like privacy, data storage and sovereignty, and right to be forgotten in different jurisdictions (e.g., US, EU, China), requirements can be fragmented across different jurisdictions. This can make it challenging for a decentralized AI network, with nodes operating across multiple jurisdictions, to comply simultaneously with conflicting or incompatible laws. In the EU, for instance, GDPR restricts cross-border data flows and requires a "right to erasure" of data. US laws regarding data use may vary by state. China's PIPL regime enforces state oversight and strict localization. Countries like India, Brazil, Singapore, and Canada also have their own mandates on data and AI. IT can be extremely difficult to ensure that data never leaves a given region, while model updates may leak certain sensitive data. Moreover, compliance with erasure rights can be nearly impossible without strong cryptographic controls and techniques for models to un-learn. Accountability in cases of harm may also be very difficult to determine.

Economics & Adoption: Incentives may over-reward activity over quality, and network effects continue to favor centralized incumbents which have more compute, data, and capital. There are high barriers to entry when new infrastructure is required to participate, making it difficult for decentralized alternatives to compete at scale.

Regulatory & Ethical Uncertainty: Supervisory oversight is made more difficult without a central operator or clear standards or harmonized regulatory requirements globally. Data-sovereignty and sectoral rules (e.g., GDPR, HIPAA, data localization and sectoral guidance, etc.) raise open questions for cross-border operations, which can complicate decentralized training.

A MORE PRAGMATIC AVENUE: TRANSPARENT, PRIVATE, SECURE, AND RELIABLE AI

To sustainably implement the benefits of AI, the role of blockchain is key to provide a governance framework to address current challenges with a focus on greater transparency, privacy, security, and reliability. Rather than focus on open-source and decentralized AI, a more realistic alternative may be to focus first on attributes that pave way toward these ideal outcomes. Because open-source and decentralized AI have yet to become a scalable reality in the space, a more realistic approach may be to treat "open" and "decentralized" as gradients, focusing instead on ways to make AI more transparent, private, secure, and reliable.

This way, even though open-source and decentralized AI are not a reality at scale at this moment, they remain aspirational as they have are aspects we can draw on today that can pave way toward a desired AI future. In the short term, a proposed architecture and infrastructure that prioritizes the attributes of transparency, privacy, security, and reliability will pave the way toward future stages of open source and decentralized. One approach can be to identify specific factors that yield measurable assurance of these three attributes and integrate them into production systems that must meet concrete regulatory and business obligations. To ensure greater transparency, privacy, security, and reliability, blockchain technology is a crucial tool to ensure desired outcomes - both for attributes for training the AI models themselves and attributes at inference time, which have important distinctions. AI solutions should adopt the following :

AUDITABILITY

This refers to the ability to independently verify how an AI system was built, how it operates, and whether its claims are legitimate, using transparent, tamper-resistant records and blockchain technology. In such a framework, third-party forensic analysts can query blockchain-based systems of record to confirm that the human-readable assertions made by an AI operator accurately correspond to verifiable on-chain evidence. This bridges the trust gap between what an AI provider claims and what an outside auditor can independently validate, relying on blockchain proofs, cryptographic guarantees, and other mechanisms for establishing legitimate claims. Auditability extends to examining data provenance, the processing of data, and the evolution of model weights, including the ability to use mechanistic interpretability queries to understand how specific inputs, prompts, or query structures influenced model behavior or tuning.

In this context, auditability ensures the quality of a system, allowing it to be reliably examined through durable records, documentation, and evidence, and ultimately ensuring compliance, accuracy, and accountability. To support this, an event-driven architecture is often required: audit events must be designated, captured, and finally processed on-chain or through equivalent mechanisms that record data provenance, runtime performance characteristics, weight attributions, or regulatory compliance checkpoints. Effective AI auditability requires a governance process that clearly defines what constitutes an audit event, encodes the relevant requirements, and ensures the system can produce human-interpretable outputs. These outputs must be paired with a cryptographic verification process that traces the entire auditing workflow. This can function through a structured checklist that validates each step of the AI system's behavior against secure, immutable evidence.

DATA SOVEREIGNTY AND PRIVACY

AI data sovereignty and privacy revolve around giving end users meaningful control over how their data is used by AI systems, including the ability to choose, both at a granular and contextual level, which parts of their data can be accessed for a specific query, and to understand exactly what portions of their interactions, integrations, or data provided are utilized. Three operating models exist with specific user interactions with AI and data control considerations.

Scenario 1	Involves consumers or organizations using an API-driven model operated by a third party. For example, an employer using an external AI service under a licensing or hosting framework, or running a corporate AI model locally where all data and operations remain inside the enterprise environment.
Scenario 2	Represents true self-sovereign AI model, in which individuals use fully local, isolated, self-contained models that do not rely on third-party infrastructure. This differs significantly from consumer tools like ChatGPT, where privacy assurances depend on provider policies rather than user-controlled guarantees.
Scenario 3	Reflects settings where AI is used on people by governments or corporations, often without individuals' meaningful ability to consent or limit data use.

The first two involve either locally hosted systems or AI accessed through an external API, such as a centrally hosted large language model where the provider retains user prompts and responses depending on whether the model is accessed through a free or paid version. The purpose of locally hosted models across these scenarios is to provide strong privacy guarantees, prevent data leakage, ensure isolation, and offer predictable compute resources for organizations. These are conditions that also make it possible to engineer robust guardrails, enforce governance rules, and define auditable events. These protections are far more difficult to ensure when relying solely on API-based external models, where users often exchange privacy for access, particularly in free tiers designed to collect usage data for training or market research. Even paid versions present verification challenges, as providers may assert that user data is not retained or used for model improvement, but without cryptographic verification or blockchain-based audit trails, it is nearly impossible for end users to prove adherence. As models proliferate and usage expands, these privacy risks grow.

To address them, cryptography plays a central role. Privacy-enhancing technologies such as secure enclaves, homomorphic encryption, zero-knowledge proofs, or selective disclosure mechanisms enable granular and enforceable consent rather than blanket data access. These tools ensure that users can authorize specific uses of their data while preventing unauthorized leakage, creating the foundation for verifiable data sovereignty in an AI-driven world.

CUSTOMIZABILITY

Customizability of AI refers to the ability to tailor models to specific users, organizations, and operational environments in order to improve accuracy, reduce errors, and create more meaningful interactions. At the individual level, customization enables personal AI agents that adapt to a user's preferences, history, style, and objectives. For corporations, customization can involve fine-tuning models, implementing graph structures, and building retrieval-augmented generation (RAG) systems that give an AI model access to curated knowledge bases. These approaches not only enhance performance but also significantly reduce hallucinations by grounding model outputs in verified information. Emerging research suggests that many hallucinations stem from the inherent compression dynamics of large models, offering a new perspective on why these errors occur and how they can be controlled through architectural and training adjustments.

Additionally, custom AI systems can incorporate quantitative analysis before a prompt is processed to predict the likelihood of a hallucination. When a prompt is flagged as high-risk, the system can trigger additional safeguards, such as human-in-the-loop review, alternative reasoning routes, or stricter grounding protocols. This layered approach to customization, which can span across personalization, model tuning, structured knowledge integration, and pre-processing analysis, creates AI systems that are safer, more reliable, and better aligned with user and organizational needs.

ETHICAL GOVERNANCE & RECURRENT VALIDATION

Ethical governance and recurrent validation for AI require a proactive and continuous approach that integrates risk management, oversight, and technical monitoring into every stage of an AI system's lifecycle. Instead of treating AI deployment as a one-time "build, deploy, and profit" exercise, organizations need mechanisms that continually assess potential harms, detect shifts in model behavior, and provide pathways for redress, updates, and corrective action. This involves embedding ethical safeguards directly into governance frameworks and making corresponding architectural adjustments to deployment models and runtime environments so that ethical requirements can be practically implemented rather than merely stated. Because AI performance in high-risk or sensitive domains (e.g., healthcare, finance, public safety) cannot be assumed to remain stable over time, ongoing technical validation must be both scientifically rigorous and sociotechnically grounded. Models trained on clinical, demographic, or behavioral data need adequate monitoring to ensure their outputs remain accurate, fair, and safe for the populations they serve, especially if performance naturally degrades or contexts change.

The need for recurrent validation is further underscored by the continual emergence of new security vulnerabilities and the corresponding countermeasures that must be deployed to maintain system integrity. As regulatory frameworks evolve, organizations must also adapt their AI systems to stay compliant, incorporating new rules into operational practices rather than retrofitting compliance after harm occurs.

Experience-based training is an essential part of this ethical foundation: AI must be able to demonstrate the authenticity and provenance of the data it was trained on, anchoring its outputs in reliable ground truths. Systems trained solely on digital or synthetic datasets will inevitably fail to capture the complexity of lived human experience, limiting their effectiveness and increasing the risk of harm. Ethical governance, therefore, is not a static checklist but a dynamic, recurring process that ensures AI systems remain accountable, safe, context-aware, and aligned with human values throughout their operational lifespan.

SELF-ASSESSMENT FOR AI TRANSPARENCY, PRIVACY, SECURITY, RELIABILITY

It is essential for all stakeholders to take proactive measures and develop a sense of shared responsibility to ensure transparent, private, secure, and reliable AI solutions that pave way toward a true open-source and decentralized AI future. Self-awareness can be a key factor to mobilize stakeholders to take steps toward more legitimate AI uses, while avoiding questionable and suboptimal procedures.

This section translates the earlier sections' argument into a practical instrument, proposing a Self-Assessment approach for individuals, companies, and organizations to evaluate the transparency, privacy security, and reliability of their AI uses. The thesis is straightforward: if AI is to create long-term value, it must be transparent, private, secure, and reliable in ways that can be evidenced, not merely asserted. Earlier, we traced how enthusiasm for open source and decentralized AI has outpaced what enterprises can actually guarantee; we also proposed a selective, evidence-first architecture where blockchain is used as an assurance utility: anchoring provenance, emitting tamper-evident audit events, and enabling selective disclosure through verifiable credentials

A self-assessment operationalizes that architecture. It helps teams and individuals locate their current assurance maturity and prioritize what to do next. Concretely, it asks whether one can show, on demand and without oversharing, what data went in, what happened at inference, and who is accountable for what. Where earlier sections framed the ideals (openness, decentralization) and the compromises (coordination, quality, accountability), this tool focuses on what can be proven today, mapping each control to verifiable evidence, such as provenance anchors for data and weights, event-driven audit for model, and policy changes.

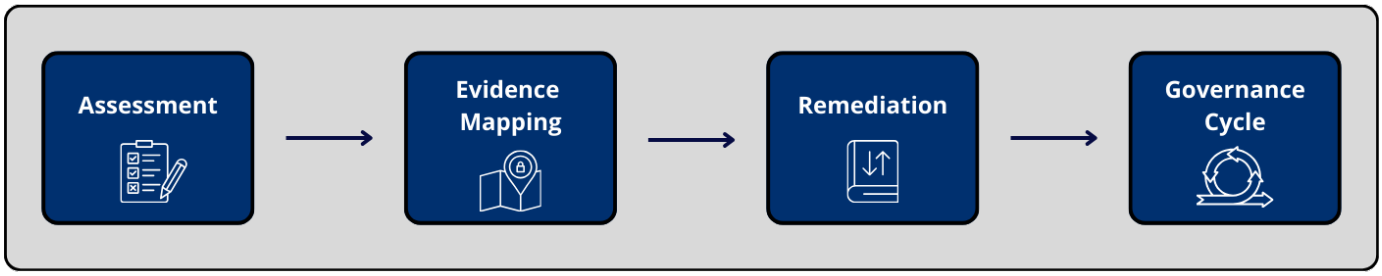
The instrument is intentionally broad in audience. Individuals running local models, SMEs fine-tuning open weights, and large enterprises orchestrating API-based copilots can all complete it. It is equally applicable to outsourced phases: labelling, fine-tuning, evaluation, even full training - by requiring machine-readable provider attestations that you can anchor into your own records. In every case, the emphasis is the same: move from claims to cryptographically backed evidence.

This full self-assessment questionnaire, which can be found in ***Annex 1***, scores AI implementations as low/medium/high in terms of transparency, privacy, security, and reliability respectively. The scoring methodology assigns points for each question to determine low/medium/high for each category (e.g., depending on answers or by yes/no answers, etc.). The final evaluation from the assessment would categorize overall AI use as fair/good/great.

The self-assessment is a tool meant to help improve AI users' awareness of what level of AI transparency, privacy, security, and reliability they are operating with, as well as present blockchain as a solution to move toward higher levels of AI transparency, privacy, security, and reliability. This is essential for users to take ownership and assess the expected accuracy of their own AI-informed decision making and outcomes, as well as how holistic their approach to AI currently is. Moreover, awareness of the resilience of AI solutions utilized can help identify any risks and take remedial steps. Eventually, this assessment framework could be tied to certifications and globally recognized standards, as a path toward compliance.

WHAT THE SELF-ASSESSMENT INSTRUMENT DOES

- Provides a structured, lifecycle-based review of AI assurance across five dimensions and produces an assurance maturity profile, plus a remediation plan indicating where web3 controls (anchors, attestations, selective disclosure, authenticity credentials) raise assurance with minimal disruption.
- Works for individuals and organizations—from a self-hosted local model to an enterprise portfolio and third-party APIs.



URGENCY OF SELF-ASSESSMENT MEASURES

As the innovation community continues to chase the next breakthrough, whether quantum advancements, new amplification tools, or novel "killer apps," there is an urgent need to communicate that responsible AI is not optional but essential. The accelerating complexity and influence of AI systems require a model of ethical governance that is not merely aspirational but structurally enforced, and this is where Web3 becomes indispensable. We need a Web3-dependent responsible AI framework because traditional AI alone cannot meet the demands of transparency, provenance, auditability, and verifiable compliance. Blockchain and related technologies provide the backbone for addressing these challenges, offering mechanisms that align with the intricacies of modern AI systems.

Adoption has outpaced assurance. Earlier sections tracked how AI moved from pilots to production across content, decision support, and domain copilots, with uptake visible across firm sizes. That same momentum exposed a gap: many programs cannot evidence the basics when challenged by a board, a regulator, or a customer—what data went in, what happened at inference, who approved the change that altered behavior. In parallel, the reference rails are hardening, with evolving regulatory requirements and standards.

Two additional pressures make the timing acute.

- **First, outsourcing and API dependence:** much of modern AI is trained, tuned, or served by third parties. Without machine-readable attestations from providers—and a place to anchor them—assurance maturity hits a ceiling, no matter how capable the model.

- **Second, data quality and sustainability:** pipelines drifting toward synthetic-on-synthetic inputs degrade silently while consuming more energy/compute. A managed ground-truth budget, verifiably sourced via web3 credentials and content authenticity tools, is the most reliable corrective (e.g., considerations for W3C DID/VC standards, C2PA, and sustainability metrics).

The Self-Assessment arrives, therefore, as a timely instrument: it internalizes this report's conceptual arc: from ideals, through compromises, to pragmatic architecture, and converts it into actionable diagnostics. It helps teams identify their current assurance maturity and shows how to move it upward using the controls already set out in this chapter, including provenance anchors, event-driven audit, selective disclosure, content authenticity, and confidential assurance. In other words, it operationalizes the central claim that responsible AI is ledger-dependent, because the forms of evidence that confer legitimacy are most credibly delivered with blockchain and related cryptography. This may also pave the way toward greater compliance as regulations like the EU AI Act, GPAI, and other requirments develop.

FROM SELF-ASSESSMENT TO A FUTURE OF RESPONSIBLE AI WITH BLOCKCHAIN TECHNOLOGY

We leave it to individuals and organizations to choose a methodology that works for best them, as long as it satisfies the criteria that we laid out in this paper. Advancing toward the future, we must resist both naive optimism (assuming that with enough data the models will eventually figure it out) and fatalistic pessimism (AGI-doom). The imperative is neither to blindly trust nor to dismiss these systems but to operate responsibly, and responsibility at scale requires cryptographic, decentralized, and verifiable infrastructure. Implementing blockchain and ledger technologies is therefore not a peripheral enhancement; it is a foundational element of how AI must function going forward. As part of this shift, it becomes increasingly important to evaluate the attributes, limitations, and governance approaches of widely used systems and large models, ensuring that they align with principles of ethical, accountable, and transparent AI.

This is precisely where blockchain as enabler matters, as verifiable provenance and tamper-evident audit are the shortest path toward trustworthy AI at scale. It is not necessary to record sensitive data, or any data at all, on chain, but instead it is necessary to anchor facts about the data and the model lifecycle. It is not necessary to make everything public, but instead it is necessary to implement a selective disclosure so third parties can check claims without seeing raw inputs. We don't need a fully decentralized stack to benefit; we instead need the minimum cryptographic commitments that make your system verifiable and replayable when it counts. Blockchain technology strengthens AI systems precisely at the data layer, where responsible AI challenges may be most acute. Regulations such as the EU AI Act, which requires foundation models to disclose training data sources, categorize high-risk systems, and specify expectations for data governance and copyright transparency, illustrate why blockchain-based verification will become increasingly necessary. Organizations operating in the EU and beyond can determine how blockchain can help them meet these requirements, from automated compliance proofs to data-lineage tracking.

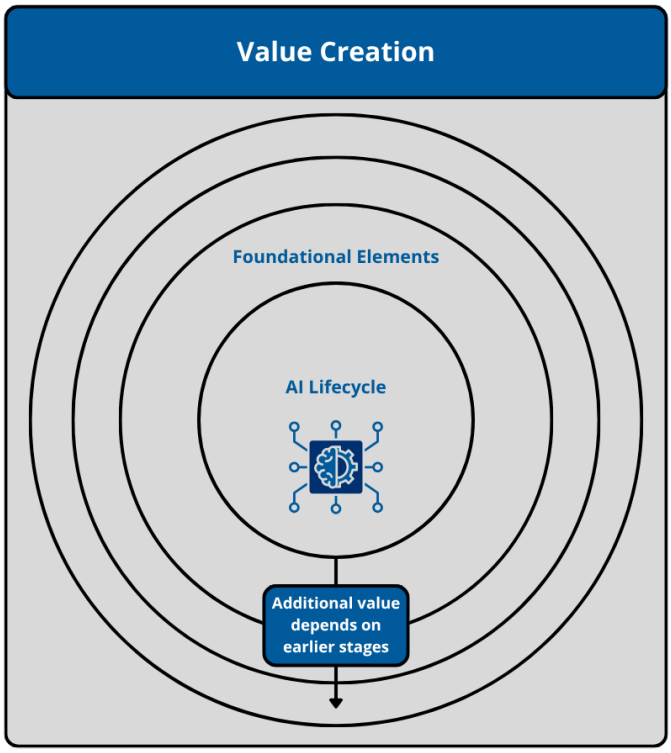
One approach we propose is to view the value that blockchain adds to AI implementations in three tiers:

Good
Ensures conformance with relevant rules and standards

Better
Introduces ledger-enabled guardrails that enforce policies and protect against misuse

Best
Applies blockchain capabilities strategically to create and deploy AI systems that are verifiably responsible, resilient, trustworthy, and aligned with human and environmental well-being

An AI lifecycle approach to unpack the results of the self-assessment into actionable strategies may be beneficial. A long-term, phased approach can be considered for moving from self-assessment to a future of responsible AI, supported by blockchain technology. The process begins by defining a clear methodology, then building the backend infrastructure, followed by the frontend interface, and finally connecting the components and executing the necessary integrations. This progression can be visualized below:



AI Lifecycle

DATA COLLECTION
(ground truth, synthetic, 3rd-party data)

TRAINING DATA

Risks	Blockchain's Role	Self-Assessment Opportunites
• Unverified or low-quality data • Bias, demographic skews • Data provenance uncertainty • IP/copyright violations • Privacy leakage from training sets	• Immutable provenance tracking (source, timestamp, rights) • Cryptographic proofs or dataset authenticity • Consent receipts & selective disclosure • Verification of lawful data usage • Audit trails for outsourcing of labeling/data	• Data diversity & representativeness • Dataset licensing & compliance • Synthetic vs. real data balance • Validate consent and privacy controls • Data minimization practices

MODELING
(training runs, fine-tuning, parameter updates, weight generation)

Risks	Blockchain's Role	Self-Assessment Opportunites
• Hallucinations from over-compression • Hidden biases in weight formation • Poisoned or manipulated training data • Undetected degradation across versions • Unverifiable claims about model behavior	• Version-controlled, tamper-proof model checkpoints • Cryptographic attestation of training events • Mechanistic interpretability records anchored on-chain • Proofs of training conditions • Secure multi-party training records	• Training documentation completeness • Hyperparameter impact on safety • Version history for improvements or regressions • Test model for bias, draft, adversarial susceptibility • Validate model grounding practices (RAG, graphs, etc.)

COMPUTATION / INFERENCE

(runtime behavior, prompt processing, context usage)

Risks	Blockchain's Role	Self-Assessment Opportunites
• Prompt injection and input manipulation • Use of user data outside approved scope • Lack of transparency in real-time decisions • Non-reproducible model behavior • Runtime vulnerabilities (e.g., jailbreaks)	• On-chain logging of inference events (privacy-preserving) • Policy enforcement via smart contracts • Selective data disclosure using 2k proofs • Proving that "data was NOT used" (negative disclosure proofs) • Runtime guardrails encoded as verifiable rules	• Prompt safety screens • Runtime privacy architecture • Adherence to data-sovereignty requirements • Hallucination-risk scoring mechanisms • Validate human-in-the-loop escalation paths

OUTPUT & ACTION

(generated results, decisions, predictions, automation)

Risks	Blockchain's Role	Self-Assessment Opportunites
• Harmful or inaccurate outputs • Unsafe automation based on faulty results • Copyright/IP misattribution • Lack of explainability • Weak accountability for downstream use	• Cryptographically verifiable output signatures • Traceability from output → model → training data • Smart-contract-based safety policies • Immutable audit logs for decisions & actions • Attribution tracking for copyrighted materials	• Accuracy & reliability metrics • Explainability and justification quality • Alignment with organizational policies • Validate that automation triggers comply with governance • Check for differential impacts across user groups

FEEDBACK, DRIFT & RETRAINING

Risks	Blockchain's Role	Self-Assessment Opportunites
• Model drift & performance decay • Feedback loops reinforcing bias • Shadow AI systems evolving without oversight • Lack of transparency in modification history	• Immutable ledger of all updates • Governance-driven "audit events" • Drift detection proofs (performance logs anchored to chain) • Verifiable model lineage across retraining cycles • Regulatory compliance-evidence submissions	• Retraining justification and criteria • Drift detection systems • Ensure governance process compliance • Validate periodic ethical and security assessments • Check tracking of human-centered & earth-centered metrics

Importantly, this framework avoids a simplistic view of "responsible vs. irresponsible" AI and instead emphasizes a layered value creation approach, where each step strengthens the overall system's reliability, sustainability, and alignment with human goals. Value in this context means the ability to achieve desired outcomes without unnecessary harm, excessive consumption of energy or compute resources, or reliance on low-quality or inappropriate data inputs.

Incorporating human-centered and earth-centered value creation is critical. These principles are not in opposition to enterprise or government priorities. Rather, they reinforce each other and serve as force multipliers when properly aligned. Yet in today's digital ecosystem, where individuals are represented as data profiles spanning thousands of parameters, significant risks arise when AI systems are trained primarily on synthetic data or when they retain uncorrected errors indefinitely (e.g., AI models cannot "forget" mistakes not identified as such). Much AI model training is outsourced, but without assurances of secure and trustworthy processes, organizations lack visibility into whether their models are built on authentic, ethically sourced information. The future of responsible AI depends on securely developed ground truths, using data that reflects real lived experiences and is anchored in verifiable provenance. Achieving this level of trust is not possible without robust web3 infrastructure.

Continued industry engagement can also help organizations ask the right questions about sustainability, ethical data sourcing, and the balance of inputs such as synthetic data, third-party datasets, and the minimum amount of certified ground-truth information required, ultimately validated through web3 mechanisms.

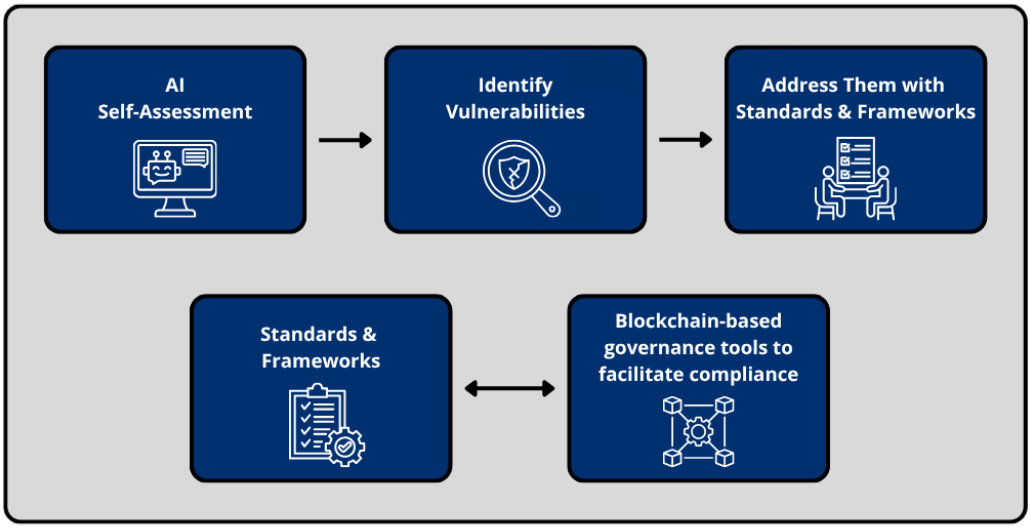
STANDARDS ALIGNMENT

Ensuring a future toward open-source and decentralized AI at scale requires a rigorous examination of existing standards and frameworks. While existing standards and frameworks for responsible AI do not generally call for blockchain explicitly, we recommend including an assessment of how they can be enhanced through blockchain technology. This involves identifying relevant AI standards and frameworks, and mapping them against decentralized solutions that strengthen provenance, auditability, governance, and verifiable compliance. Organizations can also make use of risk assessment tools, including the proposed Responsible AI Self-Assessment in Annex 1, and evaluate them against global responsibility standards using a process-driven perspective.

Key technology standards and frameworks to consider include:

- **ISO 42001** series, which provides a governance scaffold for managing AI responsibly
- **ISO 27001** to manage and protect information assets with Information Security Management Systems (ISMS)
- **W3C Verifiable Credentials**, which support trusted contributor and evaluator identity
- **C2PA credentials**, which authenticate public outputs
- **NIST AI Risk Management Framework** and **Generative AI Profile**, which translate risk concepts into operational controls
- **EU AI Act** and **GPAI Code of Practice**, which introduce legally enforceable requirements around provenance, copyright diligence, systemic-risk management, and transparency
- **The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Methodology**[10] for managing information security risks for both large and small organizations
- **EU General Data Protection Regulation (GDPR)**, which protects EU citizens' fundamental right to data privacy. It requires organizations to obtain individuals' consent before processing their data, granting individuals rights over their own personal data, including the right to access, correct, and delete it, often referred to as the "right to be forgotten."

This alignment effort also remains consistent with the broader regulatory and standards landscape discussed earlier. Each standards component has a function that can be cross-referenced to blockchain-based governance tools (e.g., ISO/IEC 42001 for AI management systems, NIST AI RMF and Generative AI Profile for operational risk controls, and EU AI Act/GPAI for data governance, disclosure, and systemic-risk expectations). The United Nations System White Paper on AI Governance[11], for instance, provides an analysis of the UN system's institutional models, functions, and existing international normative frameworks applicable to AI governance. Ultimately, the objective is to identify which types of evidence matters most and to illustrate how blockchain and Web3 technologies can make those evidence requirements durable, tamper-resistant, and testable.



In this context, the self-assessment serves as a bridge between conceptual guidance and the practical, day-one steps that any organization can take to embed responsible AI practices into its operations. Self-assessment tools facilitate identifying and addressing vulnerabilities in assets (e.g., hardware, software, IP) and people, in order to evaluate decision trees (e.g., was an unwanted outcome intentional or accidental?), and measure the impact of a given threat. With the Responsible AI Self-Assessment questionnaire, we hope to provide a meaningful first step that can toward transparent, private, secure, and reliable AI at scale, relying on web3-based governance mechanisms.

USE CASES FOR A FUTURE OF OPEN-SOURCE AND DECENTRALIZED AI

Two areas highlighted below, which can benefit from a future of responsible open-source and decentralized AI, are healthcare and education & workforce development.

HEALTHCARE

Healthcare examples can bring color the current concerns around responsible AI: when we don't have quality data inputs, reliability plummets. Especially when an AI model has little to no knowledge on what's happening to a physical being, learning from lived experience is hugely important. As a response, organizations such as the Coalition for Health AI (CHAI)[12] have emerged to help the industry establish responsible development, deployment, and oversight practices, recognizing that transparent, private, secure, and reliable AI models must learn from real lived experiences, beyond merely clinical records and synthetic datasets. Without a grounding on human experience, some models may deliver accuracy rates as low as 7%, which is especially concerning when lives are at stake. Historical examples like the nutritional "Food Pyramid," which had clear flaws, underscore the risks of suggestions and guidance that are based on weak or irrelevant data.

Today's digitization of health data, alongside the growth of data marketplaces, add new risks when the diversity of lived experiences that influence health outcomes is not captured into medical records. Open-source and decentralized AI models can help fill this gap by enabling individuals to contribute verified personal data while retaining control of their own data, with the added opportunity for economic incentives to sustain systems that truly reflect human diversity and lived experiences.

We reference a recent case where a man went blind after being prescribed GLP-1 medicines (e.g., Ozempic), illustrating serious adverse events tied to medications when certain medications interact differently across individuals. In this GLP-1/ Non-Arteritic Ischemic Optic Neuropathy (NAION) case, understanding a person's optic-disc size, a data point not found in standard health records, could dramatically change their risk calculation before starting a drug like Ozempic.

Therapies may fail to account for personal variation, leaving subsets of people exposed to serious side effects. The ensuing series of lawsuits[13] provide a reason for the next frontier in healthcare, with personal AI agents that act as digital fiduciaries for individuals. These agents would monitor evolving medical, scientific, and risk data in real-time and translate that data into personalized insights tailored to individuals' risks and benefits.

The traditional approach of waiting for slow scientific consensus or passive regulatory frameworks is no longer sufficient. Instead of "Ask your doctor first," open-source and decentralized AI allows a new paradigm of "Ask your agent first."

This underscores an opportunity for open-source and decentralized AI solutions to enable a major shift in healthcare approaches, evolving beyond medicine tailored to an average population, and instead focusing on approaches that are tailored to specific individuals. This can be made possible with a decentralized, privacy-preserving ecosystem where individuals own their data and receive meaningful, individualized support from intelligent systems built on verified ground truths.[14]

To achieve a future vision of personalized health intelligence,[15] AI and blockchain technology come together in a broader Web3 context to ensure data provenance, secure consent, decentralized identity, and mechanisms that allow individuals to benefit economically from sharing their data. Within this model, agents acting as digital fiduciaries can manage consent, privacy protections, and deliver personalized intelligence. A vision of digital health solutions, built much like a Waze model for traffic, with aggregated and anonymized lived experiences as inputs, would allow individuals to navigate complex medical decisions with tailored and context-specific guidance.

Open-source and decentralized AI solutions offer an unprecedented level of transparency, auditability, and adaptability to high-stakes medical environments, allowing clinicians and regulators to inspect how models work, validate their reasoning, and customize them for local needs. Decentralized architectures enable hospitals to run models locally, while preserving privacy complying with regulations, and supporting federated learning collaborations across institutions. Broadly shared goals like cancer detection or sepsis prediction can become shared tasks without sharing raw data.

- **Open-source frameworks can also strengthen public health research, decision support, integration of electronic health records, and even care delivery in multiple languages.**
- **Decentralized systems can enhance pharmaceutical R&D, supply-chain integrity, and surveillance of adverse drug events.**

Together, AI and blockchain technologies provide a foundation for a more equitable, interoperable, and trustworthy healthcare ecosystem. They minimize reliance on black-box systems, support global innovation, and ensure that AI remains aligned with human safety, individual context, and clinical reality.

OPEN SOURCE AND DECENTRALIZED AI FOR EDUCATION & WORKFORCE DEVELOPMENT

A future of open-source and decentralized AI at scale offers powerful benefits to education systems and the workforce by enabling transparent, equitable, and adaptable technology solutions to support diverse learning and labor environments.
For education and professional training, AI can scale personalized learning, which has proven to be the most effective (e.g., in person tutoring), in a way that adapts to each student's progress. Hyper-personalized education, once accessible only through private tutors, can now be scaled through AI. In an AI-driven world where students are already relying on tools like ChatGPT concerns have arisen around jumping from not knowing to having the answer without actually learning. The core challenge is that learning is a process that requires a necessary struggle. The solution is not to reject AI but to integrate it as a personalized guide through micro-struggles, helping students build understanding rather than merely produce answers.

- **Open-source models** can be inspected, customized, and aligned with local curricula and cultural contexts, helping educators ensure that AI-powered tutoring, grading systems, and content-generation tools operate without hidden bias and reflect institutional values.
- **Decentralized AI** reinforces privacy by allowing schools to run models locally, keeping student data on-site and ensure compliance with data protection and other laws.

These solutions can be especially transformative for expanding global access. Open-source models can be freely modified, translated, and deployed on low-resource devices, allowing underserved communities to benefit from solutions like AI tutors, literacy tools, STEM assistants, and vocational programs, even without reliable internet. This can reduce dependence on proprietary vendors and foster innovation through community collaboration on lesson plans, assessments, and specialized modules.

Moreover, students, who face pressure to prioritize grades in traditional systems, can be encouraged to shortcut learning with AI. In a future of open-source and decentralized AI, they increasingly need credentials with real utility, which provide proof of skills, which they can also control and share selectively. Soft skills like insight, communication, and emotional intelligence also become essential, as these cannot be replaced by AI.

In this context, educators must shift their goals from helping students pass tests to helping them internalize any given subject matter. Instead of treating AI as cheating, teachers can benefit from incorporating AI tools into assignments, requiring students to disclose prompts, validate outputs, and learn the strengths and limitations of these systems. Because AI often fabricates references or delivers inconsistent results across prompts, students must be taught how to critically evaluate these outputs rather than accept them as truth.

In the workforce, employers increasingly expect employees to use AI tools to be more effective, but foundational knowledge and insight remain irreplaceable. While AI surpasses humans in certain tasks (e.g., data retrieval, calculation, pattern recognition), wisdom remains uniquely human, grounded in experience, emotion, judgment, and context. As employers adopt AI broadly, they will hire and reward people for wisdom, creativity, and adaptability rather than brute information recall.

As for workforce development in particular, open-source and decentralized AI systems are essential for building transparent, fair tools for hiring, skills assessment, and workforce planning, while ensuring sensitive employee data remains within secure environments. These solutions can democratize reskilling by allowing workers to run AI-powered learning companions or career planning tools privately on personal devices. Open-source ecosystems allow employers, trade schools, unions, and public agencies to collaboratively develop training materials and interoperable skills frameworks that prepare the workforce for evolving themes such as cybersecurity, clean energy, advanced manufacturing, and AI engineering. These solutions reduce reliance on closed platforms, support accountable decision-making, expand access to learning, and protect worker and student autonomy.

With respect to the changing landscape of work, AI is rapidly transforming the economy by automating tasks across industries, changing the way employment will provide meaning, stability, and economic inclusion. As automation accelerates, societies must rethink what constitutes value, moving beyond "work equals value" toward models that include data, intelligence, and lived experience as legitimate economic contributions. This shift requires new policy frameworks, safety nets, and measurement systems that acknowledge that traditional labor cannot remain the sole foundation for income or mobility. Personal data, identity, and real-world experience will become increasingly important economically, with self-sovereign identity models where individuals can own their data and be rewarded for sharing it. Local organizations and governments, such as US states, are therefore faced with the need to invest in systems that help individuals retain agency and benefit from emerging value flows, to reduce the risk of being excluded from new economic incentive structures.[16]

Across education, employment, and economic policy, the central message is that open-source and decentralized AI—combined with thoughtful governance and new value frameworks—can create a future in which people are empowered rather than displaced, supported rather than surveilled, and able to thrive in a rapidly evolving digital landscape.

CONCLUSION: RECOMMENDATIONS FOR BLOCKCHAIN TO INCREASE TRANSPARENCY, PRIVACY, SECURITY, AND RELIABILITY OF AI

Industry self-assessment and customer assessments are important decision-making factors for engaging with AI services. In the journey toward increasing levels of open-source and decentralization at scale, which ultimately point toward reliability and governance, there is a need and a market for blockchain solutions in the AI space.

To bridge ideals of open-source and decentralized AI with enterprise and business reality, GSMI recommends a three-layer assurance architecture that uses blockchain alongside privacy-enhancing technologies (PETs). For instance, there's no reliable AI without blockchain being part of the provenance, making sure data going into AI models is reliable. The aim is not to "put everything on chain," but to anchor truth about the things that matter most: what was used, what changed, what happened, and who attested to it. Ultimately, the goal is for AI-driven informed decision making to increase in trustworthiness, toward positive outcomes for humanity and society as a whole. The interplay between AI and blockchain technology can, in this way, support the industrial and digital revolution taking place, in a responsible way.

Layer A: Provenance & Policy (Before You Ship)

- Establish a lineage registry for data, weights, prompts, and retrieval corpora, recording hashes, licenses, consents, and jurisdictional constraints.
- Use W3C Verifiable Credentials (VC 2.0) to identify and authorize contributors, evaluators, and auditors, with selective disclosure (e.g., SD-JWT/COSE) to minimize data exposure (e.g., considerations with respect to W3C VC 2.0; SD-JWT/COSE specs arise).
- Where copyright and licensing matters, bind license checks and opt-out/opt-in policies to artifacts before training or fine-tune

Layer B: Event-Driven Audit (As You Ship and Operate)

- Define audit events up front: model version changes; dataset, index, or safety-policy updates; system prompt or template modifications; and anomaly flags.
- For each event, emit a signed, time-stamped record whose commitment is anchored to a ledger, enabling independent replay of inference context (model identifier, policy bundle, retrieval set hash) without revealing personal data. Considerations arise with respect to event schema, anchoring approach, and privacy notes.

Layer C: Confidentiality & Authenticity (While You Communicate)

- Enforce purpose-bound access and consent using verifiable policies and PETs (TEEs, MPC, ZK; with FHE treated as an augment as standards mature).
- For external content, embed C2PA credentials and—where appropriate—anchor issuer attestations to provide a durable authenticity trail for downstream stakeholders.

EXAMPLE OPERATING MODELS

- Enterprise-hosted (self-managed). Maximum control over lineage, audit, and confidentiality; strongest fit for regulated workloads.
- Enterprise on open-weights (self-hosted). Prioritize supply-chain integrity (signed weights, tokenizers, loaders) and reproducibility.
- API-based (frontier third-party). Treat provider claims as attestations: require machine-readable statements on data handling, model updates, and incident response; bind them into your audit log and map to ISO/IEC 42001 and NIST controls (e.g., ISO/NIST clause mapping would be helpful). For EU exposure, incorporate GPAI Code of Practice commitments (e.g., considerations for code provisions arise).

What "good" looks like (outcomes over means):

- **Auditability:** measurable coverage of anchored lifecycle events; time to forensic replay (e.g. considerations for KPI ranges arise).
- **Data Control & Sovereignty:** proportion of inferences with license/consent-conformant inputs and selective disclosure.
- **Security & Privacy:** PET coverage, leak incidents, attested execution rates.
- **Reliability Under Change:** reproducibility rates, drift detection lead time, rollback success.
- **Governance & Compliance:** alignment with ISO/IEC 42001, NIST GenAI Profile, and EU GPAI expectations.

OPEN SOURCE & DECENTRALIZATION — OPEN QUESTIONS

1. **Minimum Provenance:** What minimum viable provenance (data, weights, prompts, retrievals) would make an organization comfortable for automating higher-stakes decisions?

2. **Placement of the Ledger:** Which audit events belong on-chain (or anchored) versus off-chain logs, and how should sensitive data and trade secrets be protected in each model?

3. **Open vs. Centralized Trade-offs:** Which "open" attributes (inspectability, reproducibility, verifiable contribution credits) deliver the most assurance even when hosting remains centralized?

4. **Decentralized Economics:** How should incentives reward quality of contributions (data cleanliness, red-team value, evaluation rigor) rather than mere activity?

5. **GPAI Readiness:** For entities exposed to the EU market, what evidence packages (model cards, safety evaluations, copyright diligence) will they prepare—and which commitments of the GPAI Code of Practice will they prioritize and adopt?

6. **Continuous Validation:** What cadence of drift testing, safety evaluation, and red-teaming is appropriate for your risk class, and how will results be anchored for audit?

ANNEX 1: RESPONSIBLE AI SELF ASSESSMENT QUESTIONNAIRE

A. PURPOSE

This questionnaire helps organizations assess the transparency, privacy & security, and reliability & governance of a specific AI system or use case. It is intended as a practical maturity check and input into risk management, not a formal audit.

B. HOW TO USE THIS QUESTIONNAIRE

1. **Scope**
   Complete the questionnaire for one AI system/use case at a time (e.g., "customer support chatbot", "credit risk model", "internal coding assistant").

2. **Response scale (for all scored questions)**
   For each question, select one:

   0 – Not in place / unknown
   No evidence, not implemented, or unknown.

   1 – Partially in place
   Implemented in some areas, informal, or incomplete.

   2 – Fully in place and documented
   Implemented, documented, and used consistently.

3. **Scoring**
   i. Each question is tagged to one of the three attributes:

   T = Transparency
   S = Security & Privacy
   R = Reliability & Governance

   ii. For each attribute:

   a. Add up the points for questions in that attribute.
   b. Calculate:

$$\text{Attribute score } (\%) = \frac{\text{points obtained}}{\text{maximum possible points (excluding N/A)}} \text{ x } 100$$

   iii. Interpret attribute scores as:

   0–39% = Low
   40–69% = Medium
   70–100% = High

4. **Overall evaluation (illustrative mapping)**

   Fair – No attribute is Low; at least one is Medium.
   Good – At least two attributes are High; none is Low.
   Great – All three attributes are High.

   Organizations may adjust thresholds and labels to fit their own risk appetite.

E. N/A answers

i. If a question is not applicable, mark N/A and exclude it from the maximum possible points for that attribute.

C. SECTION 0 – CONTEXT & CRITICALITY (NOT SCORED)

These questions provide context for interpreting the scores.

C1. System description
Briefly describe the AI system/use case (purpose, main users, and decisions it supports).

C2. Type of decision
Select the primary decision type:

- □ Advisory / decision support only
- □ Automated decision with human approval or override
- □ Fully automated decision with limited or no human intervention

C3. Potential impact of failure or misuse
What is the plausible worst case impact if the system fails or behaves incorrectly?

- □ Low – inconvenience, minor process inefficiencies
- □ Medium – financial or operational impact, reputational concerns
- □ High – impact on safety, rights, access to essential services, or legal exposure

C4. Data types involved (tick all that apply)

- □ Public / open data
- □ Internal non personal operational data
- □ Personal data
- □ Sensitive or special category personal data
- □ Children's data
- □ Trade secrets / highly confidential business data
- □ Other (describe): _____

D. SECTION 1 – TRANSPARENCY (T)

T1. Documented data sources
Training and operational data sources (including owners, licences, and collection methods) are documented.

0 / 1 / 2 / N/A

T2. Provenance & limitations
For each key dataset, provenance, known gaps, and limitations (e.g., coverage, demographic skew, time period) are identified and recorded.

0 / 1 / 2 / N/A

T3. Synthetic data use
The proportion and role of any synthetic data are known, justified, and tested so they do not materially distort real world performance.

0 / 1 / 2 / N/A

T4. Data quality management
There is a defined process to detect, track, and remediate data quality issues (e.g., missing, erroneous, outdated data) for both training and live data.

0 / 1 / 2 / N/A

T5. Performance across groups/contexts
Model performance is evaluated across relevant user groups or contexts, and material performance gaps are identified.

0 / 1 / 2 / N/A

T6. Fairness & bias measures
Fairness or bias metrics appropriate to the use case are defined, periodically measured, and action is taken when thresholds are breached.

0 / 1 / 2 / N/A

T7. Model assumptions & limitations
Key assumptions, intended use, and known limitations are documented in an artefact accessible to relevant technical and non technical stakeholders.

0 / 1 / 2 / N/A

T8. User transparency about AI use
Users or affected individuals are informed when AI is used in a way that meaningfully influences outcomes affecting them (e.g., decisions, recommendations).

0 / 1 / 2 / N/A

T9. Explainability & support
There is a clear, understandable explanation of how the system reaches outcomes (or why it cannot be fully explained) and how users can obtain support or clarification.

0 / 1 / 2 / N/A

E. SECTION 2 – SECURITY & PRIVACY (S)

S1. Security-by-design requirements
Security requirements specific to this AI system (including data, model, and infrastructure risks) are defined and integrated into design and architecture decisions.

0 / 1 / 2 / N/A

S2. Access control & logging
Access to models, training data, and configuration is restricted (e.g., role based access control) and administrator actions are logged and reviewed.

0 / 1 / 2 / N/A

S3. Protection of data in transit and at rest
Data used for training and inference is protected in transit and at rest (e.g., encryption, network segregation, key management).

0 / 1 / 2 / N/A

S4. Data protection compliance
The system's use of personal data complies with applicable data protection laws and internal policies (e.g., a DPIA or equivalent has been completed where needed).

0 / 1 / 2 / N/A

S5. Data minimisation & retention
Personal/sensitive data used for training and operation is minimised, and retention/deletion schedules are defined and implemented.

0 / 1 / 2 / N/A

S6. Data leakage controls
There are technical and procedural controls to prevent leakage of sensitive information via prompts, logs, model outputs, or third party providers.

0 / 1 / 2 / N/A

S7. AI specific threat mitigations
The system has been assessed for AI specific threats (e.g., prompt injection, model exfiltration, data poisoning), and appropriate mitigations are in place.

0 / 1 / 2 / N/A

S8. Patching & dependency management
Patching and vulnerability management covers AI related components (frameworks, libraries, model artefacts, dependencies) on a defined schedule.

0 / 1 / 2 / N/A

S9. AI incident response
There is a documented and tested incident response playbook covering AI related incidents (detection, triage, containment, communication, and learnings).

0 / 1 / 2 / N/A

F. SECTION 3 – RELIABILITY & GOVERNANCE (R)

R1. Pre deployment testing & validation
The model has been tested with representative data, including edge cases and stress tests, before deployment.

0 / 1 / 2 / N/A

R2. Defined performance targets
Baseline performance and quality metrics (e.g., accuracy, error rates, latency, business KPIs) are defined, agreed, and documented for this system.

0 / 1 / 2 / N/A

R3. Monitoring for drift and anomalies
The system is monitored in production for performance degradation, data drift, and anomalous or unsafe outputs.

0 / 1 / 2 / N/A

R4. Change & rollback process
There is a defined process for updating, retraining, and rolling back models and associated data pipelines, including approval steps and testing.

0 / 1 / 2 / N/A

R5. Human oversight for higher risk decisions
For higher impact use cases, appropriate human oversight is in place (e.g., human in the loop or human on the loop) with clearly defined roles and decision rights.

0 / 1 / 2 / N/A

R6. Ability to challenge or appeal
Users or affected individuals can challenge or request review of AI influenced decisions, and such cases are tracked and analysed.

0 / 1 / 2 / N/A

GBBC
Global Blockchain
Business Council

DECENTRALIZED FINANCE (DEFI) REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 6.0

DEFI GOVERNANCE: SETTING THE PATH FOR FUTURE GROWTH

GBBC GSMI 6.0

ACKNOWLEDGEMENTS

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

Joseph Cutler - CO-CHAIR
Partner, Perkins Coie

Hedi Navazan - CO-CHAIR
Chief Compliance Officer, 1inch

Lee Schneider - CO-CHAIR
General Counsel, Ava Labs

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

I) INTRODUCTION

Decentralized finance (DeFi) is emerging as one of the most transformative innovations for financial infrastructure, introducing new ways for individuals and institutions to transact, allocate capital, and coordinate economic activity without relying on traditional intermediaries. Built on open, programmable, and globally accessible blockchain networks, DeFi enables markets for financial services like lending, trading, payments, and asset management through code and automated, decentralized operations.

As the DeFi ecosystem matures, governance, both external via regulatory frameworks and internal via DAOs and protocol-level mechanisms, is a decisive factor shaping whether DeFi can evolve into a secure, scalable, and institutionally trusted financial system.

This paper covers the most important considerations for DeFi governance, drawing largely on selected submissions to the US Securities and Exchange Commission (SEC) Crypto Task Force's request for inputs[17] regarding the application of federal securities laws to blockchain and digital assets – specifically submissions that provide recommendations relevant for the DeFi ecosystem.

Regulatory Governance: Ideally, a globally harmonized and technology-neutral approach would allow blockchain innovation to flourish without requiring bespoke regulation for every new use case. For DeFi, and related activities such as tokenization, this means that compliance could be achieved under updated, but familiar, frameworks. This would reduce friction, encourage adoption, and support integration of Web3 with traditional finance. It would also support fairness and avoid regulatory arbitrage. For this section, we largely focus on insights from selected questions relevant for DeFi from US SEC Commissioner Hester Peirce's statement "There Must be Some Way Out of Here."[18] While some of these insights cover the US regulatory framework, many of the concepts are relevant globally, especially as DeFi operates on global liquidity pools by nature, and US regulations often influence those of other jurisdictions.

DAO Governance: Decentralized governance mechanisms remain among the least understood and most critical dimensions of DeFi. They distribute decision making across token holders, smart contracts, and global communities, creating new forms of coordination but also new vulnerabilities. This section covers how decentralized protocols and DAOs currently exercise governance, and how governance must adapt for protocols to remain decentralized while operating safely within legal and economic realities. We draw comparisons between decentralized and traditional corporate governance, identifying gaps where DAOs can adapt to provide equivalent accountability, risk controls, and investor protections.

Ultimately, effective DeFi governance, both on-chain and off-chain, is essential for transforming the evolving collection of open-source protocols into a resilient, legitimate, and globally interoperable financial ecosystem. Without thoughtful governance, DeFi risks remaining fragmented and fragile. On the other hand, with thoughtful governance structures, DeFi has the potential to reshape financial markets, expand global access to capital, and enable an open, programmable financial system for the long term.

II) WHY DEFI GOVERNANCE

What is the purpose of governance? It is crucial to ask this question before setting a governance model for any DeFi protocol. Because governance ensures legitimacy, accountability, and user trust in decentralized networks, it is essential for user retention, institutional adoption, and long-term stability. The exact format of governance likely looks different for different DeFi protocols, for which decentralized autonomous organizations (DAOs) are generally set up to carry out decision making, with no centralized party in control.

DeFi governance is important because it determines who controls financial infrastructure, how risks are managed, how value is allocated, and whether the ecosystem can scale responsibly. Governance matters at multiple layers: protocol governance, often via DAOs, user and community governance, and external governance through regulation. Each element plays a distinct role, and together they shape whether DeFi becomes a reliable, safe, and widely adopted financial system or remains fragmented, fragile, or vulnerable to abuse.

DeFi governance, whether it is carried out by DAOs, developers, communities, or regulators, is essential because it ensures that decentralization is genuine rather than superficial, preserving the core principles of distributed control. It manages risk and protects users in a permissionless environment where anyone can participate and where safeguards must be built into the system itself. Governance also allocates capital and oversees powerful financial infrastructure, determining how resources are deployed and how protocols evolve. It enables sustainable innovation by providing structured mechanisms for upgrades, improvements, and adaptation over time. Effective governance builds institutional and regulatory trust, making it easier for traditional financial actors to participate. It prevents the concentration of power and mitigates systemic vulnerabilities that could undermine the ecosystem. Ultimately, governance shapes the fairness, transparency, and legitimacy of the entire DeFi landscape.

In essence, governance is what transforms DeFi from a set of smart contracts into a functional, resilient, and credible financial system. Without governance—whether internal or external—DeFi cannot scale safely, attract mainstream adoption, or fulfill its promise of open, decentralized financial services.

Governance in DeFi is also closely connected to the broader ecosystem through social, technical, economic, and inter-protocol dynamics. Even in decentralized systems, social governance and community norms play a critical role: reputation, informal expectations, and off-chain coordination influence how contributors behave, how disputes are resolved, and how protocols evolve, helping maintain order where formal rules may be limited. Technical governance also shapes protocol behavior through code-based mechanisms such as time locks, upgradeability modules, fee switches, and circuit breakers; these embedded rules determine power dynamics, decentralization, and system resilience even in the absence of human voting. Economic and incentive governance adds another layer, as token distributions, rewards, liquidity incentives, and staking structures determine participation, alignment, and potential vulnerabilities—poorly designed incentives can lead to plutocracy, voter apathy, or manipulation, while well-designed systems encourage fairness and sustainable engagement. Finally, because DeFi protocols are deeply interconnected and composable, governance decisions in one protocol can have cascading effects on others—for example, lending markets rely on price oracles, and DEX liquidity tokens feed into vault strategies. For this reason, governance must be considered not only at the individual DAO level but across the broader ecosystem, where interdependencies create shared risks and collective responsibilities.

III) CONSIDERATIONS FOR DEFI GOVERNANCE

Below is a set of considerations that are fundamental for DeFi governance. Many of these are represented in the SEC RFI submissions for regulatory consideration, as reflected in the context of the questions below. It is important to note that considerations for DeFi governance go significantly beyond the securities classification rhetoric that has been so often raised (e.g., other issues include treasury, custody, financial regulation, money transmission, trusts, banking, AML/KYC controls). These issues have simply not been as actively focused on in legal enforcement actions. While falling within a "securities" designation may determine the jurisdiction of US regulation, there is a wide range of additional; themes that must be dealt with for DeFi governance.

3.1) REGULATORY CLASSIFICATION & SECURITY STATUS

Transactions: The nature of a transaction and distinction of purpose matter greatly for classification. For example, if a developer sells tokens they created and uses the proceeds to build a project that increases the token's value (e.g., ICOs), the arrangement fits the Howey test and is considered an investment contract. By contrast, a native blockchain token (e.g., XRP, Filecoin) may function primarily as a medium of exchange or access right, leading to the argument that these tokens are not securities, even if certain institutional sales of them might constitute securities transactions. Drawing on the experience of Ripple, programmatic sales considered as a commodities transaction are distinct from secondary sales on crypto exchanges, with the main difference being funds going directly to the founders or not. Institutional sales were originally by founders, designed fund builders to build infrastructure The argument is that XRP, as a native DLT token, is never a security.

Tokens: Yet regulators should not fixate solely on the transactional structure at the expense of recognizing the nature of the underlying asset.[19] If a token represents intellectual property, it should be treated accordingly; if it represents a commodity such as gold, it should be regulated as such, without unnecessary legal gymnastics. Moreover, securities transactions can involve non-securities, making it crucial to distinguish between the token itself and the underlying asset it may reference or represent. The goal is to create a rational framework where tokens are classified according to what they represent, rather than relying on rigid or overly prescriptive rules. This approach would help regulators account for the diverse roles tokens play while improving legal clarity for DeFi and broader digital-asset markets.

When it comes to tokens, it is important to consider differentiating "Protocol Tokens," that is, Digital Native Assets from Traditional Securities. Thus, tokens that represent classic securities on a blockchain should inherit the corresponding protections and regulatory responsibilities. Others, considered native tokens, may warrant different treatment. This differentiation helps preserve investor protections where needed, while avoiding over-regulating fundamental blockchain infrastructure.

DeFi may interact with both kinds of tokens. If regulators accept a distinct "protocol token" category, it would lower legal risk for many DeFi and blockchain projects, reducing uncertainty for builders, users, and investors, and ultimately enable broader innovation without immediate securities law constraints. Moreover, Perkins Coie's second submission to the SEC calls for the adoption of a workable taxonomy that remains merit- and technology-neutral.[20]

- **As an alternative to forcing protocol tokens into existing securities laws, the Ava Labs submission to the SEC proposes a rulemaking framework, with a new exemption for tailored disclosures, AML/KYC, and filing requirements.[21]**
- **Perkins Coie's first submission to the SEC also acknowledges that tokenized securities should be treated as traditional securities.[22]**

The Sidley Austin submission to the SEC representing Owl Explains powered by Ava Labs presents 5 categories that represent the vast majority of tokens, for an asset-based test[23]:

1) Asset token	Physical representation of something physical that is recorded on a blockchain
2) Service token	Digital representation of services (e.g., accounting services, legal services, streaming)
3) Intangible asset token	While other existing regimes already define intangible assets (e.g., accounting term), such as money transfer licenses that require maintaining a net worth, it is important to consider how this applies to crypto companies with assets in the form of digital assets? There can be a gap when cryptocurrencies, for instance, are classified as intangible assets when the majority of US of states don't count intangible assets as net worth. Yet these companies may have substantial balance sheets, which are represented inaccurately as very small when deducting cryptocurrency holdings
4) Native DLT token	This is an avenue to get out of the gap illustrated above, relevant for most Layer 1 blockchains, with tokens as bundles of rights
5) Stablecoins	Retain a stable value against an underlying reference

Lending Activities: Finally, because many DeFi protocols provide lending services, it is important to consider when a loan may or may not be classified as a security. Traditionally, loans are treated as securities, especially in retail contexts, when the funds lent belong to someone other than the lender: particularly banks reloaning customer deposits. DeFi challenges this model because lending is often peer-to-peer and involves individuals loaning their own funds directly to counterparties through smart contracts, thus removing the intermediary relationship that historically triggered securities concerns.

3.2) DECENTRALIZATION & CONTROL

As regulators and market participants evaluate DeFi systems, it is essential to consider carefully what decentralization means, how it is implemented, and where meaningful control actually resides. The mere existence of non-centralized swapping software or partially decentralized functions does not automatically make a system "DeFi." Many entities in the blockchain space remain centralized in practice and may not be leveraging blockchain technology as originally intended, or may not clearly explain their role when referring to decentralized operations.

With an initial focus on tokenized securities rather than blockchain native digital assets, smart contract automation and programmatic controls can assume roles traditionally filled by centralized transfer agents. This suggests that decentralized technical operations could be recognized as legitimate within securities law frameworks.[24]

Yet while U.S. securities law is built around concepts of control and reliance on managerial efforts, decentralization fundamentally alters this approach by reducing or eliminating reliance on a managerial team under the Howey test.[25] Many networks evolve into autonomous systems where upgrades, governance, and growth are not directed by a single promoter. This calls for a regulatory framework that distinguishes between tokens tied to entrepreneurial oversight and tokens embedded in decentralized protocols where no identifiable party "controls" the system. Decentralization changes the regulatory approach required because the foundational elements of securities analysis (e.g., control, managerial reliance, and information asymmetry) manifest themselves differently in blockchain networks, if at all.

When it comes to novel issues raised by blockchain-based solutions, regulators should recognize that where no central party exercises meaningful control, securities obligations may need be reduced or eliminated. For example, protocol tokens used for staking, validation, transaction fees, or governance should not be treated as securities because their value derives from network functionality rather than managerial promises.[26] The transparency and automation of on-chain systems, which operate through open source, non-custodial mechanisms, differs fundamentally from intermediated securities markets.[27] This transparency lowers information asymmetry and enables new forms of self-governance.

3.3) WHO NEEDS TO BE A REGULATED ENTITY

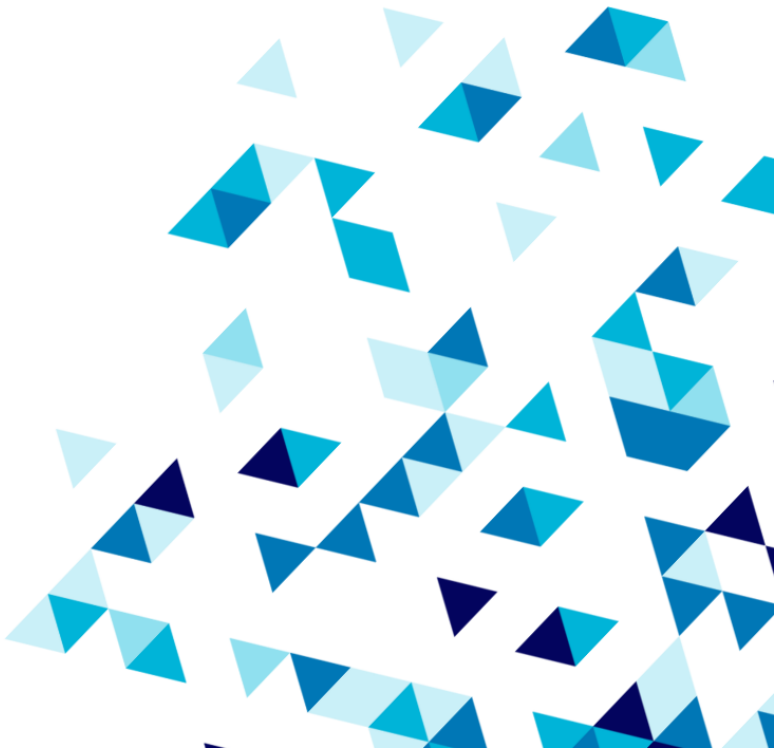
When assessing which actors in the blockchain and digital assets ecosystem should be regulated, a key principle arises: regulate the activities or intermediaries performing traditional financial functions, not the underlying protocol or token itself. Overall, regulation should follow the function, not the technology.

Under this principle, protocol-level actors (e.g., developers, validators, token holders, sequencers, smart contract deployers, DAO participants) should not be treated as regulated entities simply by virtue of interacting with a blockchain.[28] Protocol participants performing automated or mechanical roles should generally fall outside regulated classifications unless they act like traditional intermediaries. Moreover, actors involved in network operations (e.g., miners, validators) should not be treated as regulated entities because they do not exercise discretionary control or perform managerial actions on behalf of investors.[29]

Instead, regulation should focus on centralized intermediaries (e.g., exchanges, custodians, broker-dealers) and on actors who take on fiduciary or custodial roles (e.g., holding customer assets, making recommendations, running order books, soliciting investments). [Sec]When tokenized securities are issued, the issuer, transfer agent, broker-dealer, and custodian must follow existing securities rules, but the underlying blockchain infrastructure or smart contracts enabling fund transfers would not themselves become regulated financial entities.[30]

For the purposes of trading, regimes for exchanges (e.g., US ATS regimes) can be adapted for crypto trading platforms only when they perform functions equivalent to those performed by traditional exchanges.[31] Yet non-custodial and smart contract-based trading protocols should not automatically be treated as regulated entities. There remains a need for greater clarity and distinguishing the following roles:

- Centralized exchanges
- Smart contract protocols
- Front-end operators
- Network validators



3.4) MARKET FRAGMENTATION

Blockchain infrastructure is inherently token agnostic. As long as a token has compatible security and interoperability, it can trade. As open marketplaces are evolving to reinstitute the benefits of previous barter systems, market fragmentation is an important concern. This requires a system where digital assets, both blockchain native tokens and tokenized securities, can trade, settle, and be custodied across interoperable ecosystems to maintain market integrity and efficiency.

However, the current regulatory environment poses several challenges that have led to fractured liquidity, siloed markets, and eventually traders moving their activities offshore.[32] For instance:

- Digital asset exchanges cannot register or pursue licenses in harmonized ways
- Tokenized assets cannot seamlessly trade alongside blockchain native digital assets
- Inconsistent state and federal rules raise questions

Fragmentation is a negative outcome of regulatory uncertainty and incompatible frameworks. Without adequate regulatory developments, markets will continue to experience fragmentation in ways that hinder price discovery, increase market manipulation risks, and undermine U.S. competitiveness in capital formation involving digital assets. For instance, market fragmentation is concerning when tokenized securities are forced to trade within isolated permissioned ecosystems due to regulatory challenges, rather than circulating and settling on public blockchains. This fractures liquidity and prevents interoperability across trading venues. Fragmentation can also arise from a lack of taxonomy and inconsistent treatment of tokens, which leads to uncertainty and market bifurcation.[33]

In this context, rules recognizing public chains as acceptable settlement rails would reduce fragmentation between tokenized securities markets and broader crypto liquidity.[34] Moreover, a unified taxonomy would help courts and regulators reach consistent conclusions, increasing predictability and reducing both geographic and functional fragmentation of crypto networks. It would also be helpful to distinguish between protocol tokens and securities, to reduce the risk of innovation splitting between jurisdictions and between “compliant” and “grey market” ecosystems.[35]

3.5) ROLE OF PROPERTY & PRIVATE LAW

Private law (e.g., property law, commercial law, and contract law) is foundational for DeFi, providing the underlying reasoning to conceptualize digital assets and related activities. Private law concepts (e.g., possession, transfer, beneficial ownership) as essential for regulatory clarity. Moreover, the focus on transparency, private key control, and ledger verifiability for governance echoes private law notions of possession and ownership.[36] Notably, property law is central to the vision of blockchain systems, which seek to "rewire" traditional financial norms, reduce frictions inherent in monetary intermediation, and enable fractional, in-kind forms of ownership and exchange.For example, the following digital assets and related activities can be approached from a private law lens:

- Protocol tokens can be treated as property rather than securities. Specifically, protocol tokens can be characterized as intangible personal property rather than contractual claims.[37] These tokens do not create a legal relationship between the holder and an issuer but instead function as commercially fungible digital property within a network, strengthening the argument that such tokens fall outside the scope of securities law.
- Tokenized securities can be seen as digitally represented property rights.[38] Specifically, tokenized securities representing traditional property rights, such as equity ownership or debt claims, are simply recorded and transferred using blockchain technology.
- Blockchain ledgers can be interpreted to function as property registries.
- Smart contracts can be considered to implement property law concepts (e.g., transfer restrictions, beneficial ownership rules, creditor priorities)
- In the context of historical SEC positions on mining and in-protocol rewards, it can be noted that these rewards stem from the use of personal property (e.g., computing resources or staked assets) rather than from reliance on a common enterprise.[39]

This suggests that securities regulation may operate alongside, rather than override, private law principles. Thus, securities regulation can be better suited to integrate with, rather than displace, the underlying property law framework that can give digital assets legal meaning.

Yet private law remains underdeveloped when it comes to clarity for digital assets and related activities. Private law emerges as a critical missing piece for DeFi and key themes like tokenization. While tokens can represent rights to real-world assets (RWAs), most jurisdictions lack clear property law that recognizes tokenized ownership. At best, holders may have contract rights, which are enforceable but less robust and transferable than property rights. For example, tokenized real estate might contractually promise ownership, but without statutory backing (such as Article 12 amendments in the U.S. or new UK proposals), the claim is limited.

Moreover, many unresolved issues arise when attempting to ground digital asset taxonomies in private law. Tokenized real-world assets (RWAs) in particular highlight this gap. While contract law can specify that a token represents an asset, contract rights are weaker and less transferable than property rights. Contractual claims may allow damages for breach but do not provide the clarity or enforceability expected of ownership. In many jurisdictions, private law has not fully adapted to support tokenized property claims. Thus, RWA tokenization often relies on imperfect contract structures rather than robust property rights, limiting scalability and legal certainty.

As potential avenues for future steps, ongoing efforts are developing principles to harmonize private law treatment of digital assets (e.g., focused on decentralized trading and tokenized carbon credits). These initiatives recognize that private law must evolve for DeFi and areas like tokenization to achieve its potential, even though certain structural concerns (e.g., bankruptcy treatment with digital assets) may add further complexity. Still, the legal system needs frameworks analogous to the invention of deeds for real estate to support digital property. Until private law catches up with these innovations, DeFi innovation will continue to face legal constraints that hinder the ability to deliver the frictionless ownership transfer that the technology promises. Below are examples of initiatives to set key principles to harmonize private law around digital assets and related activities:

- The International Institute for the Unification of Private Law (UNIDROIT)[40], with the *UNIDROIT Principles on Digital Assets and Private Law*,[41] aims to provide clarity to facilitate transactions with digital assets for activities including control and transfer, custody, secured transactions, procedural law including enforcement, and insolvency.
- Uniform Law Commission (ULC) has developed a legal framework for digital assets through amendments to the Uniform Commercial Code (UCC), allowing the use of digital assets as collateral and ensuring their control can be established similarly to traditional property. These amendments include a new Article 12 for Controllable Electronic Records (CERs) and revisions to Article 9 for secured transactions.

3.6) ROLE OF INTERMEDIARIES

Whether DeFi protocols, or any elements of protocols (e.g., DEXes), should be treated as intermediaries, is fundamental. While traditional intermediaries formalize their relationships through contracts, DeFi often relies on code and user behavior to create implicit arrangements.

Principle suggests that regulators should not target the underlying technology but rather the applications and business activities built on top of it. Writing or deploying code should not, by itself, expose someone to liability, just as paving a road does not make one responsible for speeding drivers crashing into each other. For instance, from a purely technical standpoint, a DEX is simply software that enables peer-to-peer transactions.

However, if a DEX facilitates the trading of securities without identifying counterparties, the DEX's legal status becomes more complex, requiring clearer definitions. Moreover, if a DEX operator, or any identifiable party, earns revenue from providing trading access, collecting fees, or packaging data, that entity may be functioning as an intermediary and could reasonably fall within a regulatory perimeter. If a DEX generates trading fees, whoever receives those fees is more likely to be treated as a regulated actor. This concept can be in some way analogous to distinguishing royalties, where a creator earns income from future sales of an asset, from securities transactions, where income flows from the rising value of an investment or from facilitating trades.

Investor protections and market integrity remain essential priorities. While DeFi protocols improves capital market efficiency by reducing frictions, the challenge lies in protecting users when no centralized gatekeeper exists. A critical distinction to consider is between the technology itself and the business model that may form around it. Ultimately, determining whether a DeFi such as a DEX is an intermediary requires separating the technology from the business conducted through it and assessing who, if anyone, exercises meaningful control or benefits financially from the platform's operation.

3.7) SMART CONTRACTS & AUTOMATION

In the DeFi ecosystem, smart contracts consistently execute predefined actions, and participants interact with them in predictable ways that resemble contractual performance. This raises the question of whether and how these informal interactions driven by code should be interpreted in legal terms. A key theme for DeFi regulation is whether smart contracts themselves should be treated as brokers or other regulated intermediaries simply because they execute order routing or transactional functions.

The consensus in many emerging legal and policy discussions is that smart contracts should not be regulated as entities, but rather audited to ensure they perform as intended. Regulating technology directly is problematic: a smart contract is fundamentally a tool, much like written contracts or software systems, not a market participant. In traditional finance, a written contract is not regulated but governs a regulated activity, such as the issuance or trading of a bond. With this principle, a bond should be treated as a bond regardless of whether it trades through paper certificates or blockchain rails. Smart contracts should not be presumed to be legal contracts purely because they automate actions that resemble contractual activities.

This distinction raises aspects of the long-standing "code vs. law" debate in the space. The definition of a legally binding contract in the traditional sense requires it to have: 1) an offer (contract presents itself as such), 2) an exchange of consideration (e.g., exchange of value), and 3) performance (e.g., a user). Some state laws have begun to recognize that if a smart contract functions in a manner consistent with these principles, it may be given legal effect. However, smart contracts do not always involve two identifiable parties, a clear offer, or an explicit exchange of consideration. Code by itself does not constitute an offer; rather, legal enforceability depends on the surrounding context and whether the parties clearly manifested the intent to enter into a binding arrangement.

Therefore, a smart contract does not automatically qualify as a legally binding contract. A better regulatory may instead lie in assessing the activities facilitated by smart contracts (e.g., such as issuance, trading, custodial functions) rather than treating the technological mechanism as the regulated actor.

3.8) SECURITY & PRIVACY

KYC requirements remain outdated, and many current practices amount to performative compliance rather than meaningful risk mitigation. Decoupling KYC from AML is an important conceptual shift that can be beneficial for DeFi security, recognizing that identifying attempts to launder money is far more effective than simply knowing a user's name. From this lens, KYC can be seen as only one component of a broader risk assessment framework that incorporates blockchain analytics, behavioral monitoring, and protocol-level safeguards. AML in particular also needs to develop in effectiveness and sophistication.

Moreover, as institutions look to participate in the DeFi ecosystem, they seek models that preserve user privacy while still enabling compliance. This raises questions about whether whitelisting, selective disclosures, or more advanced systems (e.g., such as self-determined KYC/AML attestations) may be better suited for decentralized environments. A user could, for example, cryptographically prove they are not a sanctioned or high-risk individual without revealing their full identity. A global or interoperable identity verification system, conceptually similar to Global Entry or CLEAR systems for global travel, could allow wallets to display a "green check" confirming AML/KYC compliance while preserving anonymity. This way, instead of stating "metamask put xyz user through a KYC process," a DeFi protocol can add a verification that xyz user is cleared. Law enforcement would be on board because if there is a suspicious transaction, authorities would have access to the KYC data. self-determinative KYC/AML verification systems allow protocol users to self-attest to non-launderer status and retain ownership and control over their personal data.

These considerations go hand in hand with emerging developments in privacy technology (e.g., particularly zero-knowledge proofs, decentralized identity, and self-sovereign identity principles), which must evolve to keep pace with DeFi's growth. DeFi already incorporates sophisticated RegTech solutions, and future protocols are expected to increasingly embed compliance directly at the protocol layer rather than outsourcing it to centralized intermediaries. Under such a model, users would undergo verification through a trusted third party, and the protocol would only receive confirmation that the user is cleared, not their personal data. Law enforcement would also retain access to underlying information in the event of suspicious activity, while the overall system would preserve user privacy. Ultimately, more effective AML frameworks, privacy-preserving verification tools, and integrated RegTech solutions are fundamental for DeFi to remain decentralized and privacy-respecting, ensuring a "clean DeFi" future that operates cooperatively within global financial crime obligations.

IV) REGULATORY GOVERNANCE FOR DEFI

From a regulatory standpoint, effective governance is crucial because first, legal clarity reduces uncertainty and builds market confidence. Regulatory frameworks provide clarity on which activities are permitted, which tokens are securities, how custody should work, and what standards apply to trading and settlement. Without this clarity, developers and investors often limit participation, build offshore, or avoid the U.S. market entirely. Regulation, if well designed carefully, can enable DeFi growth by reducing legal risk. Moreover, regulatory clarity protects users while preserving innovation. Regulation establishes guardrails to prevent fraud, market manipulation, and systemic risk, all of which can undermine trust in DeFi ecosystems. Good regulation can coexist with decentralization: for example, recognizing self-custody, using on-chain transparency for compliance, or applying tailored rules for smart-contract-based trading platforms. Ultimately, effective regulation enables institutional participation (e.g., funds, custodians, asset managers, and banks). Institutions cannot meaningfully participate in DeFi without regulatory clarity. Tailored custody rules, tokenization frameworks, KYC/AML standards, and clear classification rules make it possible for institutions to interact directly with DeFi protocols, bringing liquidity, stability, and legitimacy.

4.1) SEC REGULATORY QUESTIONS & RELEVANCE FOR DEFI

Under U.S. securities laws, transactions involving securities or investment contracts must be handled by a registered broker-dealer. This requirement stems from the 1930s, when widespread securities fraud, often involving paper certificates stolen from unsuspecting retail investors, led to mandates requiring intermediaries as gatekeepers to protect market participants. As a result, the current legal framework does not accommodate for securities transactions occurring in a peer-to-peer manner. Securities laws were created to require the use of registered broker-dealers. Yet in distributed ledger technology (DLT), transactions are transparent, auditable, and resistant to the types of fraud that prompted existing rules. The law has not yet caught up to reflect these advances.

In this context, US SEC Commissioner Hester Peirce released a statement with the SEC Crypto Task Force Request for Information titled "There Must be Some Way Out of Here"[42], posing questions to set the stage for regulatory developments for blockchain and digital assets. While not every one of the 48 questions is equally applicable for DeFi,[43] below is a selection and assessment of those questions that are most highly relevant to DeFi's growth and governance.

The selected questions cover issues that can determine how DeFi protocols can operate, how users can interact with them, and whether these systems are lawful under existing securities laws. Many touch directly upon DeFi's foundations and where regulation must strike the right balance between innovation and investor protection. Addressing these questions for DeFi will influence everything from architecture and governance to market access and institutional participation. We highlight the importance of these questions for the DeFi ecosystem especially because regulatory clarity:

- Reduces regulatory risk, enabling developers, users, and investors to operate with more confidence.
- Encourages adoption through regulatory legitimacy for DeFi. if policymakers recognize certain tokens or activities as non-securities or create bespoke regimes for them, mainstream financial institutions and retail users will be more willing to participate.
- Unlocks innovation, where tailored frameworks like safe harbors, sandboxes, and rules specific to smart contracts and custody for DeFi can provide builders with room to experiment without fear of enforcement.
- Adds predictability to governance and decentralization, allowing DeFi to operate in both a compliant and decentralized way.
- Helps bridge DeFi with traditional finance, through updated rules for tokenized securities, custody, atomic settlement, and exchange requirements. This is key for interoperability, institutional capital inflows, and the long-term viability of DeFi infrastructure.

4.2) SELECTED DEFI QUESTIONS

SECURITY STATUS QUESTIONS

Q1: What type of regulatory taxonomy would provide a predictable, legally precise, and economically rational approach to determining the security status of crypto assets and transactions in such assets without undermining settled approaches for evaluating the security status of non-crypto assets and transactions?

Relevance for DeFi

A clear and predictable taxonomy for digital assets is foundational to the growth and governance of DeFi. It determines whether governance tokens, LP tokens, vault tokens, staking tokens, stablecoins, wrapped tokens, NFTs, and other DeFi primitives are considered "securities," which in turn dictates the regulatory obligations that apply. Because DeFi encompasses a wide spectrum of token types with different purposes and technical functions, uncertainty around classification exposes projects, users, and investors to significant legal risks. This uncertainty discourages institutional participation, complicates DAO governance design, and can cause builders to delay or halt development for fear of retroactive enforcement.

Clarity in classification is also important for tokens that fall outside traditional investment frameworks (e.g., stablecoins, wrapped assets). DeFi's composability relies on the reliable interaction of many token types across protocols. Taxonomy also matters for staking and network participation tokens, which are central to many DeFi protocols. If these tokens are to be treated as securities, common DeFi mechanisms such as staking, liquid staking, and governance-based coordination could become impractical or subject to burdensome compliance requirements. Taxonomy ultimately points to regulatory clarity for token functionality and security status, providing the certainty developers, users, and institutions need to confidently build, use, and scale DeFi systems.

Q3: Certain crypto assets are used in a variety of functions inherent to the operation of a blockchain network, such as mining or staking as part of a consensus mechanism or securing the network, validating transactions or other related activities on the network, and paying transaction or other fees on the network. These technology functions may be conducted directly or indirectly, such as through third-party service providers.

What types of technology functions are inherent to the operation of a blockchain network? Should the Commission address the status of technology functions under the federal securities laws and, if so, what issues should be addressed?

Relevance for DeFi

DeFi relies heavily on blockchain-native functions such as staking, gas payments, validator rewards, and governance mechanisms tied directly to protocol operations. Tokens that serve these functions (e.g., paying transaction fees, securing consensus, incentivizing validators, sequencers, or relayers, and enabling governance participation) are foundational to the operation of L1s, L2s, and rollups. On the one hand, if these network function tokens are to be characterized as securities, core infrastructure providers would fall under securities regulation, fundamentally altering how DeFi protocols reward validators, design staking-based governance, or structure yield products built on staking and gas tokens. Because many DeFi protocols rely on staking and liquid staking derivatives to secure networks and generate yield, the regulatory status of these assets is crucial. If staking or liquid staking tokens are deemed to be securities, DeFi platforms may face registration requirements and compliance burdens that could undermine existing consensus and yield models. On the other hand, if these tokens are recognized as non-securities, this would legitimize the foundational economic mechanisms of blockchain networks under U.S. law, providing regulatory certainty that could encourage broader adoption, institutional participation, and continued innovation in DeFi infrastructure.

Q4: Users of liquid staking applications receive a so-called "liquid staking token." This token represents their staked crypto asset, and the token can be used in other activities, all while continuing to participate in the proof-of-stake protocol. Should the Commission address the status of liquid staking tokens under the federal securities laws, and, if so, what issues should it address?

Relevance for DeFi
Liquid staking tokens (LSTs) (e.g., stETH, cbETH, etc.) are deeply integrated into DeFi as forms of collateral, Liquidity Provider tokens (LP shares), and yield-bearing assets. Their treatment as securities or non-securities will directly impact lending, leverage, and risk management across DeFi. For governance, DAOs that issue or rely on LSTs need regulatory clarity for the design of safe policies around collateralization, rehypothecation, and systemic risk.

Q5: Should the security status of certain categories of crypto assets be addressed, such as stablecoins, wrapped tokens, and NFTs?

Relevance for DeFi
Stablecoins and wrapped tokens are core building blocks of DeFi liquidity, collateral, and cross-chain composability. Their security status would shape a variety of key issues, from DEX trading pairs to money market design. Governance of DeFi protocols must account for whether these assets carry securities style constraints, particularly in cases wrapped, bridged, or synthetic assets are used as governance or collateral tokens.

PUBLIC OFFERINGS QUESTIONS

Q8: Should the Commission develop tailored disclosure requirements for offerings or classes of specific categories of crypto assets? What types of disclosures would be important for investor protection? Should disclosure occur both at the time of sale and on an ongoing basis? If so, what information should the ongoing disclosure contain and how should that disclosure occur?

Relevance for DeFi
Tailored disclosures could standardize how DeFi protocols report on token economics, protocol risks, admin keys, upgrade paths, and governance structures. This can greatly support strong DeFi market growth by improving due diligence and reducing information asymmetries. For governance in particular, tailored disclosures can compel DAOs to adhere to more formal transparency practices, making token holder voting and risk decisions better informed.

SAFE HARBOR FROM REGISTRATION QUESTIONS

Q10: Should the Commission consider a version of Rule 195, my proposed token safe harbor? Is the iteration on my proposed safe harbor known as "Safe Harbor X," or some other iteration, a better approach?

Relevance for DeFi
A regulatory safe harbor would allow early-stage and experimental DeFi protocols to launch tokens and evolve toward decentralization without facing immediate and burdensome registration requirements. This type of framework is particularly important because many DeFi projects begin as community-driven, open-source initiatives with small teams and no traditional venture backing, making full securities-registration processes unrealistic or cost-prohibitive. A safe harbor would give these projects room to innovate, iterate rapidly, raise funds, and build community ownership while still requiring basic disclosures and antifraud protections for users.

It would also support healthier governance evolution by giving protocols time to transition from founder-led development to genuinely decentralized, DAO-based control under a transparent and predictable regulatory pathway. By lowering barriers to entry and providing structured flexibility, a tailored safe harbor could significantly expand the diversity, resilience, and long-term viability of DeFi ecosystems.

Q12: If a safe harbor of some form is the right approach, what disclosure requirements would be feasible for early-stage projects to provide to token purchasers the material information regarding the blockchain project, crypto assets, and development team? What information should be required to be updated on an ongoing basis, and how should that information be provided?
Relevance for DeFi: This question points to the need for a practical "rulebook" for DeFi start-ups: what must be disclosed about token allocations, governance rights, protocol risks, and roadmap? Well-designed requirements could become standard practices for DeFi whitepapers, dashboards, and DAO reporting. This would improve market discipline and support more responsible, accountable governance structures from day one.

Q13: At the expiration of the safe harbor as envisioned, if the network were sufficiently decentralized or functional, registration of the tokens would not be required.
If decentralization is used as an indicator of network maturity, should the Commission define objective quantitative thresholds (such as percentage thresholds for ownership and control) to provide greater clarity for issuers, developers, or minters of tokens regarding whether their networks and protocols are sufficiently decentralized and to allow third parties to verify decentralization?

> **a.** Is dispersion of control a better framework than decentralization? If so, how should ownership of governance tokens and voting rights be considered in assessing dispersion of control? How should the delegation of voting rights be taken into account?
> **b.** If an exit marker is achieved, who should be responsible for notifying the Commission?

Relevance for DeFi
Determining when a protocol is genuinely governed by a DAO rather than a centralized team is fundamental to legal and operational identity for DeFi. Clear, objective thresholds for decentralization and dispersion of control would guide how teams design token distributions, governance structures, and delegation mechanisms. Today, "decentralization" is often subjective and inconsistently measured, creating uncertainty for builders and investors. If regulators were to establish concrete decentralization metrics—such as standards for token ownership distribution, voting power dispersion, or governance participation—protocols would gain a predictable compliance target. This clarity would enable projects to intentionally design governance frameworks that meet regulatory expectations while preserving decentralized ownership and decision-making. It would also strengthen investor confidence and support institutional participation by signaling when a network can be treated more like an autonomous protocol than a company. Ultimately, objective decentralization criteria would provide a roadmap for DeFi protocols to mature in a way that aligns regulatory legitimacy with the ethos of decentralization, resolving one of the most persistent tensions in DeFi governance.

Q14: How should the decentralization of a deployed protocol best be evaluated? How should permissioned aspects of crypto-adjacent software or participant roles, such as validators, relayers, and sequencers, be considered? Are there tech-neutral thresholds that can be agreed upon for determining thresholds for decentralization?

Relevance for DeFi
Most DeFi activities run on infrastructure (e.g., L1s, L2s, rollups) with specific roles like sequencers and relayers that may be partially centralized. How regulators account for these roles affects whether DeFi built on this infrastructure is considered "decentralized." Governance frameworks for DeFi and rollups need to align validator and sequencer design and incentives with any "tech-neutral thresholds" that may emerge.

TRADING QUESTIONS

Q15: Should the Commission create a new entity registration status with tailored registration requirements for any platform that trades crypto assets that are securities? Should the Commission use or adapt the existing requirements for national securities exchange registration or the alternative trading system exemption from such registration, and if so, how?
Relevance for DeFi: DeFi relies on on-chain trading platforms (DEXs, AMMs, aggregators). If any traded tokens are considered to be securities, those platforms may fall under exchange/ATS frameworks. A tailored regime that accounts for smart contract-based, and non-custodial trading is critical to maintain the composability that is inherently part of DeFi, while providing investor protections. DeFi governance approaches need to be designed with an understanding of whether and how the DAOs or front end operators may be treated as "platforms."

DeFi relies fundamentally on on-chain trading platforms (e.g., DEXs, AMMs, liquidity pools, and aggregators) that enable peer-to-peer exchange of diverse digital assets. If any of the tokens traded on these platforms are deemed securities, the platforms themselves could fall under exchange or ATS regulatory frameworks, raising profound questions about how smart-contract-based, non-custodial systems fit into rules designed for centralized intermediaries. A tailored regulatory regime is therefore essential: one that recognizes the unique nature of decentralized, automated trading while still providing investor protections. Such a regime would allow DeFi-native market infrastructure to operate legally without compromising core features like permissionless nature, composability, and decentralization. This clarity is also critical for governance, because DAOs and even front-end operators need to understand whether their activities could cause them to be treated as regulated trading platforms.

Moreover, market structure issues extend beyond registration. DeFi's power comes from its composability—the ability to combine governance tokens, stablecoins, wrapped assets, derivatives, and other instruments within unified protocols. Legal clarity around how mixed trading of "security" and "non-security" tokens is treated is essential to ensuring these innovations can scale. Additionally, because blockchains provide inherent transparency, regulators could leverage public on-chain data, APIs, and tools like proof-of-reserves or proof-of-holdings to conduct oversight more efficiently. Acceptance of such mechanisms would preserve DeFi's transparency advantage while reducing compliance burdens. The SEC's attention to MEV (Maximal Extractable Value) also highlights an understanding of DeFi's unique mechanics—where transaction ordering can create fairness concerns such as front-running or sandwich attacks. Guidance in this area would influence how protocols design fair-execution mechanisms, risk disclosures, and user protections. Ultimately, appropriately designed market-structure, transparency, and fairness frameworks are foundational to building a scalable, trusted, and institutionally compatible DeFi trading ecosystem.

Q16: What updates to the Commission rulebook are needed for side-by-side pairs trading of securities and non-security crypto assets to allow for enhanced interoperability and composability in finance?

Relevance for DeFi
Many DeFi protocols aim to blend tokenized securities (RWAs, bonds, funds) with non-security tokens in the same pools and products. Regulatory tolerance for mixed-asset pools will determine how far DeFi may bridge on-chain and traditional assets. The DeFi ecosystem should account for rule changes that might require segregating or specially handling security tokens in governance, risk, and pool design.

Q18: The crypto markets are inherently transparent because they use open-source data, from public blockchains to open application programming interfaces ("APIs"). Are there programmatic/technological ways that crypto market participants, intermediaries, potential self-regulatory organizations, or regulators can monitor crypto markets using open-source data? How would this take into consideration nested accounts on centralized exchanges, given that this activity may not appear in public ledgers? Is open-source data sufficient for the market to monitor trading and therefore what non-public information might warrant mandatory disclosure? What sort of open-source tools can be used for enhanced transparency, such as proof of reserves, or proof of holdings? What are the limitations of such tools and such data?

Relevance for DeFi
DeFi is built on transparent, publicly accessible ledgers, raising an important question about whether this openness can serve regulatory and self-regulatory functions. If regulators accept on-chain analytics, proof-of-reserves, and similar blockchain-native tools as credible mechanisms for oversight, DeFi's transparency can shift from being an uncharted challenge to becoming a regulatory advantage. This would allow DAOs and protocol teams to formalize on-chain reporting, audits, and real time dashboards as part of compliant operations, strengthening trust and operational integrity. The stakes are significant, as transparency is one of DeFi's defining features, and formal recognition of open source blockchain data as a legitimate basis for investor protection and regulatory monitoring would meaningfully legitimize the sector. This could lower compliance costs, simplify auditing, and enhance systemic-risk surveillance, ultimately paving the way for broader adoption and deeper integration between DeFi and traditional finance.

Q20: How should Commission registrants assess Maximal Extractable Value ("MEV") when they consider building or transacting in these environments? How best should Commission registrants delineate between the different types of MEV occurring onchain? In what ways is the market addressing the MEV in which MEV extractors order or re-order transactions to engage in front running, back running, or so-called "sandwich attacks"?

Relevance for DeFi
MEV is a central theme for fairness and user protections in DeFi. Regulatory focus on MEV would influence how protocols design mempools ("waiting areas" where unconfirmed transactions wait to be verified and added to a block), batch auctions, commit-reveal schemes, and other mitigations. Governance decisions about routing, block-builder relationships, and protocol-level MEV capture vs. redistribution will be shaped by how MEV risk is assessed for regulated participants.

CUSTODY QUESTIONS (ALSO RELEVANT FOR QS 24-32 GENERALLY DEALING WITH INSTITUTIONAL ADOPTION AND THE ROLE OF BROKER-DEALER CUSTODY, INVESTMENT ADVISER CUSTODY, AND INVESTMENT COMPANY CUSTODY)

Q21: Should the Commission amend existing rules, propose new rules, or provide guidance to facilitate custody arrangements for crypto assets? If so, what rule amendments or new rules would be appropriate, and to which types of activities should they apply? Should the Commission propose any specific changes to its rules to accommodate the self-custody of crypto assets by entities registered with the Commission? If so, what conditions should apply to self-custody arrangements to mitigate any related risks? Should the requirements for crypto assets that are securities and those that are not differ?

Relevance for DeFi

Self-custody and smart-contract-based custody are fundamental to how users and protocols operate in DeFi. Recognizing self-custody, multisig arrangements, and smart-contract vaults within regulatory frameworks would enable regulated institutions to interact more directly and safely with DeFi systems. For DAOs and protocol governance, this means developing custody-conscious risk policies—such as timelocks, emergency controls, or circuit breakers—that support institutional compliance without compromising decentralization. As DeFi increasingly incorporates tokenized real-world assets and permissioned tokens alongside native crypto assets, custody rules specific to these instruments will also determine whether they can be used as collateral or within liquidity pools. Governance must therefore evaluate the distinct legal and operational risks associated with native tokens versus tokenized securities, particularly regarding redemption rights, blacklisting, and compliance with enforcement actions.

Custody is a critical barrier because traditional custody regulations assume centralized intermediaries like banks or broker-dealers, which do not align with decentralized systems where users hold keys directly or rely on smart-contract custodians. If regulators update or clarify custody rules to accommodate crypto-native models—including self-custody—they would remove one of the biggest obstacles to institutional and broader retail participation in DeFi. Modernized custody guidance would support safer interaction between traditional financial entities and DeFi protocols while preserving the core user-controlled custody model that defines decentralized finance.

For DeFi to grow beyond its retail and early-adopter base, institutional participation is essential. Funds, asset managers, and investment advisers face strict regulatory requirements around custody, recordkeeping, valuation, and disclosures. Resolving these issues in a way that is compatible with DeFi's technical architecture could unlock significant institutional capital and dramatically scale the ecosystem. Because interacting with DeFi protocols typically requires the use of hot wallets or smart contracts, overly restrictive rules on hot-wallet use could prevent advisers and funds from accessing DeFi yields, liquidity, and governance opportunities. This makes it critical for DeFi governance to consider institutional-oriented design elements (e.g., non-custodial interaction models, permissioned or whitelisted vaults, and low-risk participation mechanisms) that align with evolving regulatory expectations.

Institutional exposure also hinges on whether custody rules can accommodate smart-contract-based assets, including LP tokens, governance tokens, and staking derivatives. If existing custody frameworks prove incompatible with DeFi-native custody models, institutional funds will remain on the sidelines. Conversely, if regulators clarify how funds may hold, stake, or actively participate in DeFi positions, the result could be transformative for market depth and liquidity. Participation in active strategies (e.g., staking, voting, providing liquidity, or engaging in DAO governance) is central to DeFi's value proposition, and institutional access to these activities would meaningfully increase the sophistication and stability of the ecosystem. Relatedly, funds need clarity on how to treat airdrops, staking rewards, or protocol-distributed incentives, which are ubiquitous in DeFi. Regulatory acknowledgment of these mechanisms would normalize DeFi-style yield generation for regulated products. Ultimately, enabling RIAs and funds to safely participate in DeFi's active economic mechanisms would strengthen governance, broaden user bases, and accelerate the integration of decentralized finance into mainstream financial markets.

CRYPTO LENDING QUESTIONS

Q33: How should the Commission approach various crypto lending concepts in a way that doesn't stifle the potential opportunities they provide?

Relevance for DeFi

DeFi lending (money markets, over-collateralized loans, under-collateralized protocols) is a core pillar of the ecosystem. A balanced regulatory approach can safeguard users while enabling innovation in credit markets, interest-rate products, and collateral design. Governance will need to set parameters (collateral factors, liquidations) in light of how "lending" is viewed and regulated.

TOKENIZED SECURITIES QUESTIONS

Q40: Tokenization enables dematerialized securities to be mobilized (i.e., not held in and confined to a single centralized ledger). Are there any provisions under the federal securities laws that prevent these securities from being used in new blockchain-based transactions and applications, and, if so, what steps should the Commission consider taking to facilitate this innovation while mitigating any related risks? Are there amendments or new rules that the Commission should consider to ensure a merit- and technology-neutral approach to tokenization? Does the type of blockchain used (i.e., permissioned versus permissionless) bear on this risk assessment?

Relevance for DeFi

Tokenized securities represent a major pathway for bringing real-world assets (RWAs) into DeFi, but legal barriers and regulatory preferences for permissioned or KYC-gated chains may limit how much of this activity can occur in open, permissionless environments. DeFi governance must therefore grapple with whether and how to integrate tokenized or permissioned assets without undermining composability, one of DeFi's core strengths. If regulators ultimately recognize tokenized securities and permit blockchain-based transfer agents, smart contract-driven settlement, and atomic on-chain clearing, it would create a powerful bridge between traditional finance and decentralized markets. Such a framework could support faster, cheaper, and more transparent settlement processes, unlock massive pools of institutional capital, and enable fractional ownership and greater liquidity for traditionally illiquid assets. The broader promise of tokenization is that, when combined with DeFi rails, it could catalyze new financial products and make mainstream on-chain finance a reality.

V) DECENTRALIZED GOVERNANCE MECHANISMS FOR DEFI

For the DeFi ecosystem, decentralized governance exists to give blockchain-based communities a way to collectively steer the development, resources, and evolution of a protocol without relying on a central authority. As stated above, and supported by DeFi players like Ava Labs[44] and academic research,[45] the first and most important question focuses on what its governance is meant to accomplish. Decentralized Autonomous Organizations (DAOs) use decentralized mechanisms, often powered by governance tokens, to replace the role traditionally filled by corporate boards, executives, or foundation stewards. This ensures that no single actor controls the protocol's direction and that decisions reflect the will of the community. Proper governance prevents misuse or unilateral extraction of value.

Without DAO governance as intended, most DeFi protocols would be restricted to governance by centralized teams, undermining the core value proposition of decentralization. Protocols would stagnate or rely on unilateral decisions by core developers. DAOs enable communities to decide on upgrades, set parameters, choose partnerships, and make strategic adjustments to the protocol. In all cases, governance structures must be designed thoughtfully, as low participation can undermine legitimacy, poorly designed token models can concentrate power, and excessive safeguards can paralyze decision making.

DECISION MAKING

The core purpose of decentralized governance is to coordinate decision making in a transparent, rule-based manner among participants who may be globally distributed, anonymous, or pseudonymous. DAOs may govern key decision making in a variety of ways, from allowing proposals from the community to cover any range of topics, to constraining proposals to narrow, clearly defined decisions. Smart contracts can automate the execution of these decisions, ensuring that treasury spending, token issuance, protocol upgrades, or resource transfers occur exactly as approved. This shifts the concept of traditionally contractual, off-chain processes into verifiable, on-chain actions.

RESOURCE ALLOCATION & TREASURY MANAGEMENT

One key subset of decision making focuses on mechanisms to allocate shared resources, held as treasury assets, in ways intended to reflect the priorities of token holders rather than the preferences of a centralized operator. Many DeFi protocols hold large on-chain treasuries funded by token issuance, fees, or liquidity incentives. Governance ensures that these resources are allocated transparently and in line with community priorities (e.g., funding audits, grants, protocol upgrades, partnerships, and emergency interventions).

ADAPTABILITY

Another subset of decision making supports protocol evolution and adaptability, as DeFi protocols must update smart contracts, risk parameters, yield strategies, oracle sources, and incentive mechanisms in accordance with changes in markets. DAO governance provides a structured, transparent mechanism for making these adjustments. Protocols must evolve as circumstances change, responding to security risks, changing market conditions, and technological advances. Governance provides embedded mechanisms for iteration, upgrades, and meta-governance (e.g., changing the rules of governance itself). This adaptability is crucial for long-term sustainability.

DAO governance also serves to legitimize outcomes by providing mechanisms for accountability. Voting, delegation, proposal templates, and quorum thresholds are tools meant to ensure that decisions arise from agreed-upon community rules rather than arbitrary authority. Clear governance processes give legitimacy to protocol decisions (e.g., upgrades, parameter changes, reward distribution, or partnerships). Transparent decision making increases user confidence and reduces the perception of insider control.

Ultimately, DAO governance is meant to ensure proper and trustworthy decentralization, ensuring reliability while preventing control by a single actor. DAOs are supposed to allow protocols to distribute decision making power across token holders or stakeholders, rather than concentrating it in founders or a central company (although this is not always the case in reality, reflecting how the space still needs to mature). When carried out appropriately, decentralization increases resilience against censorship, capture, corporate failure, or insider abuse.

Decentralization provides resilience. By distributing authority across many participants, DAOs reduce reliance on any single leader or jurisdiction. This makes them harder to censor, co-opt, or shut down. In essence, the purpose of decentralized governance is to empower communities to organize, allocate resources, and evolve collectively in a transparent, accountable, and sustainable manner in the long term.

5.1) DAO GOVERNANCE MECHANISMS

Research shows that DAO governance, through a variety of mechanisms, reflects many of the behavioral, psychological, and political dynamics that are manifested in direct democracies, adapted to the blockchain context. DAO governance structures produce a system that blends political theory, economics, software engineering, and social psychology to create a new form of digital, democratic coordination tailored to blockchain ecosystems.

DAO governance enables new economic and organizational models, which can be beneficial for a variety of organizations.

- Nonprofits and think tanks can find monetization opportunities through tokens
- Communities can fund real world projects such as buildings or carbon credit markets
- Tokenized assets can be governed in ways analogous to managing physical resources

Below are the key decentralized mechanisms employed by DAOs to carry out wide range of decentralized governance functions in the DeFi ecosystem, often powered by governance tokens.

DAO GOVERNANCE MECHANISMS

Mechanism	Function	Strengths	Weaknesses	Commentary
Voting	Token-based: 1 token 1 vote	• Simple, transparent, aligns influence with financial stake, and incentivizes holders to participate • Direct democracy, numerically fair	• Susceptible to plutocracy (wealth concentration = power concentration • Can encourage short-term thinking • Vulnerable to vote buying	Wealthy people may buy a significant majority of the votes
	Quadratic	• Reduces influence of whales by increasing the cost of multiple votes • Amplifies minority voices	• Requires Sybil resistance (otherwise one actor can split wallets to game the system) • Complex to explain and implement • Can deter participation, and may deter people from collaborating as a group	More compelling option that combats the problem of buying votes with buying tokens, as incremental increase in voting authority is more expensive.
	Conviction	• Rewards long-term commitment, where weight increases the longer tokens are locked • Dampens speculative or hasty decision making	• Illiquid for participants (tokens locked up) • Slow responsiveness to urgent issues • Difficult for casual contributors to engage	May only reward people with enough stake to lock up for long term, leading to a preference for "HODLers" who "bought & forgot." This may not be the best measure of selecting participants to be involved in governance, so it may not be best to trust their vote especially for issues that are evolving.
	Reputation-based	• Decouples power from wealth • Aligns governance influence with proven contributions • Can reward long-term community trust	• Reputation systems are subjective and gameable • Difficult to reset if reputation distribution ossifies • Not always transparent	Reality may be detatched from facts. People with big reputations are not always trustworthy. Reputation is not same as leadership, good work ethic. There is a need for non self-centered interests.

Mechanism	Function	Strengths	Weaknesses	Commentary
Proposals	Who can make proposals	Vetting participants	Potential for bias Lack of true decentralization	• Vetting participants is like pre-voting, which may limit breadth of what you can submit (pre-judging) • This can be in the form of thresholds, like holding a certain amount of tokens to be eligible to vote
	Kinds of proposals allowed	Vetting projects	May forego other good ideas that don't fit parameters of what's considered "acceptable" prior	Vetting participants is like pre-voting, which may limit breadth of what you can submit (pre-judging)
	Timelocks/grace periods	Gives community time to react to malicious or rushed proposals llows "emergency exits"	• Can delay urgent upgrades • Attackers may exploit a delay to front-run or prepare countermeasures	Makes the DAO less responsive to the needs of the community; cant respond fast if there's friction in proposal setting
	Quorum requirements	• Ensures broad participation • Prevents small cliques from passing impactful decisions	High quorum can lead to governance paralysis (decisions can't pass); low quorum risks capture by a small group	Quorum avoids individuals spamming the community with random proposals
	Templates/standards	• Improves clarity, comparability, and professionalism • Lowers barriers for new proposers	• May stifle creativity • Bureaucratic feel can discourage grassroots contributors	Promising tool to let people vote on what those templates/ standards are
Smart Contracts to Execute Decisions	Treasury controls	• Multi-sig or contract-based constraints reduce theft and misuse • Predictable disbursements	• Adds friction to funding decisions • May centralize control if few key signers	Assess whether controls clash w/decentralized nature of DAO. Many DAOs are not fully so, for different reasons. There can be excess voting influence - one aspect of this can be treasury control
	On-chain execution	• Transparent and automated • Eliminates trusted intermediaries • Tamper-resistant once executed	• "Code is law" rigidity, where bugs or unforeseen scenarios can cause catastrophic failures • Difficult to reverse	There needs to be significant amount of information given to participants before it happen. Need for clear disclosures and education of participants before they put assets at risk. Don't change model/limit on chain execution (off chain destroys the point), but need people appraised on what's happening. (ex -when voting to make a major purchase, funds are allocated and sent as soon as everyone votes yes).
	Emergency functions	• Safety valve for hacks or governance attacks • Builds confidence in early DAOs	• Centralization risk: who controls the emergency lever? • Potential abuse undermines decentralization	Can be effective to stop exploits quickly before permanent fix is deployed, which may rely on human intervention. This may require trust in a central entity to make this kind of decisions

Mechanism	Function	Strengths	Weaknesses	Commentary
Delegation	Participants delegating voting to others	• Increases participation by allowing passive token holders to delegate to active stewards • Concentrates expertise	• Risk of entrenched power blocs • May recreate representative politics rather than true decentralization	Increases participation and informed decision making but can lead to delegate misbehavior and "window dressing" concerns where early investors/founders still hold the majority of power. This double edged sword requires accountabilty mechanisms and careful structural design.
Governance Tokens	Mechanism for users to vote and participate in decision making	• Clear unit of governance power • Liquid and tradable • Can align incentives via ownership	• Markets for tokens invite speculation; governance power can be bought • May diverge from user/community interests	Foundational element for DeFi governance, but main challenges consist in plutocracy (whale domination), voter apathy, and a lack of legal enforcement. There is a need for robust mechanisms to counter wealth concentration and encourage broader and meaningful participation
Governance Updates	Meta-governance to change major governance aspects (e.g., voting mechanisms, modify smart contracts, etc.)	Allows adaptation as DAOs evolve Critical for resilience in a fast changing ecosystem	• Updating governance itself can be contentious or slow • Risk of capture if upgrade processes are unclear	Unprecedented transparency and adaptability to change, but may encounter difficulties when it comes to security, speed, and concentrated power structures. AI-based automated governance mechanisms are being experimented to address these challenges.

5.2) DAO GOVERNANCE VS. CORPORATE GOVERNANCE

With no centralized control, DAOs operate very differently from traditional corporations. For a corporate setting, the main purpose of governance is to act on behalf of shareholders. Directors are expected to act in accordance with this purpose, even as US regulations have allowed boards and management teams to have certain veto rights over proposals.

On the other hand, DeFi protocols carry out many of the equivalent governance processes by means of DAOs and governance tokens. These decentralized mechanisms replace the role traditionally filled by corporate boards, executives, or foundation stewards. The entire lens of governance shifts because in peer-to-peer networks, there are no shareholders to act on behalf of in the same way. The users and token holders themselves can have the opportunity to directly participate in decision making

Below is a comparison of key governance aspects for corporations and DAOs:

Governance Mechanism	Corporate Governance	DAO Governance
Purpose	Alignment of management with shareholder interests, generally by maximizing firm value, and ensuring compliance with law and fiduciary duties.	• Coordination of a decentralized community to collectively manage, fund, and evolve a protocol. • Preserve decentralization and ensure decisions reflect the community rather than a central authority.
Decision Making	Centralized: a board of directors and executives make strategic and operational decisions on behalf of shareholders.	Decentralized: decisions are proposed and voted on by token holders as direct participants in a network, or designated delegates. This is often executed automatically via smart contracts.
Accountability	Directors and officers face legal and fiduciary accountability, with regulators enforcing compliance and reporting obligations.	Accountability is embedded into transparent on-chain voting, open-source code, community oversight, and reputational incentives, with enforcement being more social and technical rather than legal (which may evolve with regulatory developments for DeFi).
Adaptability	Adaptation takes place through management initiatives, board resolutions, and occasional shareholder votes (considered infrequent or slow).	Highly adaptable, where protocols can evolve continuously through proposals, parameter changes, and upgradeable smart contracts. Governance processes can be iterated and redesigned over time.
Ownership & Control	Shares represent economic and voting rights, where voting power is usually proportional to investment Retail shareholders are generally passive.	Tokens may represent voting power, governance rights, or utility. Participation can be open to anyone, and power can be more widely distributed, though large token holders can dominate.
Transparency	Financial and strategic disclosures are provided periodically through regulated reporting (e.g., quarterly filings).	Full transparency, where treasury balances, votes, proposals, and upgrades are visible on-chain in real time.
Execution of Decisions	Decisions are executed by management and operational staff, with off-chain implementation that is subject to discretion.	Decisions can be executed automatically through smart contracts, reducing discretion and increasing determinism.
Participation	Limited, where only shareholders vote, and most retail shareholders do not participate.	Broad, global, permissionless participation, where token holders, contributors, and delegates can engage directly in governance.
Regulatory Structure	Well defined legal frameworks provide clear fiduciary duties, liability standards, and corporate reporting requirements.	Emerging and uncertain legal frameworks, where DAOs often operate without clear jurisdictional rules and rely on technological rather than legal compliance mechanisms. This may evolve with regulatory developments.
Resilience & Continuity	Continuity depends on the firm's solvency, leadership stability, and compliance with legal obligations.	Protocols can be resilient and durable through decentralization. Governance continues even if individual contributors or teams exit the network.
Resilience & Continuity	Continuity depends on the firm's solvency, leadership stability, and compliance with legal obligations.	Protocols can be resilient and durable through decentralization. Governance continues even if individual contributors or teams exit the network.

5.3) DAO GOVERNANCE GAPS

There exist clear governance gaps between DAOs and traditional corporations that reflect the immaturity of decentralized governance frameworks relative to long-established corporate structures. Although DAOs offer radical on-chain transparency, this information is not always easy for participants to interpret, unlike curated corporate disclosures designed for investor comprehension. Taken together, these gaps highlight the need for more robust governance design, legal integration, and regulatory clarity for DAOs to achieve the reliability, accountability, and strategic coherence expected of mature financial systems.

Gap 1: Accountability – Structures for accountability are much more developed for traditional corporations, leading to greater trust and scale.

- Corporations benefit from clear legal accountability. Directors and officers have fiduciary duties, can be held liable, and operate under strong regulatory oversight.
- DAOs, on the other hand, rely mostly on social, reputational, or technical accountability, with no consistent legal recourse when governance decisions go wrong.

Gap 2: Participation & Strategic Vision - Participation differs significantly, in ways that can significantly undermine the quality of decision making for DAOs: a major gap where DAOs may not operate as intended. Strategic coherence is also harder to achieve in DAOs, where decentralized voting can produce inconsistent or reactive governance rather than a unified long-term vision.

- Corporate governance is centralized and stable, with boards acting on behalf of shareholders. Corporate boards consist of experienced professionals who deliberate strategically on key priorities.
- DAOs allow broad, permissionless participation but often suffer from voter apathy, governance capture by large token holders, and unrepresentative decision-making. DAO voters may lack the technical or financial expertise needed to evaluate complex proposals, leading to fragmented or short-term choices.

Gap 3: Execution Challenges - Execution and enforcement may be unclear for DAOs in the context of their structure.

- Corporations have employees and managers who carry out decisions, with expertise and nuance required to address complex issues and unexpected problems.
- DAOs rely on smart contracts or loosely coordinated contributors, making execution either rigid (when coded) or uncertain (when human). Smart contracts are only programmed to execute based on predetermined conditions, which will not include the possibilities of unintended outcomes that eventually may occur.

Gap 4: Regulatory clarity (or lack thereof) – Regulatory developments for blockchain and digital assets are still underway, leading to a series of regulatory gray areas for DeFi and DAO governance in specific.

- Corporations operate within well-defined legal frameworks, reporting rules, and compliance standards.
- DAOs often exist in legal gray areas with uncertain tax treatment, liability, and compliance obligations.

Gap 5: Ownership and control divergences – In traditional contexts, those who own a company may be different than those who control it by making key decisions, with clear and established roles. DAO structures may bring together ownership and control in a way that better aligns interests, but the need for better safeguards remains.

- Corporate ownership structures are stable and legally registered.
- DAO token ownership is fluid and anonymous, creating risks of governance attacks or sudden shifts in control.

VI) CONCLUSION

DeFi introduces a series of structural changes that fundamentally reshape how financial markets operate, especially if adopted at scale. By reducing reliance on intermediaries and enabling peer-to-peer interactions, DeFi creates more efficient markets with broader participation, in contrast to traditional systems where large institutions dominate profitable activities (e.g., syndicated lending among top banks) while leaving smaller participants remain excluded.

Moreover, DeFi's open, global infrastructure allows anyone with an internet connection to access market-rate borrowing, lending, and trading opportunities across borders. This expands the universe of available interest rates and financial products, enabling individuals and institutions to seek opportunities globally rather than being bound by domestic market constraints. For example, where one country may experience zero interest rates and another high rates, DeFi enables capital to flow to where it is most productive, fostering more competitive and efficient pricing.

Although technology serves as the tool enabling this transformation, human relationships, trust, and responsible practices (e.g., including whitelisting, compliance mechanisms, and adherence to securities laws when relevant) remain important as DeFi integrates with regulated environments. If scaled, DeFi could significantly expand global capital flows, shift markets toward a unified global cost of capital rather than fragmented national ones, and increase access and efficiency across the financial ecosystem while preserving pathways for regulated participation.

If regulators adopt such an adequate approach to DeFi as discussed throughout this paper, the implications for DeFi and the broader crypto ecosystem could be transformative: greater regulatory clarity, reduced legal risk, more institutional participation, deeper liquidity, and broader use of tokenized assets, all while keeping the core benefits of decentralization and blockchain-native infrastructure.

If DAOs at the same time also evolve decentralized governance strategies, DeFi protocols will be able to operate more safely, transparently, and sustainably at scale. This ensures that decisions are made collectively rather than controlled by a single actor, increasing resilience and trust in the system. Effective governance also improves risk management, responsible resource allocation, and can guide the DeFi protocols' long-term strategy. By embedding accountability, clear processes, and community participation, strong DAO governance attracts users and institutional partners, reduces vulnerability to manipulation or governance capture, and supports continuous innovation. Ultimately, effective DAO governance can transforms DeFi protocols from a set of smart contracts into a stable, credible, and self-sustaining ecosystem.

RECOMMENDATIONS

The following recommendations for DeFi governance outline a practical path forward.

A roadmap for a hybrid, pragmatic regulatory regime should:

- Recognize new digital-native tokens and define a category for them (protocol tokens) rather than forcing them into traditional securities definitions.
- Update custody, exchange, and intermediary rules in a technology-neutral way to allow blockchain-native trading & settlement.
- Permit tokenization of traditional assets (equities, funds, debt), all treated as securities, but allow them to live on blockchains with smart-contract enforcement of transfer restrictions and compliance.
- Ensure disclosure, AML/KYC, and investor protections roughly analogous to what exists now, but adapted to digital realities.
- Provide transitional or safe-harbor regimes to let innovation continue while regulation catches up.

If regulators adopt such an approach, the implications for DeFi and the broader crypto ecosystem could be transformative: greater regulatory clarity, reduced legal risk, more institutional participation, deeper liquidity, and broader use of tokenized assets, all while keeping the core benefits of decentralization and blockchain-native infrastructure.

1. Establish a Clear and Harmonized Regulatory Framework

- Adopt a functional, technology-neutral regulatory model that follows the activity over the technology. Oversight should focus on actors (e.g., custodians, exchanges, brokers, and revenue-generating intermediaries), not protocol developers or validators.
- Recognize new digital-native tokens, such as “protocol tokens” that perform network functions (e.g., gas, staking, validation, governance), which should not be forced into traditional securities definitions.
- Permit tokenization of traditional assets (equities, funds, debt), all treated as securities, and allow them to operate on blockchains with smart contract enforcement of transfer restrictions and compliance.
- Provide tailored disclosure and registration pathways, with proportional disclosures for DeFi (e.g., tokens, governance structure, token supply, admin key risks, and upgradeability).
- Implement safe harbor regimes to let innovation continue while regulation catches up. For early stage protocols, this would provide DeFi projects space to decentralize before facing full regulatory obligations. This should require baseline disclosures, anti-fraud protections, and decentralization milestones.

2. Define Standards for Decentralization and Control, with measurable criteria for decentralization

- Clarify what counts as “sufficiently decentralized,” using metrics such as token distribution, governance participation dispersion, or operational independence from founders.
- Clarify treatment of sequencers, relayers, and validators. Roles essential to network operations should not be automatically treated as regulated intermediaries unless they perform discretionary or revenue-generating functions comparable to traditional financial actors.

3. Adapt Custody, Settlement, and Exchange Rules

- Update custody rules to recognize smart contract and self-custody models.
- Permit blockchain-based settlement for both securities and non-securities tokens.
- Create tailored rules for non-custodial trading venues, such as DEXs and automated market makers (AMMs), allowing them to operate under a framework distinct from centralized exchanges that can recognize code-based matching, automated liquidity, and the absence of discretionary brokers.
- Update custody, exchange, and intermediary rules in a technology-neutral way to allow blockchain-native trading & settlement.

4. Strengthen Private Law Foundations for Digital Assets

- Harmonize property law treatment of digital assets, drawing on principles such as UCC Article 12 or UNIDROIT to define digital asset ownership, transfer, custody, and creditor rights.
- Support legal recognition of blockchain ledgers as valid property registries.
- Develop clearer legal treatment for tokenized RWAs.

5. Improve DAO Governance Structures and Accountability

- Adopt governance designs that increase participation and reduce capture, using delegation, reputation systems, quadratic or alternative voting models, and incentive structures to avoid plutocratic control.
- Formalize governance processes and transparency, requiring proposal templates, disclosure of conflicts, voting thresholds, and risk assessments to strengthen decision-making quality.
- Clarify execution responsibilities, especially for situations where smart contracts cannot handle unexpected complexity. DAOs should designate teams, stewards, and service providers responsible for operational execution with clear mandates.

6. Embed Security, AML, and Privacy-Preserving Compliance into Protocol Design

- Shift from identity-first KYC to behavior-first AML, integrating blockchain analytics, behavioral monitoring, and pattern detection rather than relying solely on traditional identity collection.
- Adopt privacy-preserving compliance tools (e.g., zero-knowledge proofs), where users can prove they are not sanctioned or illicit without revealing sensitive data.
- Create interoperability layers for compliance, such as a global “green-check” verification standard to enable private, verifiable participation in DeFi.
- Encourage RegTech inside the protocol instead of around it, embedding compliance logic within smart contracts to reduce reliance on centralized intermediaries and facilitate institutional use.
- Ensure disclosure, AML/KYC, and investor protections roughly analogous to what exists now, but adapted to digital realities.

OPEN QUESTIONS

The following open questions remain to be addressed by the DeFi ecosystem in order to scale in a coordinated and compliant manner:

1. How should DeFi activities, protocol tokens, and decentralized systems be classified under law and regulation?
2. What constitutes "sufficient decentralization," and how should accountability work in decentralized systems?
3. How should smart contracts be treated legally and operationally?
4. How should decentralized marketplace actors (e.g., DEXs, AMMs, composable protocols), be regulated without undermining decentralization?
5. Should decentralized exchanges (DEXs) or elements of DeFi protocols be treated as regulated intermediaries, and under what conditions may this treatment be considered?
6. How should digital assets be treated under property, custody, and bankruptcy law?
7. How should DAOs draw on traditional corporate governance structures to carry out governance activities?
8. How should existing weaknesses in DAO governance mechanisms be addressed in a harmonized way, such that the strengths of decentralized governance remain while ensuring user protections?
9. How should DeFi integrate compliance (KYC/AML) while preserving privacy and decentralization?
10. How should systemic risks be managed in a composable ecosystem where protocols may be significantly interconnected and dependent on one another on many levels?
11. What is the right balance between decentralization and centralized control if at all necessary?

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

GBBC GSMI 6.0

ACKNOWLEDGEMENTS

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

ShuhYun 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 using 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 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.

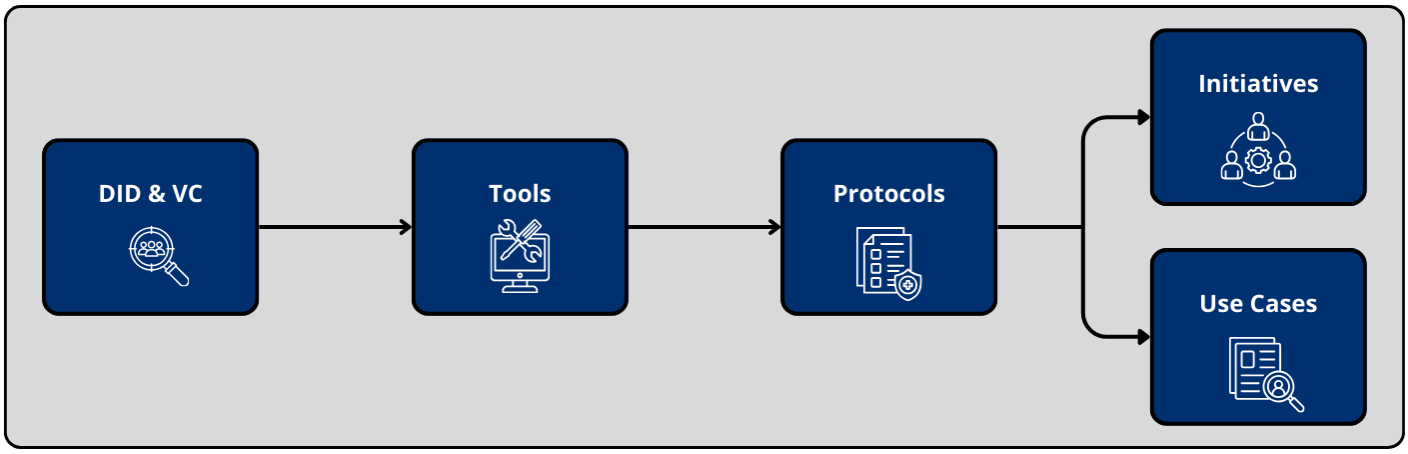
Consent-Based Practices: Best practices support a consent-based model for data sharing. These include:

- 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.	*HTTPS:* 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) *Virtual Private Networks (VPNs):* 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	*Zama.ai* – 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 hasing 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	*Secure Hash Algorithm (SHA)* - cryptographic hashing family, commonly used in various security protocols and applications *Argon2* - Secure hashing algorithm designed for password hashing *CRC32* - 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	*Blockhcian Transactions* - 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	*Zero-Knowledge Succinct Non-interactive Argument of Knowledge (zk-SNARKs) & Zero-Knowledge Scalable Transparent Argument of Knowledge (zk-STARKs)* – Cryptographic techniques used for scalable, verifiable privacy *Zcash* – A privacy-focused cryptocurrency that uses zk-SNARKs to enable shielded transactions *Polygon zero-knowledge Ethereum Virtual Machine (zkEVM)* – A zero-knowledge Ethereum Virtual Machine supporting private smart contracts *Aztec Network* - Privacy layer for Ethereum using ZK rollups to enable confidential transactions *Zero-Knowledge Rollups (ZK Rollups)* - 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	*Blockchain Transactions* - 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	*Partisia Blockchain* – 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)[57]	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 trustworkthy 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 auditabilit	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.	*W3C VC in Sovrin/Indy, EU EBSI pilots, UNJSPF PoL.*
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.	*Hyperledger Indy, EU EBSI, W3C DID.*
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.	*Idemix, AnonCreds (Hyperledger), eIDAS pilots.*
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	*ToIP, Sovrin, Kiva pilot, EU EBSI, UNJSPF/UN pilots*
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 trrorist financing, leading to a bad reputation in the industry • Some jurisdictionis 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	*Monero (XMR)* - Uses ring signatures, stealth addresses, and RingCT to obscure sender, receiver, and amount in all transactions by default *Zcash (ZEC)* - Allows users to choose between transparent or shielded transactions, which use zero-knowledge proofs to hide transaction details *Dash (DASH)* - 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	*Tornado Cash* – Ethereum-based mixer using zero-knowledge proofs to anonymize ETH and ERC-20 tokens *Wasabi Wallet* – Bitcoin wallet with built-in coinjoin features for privacy *Samourai Wallet + Whirlpool* – Bitcoin mixing focused on financial privacy Monero, Ethereum Tornado.
Privacy Pools Protocol[58]	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	*Tornado Cash* - uses early privacy pool anonymizing transactions on platforms like Ethereum, requiring users to provide cryptographic proof to withdraw funds *Aztec Network* - Built privacy-enhancing layers and private execution environments on blockchains *Penumbra* - 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 tokenks/ tools, they're vetted • Audit contract bytecode, runtime proofing	*Secret Network* – Uses Trusted Execution Environments (TEEs) to execute smart contracts privately *Oasis Network* – Supports confidential smart contracts with on-chain/off-chain data separation *Phala Network* – A privacy-preserving cloud computing platform using TEEs and blockchain *Enigma (SCRT)* – 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'ssystem • Safeguarding of data • Data sovereignty • Audited outputs, price fairness mechanisms	*Ocean Protocol* – Allows data providers to share data while maintaining control and privacy *Numeraire (Numerai)* – 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 is 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 it's 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.[46] 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 DCE[47] 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."[48]

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 SingPass[49] 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 guidance[50] and known AML high false positive statistics.[51] 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. his 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 sanctions[52] that were later removed[53], while the privacy coin Monero has faced regulatory scrutiny[54] 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.[59] • **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. [60] • **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 authentica-tion mechanisms), providing a foundation for legally recognized eID, eSignatures, and trust services under eIDAS (Electronic Identification, Authentication, and Trust Ser-vices). • **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.[61] • **Web3 relevance:** provides strong MFA and hardware-bound keys that can be com-bined 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.[62] • **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.[63] • **Web3 relevance:** used by many Web3 frontends, custody platforms and APIs for ac-cess 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.[64] • **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 ecosys-tems, 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.[65] • **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.[66] • **Web3 relevance:** In context where identity cane 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 Pri-vacy Information Management System, helping controllers and processors manage PII privacy risks.[67] • **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.[68] • **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.[69] • **Web3 relevance:** provides a conceptual model for "assurance levels" of Web3 identi-ties 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.[70] • **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 refer-enced)	• Suite of documents (63-3, 63A, 63B, 63C) specifying identity proofing, authentication, and federation assurance levels and technical requirements.[71] • **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.[72] • **Web3 relevance:** applies to card-based on-/off-ramps, custodians, and payment pro-cessors that bridge Web3 tokens with card rails. Strong overlap with wallet KYC, to-kenization 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.[73] • **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.[74] • **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.[75] • **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.[76] • **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 infrastruc-ture with governance and legal layers to define "Internet-scale digital trust."[77] • **Web3 relevance:** provides an architectural blueprint for layering DIDs, VCs, govern-ance frameworks, and trust registries over Web3 networks, aligning them with enter-prise 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.[78] • **Web3 relevance:** core identity primitive in Web3, used to represent wallets, organiza-tions, 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.[79] • **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.[80] • **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).[81] • **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 let 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)[55], 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)

SEDI[56] 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 Limitatin	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?**

GBBC
Global Blockchain
Business Council

DIGITAL MONEY & PAYMENTS REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 6.0

DIGITAL MONEY & PAYMENTS: PATH TOWARD CONVERGENCE BETWEEN LEDGER-BASED AND TRADITIONAL SYSTEMS

GBBC GSMI 6.0

ACKNOWLEDGEMENTS

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

Rahul Advani - CO-CHAIR
Global Co-Head of Policy, Ripple

Wee Kee Toh - CO-CHAIR
Global Head of Business Architecture,
Kinexys by J.P. Morgan

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

For the purposes of this paper, 'blockchain-based digital money' refers to a subset of digital currencies: stablecoins, CBDCs, and deposit tokens, whose issuance, transfer, and record-keeping rely on distributed ledger technology (DLT) or blockchain rails.

INTRODUCTION

Digital money encompasses a broad spectrum of models, ranging from private issuance to sovereign issuance, deployed across both traditional banking and DLT rails, over public and private blockchains. We start with a basic taxonomy defining the range of models of digital money that this paper will focus on, and they differentiate themselves. This paper focuses on a specific subset of blockchain-based digital money models, specifically those that are backed by assets in a regulatory compliant manner, with the objective of explaining digital money payments using traditional payment processing frameworks.

Taxonomy of Digital Money Models: We start with an overview of the digital money models under the scope of this paper, their: stablecoins, central bank digital currencies (CBDCs), and deposit tokens. We cover the opportunities of each, use cases, and challenges that need to be addressed for scale.

Ecosystem View of Digital Money: Next we cover the ecosystem of key stakeholders and their interactions for payments with stablecoins, CBDCs, and deposit tokens. While they present different starting points from traditional systems by operating on DLT infrastructures, once all regulations and risk management measures are put into place, both ledger-based and traditional payments models start to converge.

Value Chain of Payments with Digital Money: We build on the ecosystem view by illustrating a blueprint of payments using standards in the context of existing payment processes along the value chain.

- We provide an end-to-end view of payment processes mapped out against regulations and standards (both for payments and for blockchain/digital assets)
- We provide a parallel end-to-end view of payment processes mapped out against new considerations for blockchain-based digital money, and any gaps in regulations and standards
- We expect that as standards and regulatory requirements continue to develop, existing gaps will be addressed, and the blockchain-based digital money payments space will continue to converge with the traditional payments structures and approaches

Regulations: Finally, we discuss the case of global stablecoins, CBDCs, and deposit tokens in light of regulatory developments.

As digital money introduces novel issues with the use of blockchain technology and decentralized ledgers, this paper focuses on themes specific to blockchain-based digital money models and their use for payments. These themes in general should apply equally regardless of whether digital money operates on public or private blockchain networks, or if it takes the form of stablecoins, CBDCs, or deposit tokens. This leads us to conclude with open questions and recommendations to achieve scalability for these digital money models that point to the future of ledger-based payment systems.

I) TAXONOMY OF DIGITAL MONEY MODELS

While digital money on blockchain rails[82] may vary widely in its design and incentives – from privately issued representations of fiat currency in the form of stablecoins, to tokenized representations of central bank-issued money, or purely decentralized cryptocurrencies issued by the networks on which they operate – this paper focuses on payments operations, and thus the scope of digital money covered by the following discussion includes solely models that are backed by assets in a regulatory compliant manner. This paper focuses on a specific subset of blockchain-based digital money models: stablecoins, CBDCs, and deposit tokens. Below is an overview of each, illustrating the benefits, opportunities for usage, and challenges to scale.

I.I) STABLECOINS

Most recently, there has been a surge in stablecoin popularity as a form of digital money.

SELECTED DEFINITIONS

- **CFTC (GMAC - DAMS):** Privately-issued, money-like, digital token that aims to maintain a stable value relative to a peg specified by a reference asset(s) and designed to minimize value fluctuations relative to these reference assets(s). They are not issued by a central bank. They must also be at least fully backed by one or more assets specified under the specific regulatory framework, including:

    a. Cash: to one or a combination of fiat currencies
    b. Securities: low risk, highly liquid securities such as those classified as High-Quality-Liquid Assets ("HQLA") under the BCBS LCR30 framework (e.g., US Treasury Bills)

- **Financial Stability Board (FSB):** The FSB considers that so-called stablecoins are a type of crypto-asset 'that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets to other assets.'

- **International Securities Services Association (ISSA):** A class of crypto-currency designed to eliminate the price volatility of cryptocurrencies by backing them with real assets, fiat currencies or a mixture of both. A stablecoin whose price reference is the US Dollar, for example, would be backed 1:1 by US Dollars in a custody account. Investors redeeming the stablecoin would receive one US Dollar for each stablecoin.

- **US GENIUS Act:** The term "payment stablecoin"—(A) means a digital asset— (i) that is or is designed to be used as a means of payment or settlement; and (ii) the issuer of which— (I) is obligated to convert, redeem, or repurchase for a fixed amount of monetary value; and (II) represents it will maintain or creates the reasonable expectation that it will maintain a stable value relative to the value of a fixed amount of monetary value; and (B) that is not— (i) a national currency; or (ii) a security issued by an investment company registered under section 8(a) of the Investment Company Act of 1940 (15 U.S.C. 80a–8(a))

Examples	Description	Market Size (Market Cap)[118]
USDT	Stablecoin – USD backed	$184.5B
USDC	Stablecoin – USD backed	$75.8B
RLUSD	Stablecoin – USD backed	$1.2B
EURC	Stablecoin – EUR backed	$327.3M

STABLECOIN USE CASES

- Facilitate payments as digital money, with less volatility and over more efficient blockchain infrastructure
- Facilitate remittances at lower costs and greater efficiency to move money across borders
- Used in Decentralized Finance (DeFi) to lend, borrow, trade, and liquidity provision (where many stablecoin deposits also earn yield)
- Used as a bridge between crypto & traditional finance (e.g., crypto traders going in and out of trades without having to go back & forth between the traditional banking system & crypto rails)
- Hedge against crypto market swings
- Retail & emerging markets can use stablecoins as an alternative to unstable local currencies, and for small/micro p2p transactions as an alternative to slow or expensive banking services
- Institutional & TradFi benefits in treasury functions

STABLECOIN GROWTH TRENDS

- **Increasing total supply & market cap:** $300B in supply, with strong yearly growth projections (50% or above)[83]
- **Active addresses/users increased** from 19.6M to 30M (Feb 2024-Feb 2025)[84]
- **Monthly transfer volume increased** from 1.9T to 3.9T (Feb 2024-Feb 2025)[85]
- **USD-pegged stablecoins dominate**, with 99% of market share[86], with USDT ($186.67B market cap) & USDC ($76.54B market cap) as clear leaders.[87] USDC is growing faster and may surpass USDT by 2030[88]
- **Regulatory developments are boosting confidence**, as key enabler driving adoption
- **Regulatory developments perceived as a green light for expansion:** For instance, the US GENIUS Act authorizes banks and other institutions to issue stablecoins backed by fiat or high-quality collateral. Institutional adoption has advanced, with stablecoin adoption for activities such as treasury operations, corporate cash management, and overall integration with traditional finance.

STABLECOIN CHALLENGES FOR SCALE

- Regulatory uncertainty remains, as gaps remain across jurisdictions
- Peg stability & reserve transparency are key. If this comes into question, the peg can be broken and erode trust
- Counterparty & network risks if stablecoin issuer or custodian has poor quality assets, risk exposures, and poor governance
- CBDCs in certain jurisdictions may compete with stablecoins
- Stablecoins may pull capital out of banking system in emerging markets where they're perceived as safer value storage alternative

I.II) CENTRAL BANK DIGITAL CURRENCIES (CBDC)

Pilots and prototypes have arisen around the world for several models of CBDC, with a few full launches to date, signaling that many nations perceive CBDCs as a strategic infrastructure. A wide range of design models (retail vs wholesale, offline vs online, account-based vs token-based) can be implemented with various approaches and priorities. When it comes to CBDCs and overall framing of how digital money is used with them, a critical differentiation is retail vs. wholesale. These have significant differences functionally, target user-base wise, regulation-wise, and in terms of adoption and market size. Much of the initial CBDC infrastructure being rolled out, in terms of size, function, and initial adoption, is expected to be at the wholesale level (e.g., largescale settlements between central banks and institutions), where the value proposition focuses more on instant settlement, ledger transparency, reduced costs of moving funds, etc., without the retail-level concerns about privacy in day-to-day transactions.

SELECTED DEFINITIONS

- **Bank of England:** Central bank digital currency (CBDC) is money that a country's central bank can issue. It's called digital (or electronic) because it isn't physical money like notes and coins. It is in the form of an amount on a computer or similar device.
- **CFTC (GMAC - DAMS):** digital tokens representing a claim on a central bank for a fixed amount of central bank money denominated in a single currency; also, a liability of a central bank, with no credit or liquidity risk. It may or may not be programmable.

  a. "General Purpose" or "Retail" CBDC: a CBDC that is specifically designed for use in transactions and holdings by individuals and/or small and medium-sized enterprises;
  b. "Wholesale" CBDC: a CBDC that is specifically designed for wholesale use in transactions and holdings by regulated financial institutions and could be used in the facilitation of regular financial markets functions (e.g., settlement of securities transactions).

- **International Organization for Standardization (ISO):** A CBDC is a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank.
- **International Monetary Fund (IMF):** Potentially a new form of digital central bank money that can be distinguished from reserves or settlement balances held by commercial banks at central banks. It is a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value. CBDCs are not cryptoassets.

- **International Securities Services Association (ISSA):** In broad terms, a CBDC is simply a new form of digital liability of a central bank. Because it is issued by a central bank, CBDC is typically thought of as being denominated in the currency of that central bank.
- **National Institute of Standards and Technology (NIST):** Central bank digital currencies (CBDC)... would represent central bank reserves, for reasons such as reinforcing the transmission of monetary policies, establishing new transmission channels, or just in response to a decline in cash.

Examples	Jurisdiction	Description	Market Size (Funds in Circulation)
SandDollar	Bahamas	CBDC - retail	$2.1M in circulation (March 2024 – Central bank statistics)
eNaira	Nigeria	CBDC - retail	$9.16M in circulation (Jan 2025 – Central Bank statistics)
JAM-DEX	Jamaica	CBDC - retail	J$ 257M in circulation (Feb 2023 – central bank statistics)

CBDC USE CASES

- Retail payments, ranging from instant peer-to-peer payments (e.g., phone-to-phone transfers), merchant payments with lower fees and faster settlement, micropayments (e.g., streaming services, per-use digital goods and pay-per-article consent), and even offline payments functionalities.
- Government and public sector innovation, improving the efficiency, transparency, and delivery of public services including government-to-person payments (e.g., social benefits, stimulus checks, disaster relief), tax collection and automatic remittances, delivery of subsidies and grants. CBDCs allow programmable disbursements tied to specific conditions.
- Modernization of payments systems with 24/7 instant and programmable settlement across banks and payment providers, automated reconciliation between financial institutions, and greater reliability.
- Cross-border payments with open and interoperable rails, direct FX settlements between countries, instant trade settlement, real-time fund flows at lower costs, and multi-CBDC platforms reducing layers of correspondent banking processes, and improved compliance with harmonized AML/KYC
- Capital markets modernization, especially for wholesale financial market innovations, allowing tokenized asset settlement, atomic settlement, better intraday liquidity management solutions, and programmable treasury operations. CBCDs support digital asset and tokenized economies
- Monetary policy and macro financial tools for central banks, to be used cautiously, with opportunities for direct transmission of monetary policy, interest-bearing CBDCs as a policy tool, and programmable incentives (e.g., stimulus with expiration dates). All these tools can also provide economic data for macro analysis.
- Cash replacement or complement in societies with declining cash use

CBDC GROWTH TRENDS

- **137 countries and currency unions** (representing 98% of global GDP) have explored CBDCs, with 3 launches, 49 pilots, 20 models in development, and 36 models in research stages[89]
- **Approximately 94% of central banks are actively exploring CBDCs,** according to survey results from the Bank for International Settlements (BIS)[90]
- **34% of central banks now expect to issue a CBDC within the next 3-5 years**, up from 26% a year earlier[91]
- **Payments value using CBDCs** is projected to surpass **USD $200 billion by 2030**
- **Transaction volumes** for the retail pilot of China's digital yuan (e-CNY) reached **RMB 7 trillion** (USD $986 billion) in June 2024 across 17 provinces[92]

CBDC CHALLENGES

- Privacy and civil liberty concerns arise when trying to balance transaction-level visibility for compliance purposes with individual privacy protections (e.g., how to maintain cash-like anonymity while preventing illicit finance), with the risk of government surveillance or overreach.
- Cybersecurity and Operational risks (e.g., fraud, double-spending, counterfeiting), where CBDCs can become a target for nation-state level cyberattacks, make the need for extremely robust, quantum-resilient, and continuously updated security systems imperative. Attacking the infrastructure of a CBDC system can lead to financial instability.
- While many central banks are exploring CBDCs, there are very few actual full launches remain few. The vast majority of implementations are in the form of pilots and prototypes. The lack of live examples can be a hindrance to scalability.
- Retail CBDC models face significant barriers for widespread adoption and usage with respect to updates needed in infrastructure, regulation, and user behavior.
- Given the wide range of CBDC designs, comparability becomes complex
- The rollout of CBDC launches has been slowed among major economies due to various concerns including geopolitical, regulatory, privacy, and financial stability uncertainties.

DEPOSIT TOKENS

Increasing opportunities with deposit tokens arise to bridge traditional banking and digital assets, as they combine legal clarity of traditional banking with the programmability and interoperability of blockchain networks. As on-chain representations of bank deposits, these instruments are subject to the same standards as traditional bank deposits. Blockchain Deposit Accounts by J.P. Morgan's Kinexys is a prominent early example of a blockchain based bank deposit, while JPM Coin is an example of a deposit token.

SELECTED DEFINITIONS

- **CFTC (GMAC - DAMS):** Deposit Tokens - transferable digital tokens issued by a licensed depository institution which evidence a deposit claim against the token-issuing bank or depository institution, for fixed amount of commercial bank money or fiat cash denominated in a single currency.
- **CFTC (GMAC - DAMS):** Tokenized Deposits - digital tokens that represent an existing record of a traditional ownership claim for a bank deposit on the token-issuing bank or depository institution, for a fixed amount of commercial bank money denominated in a single currency.
- **JP Morgan:** Blockchain-based deposits, i.e., distributed ledger-based deposits issued by a licensed depository institution, including deposit tokens, which are forms of commercial bank money.[93]
- **KPMG:** Tokenization of commercial bank money can be in the form of tokenized deposits or deposit tokens. Tokenized deposits are token representation of the commercial deposits where each token is backed by retail or institutional deposits. Whereas a deposit token is the native token on blockchain which directly represents the retail or institutional deposits in form of tokens.[94]

Examples	Description	Transaction Volume
Blockchain Deposit Accounts - Kinexys by JP Morgan	Blockchain Deposit Accounts on private permissioned blockchain (sometimes referred to as a tokenized deposit)	~$5B USD daily Launched in 2019
JPM Coin (JPMD) - Kinexys by JP Morgan	Deposit Token on public blockchain	Launched in Nov 2025

DEPOSIT TOKEN USE CASES

- Instant and programmable payments, enabling instant settlement with embedded logic. This can be beneficial for automated B2B payments, escrowless real estate transfers, automated recurring transfers (e.g., on-chain payroll), and programmable payments. Because deposit tokens can support high volume digital commerce, they can support the scalability of Web3 commerce and a variety of transaction forms at scale, including merchant and retail commerce, and supply chain and trade finance payments.
- Tokenized asset settlement can benefit from a reliable cash with deposit tokens, minimizing counterparty and settlement risks, while reducing capital requirements. This can be beneficial for bond, equity, and fund tokenization, trading of tokenized real-world assets (RWA), atomic settlement of digital securities, repo and securities lending with instant collateral movement, and FX settlement against tokenized currencies or deposits.
- Institutional DeFi, where deposit tokens provide a safe money leg within permissioned DeFi protocols that have passed KYC checks. This allows for a regulated version of solutions like institutional liquidity pools (e.g., FX, lending, repo), automated market makers (AMMs) for wholesale players, credit lines and collateralization based on smart contracts, and on-chain derivatives and structured products
- Automated treasury and management, where corporates can utilize deposit tokens to optimize liquidity, reduce trapped capital, and streamline a range of financial operations with smart contracts, such as 24/7 treasury sweeps, working capital, reconciliations and ERP integrations, and instant transfers across subsidiaries or groups within an organization.
- Interoperability, where deposit tokens can operate as a regulated and bank-issued component of a multi-rail digital money ecosystem, bridging stablecoins with traditional finance, cash instruments across various chains, wholesale settlement across networks, and providing a settlement layer for mixed CBDC and deposit token systems.

DEPOSIT TOKEN GROWTH TRENDS

- **Increased interest and pilots from institutions and banks**, with active experimentations of deposit token uses in areas like cross-border payments, conditional settlements, and yield optimization
- **Growing recognition of opportunities for deposit tokens** as a bridge between traditional banking and digital asset ecosystems
- **Increasing momentum of adoption alongside broader tokenization growth**, with the tokenized real-world asset (RWA) market surpassing $24B in on-chain value in 2025[95] and projections of $16T in RWA tokenization by 2030[96] as banks and asset managers continue to tokenize additional securities
- **Opportunities as a tokenized cash solution** to operate on expanding ledger-based payments infrastructure[97]
- **Improving regulatory and operational readiness** strengthening the infrastructure and business case for deposit tokens, with global regulatory developments for tokenization, blockchain, and digital assets, enabling banks to adopt these solutions.

DEPOSIT TOKEN CHALLENGES

- Despite strong growth, many deployments remain pilots except for a handful in full production, which may slow down scale. The market for deposit tokens has yet to mature and is primarily institutional.
- Relatively small size of overall deposit-token issuance compared to the broader financial system, indicating that large-scale adoption is still emerging.
- Scalability depends on addressing existing regulatory, operational, liquidity, interoperability and risk-management challenges
- While data often refers more broadly to tokenized deposits, which include deposit tokens, separating deposit tokens from larger tokenization trends and stablecoins can be difficult.

II) ECOSYSTEM VIEW OF DIGITAL MONEY

This section provides an ecosystem view of key stakeholders and their interactions. We start with an ecosystem table below, specifying the entities involved and their respective roles:

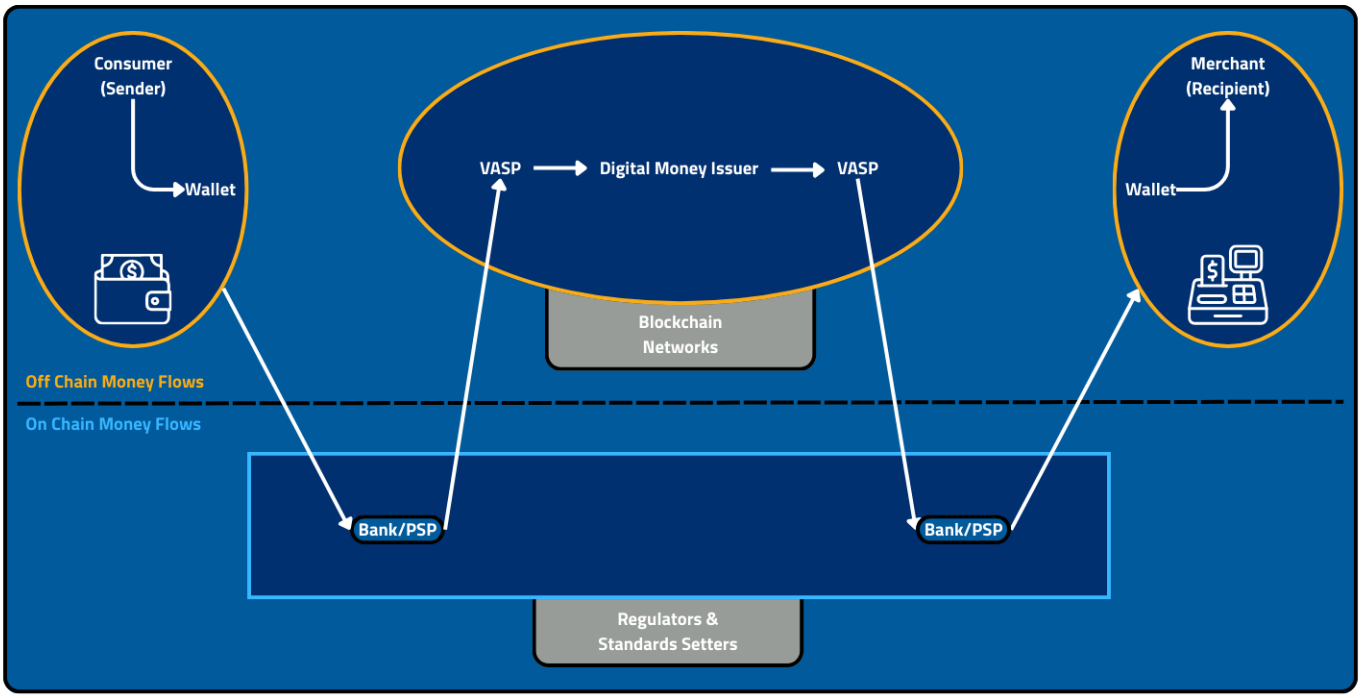
Key Stakeholders in Digital Money Ecosystem

Examples	Jurisdiction
Issuers of Digital Money	Create the digital asset/token used for payments
Wallets & Account Providers	• Enable users to hold digital money and make transactions • Wallets act as the interface into the blockchain space, with functions like key management • Wallets represent/act on behalf of users in the blockchain space
Banks & Payment Service Providers (PSPs)	Facilitate value transfers across entities and individuals
Blockchain Networks	Infrastructure to record and verify transactions
Virtual Asset Service Provides (VASPs)	On/Off Ramps, providing a bridge between traditional finance and digital assets
Merchants/users (end pt)	Accept payments with digital assets
Consumers/users (starting pt)	Make payments using digital assets
Regulatory Oversight/Authorities & Standards Setting Bodies	Ensure compliance with regulatory requirements, standards, and risk management practices

Although traditional and ledger-based scenarios may have a different set of key stakeholders, they share a common objective when it comes to payments functionality. While different infrastructure and different sets of stakeholders between ledger-based and traditional payment systems may define separate starting points with respect to operations, the common end goal of facilitating payments brings convergence.

Below is a generic use case of blockchain-based digital money for payments, illustrating the interactions between the key stakeholders. The digital money flows and key stakeholder interactions would be similar for all payments use cases of blockchain-based digital money, including e-commerce, in-store POS, B2B payments, and peer-to-peer (P2P) transfers – all payment flow models that can also be carried out with traditional systems.

Generic Model of Stakeholder Interactions using blockchain-based digital money

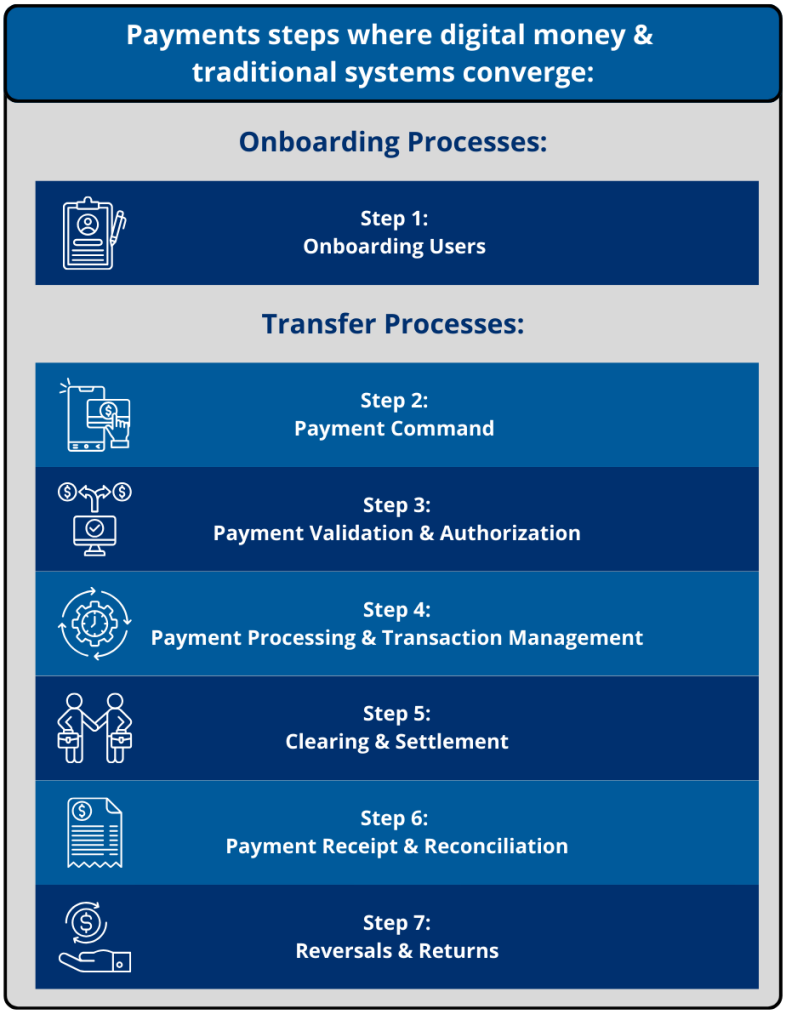


Ultimately, the activities performed to ensure a successful payment transaction, although carried out by different parties in the traditional and ledger-based scenarios, are similar in nature. Thus, the stakeholders involved in the blockchain-based digital money ecosystem take on similar roles as those in traditional payment arrangements. This becomes especially clear as regulations and risk management frameworks are put into place. With the broader regulatory approach of same activity - same risk - same regulation, we begin to observe the two worlds of traditional and ledger-based systems coming together.

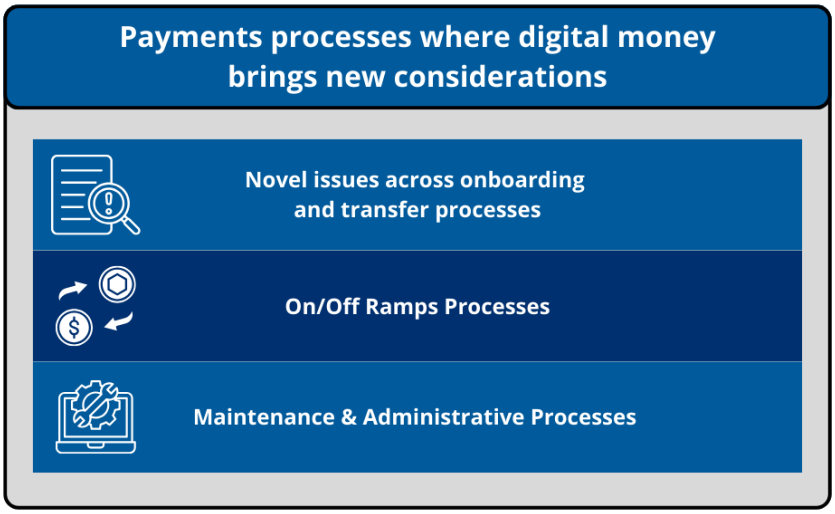
III) VALUE CHAIN OF PAYMENTS WITH DIGITAL MONEY

This section assesses the end-to-end flow of the payments process, from the steps required to complete a payment operation, to the processes involved. We evaluate the processes involved in the payments value chain using blockchain-based digital money. While many of these steps converge with traditional payment systems, there also arise novel issues. All these processes are subject to a series of regulatory requirements and standards – both for traditional payments and also blockchain-specific standards.

Convergence between traditional & digital money: As stated, prior, when regulatory requirements and risk mitigation frameworks are put into place, the payments process for blockchain-based digital money converges with traditional models. We find that many steps involved along the payments process for blockchain based digital money mirror the steps involved for traditional payments.



Novel Processes arising from blockchain-based digital money: Nevertheless, blockchain based digital money stills add certain novel issues for payment processes



Importance of Standards

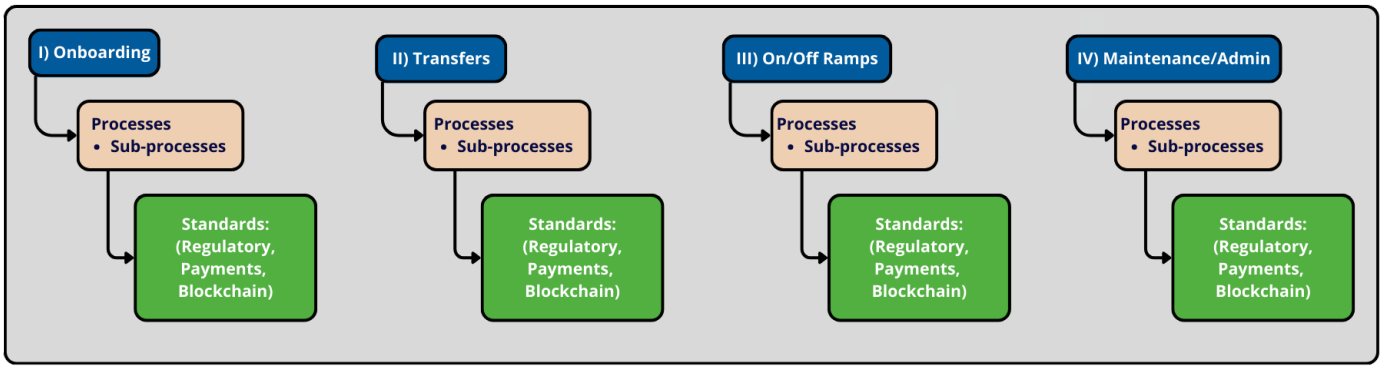
An end-to-end blueprint for payments – where each process is mapped out against relevant regulatory requirements and standards – is meant to help design a payment system architecture that is compliant with global standards for payments and data. A well-defined blueprint that identifies standardized requirements across every step of the payments value chain is meant as a useful tool to ensure interoperability, security, and scale, ultimately supporting the various payments use cases. With this intent, for each stage of the payments lifecycle, we highlight relevant standardized requirements that may take the form of regulatory requirements, payments standards and messaging protocols, and blockchain standardization efforts. This mapping can be a useful tool guiding how to build a system - specifically what standards to adhere to and best practices to ensure viability.

We note that for blockchain and digital assets, there have been substantial efforts toward standardization – a field that is mapped out in the Technical Standards GSMI report and Landscape. We highlight those standardization efforts that are relevant for payments, ranging from standards produced by globally recognized bodies which have gone through formal approval processes (e.g., ISO, IEEE, ITU-T), to industry-led standardization initiatives that have gained widespread adoption in the absence of more formal standards (e.g., ERC). Many of these are standardization approaches are for structuring payment tokens and their use, in addition to interoperability. For instance, existing token standards, which are crucial for settlement, must be shared between parties to ensure fund flows.

II.I) PROCESSES FOR DIGITAL MONEY PAYMENTS & STANDARDS

Below is a detailed end-to-end flow of specific processes involved in digital payments processing with blockchain-based digital money and the relevant frameworks (regulations and standards) for each step. The process map below categorizes payment processes according to the nature of payment activity (onboarding, transfers, on/off ramps, and maintenance/admin), and the identifies relevant existing standards. We note that processes may occur simultaneously, or get split up across the different steps of the payments lifecycle illustrated above. Rules may apply to the entire lifecycle or apply to certain stages or jurisdictions.

Processes Landscape*



**Note: Standards are listed below each overall process. Any exceptions or additions relevant to a specific process/sub-process are placed below that process/sub-process*

I) ONBOARDING: Registering users onto a payments platform

1.1) Onboarding Processes

1.1.1) KYC

- Identity Verification & Digital Identity
- Government ID & verification
- Biometric ID verification (e.g., you are who you say you are)
- Users provide basic data (e.g., address, email, phone number)

1.1.2) Account opening/Wallet creation

- Associate name in acct (connected to email/phone/govt ID, connected to key generated for acct) to info from KYC
- Verification levels as annotation to acct, allow user to do diff volumes of transactions based on KYC level

1.1.3) Key Generation (to enable transactions)

- Whitelisting after key is generated (allowing address to transact vs not)
- Providing digital identity to users

1.1.4) AML/CFT

- Source of funds verification
- Transaction Monitoring
- Screening & Reporting

1.2) Onboarding Standards

1.2.1) Legal & Regulatory

- EU Payment Services Directive (PSD2) - European open banking requirements[98]
- European Banking Authority (EBA) Guidelines - Various guidelines for several aspects of payment services, to enhance security, competition, and consumer protection[99]
- European Digital Identity Framework - framework for universal, trustworthy, and secure European digital identity, enabling creation of a digital identity wallet[100]
- EU Fifth Anti-Money Laundering Directive (AMLD5)[101] - AML/CFT regulations, addressing risks associated with virtual currencies
- FATF Recommendations[102]: AML and CFT procedures, including customer due diligence (CDD), with provisions for virtual currencies
- EU eIDAS (EU): Electronic identification and trust services; defines assurance levels for onboarding in the EU
- EBSI DID/Verifiable Credentials Framework - framework for expressing, exchanging, and verifying information
- Additional legal/regulatory requirements may depend on licensing requirements

1.2.2) Payment Standards

- ISO/IEC 29003: Guidelines for digital identity proofing, authentication, and validation.
- ISO 20022 - Standard for electronic data exchange between financial institutions. Includes standardized data structures for legal entity identifiers (LEIs)
- ISO 17442 (GLEIF) - Global Legal Entity Identifier (LEI) System to identify participants in financial transactions
- ISO 17442-3 (GLEIF) - verifiable Legal Entity Identifier (vLEI) for a digitally signed, tamper-resistant credential for decentralized authentication of legal entities
- ISO/IEC 29115 - Standard framework for managing entity authentication assurance
- NIST SP 800-63-3 (US): Digital Identity Guidelines NIST Levels of Assurance (LOA) - IAL1–3, AAL1–3 - Guidelines for digital onboarding

1.2.3) Blockchain Standards

- RMF: Risk Mitigation Framework (RMF)[103] – for non-financial risks of blockchain infrastructures
- IEEE standards on interoperability and payments
- IEEE 3205-2023 - IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol
- P3205/D5.0, Aug 2022 - IEEE Draft Standard for Blockchain Interoperability - Data Authentication and Communication Protocol
- P2143.3 - Standard for Risk Control Requirements for Cryptocurrency Payment (Under Development)
- P2048.202 - Standard for Security Specifications of Blockchain-Based Metaverse Data (key for payment security in metaverse)
- ITU-T: Study Group 17 (Security): Addresses DLT security, threats, frameworks, and guidelines for digital identity and payments. Standards include definitions (X.1400), security threats (X.1401), and security for digital payment services (X.1405).
- IETF: Network & Data Transport Layers[104] - RFC 8578 (DetNet Use Cases), including point-to-multipoint and low-latency transport suitable for blockchain traffic in deterministic networks

II) TRANSFERS: Sending funds across registered users

2.1) Transfer Processes

2.1.1) Payment Command

- Payment Instruction & Initiation
- Data Exchange
    - Blockchain Standards for Data Exchange
        - **IVMS101:** InterVASP Messaging standard providing common language for communication of required originator and beneficiary information between VASPs, focused on Travel Rule compliance.[105]
        - **TRUST (IEEE 2418.2-2020):** data format requirements for blockchain systems.[106]
        - **Notabene/Transaction Authorization Protocol (TAP):** Built on TAP, Notabene provides an open, interoperable messaging layer for pre-transaction authorization and compliance. TAP uses IVMS101.[107]
        - **ITU-T: Study Group 17 (Security):** Addresses DLT security, threats, frameworks, and guidelines for digital identity and payments. Standards include definitions (X.1400), security threats (X.1401), and
- AML/CFT (triggered after user initiates transfer)
    - Blockchain Standards for AML/CFT
        - **Notabene/Transaction Authorization Protocol (TAP):** Built on TAP, Notabene provides an open, interoperable messaging layer for pre-transaction authorization and compliance. TAP uses IVMS101.[108]
        - **ITU-T: Study Group 17 (Security):** Addresses DLT security, threats, frameworks, and guidelines for digital identity and payments. Standards include definitions (X.1400), security threats (X.1401), and security for digital payment services (X.1405).

2.1.2) Payment Validation & Authorization

- Payment Approval
- Payment Standards may not be relevant for Payment Validation & Authorization, as internal processes focus on regulatory compliance

2.1.3) Payment Processing & Transaction Management

- Internal operations by an entity or network for payment to go out
- Payment qualification
- Deposits & Withdrawals: Movement of funds between bank accounts and blockchain addresses (typically performed internally by a single entity)
- Sending of funds
- Receipt of funds
- Delegated transfers: authorized by 3rd parties including other smart contracts
- Alias-based transfers: Use easy to remember identifiers instead of wallet addresses
- Legal & Regulatory Requirements for Payment Processing & Transaction Management
    - Jurisdiction-specific stablecoin regulations - Jurisdiction-specific
    - Jurisdiction-specific taxation requirements, including capital gains taxes
- Payment Standards may not be relevant for Payment Processing & Transaction Management, as internal processes focus on regulatory compliance

2.1.4) Clearing & Settlement

- Atomic transactions
- Legal & Regulatory Requirements for Clearing & Settlement
    - **EU Settlement Finality Directive (SFD) –** designed to avoid systemic risk, ensuring transfer orders within systems become legally final and enforceable, even if a participant becomes insolvent
- Payment Standards for Clearing & Settlement
    - **ISO 20022 -** Standard for electronic data exchange between financial institutions. PACS.008 - ISO 20022 message for financial institution to financial institution customer credit transfers, crucial for cross-border payments
    - **SWIFT MT 103 -** customer payment message to transfer funds from one bank account to another
    - **SWIFT MT 202 -** bank-to-bank transfer message to transfer funds between financial institutions
    - **US NACHA File Format (ACH) -** standardized file format used for Automated Clearing House (ACH) transactions
    - **Single European Payments Area (SEPA) Clearing and Settlement Mechanisms (CSMs) -** payments are processed by CSMs as intermediaries between Payment Service Providers (PSPs), with settlement occurring between PSP accounts at the European Central Bank (ECB)
- Blockchain Standards for Clearing & Settlement
    - Existing token standards' (e.g, TTF, ERC-20 included in Transfers – Blockchain Standards list below) provisions for settlement require sharing data between parties

2.1.5) Payment Receipt & Reconciliation

- Deposit of funds into recipient wallet
- Confirmation of receipt of funds
- Legal & Regulatory Requirements for Payment Receipt & Reconciliation
    - Reconciliation of omnibus allocation - required for certain entities depending on the jurisdiction
    - AML regulations (included in Transfers- Legal & Regulatory Requirements list below) may require reporting source of funds, specifying those with greater AML risks

2.1.6) Reversals & Returns

- Identify principal custody
- Initiate new transaction to return funds - decision making and approval structures for "reversing" a validated transaction (e.g., usually request funds to recipient wallet, but in extreme cases a fork)
- Payment network rules and merchant policies may determine internal procedures
- Legal & Regulatory Requirements for Reversals & Returns
    - Requirements for Automated Clearing House (ACH) transactions including timeframes, reason codes to process returns, and formatting
    - Jurisdiction-specific consumer protection regulations for unauthorized transactions (e.g., UK Payment Services Regulations) and accurate reporting (e.g., US Fair Credit Reporting Act (FCRA))

- Payment Standards for Reversals & Returns
    - **ISO 20022 -** Standard for electronic data exchange between financial institutions. Includes standardized data structures for legal entity identifiers (LEIs)
    - S**WIFT MT & MX -** SWIFT messages, considering MX messages, built on ISO 20022, offer more structured and richer data that reduces ambiguity and facilitates greater automation for reconciliation
    - **National Automated Clearing House Association (NACHA) operating rules and return codes -** rules govern ACH Network, including return codes indicating why an ACH transaction may have been unsuccessful

2.2) Transfer Standards

2.2.1) Legal & Regulatory

- **FATF Travel Rule -** Requires sharing information about fund transfers, senders, and recipients, including those involving crypto assets
- **EU Wire Transfer Regulation (WTR) –** For EU compliance with the Travel Rule
- **EU Payment Services Directive (PSD2)[109] -** European open banking requirements
- **European Banking Authority (EBA) Guidelines[110] -** Various guidelines for several aspects of payment services, to enhance security, competition, and consumer protection.
- Additional legal/regulatory requirements may depend on licensing requirements

2.2.2) Payment Standards

- **ISO 20022 -** Standard for electronic data exchange between financial institutions. Includes standardized data structures for legal entity identifiers (LEIs)
- **SWIFT MT 101 & MX -** SWIFT message type to request transfers of funds, considering MX messages are built on ISO 20022, which offers more structured and richer data that reduces ambiguity and facilitates greater automation for reconciliation, such that ISO 20022 compliance most likely leads to SWIFT compliance by default
- **Single European Payments Area (SEPA) Credit Transfer (SCT) -** electronic funds transfers between bank accounts within the SEPA region
- **Single European Payments Area (SEPA) TARGET Instant Payment Settlement (TIPS) -** Extension for instant retail payments

2.2.3) Blockchain Standards

- IEEE standards on interoperability and payments
    - **IEEE 3205-2023 -** IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol
    - **P3205/D5.0, Aug 2022 -** IEEE Draft Standard for Blockchain Interoperability - Data Authentication and Communication Protocol
    - **2143.1-2020 -** IEEE Standard for General Process of Cryptocurrency Payment
    - **P2143.2 -** Standard for Cryptocurrency Payment Performance Metrics (Under Development)
    - **P2143.3 -** Standard for Risk Control Requirements for Cryptocurrency Payment (Under Development)
    - **P3272.01 -** IEEE Standard for Blockchain Based Stablecoins Payment Service

Requirements
    - Survey on Blockchain-based IoT Payment and Marketplaces
    - **P2048.202 -** Standard for Security Specifications of Blockchain-Based Metaverse Data (key for payment security in metaverse)
    - **IEEE P2145 -** Standard for Framework and Definitions for Blockchain Governance
- IETF
    - **Network & Data Transport Layers[111] -** RFC 8578 (DetNet Use Cases), including point-to-multipoint and low-latency transport suitable for blockchain traffic in deterministic networks
- **Secure Asset Transfer Protocol (SATP) & Interoperability Drafts[112] -** intended to standardize secure movement of digital assets across blockchain networks through API gateway architectures
- **Token Taxonomy Framework (TTF) -** for token design and issuance, designed to improve interoperability
- **ERC Standards -** focus largely on token standards and functionality
    - *ERC-20* – standard set of functions for fungible tokens, transfers, and delegated transfers. Relevant for account-based ledgers and setting a foundation for other standards
    - *ERC-721* – NFTs
    - *ERC-777* – Enhanced functionality over ERC-20
    - *ERC-1155* – Multi-token standard, supporting single and batch transfers, introducing operator approvals for delegated transfers
    - *ERC-1400* – Security tokens, and tokenizing traditional financial assets, allowing delegated transfers with compliance checks
    - *ERC-3643* – Permissioned token standard focused on compliance & transfer, relevant for security tokens. Enhanced version of ERC-20 model with additional compliance verifications. Supports on-chain identities.
    - *ERC-865 (proposed)* – Simplifying token transfers through fees embedded in the transferred token itself to reduce frictions
    - *ERC-4337* – facilitates delegated transfers and account-abstraction functionalities
- **Interledger Protocol -** Interoperability for cross-ledger payments
- **Risk Mitigation Framework (RMF)[113] –** for non-financial risks of blockchain infrastructures

III) ON/OFF RAMPS: Converting funds between fiat and blockchain-based digital money

3.1) On/Off Ramp Processes

1. **Fiat side: Reserve management**
2. **Blockchain side: Issuance & destruction of tokens**
    - Minting tokens
    - Burning tokens
3. **Reconciliation of blockchain side against fiat side**
    - Reconcile mint/burn against on chain tokens

3.2) On/Off Ramp Standards

3.2.1) Legal & Regulatory

- Regulatory requirements under development, as this is an emerging space

3.2.2) Payment Standards

Payment standards under development, as this is an emerging space

3.2.3) Blockchain Standards

- Token standards
    - Token Taxonomy Framework (TTF): for token design and issuance, designed to improve interoperability
    - ERC-20
- Risk Mitigation Framework (RMF)[114] – for non-financial risks of blockchain infrastructures
- IEEE standards on interoperability and payments
    - IEEE 3205-2023 - IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol
    - P3205/D5.0, Aug 2022 - IEEE Draft Standard for Blockchain Interoperability - Data Authentication and Communication Protocol
    - P2048.202 - Standard for Security Specifications of Blockchain-Based Metaverse Data (key for payment security in metaverse)
    - IEEE P2145 - Standard for Framework and Definitions for Blockchain Governance

IV) MAINTENANCE/ADMIN: Support processes to ensure adequate functions throughout, including governance, administrative controls, and privileged functions

4.1) Maintenance/Admin Processes

4.1.1) Accounting Ledger

- View activities from processes above
- Track and update records of balances
- **Blockchain Standards for Accounting Ledger**
    - *ERC-20 (for account based)*
    - *ERC-721: (for fixed denomination)*
    - *E-cash for fixed denomination tokens*

4.1.2) Remuneration

- Calculation, accrual, and crediting of returns
- DeFi functionalities to calculate interest may apply

4.1.3) Deposits & Withdrawals

- Allow movement of funds between accounts and blockchain addresses

4.1.4) Permissioning

- Manage permission levels for administrative access
- Allow permissioned transfers, with underlying rules to approve or deny token transfers
- **Blockchain Standards for Permissioning**
    - *ERC-1400: transfer restrictions and regulatory compliance for permissioned transfers*
    - *ERC-3643: On chain ID verifications and whitelist controls*
    - *ERC-6997: Adds transaction validation step to ERC-721*

4.1.5) Payment Information: Collection & Communication

- **Blockchain Standards for Payment Information**
    - *ERC-735: allows third parties to issue claims about a specific identity*
    - *ERC-3643: enables off chain rule specification on an on chain registry*

4.1.6) Federated Access Control: Trusted entities can enforce policies for token access

- **Blockchain Standards for Federated Access Control**
    - *ERC-1400: Access control can be part of compliance framework*
    - *ERC-3643: Allows multiple trusted entities to manage and enforce policies for access over token transfers*
    - *ERC-6617: Bit-based permissioning scheme*
    - *EIP-7820: Allows standardized access control registry*

4.1.7) Key Rotation & Account Recovery: Allow users to update keys or recover accounts in cases of lost keys

- **Blockchain Standards for Key Rotation & Account Recovery**
    - *ERC-1400: Partial key recovery support*
    - *ERC-3643: Enables key recovery and rotation mechanisms for regulated assets, integrated with on-chain identity*

4.1.8) Enabling/disabling of accounts

- Freezing tokens and seizing tokens under specified conditions

4.1.9) Pausing Transactions

- **Blockchain Standards for Pausing Transactions**
    - *ERC-3643: Includes functions to pause/suspend transactions in case of emergency*
    - *OpenZeppelin Pausable Function: Smart contract module allowing a smart contract to halt critical functions temporarily*

4.1.10) Smart contract upgrades

- Upgrading token logic
- **Blockchain Standards for Smart Contract Updates**
    - *ERC-1882: Upgrade path with minimal and efficient means*
    - *ERC-2535: Diamond Standards, specifically engineered for modular upgrades*
    - *ERC-3643: Allows updates to contract logic without disrupting token balances*

4.1.11) Gasless Transactions

- Allowing third parties to cover gas fees on behalf of users
- **Blockchain Standards for Gasless Transactions**
    - *ERC-3009: Allows third parties to submit authorized transactions and pay gas fees*
    - *ERC-4337: decentralized entities can sponsor gas fees for bundled transaction object*

4.2) Maintenance/Admin Standards

4.2.1) Legal & Regulatory

- Regulatory requirements under development, as this is an emerging space

4.2.2) Payment Standards

- Payment standards under development, as this is an emerging space

4.2.3) Blockchain Standards

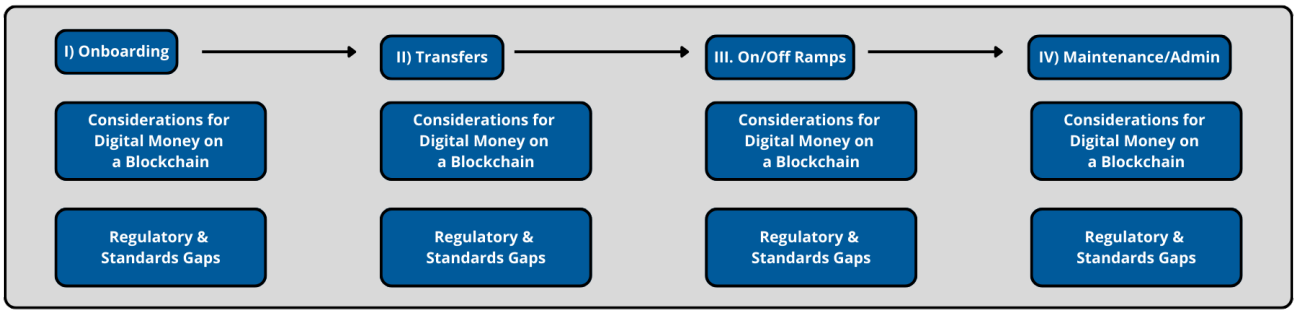
- Token standards
    - *Token Taxonomy Framework (TTF) - for token design and issuance, designed to improve interoperability*
    - *ERC-20*
- Risk Mitigation Framework (RMF)[115] – for non-financial risks of blockchain infrastructures
- IEEE standards on interoperability and payments
    - *IEEE 3205-2023 - IEEE Standard for Blockchain Interoperability Data Authentication and Communication Protocol*
    - *P3205/D5.0, Aug 2022 - IEEE Draft Standard for Blockchain Interoperability - Data Authentication and Communication Protocol*
    - *IEEE P2145 - Standard for Framework and Definitions for Blockchain Governance*
    - *P2048.202 - Standard for Security Specifications of Blockchain-Based Metaverse Data (key for payment security in metaverse)*
    - *IEEE P2145 - Standard for Framework and Definitions for Blockchain Governance*

III.II) DEEP DIVE INTO NEW CONSIDERATIONS

Digital money introduces novel issues across each stage of the payments lifecycle. In assessing the payments lifecycle for digital money, we identify these new considerations for blockchain-based digital money and existing gaps in regulations and standards. With a wide variety of different senders and recipients, alongside different standards that may apply to apply to various stages of the payments lifecycle, we identify areas where there may be no clear standards for payments with digital money.

These are issues where the industry needs to come together beyond the existing standards to agree on harmonized rules for payments. While many of these novel issues, especially where there may be gaps in regulatory requirements and global standards, are already being addressed by the industry, there is still a need for greater harmonization.

New Considerations for Digital Money and Existing Regulatory & Standards Gaps



I) ONBOARDING

- Considerations for Blockchain Based Digital Money
  - AML/CFT may be carried out differently in the context of tracing flows of funds on a blockchain. There may be use of a plugin (e.g., Chainalysis/Elllyptic), which requires ensuring the plugin works and integrations with the right wallets, senders/recipients, and any other relevant entities.
  - For AML, depending on backside of any bank connections, there may be a principal bank omnibus account or 3rd party banks that can make deposits or withdrawals
  - KYC for onboarding may be conducted in various forms, requiring use of an SDK or other internal processes
  - Digital identity is fundamental for decentralized transactions to take place - both for individuals/entities; and for funds, whether they be digitally native or representations of fiat funds on a blockchain

- Regulatory & Standards Gaps
  - Identity standards, which consist in proving the identity of individual sand entities, may fall largely outside the scope of payments. There are several digital identity standards globally and various national identity models (e.g., Aadhaar - API based electronic KYC framework for biometric-based ID verification), some of which may provide KYC frameworks for secure identity verification
  - AML/CFT/KYC & DID - mostly set requirements for traditional rails
  - Gaps around wallet initialization requirements
  - Gaps around custody requirements

II) TRANSFERS

- Considerations for Blockchain Based Digital Money
    - US Fed's FedNow Integration with ISO[116]: FedNow instant payment service (launched in July 2023) uses the ISO 20022 messaging standard. Standardization facilitates interoperability between payment systems and supports integration for blockchain-based payment solutions.
- Regulatory & Standards Gaps
    - ISO is highly rigorous and specialized, in ways that may not translate to transactions with tokens. ISO is meant to be broad, capturing varied scenarios, but the nested structure becomes complex and challenging to apply to blockchain-based digital money models.
    - SWIFT messaging standards (MT standards and updated MX standards) are aligned to ISO 20022, such that compliance with ISO also implies compliance with SWIFT. The same challenges to apply to digital money tokens apply.
    - European open banking messaging standards are also envisioned for traditional banking models, requiring nuance for application to blockchain-based digital money
    - Regulatory requirements are yet to be harmonized
    - Adherence to standards that may remain as blockchain industry initiatives
    - Absence of risk reporting requirements
- **Additional considerations specific to processes for payment transfers below**

2.1) Payment Command

- Considerations for Blockchain Based Digital Money
    - Peer to peer vs. intermediation
    - Additional legal/regulatory requirements may depend on licensing requirements

2.2) Data Exchange

- Considerations for Blockchain Based Digital Money
    - Format in which to exchange data
    - Privacy considerations and best practices (e.g., not sharing PII on chain)
    - Separate avenues to share confidential data vs what can be shared on chain
    - Data flows determine the ability to perform authorizations for payment operations using digital money. First, it is fundamental to identify what players are communicating with each other, understanding the business logic of any payments process using digital money. Second, it is necessary to identify how these players are communicating (e.g., over APIs, on a blockchain), and if existing standards are applicable for these communications (e.g., API connectivity structured according to ISO 20022).
    - For instance, VASPs need data (e.g., sufficient funds checks, economic activity correlations) to apply controls they are obliged to perform. Exchanging data and communicating with other VASPs can increase frictions, due to the need for separate off-chain networks to exchange confidential information.

        - Some VASPs have addressed this issue by developing trust networks that simplify the required exchange of data.
        - Reporting is contingent upon VASP internal risk analyses. This can raise concerns in light of the Travel Rule under FATF recommendations, which requires senders and recipients to share data. Payment information must always go from the sender to recipient financial institution. Yet certain jurisdictions may have a threshold under which these rules may not apply. Therefore, there can be cases where senders may not release tokens to recipients when the required data is not available, and other cases where there fund transfers may take place with no need for the data sharing (e.g., raising concerns for EU customers where Travel Rule requirements are clearly specified).
- Standards Gaps
    - Standards for many blockchain-based privacy preserving tools may remain as industry initiatives, prior to recognition by globally recognized standards setters

2.3) AML/CFT

- Considerations for Blockchain Based Digital Money
    - Format to share data and privacy considerations

2.4) Payment Validation & Authorization

- Considerations for Blockchain Based Digital Money
    - Payment approval may not be carried out by a centralized party and may be automated with a smart contract based on pre-set conditions
    - Travel Rule considerations in the context of exchanges, decentralized infrastructure
    - Jurisdiction specific requirements may vary
    - The greatest focus at this stage is to adhere to regulatory requirements, highlighting the importance of internal processing to remain compliant. Standards other than regulation become less relevant.

2.5) Payment Processing

- Considerations for Blockchain Based Digital Money
    - Smart contract considerations for automated payments (e.g., conditions for payer to have funds and recipient to have an adequate wallet to receive them)
    - Considerations for fund transfers between centralized and decentralized systems
- Standards Gaps
    - Payment processing involves multiple internal processes, where regulatory requirements for risk mitigation may precede technical standards. Payment routing to determine the optimal path for funds to travel from payer to recipient may no longer be relevant for digital money over p2p and disintermediated transfers.

        - There are no harmonized requirements to address smart contract vulnerabilities
        - Authorized forms of digital money to carry out transactions may be unclear (e.g., in Japan it's illegal to use stablecoins that are not authorized (e.g., USDT), but there are no sanctions if people do use these stablecoins)

2.6) Clearing & Settlement

- Considerations for Blockchain Based Digital Money
    - Digital money operates outside the traditional 2-tiered model of money, where clients of different banks can settle on central bank money. For digital money, atomic settlement combines both clearing and settlement into a single operation. There is no central bank behind transacting parties to enable fungibility between different forms of money, which highlights the importance of interoperability (e.g., exchanging between stablecoins and CBDCs).
- Standards Gaps
    - In the traditional banking model, central banks provide a public good by enabling fungibility across parties to exchange currencies. Local fiat money exchanges are generally standardized across local payment networks.
    - For digital assets, FX considerations among different currencies are an area in need of standardization. For instance, liquidity pools may use external exchange rates, while other parties may use internal exchange rates. Exchanging between currencies may result in spreads and earnings. Certain payment solutions may have plugins to omnibus accounts with access to several forms of digital money, including fiat-based models that operate on SWIFT and ACH networks.
    - This becomes an issue with economic implications.

2.7) Payment Receipt & Reconciliation

- Considerations for Blockchain Based Digital Money
    - While traditional models involve internal bank processes to carry out reconciliations in compliance with standards (e.g., linking payment receipts with bank entries, requirements for automating reconciliations), digital money introduces novel issues for depositing funds directly into recipient wallets.
    - Architecture of payment infrastructure impacts reconciliation of user funds (e.g., using omnibus on/off ramp accounts vs. sending funds directly to individual wallets).
- Standards Gaps
    - For digital money using blockchain, it has become a best practice to utilize forensics tools designed for blockchain fund transfers, to track and trace funds, which allow filtering & analyzing the source of funds
    - For funds sent directly to user wallets, there is an expectation for them to pass AML requirements, but they may not need to reconcile with omnibus accounts and subaccounts.
    - For funds sent to wallets/exchanges that utilize omnibus accounts, there's an expectation for omnibus account allocations to credit users' individual wallets

- In the absence of risk reporting requirements, certain players have developed a wallet network-based approach to segregate funds by risk, where funds that trigger higher risks are sent to certain designated wallets, or in an omnibus structure, to sub wallets categorized by AML that are segregated from both main omnibus funds and users.

2.8) Reversals & Returns

- Considerations for Blockchain Based Digital Money
  - From a rulebook perspective, VASPs can be treated as intermediaries in traditional payments systems
  - From a technical perspective, reversing a payment would not cancel the original payment but add a new payment
  - From a legal perspective, if funds were sent to the wrong address (either by mistake or maliciously), there are usually structures to compel the recipient to return the funds (e.g., suing if needed), along with operational processes to perform the reversal. In a decentralized structure, however, it may be unclear whom to target (e.g., the network deciding to unwind funds, the recipient, the wallet, etc.)
  - Transactions between self-hosted wallets, however, add complex challenges and uncertainties. When users maintain their own wallet, hosted within a multi-party computation system (MPC) in a co-hosting application, the wallet's host maintains the ability to send funds back to the source (e.g., AML reasons or other motives). This brings considerations regarding governance structures
  - Considerations around self-hosted, custodial wallets
  - Governance structures and clawback features to make unwinding a possibility
- Standards Gaps
  - Need for agreement to develop standards - by token, by VASP, etc.
  - While ERC-20 has no reference code, transaction codes may be a possibility for on-chain settlement

III) ON & OFF-RAMPS

- Considerations for Blockchain Based Digital Money
  - Compliance with regulations & standards (payments & blockchain)
- Standards Gaps
  - Globally recognized standards and regulatory frameworks are still in development

IV) MAINTENANCE/ADMIN

- Considerations for Blockchain Based Digital Money
    - Decentralized governance
    - Most processes are specific to blockchain infrastructure
- Standards Gaps
    - Accounting Ledger: No standards to record UTXO form on EVM
    - Remuneration: No standard or widely adopted practice
    - Collection & communication of payment information with banks: No standard exists for this feature
    - No adequate standards for enabling/disabling accounts
    - Globally recognized standards and regulatory frameworks are still in development

III.III) ADDRESSING REGULATORY & STANDARDS GAPS

The gaps in existing frameworks must be addressed to respond to the novel issues introduced by blockchain based digital money. We expect that as standards and regulatory requirements continue to develop, existing gaps will be addressed, and the blockchain-based digital money payments space will continue to converge with the traditional payments structures and approaches.

We find that most of the regulations and payments standards are envisioned for traditional payments architectures. Regulations are under development for blockchain and digital assets, while existing payment standards have yet to incorporate blockchain infrastructure considerations. Even among blockchain-based standards, there are elements in the digital money payments process that may not be covered. For instance, there are no clear standards for digital assets when it comes to clearing & settlement. While certain token standards may be applicable for settlement, requiring information sharing between parties, their applicability requires nuance.

Addressing standards gaps is especially important for processes related to on/off ramps, and for maintenance/governance, which raise novel issues almost in their entirety. In the absence of regulations and payments standards, blockchain standards specific to many of payment processes have arisen and gained significant adoption to harmonize practices. This is a space where blockchain standards may drive the development of mandatory regulations and formal payment standards in the future.

IV) REGULATORY DEVELOPMENTS FOR DIGITAL MONEY

Below is a global mapping of major regulatory developments relevant for blockchain-based digital money models we cover across this report. While stablecoins and deposit tokens are mapped against regulatory developments from major jurisdictions that have released requirements for blockchain and digital assets, CBDCs are subject to regulatory framework in their respective issuing countries. Therefore, CBDCs are not the focus the major global jurisdictions in the same way as stablecoins and deposit tokens, especially as none of the selected major jurisdictions below has yet launched a CBDC solution in production.

In order for payments solutions using blockchain based digital money to be seamless at a global level, digital money should be fungible across jurisdictions. For instance, a stablecoin that falls under a certain regulatory regime in one jurisdiction should be treated in a similar way under a separate regulatory regime for its adoption in another jurisdiction. In many cases, regulatory requirements may be specific to a token, but more commonly they apply to the entities engaging activities with these tokens (e.g., designated as VASPs or CASPs depending on the jurisdiction) – in line with the common practice to regulate the activity over the technology. There exist certain gaps for the seamless interoperable fungibility to occur today, especially when it comes to digital money models that are not fiat-backed. These forms of digital money generally don't fall under stablecoin-specific rules. Moreover, whether requirements which would apply for CBDCs may or may not be aligned with the frameworks above is yet to be determined.

Generic landscape of regulatory requirements for digital money

Digital Asset	Issuer/ Type	United States	EU (MiCA)	UK	Singapore	Hong Kong	Japan
Stablecoin	Private company / fiat-backed	• Compliance with GENIUS Act required to offer to US users for federal issuers • State regulators (e.g., NYDFS) for state-chartered issuers • AML/KYC (OFAC)	Electronic Money Institution (EMT) authorization required to offer to EU users	FCA authorization expected for fiat-redeemable stablecoins under UK regime when live	MAS SCS issuer license required, else falls within the DPT regime	HKMA FRS stablecoin issuer license required to offer to HK retail users. Professional investors and institutions can access non-HK stablecoins under the SFCs virtual asset regime	Distribution allowed only via licensed intermediaries; issuance restricted to banks/trusts/ FTSPs
CBDC	Central Bank / retail CBDC	• Issued and regulated by the Central Bank of the country issuing the respective fiat currency. • AML/CFT/KYC requirements, which financial institutions involved with the CBDC must adhere to					
CBDC	Central Bank / wholesale CBDC	• Issued and regulated by the Central Bank of the country issuing the respective fiat currency. • AML/CFT/KYC requirements, which financial institutions involved with the CBDC must adhere to					

Digital Asset	Issuer/ Type	United States	EU (MiCA)	UK	Singapore	Hong Kong	Japan
Deposit Token	Banking Institution / Deposit Token	Falls under the existing regulatory framework for commercial banks, including bank-specific prudential regulations, deposit insurance requirements, AML/KYC requirements, and compliance and internal procedures. Oversight includes U.S. federal and state banking and securities regulators, the Federal Reserve, the Office of the Comptroller of the Currency (OCC), and the U.S. Treasury Department's Office of Foreign Assets Control (OFAC)	Issuing banking institution authorization required or partnership with authorized entity under MiCA to offer deposit token in the EU, alongside specific requirements (e.g., reserves, liquidity, transparency disclosures, consumer protections)	Oversight under either the Financial Conduct Authority (FCA) or a dual regime with the Bank of England (BoE), depending on whether it's deemed "non-systemic" or "systemic" respectively.	• Oversight under the Monetary Authority of Singapore (MAS), and regulated under existing banking laws (Banking Act). They are distinct from the stablecoin regulatory framework, which applies to non-bank issued single currency stablecoins • Deposit tokens may fall within the ambit of digital payment tokens under the Payment Services Act 2019 depending on how they are structured and used	• Deposit tokens are treated as bank liabilities, falling under existing banking regulation • The Hong Kong Monetary Authority (HKMA) is actively developing regulations for deposit tokens through Project Ensemble, under the pilot EnsembleTX	• Regulated under the Payment Services Act (PSA), which established a framework for electronic payment instruments and stablecoins • Deposit tokens are treated as a form of electronic payment instrument if they represent a claim against a licensed bank. The PSA ensures stringent rules around issuance, reserve management, and segregation of funds.

IV.I) RECENT REGULATORY TRENDS FOR STABLECOINS

US

In the US, regulatory requirements must meet federal requirements and any relevant state-specific requirements, out of which we highlight NYDFS rules as a state that has released substantial guidance. While the U.S. has been a relatively fragmented in its approach, 2025 has shown a massive leap forward. The passage of the Guiding and Establishing National Innovation for U.S. Stablecoins Act, or the GENIUS Act, is a monumental achievement. After years of legislative debate, this law finally provides a clear federal framework for payment stablecoins. It codifies what much of the industry has been advocating for: a requirement for 100% reserve backing in cash or cash equivalents, regular public attestations from a third-party auditor, and clear redemption rights. The US GENIUS Act introduces a licensing framework where only approved Permitted Payment Stablecoin Issuers (PPSIs) can issue U.S.-pegged stablecoins, and must fully back them with high-quality liquid assets (e.g., T-bills), segregate reserves, avoid rehypothecation, and undergo monthly attestations.

Critically, it gives both federal and state regulators a clear mandate to oversee these assets, removing the regulatory ambiguity that has stifled innovation for so long. The GENIUS Act signals that the U.S. is serious about maintaining its role as a leader in financial innovation, and it provides a clear path for compliant issuers like Ripple to operate with confidence.

EU

The EU's Markets in Crypto-Assets regulation, or MiCA, is a landmark piece of legislation. It's the most comprehensive framework in the world for digital assets, and in some ways it can be a model for other jurisdictions. MiCA's approach to stablecoins is particularly robust. It creates two distinct categories:

- Asset-Referenced Tokens (ARTs): Stablecoins backed by a basket of currencies or assets.
- E-Money Tokens (EMTs): Stablecoins pegged 1:1 to a single fiat currency, like the euro or dollar.

For both, MiCA mandates stringent requirements. Issuers must be authorized by a competent authority, maintain full reserves of high-quality liquid assets, and publish transparent whitepapers and regular audit reports. For "significant" stablecoins - those with a large market cap and transaction volume over defined thresholds - the rules become even stricter, with enhanced supervision from the European Banking Authority.

This is a game-changer. It provides a clear legal pathway for compliant issuers and a high degree of confidence for institutional and retail users.

UK

The United Kingdom is also moving quickly, with new legislation aiming to bring stablecoins into its existing payments and e-money regulations. The focus is on fiat-backed stablecoins used for payments, with a phased approach to bring other crypto assets into the fold later.

Singapore

The Monetary Authority of Singapore has also finalized its regulatory framework, introducing a new "MAS-regulated stablecoin" label for Single Currency Stablecoins pegged to the SGD and G10 currencies. Issuers must meet stringent reserve, capital, and disclosure requirements to use this label, providing a clear seal of approval for users.

Hong Kong

In Hong Kong, the Hong Kong Monetary Authority has created a sandbox for stablecoin issuers, which allows issuers to experiment in a controlled environment with regulatory oversight until licenses for Fiat Referenced Stablecoins (FRS) are issued.

Japan

In Japan, authorities have long held a forward-looking stance, recently amending their Payment Services Act to regulate stablecoins. Only licensed banks, trust companies, and fund transfer agents can issue them, and they are required to hold reserves and ensure par redemption.

UAE

UAE regulators have introduced frameworks that support both fiat-backed stablecoins and tokenized assets, with an eye toward interoperability.

IV.II) RECENT REGULATORY TRENDS FOR CBDCs

US

The United States has taken an approach favoring stablecoins as the preferred form of digital money, with implications on the use of the US Dollar as the most popular reserve currency. With respect to CBDCs, a 2025 executive order essentially banned them by prohibiting federal agencies from taking action to create or promote a US CBDC, due to concerns regarding financial stability, privacy, and government overreach. The stance reverses previous research efforts and remains in contrast with other jurisdictions' trends exploring CBDCs.

EU

The EU is expected to release a Digital Euro, favoring a CBDC model over stablecoins. Stablecoins may be perceived as a less approachable option for banks due to a high deposit percentage requirement under current regulations.

UK

The UK is cautiously proceeding into, with the government and the Bank of England (BoE) in exploratory phases to assess the potential to introduce a digital pound CBDC.

Singapore

Singapore has a progressive regulatory stance toward CBDCs, focusing on a wholesale CBDC model for interbank settlements, and stating no immediate need for a retail CBDC model. The Monetary Authority of Singapore (MAS) has been actively involved in tests involving wholesale CBDCs and tokenized assets, with collaborative initiatives across jurisdictions including Project Ubin[119] and Project Guardian[120].

Hong Kong

The Hong Kong Monetary Authority (HKMA) has an active and progressive stance toward CBDCs, having led research and pilot programs since 2017 toward the development of a retail and wholesale model of an e-HKD. This CBDC is part of Hong Kong's endeavors to position itself as a digital finance hub.

Japan

Japan has a highly cautious approach, with the Bank of Japan (BOJ) stating no immediate plans to issue a digital yen CBDC despite being actively involved in research and pilot programs that would prepare for a potential future issuance. The country's high cash usage is recognized as a factor in the decision to evaluate a CBDC with caution.

China

China is actively developing and promoting its digital yuan (e-CNY), state control over its digital currency while maintaining strict controls the use of over other digital assets including cryptocurrencies. The e-CNY is being used for extensive pilot programs across various sectors, ranging from retail payments to public services.

IV.III) RECENT REGULATORY TRENDS FOR DEPOSIT TOKENS

US

Deposit tokens fall under the existing regulatory framework for commercial banks, including bank-specific prudential regulations, deposit insurance requirements, AML/KYC requirements, and compliance and internal procedures. Oversight includes U.S. federal and state banking and securities regulators, the Federal Reserve, the Office of the Comptroller of the Currency (OCC), and the U.S. Treasury Department's Office of Foreign Assets Control (OFAC)

EU

In the European Union (EU), the Markets in Crypto-Assets (MiCA) Regulation provides a detailed framework for stablecoins, but deposit tokens issued by licensed credit institutions are generally excluded from MiCA's requirements for Electronic Money Tokens (EMTs) and Asset-Referenced Tokens (ARTs), remaining under the established banking regulatory perimeter.

UK

Similarly, the United Kingdom (UK) treats bank-issued deposit tokens as traditional bank liabilities, with the Bank of England (BoE) focused on managing the potential systemic risk of deposit outflows to digital monies, particularly those associated with the ongoing Tokenised Sterling Deposits industry pilot

Singapore

In Singapore, the Monetary Authority of Singapore (MAS), regulates deposit tokens under existing banking laws (Banking Act). They are distinct from the stablecoin regulatory framework, which applies to non-bank issued single-currency stablecoins. However, deposit tokens may fall within the ambit of digital payment tokens under the Payment Services Act 2019 depending on how they are structured and used.

Hong Kong

In Hong Kong, the Hong Kong Monetary Authority is actively exploring tokenized deposits through initiatives like Project Ensemble, which is testing the use of tokenized deposits alongside a potential CBDC. Deposit tokens are treated as liabilities of Authorized Institutions (AIs), requiring them to comply with all existing banking and consumer protection standards.

Japan

Japan regulates tokenized deposits as a form of Electronic Payment Instrument (EPI) under the Payment Services Act (PSA), allowing licensed banks and trust companies to issue them, with strict rules on 1:1 reserve backing and segregation of funds.

V) CONCLUSION

Future considerations for payments systems using stablecoins, CBDCs, and deposit tokens as digital money will rely on current developments in regulatory frameworks and standards. Regulatory clarity, including consumer protections, will continue to evolve with rules specific to each form of digital money, and provisions for liability and accountability in the case of unwanted events. Payment systems will therefore require rails harmonized with these regulatory and standards developments.

While the United States has clearly taken a stance favoring stablecoins – particularly supporting regulatory clarity for USD-backed stablecoins, other jurisdictions - notably the EU - favor CBDC models which may compete with stablecoins. This may lead to a future where privately issued and sovereign issued forms of money compete and coexist and create new economic dynamics.

As blockchain rails converge with traditional rails, we're heading toward a global multi-rail world where deposit tokens, public or private stablecoins, and one or multiple CBDCs will coexist. Payment systems will require interoperability layers so a user can pay in one form (e.g., stablecoin) and a merchant can receive in another (e.g., CBDC or deposit token). Future payment systems will look more like routers/orchestration layers than single monolithic rails.

RECOMMENDATIONS

1. Harmonize Regulatory Frameworks Across Jurisdictions to minimize fragmentation, promote seamless global payments, and enable fungibility of digital money across markets

- Mutual recognition of compliant fiat-backed digital money should be treated equally
- Convergence toward the "same activity, same risk, same regulation" approach should ensure equivalent oversight for equivalent payment functions
- Alignment of travel rule, AML/CFT, and licensing standards to support cross-border interoperability

2. Establish Clear Standards for On/Off-Ramps, closing standards gaps to support compliance and minimize fragmentation

- Globally accepted requirements for minting/burning, reserve reconciliation, reporting, and transparency
- Uniform requirements for reserve audits, liquidity management, and segregation of funds across issuers

3. Standardize a Digital Identity layer and KYC for Blockchain-Based Payments for greater portability, privacy, and compliance

- Integrate digital identity credentials (e.g., vLEI, national ID systems, KYC frameworks) with wallet onboarding
- Adopt privacy-preserving identity models compatible with AML/CFT, avoiding on-chain PII and enabling verifiable compliance
- Wallet initialization standards (e.g., whitelisting, verification tiers, and key-management requirements)

4. Develop Interoperability Frameworks Across Digital Money Types, preparing for a multi-rail world where many forms of money will interoperate (e.g., payer sends one form of digital money and receiver can receive another)

- Implement interoperability bridges and secure asset transfer protocols (e.g., SATP, IEEE interoperability standards)
- Support atomic settlement across money types, especially for FX
- Create uniform token standards for settlement between rails (e.g., cross-chain TTF extensions, ERC-1400/3643-style compliance layers)

5. Strengthen Standards for Clearing, Settlement, and Reconciliation to reduce operational risk and align settlement on the blockchain with established financial market standards.

- Define canonical settlement rules for each digital money model, especially for atomic settlement
- Standards for FX rate determination, liquidity pools, and cross-currency settlement for stablecoins, CBDCs, and deposit tokens
- Requirements for reconciliation between wallets, blockchain ledgers, and omnibus accounts

6. Formalize Risk Mitigation Standards for Smart Contracts (e.g., security, upgrades, governance)

- Standardized smart-contract audit requirements (e.g., code scanning, formal verification, upgrade procedures)
- Governance rules for pausing transfers, freezing assets, and clawback mechanisms
- Build on existing frameworks for payment-specific contract governance standards

7. Improve AML/CFT Traceability While Preserving User Privacy

- Off-chain encrypted data-sharing networks for Travel Rule compliance
- Selective disclosure and zero-knowledge proof attestations for KYC, source-of-funds, and sanctions checks
- Risk-segmented wallet structures, (as some VASPs already use), to handle high-risk and low-risk funds separately

8. Establish Governance Models for Reversals, Disputes, and Consumer Protection, as governance is key for mainstream adoption

- Clear operational rulebooks for error handling, consumer disputes, and fraud claims
- Standards for reversible transactions (e.g., tagged transactions, hash-linked metadata, timelocks)
- Standardize clawback governance models for VASPs and custodians.

9. Promote Institutional-Grade Infrastructure for Deposit Tokens and Stablecoins

- Institutional-grade custody, treasury integration, settlement workflows, and role-based permissions
- ERP and corporate treasury integrations for automated on-chain cash management
- Multi-rail treasury systems compatible with existing payment standards and blockchain rails

10. Establish Collaborative Standards Working Groups, as collaboration is essential to prevent fragmentation and ensure scalability

- Public-private technical working groups bringing together central banks, banks, VASPs, standards bodies (ISO/ITU/IEEE), and blockchain communities
- Harmonize standards across all stages of the payments lifecycle
- Transition industry-driven blockchain standards into formally recognized global standards

OPEN QUESTIONS

- What information should be stored on-chain, and what must remain off-chain?
- For off-chain data, what storage models and security mechanisms should be required?
- What is the right balance between privacy and compliance—and should that vary by use case?
- How should interoperable information flows be facilitated across stakeholders?
- How should digital identity be standardized across all forms of digital money?
- How should requirements for digital money models be aligned across stablecoins, CBDCs, and deposit tokens, and potentially other forms of digital money?
- How should requirements be aligned across jurisdictions to support seamless global payments?
- What interoperability standards should govern multi-rail payments (across blockchain/banking/CBDC rails)?
- How should FX rates, cross-currency settlement, and liquidity be standardized?
- What governance model should define reversals, refunds, and dispute resolution?
- How should liability be distributed across issuers, wallets, VASPs, and networks?
- How should risk scoring and AML monitoring be standardized across chains and off-chain financial systems?
- How should settlement finality be defined in networks that can fork, reorganize, or pause?
- What global security standards should govern smart contracts?
- What consumer protection requirements are necessary for mainstream adoption?
- How should integration layers be designed for real-world deployments?

R7. Clear accountability
Accountability for the AI system is explicitly assigned (e.g., business owner, technical owner, risk/ compliance contact).

0 / 1 / 2 / N/A

R8. Governance oversight
An AI governance or risk body (or equivalent) reviews high risk AI use cases at defined points (e.g., design, pre launch, periodic review).

0 / 1 / 2 / N/A

R9. Periodic re assessment & improvement
The system and its controls are periodically re assessed (e.g., annually or after significant change), with documented improvement actions and tracking to closure.

0 / 1 / 2 / N/A

G. SUMMARY & NEXT STEPS (OPTIONAL TEMPLATE)

After completing the questionnaire:

Transparency (T) score: ___ / ___ → ___ % → □ Low □ Medium □ High
Security (S) score: ___ / ___ → ___ % → □ Low □ Medium □ High
Reliability (R) score: ___ / ___ → ___ % → □ Low □ Medium □ High

Overall assessment (using your chosen thresholds):

- □ Fair
- □ Good
- □ Great

Top 3 improvement actions for this AI system:

1. _____
2. _____
3. _____

GBBC
Global Blockchain
Business Council

SUPPLY CHAINS & CRITICAL MINERALS REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 6.0

FROM MINE TO MARKET: UNLOCKING SUPPLY CHAIN VISIBILITY FOR CRITICAL MINERALS THROUGH DISTRIBUTED LEDGER TECHNOLOGY

GBBC GSMI 6.0

ACKNOWLEDGEMENTS

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

Kayode Babarinde - CO-CHAIR
Executive Director, Africa Blockchain Institute

Blake Goud - CO-CHAIR
Chief Executive Officer, RFI Foundation

Raymond van Ermen - CO-CHAIR
Executive Director, The-EPE

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

We are living a in a 'new reality' from a geopolitical, trade and technology standpoint.

Cooperation among stakeholders, even traditional competitors – coopetition – is key. In this framework digital tools providing trust, accountability, efficiency, and values sharing have a critical role to play to improve business performance as well as an inclusive, twin and just transition.

This report is focused on critical minerals, key for peace, trade, electricity transition, and prosperity, with blockchain as a "*game changer*." It is not limited to a global 'supply chain' agenda. It concerns as well agreements between countries, investors risk management, tax collection and use, workers, and population rights. This paper is inspired by the World Resource Forum report '*Rethinking Value – Resources for Planetary Wellbeing*' to make resources a driver for shared wellbeing within planetary boundaries, and it also presents an overview of the blockchain ecosystem and blockchain public infrastructure to *enable implementation of relevant regulatory initiatives and international agreements, improve knowledge and governance in the supply chain due diligence, coordinate funding, and attract investors*. It presents a global overview, with an African pilot and recommendations.

Supply Chain: *"A supply chain is made up of interconnected parts of a whole, all of which add up to finished products bought by customers"* (McKinsey)[121]

Value Chain: "The full range of interactions, resources and relationships related to a reporting entity's business model and the external environment in which it operates." (ISSB)[122]

The distinction with supply chain, is that SC refers only to upstream inputs supplied for production of a good or service. Value chain extends that to a wider range of relationships (not only suppliers) and also includes other issues after goods and services are produced and delivered to customers (e.g., disposal, emissions related to product use, which refers to Scope 3, category 11 emissions under the GHG Protocol). Across this report, we refer to both supply chain and value chain as they are relevant according to these definitions.

INTRODUCTION

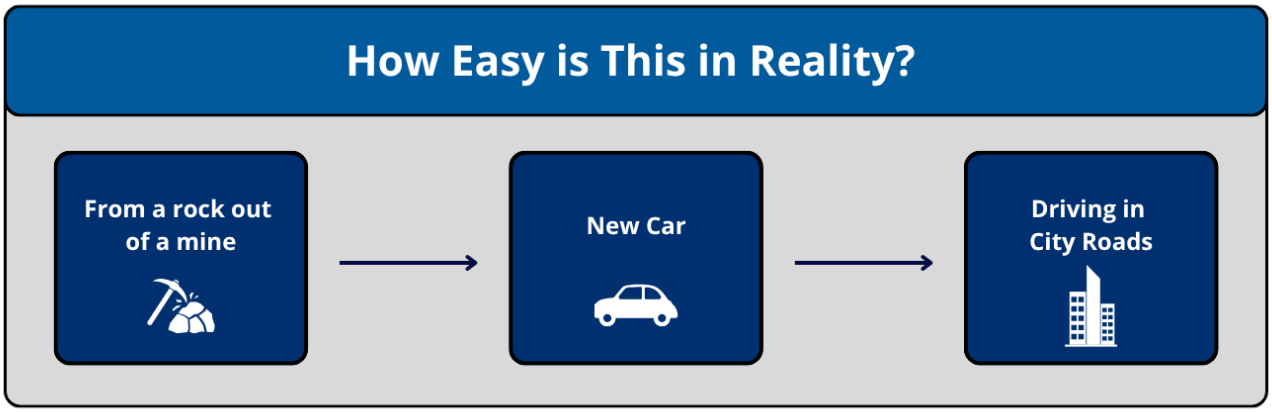
Critical minerals are raw materials that human civilization relies on for technological innovation, economic activity, and national security. Much of modern daily life is made possible by these minerals, which we find all around us in the form of our electronic devices, basic public infrastructure, clean energy equipment, and even our household appliances.

We are mindful that different countries may have certain differences across their official lists of critical minerals and rare earth minerals. For the purposes of this report, we refer to critical minerals in a broad sense, such that the issues we raise for critical minerals are also relevant for rare earth minerals.

Examples of critical minerals include:

Mineral	Primary Uses
Aluminum	Aircraft, transportation, packaging
Cobalt	Battery electrodes (including electric vehicles)
Copper	Electrical wiring (e.g., cars, cities, wind turbines), renewable energy infrastructure, electronics
Graphite	Battery anodes (including electric vehicle batteries)
Iron	Steel production (buildings, infrastructure)
Lithium	Batteries (including electric vehicle batteries)
Nickel	Batteries (including electric vehicle batteries), stainless steel
Rare earth elements (REE)	Electronics, magnets, defense systems
Silicon	Solar panels, semiconductors, computer chips

The supply chain of critical minerals – from initial extraction, to processing, refinement, transportation, and final delivery and recycling at the end of use for the item produced using critical minerals – is highly complex and may be vulnerable to supply disruptions.[1][2][3] Given these intricacies and challenges, emerging technology – specifically blockchain based tools for data verification - may be the only answer to ensure more robust and resilient critical minerals supply chains.



This report builds on previous GSMI supply chain reports, narrowing down on the specific issues raised by critical minerals supply chains that are an essential component to enable future economic growth. The essence of this is how critical minerals advance the themes introduced in foundational previous GSMI supply chain reports, carving out an especially important case where emerging technologies can provide tools that other traditional approaches have been incapable of delivering.

Critical mineral supply chains are complex and are intertwined with business competitive advantage and national security interests for companies involved at many stages. These challenges are heightened versions of well-known opacity in supply chains, especially beyond Tier 1 suppliers. Traditional supply chains are opaque for many reasons, and as a result, developing full transparency may be inaccessible to deliver the necessary traceability that entities along the supply chain, and stakeholders impacted by it, need to conduct due diligence in their interactions, as well as for those seeking to build resilience of supply chains.

A common misconception equates blockchains solely with public–aka *permissionless*–networks like Bitcoin. In reality, blockchains can also be *permissioned*, where participants are known and access is controlled, making it suitable for most enterprise use cases. And, blockchain itself is just one type of distributed ledger technology (DLT). Other DLTs use different designs–such as directed acyclic graphs (DAGs) or hashgraphs–to achieve similar goals.

Another misconception is that simply setting up a blockchain or distributed ledger gives you a provenance solution. It doesn't. A blockchain or distributed ledger is the safe home where provenance data can live transparently and be trusted. But, a key challenge is capturing, recording, and querying the right provenance information.

This is where provenance becomes central to supply chain visibility. Provenance provides the 'life story' of a critical mineral, making it possible to trace origins, transformations, and movements across complex global networks. Without it, supply chains operate in the dark, leaving blind spots around compliance, risk, and sustainability. With it, visibility becomes actionable: organizations can anticipate disruptions, verify sourcing claims, and build resilience and trust into their supply chains.

PURPOSE

The purpose of this paper is to provide tools to facilitate a desired future of more robust critical minerals supply chains. With a systems design thinking approach, it advocates for a paradigm shift in global critical minerals supply chains, leveraging emerging technologies – particularly blockchain and other distributed ledger technologies (DLTs), in convergence with other emerging or frontier technologies like AI, IoT and Edge computing, and internet connectivity and 5/6G:

- **to establish verifiable trust across supply chain complexities, while protecting sensitive data (e.g., commercial, personal, etc).**
- **to influence effective governance models for critical minerals supply chains**
- **to enhance due diligence and ultimately improve transparency and accountability**

The ultimate benefit: trust in global commerce.

Overall, this report is a response to a widespread observation by key stakeholders that implementation of most due diligence frameworks for critical minerals supply chains fall short of robust risk management objectives.[124] For instance, many key global forums on critical minerals have not yet fully acknowledged the benefits of emerging technologies like blockchain to support a solution-driven approach that can greatly enhance outcomes.

By identifying and addressing due diligence gaps, this report intends to provide a methodology and toolbox (Specified in Annex 2) to enable a level playing field globally for responsible sourcing and end-to-end supply chains of raw materials. In addressing clear needs, this report builds on state-of-the-art advances to enhance robustness of global supply chains for critical minerals through digital tools, (e.g., traceability, transparency, accountability, and decentralized collaboration). It is also consistent with existing global projects to strengthen responsible sourcing agendas, sustainable raw materials, responsible business/governance practices, and responsible financing.

We start with an overview of challenges in critical minerals supply chains, and ways emerging technology can help address them. We particularly highlight the complex landscape of multiple guidelines and requirements for stakeholders, identifying ways to address any barriers in applying innovative tools to facilitate compliance, and providing a blockchain toolkit to consider for facilitating compliance. We then provide a brief overview on the nature of guidelines, providing further detail on how blockchain technology can be deployed to better meet those guidelines and provide proof of compliance for reporting and audits. This report provides insight on current responsible sourcing standards, requirements, and related guidelines, particularly in light of how blockchain technology can help stakeholders throughout critical minerals supply chains comply. This leads to a proposed methodology for compliance, highlighting ways blockchain can enhance each verification.

Finally, the report identifies the needs of key stakeholders across critical minerals supply chains, gaps and challenges in meeting these needs, ways technology can help meet these needs. We conclude by proposing recommendations, conclusions, and open questions.

CRITICAL MINERALS, CRITICAL TRUST: FIXING BROKEN SUPPLY CHAINS WITH TECHNOLOGY

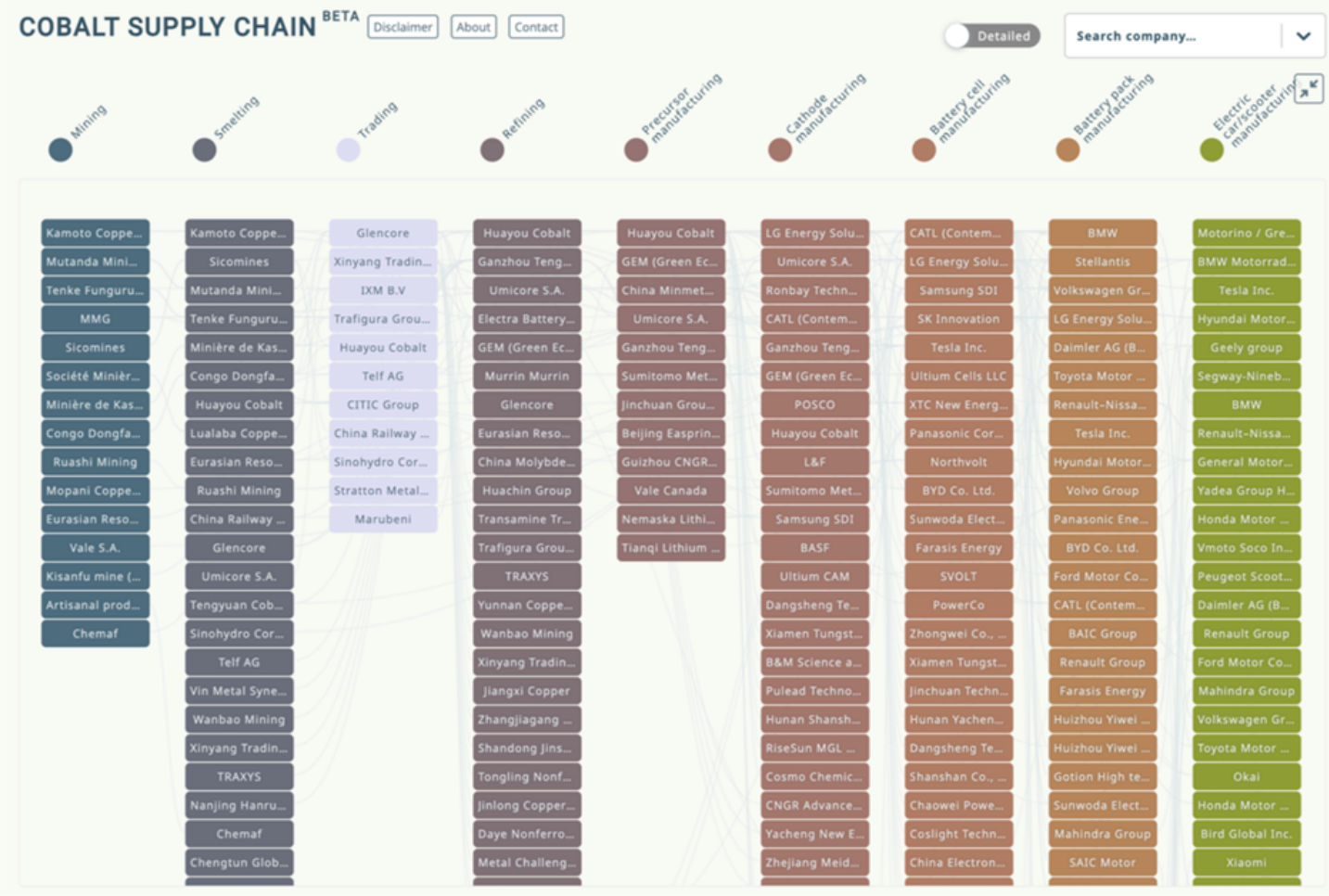
There is immense market value to be gained from improving trust and transparency, even across the most complex of critical minerals supply chains. For instance, major brands are looking to use supply chain data to create new customer experiences that allow users to obtain insights into the labor practices behind their products. Research initiatives like these calls for total visibility of all commercial transactions, prior to the deployment of enhanced commercial solutions. Yet as much as the world would benefit from supply chain transparency for critical minerals, there are complex global challenges that must be addressed:

CHALLENGE: SUPPLY CHAIN COMPLEXITY

Supply chains for critical minerals are highly complex, with multiple jurisdictions and processes involving multiple stages, players, modes of transportation, documentation and data sharing, and regulatory requirements.

These processes also involve an interplay between both physical and digital corridors. The first refers to physical infrastructure like railways and ports, while the second refers to information technology deployed to optimize these supply chains. Digital corridors record extensive logistics networks to track and manage the movement of minerals from their source to global markets, and ultimately to end users. While security and efficiency are fundamental, the inherent complexity of these supply chains poses substantial challenges.

As an example, below is the supply chain for cobalt:



Source: Resource Matters.

OPPORTUNITY WITH EMERGING TECHNOLOGY: BETTER CORRIDOR MANAGEMENT

Facilitating critical trade corridors possesses the potential for eliminating major bottlenecks in trade. As corridors manage goods in transit, corridor efficiency naturally involves improving the transit process of goods across countries and regions. The United Nations Conference on Trade and Development (UNCTAD) report on blockchain and trade facilitation performance[125] states:

"International corridor management is a major component of the global trading system. Given the increasingly interconnected global economy, goods go across many countries and sometimes multiple regions to make it to the target destination. This is not without challenges, especially when the multiple stakeholders within critical corridors do not have a commonly shared digital backbone for trade data and information sharing. The complexity of multinational trade flows makes critical corridors particularly important for ease of trade flows and serve as critical determinants of the time and cost to trade."

Digital corridors in particular can be optimized with emerging technologies, especially in alignment with the Global Digital Compact adopted at the UN Summit of the Future held in September 2024 in New York. Emerging technologies can also improve the effectiveness of implementation of strategies like the World Bank Trade and Transport Corridor Management Toolkit.[126]

CHALLENGE: GEOPOLITICAL RISKS

National and global economies depend on resilient supply chains. Yet ideological conflicts often drive the geopolitical context in which the modern economy and global supply chains operate. If any actor disrupts the supply chain, it can have global implications, bringing disruptions to economic trajectories and power structures, such as competition in the semiconductor industry.

Geopolitical risks in critical minerals supply chains stem from concentration of resources in certain countries, with manufacturing and final consumer demand often located in disparate regions. Resource concentration increases supply vulnerabilities, especially in cases of unwanted events - global conflicts, political instability, and economic sanctions can directly affect supply and lead to volatility in prices. Resource concentration thus also impacts power dynamics between nations, with resource nationalism and export controls arising as mechanisms to gain leverage with trading partner nations.

Ultimately, geopolitical risks arising from critical minerals-driven disputes may threaten national security and destabilize efforts toward economic development and the energy transition. In a context of shifting power dynamics and increasing uncertainty, there is a rising multipolar struggle for resources among powerful nations, where often countries that have those resources retain limited power and are subject to political pressures.

For instance, countries like the United States, China, Japan, and Russia are building corridors globally to strengthen their position with respect to access to critical mineral resources. The United States and China have already demonstrated a rivalry in exerting global political influence, stemming from efforts to access mining resources in places like Latin America. China[127] and Japan[128] are also financing corridors in Africa.[129] Access to critical minerals can be the source of armed conflicts and wars, which disproportionately hurt local communities in those nations where raw materials originate, which are often lower income nations with greater vulnerabilities.[130]

Expected outcomes from these geopolitical dynamics can draw lessons from historical events such as the 1970s oil shock and following US embargo[131], where a higher price of oil created incentivized the US to search for alternative oil resources domestically and increased its bargaining power over the Organization of the Petroleum Exporting Countries (OPEC), which now provides a significantly lower percentage of petroleum resources globally. Similarly, US-China rivalries have created incentives for mining critical minerals on US soil[132], as geopolitical risks have prompted efforts to diversify sourcing overall. Ultimately, the implication in the long-term is to reduce exposure to geopolitical risk by further diversifying supply, but in the short-term, this could it heighten it (especially if suppliers are worried about their sourcing being disrupted by supplier cuts to raise pricing ahead of losing pricing power when supplies come on line).

OPPORTUNITY WITH EMERGING TECHNOLOGY: GLOBAL JUSTICE

In a time of increasing geopolitical complexity and trade wars, emerging technologies can help countries shift the balance of power[133] toward a more equitable global economy, away from extractive models where financial flows disproportionately favor "consumer" nations in the Global North at the expense of resource-rich countries in the Global South.

Is the logic here may be of a 'race to the bottom' via opaque supply chains to conceal activities that violate international obligations. While removing that opacity necessarily leads to investment in downstream production capacity in developing countries to help them move up the value chain, it may also merely reduce one form of harm (conflict minerals) from supply chains while leaving the extractive economic model intact where Global South countries are unable to advance, by being constrained as producers of low-value added commodities.

For instance, there is a need for a global strategy on responsible sourcing, where blockchain technology can be critical in developing a trusted ecosystem for global trade performance, ultimately supporting global peace and prosperity. Innovation can lead to a turning point, as a source of competitiveness that can facilitate "co-opetition" dynamics for win-win outcomes for all stakeholders and local communities.

Blockchain technology, which enables data sharing in ways that benefit all stakeholders, can transition dynamics toward greater convening and collaborating. In working together to build supply chain resilience with greater transparency and trust enabled by technology, trading partners can increase the market opportunity for all, in ways that favorably influence international relations rather than conflict.

As António Guterres, United Nations Secretary General stated at the Launch of the Panel on Critical Energy Transition Minerals, April 26, 2024 "One principle shines from the heart of this initiative – and that principle is justice. Justice for the communities where critical minerals are found… Justice for developing countries in production and trade; and justice in the global energy revolution."

CHALLENGE: SYSTEMIC VULNERABILITIES DUE TO LACK OF TRANSPARENCY/ SECURITY

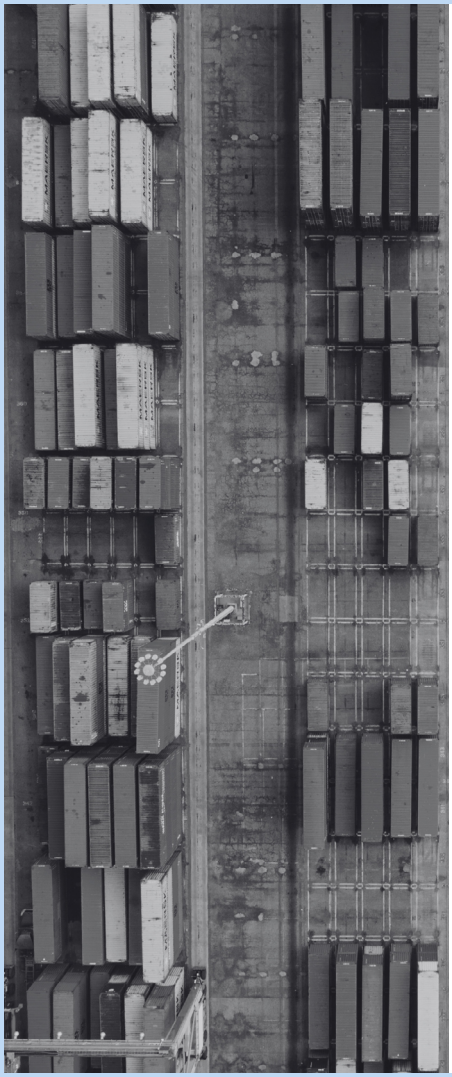
Global reliance on critical minerals and rare earth elements has exposed systemic vulnerabilities: opaque sourcing, geopolitical manipulation, and rampant counterfeiting and forgery, with respect to both critical minerals and the documentation supporting their provenance respectively. Traditional supply chain models, dependent on centralized databases or paper trails, fail to provide the transparency, security, and multi-tier traceability required to mitigate these risks. Often these supply chains are made up of widely spread tasks, managed by analog systems that remain disconnected from each other, with limited data visibility and limited data sharing for stakeholders who need it most. In an analog context, making data available may mean disclosing the full ledger of records, which would require disclosing confidential information – both personal data and trade secrets.

The Pitfalls of Traditional Transparency

Current approaches to traceability often consolidate data into centralized “buckets,” creating vulnerabilities:

- **Honeypot Risks:** Central repositories, storing a high amount of data in one place, attract hackers
- **IP Exposure:** Sharing full production details with auditors or partners risks reverse engineering
- **Oversimplification:** Aggregated data obscures critical nuances across tiers (e.g., unethical subcontractors)

Supply/Demand Imbalances



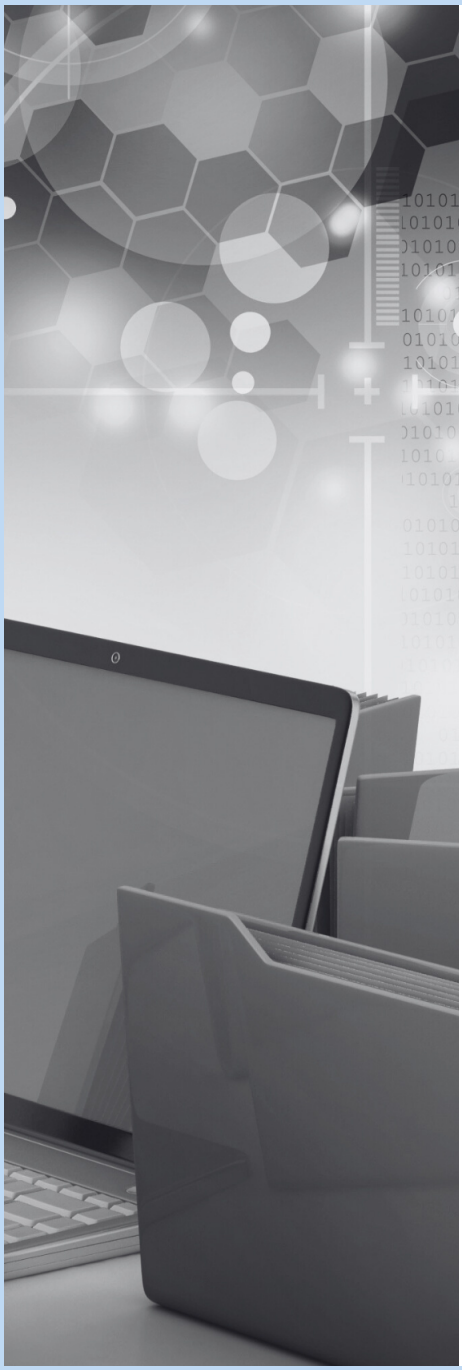
Moreover, lack of transparency can exacerbate supply and demand imbalances. For instance, the energy transition can rapidly increase the demand for certain critical minerals without providing the necessary data for producers to ramp up supply accordingly. This could point to issues where producers want to increase production but are unable to supply due diligence data to purchasers (assuming energy transition is more likely to demand compared to other sources of demand).

For instance, in palm oil biofuels, import restrictions were imposed to cut off imports of specific products related to sustainability risks, and had the unintended consequence of harming producers who had gone through the process of sustainability certification because a large market for their production was closed after the fact. These issues affected modern diplomacy conversations, including Indonesia vs. European Union regarding palm oil and biofuels disputes at WTO Panels. Moreover, the Covid pandemic also highlighted numerous supply chain fragilities and concentrations, with supply chains facing major challenges in the face of rapid shifts in demand, transportation bottlenecks, and shortages in raw materials.

Sustainability Concerns

From a sustainability standpoint, lack of transparency also creates obscurity with respect to environmental impacts in production processes, as well as labor conditions including the presence of slave labor. A recent McKinsey study estimates that the majority of companies globally have no supply chain visibility beyond Tier 1 which means they are effectively flying blind in relation to many material sustainability-related risks buried in their supply chains.[138]

Challenges Arising from the Informal Economy



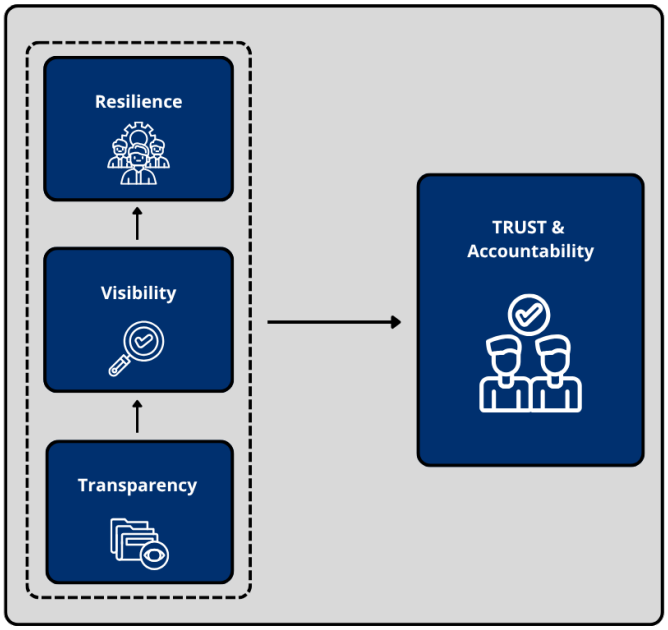
In much of the developing world, the majority of economic activity remains in informality – that is – outside of legally registered and regulated activities. Informal economic activities, including many small enterprises, are not taxed but also cannot access basic services and protections, such as access to financing, training, social security. In the case of critical minerals, this may include the activities of small and artisanal miners and their cooperatives, transportation providers, vendors of supplies and equipment, and other essential labor and supporting services. In some countries, the process to legally register a business, alongside basic activities such as owning property, are so onerous relative to the benefits for average citizens that many prefer to remain in a status of informality. Thus, while there is a massive estimated aggregate wealth in the informal economy, much of it may remain illiquid and tied to lack of visibility, which may increase the risk of corruption and undesired activities.

In addition to the negatives associated with wealth accumulated in the informal economy, it also reduces domestic resource mobilization (e.g., taxes) for infrastructure investment and (e.g., lack of participation in the formal financial sector) increasing financial market depth and local liquidity, which reduces external financing requirements for the formal private sector companies. Both issues contribute to high perceived risk by external investors (leading to high interest rates) at the same time the domestic industry (including downstream production) may be rendered less competitive by Dutch disease (overvalued exchange rate as a result of natural resource wealth).

Challenges Arising from the Informal Economy (cont.)

The conventional view is that moving informal economy to the formal economy is always a net positive, but that may be a perspective that reflects an imposition of a Western attitude towards different forms of economic organization. There could be value produced if emerging technology is employed in a way that allows for interfacing between formal and informal economy without requiring a wholesale change, while still providing visibility in supply chains.

This takes into account the UNCTAD research related to stakeholder capabilities and participation and report recommendation on Policy guidance for stakeholders: *"While blockchains could speed up processes at both local and global levels, stakeholder preparedness, readiness and awareness play a crucial role in the success and sustainability of the technology in a national context. Implementation will require a holistic approach of training, preparing and supporting the broader stakeholder ecosystem to understand and fully engage in the development, design and deployment of the technology. As multi-stakeholder systems by design, blockchains not only need stakeholder acceptance, but also stakeholders' active participation to attain proper function and to achieve the intended purpose."*[134]



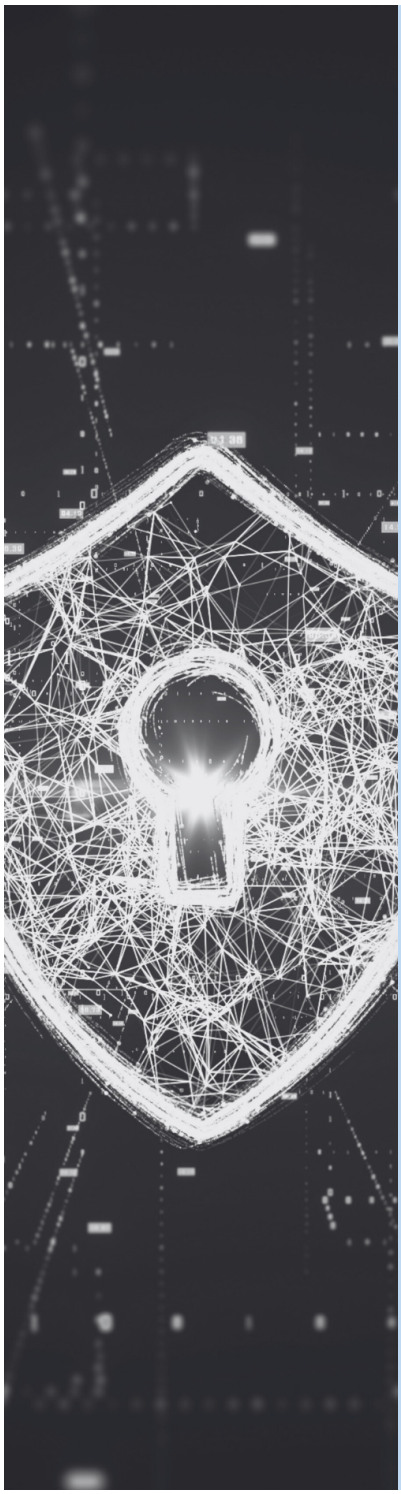
OPPORTUNITY WITH EMERGING TECHNOLOGY: TRANSPARENCY & SECURITY

Supply chain resilience is made possible by greater visibility, which in turn is built on transparency. Blockchain technology can enhance existing initiatives and greatly increase transparency, in ways that improve both traceability alongside security.

Transparency

When it comes to traceability & provenance, blockchain technology can record key interactions following processes to make products (e.g., geo-location date/timestamps of interactions, physical movement), as well as facilitate evaluations (e.g., conduct evaluations, 3rd-party audits, facility inspections, and product test results linked to specific batches). Public protocols provide the benefit of data access for all network participants, allowing companies to build solutions with a shared protocol in ways that increase opportunities for all stakeholders and facilitate coopetition.

Security



As for security, privacy preserving tools are especially useful when it comes to selective disclosure of data and self-sovereign ownership of data, such that the necessary data is made available, when needed, to designated stakeholders. This can point to the right data necessary to balance supply and demand. Transparency is also a fundamental condition for AI-based tools for demand planning and response, which can improve supply chain resilience. For supply chains, permissioning measures and other privacy preserving tools enabled by blockchain technology are critical and enable:

- **Data Property Rights:** Ensuring companies retain ownership of intellectual property (IP), pricing, and proprietary processes.

  - A related element is that companies in EMDEs should benefit from participating in more transparent supply chains, and should not just face 'stick' of loss of market access & financing as the principal reason for producing & supplying this data. Current market ecosystem has intermediaries demanding data on behalf of end-users (investors, financial institutions) and then selling that data back to the companies that supplied it (e.g., for peer benchmarking). The payments ecosystem related to blockchain systems (e.g., stablecoins, CBDC) should enable payment for data on a granular level (data item for particular company) in addition to other important data property rights.

- **Selective Disclosure:** Sharing cryptographic proofs of claims (e.g., mineral provenance) without exposing raw data.

- **Interoperability:** Integrating legacy systems with emerging web3 tools through emerging protocol abstraction layers.

Economic Growth & Formalization

The transparency provided by blockchain technology can shed light on the value of informal economic activities, helping quantify and record essential data. It can also facilitate access to markets and connect important players into integrated records of global critical minerals supply chains.

CHALLENGE: MANY GUIDELINES; MAKING DUE DILIGENCE DIFFICULT

Given the complexity and global importance of critical minerals supply chains, there are a plethora of guidelines, standards, and regulatory requirements intended to address the challenges of these supply chains and improve their resilience. In addition, international convenings, protocols, and trade agreements set commitments to support resilience in critical minerals supply chains. In this context, supply chains for critical minerals are governed by a wide array of government policies, industry standards, and international frameworks. Multiple initiatives and platforms – ranging from responsible raw materials sourcing, mining management, sustainable finance, value chain management, and fair trade – may be useful for stakeholders seeking to adhere to responsible business conduct, but assessing and ensuring due diligence can be extremely difficult.

- **Systems not up to par:** With current systems, there is a wide array of tasks and data to be checked across various stages of the supply chain (e.g., documents, authenticity verifications, use of standards). The data gathered and revised must also be congruent across jurisdictions and platforms. This adds great complexity into due diligence assessments – essentially for the "yes/no" decision on whether an entity meets due diligence requirements whether for financing or other commercial decision-making.

- **Requirements are not harmonized:** When it comes to supply chain resilience, there is currently no widely accepted system definition and parameters, governance model with specifications like data property rights & selective disclosure licensing, or standards for data management.

There is also a need for interoperability across supply chains, similar to internet and computer protocols. In complex supply chains, different supplier groups and other stakeholders may be subject to different standards utilize technology differently. Moreover, different layers of the supply chain may be considered part of different industries, with different considerations and requirements.

The palm oil and biofuels issue mentioned before is also an example from a different context, but illustrates a similar point. Standards that were developed for sustainable palm oil were primarily designed for the food sector (to protect the value chain intermediaries and final manufacturer of consumer goods where validating sustainability back to the individual inputs was important to avoid deforestation-related production).

Where other sustainability concerns arise (e.g., macroeconomic incentives for deforestation related to biofuels), the ban was designed because any use of biofuels with deforestation risk is likely to increase aggregate deforestation to meet both food & energy requirements. However, in imposing an import ban, those who had met the requirements for the consumer food production sector were punished with loss of access, while those that were excluded from the EU's market already faced no incremental harm, penalizing companies for doing the right thing.

OPPORTUNITY WITH EMERGING TECHNOLOGY: BLOCKCHAIN TO ENHANCE DUE DILIGENCE

Blockchain technology can be a promising tool to better assess adherence to ethical best practices, guidelines, and regulatory requirements. Stakeholder priorities can be broadly considered, in ways that take less effort to perform required tasks (e.g., basic traceability tests) to meet minimum standards and maintain a basic level of trust. If a greater portion of the due diligence process becomes automated and transparent, with less resources, it can cover a wider scope of data, tiers, and processes across the supply chain. Ultimately, organizations can move beyond meeting minimum requirements to consider a broader array of stakeholder concerns (e.g., double materiality).

Awareness, education, and engagement are key to align stakeholders toward a coordinated adoption of blockchain technology to enhance due diligence across supply chains, addressing any barriers toward this adoption. For instance, contrary to certain public perceptions that blockchain makes the data it records public (e.g., it would also be a concern if a private blockchain allows all users of that blockchain to view all the on-chain data), there are solutions available to protect IP and data privacy, with sensitive information never shared beyond those specifically granted access.

First, it will be important to address current barriers to implement blockchain to optimize due diligence for critical minerals supply chains, which consist of:

Barriers to adopt blockchain for due diligence	Mitigants
Perception of blockchain making all data public, leading to reluctance to share sensitive data with competitors (e.g., suppliers, volumes, contracts).	• **Awareness & Training** on how to implement shared transparency without full disclosure: Blockchain based privacy tools include solutions to allow validation without exposing trade secrets (e.g., zero-knowledge proofs). • **Permissioned ledgers** also allow companies to share compliance-related proofs (e.g., origin, ESG data, due diligence data) while keeping commercially sensitive data private. • **Best practice**s point to storing sensitive information off-chain, sharing proofs on the blockchain (e.g., as hashes)
System integrations and costs, limiting scalability	• **Stakeholder collaboration** toward shared and open systems (e.g., offer shared industry utilities through consortium blockchains). Layer 2 and permissioned solutions can also improve scalability. • **Subsidies and capacity building**, especially for small organizations, considering low cost mobile solutions over expensive tech.

Barriers to adopt blockchain for due diligence	Mitigants
Desire for opaqueness in parts of the supply chain, to conceal poor practices or informality, contributing to traceability gaps.	• **Incentives toward transparency**, including economic incentives, and sanctions for poor behavior and lack of due diligence. • **Digital identity tools** for artisanal miners and smallholder players & partnerships with NGOs and local cooperatives to digitize transactions, helping informal players integrate into the global system.
Lack of quality data to record (Garbage in, garbage out concept)	• **Investment in infrastructure** (e.g., sensors, satellite monitoring)
Different data formats and measurements, reducing interoperability	• **Data standards** (Development and adoption) • **Multistakeholder initiatives** • **Government-sponsored pilot** projects toward standards adoption
Poor governance practices	• **Develop clear contractual rules**, especially for liability, and embed smart contracts with these responsibilities. • **Develop inclusive governance models** that give voice to upstream suppliers.
Lack of interest in blockchain adoption, due to unclear ROI or comfort with status quo	• **Regulatory sandboxes for blockchain** traceability and acceptance. • **Education, training, and engagement** toward formal recognition of blockchain records as compliance evidence of due diligence requirements. • **Tie blockchain to market access** advantages and highlight efficiency gains
Power and information asymmetries	• **Cost sharing approaches** so downstream buyers, generally with deeper pockets, cover a greater portion of the implementation burden

BLOCKCHAIN TOOLBOX FOR DUE DILIGENCE IN CRITICAL MINERALS SUPPLY CHAINS

Blockchain can provide granular data on inputs, outputs, and changes of title and custody, allowing visibility for an entire product with respect to the origin and destination of critical minerals. Below is a list of blockchain attributes that can be beneficial to enhance the resilience of critical minerals supply chains by strengthening due diligence mechanisms. We offer this toolbox as a reference for stakeholders to consider in performing due diligence to meet requirements:

Tool	Benefit
Shared records	Verified records on supply chain data, compliance with requirements, and certifications facilitate auditability, regulatory compliance, and other due diligence requirements. Auditable data trails reduce reliance on self-reporting
Tokenization	Trace materials as they move across physical boundaries
Digital identities	Interoperable identity systems (e.g., for workers) integrate into supply chain data
Smart Contracts	Automate transactions, compliance, payments, benefit sharing, and reporting, upon meeting key requirements
Immutable records	Prevent corruption and fraud, with no retroactive record changes
Shared ledgers	Enable collaborative practices and standardized digital certifications (e.g., conflict-free minerals, fair trade practices, carbon footprint) and compliance frameworks (e.g., harmonized regulatory requirements)
Incentive mechanisms	Encourage positive behaviors (e.g., tokenization and credits to incentivize metal recycling)
Privacy & Security Tools	Enable selective disclosure of necessary data. Zero knowledge proofs can reveal only necessary data for any given decision, without revealing sensitive information that is better kept private. Cryptographic key management, for instance, ensures data confidentiality and data integrity for greater security. Multisig (multi-signature) validation enables collaboration and security with shared control and improved accountability, in a way that reduces single points of failure.
Real-Time Data records	Facilitate assurances for regulators, manufacturers, investors, etc.
Decentralized governance mechanisms	Enhancing collaboration across key stakeholders, including voices of traditionally underrepresented groups. Decentralized Autonomous Organizations (DAOs), for instance, can implement measures such as voting, project proposals, and automated execution of transactions.
Integration with IoT devices	Real-time access to data captured on the ground by IOT devices, securely recorded on a blockchain
Integration with AI Solutions	Blockchain provides verified data going into AI algorithms, the methods in which data is processed by AI algorithms (foundation models, and the outcomes of AI-driven informed decision making for better monitoring & evaluation of impacts.
Decentralized Finance (DeFi) and Regenerative Finance (ReFi)	DeFi might provide the infrastructure for supporting both payment for licensing of ESG data (to incentivize companies to provide it) and also topics like ReFi to act in ways that are regenerative rather than extractive. ReFi can improve the effectiveness and monitoring of environmental and social protections, such as community engagement, management of water and other resources, and emissions targets

BLOCKCHAIN STRUCTURE

Blockchain technology should ideally be deployed in two dimensions: to capture production data and to capture commercial transactions. This way, each tier in the supply chain can be accurately followed, as raw minerals end up in many different goods. This bifurcation allows companies and consortia to determine the appropriate technology tool to use for each function; enables granular, multi-tier supply chain visibility while safeguarding competitive advantages and sensitive data; and provides the structure to evaluate various standards and assess technology adoption.

TRANSPARENCY: PRODUCTION VS. COMMERCE

1. **Production Data:** Immutably record the journey from inputs to outputs. This includes records of how materials are extracted, refined, and processed (e.g., energy usage, labor conditions).

2. **Commercial Data:** Immutably record commercial events, where transactions indicate change of custody and title, to link the multiple tiers of the global supply chain. This provides verifiable proof of ownership and custody transfers, contracts, and payments across suppliers, without disclosing pricing.

BLOCKCHAIN AS A TOOL FOR DUE DILIGENCE

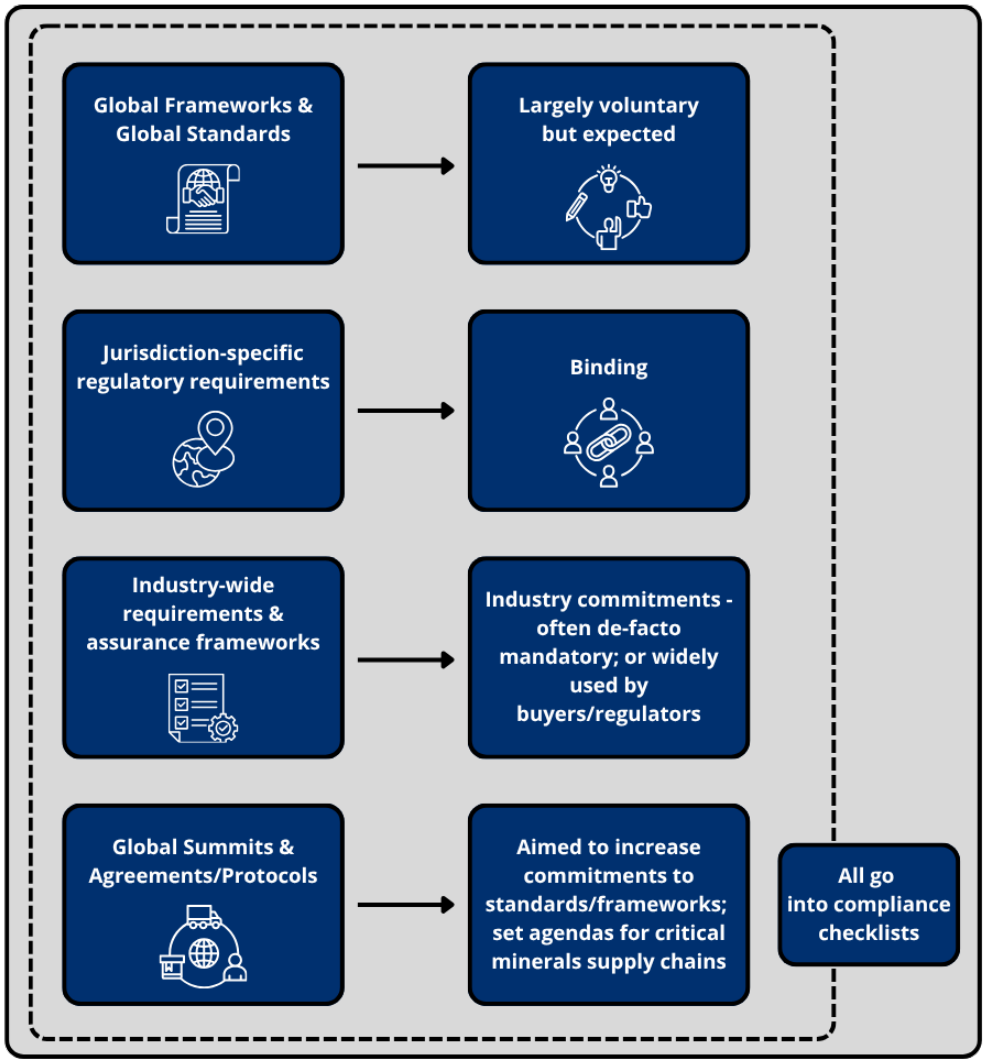
Because of the complexity of due diligence and the various specific requirements, below we identify the main themes covered by due diligence requirements across critical minerals supply chains, followed by ways blockchain technology can help enhance due diligence to meet those requirements.

DUE DILIGENCE PRINCIPLES

Principles drawing from existing international norms, commitments, and legal obligations across critical minerals supply chains can be summarized as the following:

Principle 1	Human rights must be at the core of all critical mineral value chains.
Principle 2	The integrity of the planet, its environment, and biodiversity must be safeguarded.
Principle 3	Justice and equity must underpin critical mineral value chains.
Principle 4	Economic development must be fostered through benefit sharing, value addition, and economic diversification.
Principle 5	Investments, finance, and trade must be responsible and fair.
Principle 6	Transparency, accountability, and anti-corruption measures are necessary to ensure good governance.
Principle 7	Multilateral and international cooperation must underpin global action while promoting peace and security.

A detailed landscape of the various guidelines for critical minerals supply chains can be found in Annex 1, with the main concepts and players illustrated below:



DUE DILIGENCE METHODOLOGY

The landscape of guidelines can be applied into a practical compliance checklist, with the following considerations. The blockchain toolbox referenced above can be referenced to meet the points below. For mineral-specific compliance checklists, see Annex 2:

1. **Governance & Policy:** Adopt policies for responsible sourcing and human rights, aligned with OECD, UNGPs, and IFC.

2. **Traceability & Chain of Custody:** Implement chain of custody controls from mine to smelter/refiner to components to final product, selecting a model defined by ISO 22095. Adopt recognized audit protocols (e.g., RMAP, IRMA, Copper Mark, ASI) as relevant.

3. **Risk Assessment for conflict areas & forced labor:** Screen for exposure to conflict-affected and high-risk areas (CAHRA) and forced labor across the supply chain, and subsequently prioritize risk mitigation measures, according to relevant frameworks like (e.g., US Uyghur Forced Labor Prevention Act (UFLPA), UK Modern Slavery Act)

4. **Corrective Actions & Supplier Engagement:** Implement risk mitigation measures, escalating or disengaging where necessary, in alignment with OECD.

5. **Independent Assurance:** Adopt required and expected assurance and audit mechanisms (e.g., LME assurance, RMAP audits, GISTM facility audits, etc.)

6. **Public Reporting:** File legally required disclosures (SEC Form SD; Canada S-211; EU Battery/CSRD reports) and any voluntary reporting disclosures.

7. **Market-Specific Rules:** Adhere to rules for specific sectors (e.g., for EV/battery supply chains, IRA §30D critical minerals thresholds and FEOC exclusions prior to making claims for tax credits)

EXAMPLES OF BLOCKCHAIN FOR DUE DILIGENCE

The following organizations and initiatives have begun to recognize the role of blockchain to facilitate compliance with relevant regulatory and other requirements:

Frameworks recognizing blockchain's role

United Nations Conference on Trade and Development (UNCTAD): Released Global Report on Blockchain and its Implications on Trade Facilitation Performance, which provides a policy and technical framework, considerations, and recommendations for blockchain deployment in global trade. Blockchain can help advance proposals for UNCTAD blockchain and trade facilitation initiatives, among others.

Responsible Minerals Initiative (RMI): Released RMI Blockchain Guidelines as a voluntary framework to standardize the application of blockchain in critical minerals supply chains, focusing on common principles to improve due diligence and promote interoperability.

Commercial Trust™ Protocol (CTP)[135]: Developed by The Provenance Chain™ Network, facilitating verifiable blockchain-based digital credentials and management of intellectual property. CTP provides a standard framework to verify the claims made of people, parties, places, products, and processes across supply chains. It goes beyond classical web2 and web3 solutions by functioning as an abstraction layer of proprietary and web3 technologies to facilitate component-level data property rights, evaluations, and selective disclosure of requirements, incentives, claims, and evidence (RICE™) in commercial transactions. The CTP captures an immutable record of: production; orders; shipments; settlements; requests; and the results of evaluations of evidence needed to verify claims, without centralizing or disclosing sensitive data, intellectual property, or trade secrets. Companies can be transparent and run their business without giving away sensitive data or trade secrets.

Selected initiatives adopting blockchain

Lobito Corridor: Blockchain technology is enhancing transparency, security, and efficiency for this trade route, consisting in a railway and infrastructure project to transport critical minerals including cobalt and copper from the Democratic Republic of Congo (DRC) and Zambia to the port of Lobito in the Angolan Atlantic. This corridor is strategic for Western nations seeking to diversify their sourcing of critical minerals, and blockchain technology is being used to address critical challenges from complex logistics to illicit trade and corruption. [clarify stage of blockchain implementation or evaluation]

MineHub[136]: Digital trade platform providing open, enterprise-grade solutions for end to end traceability in mining and metals to ensure resilience and responsibility in supply chains. Provides a digitally integrated workflow that connects a vast network of partners and stakeholders and their transactions, as an alternative to paper-based and manual processes. Integrates blockchain technology to track minerals like gold and copper from mine to end user. MineHub recorded the first blockchain-based iron ore trade in 2020.

Auto Makers: Major companies (BMW, Ford, Hyundai/Kia, Mercedes-benz, Tesla, Volvo) are using blockchain technology to trace minerals like cobalt and mica. Industry consortium Responsible Sourcing Blockchain Network (RSBN)[137] was founded in 2019 by Ford, Volkswagen, and Volvo alongside mining and technology companies, with the purpose to track and verify ethical mineral sourcing form mine to market. Blockchain technology is being used to promote environmental and human rights standards, and ensure global traceability for customers.

Jewelry: Blockchain implementations focus on ethical sourcing and authenticity for tracking of diamonds and rare earth minerals. This increases trust with certifications of traceability from mine to consumer, with immutable records of ownership and origin, to address concerns of counterfeiting and illicit practices across the supply chain. Jewelry can be tokenized on a blockchain, provided with a unique identity.

Battery materials: "Battery passport" solutions can track key materials going into electric vehicle batteries, which not only confirm ethical sourcing and prevent counterfeits, but also simplify compliance through real-time audit trails that facilitate adherence to requirements for battery safety, environmental impact, and end of life management. These verifications about battery materials and history also optimize recycling processes, allowing recyclers to recover valuable materials more effectively.

Blockchain Platforms

Circulor, IBM Blockchain Platform (in partnership with MineHub), Minexx, and Re|Source are examples of blockchain solutions and consortia being implemented to track critical minerals from mines to end users.

MAPPING OF GUIDELINE MAIN THEMES AND BENEFITS OF BLOCKCHAIN

Guideline Topic		
Supply Chain Transparency & Traceability		Blockchain Benefits
Objective	Provide visibility on where and how minerals are sourced and processed, as requested by governments and investors	Provides a tamper-proof ledger recording every transaction or movement of critical minerals across the supply chain: • Tracks provenance from mine to market by logging each step (e.g., mining, smelting, refining, shipping, final use). While blockchain is a safe home for provenance data, in itself, it doesn't provide provenance. • Immutable records reduce risk of fraud or misinformation because data can't be altered once entered and validated • Chain of custody provides a clear and secure record of who handled a given critical mineral at each step.
Themes	Blockchain or digital tracking tools Reporting on origin, transit routes, and processing facilities Public disclosures and ESG reporting	
Examples	EU Battery Passport (for lithium, cobalt, etc.) SEC and EU non-financial reporting directives	A company can reference blockchain entries to confirm that a battery's cobalt came from a certified, conflict-free mine in the Democratic Republic of Congo
Ethical & Responsible Sourcing		Blockchain Benefits
Objective	Prevent human rights abuses, child labor, and financing conflict zones	Supports due diligence and human rights compliance by enabling: • Verification of certifications (e.g., child-labor-free, conflict-free) • Community reporting mechanisms (e.g., recording community consent like FPIC) • Audit trails for compliance checks
Themes	Traceability and chain of custody systems Third-party audits Certification schemes (e.g., IRMA, RMI) Community consent and engagement (e.g., FPIC – Free, Prior and Informed Consent)	
Examples	U.S. Dodd-Frank Section 1502 (for conflict minerals) EU Conflict Minerals Regulation	Blockchain integration with OECD Due Diligence Guidance enables all parties to verify sourcing claims and ethical practices.

Guideline Topic		
Sourcing Security & Resilience		**Blockchain Benefits**
Objective	Ensure supply continuity, reducing dependency on a single source or country	Increases visibility and coordination across the supply chain: • Detect bottlenecks or delays early • Map risks and vulnerabilities in real time • Manage inventory or contracts transparently (e.g., smart contracts)
Themes	Diversification of supply sources (geographic and commercial) Strategic stockpiling Onshoring or nearshoring parts of the supply chain Redundancy and flexibility in logistics and production	
Examples	U.S. Critical Minerals Strategy (DOE, DOI, DOD) EU Critical Raw Materials Act Japan's METI mineral sourcing policies	A battery manufacturer can quickly identify supply chain disruptions from a specific smelter and switch suppliers accordingly.
Sustainability & Environmental Standards		**Blockchain Benefits**
Objective	Minimize environmental damage from extraction, processing, and transport	Allows stakeholders to audit environmental impact in real time with a verifiable data trails, linking to IoT devices, satellites, or other entries that track data on: • Emissions • Water/energy usage • Waste management or reclamation
Themes	Environmental Impact Assessments (EIA) Lifecycle analysis (LCA) for carbon footprint Water/energy usage regulations Requirements for mine reclamation and closure	
Examples	International Council on Mining and Metals (ICMM) Principles OECD Due Diligence Guidance for Responsible Supply Chains	Data on energy usage captured on IoT devices can be recorded on a blockchain and made available to stakeholders who make assessments and perform audits
Downstream Integration & Recycling (Circular Economy)		**Blockchain Benefits**
Objective	Support for domestic refining, processing, and recycling to reduce dependence on raw material imports	Provides a log of the entire lifecycle of a mineral, from extraction to end-of-life, which helps identify when and where materials can be recovered, reused, or recycled. • Enables secondary market tracking of materials • Supports tracking and reporting of circular economy targets • Verification of shared value/corporate responsibility claims of supporting local communities and smallholder recyclers
Themes	• Tax incentives and subsidies • Support for R&D in alternative materials and recycling • Circular economy strategies	
Examples	EU Circular Economy Action Plan Japan's Circular Economy Roadmap US Inflation Reduction Act	Track recycled lithium from one EV battery going back into a new one

Guideline Topic		
Cross-Border Regulatory Compliance		Blockchain Benefits
Objective	Comply with rules from various jurisdictions	Facilitates cross-border compliance easier by creating standardized digital records that governments and trading partners can access.Consistent, verified data across jurisdictions.
Themes	• Critical minerals supply chains are complex and span multiple jurisdictions • Requirements across jurisdictions and activities can vary widely • Doing business with certain jurisdictions makes stakeholders subject to their rules (e.g., EU requirements may apply to EU stakeholders and all those doing business with them) • Trade agreements between multiple countries require compliance with requirements from all jurisdictions involved	
Examples	• Bilateral and multilateral agreements (e.g., U.S.-Australia Critical Minerals Partnership, Minerals Security Partnership) • Trade classifications, tariffs, and export controls (e.g., China's rare earth export policies) • WTO rules and bilateral free trade agreements with critical minerals chapters	Alignment with multiple relevant regulatory requirements, such as compliance with both the EU Battery Passport, US-Mexico-Canada Trade Agreement
International Collaboration & Trade Policy		Blockchain Benefits
Objective	Adherence to trade agreements and conditions set by governments on following trade policy	Accountability & monitoring of international agreements and protocols among governments • Connects company level records with requirements for trade policy and international agreements • Connects all interested parties across corridors (e.g., corporates, suppliers, governments, civil society) with consistent and verified data • Combats illicit trade, corruption, and fraud
Themes	Bilateral and multilateral agreements Trade classifications, tariffs, and export controls WTO rules and bilateral free trade agreements with critical minerals chapters Navigating tariff or non-tariff trade barriers	
Examples	Digital Corridors Agenda Agendas and forums through G20, WECD, and development banks U.S.-Australia Critical Minerals Partnership Minerals Security Partnership China's rare earth export policies	Blockchain infrastructure deployment across the Lobito Corridor, connecting critical minerals from the DRC and Zambia to the Angolan port of Lobito

Guideline Topic		
International Collaboration & Trade Policy		Blockchain Benefits
Objective	Adherence to requirements companies must follow to source critical minerals from any particular place	Facilitates compliance with corporate due diligence, including regulatory requirements - Creates standardized digital records - Governments and trading partners can access consistent, verified data across jurisdictions.
Themes	Corporate due diligence requirements Regulatory compliance Reporting on labor and environmental practices Providing data to ensure customers of responsible supply chain practices	
Examples	Global Battery Alliance EU Battery Passport US-Mexico-Canada Trade Agreement (USMCA)	Auto makers have begun using blockchain technology to trace cobalt from mine to electric vehicle

STAKEHOLDER PRIORITIES FOR STRONGER GOVERNANCE

The toolbox and methodology proposed above can connect the entire landscape of stakeholders with shared data and knowledge, with the prospect of a better governance model toward supply chain resilience. Any successful framework toward a just transition in critical minerals supply chain governance must involve all stakeholders: from the public sector, civil society, and the private sector – from large companies to small companies and artisanal miners, and the substantial informal economy in many developing countries. Although some players may not be willing to or incentivized to provide transparent data, in cases of concealing sub-par practices, a broader governance system with stronger visibility would make it more difficult to maintain opaque operations.

Despite their various needs and incentives, all stakeholders benefit from greater visibility and validation on data and claims. Once a full blockchain-based chain of custody is achieved, all other concerns and externalities can be better understood and addressed. For instance, if refinery capacity is outsourced to a jurisdiction with lax regulatory requirements, a better system to measure impact (e.g., satellite-based data oracles on water usage, emissions, and forced labor conditions) can shed light on concerning data and justify relocating business to another region. The value of blockchain therefore points to the capacity to strengthen the governance process.

STAKEHOLDER LANDSCAPE: NEEDS, DUE DILIGENCE GAPS, BLOCKCHAIN OPPORTUNITIES

While due diligence gaps risk stakeholder needs remaining unmet, blockchain directly addresses gaps in traceability, transparency, and trust across all stakeholders. In general, upstream tiers of the supply chain (mining, refining) face higher gaps with traceability and ESG verifications. Midstream tiers of the supply chain (manufacturing, OEMs) face gaps around multi-tier visibility and reliance on supplier self-reporting that may not be verified by a third party. Downstream tiers of the supply chain (end users, investors, governments, NGOs) face gaps around data harmonization and monitoring, alongside technical needs to ensure quality of products.

While blockchain doesn't directly solve physical risks (e.g., water pollution, unsafe mining), the visibility it provides enables verifiable accountability, facilitating enforcement and creating incentives toward greater compliance, which eventually should lead to increased investment and opportunity.

Below is a landscape of key stakeholders, specifying their roles, needs, due diligence gaps, and blockchain based tools to address those gaps. (Note: Main stakeholders are marked in navy blue cells, and the information along those rows applies to all stakeholders of their kind. Some stakeholders have sub-categories, listed below them in white cells. Some of those sub-categories may have particular roles, needs, due diligence gaps, and blockchain benefits, filling their respective rows)

MAPPING OF STAKEHOLDER NEEDS

Stakeholder	Role	Needs	Due Diligence Gaps/Risks	How Blockchain Helps
Companies	Companies play the key roles of extraction, manufacturing, and transportation. All companies along the value chain are expected to be regulated. Actors directly involved in the extraction, transformation, and commercialization of critical minerals across the value chain.	Ethical supply chain proofs, especially ensuring provenance and correctly sourcing Regulatory compliance Optimization to improve profit margins: Cost efficient & resource efficient supply chains, alongside methodologies to build and scale their solutions	Multiple requirements across multiple supply chain stages make end to end traceability difficult	End to end chain of custody
Extraction: Exploration & Mining	Search for and extract ores and minerals from deposits	Access to capital and financing Access to skilled labor, especially in remote areas Access to equipment and infrastructure Secure long term mining rights and permits Regulatory clarity and compliance with regulations (e.g., permits, land access, ESG requirements) Local community acceptance to avoid social conflicts Stable price and demand Long-term offtake agreements to de-risk operations and secure cash flow Basic services (e.g., energy, accommodations, water, digital infrastructure/connectivity, tools)	Limited 3rd party verifications on ESG and safety claims Limited community consultation records Limited subcontractor tracking (e.g., small scale and artisanal miners) Challenges proving compliance with requirements, especially (e.g., anti-corruption, royalty payments, regulations)	Smart contracts and tamper proof records for permits, licenses, royalties paid, reducing corruption Digital identities for subcontractors ensure traceability for artisanal mining and smallholder operations Transparent reporting of compliance with ESG requirements and other requirements, for regulators and investors Trusted impact disclosures help build trust with local communities

Stakeholder	Role	Needs	Due Diligence Gaps/Risks	How Blockchain Helps
Artisanal Miners & SMEs	Small scale mining operations	Access to markets, financing, training, and safety equipment (difficult in informal sector) Access to mineral deposits Reliable sources of water, energy, and inputs to perform job Demand for labor Avenues to facilitate formalization Alternative and supplementary livelihood options Basic services (e.g., energy, accommodations, water, digital infrastructure/connectivity, tools)	May not be legally registered, and as such not subject to legal requirements but may regardless need to provide assurances to downstream partners. While artisanal/SME miners may be formally subject to fewer regulations, they will nonetheless face requirements of downstream buyers. These may not be in the form of hard requirements, but due diligence requirements filter down to them	Digital identities can record essential data for reporting and quantify their economic activities
Processing & Refining	Convert raw ores into usable materials, including intermediate stage products, which they sell (passing along validation of upstream supply chain)	Stable and diversified feedstock supply Advanced technologies for processing (e.g., separation, purification, and value addition) to increase yields and reduce waste Regulatory clarity and compliance (e.g., emissions controls, waste management, water usage, chemical usage) Certifications to ensure responsible sourcing and compliance Affordable inputs Energy security Proximity to downstream customers Data from observers and contributors to support compliance Financing	Limited visibility on origin of ores (e.g., mixing legal & illegal supply) Limited and inconsistent reporting on regulatory requirements, ESG and waste management Unclear methodologies for ESG compliance Data silos across miners, refiners, regulators, etc.	Tokenization of ore batches allows end to end traceability from mine to refinery Shared ledgers facilitate standardized disclosures on compliance with requirements, including ESG and waste management Shared and interoperable blockchain records can integrate miners, refiners, and regulators
Manufacturers & Original Equipment Manufacturers (OEMs)	Manufacture materials into parts, components and finished goods (e.g., EV makers, battery producers, electronics producers)	Price stability and predictability to manage supply chain costs Long-term contracts with suppliers Reliable and diversified sources of processed minerals (e.g., high purity materials for magnets, semiconductors, batteries, etc.) Certifications to ensure compliance with standards, sustainability practices, and regulatory requirements (e.g., traceability from mine to factory where electric batteries are manufactured, no conflict minerals, adequate due diligence) Data from observers and contributors to support compliance Substitution R&D research to reduce reliance on scarce minerals	Challenges verifying traceability, human rights standards, and environmental requirements across various tiers of suppliers Rely on supplier verifications, which often self-report and may be unaudited Unclear methodologies for ESG compliance within procurement processes	End to end traceability from mine to refinery, from mine to processing to final product Smart contracts to ensure suppliers are compliant with ESG and other requirements Blockchain records can integrate into procurement processes, product passports, and certifications
End Users & Industries	Sectors that rely on critical minerals in final products. Utilize final products made from critical minerals (e.g., energy, defense, automotive, electronics, aerospace)	Reliability of critical minerals supply to prevent bottlenecks in production Custom material specifications Long-term contracts and supplier diversification Recycling and circular economy strategies (e.g., policy incentives for alternative materials, recycling, etc.) Access to innovation (e.g., batteries requiring less scarce minerals)	Limited visibility on supply chain dependencies and concentration (e.g., reliance on a single country for resources) Limited risk management for geopolitical disruptions Limited collaboration across industries for shared due diligence standards International regulatory requirements are not harmonized	Real time blockchain data provides insights for risk modeling (e.g., supply chain dashboards) Shared ledgers with privacy tools allow coopetition - collaboration without exposing trade secrets Blockchain-based certifications can help align global standards

Stakeholder	Role	Needs	Due Diligence Gaps/Risks	How Blockchain Helps
Recyclers & Circular Economy Players	Recover minerals from used products (e.g., batteries, electronics) and deliver them for production into new products	Efficient collection systems at products' end of life Regulations to encourage recycling and reuse Innovation for cost effective recovery Access to markets for recycled materials (e.g., OEM acceptance) Validation of quality materials recovered	Limited chain of custody verifications for recycling Lack of certifications and standards on recycled materials Limited collection systems make it difficult to prove responsible sourcing for secondary materials Lack of harmonized reporting frameworks on recovery efficiency	Tokenization of recycled materials improves chain of custody verifiability Blockchain based certifications of recycled content can be approved by OEMs for processing Incentive mechanisms using tokenization and credits can encourage collection and recovery behaviors
Logistics & Distribution Entities	Actors enabling the physical and commercial movement of minerals across borders and between supply chain stages. Ensure physical movement of goods across the stages of the supply chain and across country borders	Assurances of supply chain transparency and compliance with relevant requirements (e.g., documentation, certifications) for goods to be accepted at the next stage of supply chain processing or consumption) Adequate infrastructure	Limited visibility across tiers of the supply chain Limited verifications to support claims and documentation provided	End to end traceability and verifications of compliance
Transportation Providers	Move raw materials, intermediates, and finished products across supply chain stages and borders. Physically move goods to next level of processing across supply chain stages, often mobilizing products across borders	Adequate physical infrastructure (e.g., roads, ports, railways) Collaboration with importers/exporters/ customs authorities when transporting over a border Transportation Documentation to clear customs at borders: Freight documentation (e.g., ProForma Invoice, Commercial Invoice, Packing List, Certificate of Origin, Insurance Certificate, Export License, Import License, Bill of Lading, Dangerous Goods Documents, Safety Data Sheets); additional documents including Letters of Credit, Bank Drafts; Jurisdiction specific requirements (e.g., local labor law compliance, inspection certificates and results, signature stamps)	(same as above)	(same as above)
Importers	Bring raw or processed materials into domestic markets for further processing or final consumption. Import materials and products for further processing domestically, or final products for consumption and use	Reliable supply of raw or unfinished materials, or final products Collaboration with brokers and transportation providers Compliance with multiple standards and requirements for trade and trade financing Transportation Documentation: Freight documentation (e.g., ProForma Invoice, Commercial Invoice, Packing List, Certificate of Origin, Insurance Certificate, Export License, Import License, Bill of Lading, Dangerous Goods Documents, Safety Data Sheets); additional documents including Letters of Credit, Bank Drafts; Jurisdiction specific requirements (e.g., local labor law compliance, inspection certificates and results, signature stamps)	(same as above)	(same as above)

Stakeholder	Role	Needs	Due Diligence Gaps/Risks	How Blockchain Helps
Exporters	Ship raw, refined, or finished products to international markets. Export materials and finished goods to markets abroad	Reliable markets with buyers to purchase goods provided Collaboration with brokers and transportation providers Compliance with multiple standards and requirements for trade and trade financing Transportation Documentation: Freight documentation (e.g., ProForma Invoice, Commercial Invoice, Packing List, Certificate of Origin, Insurance Certificate, Export License, Import License, Bill of Lading, Dangerous Goods Documents, Safety Data Sheets); additional documents including Letters of Credit, Bank Drafts; Jurisdiction specific requirements (e.g., local labor law compliance, inspection certificates and results, signature stamps)	(same as above)	(same as above)
Brokers	Intermediaries connecting buyers and sellers, aggregating volumes, and sometimes handling customs, duties, or VAT. Liason between exporters, importers, and manufacturers, often acting as sourcing agents, distributors, and aggregators that can facilitate volume discounts, and may at times pay duties/ VAT fees	Reliable sources of supply and markets with demand Quality assurances and certifications Supply chain visibility for accountability on sourcing of products they sell (e.g., for duty drawbacks) Transportation Documentation: Freight documentation (e.g., ProForma Invoice, Commercial Invoice, Packing List, Certificate of Origin, Insurance Certificate, Export License, Import License, Bill of Lading, Dangerous Goods Documents, Safety Data Sheets); additional documents including Letters of Credit, Bank Drafts; Jurisdiction specific requirements (e.g., local labor law compliance, inspection certificates and results, signature stamps)	(same as above)	(same as above)

Stakeholder	Role	Needs	Due Diligence Gaps/Risks	How Blockchain Helps
Governments & Regulators (public authorities)	Entities shaping the policy, legal, and trade environment for critical minerals. National governments define and enforce regulatory requirements, trade controls, and policy (e.g., managing tariffs, export controls, and strategic alliances). Governments act on behalf of citizens, negotiating critical minerals agreements with other nations and companies globally. Governments levy taxes or other fees (e.g., portion of sales) in exchange for making land available for extraction and production. For some countries, this is a significant portion of government revenue. Regulatory Agencies monitor industry practices, transparency, and environmental/social standards.	Strategic stockpiles and alternative sources of critical minerals to ensure diversification of supply Investment in domestic production and recycling to support domestic markets Mechanisms to reduce dependence on suppliers from geopolitically sensitive jurisdictions Investment incentives to attract domestic exploration and processing Assurances that national security and energy transition goals are being met Assurances of environmental and labor standards compliance Assurances on provenance and governance, especially regarding ethical sourcing System of monitoring and reporting (e.g., regarding commitments made, permits delivered, etc.) Mineral royalties	Inconsistent regulatory frameworks between jurisdictions Lack of real time monitoring of movement of minerals (including imports & exports) Limited enforcement capabilities for labor, environmental, and anti-corruption requirements especially in mining regions Limited capabilities to audit complex and global supply chains	Real time tracking of imports and exports for customs Immutable records facilitate compliance and enforcement Shared data ledgers facilitate cross-border cooperation and standardization of requirements
Port and Customs authorities	Oversee product flows at borders, ensuring compliance with trade and security rules. Validate products passing through borders and key checkpoints	Proof of certifications and validation (e.g., certificates of origin and provenance, compliance checklists) Data on latest requirements to be verified	(same as above)	(same as above)
Investors & Financial Institutions	Organizations providing capital and risk management for supply chain actors. These include financial institutions, private investors, and development banks. They finance large projects to explore and extract minerals, and also companies throughout processing and other steps of the supply chain.	Risk-adjusted returns, especially long-term project stability for large investments Verifications of project compliance with ESG metrics (e.g., emissions reporting to satisfy green finance requirements) and other disclosure requirements (depend on characteristics of the customer) Understanding of the supply chain involved in their investments Supply chain transparency to reduce any reputational risks Government incentives or guarantees to reduce geopolitical risks Policy stability and investment incentives Scalability and return on investment (ROI)	Multiple guidelines and lack of standardized metrics for supply chain risks, hindering due diligence for de-risking assurances Opacity across multiple stages of the supply chain Reliance on company self-reporting and limited verifications on claims (e.g., greenwashing risks) Limited ESG verifications from mining and processing Difficulty tracking geopolitical exposures in investment portfolios	Verified ESG and regulatory reporting directly from source Blockchain-based risk scoring models integrating geopolitical and supply chain data Auditable data trails reduce reliance on self-reporting

Stakeholder	Role	Needs	Due Diligence Gaps/Risks	How Blockchain Helps
Project Finance Entities & Development Banks	Finance large-scale extraction and infrastructure projects, often through syndicated loans. Focus on large and complex investments, often involving negotiations among various financiers for syndicated loans, etc.	Project de-risking and transparency Clear ESG (Environmental, Social, Governance) metrics	(same as above)	(same as above)
Trade Finance Entities	Facilitate global transactions with risk mitigation tools for importers and exporters. Provide financial solutions and risk mitigation services to importers and exporters, to facilitate trade	Understanding of the supply chain involved in their investments, to prevent goods from being seized by customs Derisking measures Assurances on disclosure requirements (depends on characteristics of the investment)	(same as above)	(same as above)
Insurance Companies	Manage operational and political risk exposure in exchange for premiums.De-risking projects by assuming financial risk of projects in exchange for regular payments	Accurate data and understanding of the supply chain, to price the risk accurately	(same as above)	(same as above)
Indigenous Groups & Local Communities	Stewards of ancestral lands and potential partners in agreements toward equitable development (as opposed to companies, especially foreign, extracting and depleting their lands for their own profit maximization at their expense). Rightsholders and land stewards directly impacted by mining and processing activities. Indigenous Groups are custodians of ancestral territories; potential partners in equitable development agreements. Local Communities are populations affected by extraction and production, whose livelihoods and environments must be considered.	Fair compensation and benefit-sharing from mining projects Protections of the environment (e.g., land, water) and cultural heritage Employment, capacity building, and local development opportunities. Transparency and participation in decision making, including free, prior, and informed consent (FPIC) Health protections (e.g., in cases of risks of heightened pollution)	Difficulty accessing transparent data on mining impacts (water use, emissions). Weak mechanisms to verify claims, benefit-sharing agreements, and payments. Limited legal or technical capacity to challenge violations. Lack of participation in formal due diligence frameworks.	Blockchain-based records provide verified data on compliance and environmental and social metrics Smart contracts can automate direct benefit sharing payments

Stakeholder	Role	Needs	Due Diligence Gaps/Risks	How Blockchain Helps
Civil Society & NGOs/ International Organizations	Advocate for community rights, social and environmental justice, and facilitate engagement with governments and companies regarding accountable resource management and development. and development. NGOs & Advocacy Groups promote social, environmental, and governance standards. International Organizations foster multilateral cooperation on resource governance.	Monitoring and accountability frameworks Verifications of enforcement regarding human rights, labor, and environmental standards Transparency in sourcing (e.g., avoidance of conflict minerals) Global cooperation to ensure fair access to markets and economic opportunity for all	Difficult to verify authenticity of claims Limited access to reliable, verifiable supply chain data Lack of global harmonization of certifications Limited resources for monitoring on the ground, and connecting local impacts with global corporate accountability	Automated and verifiable reporting reduces monitoring burden and adds clarity on compliance with requirements and best practices Blockchain records on supply chain data, compliance, and certifications Standardized digital certifications (e.g., conflict-free minerals, fair trade practices, carbon footprint)
Academia & Research Entities	Generate knowledge, innovation, and technical expertise for industry and policy. Expertise and investigations on research on key themes and solutions for the industry use	Funding for innovation in extraction, processing, and recycling Data access and industry collaboration Policy engagement Skills development programs	(same as above)	(same as above)
Workers	Provide basic labor, including miners. This includes the labor force powering the sector, from mine sites to manufacturing plants. Miners provide extraction and on-site labor. Industrial Workers provide operatives in processing, refining, and manufacturing stages.	Considerations: risks they take; health problems faced; wages they may/may not receive	May not know their rights or how to enforce them	Digital identities to better access essential services and make informed decisions Smart contracts to automate direct payments
Other (Data, Standards & Assurance Bodies)	Actors ensuring transparency, accountability, and quality across the supply chain. This includes data providers that are key for decision making.	Assurances of data accuracy	Limited assurances on accuracy of data	Verified data on immutable records, directly from source

Stakeholder	Role	Needs	Due Diligence Gaps/Risks	How Blockchain Helps
Observers	Independent organizations (e.g., trade associations, watchdogs, government observers) that provide risk, compliance, and sustainability data. They provide objective data to help manage risks, without taking part in transactions as direct stakeholders (e.g., lack of compliance with standards/ requirements, geopolitical concentration, volatility). Focus on transparency, accountability, and long term sustainability of critical minerals supply chains.	Accurate data from supply chain stakeholders, used to make decisions Assurances of data accuracy across the supply chain Assurances that data is not tampered with across mine, to OEMs & manufacturers, to consumers, to recyclers, to new production cycles	(same as above)	(same as above)
Contributors	Key stakeholders involved in physical and commercial flows of critical minerals, with a more involved role than observers. Provide data to help make decisions, driving drive production and processing to support critical minerals' use in high tech applications (e.g., scores for raw materials for use in specific industries).). Entities directly shaping standards and practices (e.g., testing labs, certification bodies, standards setters).	Accurate data from supply chain stakeholders, used to make decisions Assurances of data accuracy across the supply chain Assurances that data is not tampered with across mine, to OEMs & manufacturers, to consumers, to recyclers, to new production cycles	(same as above)	(same as above)
Auditors	Independent third parties verifying compliance with regulations and sustainability frameworks.	Accurate data and requirements for verifications	Data silos and lack of accurate data along entire supply chain	Verified data on immutable records, directly from source

COOPETITION IS THE NAME OF THE GAME

Blockchain technology can be a source of competitiveness for all stakeholders, while better promoting peace and prosperity, especially for an industry that is inherently global. While critical minerals supply chains are deeply embedded into the interests of multiple nations, with various players and competing agendas that have historically resulted in multiple conflicts, technological solutions that improve visibility can lead to win-win situations among stakeholders toward a better governance framework that benefits all.

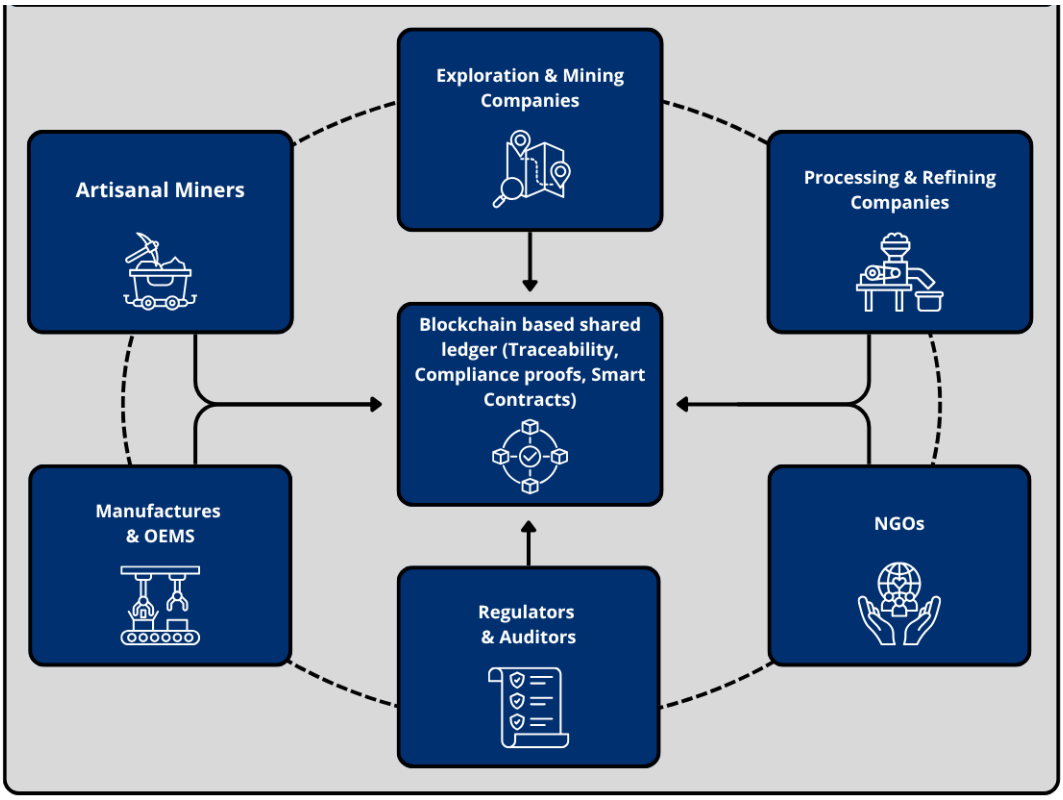
By facilitating compliance with requirements and strengthening due diligence, blockchain technology can be a tool to support alignment of interests, with numerous resulting benefits that broaden economic opportunities for all, including:

- **Minimizing data silos to better address any supply chain vulnerabilities**
- **Better coordination to attract investment and direct financial aid more effectively**
- **Optimized technical support**
- **Technology transfer to support the needs of low-income nations**
- **Enhanced international cooperation to harmonize standards and requirements**
- **More effective risk mitigation initiatives**

For instance, mining entities derive the greatest value from blockchain-based traceability, auditability, and smart contracts. Recycling entities would greatly benefit from incentives toward collection and recovery. Governments, investors, and NGOs can lean on standardization, auditability, and transparent records.

"Coopetition," a concept of cooperative competition, is particularly promising for critical minerals supply chains where both nations and companies compete for access to limited resources, as well as the rights to extract them upon meeting regulatory, environmental, and other ethical requirements. Blockchain facilitates coopetition by providing a neutral and trusted shared infrastructure that allows competitors to collaborate toward shared goals of compliance, traceability, and risk management, while still seeking competitive advantage based on other factors such as price, efficiency, and customer loyalty.

Innovation can lead to a turning point, as a source of competitiveness that can facilitate "co-opetition" dynamics for win-win outcomes for all stakeholders and local communities. In collaborating toward greater transparency and trust, trading partners can increase the market opportunity for all, in ways that favorably influence international relations.



PROPOSED AFRICAN PILOT: DIGITAL STRATEGY FOR MONITORING CRITICAL MINERAL VALUE CHAINS, MINING AGREEMENTS, PROTOCOLS AND LICENSES AND DIGITAL CORRIDORS

INTRODUCTION

Enhanced international collaboration is crucial for a sustainable global raw material governance, including technical support, financial aid and technology transfer to support the needs of low-income nations. There are a number of initiatives and platforms in the field of responsible mining management and responsible value chain management in DRC. The project intends to offer three added value to the several initiatives in place, as well as companies, development banks and private investors from China, Europe, USA, willing to *Improve responsible sourcing of raw materials and responsible business conduct initiatives with regard to raw materials* in DRC:

i. The project is designed to offer a meeting place to address responsible sourcing governance, responsible business, impact financing and “regional” development under the leadership of the DRC authorities.
ii. There are a number of regulations, standards, etc. in the mining sector. Without funding to implement them we will not progress. The project Is designed to develop a collaborative process between investors and donors to finance a responsible sourcing blockchain eco-system to improve the implementation of existing rules.

iii. This blockchain strategy should aim to have a strong market structuring power while China controls 80% of the cobalt production in DRC and the EU as well as the USA and Zambia have signed 'batteries protocols' with DRC while the EU is announcing a "*blockchain batteries passport*".

This project, based observations that *most due diligence framework fall far short of robust risk management*[139] and based *on the experience of existing responsible sourcing initiatives supported by the EU and USA*, intends to be the kind of pilot *needed to enable a level playing field for responsible sourcing of raw materials, Identify and address gaps in the raw materials supply chains due diligence in close cooperation with the* Digital Development Agency (ADN) within the Cabinet of the President of the Democratic Republic of COngo which supports this project and has identified 3 main challenges: (i) Management in the context of an ongoing armed conflict in Eastern DRC (ii) Multiple Legislations at national, regional and local levels in the DRC and at the EU level (iii) Financial resources. As demanded by ADN this project aims to:

- A cooperation agreement between countries of the Region leading to a regional standard
- Consistency between multiple legislative provisions by creating a place for joint review
- An intelligent border control system
- Sharing and pooling of IT infrastructures

Batteries will be the first product category to be legally required to comply with DPP, sometime in 2026. To be impactful, digital product passport technology needs to be based on open standards, be open source, permissionless and decentralized. This *project* will *build on the state of the art in sustainable raw materials traceability, transparency, accountability and decentralized collaboration organization. It will link with existing EU projects related to international* ***responsible sourcing, responsible business, digital tools*** *to contribute to strengthening responsible sourcing agenda from a geopolitical, technological, governance and financial standpoint*.

Promoting knowledge exchange among countries and regions plays a pivotal role in enhancing governance standards. To ensure effectiveness, measures and initiatives should be tailored to local conditions and aligned with national capacities and frameworks. Only a collaborative and coordinated approach can avoid redundancies among existing instruments and initiatives, and enable a cohesive response to the diverse challenges of resource management.

This proposed pilot aligns with current and upcoming African leadership of key global bodies including South Africa, hosting the G20, Angola and Burundi chairing the African Union in 2025 and 2026 respectively, and the Democratic Republic of Congo (DRC) sitting as member of the Security Council in 2026. This digital strategy could benefit from being highlighted both within the framework of processes under the aegis of both the African Union and the American Administration, as well as at the level of the United Nations and during the 7th Africa-Europe Summit.

The implementation of a strategic partnership between the Democratic Republic of Congo (DRC), Rwanda and the United States of America (USA) and its Companies (KOBOLD METALS) relating to critical minerals, is one of these agreements that should have a digital strategy.[140] A digital strategy is an essential element of governance in the age of the digital revolution in order to ensure African countries a decisive and fair place in the global chain of transition minerals (green economy, digital and energy transition). The developments towards peace between the DRC and Rwanda would expand opportunities underlying development of the Lobito Corridor (Angola, Zambia, DRC) as well as other critical minerals value chains across southern Africa.

The digital strategy, which we define as "*a driving force for strategic change and transformation of economic, financial, social and cultural models*", should have the following components:

1. **Integrated digital corridor for strategic and critical minerals:** development of an "*Integrated Development & Value*" approach intended to ensuring that maximum value remains in Africa for the economic growth and socio-cultural development of local populations.

2. **Creation of a digital ecosystem** for "*Monitoring, reporting, verification, accountability, trust*" intended to cover the expectations of States, Investors, Rating Agencies and Companies (having an exploitation or exploration permit or being involved downstream in the value chain) to ensure traceability, verification of commitments made (critical minerals passport, taxation system) and thus facilitate international trade.

3. **Creation of an international forum** on strategic and critical minerals (in line with the dynamics of the ongoing partnership discussed above): bring everyone around the table to have governance that leads to "stimulating excellence". This would also constitute a means of "balancing pressures" emanating from multiple actors, gathered in "hubs" each covering a specific ecosystem in view of the lessons learned from the OECD 2025 Forum on *Responsible Mineral Supply Chains* (5-7 May 2025). These would be the following hubs:

    iv. the African ecosystem, including government, civil socierty and business;
    v. the US ecosystem, including government, financial institutions, businesses including those involved in exploration & extraction as well as end-users, and civil society (NGOs, networks and foundations including the (GBBC);
    vi. the Chinese ecosystem, which includes, in addition to the Government, the Chamber of Commerce for Metals and Minerals (CCCMC), networks, and the 500 companies involved in an "Africa-China Alliance for the Protection of Human Rights";
    vii. the European ecosystem in all its diversity;
    viii. ecosystem of emerging actors: Saudi Arabia, Australia, Canada, United Arab Emirates, India, Qatar, Turkey, present or negotiating with the DRC and/or partner countries in the region (Zambia) for critical minerals.

This digital strategy prepared with the BC100+ and GBBC organizations would define a strategy to use technology to:

i. Establish a robust traceability framework that would build on the United Nations call for a "*Global Traceability System for Transition Minerals*," by jointly establishing a framework among trading partners, with technical support, to prevent social and environmental harms along supply chains;
ii. Cover the entire transition minerals value chain and its actors, including in importing countries, monitoring revenue distribution while eliminating illicit flows of resources and funds;
iii. Be integrated to provide transparency into fiscal operations to ensure that all minerals are accounted for and taxes are collected appropriately;
iv. Provide support for agreements with neighboring countries to facilitate cross-border traceability, especially for regionally processed minerals.

Blockchain for the UN Charter Values and the SDGs (BC100+), of which GBBC is a signatory, could collaborate together with the organizations responsible for digitalization issues in the African countries affected by the Lobito Corridor (Angola, Zambia, DRC) and provide expertise relevant to:

i. The implementation of blockchain technologies and artificial intelligence (AI) to support transition mineral value chains, the search for alternative investments, permits, industrialization in Africa, and digital trade;
ii. A digital strategy to support existing and complementary initiatives for regional peace, those of the United States, the African Union, and the United Nations;
iii. Building the confidence of investors and rating agencies;
iv. The USA-DRC-Rwanda Agreement,
v. The Africa-Europe Partnership and related protocols.

To ensure the relevance, consistency, and added value of this strategy, an **Observatory and Forum on digital related developments** could be established to provide all stakeholders with the necessary information and report on progress, which constitutes a confidence-building factor and a starting point for further progress.

We remain available to assist authorities and businesses in developing this digital strategy, identifying desirable ecosystem members and the digital infrastructure to be put in place to achieve the objectives, and, as an integrator, ensuring an integrated systems approach utilizing all the tools offered by the digital revolution, including AI.

CONCLUSION

In light of the complexity of critical minerals supply chains, this report offers a 'methodology' and a 'tool box' for global supply chains that can enable greater supply chain resilience through a stronger governance framework that is by definition trans frontier.

Accountability and trust processes are necessary for sustainable and ongoing projects across critical minerals supply chains. Stakeholders are expected to require increasing transparency assurances (e.g., requirements for purity of materials, assurances of no conflict minerals or forced labor), and compliance can be accelerated with the use of blockchain technology for the benefit of all.

Many of the recommendations below apply to today's particular geopolitical context: with a global tariff environment, global political ideological competition, and a regulatory environment that demands provenance, as indicated by increasing international agreements and protocols. Ensuring access to markets for goods produced with critical minerals requires taking measures to prevent shipments from getting blocked at a border or sent back due to lack of import/export requirements, or lawsuits around lack of compliance (e.g., tech companies being sued due to conflict minerals, trade related issues in rubber glove manufacturing).

By adopting the proposed approach, stakeholders across the critical minerals supply chain ecosystem can achieve unprecedented visibility without sacrificing security – turning trust from a vulnerability into a strategic asset, while ensuring the financial benefits of the value chain are realized locally.

RECOMMENDATIONS

1. A blockchain-based governance framework for critical minerals supply chains should:

- Initially focus on high-level themes to address (e.g., structure of the project and logic of the solutions), and at later stages focus on technical aspects
- build on the experience of existing responsible sourcing initiatives and international discussions (e.g., OECD program on critical minerals)
- Take steps to disrupt and dismantle any illegal infrastructure used by bad actors to distribute and operate unauthorized versions of data

2. Engage diverse blockchain players (from blockchain consortia, DAG-based IoT platforms, etc.) alongside critical minerals supply chain stakeholders to address supply chain challenges holistically

- Conduct initial assessments, including implementation of penetration & security testing tools to identify cyber-attacks and other supply chain vulnerabilities

3. Pursue agreements with key stakeholders toward a global blockchain strategy that is integrated with their common concerns and considers their various needs.

- Engage key stakeholders for a global strategy on responsible sourcing, where blockchain technology can be critical in developing a trusted ecosystem for global trade performance.
- Identify a designated entity to enforce conformance to a single framework/standard
- Unitize DLT Innovations: Recognizing hashgraphs, Directed Acyclic Graphs (DAGs), public ledgers, and permissioned blockchains as equally valid tools for supply chain resilience.
- Split Traceability & Provenance: Align solutions with specific use cases rather than forcing one-size-fits-all systems.

4. Define common global standards for transparency and security of data

- Education, training and awareness to address public perception is that blockchain makes sensitive data public, and instead focus on privacy preserving tools and best practices
- Define who should own and be entitled to access what data on shared ledgers, and what data should remain private vs. made public
- Define requirements around data property, drawing on lessons from other open data frameworks (e.g., open banking)
- Ensure interoperability and data sharing parameters across supply chains and across blockchains, drawing on lessons from internet and computer protocols
- Consider when and how it would be beneficial to classify data as property, to shift focus from data privacy to data property rights. Draw on W3CI verifiable credentials standards for selective disclosure.
- Prioritize Data Ownership: Ensure participants control what is shared, with whom, and under what terms.

ANNEX

ANNEX 1: TAXONOMY

- **CAHRA:** conflict-affected & high-risk areas
- **CoC:** chain-of-custody;
- **RMAP:** Responsible Minerals Assurance Process (RMI)
- **Upstream:** processes and network of suppliers and raw material providers that are located before a company's main manufacturing or production stage
- **Downstream:** activities that occur after a product is manufactured, which are focused on delivering it to the final consumer
- **Tiers:** Categorize suppliers based on their relationship to the final product, creating a hierarchical structure that moves from direct suppliers to raw material providers (e.g., Tier 1 suppliers are direct partners who provide goods or services to a company, Tier 2 suppliers are the companies that supply Tier 1 suppliers, and Tier 3 suppliers supply the Tier 2 suppliers, etc.)
- **Conflict Minerals:** mined in conflict-affected regions, whose sale provides funding for armed groups, human rights abuses, and violence

ANNEX 2: STANDARDS & FRAMEWORKS FOR CRITICAL MINERALS

GLOBAL FRAMEWORKS

- OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected High-Risk Areas – Due Diligence and guidance, with a 5-step framework for risk-based due diligence (strong management systems, identify and assess risk, strategy to respond to risks, due diligence audits, due diligence report), model policy, and suggested measures for risk mitigation. This provides a template that many laws and exchanges reference.

- UN Guiding Principles on Business & Human Rights (UNGPs) — Due diligence framework for human rights that many regulators and standards align with.

- IFC Performance Standards on Environmental and Social Sustainability — Project-level expectations to identify, avoid, and manage risks, frequently applied to mining and used by lenders. Based on 8 Performance Standards: risk management, labor, resource efficiency, community, land resettlement, biodiversity, indigenous people, cultural heritage.

- Extractive Industries Transparency Initiative (EITI) Standard (2023) — Global benchmark for transparency and accountability in the oil, gas, and mining sectors, often a country-level requirement. Provides a framework for disclosure and multi-stakeholder oversight for transparency in extractive industry practices (e.g.., revenues, contracts, beneficial ownership).

- Global Industry Standard on Tailings Management (GISTM) — Principles for tailings safety and disclosures, which key stakeholders including the International Council on Mining and Metals (ICMM) targets conformance with.

- United Nations Conference on Trade and Development (UNCTAD) Global Report on Blockchain and its Implications on Trade Facilitation Performance — Provides a policy and technical framework, considerations, and recommendations for blockchain deployment in global trade.

- UN Secretary-General's Panel on Critical Energy Transition Minerals — Intended to guide a just and sustainable transition for critical minerals, producing 7 Guiding Principles and a subsequent UN Guidance for Action emphasizing environmental and social standards, community benefits, and responsible governance across the lifecycle of critical minerals.

- International Labor Organization (ILO) Skills and Lifelong Learning Strategy and related initiatives – Focus on to creating equitable and resilient skills systems strengthening policies, governance, and financing with specific pillars.

MAJOR REGULATORY REQUIREMENTS

European Union

- Conflict Minerals Regulation 2017/821 — OECD-aligned due diligence for EU importers of tin, tantalum, tungsten, and gold (3TG).
- Battery Regulation 2023/1542 — Due diligence on raw materials (e.g., cobalt, lithium, nickel) used in batteries, in addition to traceability, data, and public reporting.
- Corporate Sustainability Reporting Directive (CSRD) — Requires large companies to disclose supply chain impacts under the European Sustainability Reporting Standards (ESRS), impacting mineral sourcing disclosures.
- Corporate Sustainability Due Diligence Directive (CSDDD) — Human-rights and environmental due diligence across value chains.
- Critical Raw Materials Act (CRMA) — Sets 2030 benchmarks for EU extraction, processing, recycling capacity, faster permits, and risk monitoring for listed "strategic/critical" materials.
- Carbon Border Adjustment Mechanism (CBAM) – trade policy tools to ensure competitiveness for domestic industries, with measures to prevent carbon leakage (moving carbon-intensive production outside of a jurisdiction with stricter climate policies). CBAM places a carbon cost on imported goods, based on their embedded greenhouse gas emissions. This largely applies to high-carbon industries (e.g., cement, steel, and fertilizers).
- EU Digital Product Passport (DPP) for Electric Batteries– Implementation of the EU Digital Product Passport (DPP) for Electric Batteries supports the collection and sharing of product-related data among supply chain actors, addressing information gaps for products and components and enabling circularity.

United States

- SEC Conflict Minerals Rule **(pursuant to Dodd-Frank - section 1502 and Code for Federal Regulations)** — Form and rule requiring annual disclosures of critical minerals originating from certain jurisdictions (in and around Democratic Republic of Congo) and due diligence measures on source and chain of custody.
- Uyghur Forced Labor Prevention Act (UFLPA) — Establishes rebuttable presumption of forced labor for goods mined, produced wholly or in part to the Xinjiang Uyghur Autonomous Region (XUAR) of China, or by an entity on the UFLPA Entity List, requiring intense scrutiny upstream inputs such as polysilicon.
- Inflation Reduction Act (IRA) and Treasury final rules/IRS regulations — Provisions under federal income tax credits for the purchase of qualifying new and previously-owned clean vehicles, requiring a tracing methodology. Guidance for Advanced Manufacturing Production Credit clarify that vehicles only qualify if critical minerals for batteries and components meet sourcing thresholds and do not originate from a Foreign Entity of Concern (FEOC). Department of Energy issued final Guidance on Definition of Foreign Entity of Concern in parallel.

Other Jurisdictions

- Fighting Against Forced Labour and Child Labour in Supply Chains Act (Canada) — Requires annual reporting on steps to prevent and mitigate forced labor and child labor in supply chains.
- UK Modern Slavery Act (UK) – Criminalizes slavery and human trafficking, requiring transparency statements on modern slavery risks in supply chains and responses.
- Modern Slavery Act (Australia) — Requires large Australian businesses to report on their measures to combat modern slavery in their operations and across their supply chains.

GLOBAL STANDARDS FOR MANAGEMENT & MEASUREMENT

- ISO 22095:2020 **(Chain of Custody — terminology & models)** — Defines a framework for accepted design, implementation, and management of chain of custody (e.g., segregation, mass-balance, etc.) in mining schemes.
- ISO 14001 (Environmental Management Systems (EMS) & 2024 Climate Action Amendment — Framework for organizations to design and implement site and corporate EMS, and continually improve their environmental performance, integrating readily with mining standards
- **ISO 14040/14044 Life Cycle Assessments (LCA)** — Framework to evaluating environmental impacts of a product or service throughout its lifecycle, with ISO 14040 defining the principles and ISO 14044 providing detailed requirements for each phase.

INDUSTRY INITIATIVES & FRAMEWORKS

- London Metal Exchange (LME) Responsible Sourcing — Metal brands listed for trading on LME must meet human rights and responsible sourcing standards, aligned with OECD Guidance. Non-conformance risks suspension.
- Responsible Minerals Initiative (RMI) – Responsible Minerals Assurance Process (RMAP) – Audit program for smelters and refiners across multiple minerals, aligned with OECD Guidance. RMI Blockchain Guidelines also establish a voluntary framework to standardize the application of blockchain in critical minerals supply chains, focusing on common principles to improve due diligence and promote interoperability.
- Initiative for Responsible Mining Assurance (IRMA) — Comprehensive site-level mining standard referencing ISO 22095, with chain of custody models (e.g., segregated, controlled blending, mass balance).
- Copper Mark — Site-level responsible production and chain of custody requirements for product claims, in addition to climate, circularity, and other supply-chain considerations. Also provides Nickel, Molybdenum, Zinc Marks for those respective mineral supply chains.
- Aluminum Stewardship Initiative (ASI) — Performance standard and chain of custody requirements for bauxite-to-aluminum supply chains.

GLOBAL SUMMITS & CONVENING INITIATIVES

- G20: Includes agenda to harness critical minerals for inclusive growth and sustainable development
- OECD Forum on responsible mineral supply chains: Addresses key topics related to responsible business conduct and due diligence of minerals through plenaries, partner sessions and deep-dives
- European Commission Raw Materials Week: High-level sessions, policy discussions, and networking opportunities focused on the sustainable and secure supply of raw materials in Europe.

- Global Batteries Alliance: convening actors across the value chain to align on sustainability performance expectations for batteries around principles of transparency, traceability, accountability and circularity.
- Just Transition: principles, processes, and practices that build economic and political power to shift from an extractive economy to a regenerative economy

ANNEX 2: CONSIDERATIONS FOR BLOCKCHAIN TOOL BOX

SECTION 1: SECTOR CRITICAL MINERALS SUPPLY CHAIN, TRADE PERFORMANCE AND COMPANIES' PRIORITIES AROUND ETHICS, SAFETY, ANTI-CORRUPTION, COMMUNITY SUPPORT, ENVIRONMENTAL PROTECTION, ANTI-DISCRIMINATION, AND INTEGRITY.

- The digital product passport and mineral exports in a cradle-to-grave value chain (see with EU), supply chain transparency and value chain traceability
- Intelligent Border System and cross border clearance
- Stakeholder coordination
- Payment processing and trade finance
- Trade risk management
- Trade reporting
- Sharing and pooling of IT infrastructures, training.
- Traceability platform for mining and raw materials tracking systems (e.g., active in DRC, Kenya or Rwanda)
- Responsible sourcing of cobalt through an OECD-compliant blockchain certification platform (e.g., as in DRC)
- Enhance the traceability of tantalum, (e.g., Rwanda)
- Tax transparency (e.g., Roadmap protocol EU/DRC)
- Tax revenues collected and redistributed
- Workers' safety
- Workers' revenues
- Child Labor

SECTION 2: STAKEHOLDER CO-DEVELOPMENT ACTIONS

Digital tools so that no one is left behind, in line with globally-identified targets.
The 'digital corridors' will not be limited to sectoral aspects, minerals in this case. They will cover all aspects of the lives of local populations that can be improved (access to finance, loans, education, health, trade, insurance, etc.) including consideration of stakeholder priorities such as:

- Diploma Certification (as in Ethiopia and Congo)
- Digital identity and payment solutions for the unbanked and underserved across Africa
- Certify Land Ownership in Agricultural and Forestry Areas
- Cryptocurrencies serving the poorest (e.g., Kenya, Niger, South Africa, and Uganda)
- Fintech apps fighting against financial exclusion (e.g., Cameroon)
- Micro-jobs (e.g., with the World Food Program)

- Micro-insurance (e.g., Kenya)
- Health aid through the diaspora (e.g., Cameroon)
- Enhanced transparency, security, and efficiency in African healthcare (e.g., Nigeria)
- Affordable home financing (e.g., Mozambique, Zambia and other African countries)
- Education (e.g., with UNICEF in Rwanda, Niger, and Kenya)
- Renewable Energy DRE solutions provider (e.g., Nigeria)
- Training in blockchain technologies

SECTION 3. ACTIONS THAT FALL UNDER THE SOLE JURISDICTION OF GOVERNMENT

- Digital identity (e.g., Kenya)
- Management of public funds (e.g., Burkina Faso and Ethiopia)
- Monitoring of judicial decisions and the protection of children

ANNEX 3: COMPARATIVE REVIEW | CTP ENHANCEMENTS ACROSS 12 MINERAL SUPPLY CHAIN STANDARDS

View the Comparative Review here.

ANNEX 4: EXCERPTS FROM THE WORLD RESOURCES FORUM ANNUAL REPORT 2023[141]

'Rethinking Value – Resources for Planetary Wellbeing' has focused on three key transitions with the potential to make resources a driver for shared wellbeing within planetary boundaries. Here is a snapshot of some of the main takeaways highlighted in the conference report.

GOVERNANCE OF RAW MATERIALS KEY TO ACHIEVING THE SDGS

There is a pressing need to institutionalise resource governance in the global agenda, while simultaneously redefining resource utilisation strategies. Raw materials governance needs to be better integrated with the Sustainable Development Goals, beyond a mere association with sustainable production and consumption patterns (SDG12). Institutionalising resource governance is crucial because it acknowledges the pivotal role of resource use in achieving sustainability across multiple facets of development, such as ending poverty, advancing health and wellbeing and protecting terrestrial and marine ecosystems.

NO ALTERNATIVE TO RESPONSIBLE SOURCING

The rapid growth of the critical raw materials market has given rise to environmental and social concerns related to their extraction. A comprehensive approach to responsible sourcing is required, one that is grounded in collaborative multi-stakeholder cooperation involving businesses, governments, financiers, workers, communities and civil society representatives. Monitoring and reporting mechanisms for responsible sourcing should be developed and implemented across global supply chains. Expectations for responsible extraction have moved ahead of legal compliance, requiring companies to demonstrate social performance beyond what is regulated. Shifting from risk management to value creation is essential for sustainable supply chains.

WE NEED TO HARNESS THE INFLUENCE OF THE FINANCIAL SECTOR

The finance sector has an important role in demanding best practices from companies across various industries, particularly in an environment where reporting standards are predominantly voluntary and diverse. Strengthening sustainability requirements for financing and enhancing the availability of robust data for informed financial decision-making are critical.

Finance can also play a key role in enabling nature-positive funding, such as for the restoration of healthy natural ecosystems. Public and private finance should also be strategically leveraged to phase out environmentally damaging activities

A MORE EQUITABLE VALUE DISTRIBUTION IS NEEDED

Currently, the distribution of value created is highly unequal and concentrated at the top. This calls for strong democratic institutions that actively promote the engagement of local communities. Policy-makers should set in place policies and processes that empower individuals to assert their rights and partake in decision making, ensuring a more equitable distribution of value throughout society (p14)

ENABLE TRANSPARENCY THROUGH OPEN, TRUSTWORTHY AND DECENTRALISED DATA EXCHANGE

Digital product passports have a huge potential to enable businesses and consumers to access comprehensive information about a product's origins, materials, and lifecycle. Transparency promotes the circular economy by facilitating repurposing, remanufacturing and recycling, and encourages companies to design products with sustainability in mind from the outset. It also acts against green-washing attempts, as it proves that products are coming from sustainable sources and that the ESG criteria are met. To be impactful, digital product passport technology needs to be based on open standards, be open source, permissionless and decentralized

STRENGTHEN GLOBAL COLLABORATION ON RAW MATERIALS GOVERNANCE

Enhanced international collaboration is crucial for a sustainable global raw material governance, including technical support, financial aid and technology transfer to support the needs of low-income nations. Promoting knowledge exchange among countries and regions plays a pivotal role in enhancing governance standards. To ensure effectiveness, measures and initiatives should be tailored to local conditions and aligned with national capacities and frameworks. Only a collaborative and coordinated approach can avoid redundancies among existing instruments and initiatives, and enable a cohesive response to the diverse challenges of resource management

RESTORING CONFIDENCE IN THE MINING SECTOR THROUGH ACCOUNTABILITY AND TRANSPARENCY

The mining sector faces a notable crisis in trust and confidence, particularly among local communities, civil society organisations, and consumers. Given its pivotal role in enabling the trasition to clean energy, it is of paramount importance that the mining industry regains the trust of these key stakeholders. Accountability and transparency play a central role in rebuilding this trust. To achieve this, the mining sector must provide accessible and comprehensive data sharing and transparent information regarding its social, environmental and economic performance.

HARMONISING STANDARDS FOR RESPONSIBLE MINING

As mineral value chains are global in nature, varying standards can lead to inconsistencies and challenges in assessing environmental and social impacts. By harmonising these standards, we can create a unified and globally recognised set of guidelines that not only streamline compliance, but also enhance transparency, accountability and the overall sustainability of mining activities. The convergence of standards fosters a shared commitments to responsible mining practices, benefitting not only the environment but also the wellbeing of local communities and the industry as a whole (p19).

Materials-as-a-Service (MaaS) are new potential approaches to resource governance and business models for metal and mineral value chains. The model is based on the idea that resource rich countries/communities retain the ownership of metals and minerals mined on their territory and market. the materials as a service (i.e. leasing). This means instead of selling the materials themselves only the usufruct (the right to use these materials and gain a benefit from their use) would be sold along the value chain. The sale of the usufruct would be combined h the contractual obligation to guarantee the recoverability of materials at any point in time (p21)

Innovative Partnerships for Responsible Resource Use in Africa

In the context of a general decreasing trendline for Africa's natural capital, it should be re-minded that African land is critical to resilience and the urgent need for sustainable management to move from natural reliance to natural resilience. The move from 'natural resources' to 'natural capital' could cause a shift in the understanding of value and materiality.

- There is still an imbalance in the relationship between the African continent and the global north, with Africa bearing the ecological and social costs of high-income country's resource use. Systematic transitions could transform natural resources and capital into social wellbeing.

- Effective governance is the first step to overcome the challenges Africa is facing today with natural resources management. Among those challenges, are illicit financial flows, political instabilities, a lack of transparency and accountability, the absence of clear legal and policy frameworks for natural resources management, and also the asymmetry of power between global north and global south. A framework which integrates human rights and responsive business practices is needed to ensure both the protection of the environment and symmetric relationships.

The valuation of natural resources should not only be looked at from a global lens, but also from the perspective of local communities. Especially, innovative partnerships are important tools to empower local communities and ensure that they share in the benefits of resource use. Three critical levers need to be activated. First, we should look beyond the private and public sector to move toward integrated finance and thus make available new resources.

Second, an improved financial literacy to translate knowledge into action but also to foster synergies and cooperation between finance and other stakeholders of biodiversity cooperation. Third, local and national discussions along the ones at global scale are needed to enable a responsible use for Africa (p37).

ADDITIONAL RESOURCES

- https://www.congress.gov/crs-product/R47982
- https://www.wrforum.org/wp-content/uploads/2023/07/ECTR-2023.pdf
- https://www.oecd-events.org/responsible-mineral-supply-chain-2025/en; https://www.oecd.org/en/events/2025/05/oecd-forum-on-responsible-mineral-supply-chains.html
- https://www.sustainablemanufacturingexpo.com/en/articles/digital-traceability-metals.html
- https://www.africaeuropefoundation.org/areas-of-action/new-aef-scoping-paper:-revamping-africa-europe-cooperation-on-transition-minerals/
- https://drive.google.com/file/d/1xsN-_QnX48W9aAcccxy6YYXkXckeFzxw/view
- https://www.peerledger.com/ev-and-critical-minerals
- https://www.responsiblemineralsinitiative.org/news/rmi-releases-new-standard-suite/
- https://www.cobaltinstitute.org/global-cobalt/cobalt-value-chain/
- https://assets.ctfassets.net/so75yocayyva/1rFWV6NOCREBzPgWIyJ0GY/589d2e140aa9d64a70ab31e04637587a/As_of_May_14_-_Just_the_Facts_Supply_Chains.pdf
- https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/battery-2030-resilient-sustainable-and-circular
- https://www.globalbattery.org/media/publications/WEF_A_Vision_for_a_Sustainable_Battery_Value_Chain_in_2030_Report.pdf
- https://www.mckinsey.com/capabilities/operations/our-insights/supply-chain-risk-survey
- https://www.bbc.com/news/articles/cn8g540wz3jo
- https://www.koboldmetals.com
- https://positiveblockchain.io/africa-impact-web3-report

GBBC
Global Blockchain
Business Council

STANDALONE REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 6.0

TECHNICAL STANDARDS

GBBC GSMI 6.0

ACKNOWLEDGEMENTS

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

Dan Conway - CO-CHAIR
Teaching Professor, Associate Director of the Blockchain Center of Excellence, University of Arkansas

Neil Wasserman - CO-CHAIR
Adjunct Professor in Computer Science, The George Washington University

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

INTRODUCTION

Technical standards are documented, agreed upon rules for design, production, and use of a technology or system. Technical standards may impact design, performance, processes, or testing, in addition to establishing basic safety and quality benchmarks. They provide harmonized criteria, guidelines, and characteristics that ensure consistency for a given product that have been reconciled amongst a Committee, over a period of time, in consultation with the intended users and providers of the deliverable. With greater uniformity comes increased interoperability and reliability. Standards enable technology to thrive by minimizing unproductive options and decision making. Ultimately, standards are fundamental for scale for any emerging technology and are relied on by both early implementers and later adopters to guarantee interoperability across platforms.

WHY STANDARDS?

The goal of standards:

- Common guidelines based on agreed upon rules and definitions
- Ensure functionality, with interoperability for scale
- May precede regulatory developments
- Necessary for reliable, safe, continued innovation

Standards also support a dynamic of “coopetition,” where the opportunities become greater for all players by collaborating on certain parameters. Standards are the “cooperation” part of coopetition, bringing alignment to areas where entities are not competing but that represent common goals among them, even among competitors. From a commercial viewpoint, the reason for many organizations to participate as experts in standards setting committees is to get insight on upcoming trends and be able to take action in that direction.

STANDARDS SETTING BODIES

There is a wide range of organizations involved in standards setting initiatives blockchain and digital assets.

GLOBAL STANDARDS SETTERS

Globally recognized, formal standards setting bodies sit at the top of the hierarchy of standards setting – namely organizations like the International Organization for Standardization (ISO), which influence regulations as well as regional and national standards. They have the greatest weight in standards, with their work driving the output and activity of most other organizations in the ecosystem of standards setting. In the ecosystem of standards setting initiatives, formal standards setters can be distinguished from all other organizations by the status and authority they command.

These organizations function solely to develop, publish, and promote technical standards to be accepted and used internationally. They are fundamental for a technology to scale by promoting harmonized rules and understandings with the greatest weight.

As formal bodies, they collaborate across nations (through representative expert organizations) and industries, bringing together key stakeholders and experts toward agreement. Technical committees, generally comprised of member organizations, lead standards development work (e.g., ISO/TC 307 focused on blockchain), alongside national standards bodies representing countries (e.g., BSI for UK, ANSI for US), liaison organizations which may be other standards bodies, and expert individuals appointed by member bodies. While formal standards setters have global influence, these organizations remain neutral in their mission to harmonize technical standards globally through rigorous consensus-driven processes.

The respect granted to global standards setters is largely due to their impact promoting global trade and globalization, in addition to consumer safety. Global standards setters also facilitate regulatory compliance, ultimately improving trust in any given product, innovation, or industry subject to the technical standards they develop. By improving interoperability and global compatibility, they also facilitate ongoing innovations and their scale.

REGIONAL STANDARDS ORGANIZATIONS

These bodies aim to harmonize standards among countries or states (which may participate as members), serving as a bridge between national and international standards. They promote trade and interoperability across their respective regions, while supporting regional regulatory integration. One example of such integration is the EU Single Market initiative.

NATIONAL STANDARDS ORGANIZATIONS

National bodies are responsible for developing and maintaining common standards within a given country, helping businesses understand and implement them. They also represent their respective countries in international standards bodies. Some countries have formalized national standardization committees (e.g., INCITS/Blockchain for USA, SAC/TC 180 for China, Slovenian Institute of Standardization – SIST/TC Blockchain) that author and publish national standards, while also serving as the Technical Advisory Group (TAG) representing the country at international standards committees (e.g., ISO/TC 307 for blockchain technology), where they provide inputs for global standards setting process and also help adopt global standards.

INDUSTRY-SPECIFIC STANDARDS ORGANIZATIONS

Industry-specific standards bodies develop standards for a specialized field or technology, focusing on rapid development of technical standards to drive innovation and interoperability. Their standards are often considered de facto standards prior to formal adoption by a formal standards setting body.

CONSORTIA & ALLIANCES

These refer to private groups and partnerships that publish widely adopted standards that are, however, developed outside of formal processes. They focus on practical and fast-track specifications, coordinate testing and certifications, and generally influence the development of formal standards.

INDUSTRY INITIATIVES

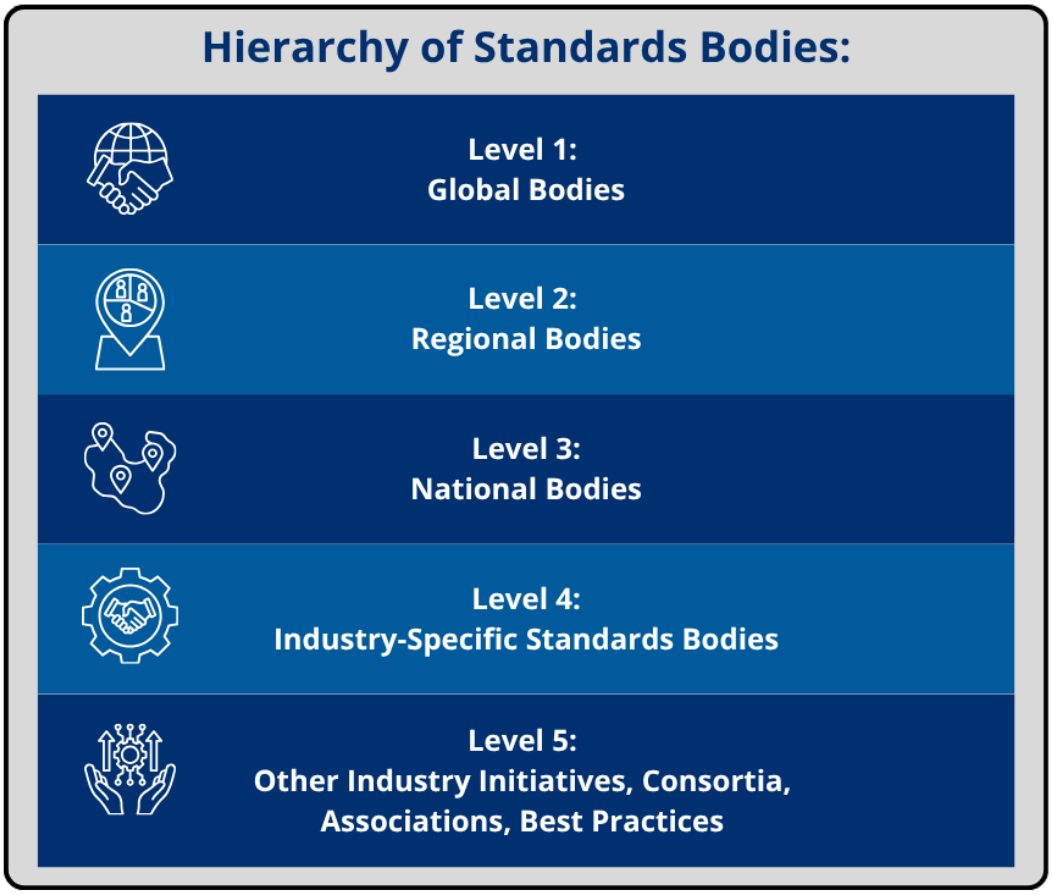
These may include protocol-specific specifications and sets of agreed-upon rules that go through an approval process within the ecosystem where they operate, such as Ethereum Request for Comments (ERC), or protocols specific to Layer 1 blockchains. While they may be designated as "standards" by the industry, they do not follow the formal standards setting process of global bodies, and they often consist in a set of APIs within a standard (requiring implementation of a number of AIP function calls to be considered "compliant"), or even a standard interface. Rather, the process for approval may vary widely across protocols, which may have different governance structures involving different voting processes. Often, when there is a use case in need of harmonized specifications (e.g., NFTs or other token types), a community centered around a protocol may propose and approve a set of rules. This "standard" may indeed evolve into an official standard if it gets endorsed by a globally recognized body and goes through the formal approval process. In the case of ERC standards, ad hoc industry adoption has led to significant harmonization and alignment (especially in the absence of globally recognized standards for the latest trends in innovation), to the point where even national standards bodies may take part in the governance committees of industry-based initiatives working toward harmonization at the forefront of latest trends.

REGULATORY ENTITIES

Regulators often engage with standards setters to adopt standards into regulatory requirements, or at times provide inputs into the standards setting process. For instance, regulatory sandboxes, which allow testing innovations within controlled environments that generally aim to provide lessons in the development of new regulations, can benefit greatly from technical standards. Alignment of regulatory developments with industry standards can be driven by a demand to ensure the entire ecosystem follows the standard. While government action is not necessary for the formation of standards, standards can be referenced by regulations, and in some cases required by regulations.

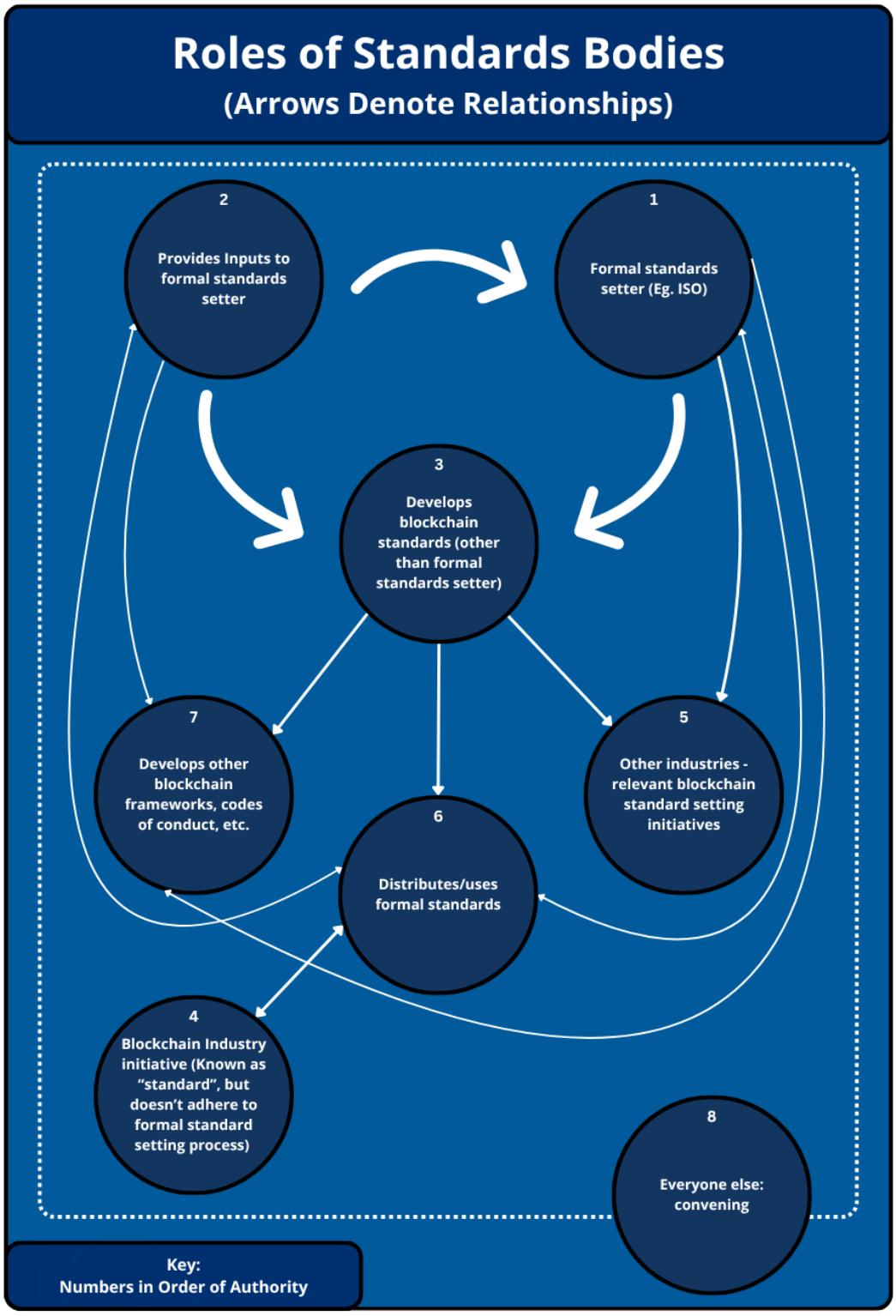
ASSOCIATIONS

These bodies focus on a wide range of activities including convening, research, and engagement across stakeholders to promote understanding and adoption of standards within an industry. In certain cases, associations may also provide an industry voice as an input to standards organizations in the process of developing standards.



ROLES OF STANDARDS BODIES

The various organizations involved in the standards setting ecosystem can take several roles, interacting on multiple layers involving top-down influence and bottom-up innovation (e.g., de facto or industry-specific rules) that may be later formalized as official standards. These layers of influence and collaboration are illustrated below:



STANDARDS SETTING PROCESS

The ideal outcome of standards development is to set effective standards, which industry players will use and purchase. This should start with a clear definition on the basis for a standard (e.g., for whom and what, when and where to use, who will use it, cost, etc.). When structured effectively, standards can drive major industry trends, and even entire enterprises and industries. For instance, the entire space of contactless cards was driven by clear and effective standards. The blockchain and digital assets space needs similar developments to promote scale, starting with definitions and taxonomies, and trickling to harmonized regulatory requirements.

Technical standards undergo an adoption and approval process that generally aims to attain the authorization of an internationally recognized standards organization. Often, the journey to develop standards starts with building locally, upon agreement of common rules. Next these common rules gain recognition at a national level, and ultimately attain acceptance internationally, which represents the most widely respected authority.

Local or industry-specific standards initiatives have stronger economic incentives toward rapid standards development, acceptance, and adherence.

National standards initiatives, which involve more stakeholders, may bring additional incentives (e.g., opportunity to win government contracts), but also bring additional bureaucracy and processes.

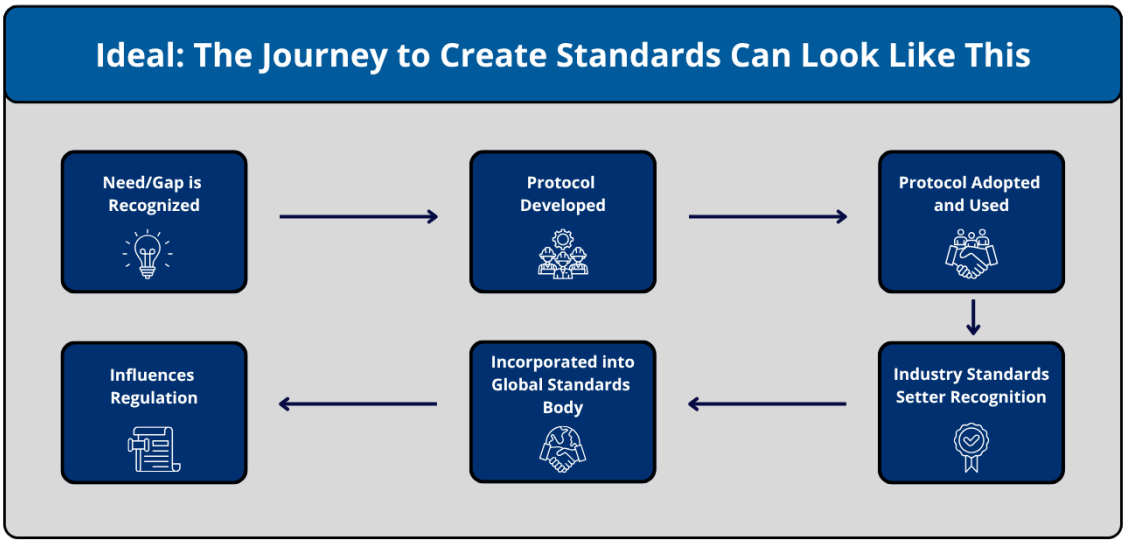
International standards initiatives may not have as many incentives for rapid approval, so the process to develop global standards can be time consuming and involve multiple iterations and assessments. Yet the value of global standards comes in the consensus of key stakeholders that they represent (e.g., several governments, corporations, and industry organizations), as well as additional opportunities for economic activity (e.g., doing business in a particular region).

Dedicated resources and expertise are fundamental to ensuring effective standards. International standards setters need direct feedback and inputs from countries and experts. Global standards may also require governments, large institutions, and corporates to update their systems. These are compelling reasons for major decision makers, especially public authorities, to participate in global standards committees for blockchain and digital assets, such as those hosted by ISO, to set a focused agenda, structure, and strategy for innovation. Effective standards development can be greatly enhanced through public-private partnerships, promoting collaboration among standards bodies and between standards bodies and the industry.[142]

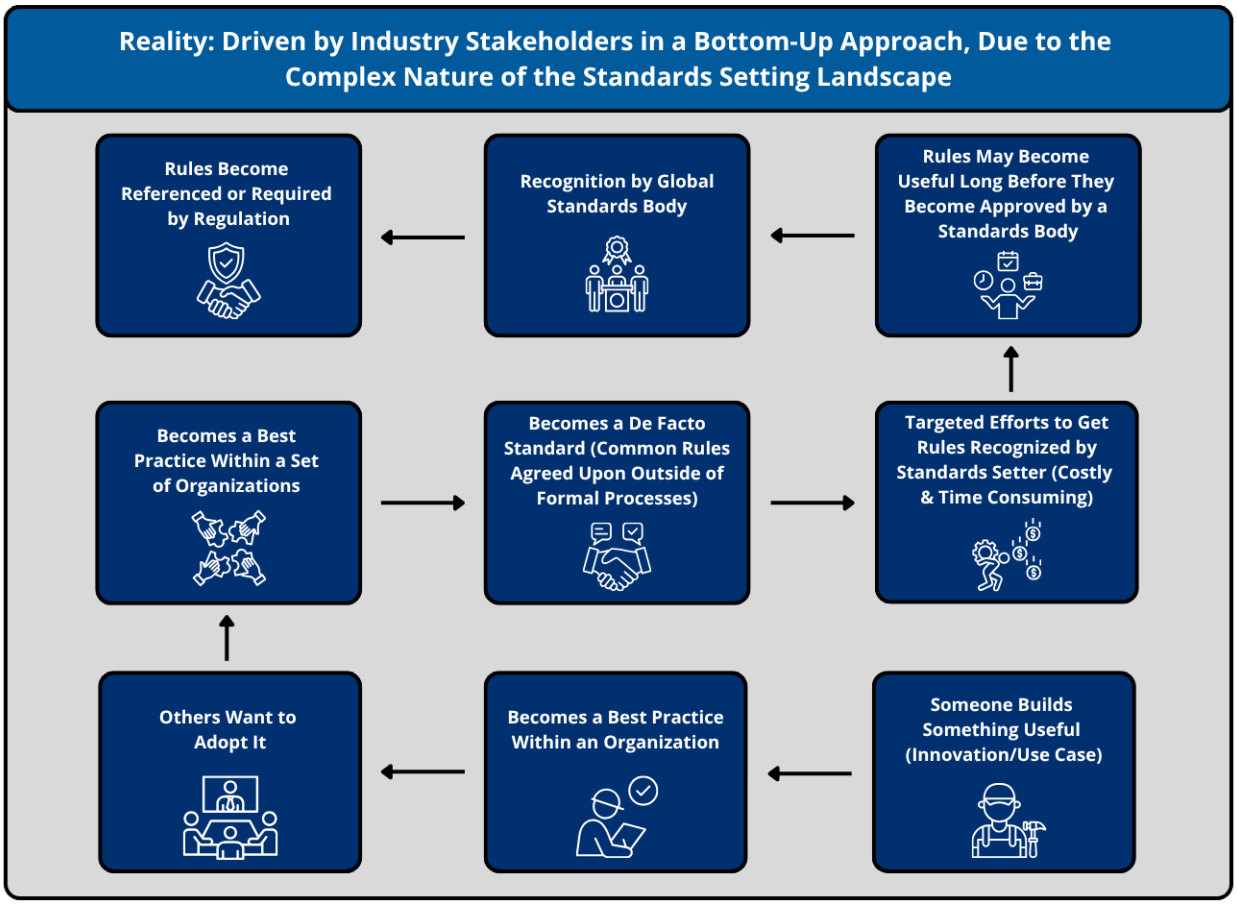
The World Trade Organization has developed 6 Principles for the Development of International Standards, which are relevant for the standards setting landscape:[143]

1. **Transparency**
2. **Openness**
3. **Impartiality and Consensus**
4. **Effectiveness and Relevance**
5. **Coherence**
6. **Development Dimension**

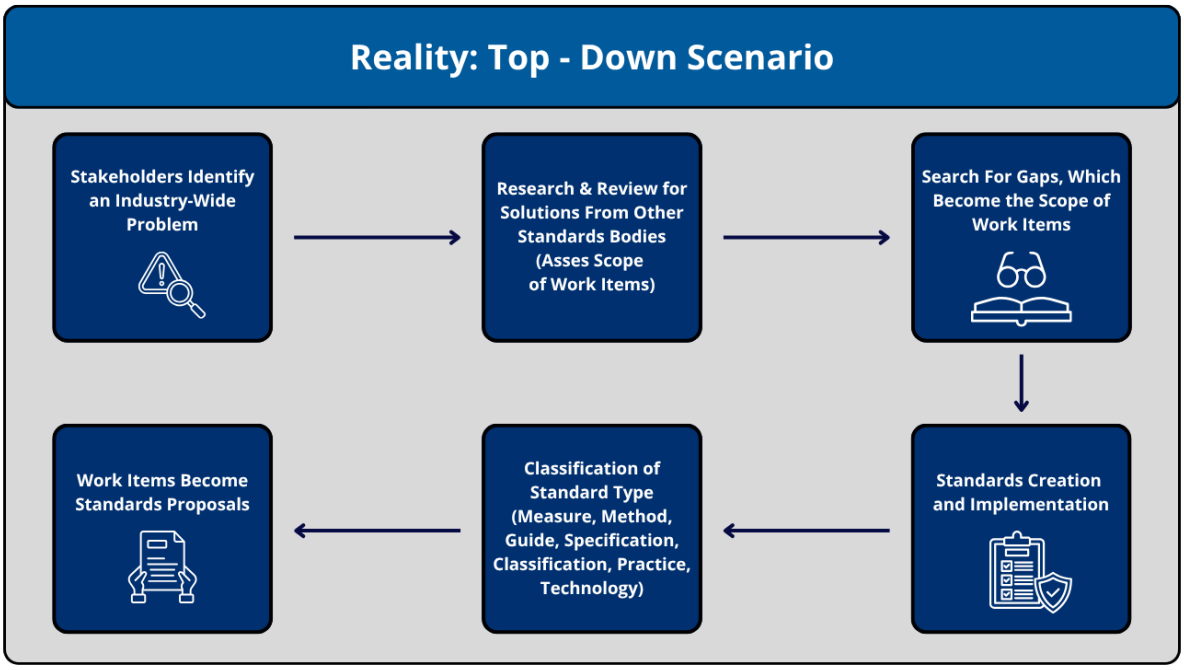
While the journey to create standards can look like this:



In practice, it often becomes driven by industry stakeholders in a bottom-up approach that looks like this, due to the complex nature of the standards setting landscape:



Adding to the complexity, when a gap is recognized, different standards organizations may start addressing it separately, creating counterproductive silos and duplicate work. From the perspective of a standards setting body, a top-down approach to setting standards in this context can also look like this:



To address the issue of fragmentation and duplicate work, certain standards bodies have agreed to not only collaborate in joint workstreams (e.g., ISO/IEC Joint Technical Committee 1 for blockchain standards), but also share information on their workstreams, such as the ISU/ITU/IDC commitment to shared listings of published work items.[144]

FORMAL STANDARDS SETTING

The key principles for global standards development are centered on consensus-based processes, where all views are considered, and ultimate agreement is attempted in the case of disagreements. Several steps involve formal balloting procedures, which can occur remotely or in person, with a threshold of votes required for approval (e.g., 2/3 "yes" votes to move to next stage). Inclusiveness is key, where input is sought from various sectors, interest groups (e.g., industry, regulators, consumers, etc.), and country representatives. These developments are only achieved with openly transparent communication, where documents and progress must be made visible to all relevant members and stakeholders.

The process of formal standards setting generally involves the following stages:

1. **Proposal:** Submitted by an authorized group, such as a member organization or technical committee, to introduce a new standard or revise an existing standard. In order to move forward, the proposal must be reviewed by the standards body members, voted upon, and accepted.

2. **Drafting:** Relevant technical committees or subcommittees are assigned to a working group comprised of experts, who also represent different participating countries, to draft a given standard.

3. **Expert Review:** Once an initial draft standard is finalized, it is distributed to relevant members for feedback and comment, and there may be several rounds of iterations and reviews.

4. **Public Review:** The updated draft standard is circulated to all member bodies of the standard setting body for a broader review and vote. Upon reaching a threshold of positive votes (e.g., 2/3 majority), the draft standard may move ahead in the process.

5. **Approval:** A final draft of a standard is issued and may undergo a final vote for approval.

6. **Publication:** The finalized standard is published and made available for adoption.

7. **Maintenance:** Standards are often revised on a recurring basis (e.g., 5 years), with potential outcomes to confirm them as they are, revise them (with the same process delineated above), or withdraw them.

This journey to develop formal standards, however, can be as rigorous as it is time-consuming. Certain challenges can also get in way of a standard being relevant. A standard may exist but the relevant stakeholders it covers may not adopt it as expected. For instance, as soon as ISO publishes a standard, it can be expected that a portion of the industry may already be adopting other standards with less global weight that have been released at an earlier time.

Moreover, a standard may become outdated if the approval process takes a longer time than expected, while a technology continues to evolve and present novel issues. For fast moving sectors like emerging technologies, the latest trends in innovation may remain out of scope of global standards setting initiatives for some time – during which more localized, fragmented, and informal industry initiatives may attempt to produce common rules for the sake of harmonization, with varied results and limited scope. Nevertheless, it is relevant for global standards setters to gain awareness of these smaller scale endeavors, as they may provide important inputs in the formal standards setting process as the voice industry experts.

COMPLYING WITH STANDARDS

The path toward adherence to standards can be approached as a journey propelled by specific drivers, to address specific needs for any company or organization. It is important to be mindful of the relationship between a standard and an organization seeking to adhere to it.

While formal standards are generally voluntary and not legally binding or proscriptive, they may be adopted into regulatory developments, and thus made mandatory. An entity that is compliant with a standard supports the technical functionality and uses the designated vocabulary set by the standard.

The process to comply with formal standards, especially those put forth by globally recognized bodies, can be rigorous for companies and organizations, which must employ a structured approach with several steps. Once compliant with a standard, these entities generally must maintain their status through internal audits, management reviews, both corrective and preventive actions, and ultimately periodic recertifications. Recent initiatives to address this issue have involved standards setters' cooperation with industry adoption, providing tools for working together, enhancing standards delivery in a more digitally native and agile format.[145]

There are, of course, clear benefits to standardization. Leadership buy-in, cross-functional teams for implementation, and frequent engagement with stakeholders can greatly improve an entity's success to achieve and maintain compliance. Moreover, ISO provides guiding principles, treating standards compliance not merely as a one-time initiative but as an effort toward continuous improvement.

Effective standards adoption requires intentional communication and educational initiatives to improve understanding on the importance of standards. In a future pointing toward leadership in mixed reality contexts with increasing connectivity, management challenges are made even more complex by emerging technologies like blockchain. Standards are fundamental to the future of businesses adopting these emerging technologies. This will also require integrations in various forms, form system upgrades, acquisitions, and partnerships. Blockchain technology is being recognized increasingly as a mitigation tool to address and prevent modern risks and provide resilience to data systems in the face of potential intrusions.

The process to comply with formal standards generally entails the following:

1. **Identification of Relevant Standards:** A number of different standards may be relevant for a company or organization, depending on the industry and operations.

2. **Understanding of Standards Requirements:** Obtaining and evaluating an official standard document, which may also involve training and additional consulting services.

3. **Gap Analysis:** Comparing current systems and processes with those required by the standard, to identify areas that don't meet those requirements.

4. **Establishing a Plan for Compliance:** This involves documenting policies and processes to meet requirements set by the standard, in addition to setting milestones, timelines, and corrective actions where needed.

5. **Implementing Compliance Plan:** This involves implementing processes and integrating required systems (e.g., controls, audits, risk assessments), communicating expectations, training staff, and integrating required systems.

6. **Ongoing Management Reviews and Internal Audits:** Periodic reviews to ensure compliance over time, improve processes, and address any nonconformities.

7. **Selection of a Certification Body and Certification Audits (if relevant):** An external body may conduct audits by first conducting documentation reviews and readiness assessments, followed by an on-site audit of practices in compliance with a standard.

Case Study: Standards Compliance

A typical startup in the digital assets space can provide a generic example of an entity's journey to comply with standards:

Company: US based digital asset exchange, seeking interoperability with other exchanges, and seeking to operate in a compliant manner

Challenges:

- Globally recognized standards setters do not yet drive harmonization in the latest trends on latest blockchain innovations, so they're not the most relevant
- Globally recognized standards may be expensive to attain
- The value of globally recognized standards may not appeal to a startup in earlier stages as they would for a large corporate with high volumes of activity
- Stage of startup is in proof-of-concept, meaning funding is limited

Solutions:

- Registration/licensing pursued in a state with clear regulatory structures (e.g., Wyoming)
- Industry initiatives toward harmonization provide the most attainable and relevant technical standards
- Selection of a widely adopted Layer 1 blockchain infrastructure to build solutions upon, aligned with industry standards initiatives (e.g., ERC)

TECHNICAL STANDARDS STRATEGY FOR BLOCKCHAIN INNOVATORS

Much of the value that blockchain brings for companies and organizations revolves around trust. There are costs to mistrust and uncertainty in any system, which blockchain technology can help mitigate. In the standards development ecosystem, blockchain technology can have 2 roles:

1. **Tool to help comply and verify compliance with standards for any company or organization**
2. **Blockchain technology itself is subject to technical standards, which ultimately aim to improve trust in this innovation and its use cases**

ETHICAL MATURITY MODEL FOR BLOCKCHAIN INNOVATIONS

While a company/organization may identify the standards available and relevant for its operations (refer to GSMI Technical Standards working group documented landscape of standards), an ethical maturity model provides a blueprint for developing a strategy around standards compliance. Ultimately, trust in a system enables it to thrive. In the blockchain and digital assets space, different levels of compliance with standards can pave the way toward greater trust. Standards reduce and quantify uncertainty in operations between parties, becoming a part of a risk management approach. Adherence to standards presents an expectation of certain activities and quality. This section presents a competitive model that goes hand in hand with an ethics maturity model.

Standards should be driven by value, and an ethical maturity model provides a structured framework to self-assess one's performance relative to standards requirements, allowing companies to decide their desired positioning considering the business, operational, and ethical implications. A given set of rules defines each level of maturity. These levels point to the degree of capability and sophistication, which can be defined as follows:

Layer 1: Compliance with legal and regulatory frameworks. In the blockchain and digital assets space, these are often emergent or yet to be developed. This makes Level 1 the lowest stage in the ethical maturity model (e.g., "thou shalt not").

Layer 2: Compliance with industry best practices and internal guidelines and standards. These rules generally function to maintain an organization's brand and reputational status. Level 2 therefore revolves around safeguarding the integrity of other stakeholders – a Golden Rule in ethics (e.g., "don't do to others what you don't want them to do to you").

Layer 3: Compliance with relevant globally recognized formal standards, in a way that indicates a firm commitment, and significant resources devoted to meeting high expectations. Level 3 is an indicator of leadership in ethics.

Layer 4: Adherence to standards and best practices in such a way that extends value to other stakeholders (e.g., Shared Value concept going beyond Corporate Social Responsibility). Level 4 indicates the highest level of ethical maturity (e.g., "blessed are they").

	Governance	Smart Contracts	Digital Assets	Interoperability	Identity	Use Cases
International and Global Standards						
National Standards						
Interorganizational Standards						
Industry Best Practices, Internal Guidelines, and Standards						
Local Legal and Regulatory Compliance						

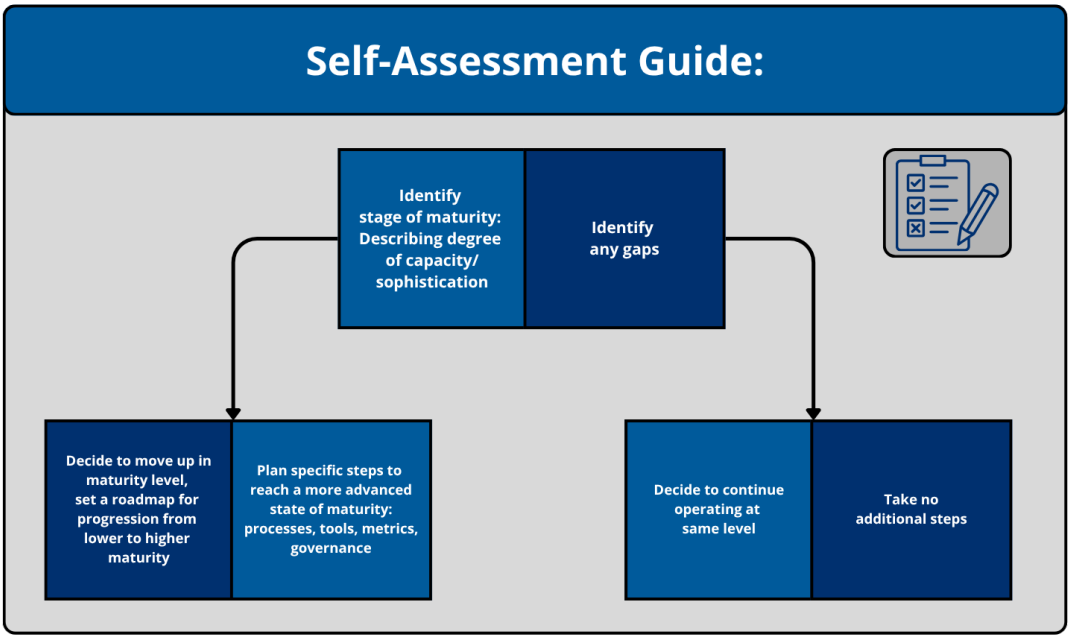
Name of Standard:
Standards Organization :
Other Metadata:
Example of Use Case:
Cost/accessibility
Level of Maturity (KPIs):

Value Offering:
- Compliance
- Transact directly
- No reconciliations
- Instant status
- Data integrity and provenance
- Automatically execute agreements
- Lower transaction costs
- Fault tolerant, resilient, available
- Predictability of smart contracts
- Inclusion
- Self-sovereignty
- Empowerment

Risks
- Misuse of blockchain capabilities (securities fraud)
- Regulatory risks
- Are the risks predictable?
- How large are the risks and are they reversible?
- Are the benefits worth the risks? Who should decide?
- Do those persons on whom the risks will fall know about the risks? Have they consented to bear these risks?
- Will they be justly compensated for their losses
- Are the risks fairly distributed among the various segments of society?

Mitigation
- Policy
- Risk mitigation best practices
- Other Approaches

The parameters laid out above (governance, smart contracts, digital assets, interoperability, identity, use cases) with respect to standards compliance at the levels of ethical maturity point to essential aspects of blockchain-driven digital transformation within the organizational space, affecting people, processes, and technology. For innovation use cases to be effective, it is essential to define necessary fields and characteristics, and especially define value. A statement of business value and social values (e.g., inclusion) clarifies the purpose behind business practices.



At each level of ethical maturity, a company/organization can evaluate the set of applicable standards and decide whether to remain compliant at that level, or define additional standards to comply with to reach the next level of maturity. It is an ethical and competitive choice to make a conscious decision to adhere to a particular maturity level (after assessing pros/cons, benefits/costs of remaining at the same level or progressing to the next level), as opposed to operating unaware of such strategic assessment. For instance, a company that is legally operating in a given US state may need to comply with ISO standards in order to operate globally.

At the lowest level, which comprises regulatory requirements, the blockchain industry has yet to agree on harmonized requirements, as a lowest form of ethical considerations. In a context of regulatory uncertainty, volatility and uncertainty may remain, and it is difficult for companies to become leaders in their industry. Incumbents may even resist the development of a proper risk framework to keep their own competitive advantage. Moreover, local regulatory compliance is different for different jurisdictions, which may present conflicts at a local level vs. broader geographical level. Ethical choices involve protecting local interests vs. global interests.

On the other hand, at the highest level, compliance with standards, in a way that embraces leadership and ethics in the highest degree, requires long term strategic considerations that go beyond short-term business goals. At the highest level, an organization's governance structure would not only embrace compliance with regulations and standards but subsume them into a broader ethical model of transparent compliance and decision making.

RECOMMENDATIONS

1. Take measures to address the concern of overlapping standards and efforts toward standardization (e.g., sharing lists of new standards among standards bodies)
2. Promote open standards and alternative revenue models for standards setters
3. Promote harmonized terminology for processes of standardization

GBBC
Global Blockchain
Business Council

TOKENIZATION & CUSTODY REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 6.0

TOKENIZATION OF OFF-CHAIN ASSETS: OPPORTUNITIES FOR THE FUTURE OF FINANCE

GBBC GSMI 6.0

ACKNOWLEDGEMENTS

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

John Lee - CO-CHAIR
Global Managing Director, Accenture

Rajeev Bamra - CO-CHAIR
Head of Strategy, Digital Economy, Moody's Ratings

Deborah Algeo - CO-CHAIR
Managing Director, Zodia Custody

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

WHAT IS TOKENIZATION?

Tokenization refers to the process of tracking the ownership of traditional assets like treasuries, stocks, and bonds on a blockchain. This may also convert rights to an asset into a digital token on a blockchain. It is a widely used concept, relevant for many contexts in the blockchain and digital assets space. While there is still a need for greater harmonization toward a common taxonomy and understanding, below are a few broadly recognized definitions of tokenization:

> *"The process by which real-world assets are turned into something of digital value called a token, often subsequently able to offer ownership of parts of this asset to different owners."* International Capital Market Association (ICMA)[146]

> *"Tokenisation of assets involve[es] the digital representation of real assets on distributed ledgers (digital twins) or the issuance of traditional asset classes in tokenised form (native tokens), excluding crypto-assets."* Organisation for Economic Cooperation and Development (OECD)[147]

> *"Asset-referenced tokens (ARTs): crypto-assets that purport to maintain a stable value by referencing another value or right or a combination thereof (e.g. official currency, commodities, other assets). You can redeem ART at the market value of the asset(s) it references."* European Securities and Markets Authority (ESMA)[148]

> *"Tokenization refers to the practice of using blockchain technology to record ownership of an asset. These assets can take the form of traditional financial assets, such as money market fund shares or bank deposits, or non-financial assets, such as trade receivables or interests in rare items such as art or collectibles."* (US President's Working Group Report on Digital Asset Markets Report) [149]

In addition, the CFTC's GMAC-DAMS Digital Assets Classification Approach & Taxonomy[150] defines and categorizes digital assets, including tokenized forms of digital assets, based on their specific features. This taxonomy approach is recognized for the purpose of facilitating a way for stakeholders – particularly regulators – to evaluate these types of assets, with a use case driven approach.

As taxonomies continue to evolve, the concept of tokens may include those that are native to the blockchain, which exist and trade only on-chain (e.g., cryptocurrencies), and tokenized assets that may represent other off-chain assets or, including cars, paintings, homes, and intellectual property. The latter is the focus of this paper.

Asset tokenization digitally represents real-world assets, both physical and intangible, or services on a blockchain or distributed ledger technology (DLT) that establishes consensus among diverse participants. This digital form is referred to as a "token." While this paper centers on asset tokenization, many observations also extend to other token types.

FEATURES OF TOKENIZATION

While definitions of tokenization provide a structure for understanding the concept, the essential components of tokenization point to the key features and benefits for real applications and use cases. It is these components, listed below, that allow for a deeper, and more empirically based, understanding of the meaning of tokenization in different contexts and fields.

Representation: On-chain representation of something that exists off-chain (e.g., digital twin), or something that exists inherently on-chain (e.g., DLT native). For DLT native assets, tokenization may be the only legally acceptable means to record them.

Memory Aid: Tokens can serve as digital memory aids, functioning as ledger-based equivalents of contracts and records. In this sense, they can become ledger equivalents of contracts and records, memory aids can serve social and economic functions. Tokens have been used as memory aids since prehistoric eras throughout the history of humanity, starting with physical tokens such as clay or stone artifacts used for counting and accounting[151] that represent the measurement of goods. These tokens evolved into counting technologies, writing mechanisms, and various forms of accounting for trade and economic activity.

Ownership Records: Verification of ownership and provenance are enabled by registration mechanisms that allow for the right to ownership (e.g., real estate records). Settlement finality is an important component to verify when assets are legally considered to have changed hands.

Fractionalization: Assets can be divided into smaller, tradeable units, allowing economic exchanges at a more granular level (e.g., smaller portions of currency units, trading portions of high-value assets like real estate or private equity) and facilitating secondary trading at a larger scale.

Liquidity: Increasing, and even unlocking liquidity, is facilitated by the ability to list and trade fractionalized tokens in secondary markets. This can unlock otherwise trapped capital to improve market efficiency, especially for assets that have been traditionally illiquid.

Authentication: Digital identifiers attached to tokenized assets allow verifications of key features (e.g., authenticity, digital identity) that may be required for certain products and services. Real value is confirmed by provenance, which is especially important for sectors like supply chain, art, and medical devices.

OPPORTUNITIES OF TOKENIZATION

As the digital economy evolves and expands across emerging technologies, tokenization – of both money and assets – presents an opportunity to form a new backbone for transactions, setting much of the structure for financial market innovation. As digital finance evolves from dematerialization to tokenization, payment and investment rails can be better connected, and players can maximize opportunities from fractionalization and greater efficiencies. The digital asset space fuels innovation with tokenized assets in an evolution that broadens markets and redefines asset classes, exemplified by the rise of asset tokenization in financial markets that marks the next generation of value exchange.[152] Tokenization is also becoming a key component to bridge traditional finance (TradFi) and decentralized finance (DeFi).

Market Size: Tokenization presents a new universe of opportunity with the exchange of any asset represented on a blockchain. As traditional networks and blockchain based networks converge, financial market infrastructures, alongside the assets and currencies to be traded on them, are expected to rely on tokenization. Indicating the magnitude of the tokenization opportunity ahead, the fixed income market globally spans $150 trillion, of which $17 billion consist in digital bonds (not tokenized)[153]. Here it is important to distinguish between "total issued" and "outstanding" amounts. The figure of $17 billion refers to the total issued amount, which includes those that have been repaid or redeemed. Arguably, the whole fixed income market can be tokenized. Illustrating how much of the market remains to be tokenized, estimates point to only 0.01% of the total value of global fixed income and equity securities combined being currently tokenized.[154] As the evolving digital ecosystem integrates with existing legacy systems, the need for more efficient solutions and infrastructure rises.

Broad Opportunity: Tokenizing assets, products, or services by creating tokens linked to real assets through smart contracts can dramatically increase transaction speed, security, and reduce costs. While many token projects remain experimental, the technology is rapidly advancing. Common tokenized asset classes include:

- Securities (stocks, bonds)
- Commodities (gold)
- Real assets (real estate)

Removing Frictions & Intermediaries: With improved transparency, efficiency, and liquidity in financial systems, tokenization also allows users to bypass legacy intermediaries. Tokenized assets (e.g., gold, stablecoins, real estate, and even intellectual property) can coexist and trade on the same blockchain without traditional intermediaries. This lowers costs, speeds transactions, and unlocks fractional ownership, democratizing access to previously illiquid or exclusive markets. Open-source blockchain protocols built on global standards (e.g., ISO 27001) ensure seamless cross-platform interoperability and foster innovation.

Operational Efficiencies & Smart Contracts: Tokenization solves many operational challenges. With traditional financial infrastructure, assets stored in different jurisdictions and by different companies are cordoned off into silos that reduce liquidity and make them difficult to reconcile. On distributed, shared ledgers, assets can be automatically reconciled. For instance, smart contracts can nearly instantly conduct complex trades, greatly reducing the need for slow and expensive compliance checks and audits.

Key benefits include automation, faster clearing and settlement, enhanced transparency, and improved liquidity. Tokenization uses blockchain and smart contracts to revolutionize asset issuance, transfer, and management. By enabling programmable, self-executing transactions, it delivers near-instant settlement, cuts counterparty risk, and guarantees immutability and transparency via decentralized ledgers. This automation removes many inefficiencies of traditional finance while giving regulators real-time asset traceability and compliance insight. These features boost efficiency, prevent fraud, and simplify complex processes like trade settlement and bankruptcy resolution.

Efficient Ledger-based Infrastructure: Adopting blockchain-based ledgers delivers substantial advantages, including stronger risk management and improved operational efficiency, driven by their decentralized, immutable, and transparent transaction records. Blockchain also boosts transaction efficiency by cutting intermediaries, lowering costs, and speeding up processes like cross-border payments and trade finance.

24/7 Markets: Operating 24/7 market operations beyond traditional market hours, tokenized systems offer greater cost efficiency by replacing legacy infrastructure, cutting intermediaries, and automating with smart contracts. Yet fully unlocking this potential depends on regulatory developments to support decentralized protocols, new asset classes, and embedded compliance.

Velocity of Money: Moreover, tokenizing traditional financial instruments like securities can improve the velocity of money, allowing funds to move through the system more quickly, while reducing fragmentation and enhancing liquidity (not to be confused with creating liquidity) across digital markets.

Democratization & Accessibility: While the traditional financial system has restricted certain activities (e.g., liquidity provision, portfolio management) to entities like brokers, tokenization allows all network participants to perform those activities, allowing investors more autonomy over their instruments and customized solutions. For instance, DeFi protocols can facilitate the use of tokenized securities as collateral, open opportunities for monetization by placing funds in pools and automated market makers that pay fees, and enable more efficient movement of portfolios across platforms.

Tokenization can also extend financial access globally by making them available anywhere there's an internet connection, while preserving trust and oversight by embedding the assets with jurisdictional requirements. By enabling fractional ownership, tokenization contributes to lowering investment barriers and broadening retail access to traditionally illiquid markets. Digital assets and blockchain drive financial inclusion by removing traditional barriers. They empower underserved populations in remote or economically challenged regions to access services like digital wallets, remittances, and lending, advancing global financial access. Decentralized Finance (DeFi) platforms further democratize finance by eliminating intermediaries, reducing costs, and lowering entry barriers, especially in areas lacking banking infrastructure. Tokenization supports

Security: Tokenization's growing role in data protection and payment security is crucial. Well designed smart contracts automate complex agreements, reducing human error and fraud risk. By leveraging distributed, decentralized ledgers, tokenization safeguards sensitive digital assets from unauthorized access. Beyond financial gains, blockchain's traceability and transparency restore trust in opaque processes. Tokenization protects privacy while strengthening efforts to prevent money laundering and the financing of criminal or terrorist activities.

PURPOSES OF TOKENIZATION: PAYMENT & ASSET

Tokenization implementations in digital asset markets can be broadly categorized based on two main purposes:

- **Payments: Tokenization of generally stable assets to serve as currency for transactions on the blockchain**
- **Tokenizing off-chain assets: Representation of assets that fluctuate based on market prices, to be traded through on chain transactions**

Tokenized cash (stablecoins) & tokenized assets (RWA) can be the foundation of on-chain capital markets. While tokenization can span across use cases for payment solutions, it can also span digital twins for any form of asset. Each of these two "sides" of tokenization is meant to provide solutions to different needs and create different forms of value, involving a collection of activities that often interact with each other. The first category provides a currency to facilitate transactions, while the second category provides an asset to be traded in tokenized format. Specific definitions would vary depending on the asset class involved.

PAYMENTS – FASTER, CHEAPER, AUTOMATED

Tokenization for payments may include both digitally native tokens, such as network-specific tokens utilized by specific protocols for various transactions[155], on-chain representations of off-chain fiat funds (e.g. stablecoins, tokenized deposits), and central bank digital currencies (CBDCs).[156] Tokenized currencies operate on blockchain infrastructure that offers several benefits – notably greater transparency, near-instant clearing and settlement, disintermediation, security, and lower costs – where every transaction is traceable and verifiable on a ledger record. Tokenized money enables atomic (instant and final) settlement for transactions – both for delivery versus payment (DvP) and payment versus payment (PvP) – minimizing frictions and risks arising from settlement delays and counterparty exposure.

Beyond delivering speed and efficiency to transactions, the on-chain currency also allows programmability features that would not be available in traditional systems. Programmable tokenized money, which points to the integration of money and code, enables rules and logic embedded into payment behaviors (e.g., automatic interest, dividends, tax payments, or other fees). Tokenized money is also integrated into smart contracts, supporting automated workflows and conditional payments (e.g., payments upon delivery of goods, payments for approved goods or services) and even granular customization and controls based on token property definitions and permissions. This can also enable compliance-by-design, where regulatory and governance rules can be coded into token logic and transaction validation (e.g., whitelisting wallet addresses, automated compliance reporting, jurisdictional controls).

As such, tokenized currencies are inherently integrated to the digital asset ecosystem, providing the settlement layer for tokenized assets, securities, and DeFi applications. Tokenized money can support the growing ecosystems of tokenized securities, commodities, and derivatives, improving access to markets at a global level by supporting seamless cross-border transactions. Tokenized currency on a blockchain is key for successful end to end tokenization.

Moreover, because tokenized currency can be accessed through digital wallets, this bypasses the need for traditional bank accounts. This can lead to greater financial inclusion and access to financial services for unbanked and underbanked communities, with reduced onboarding and servicing costs especially for small scale users.

TOKENIZING OFF-CHAIN ASSETS – INNOVATIVE FINANCIAL PRODUCTS

Asset tokenization refers to the process of issuing a digital on-chain representation of an asset that exists off-chain, such as a real-world asset (RWA -e.g., art, real estate) -specifically a financial asset (e.g., securities, commodities, debt) - and even data and concepts (e.g., intellectual property, ratings).

RWA tokens represent pre-existing real assets that both exist and trade off-chain and on-chain through digital twins and are backed by the real, tangible assets off-chain. The tokenization process creates digital twins that can be issued, recorded, traded, and traced on a blockchain, such that off-chain activities are still recorded on-chain. This provides a bridge between traditional finance and on-chain finance, where assets like real-world money, securities, and credit can be represented on a blockchain. The efficiencies and benefits of tokenization can streamline issuance, governance, and lifecycle management of tokenized assets, where asset rights are digitally represented on the blockchain.

For instance, tokenized securities and security tokens can be traded in global markets operating on a blockchain, under requirements as securities in traditional markets. Tokenized real-world assets (RWA) encompass an even broader range of tangible and intangible assets that have traditionally existed off-chain – unlike cryptocurrencies and related activities which are digitally native. As RWAs hold value in the physical world and have traditionally operated within centralized systems subject to frictions from various intermediaries, lengthy settlement processes, and limited accessibility, tokenization provides opportunities to benefit from greater efficiencies offered by blockchain infrastructure.

Tokenized assets enable innovative financial products and new ways to own, transfer, and trade them over blockchain infrastructure. In recent years, tokenization is spanning the entire spectrum of capital markets products, with tokenization platforms facilitating issuance under regulated conditions as regulatory developments unfold.

Notably, the business value behind tokenization points to new products and markets, operational efficiencies in transactions and dealings (e.g., automation for compliance and corporate actions), and wider investor participation alongside greater liquidity.

Tokenized RWA growth trends

- **Increasing tokenized value**, with tokenized RWA market surpassing $30B in on-chain value in 2025 (tokenized US treasuries account for over $8B with players like BlackRock, Franklin Templeton, Ondo Finance, Maple Finance)
- **Fast growth** with projected $1-3T in RWA tokenization by 2030, as banks and asset managers are expected to tokenize additional securities
- **High yields and safety** (e.g., US Treasury backed RWA) can lead to stable returns and straightforward processes for tokenization
- **Efficiency** with faster settlement, 24/7 trading, disintermediation
- **Liquidity enhancement** with fractional ownership and trading, providing investors access to larger or illiquid assets
- **Transparency** where blockchain shows holdings and transactions in real time
- **DeFi integration**, where RWA tokens can be used as collateral and in liquidity pools

Examples of tokenized assets issued on a blockchain include:

Debt Instruments

Type	Issuer	Blockchain	Key Facts
Sovereign Bond	World Bank (bond-i)	Ethereum	1st blockchain-issued bond in 2018, raising AUD 110M, built as a private network on Ethereum
Sovereign Bond	European Investment Bank (EIB)	Ethereum	Raised 100M Euros, issued in partnership with Goldman Sachs and Société Générale, HSBC Orion as tokenization platform
Corporate Bond	Siemens Digital	Polygon	1st German corporate bond on a blockchain, Issued 60M Euros in 2023
Corporate Bond	Santander	Ethereum	Tokenized bond for internal treasury, issued $ 20M in 2019
Municipal Bond	City of Lugano, Switzerland	Polygon	Purpose to fund city infrastructure, accessible to retail and institutional investors
Private Credit	WisdomTree	Ethereum; Stellar	WisdomTree Private Credit and Alternative Income Digital Fund (CRDT) – Diversified portfolio of private credit assets in tokenized form, with a low minimum investment.
Private Credit	Figure Technologies	Provenance Blockchain	Over $10 billion in home equity lines of credit, consumer loans, and mortgage-backed assets tokenized in a marketplace to streamline loan origination, servicing, and trading through smart contracts

Money Market Instruments

Type	Issuer	Blockchain	Key Facts
Money Market Fund Tokens	Franklin Templeton	Stellar/ Polygon	OnChain U.S. Government Money Fund (FOBXX) – SEC-registered fund, 1st of its kind, represented as blockchain tokens, allowing direct digital shareholder recordkeeping
Money Market Fund Token Pilot	WisdomTree	Stellar/ Ethereum	WisdomTree Prime Digital Funds – Tokenized money market treasury funds
Treasury-Backed Stable Instruments	Ondo Finance	Ethereum/ Solana	OUSG & USDY – tokenized notes backed by US Treasuries, providing yield-bearing stable instruments

Equities & Fund Instruments

Type	Issuer	Blockchain	Key Facts
Private Equity Shares	KKR	Avalanche	KKR Health Care Strategic Growth Fund II - 1st tokenized representation of major private equity fund, using Securitize as tokenization platform
Mutual Funds & ETFs	Hamilton Lane	Polygon	Hamilton Lane Equity Opportunities Fund V – Tokenized feeder fund for broader investor access, using Securitize as tokenization platform
Synthetic Digital ETFs	Mirror Protocol/ Synthetix Assets	Ethereum/ Terra	Synthetic token representations of US equities for trading on DeFi platforms

Real Estate & Infrastructure

Type	Issuer	Blockchain	Key Facts
Real Estate – Equity Tokens	RealT	Ethereum/ Gnois	Fractional ownership for US rental properties, where investors receive rent in the form of stablecoins
Real Estate – Debt Tokens	Lofty.ai	Algorand	Property-backed loans with investor voting rights
Commercial Real Estate Pilot	UBS & Swiss Real Estate Tokens	Ethereum	Institutional grade real estate for investment at a fractional level

Commodities & Alternative Assets

Type	Issuer	Blockchain	Key Facts
Gold	Paxos	Ethereum	Pax Gold (PAXG) – Tokens backed 1:1 by a fine troy ounce of allocated gold, regulated by the New York Department of Financial Services (NYDFS)
Gold	Tether	Ethereum/ Tron	Tether Gold (XAUT) – Tokenized representation of gold ownership stored in Swiss vaults
Carbon Credits	Toucan Protocol, KlimaDAO	Polygon	Tokenized carbon credits allowing transparent trading, offsetting, and verifications
Wine, Art & Collectibles	VNX Commodities, Artrade, Masterworks	Ethereum/ Avalanche	Tokenized alternative assets enabling fractional investments
Art	6529 Capital	Decentralized public blockchains (various)	Investing in NFTs with NFT-native user wallets, toward a decentralized and tokenized approach

Structured & Hybrid Instruments

Type	Issuer	Blockchain	Key Facts
Structured Notes	Société Générale – Forge	Ethereum	Tokenized covered bonds and structured products, under France's AMF Framework
Repo/ Collateral Tokens	HQLAx	Corda	Tokenized collateral mobility platform for securities lending and repo markets
Digital Commercial Paper	Mitsubishi UFJ Trust and Banking Corporation	Proprietary DLT	Programat Platform – for tokenized short term debt instruments, integrated with Japanese market infrastructure

Other Industry Use Cases

Type	Issuer	Blockchain	Key Facts
Education	Learning Tokens	Hyperledger	Tokens represent knowledge transfer and skills acquired. Milestones achieved in the educational process are tokenized, facilitating talent upskilling, reskilling, and authenticating skills for job and future training opportunities.
Biotech Patents/ IP	VitaDAO & Molecule	Ethereum/ Ocean Protocol	Tokenized ownership and licensing rights in biomedical research IP
Authentication for Supply Chains	Birina Handmade	Algorand	Authentication of traditional Asamese Indian woven Gamosa's provenance to trace its origins directly from artisan to customer
Enabling interoperability between ratings data and digital finance ecosystem	Moody's Ratings	Solana / Alphaledger and Polygon via Untangled. Finance Oracle Solution	Developed proof-of-concept solution that enable seamless integration with digital finance ecosystems, allowing ratings data to be efficiently ingested and disseminated
Developed proof-of-concept solution that enable seamless integration with digital finance ecosystems, allowing ratings data to be efficiently ingested and disseminated	6529 Capital	Decentralized public blockchains (various)	Investing in NFTs with NFT-native user wallets, toward a decentralized and tokenized approach

CASE OF COLLATERAL MANAGEMENT

Collateral management refers to the underlying assets used for backing, and often pledged as security to reduce credit risk in financial transactions. Both the payment and asset representation roles of tokenization feed into collateral management, providing several benefits.

Efficiency & automation for collateral movement: Holding value on a blockchain facilitates collateral movement and placement – including global collateral movement without the added complexities of legacy custodians or clearing systems. For instance, stablecoins can facilitate the transactions to achieve these purposes. Tokenized assets and blockchain infrastructure can enable programmatic collateral mobility, with increased efficiencies and security measures, while reducing costs.

Inventory management: For tokenized assets, inventory is generally held in digital wallets. While moving large volumes of assets between custodians in traditional finance takes time and money, inventory held in digital wallets directly under the user's control can be moved much more quickly on blockchain rails. Both speed and inventory are major benefits, in addition to pricing and liquidity considerations.

DeFi opportunities for collateral and interest: In the DeFi space, liquidity pools challenge the model of operations of typical banking rails. Pools consisting of tokenized RWA can allow users to deposit tokens as collateral and earn interest in the form of stablecoins, which can be used to reinvest. While traditional finance wouldn't envision the concept of interest bearing stablecoins, DeFi utilizes stablecoins to serve as collateral and generate income, such that they function as payment currencies and tokenized RWA (e.g., tokenized treasury bills) that earn interest.

Capital Optimization: Fractionalization can broaden the pool of eligible collateral, while easier collateral movement can enhance liquidity utilization and instant capital re-pledging. Moreover, certain token standards not only improve interoperability but also allow the use of the same collateral across different platforms, markets, and protocols.

Inclusion & Market Access: Smaller investors and organizations can access tokenized assets, whereas they may have been traditionally limited by factors like size, geography, or operational frictions.

Transparency, Compliance & Risk Management: Tokenization provides real-time visibility and facilitates auditability, where collateral positions can be monitored on-chain in ways that improve regulatory reporting accuracy, provide proof of reserves, and reduce counterparty risks. On-chain escrow accounts and programmable settlement also reduce reliance on third party intermediaries. Tokenized assets can integrate with embedded regulatory logic for automatic enforcement of compliance rules, and collateral management can be made dynamic, with parameters (e.g., haircuts, eligibility) updated automatically based on regulatory updates and latest market feeds.

REQUIREMENTS FOR SCALE & CHALLENGES – WHAT WILL IT TAKE TO SCALE?

While the market has recognized promising use cases of tokenization (e.g., stablecoins, RWAs) – especially where demand and liquidity for them would exist - there still remain challenges to provide broader access. These gaps range from operational challenges to lack of broader access, to gaps and lack of clarity in regulations and standards. Scale, therefore, may pose additional costs.

1) OPERATIONAL CHALLENGES

While banks and other financial institutions have been increasingly interested in tokenizing assets, significant challenges remain when it comes to operational efficiency.

- **Fragmented liquidity** where RWA tokens trade on isolated platforms, leading to limited secondary markets
- **Custody challenges**, requiring reliable custodians and transparency of backing
- **On & Off-chain integration**, where link to off-chain assets requires ensuring token matches real world asset's status
- **Primary Markets:** Lack of streamlined avenues from asset tokenization to issuance and access to banks, institutions, etc.
- **Settlement:** Lack of stable settlement asset, especially leading to fragmentation when transactions have to come off chain
- **Secondary Markets:** Distribution challenges for asset managers and investors, limiting access. For instance, a web2 wrapper may be needed to access a web3 ecosystem where tokenized assets operate.
- **Fragmentation of Participants:** From primary markets, to secondary markets, and settlement processes, participants in the tokenization value chain don't necessarily communicate with each other.

2) CHALLENGES TO BOARDER ACCESS

Both payment tokens and tokenized assets have specific requirements in order for users to access them. The table below highlights such requirements, as well as the existing gaps and frictions that can deter widespread access. For instance, while certain major stablecoins may represent the lion's share of how acquire these tokenized assets, as the space evolves, we expect broader opportunities for market integration and interoperability across greater touchpoints.

	How to access & pay for it	Gaps/Frictions
Payment Tokens	• Requires fiat currency to exchange for it and an on/off ramp between fiat rails and blockchain rails, especially if later conversion back into traditional fiat is envisioned. • Fiat funds may be required to transfer to a centralized exchange or other form of distributor of tokens, or if there is a direct relationship with the issuer, funds can also be transferred directly to the issuer.	• Fiat rails are not always easily connected to blockchain based rails to facilitate widespread exchange. • Access to wallets for investors to hold tokens they purchase is a necessary part of distribution following token issuance on a blockchain
Tokenized Assets	• Fiat funds or payment tokens may be required to transfer to a centralized exchange or other form of distributor of tokens, or if there is a direct relationship with the issuer, funds can also be transferred directly to the issuer. • In the DeFi space, swaps can bypass the need for stablecoins, allowing swapping one asset directly for another, and even creating pools of tokenized assets without stablecoins.	• There currently exists no equivalent to seamless web3 services to make access to many tokenized assets easily and widely available (e.g., access to tokenized bonds over an app). • Access to wallets for investors to hold tokens they purchase is a necessary part of distribution following token issuance on a blockchain

3) GAPS IN STANDARDS & FRAMEWORKS

We emphasize the importance of common rules as a necessary condition for interoperability – especially when it comes to crating robust secondary markets for tokenized assets. Commonly agreed upon rules set expectations that ensure compatibility, enabling tokenization to meet its purpose of seamlessly moving assets across markets and platforms. Regulatory developments also play a role toward harmonizing requirements.

Regulatory uncertainty, where legal classification varies in different jurisdictions, and most RWA tokens treated as securities

- **Regulatory Gaps for Stablecoins:** Regulatory treatment of stablecoins globally is still unclear, so they should not be considered equivalent to cash
- **Regulatory Gaps for Tokenized Assets:** Lack of regulatory clarity for secondary markets, if any at all
- **Contractual Frameworks for New Infrastructure:** The shift to tokenized systems requires new contractual agreements to define custody, ownership, and control of digital representations of assets. Existing legal frameworks often lack provisions for storing claims on distributed or blockchain-based infrastructure.
- **Absence of Recognized Third-Party Custodians:** In many tokenization models, traditional third-party custodians may not exist or be clearly defined, creating uncertainty about who is responsible for asset safekeeping and fiduciary duties.
- **Complexity of Securities Classifications:** Securities are not uniform in nature, and tokenization introduces additional complexity regarding their classification, treatment, and regulatory oversight. This makes consistent supervision across asset types difficult.
- **Gaps in Activity-Based Regulatory Approaches:** While activity-based regulation can theoretically cover most tokenization activities, it depends on a clear equivalence between on-chain and off-chain economic functions. Regulators have yet to map how tokenization might create new economic behaviors or structures that do not align neatly with traditional financial activities.
- **Lack of Economic Function Mapping for Tokenization:** There is a need for clearer regulatory analysis of the unique economic activities enabled by tokenization technology—such as programmable ownership, fractionalization, and automated settlement—to ensure appropriate oversight and investor protections.
- **Cybersecurity and Operational Risk:** Moving large amounts of value across blockchain networks exposes custodians to heightened cybersecurity threats, operational risks, and potential systemic vulnerabilities that existing financial regulation may not fully address.

Lack of harmonized standards across platforms limit interoperability

Lack of regulations and standards for novel issues

- For instance, there is a need for standards for cross-chain interoperability, integrations with the DeFi ecosystem for tokenized assets (especially where TradFi and DeFi exchanges are involved), governance, and overall token structure

Novel issues posed by tokenization may signify a lack of standards and regulations, and therefore major gaps, for certain important issues. For instance, while some jurisdictions have frameworks providing legal wrappers for DAOs (e.g., BVI, Cayman Islands, Abu Dhabi), there is still no clarity on liability (e.g., pari passu defining who gets paid first when something goes wrong) or standardized requirements for different cases. Ultimately, lack of clarity makes it difficult to hold a license in different places where requirements may vary, such that it remains unclear who is responsible when an undesired event occurs. In the institutional space, on the other hand, traditional structures are still kept in place, even when digital finance is implemented. This may also lead to a high concentration risk.

TOKENIZATION VALUE CHAIN

This section provides a landscape of the end-to-end value chain of tokenization, evaluating each step involved – from primary markets, to settlement, and secondary markets. The table below lays out the steps involved in the process of tokenizing any asset and issuing it using distributed ledger technology (DLT)/blockchain infrastructure. For each step in the process, we provide an overview that includes actions taken (what happens), key stakeholders involved (who), and considerations for business value (why). We also identify relevant rules, standards, and guidance to inform the decision-making process for each step.

These rules are grouped generally based on the degree of compulsion (Annex 1 also includes a glossary of these publications which will provide links directly to the relevant documentation):

- **Official regulations**
- **Standards and recommendations for traditional finance**
- **Globally recognized standards (e.g., ISO) for blockchain and digital assets**
- **Other standards and guidance for blockchain and digital assets, including Ethereum Requests for Comments (ERCs) as widely adopted sets of common rules**

Considerations for Selecting Standards:

- Interoperability is key for wider adoption, such that standards that are more widely used can facilitate greater interoperability
- Consistent data fields improve interoperability across different assets, with greater comparability in data
- How proscriptive is a given standard

Those interested in tokenizing assets can use this table as a reference for the tokenization process and to identify relevant guidance to help ensure that they are compliant with relevant requirements. This landscape also serves to better clarify the role of key stakeholders (e.g., exchanges, banks, DeFi players) with respect to tokenization. It provides a view of how tokenization is disrupting traditional roles and participants, while reinventing their role (e.g., clearinghouses, transfer agents, etc.). We hope it can become a tool for increased collaboration, dialogue, and synergies.

DOWNLOAD THE TOKENIZATION LIFECYCLE TABLE

DEEP DIVE - CONSIDERATIONS FOR CUSTODY

An end to end value chain assessment for tokenization must go hand in hand with custody considerations. Given that tokenization is expected to be a massive market in numbers, involving several chains and tokens, the need for effective custody solutions to support the scale, volume, and breadth of assets is fundamental. While some risks and liabilities may shift across custodians in primary and secondary markets, and across self-custody models and 3rd party or institutional models, the general concepts remain the same across the value chain.

Custody for tokenized assets, from stablecoins, to tokenized securities, and other real-world assets, combines traditional principles of asset safekeeping with the new security and governance demands of blockchain-based systems. In this context, custody can refer to several layers: the custody of the underlying real-world asset (such as real estate, commodities, or reserves), the custody of the digital token that represents ownership of that asset, and the custody of the private keys that grant control over the token on-chain. Understanding how these layers interact is essential to determining who has legal ownership, operational control, fiduciary responsibility, and overall best practices (e.g., segregated account, use of omnibus accounts, reporting requirements, concentration of volume/ value held).

First, from a legal and regulatory standpoint, the classification of the token — whether as a security, commodity, or payment instrument — determines the type of entity permitted to act as custodian and the compliance requirements they must follow. Regulators set rules for custody, often depending on whether a given regulator has approved a tokenized digital asset in question. Regulated entities generally are required to uphold custody requirements (whether with a 3rd party custodian or self-custody), which may depend on the underlying asset.

For instance, the EU allows passporting to be able to operate in the region's 27 member states. To be a licensed custodian, an entity needs a license in a jurisdiction (subject to an application, approval process, and license granting), to hold certain types of digital assets in that jurisdiction. Licenses allow certain assets and are specific to asset classes. Non-regulated and non-compliant entities do not hold such registrations or licensing (e.g., USDT remains non-compliant in the EU based on MiCA requirements).

Custodians must ensure proper segregation of client assets both on-chain and off-chain to prevent commingling, while jurisdictional differences can complicate compliance in cross-border arrangements. Regulators around the world, such as the SEC in the U.S., the EU under MiCA, and the Monetary Authority of Singapore, are developing frameworks that increasingly recognize digital asset custodians and set standards for their operations. In parallel, a growing number of regulated entities, such as Zodia Custody, have pursued key registrations and authorizations across multiple jurisdictions (UK, Ireland, Luxembourg, Hong Kong), signaling it operational as a "qualified digital asset custody" provider for institutional clients. In other jurisdictions, entities (e.g., Anchorage, BitGo, and Hex Trust), are securing banking or trust licenses to provide qualified digital asset custody services.

Investor protection remains central to any custody framework. Custodians have fiduciary duties to ensure clear ownership rights, transparent audit trails, and alignment with applicable trust or securities laws. These protections help build confidence in the tokenized asset ecosystem and ensure compliance with evolving standards.

Second, from a technology and security perspective, the method of private key management defines much of the custody model's risk profile. Hot custody solutions store keys online for faster transactions but increase cyber exposure, while cold custody keeps keys offline for higher security. More advanced solutions, such as multi-party computation (MPC) and hardware security modules (HSMs), are gaining traction among institutions for their balance of safety and accessibility. Best practices include multi-signature authorization, strict access controls, continuous monitoring, and insurance coverage against theft or loss.

For tokenized real-world assets, effective custody also requires reconciliation between the on-chain tokens and the underlying physical or financial assets. Safe custody solutions are important for tokenized assets, especially tokenized RWA. For assets that exist off chain, tokenized representations prove the record exists and belongs to someone who holds it in a wallet. In the event an investor wants to redeem, collateral has to be available. Custodians or trustees must verify that the real assets exist, are unencumbered, and correspond to the number of tokens in circulation. Periodic audits and real-time attestations—sometimes through blockchain oracles—help maintain this alignment, and clear redemption procedures must be in place to allow token holders to convert tokens back into the underlying asset when desired.

Third, operational and governance considerations are fundamental. Recent hacks have challenged the initial view of security for digital asset custody. The default position that cold storage/offline storage is the safer option is shifting with increasing awareness on the role of governance and conduct to ensure safety of assets (e.g., if a custodian does not employ good conduct and governance practices, assets can be unsafe even if held in cold storage). For instance, custodians must review the smart contracts underlying tokenized assets to ensure proper administrative controls, upgrade mechanisms, and recovery processes. They should also manage counterparty risk by conducting due diligence on issuers and other service providers, while maintaining robust business continuity and disaster recovery plans to safeguard client assets in the event of system failures.

Finally, standards and best practices are key, such as ISO 24165 for digital token identifiers, ISO 20022 for standardized messaging, and the codes of conduct from industry groups. These sets of common rules and understandings are helping establish consistent practices for custody, governance, and interoperability. As these standards mature, they are expected to bridge the gap between traditional financial custody models and the emerging infrastructure for tokenized assets.

CONCLUSION: SHAPING THE FUTURE OF FINANCE

Tokenization has major implications for the future digital economy and its underlying infrastructure. This report outlines key lessons learned, principles to keep in mind, and a set of recommendations designed to help tokenization deliver real business value. Central to this discussion is the importance of building a robust ecosystem: one capable of supporting the trillion-dollar opportunity that many expect tokenization to unlock. As the digital economy continues to evolve, further infrastructure development is essential, especially given that the institutional tokenized market in capital markets remains largely untapped due to persistent challenges around interoperability and the absence of unified standards. Although various regulations and frameworks are emerging or awaiting approval, fragmentation remains a major barrier; siloed regulatory approaches hinder the efficiencies that tokenization promises, such as truly continuous, 24/7 markets. The recommendations that follow aim to address these gaps, beginning with defining what is required for tokenized funds to move seamlessly across platforms and jurisdictions.

The evolving digital financial landscape presents a powerful paradox: tremendous opportunities for innovation, efficiency, and inclusion, alongside complex challenges in ensuring stability, security, and fairness. As traditional finance merges with digital finance, regulatory, security, and market complexities intensify, creating a connected ecosystem that aims to combine legacy banking's reliability with the speed and flexibility of digital assets. Success depends on regulators adapting frameworks to prioritize safety while enabling financial institutions to embrace digital innovation.

Two pillars — soundness and innovation — are crucial for this transition. Technologies must be secure, resilient, and flexible. Close collaboration between regulators and financial institutions will build trust, ensure compliance, and promote the seamless integration of digital assets into existing systems. When established players adopt these changes, consumer confidence grows, accelerating broader market acceptance.

OPEN QUESTIONS TO BE ADDRESSED

How can harmonized regulations evolve? Currently, there is no unified legislation on tokenization. Countries vary in their approach based on market maturity—some apply existing financial laws to tokenized assets, while others create or adapt regulations for Distributed Ledger Technology (DLT). The rapid growth of decentralized finance (DeFi) and token markets exposes gaps, risks, and innovation potential. It is essential that token users receive protections equal to those offered for traditional assets.

What will be the tax treatment? A fair tax environment is also critical. Tokenized and traditional forms of the same asset should face identical taxation. Since DLT transactions are often cross-border, the OECD developed the Crypto-Assets Reporting Framework (CARF) in 2022 through international cooperation. CARF builds on existing standards like the OECD's Common Reporting Standard and FATF guidelines to improve tax transparency and KYC procedures for crypto assets. At the EU level, the proposed DAC8 directive aims to harmonize tax treatment of cryptocurrencies based on MiCAR definitions, fostering legal certainty to support the EU's digital market growth.

How do we address consolidation challenges that arise? Mergers and acquisitions (M&A) in DeFi face unique challenges due to token-based governance and complex securities laws. Decentralized protocols resist traditional centralized ownership models, complicating integration and valuation. M&A in crypto demands creative governance and compliance solutions to blend decentralized finance innovation with regulatory realities. As the industry matures, consolidation is expected, yielding fewer but stronger, better-regulated platforms serving retail and institutional investors. Hybrid regulatory frameworks and evolving M&A approaches will shape this transition, balancing innovation with practical compliance.

RECOMMENDATIONS TO ADVANCE TOKENIZATION

1. Establish & Adopt Common Standards

- Develop shared standards for token minting to ensure payment tokens can be easily integrated into wallets, platforms, and payment systems.
- Promote interoperability across networks and service providers to enable seamless token transfers and use in different ecosystems.

2. Strengthen Compliance and Risk Management

Implement consistent KYC and AML practices both at the point of token issuance and throughout secondary market activity.
Address operational and financial risks related to token redemption and conversion back into fiat, ensuring consumer protection and liquidity safeguards.

3. Set Collateral Requirements for Algorithmic Stablecoins

- Although not yet a primary regulatory focus, algorithmic stablecoins should require sufficient collateral—such as cryptocurrencies or tokenized real-world assets—to support stability and reduce systemic risk.

4. Accelerate Strategic Execution and Ecosystem Development

- Launch strategic tokenization initiatives that create measurable business value and accelerate time to market.
- Recognize that meaningful value emerges from an ecosystem approach, requiring collaboration across institutions and infrastructure providers.

5. Drive Organizational Commitment and Leadership Engagement

- Make tokenization a C-suite priority, allocating dedicated leadership, governance, and resources.
- Develop a clear tokenization strategy aligned with long-term business objectives, customer needs, and regulatory compliance goals.

OPEN QUESTIONS THAT NEED TO BE ADDRESSED

1. MARKET STRUCTURE & RISK

- How should risk be assessed and mitigated in secondary or retail token markets, where investors may not interact directly with issuers?
- What are the implications of tokenized post-trade processes—how do clearing, settlement, and custody differ from traditional systems?
- What constitutes finality in atomic settlement when one tokenized asset is exchanged for another (e.g., a stablecoin for a tokenized RWA)?
- How can regulators ensure control and security over permissions—who is allowed to alter books and records, and under what conditions?
- Should self-custody be a protected right? If so, under what safeguards or limitations?
- Should qualified investors have flexibility in choosing custody models, while retail investors are required to use regulated custodians?

2. STRATEGIC & CONCEPTUAL QUESTIONS

- How do money and assets differ in the context of digital economies, and what does that mean for tokenized financial systems?
- Should the "power to the people" concept—self-custody and disintermediation—be embraced or limited to maintain systemic stability?
- How can tokenization become a tool for collaboration and shared innovation, rather than a repetition of siloed initiatives?
- What role should financial market infrastructures (FMIs) play in the tokenized era, and how will traditional and digital networks coexist?

3. REGULATORY FRAMEWORKS & POLICY ALIGNMENT

- Do we need special rules for tokenized securities, or can existing securities laws adapt effectively?
- How should MiCA, MiFID II, and the DLT Pilot Regime interact to provide clarity for tokenized instruments in the EU? Is the EU at risk of an overregulated approach?
- How should stablecoins and CBDCs be regulated consistently given their role in settlement and payments?
- Should AML/KYC controls extend beyond on- and off-ramps to cover transactions within tokenized ecosystems or "walled gardens"?
- How can regulators enforce controls and ensure investor protection as value and collateral become tokenized?
- What should standards for good governance and third-party risk management look like in a tokenized environment?
- Most tokenized offerings may fall under exempt securities regimes—what does this imply for disclosure and investor protection requirements?

4. ECONOMIC DESIGN & MARKET EFFICIENCY

- How can the return on equity (ROE) or measurable business value of tokenization projects be determined when use cases remain isolated and infrastructure is incomplete?
- To what extent must the broader ecosystem participate to unlock real network effects and scale?
- How can cost and scalability challenges (the "chicken-and-egg" problem) in token issuance and operations be overcome?
- Is cost efficiency actually realized at each step of digital asset issuance, transfer, and redemption?
- To what extent is tokenization hampered by the lack of digital money or interoperable payment rails?

5. INFRASTRUCTURE, INTEROPERABILITY, & OWNERSHIP

- Who will own the payment rails of the future—banks, fintechs, or public-sector infrastructures?
- How can interoperability between digital and traditional systems be achieved (e.g., API-based access to digital assets via conventional apps and banking channels)?
- What role should consortium or cross-industry models play in building scalable tokenization infrastructure?
- What does the absence of trusted infrastructure mean for market readiness, and how can it be addressed through regulation or collaboration?
- How should post-trade and settlement standards evolve to ensure on-chain transactions meet legal and operational requirements?

6. INSTITUTIONAL READINESS & GOVERNANCE

- How can traditional financial institutions adapt their strategies as tokenization blurs the line between traditional and crypto markets?
- How do we ensure trust and collaboration between incumbents and new entrants, rather than fragmentation or redundancy?
- What level of education and digital literacy is needed among regulators, control functions, and institutional staff to manage tokenized finance responsibly?
- How can change management be structured so tokenization initiatives aren't siloed within small innovation teams but embraced organization-wide?
- What governance models will ensure control functions (risk, compliance, audit) mature alongside tokenization technology?

7. GLOBAL COORDINATION & REGIONAL DYNAMICS

- How should global standards and interoperability frameworks be developed to avoid regulatory fragmentation?
- How do regional differences—such as MiCA in the EU, stablecoin bills in the U.S., or Brazil's digital asset framework—affect competitiveness and cross-border token operations?
- How is progress in any given jurisdiction (e.g., Latin America - Brazil, Argentina, Paraguay) shaping regulatory momentum, and what lessons can global policymakers draw from it?
- Will the rise of sovereign or multilateral organization-sponsored blockchains (e.g., World Bank, IDB) create regional ecosystems that fragment or enhance global connectivity?

ENDNOTES

AI CONVERGENCE

1 GSMI 5.0: Use Cases, Foundation Models, and Key Principles for Growth: https://www.gbbc.io/uploads/reports/gsmi50/AI-&-Blockchain-Stand-Alone.pdf; GSMI 4.0 AI Convergence Foundations: https://www.gbbc.io/uploads/reports/Standalone-AI-GBBC-GSMI-4.0-Update.pdf
2 https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises
3 https://www.iso.org/standard/42001
4 https://www.nist.gov/itl/ai-risk-management-framework
5 https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence
6 https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act
7 https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai
8 https://venturebeat.com/security/report-finds-82-of-open-source-software-components-inherently-risky
9 https://openssf.org/blog/2025/01/23/predictions-for-open-source-security-in-2025-ai-state-actors-and-supply-chains/
10 https://insights.sei.cmu.edu/library/introduction-to-the-octave-approach/
11 https://docs.google.com/viewer?url=https://unsceb.org/sites/default/files/2024-04/United%2520Nations%2520System%2520White%2520Paper%2520on%2520AI%2520Governance.pdf
12 https://www.chai.org
13 https://www.linkedin.com/pulse/ozempic-lawsuits-have-arrived-personal-ai-revolution-piniewski-md-wgzwc/
14 This vision can be structured through a three-zone model for processing data with open-source and decentralized AI: Zone I: the individual's "home-base" where their personal lived experience is collected and managed; Zone II a correlation engine that aggregates anonymized data contributed from many individuals to find correlations, patterns, and risk/benefit insights; Zone III is the commercial/research zone, where insights are used for broader studies, industry, or public-good applications, while preserving privacy.
15 https://www.linkedin.com/pulse/personal-data-economies-waze-future-personalized-piniewski-md-sckzc/
16 https://www.linkedin.com/pulse/world-ai-unemployment-states-must-redefine-value-piniewski-md-j6anc

DECENTRALIZED FINANCE (DEFI)

17 https://www.sec.gov/about/crypto-task-force
18 https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125
19 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBoIgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs___Crypto_Task_Force_Written_Submission.pdf; https://www.sec.gov/files/ctf-written-input-digital-chamber-073125.pdf

20 https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf
21 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBoIgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs___Crypto_Task_Force_Written_Submission.pdf
22 https://www.sec.gov/files/ctf-written-input-digital-chamber-073125.pdf
23 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBoIgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs___Crypto_Task_Force_Written_Submission.pdf
24 https://www.sec.gov/files/ctf-written-input-securitize-050725.pdf
25 https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf
26 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBoIgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs___Crypto_Task_Force_Written_Submission.pdf
27 https://www.sec.gov/files/ctf-written-input-digital-chamber-073125.pdf
28 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBoIgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs___Crypto_Task_Force_Written_Submission.pdf
29 https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf
30 https://www.sec.gov/files/ctf-written-input-securitize-050725.pdf
31 https://www.sec.gov/files/ctf-written-input-digital-chamber-073125.pdf
32 https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf
33 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBoIgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs___Crypto_Task_Force_Written_Submission.pdf
34 https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf
35 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBoIgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs___Crypto_Task_Force_Written_Submission.pdf
36 https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf
37 https://assets.ctfassets.net/eynrhjw8vyk9/3EYG7pCfLoXHeBoIgKXQfu/3690038182428ae1bf0bb35b18d73541/Sidley_Austin_on_behalf_of_Ava_Labs___Crypto_Task_Force_Written_Submission.pdf
38 https://www.sec.gov/files/ctf-written-input-securitize-050725.pdf
39 https://www.sec.gov/files/ctf-written-securities-questions-responses-081525.pdf
40 https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf
41 https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/
42 https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125
43 Some questions focus on traditional registered offerings, exchange-traded products, or investment companies, which are more relevant to tokenized securities than to permissionless DeFi protocols.
44 https://www.owlexplains.com/en/podcast/ava-labs-x-cber-ep-2-governance-of-decentralized-autonomous-organizations/
45 https://www.worldscientific.com/doi/10.1142/S281100482350001X?srsltid=AfmBOoofMXWXnJCQWdoW5WYe4_TL9XQdHrH_IwXlvPX_dEmCVRNhSWGm

DIGITAL IDENTITY & PRIVACY

46 https://committee.iso.org/sites/tc68/home/news/content-left-area/news-and-updates/iso-17442-3-verifiable-leis-vlei.html
47 https://www.unjspf.org/for-clients/digital-certificate-of-entitlement/
48 https://www.iso.org/standard/75302.html
49 https://www.singpass.gov.sg/main/
50 https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
51 https://finance.yahoo.com/news/hidden-cost-aml-95-false-134601048.html
52 https://home.treasury.gov/news/press-releases/jy0916
53 https://home.treasury.gov/news/press-releases/sb0057
54 https://www.dlnews.com/articles/defi/regulators-turn-on-privacy-coin-monero-after-bitcoin-booms
55 https://contentauthenticity.org
56 https://rufftimo.medium.com/sedi-details-for-identity-nerds-e1949af5cc30
57 https://people.csail.mit.edu/mengyuanli/files/asiaccs_sok.pdf
58 https://privacypools.com/
59 https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2
60 https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
61 https://fidoalliance.org/specifications/
62 https://www.icao.int/sites/default/files/publications/DocSeries/9303_p1_cons_en.pdf
63 https://datatracker.ietf.org/doc/html/rfc6749
64 https://www.iso.org/standard/85628.html
65 https://www.iso.org/standard/75061.html
66 https://www.iso.org/standard/24760-1
67 https://www.iso.org/standard/71670.html
68 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf
69 https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14260
70 https://www.nist.gov/privacy-framework
71 https://pages.nist.gov/800-63-3/
72 https://www.pcisecuritystandards.org/standards/
73 https://openid.net/developers/how-connect-works/
74 https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#name-introduction
75 https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
76 https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0-05.html
77 https://trustoverip.org/our-work/technical-architecture/
78 https://www.w3.org/TR/did-1.0/
79 https://www.w3.org/TR/webauthn-2/
80 https://www.w3.org/TR/vc-data-model-2.0
81 https://www.w3.org/TR/webauthn-2

DIGITAL MONEY & PAYMENTS

82 Does not include non-blockchain DLTs, or hybrid ledgers.
83 https://www.theblock.co/post/373314/stablecoin-market-cap-surpasses-300-billion-for-first-time-amid-crypto-rebound
84 https://www.pwc.com/m1/en/publications/2025/docs/unlocking-the-future-of-finance-with-stablecoins.pdf

85 https://www.pwc.com/m1/en/publications/2025/docs/unlocking-the-future-of-finance-with-stablecoins.pdf
86 https://www.jpmorgan.com/insights/global-research/currencies/stablecoins
87 Coinmarketcap data as of Nov 28, 2025
88 https://www.theblock.co/post/377031/jpmorgan-circle-usdc-stablecoin-tether-usdt-onchain-growth
89 https://www.atlanticcouncil.org/cbdctracker
90 https://www.atlanticcouncil.org/cbdctracker
91 https://www.gi-de.com/en/spotlight/currency-technology/cbdc-its-time-to-act
92 https://www.atlanticcouncil.org/cbdctracker
93 https://www.jpmorgan.com/kinexys/documents/deposit-tokens.pdf
94 https://kpmg.com/xx/en/our-insights/value-creation/deposit-tokens-bridging-traditional-banking-and-the-digital-economy.html
95 https://www.forbes.com/sites/digital-assets/2025/09/09/real-world-assets-nearly-died-now-theyre-soaring-in-crypto/
96 https://www.addx.co/files/bcg_ADDX_report_Asset_tokenization_trillion_opportunity_by_2030_de2aaa41a4.pdf
97 https://www.mckinsey.com/industries/financial-services/our-insights/the-stable-door-opens-how-tokenized-cash-enables-next-gen-payments
98 https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng
99 https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money
100 https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng
101 https://eur-lex.europa.eu/eli/dir/2018/843/oj/eng
102 https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-rba-virtual-currencies.html
103 https://assets.ctfassets.net/so75yocayyva/4Plcwx7j9lfGuLHUnvnFKW/864b0955a33ab1467d2971825f7273ae/Proposed_Risk_Mitigation_Framework_for_Non-Financial_Risks_of_Blockchain_Infrastructure.pdf
104 https://datatracker.ietf.org/doc/rfc8578/
105 https://cdn.prod.website-files.com/648841abc97f28489cc3f2ce/6656e9c60c3029989dcd7431_IVMS101.2023%20interVASP%20data%20model%20standard.pdf
106 https://sagroups.ieee.org/bdlsc/
107 https://notabene.id/tap
108 https://notabene.id/tap
109 https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng
110 https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money
111 https://datatracker.ietf.org/doc/rfc8578/
112 https://datatracker.ietf.org/doc/draft-ietf-satp-architecture/
113 https://assets.ctfassets.net/so75yocayyva/4Plcwx7j9lfGuLHUnvnFKW/864b0955a33ab1467d2971825f7273ae/Proposed_Risk_Mitigation_Framework_for_Non-Financial_Risks_of_Blockchain_Infrastructure.pdf
114 https://assets.ctfassets.net/so75yocayyva/4Plcwx7j9lfGuLHUnvnFKW/864b0955a33ab1467d2971825f7273ae/Proposed_Risk_Mitigation_Framework_for_Non-Financial_Risks_of_Blockchain_Infrastructure.pdf
115 https://assets.ctfassets.net/so75yocayyva/4Plcwx7j9lfGuLHUnvnFKW/864b0955a33ab1467d2971825f7273ae/Proposed_Risk_Mitigation_Framework_for_Non-Financial_Risks_of_Blockchain_Infrastructure.pdf
116 https://www.frbservices.org/financial-services/fednow/what-is-iso-20022-why-does-it-matter
117 Definitions below come from CFTC – GMAC – DAMS taxonomy: https://www.cftc.gov/media/10321/CFTC_GMAC_DAM_Classification_Approach_and_Taxonomy_for_Digital_Assets_030624/download&sa=D&source=editors&ust=1755814393564217&usg=AOvVaw3gDYhL95fgP0FusGMzpkkk

118 Source: coinmarketcap, as of Nov 26, 2025 noting that market capitalization as an indication of size an adoption may reflect market dynamics more than payments utility
119 https://zodia-custody.com/singapores-bold-approach-to-regulating-digital-assets/
120 https://www.mas.gov.sg/schemes-and-initiatives/project-guardian

SUPPLY CHAINS & CRITICAL MINERALS

121 https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-supply-chain#/
122 https://www.ifrs.org/content/dam/ifrs/supporting-implementation/issb-standards/issb-materiality-education-material.pdf
123 https://www.congress.gov/crs-product/R47982#:~:text=Pursuant%20to%20the%20Energy%20Act,domestic%20resources%20and%20other%20research
124 https://www.wrforum.org/wp-content/uploads/2023/07/ECTR-2023.pdf p8
125 https://unctad.org/system/files/official-document/tcsdtlinf2023d1_en.pdf
126 https://documents1.worldbank.org/curated/en/719971468325781473/pdf/Trade-and-transport-corridor-management-toolkit.pdf
127 USD 50 billion invested
128 JICA
129 https://www.yahoo.com/news/articles/china-us-japan-race-control-093000426.html
130 https://apnews.com/article/congo-rwanda-drc-peace-deal-m23-trump-5e5b52100729ad6587a6f267c6c79ae0
131 https://www.break-down.org/post/on-this-day-opec#:~:text=OPEC%20sought%20to%20challenge%20this,number%20of%20Arab%20oil%20producers
132 WY Multi Trillion find on rare earth mineals; OR & NV Lithium deposits
133 J. Borrell
134 https://unctad.org/system/files/official-document/tcsdtlinf2023d1_en.pdf
135 https://www.c-star.io/commercial-trust-protocol#:~:text=The%20Commercial%20Trust™%20Protocol,throughout%20the%20global%20trade%20ecosystem.
136 https://minehub.com/minehub-ensures-timely-and-accurate-data-sharing-with-blockchain/#:~:text=MineHub%20has%20established%20a%20consortium,component%20to%20driving%20operational%20efficiency
137 https://www.prnewswire.com/news-releases/volvo-cars-joins-responsible-sourcing-blockchain-network-launched-by-ibm-ford-and-volkswagen-group-advancing-ethical-sourcing-of-minerals-continues-to-scale-with-this-network-300952585.html
138 https://www.mckinsey.com/capabilities/operations/our-insights/supply-chain-risk-survey
139 https://www.wrforum.org/wp-content/uploads/2023/07/ECTR-2023.pdf
140 Peace Agreement Between the Democratic Republic of the Congo and the Republic of Rwanda - United States Department of State
141
142 https://www.ansi.org/standards-news/all-news/9-9-24-new-ansi-report-enabling-standards-development-through-public-private-partnerships
143 https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm#:~:text=The%20principles%20include:%20*%20Making%20essential%20information,Constraints%20on%20developing%20countries%20should%20be%20considered
144 https://www.worldstandardscooperation.org/; https://www.ansi.org/standards-news/all-news/2024/08/8-6-24-iso-iec-and-itu-july-2024-listings-of-work-items-published
145 https://www.archyde.com/astm-compass-platform-expanded-access-resources/

146 https://www.icmagroup.org/fintech-and-digitalisation/fintech-resources/fintech-jargon/
147 https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/01/tokenisation-of-assets-and-distributed-ledger-technologies-in-financial-markets_be149012/40e7f217-en.pdf
148 https://www.esma.europa.eu/sites/default/files/2025-10/Joint_ESAs_Factsheet_on_crypto-assets.pdf
149 https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf
150 https://www.cftc.gov/media/10321/CFTC_GMAC_DAM_Classification_Approach_and_Taxonomy_for_Digital_Assets_030624/download
151 https://old.maa.org/press/periodicals/convergence/mathematical-treasure-mesopotamian-accounting-tokens
152 https://www.sec.gov/files/ctf-written-antonio-lanotte-global-blockchain-business-council-051425.pdf
153 https://www.sifma.org/research/statistics/fact-book
154 https://research.grayscale.com/reports/the-link-between-worlds
155 This designation can include tokens designated as network or protocol tokens by the White House report "Strengthening American Leadership in Digital Financial Technology," as digitally native tokens that are intrinsically connected to the operation of a network or protocol, which includes payment transactions within the network. Examples include Bitcoin and ether.
156 While stablecoins might not be settled until they are redeemed for the "real" money in custody elsewhere, CBDCs are the asset in their own right and don't need to be redeemed.

GBBC