GBBC
Global Blockchain
Business Council

UPDATE

GLOBAL STANDARDS MAPPING INITIATIVE 5.0
DECEMBER 2024

GBBC GSMI 5.0

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 5.0

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 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 5.0, GBBC is profoundly grateful for the active participation of 110+ entities spanning government, corporates, startups, nonprofits, and academia, who also took part in 7 specialized working groups that continue to produce the most meaningful discussions on the most crucial issues in the space: focused on Blockchain & AI Convergence, Decentralized Finance (DeFi), Digital Identity, Supply Chain, Sustainability, Taxonomy, and Technical Standards, where all other topics converge.

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.

This is the fifth annual release of GSMI, and with it comes a new website with improved user friendliness, that better captures the history of GSMI and the key accomplishments that the GBBC community has produced every year, as reflected in key statistics for every GSMI launch. These accomplishments cumulatively build upon each other, making GSMI 5.0 the most robust and comprehensive release to date.

GSMI 5.0 KEY FINDINGS

- 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

GSMI 4.0 KEY FINDINGS

- 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

GSMI 3.0 KEY FINDINGS

- 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

GSMI 2.0 KEY FINDINGS

- 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

GSMI 1.0 KEY FINDINGS

- 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

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 regulatory map, the team expanded the content and made it more user-friendly, covering **over 3,400 individual regulatory developments across 230 jurisdictions** & **6 international regulatory bodies**, while introducing enhanced filtering features.

GSMI 5.0 also expanded the taxonomy to include 391 terms, including multiple definitions for blockchain and digital assets terms, from globally recognized standards setters, that users can also filter over an interactive format. This is meant to document the landscape of definitions as they exist today, mindful that these definitions will evolve with further development of the space. These definitions include the work of GBBC as co-chair of the US Commodity Futures Trading Commission (CFTC) Global Markets Advisory Committee (GMAC) – Digital Asset Markets Subcommittee (DAMS), which presented a Digital Assets Classification Approach and Taxonomy that was approved on March 6, 2024. In addition to updating the relevant definitions, the GSMI 5.0 also added a set of visuals to portray related definition clusters.

The technical standards section continues to become more comprehensive, this time including **67 bodies advancing standards**, characterized as globally or regionally-focused standards setters, associations, and regulators setting standards for various aspects of the industry. In addition to the technical standards listing, GSMI now introduced a set of cross-cutting use cases for technical standards that can improve business and organizational competitiveness across all industries and sectors: organizational resilience, use of resources, identity verification, and tokenization. These use cases are presented in the context of the increasing importance of decentralized governance, and key principles where technical standards are fundamental to advance the necessary governance that will enable this new generation of models of business and organizational activity to unlock massive industries in the future.

GSMI 5.0 also continues to updates 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 courses from accredited educational institutions is also expanded to include **1,500+ courses**.

Finally, GSMI 5.0 releases 5 in-depth reports as the output of 5 of its working groups, focused on areas where the GBBC community recognizes significant opportunities for blockchain technology developments: Blockchain & AI Convergence, Decentralized Finance (DeFi), Digital Identity, Supply Chain, and Sustainability. While the DeFi report provides foundational topics on the space, with the launch of the new DeFi working group with GSMI 5.0, the other reports build on the previous year's foundational reports, focusing this year on tangible use cases and principles for standards and regulations.

In addition, in collaboration with key stakeholders, GSMI produced a **Country Spotlight on India**, covering the latest developments in blockchain and digital assets in the country. India sets an example of startup activity and government openness to supporting blockchain technology implementations to improve lifestyles.

With this comprehensive body of resources, we hope it will serve our community and continue to develop in meaningful ways for the years to come.

CONTRIBUTORS

We would like to thank our many partners, members, and supporters who worked tirelessly and enthusiastically over the past months to produce GSMI 2024, version 5.0, including

WORKING GROUPS

AI CONVERGENCE
CO-CHAIRS

JOHN DEVADOSS
Board Director, GBBC; Founder, NeuralFabric

TANVI SINGH
Board Director, GBBC; Former Managing Director, Digital Assets, Data & AI, UBS; Venture Capital and Co-Founder

JULIE STITZEL
Senior Vice President, Policy, Digital Currency Group

DEFI
CO-CHAIRS

JOE CUTLER
Partner, Perkins Coie

LEE SCHNEIDER
General Counsel, Ava Labs

YVETTE VALDEZ
Partner, Latham & Watkins LLP

DIGITAL IDENTITY
CO-CHAIRS

SANKARSHAN MUKHOPADHYAY
VP, Customer Experience, Dhiway

MICHAEL WAGNER
Partner, Oliver Wyman

SUPPLY CHAIN
CO-CHAIRS

DALE CHRYSTIE
Chairman, BITA Standards Council; Business Fellow and Blockchain Strategist, Fedex

GREG BROWN
Vice President – Technology Strategy and R&D, UPS

SUSTAINABILITY
CO-CHAIR

JONATHAN RACKOFF
VP, Head of Global Policy, The HBAR Foundation

TAXONOMY

GBBC

TECHNICAL STANDARDS
CO-CHAIRS

DAN CONWAY
Teaching Professor, Associate Director of the Blockchain Center of Excellence, University of Arkansas

NEIL WASSERMAN
Adjunct Professor in Computer Science, The George Washington University

PARTNER PROGRAMS

IFC-MILKEN SCHOLARS

SHERECE NEAL
Investment and Reserve Management Officer III, Central Bank of Belize

RITHY PICH
Head of CIS & Derivatives Business Supervision Division, Securities and Exchange Regulator of Cambodia (SERC)

IFC International Finance Corporation WORLD BANK GROUP

MILKEN INSTITUTE

GSMI 5.0 FELLOWS

ADRIAN MATAK
London School of Economics and Political Science

NAMRRITHA SENTHILKUMAR
The George Washington University

LSE THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

GW

THANK YOU

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

Abed Group, Addiko Bank, ADM Risk, Regulation & Strategy Ltd, AgriLedger, AIFC Authority, Alliance Block, AnChain AI, Antonio Lanotte, Aptum Technologies, Association of National Numbering Agencies (ANNA), Ava Labs, avanade, Babesta, Banco do Brasil, Bell Rock Group, Blockchain Laboratories, BlockHealth LLC, Buki Ogunsakin, Carbonmark, Central Bank of Belize, Central Bank of Jordan, Champaka Bindigenavile, Citi, Citizens Bank, CoinShares, Commercial Bank of Dubai, ContractClarity™ AI, Crypto Index Series, CUNY Queens College, Cybercorp Limited, Denise McCurdy, DFM Data Corp., Inc., Dhiway, Diane R Maurice (US Treasury Ret), Digital Asset, DLx Law, DTIF, Emc3, EUBOF, Excellence Consulting International, EY, FedEx, Florida Tech, Folks Finance, FTI Consulting, George Washington University, Georgetown University, GFT, GLEIF, GoingVC, Grant Thornton Indonesia, HCL Tech, HKSI Institute, HRB GROUP, Hyperledger Latinoamerica Regional Chapter, ICN Business School & Minespider, IEEE, Impera Strategy, Instituto New Economy, ISO, Japanese Ministry of Finance in New York, Justin Atwell, Kintsugi Tech, KlimaDAO, Landis & Co, Latham & Watkins, Leadingbit Solutions, Liongate Bahamas Limited/One X Solutions, Lyn Brooks, Makki Elfatih, Mary Lacity, Mayer Brown LLP, Minervavaluations.com, NeuralFabric, Nexera & MarketXM, NorthstarDAO, Oliver Wyman, OpenID Foundation, OTA, U.S. Department of Treasury, Paul Rapino, Paypal, Perkins Coie, Polymesh, QFCA, Ramena OÜ, Rebecca Spour , RecycleGo, Reti S.p.A., RFI Foundation, Ripple, Rosario Tech Law, LLC, RSNDL, Schroders Investment Management Ltd., Schulich School of Business, Securities and Exchange Regulator of Cambodia (SERC), SLLS Global Legal and Consulting Group, Stability Protocol, Standard Chartered Bank, SUNN Blockchain, Tassat Group, Tergo, The George Washington University, The HBAR Foundation, The Provenance Chain, TICsLegal, Token City, TRANSOM, UNCEFACT, United Nations Joint Staff Pension Fund (UNJSPF), University of Arkansas, University of Wyoming, UPS, USBC, Veritas Tech, Women in Digital Assets Forum, World Summit Awards, WU University Vienna

Special thanks to the GBBC team for their contributions:

- Diana Barrero Zalles
- Greg Buron
- Tristen Dague
- Riley Fay
- Philip Gant
- Summer Graham
- Sierra Lewis
- Alfredo Oballos Diaz
- Sandra Ro
- Jackson Ross
- Mariana Sarmiento

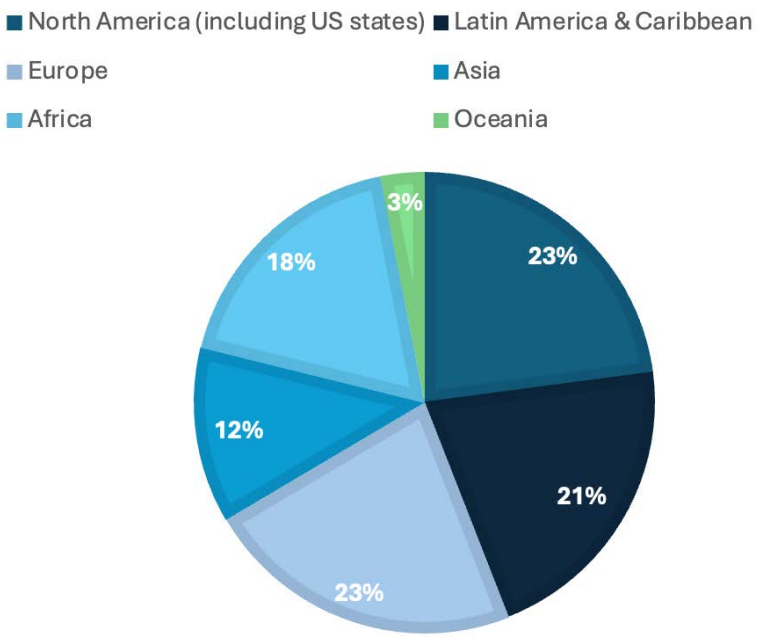
SECTION II

LEGISLATION & REGULATORY DEVELOPMENTS

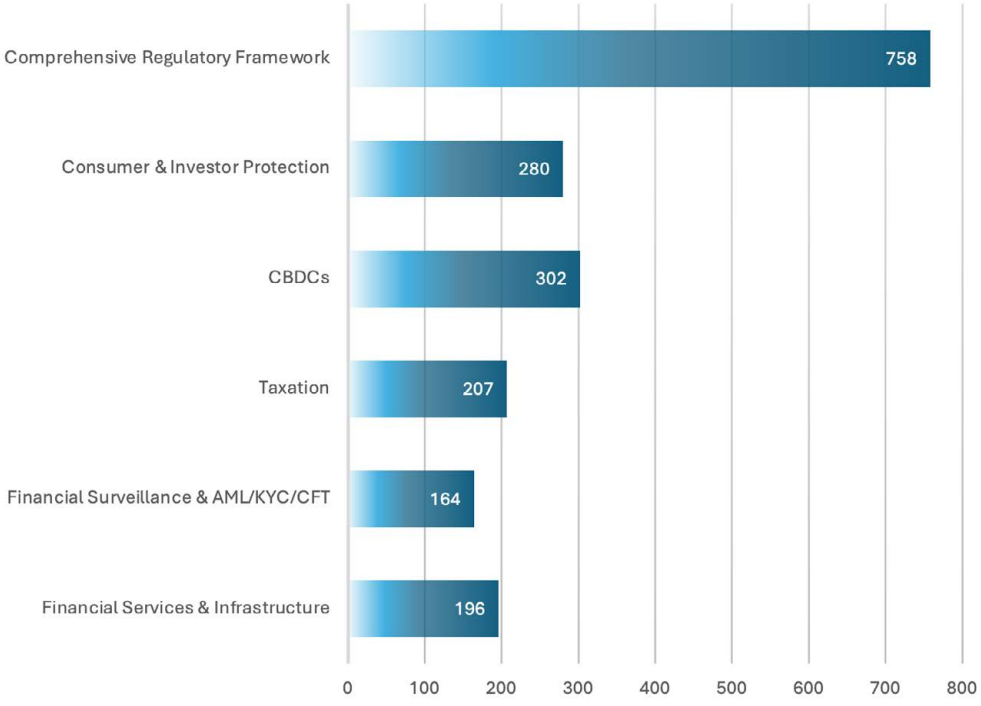
Regulatory developments around the world for blockchain and digital assets continue to take form, as government bodies increasingly recognize the role of this technology in financial markets, infrastructure, and all economic sectors. GSMI 5.0 has documented the latest trends toward increasing regulatory clarity, harmonized approaches across jurisdictions, and attempts to develop rules and requirements that will support innovation and inclusion, while ensuring adequate security and consumer and investor protections. Governments bodies continue to take part in relevant discussions, assessments, and collaborative endeavors to share lessons learned and coordinate global approaches to regulation. Regulatory sandboxes are continuing to facilitate testing environments, and many efforts are taking place to clarify rules beyond enforcement actions setting precedent for the legal treatment of blockchain technology. There remain open questions for risk assessments ahead and other key issues, but progress is being made, often through industry bodies and key principles driven by industry players.

GSMI 5.0 has documented **over 3,400 documents**, many of these primary resources, pertaining to regulatory developments for blockchain and digital assets in **230 jurisdictions** and **6 international bodies**. These include sovereign countries, monetary unions (e.g., European Union and African monetary unions), states (e.g., US states), and major global policymaking bodies (e.g., Financial Action Task Force) that set standards and requirements for countries globally to embed into their respective regulatory frameworks. Regulatory developments span a wide range of issues, with financial surveillance & AML/KYC/CFT, consumer & investor protections, taxation, CBDCs, and financial infrastructure being the most common, aside from comprehensive regulatory frameworks that cover several issues. This trend of the most common themes for regulatory developments continues from GSMI 4.0 and prior. Among these major issues of focus for regulatory developments, the most common ones have been selected and quantified in the diagram.

Jurisdictions by Geographic Region



Number of Regulatory Developments by Major Issue



Access the Interactive Map of Regulatory Developments

SECTION III
TAXONOMY

GSMI 5.0 Taxonomy: 391 Terms

In order to foster the level of collaboration across stakeholders necessary for scale, it is essential to operate under a common language. 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 5.0 Taxonomy includes **391 total terms** specific to blockchain and digital assets and sector-specific terms relevant for key applications in supply chain, sustainability, convergence with Artificial Intelligence, and digital identity. At the core, **217 essential blockchain and digital assets terms** are further into main subject areas specific to the space, drawing on prior academic categorizations utilized in existing taxonomies. Each term has been cross-checked against definitions from multiple globally respected standards setting bodies and industry-specific glossaries. Therefore, there are multiple definitions for most blockchain and digital assets terms, in order to reflect the fact that the space is still developing and that the definitions are continuously evolving. 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.

ACCESS INTERACTIVE TAXONOMY

DEFINITION CLUSTERS

SECTION IV

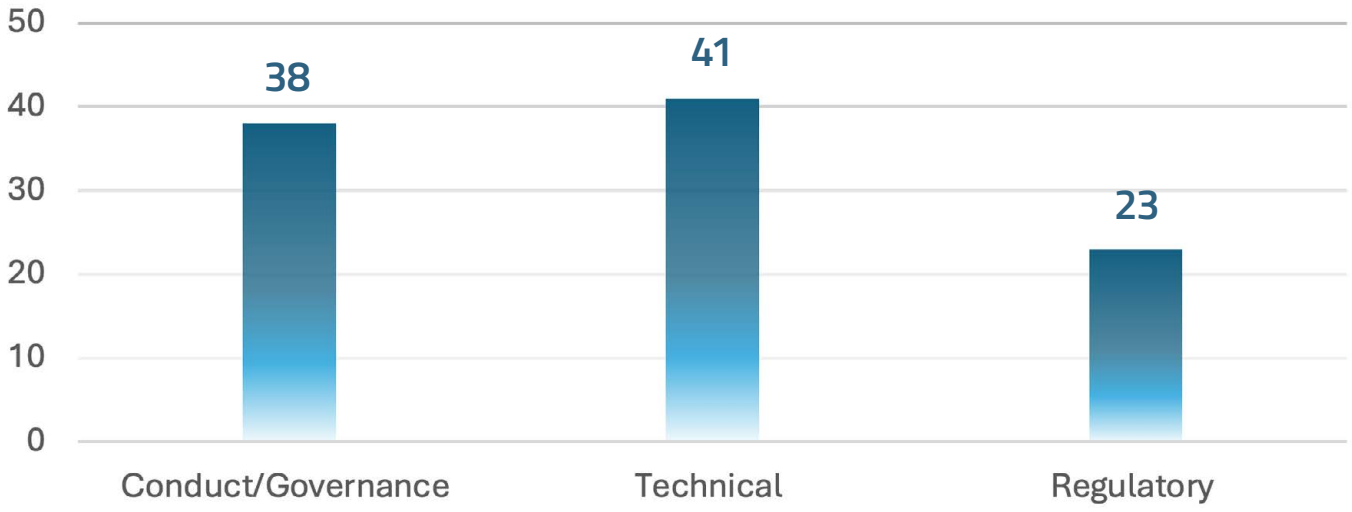
TECHNICAL STANDARDS

Technical standards for developments in blockchain and digital assets, as in any new technology, are fundamental to ensure safety, reliability, and further innovation. Technical standards are fundamental for all use cases and sectors in which this technology is being adopted. They establish common guidelines, definitions, and rules of the game through technical criteria, specifications, methodologies, and practices which all serve to ensure adequate functionality as well as the levels of interoperability, trust, and ease of use necessary for stakeholders to work together. Collaboration is fundamental for the growth of an industry, in ways that will ultimately lead to widespread acceptance of formalized rules and regulations. This repository of **67** technical standards bodies is meant to provide an objective overview of the state of standards developments today for blockchain and digital assets, with no vested interests from any particular organization.

Technical Standards are fundamental for governance, especially as decentralized governance structures arise enabled by blockchain technology. Below we provide a commentary on standards as they relate to a value chain of governance. In this context, technical standards are also enabling overarching foundational use cases that are key for success across industries and sectors: tokenization, identity verification, business continuity, and resource management.

In the content provided, we continued to facilitate ways for readers to identify how they can work with other groups, and for industry standards organizations to identify for gaps, opportunities, and areas for alignment. We also worked to make it easier to compare across standards bodies based on their purpose and proposed outcome, while also allowing for self-identification based on their topics and industries of focus. Standards in the space are marked according to their proposed outcome, which may be technical standards and specifications, regulatory compliance, or best practices and governance. The standards bodies are also categorized by their main function as global or regional standards setters or associations, and whether they may have a regulatory affiliation.

Number or Technical Standards Bodies by Proposed Outcome



TECHNICAL STANDARDS AND GOVERNANCE

TECHNICAL STANDARDS USE CASES

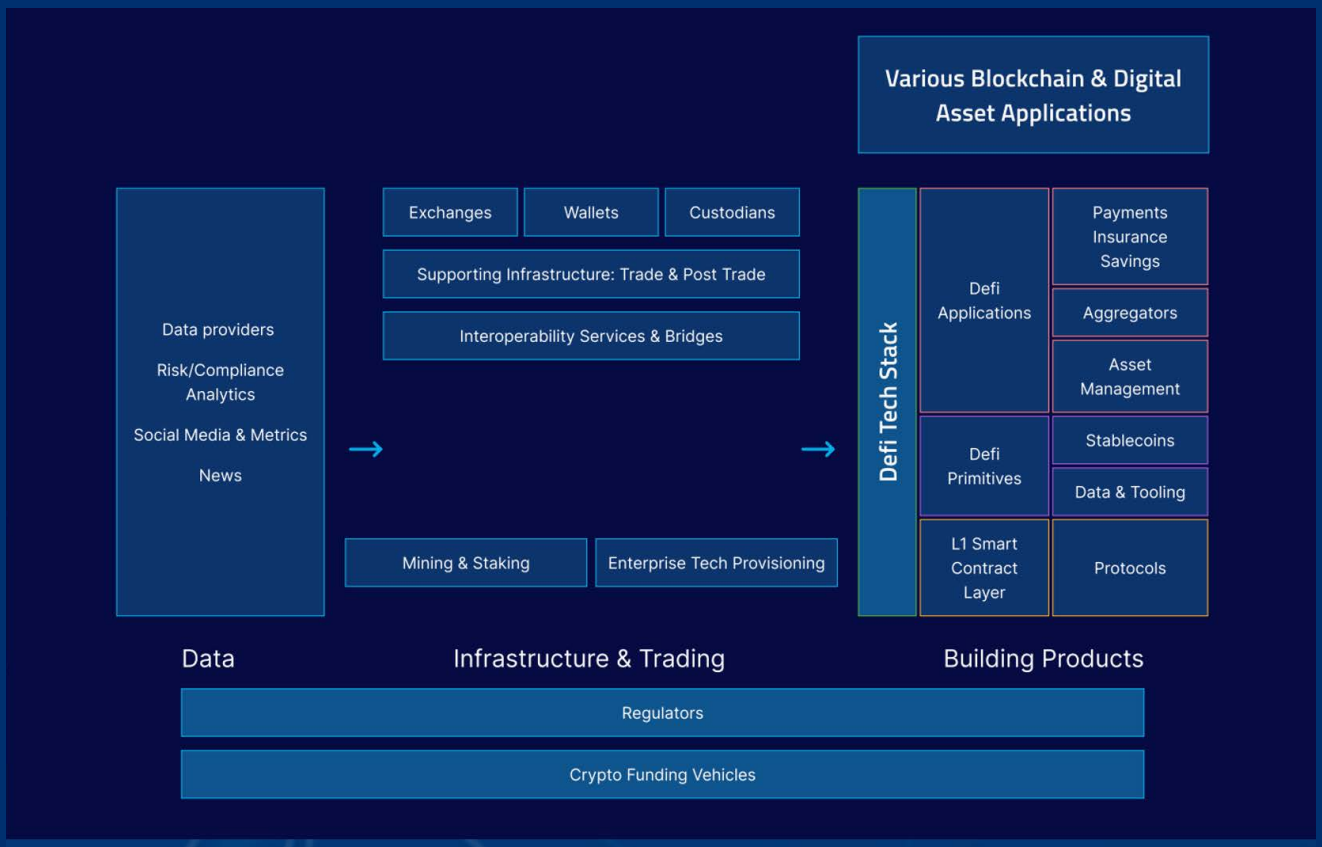
TECHNICAL STANDARDS LISTING

SECTION V

BLOCKCHAIN & DIGITAL ASSETS LANDSCAPE

The blockchain and digital assets landscape is made up of products, services, platforms, and infrastructure that together support a wide range of developments and applications. 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. GSMI 5.0 offers a continually updated global mapping of this landscape, with key stakeholders and their interactions, as summarized in the diagram. GSMI 5.0 also provides access to the full list of 2,000+ players, and welcomes further suggestions from the community. We are beginning to mature and institutionalize this multi-trillion dollar industry, with many more developments underway and innovations to come.

Key Stakeholders in the Blockchain & Digital Assets Landscape



Source from here: https://gbbc-nextjs-production.up.railway.app/gsmi/landscape

ACCESS THE LIST OF 2,000 + STAKEHOLDERS

SECTION VI

COURSES FROM ACCREDITED EDUCATIONAL INSTITUTIONS

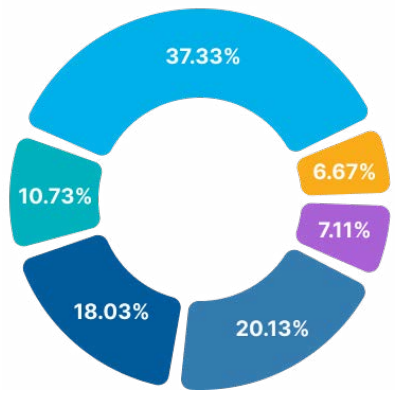
Where is Blockchain Being Taught? Blockchain is being increasingly incorporated into the curriculum taught at universities and other educational institutions around the world, offering academic degrees and other certifications. We have compiled this repository of over 1,500 courses spanning multiple academic disciplines. We hope that by compiling this repository of courses 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. Below is a listing of blockchain-related courses in universities and other educational institutions, as well as a **form** to collect additional submissions for courses. Students, professors, and other university staff can submit their blockchain courses for inclusion through this form and apply for the GBBC observing membership program.

ACCESS THE COURSE LISTING

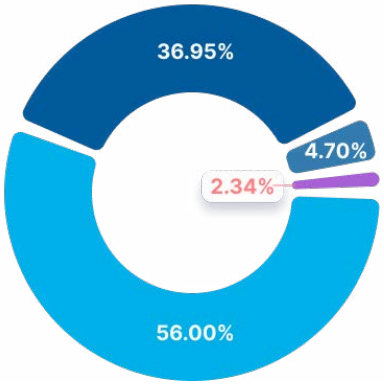
ANALYTICS

1,575 COURSES

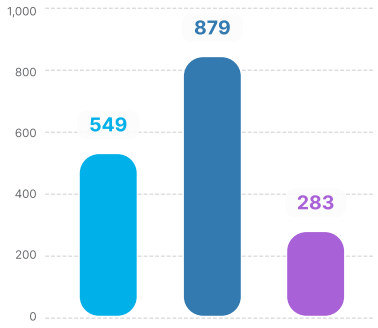
By Region



By Academic Field



By Degree Level*



*Courses may be offered at multiple degree levels

SECTION VII

AI & BLOCKCHAIN CONVERGENCE: USE CASES, FOUNDATION MODELS, AND KEY PRINCIPLES FOR GROWTH

EXECUTIVE SUMMARY

With the rapid expansion of AI across all industries, interactions between humans and machines are creating endless possibilities, which can make existing solutions better but also make existing problems worse, all while creating new and unanticipated issues. Now more than ever, cooperation among stakeholders is essential to ensure responsible innovation that will benefit humanity. Blockchain can provide a spectrum of verified and trusted data going into AI algorithms, which can then draw patterns to guide informed decision making. AI, on the other hand, can improve blockchain applications. The use of data verified on a blockchain can address many of our concerns over unchecked AI applications, and also provide more legitimacy to AI-driven outcomes. How does this get real today for all of us? Many use cases are already leveraging this convergence, often through foundation models, and driven by global regulatory developments.

In the context of emerging technology convergence and the rise of Web3, the sections below highlight when and where the combination of AI and blockchain can bring the most value. This report will bring awareness to strategic use cases at the convergence of blockchain and AI, the role of foundation models, and how companies can take advantage of these opportunities, remaining competitive while also mitigating potential risks. Finally, there is a commentary on essential standards and regulatory developments, including recommendations to fill any gaps.

PUTTING THE AI EXPLOSION INTO PERSPECTIVE

With the rise of ChatGPT, ChatGPT-4, and a myriad of AI tools to enhance virtually every facet of our human activities, important questions are being raised with respect to the interaction between humans and machines. For instance, if an estimated 44% of legal tasks to be automated,[1] where does that leave humans? As company cultures are being adapted to AI, the roles of humans and machines are evolving. Yet machines may struggle to replace human insight, our emotional connections, and our lived experiences.

AI is essentially an archipelago of various sciences and technologies that are built on logic, statistics, deduction, and associations. AI divorces agency from intelligence, creating a new form of agency that is automated in nature. This automated agency alone, without human intelligence, can result in

misfortunes rather than solutions. If AI is not doing its job properly, it can lead to serious harms (e.g., privacy breaches, increased biases, etc.).

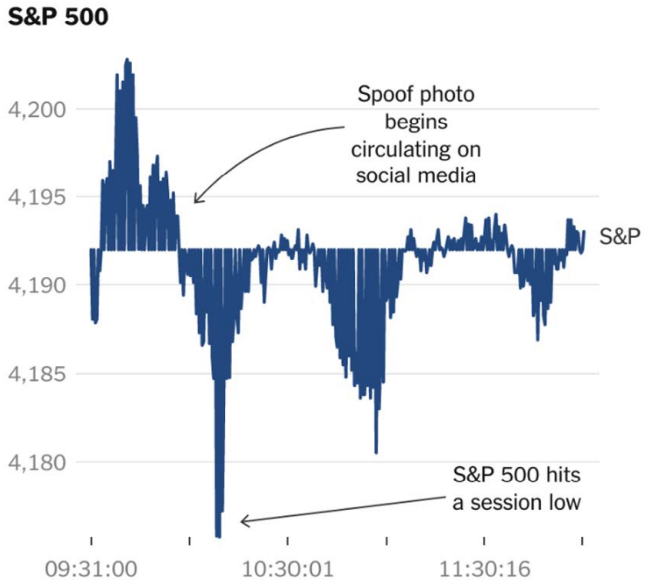
When AI solutions can maximize our possibilities to carry out and achieve any task, the point may not be to maximize activity and functionality alone, but to do so in the right way. Attention to responsible AI, from its very design and throughout its developments, can avoid significant monetary and reputational risks, while ensuring sustainable innovation and long-term competitiveness. A taxonomy of key AI terms can be found in Annex 1.

Better solutions & worse problems?

In expanding human capabilities, AI can improve existing solutions greatly. Yet the downside can be equally large in magnitude by making existing problems worse, and creating new ones along the way. AI is built on data, which can be used to make more informed decisions, but can also be misused for harmful purposes, and no one knows what can happen in the future. The potential dangers and their future repercussions are unknown. For instance, an AI algorithm using data that heavily represents a majority population may conclude that minority populations need less services, when on the contrary they are underserved and underrepresented in the data. This may lead to actions with the opposite effect than what is in fact needed, broadening inequalities rather than solutions. Unintended consequences and malicious activities with data can lead to unprecedented harms that need to be considered.

In what can be considered the first documented account of an AI-generated "fake image" widely shared on social media, a spoof image posted in in May 2023 led to a dramatic stock sell-off on the S&P market.[2] A fabricated image of a major explosion near the Pentagon, the headquarters of the US Department of Defense, was posted on the social media platform X by an account posing to be a "Bloomberg Feed," causing a social media uproar alongside a major market downturn.The false reported incident was even spread by several media outlets internationally, reaching an audience of millions before local authorities responded as swiftly as they could to assure the public that no such explosion had occurred.

Figure 1: Stock Market Effect of AI-Generated Fake Image



Source: Sentieo/AlphaSense • By The New York Times

While it is widely recognized that leaders across sectors can make better informed decisions with AI tools, it is less widely known is that blockhcian technology can optimize those solutions and also help address the risks that AI may bring. Emerging technologies are best equipped to work in convergence, which makes data science an increasingly crucial skill for corporate and organizational decision makers. Blockchain technology can bring trust to AI-driven processes, and even AI artifacts themselves can be better validated when represented entirely as digital assets.

Data Provenance

Data provenance is essential for trustworthy AI solutions. Blockchain technology can provide transparency on the source of data utilized for AI algorithms. Provenance of data is essential for a multiplicity of activities, industry sectors, and business practices, from supply chain traceability to ensuring the authenticity of products (e.g., champagne can only be called champagne if comes from the designated area of France). It can provide a stamp of approval that there has been no forfeiture, and that ethical business practices have been adhered to throughout a given process (e.g., no forced labor).

Blockchain technology can also validate that the origin of data comes from legitimate sources, increasing the reliability of AI implementations that are built with that data. If an algorithm utilizes data protected by copyright or behind paywalls, data derived from children, or worse yet, from dark markets, actions can be taken to refrain from using that model, and if it's an entity's power, to quarantine and destroy the model altogether.

Moreover, visibility on the origin of data can also enable better evaluating its adequacy for implementing AI solutions intended to address specific needs. Transparency on data sources helps identify the existence of potential risks from relying on biased or limited information, and take necessary measures to address and mitigate these risks. Not all data may be fit for purpose, and data deserts are important to identify. For instance, data sets that heavily represent a narrow population may not be adequate for AI solutions applied to broader populations, for the risk of spurious connections and irrelevant conclusions.

Data Quality:

There is a vast amount of data available, of which the majority has been created during this generation. Moreover, not all the data created in this generation has been about ground truths of human lived experience; rather, much is interpreted, 3rd party, synthetic data. The further the distance from ground truths, the greater the issue of potential AI model failure.

Potential issues can also result from the fact that older data records (e.g., paper archives, black and white movies, and even ancient papyrus records) are much less pervasive, and not designed for AI. Blockchain can bring light to these concerns and identify potential biases, empowering companies and organizations to redesign processes accordingly.

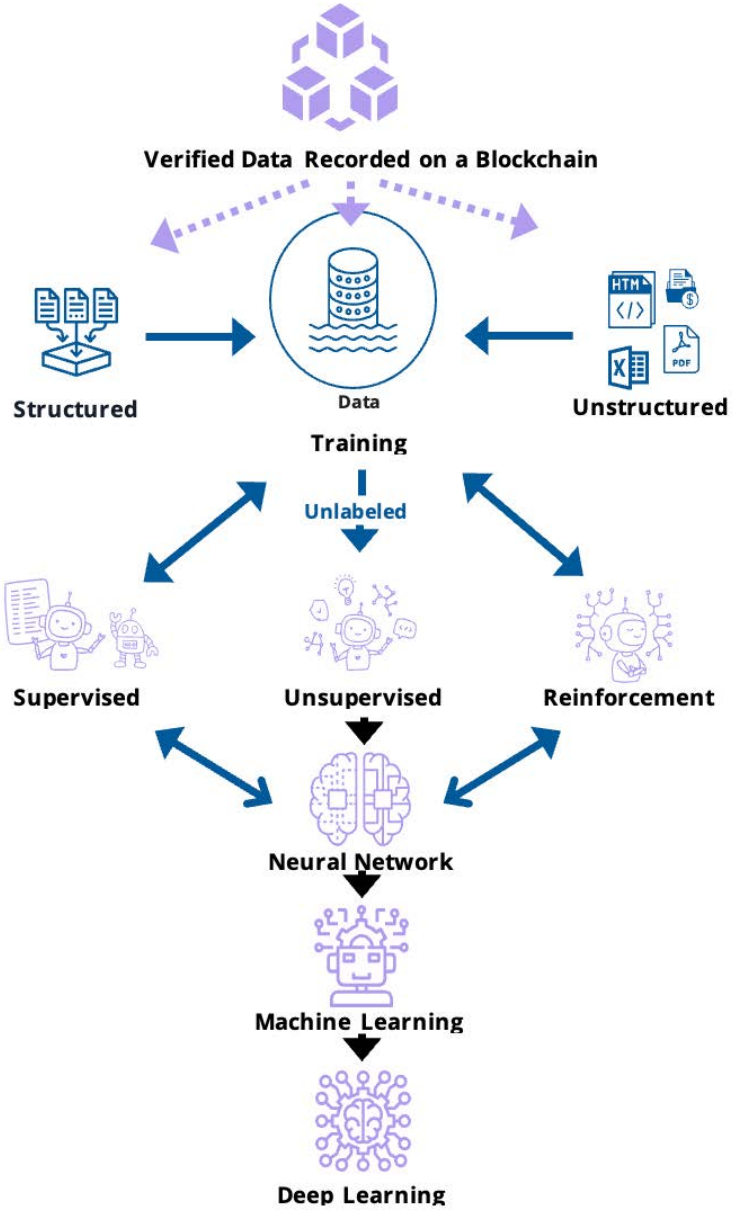
Furthermore, data quality can be regarded as a spectrum, starting with direct from source vs. interpreted data, 3rd party data, synthetic data, and beyond. Models are likely to be most reliable when they minimize the low-quality data used in training. This enables a future where humans become extremely valuable as data providers, given that human lived experiences become the preferred form of data to ensure AI model robustness. Blockchain technology can provide a scoring system that rates the extent to which the data used by an AI algorithm is sourced from direct lived experience (higher quality data) vs. synthetic data (less quality data).

Data Privacy & Security

Currently, it is not the data itself but trade secrets that can be protected by copyright laws. If data is disclosed, it is not protected. If confidential data is leaked and misused, the results and implications can be devastating and may be largely unknown. There is uncertainty on where potential integrations can go using leaked data. Especially when data alone is not regulated, the countermeasures may be very limited. This creates a backstop, and an incentive not to disclose data even when data sharing would be beneficial, potentially leading to multiple difficulties for companies and organizations adopting AI solutions.

Blockchain technology enables better privacy protection mechanisms to ensure data is safeguarded, allowing personal data to be exchanged as needed and protected simultaneously. Cryptography & zero-knowledge proofs (ZKPs) can be used to verify the necessary data for a given activity without revealing additional and unnecessary information. Pseudonymity may enable compliance with privacy requirements, and data may be made available only to authorized parties. Blockchain-based verifications can also ensure that data is not manipulated. These measures can bring multiple benefits to operational processes, laws and policies.

Figure 2: Blockchain-based AI solutions (source: GSMI 4.0 AI Convergence report)



Blockchain capabilities can enhance processes to manage third-party risk and reduce vulnerabilities. Moreover, authentication of data by a blockchain can prevent cyberhacks. As a best practice, sensitive data would not be stored in central repositories or recorded directly on the blockchain. Code would be audited to prevent data theft and other risks, and both risk analysis and KYC reporting can draw on existing practices used in financial services today.

Transparency on Processes & Outcomes

Beyond the data sources, blockchain adds transparency to methods of processing data with AI algorithms, as well as their final outcomes. With greater visibility on approaches to data processing and decisions resulting from AI uses, the entire lifecycle can be traced and validated. For instance, blockchain can document the properties of tools like Large Language Models (LLMs). Records can be kept for monitoring and evaluating results and effectiveness of AI solutions, and ultimately as a mechanism to enforce established ethical guidelines.

Transparency can help identify instances where AI suggested solutions may be irrelevant, and even harmful to carry out. For instance, an AI algorithm drawing on data that heavily represents a population other than that of users can be identified for adequate action to be taken.

Decision makers can better understand the potential and limitations of AI developments and their resulting outcomes. Based on the insights provided by blockchain records, processes can be reinvented to preserve equality and inclusion, rather than economic and social disparities. Measures can be taken to ensure automation does not cause job losses when certain functions are replaced by machines, but rather optimize the use of human capabilities to ensure adequate AI deployments. Finally, decentralization of data and processes can address concentrations of power, avoiding single points of failure to add resilience to systems.

USE CASES OF BLOCKCHAIN & AI

The use cases below are a testament to all the innovations where blockchain technology and AI are working together toward better and more reliable solutions, in ways that can affect every aspect of human civilization. Convergence between these technologies is improving solutions at the very infrastructure level, enabling foundational use cases on which a wide range of innovations can be built across sectors. A second category of use cases comprises solutions that build on these foundational use cases, enabling solutions tailored to specific industries and sectors. Many of the use cases in the table below are expected to continue to evolve with new sub-applications.

A key feature to highlight among the use cases below comprises decentralized AI, which inherently merges blockchain and AI, in ways that fundamentally transform the way artificial intelligence is developed, governed and used. Decentralization allows AI models to be created in a grassroots manner rather than relying on centralized models, providing an alternative to a scenario where few centralized players would dominate resources and compute capacity. Any participant can create, share, and monetize AI solutions through decentralized AI networks. Allowing decentralized players to build models can help reduce potential concentration of control and power.

While blockchain can decentralize the AI stack, AI can learn and run processes based on distributed sources of data and compute. The decentralization of AI systems takes us to a level of transparency that is often lacking and deeply needed in our current centralized systems. Decentralized AI prioritizes transparency, ethical governance, and empowerment of individuals and actors.

Figure 3: Decentralized AI

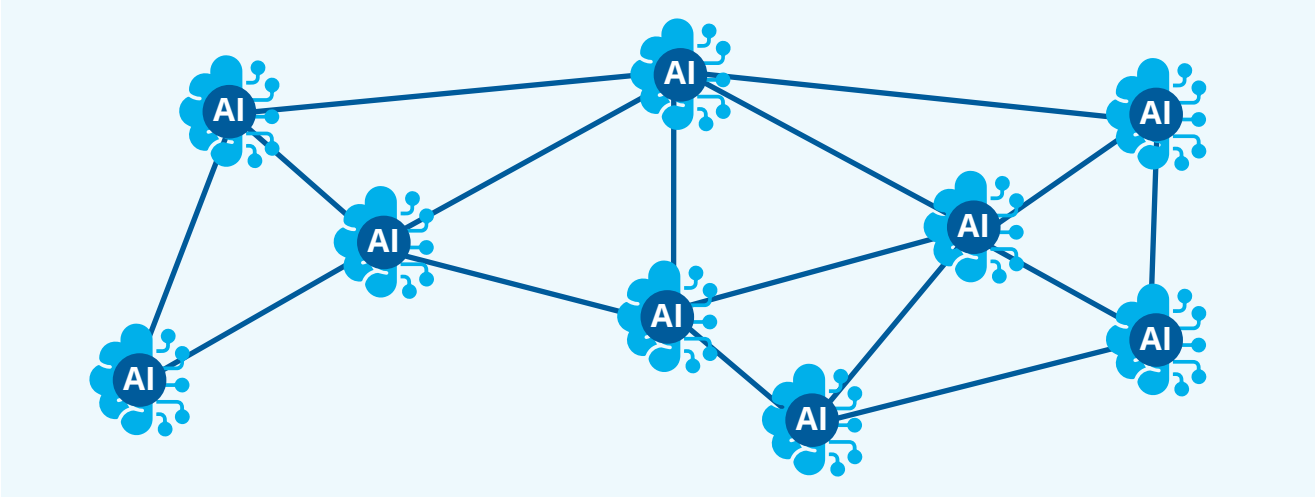


Table 1: Use Cases of Blockchain & AI Convergence

Use Case	Role of Blockchain	Role of AI	Examples & Benefits
Foundational Use Cases			
Decentralized AI	• Verified data from decentralized sources. • Security of data and immutability of records. • Decentralized compute capacity. • Data distribution for training data to build models. • Incentive payment layer for individuals to provide data or compute capacity to decentralized AI models. • Decentralized data oracles.	• Training on different sources of data. • Utilizing unused computing power to build open-source AI models.	• Solutions that enable more users to create, manage and monetize their own data, models, and compute capacity • Technology: Allowing devices to enable additional compute, to support participation of decentralized players. • Healthcare: Contributing patient data from distributed sources to support pharmaceutical research, using AI for molecule discovery, etc. • Healthcare: Patient matching to clinical trials to encourage greater and more decentralized participation.
Digital identity and identifiers	• Decentralized storage and enhanced security of personal data (e.g., biometric data). • Digital asset identifiers can record the source of data. • Immutable audit trails, with validation control throughout an entire process lifecycle. • Enhanced identity verification and authentication for individuals and legal entities, as well as their certificates and licenses.	• Passing regulatory reviews as precursor for acceptance • Maintaining regulatory compliant operations	• Basic & Public Services: Enhancing identity checks to facilitate broader access • Global Supply Chains: A textile product can carry data recorded across the supply chain and production process (e.g., type of cotton used, labor involved, points of shipment and sale) • Circular Economy: Tracking the recycling of products, to monitor effectiveness and impact • Global Supply Chains: Digital Asset Identifiers can facilitate global trade, improving supply chain traceability • Healthcare: Enhancing research & development while safeguarding patient data

Data Integrity	• Validating provenance of data in enterprise level AI models and LLMs • Ensuring quality of data for intended purposes • Applying metrics for foundation models, to ensure reliable data sources and results • Timestamps ensure latest version of AI model is in use	• Data processing using legitimate data for a variety of tasks • Translating data between data sets that may use different measurements, helping break data silos and ensuing "apples to apples" comparisons	• Enterprise decision making enhanced by control over data provenance (mitigating "garbage in garbage out" situations) • Enhanced governance systems • Healthcare: Harmonizing workflows and assets (e.g.,, blood sugar measured in different units from different countries) • Reliable foundation models for use across sectors
Security & Privacy	• Security for data ownership and data sharing (e.g., timestamping, zero-knowledge proofs) • Developments in encryption and hash functions (e.g., chameleon hash functions) can allow for changes in blocks without breaking cryptographic chain, securing access to authorized parties and also enabling GDPR compliance.	• Training data and generation of content based on best practices for data ownership and data sharing	• Solutions that can ensure availability and adequate sharing of data that is kept secure and private (e.g., sharing patient records)
Smart Contracts	• Ensuring security and data provenance • Supporting scalability of blockchain solutions	• Formal verification and testing of smart contracts • Assessment of oracles • Analyzing smart contract code • Automating identification of vulnerabilities	• Smart contract audits can benefit from AI's ability to improve security, efficiency, and compliance • LLMs can enhance security audits of smart contracts • Enhancing security and scalability of smart contract-based solutions across sectors
Sector-Specific Use Cases			
Addressing deepfakes & misinformation	• Authenticity of data sources	• Data processing • Limiting the use of personal data	• As new tools like Chat GPT 4 are unveiling new voice and video capabilities that closely resemble humans, the source of a video or audio message can be authenticated with blockchain • Authenticating media, entertainment, and other public content including videos of public figures, coverage of elections, etc.

Audit	• Record of audit trails and audit history log • Securing evidence • Visibility on owners of on-chain assets/wallets, which can be tagged if connected to illicit activities (e.g., tainted funds, sanctioned individuals or countries)	• Sampling of evidence, discovery, and audit testing • Comprehensive testing of audit scenarios	• Audit companies enhancing their procedures • Ensuring regulatory compliance, such as payment of taxes • Audit trails of on-chain activity, to track and trace illicit funds and identify the individuals behind them, enhancing effectiveness of law enforcement
Autonomous Vehicles	• Securely recording and validating data from sensors • Validated records of users and secure identity management	• Predictive modeling • Informed decision making • Optimized natural language processing to communicate with passengers	• Optimized processes and security, reducing accidents and fraud • Enabling new and trusted opportunities for services like ride hailing and trucks • Enabling new mobility trends in cities and outside cities
Carbon credits Access to Land and Water Resources	• Validation of legitimate sources of carbon credits • Validation of carbon credits • Tracking the lifecycle of carbon credits, from issuance and sale to retirement • Ownership records • Records of land and water resources, including key infrastructure and IoT • Tokenization and distribution of land and water resources	• Evaluation of projects, and assessment of emissions reduced/avoided • Setting pricing based on carbon credit quality • Tracking progress toward Sustainable Development Goals • Identify and document existing contracts and rights currently in place • Predict potential geopolitical conflict • Evaluate contracts	• Certified ecological projects accessing markets to sell carbon credits • Reducing fraud or double selling in carbon markets with enhanced transparency • Enhanced digital monitoring, reporting, and verification (dMRV) to monitor and evaluate efforts to mitigate climate change • Identification and mitigation measures when there is rising geopolitical tension, given that land and water rights are a trigger for geopolitical conflict • Enhancing peaceful negotiations with transparency • Streamlining sales and transactions • Managing decentralized physical infrastructure network (DePIN) more effectively
Compliance & Regulatory	• Validation and registration of the use of personal data • Records of personal information usage by LLMs • Verifiable credentials • Enhancing citizens' ability to comply with rules via greater transparency	• Identify and set the level of access to information for any individual or entity • Identify compliance trends and activities • Assessing impact and outcomes of policies and regulations • Audits of tokenomics for smart contracts using AI • Audits of smart contracts and credentials	• Managing access to information in government and corporate environments • Political monitoring platforms for public affairs activities and strategic engagements • Enhancing audit, accounting, and consulting practices • Enhancing adherence to relevant laws and regulations with data and analytics (e.g., Companies identifying relevant requirements to comply with as they expand to new jurisdictions) • Enhancing regulators' view of effectiveness of citizens' level of compliance with requirements (e.g., tax collected vs. taxes owed)

Public Policy	• Capturing and recording relevant data on various topics	• Models can go through documents and identify important content for any entity	• Enhancing discussions among regulators and government bodies • Supporting democratic processes
Healthcare	• Securely protecting individual identities • Ensuring each data entry involved is verified optimally	• A non-rivalrous AI can search for correlations (e.g., fertilizers & cancer, microplastics in hot beverage lids, etc.) • AI agents do not act as personalized recommendation engines but rather as transparency engines that identify individualized risks and potential mitigation measures in time to make a difference	• Protecting individual citizen while providing crowdsourced and pre-licensed correlations to commercial entities for scientific rigor and product development • 3-Zone model[3] : Zone 1) Personally controlled longitudinal records of life experiences; Zone 2) Benevolent correlations only; 3) Use by commercial, government, industry, research entities, etc.
Financial Services	• Immutable and secure record of transactions • Record of asset ownership • Built-in auditability	• Predictive analytics for pricing and performance • Portfolio analytics and recommendations • Generating and executing tests (e.g., A/B testing) to optimize solutions • Automating and streamlining portfolio and investment decisions • Processing market data with more speed, accuracy, and efficiency to determine trends, risks, etc.	• Enhancing portfolio analytics • Optimizing fintech solutions, wealth tech, and banking operations • Allocating shareholder votes and enhancing governance processes • Investment funds can optimize buy/hold/trade decisions based on current portfolio status • For on-chain traders, AI wrappers can allow token conversions across blockchains without requiring wallets on each blockchain
Economic Development	• Enabling infrastructures supporting greater access to basic services, universal basic income programs, and humanitarian aid • Using data as an economic asset, an alternative to taxation for generating universal basic income • Validating identity of aid recipients and safeguarding privacy	• Testing and tacking management and effectiveness of social and economic assistance interventions, including universal basic income programs • Assessing the benefits of traditional finance, financial innovations, and decentralized finance infrastructures for economic assistance programs • Designing and managing incentive structures	• Streamlining processes and reducing corruption in government assistance programs • Enhancing effectiveness of foreign aid programs in developing nations • Improving monitoring and evaluation of results • Enhancing incentives to create profitable jobs in the AI sector that align with sustainability principles or universal basic income initiatives

Ethical Considerations

With greater power to effect change comes greater responsibility. Ethical considerations point to the underlying purpose of AI deployments, as intended by a sense of morality and values to ensure the wellbeing of humanity. As any other tool, AI can be used for good or for harm, but in this case the potential impacts in either direction can be exponential. It is important to define basic shared values to ensure AI implementations ultimately support the common good. It is imperative for AI use cases to take these ethical considerations seriously from the very design and intent, and monitor adherence to ethical considerations throughout their lifecycle. Ethics and safety measures must be built into the very model, not tacked onto the end of a process.

It is equally important to note, however that ethics is a process more than an end point, especially given the rapid developments in the technology and the novel issues they raise. Participatory ethics can be difficult due to the challenges of equally and fairly representing all diverse views and populations into AI models. While we may not approve of an elected official, for instance, we hopefully can trust in the democratic processes for electing leadership. In a similar way, trust and reliability in the process for ensuing ethical AI are key. Buy-in from senior leadership is essential whenever possible.

Companies and organizations must also be cautious and humble about the unknowns that AI can bring, acknowledging the multiplicity of future outcomes that can take place. With the increasing pace of change and acceleration, it is crucial to be fast and nimble in order to adapt to changing circumstances, needs, and potential concerns. There will be a constant back and forth between AI and the world's complex challenges. There should also be a "hierarchy" in ethical considerations to prioritize key issues in these complex scenarios.

Ethics for AI becomes a multifaceted endeavor that can involve multiple tasks and considerations, summarized in the following basic principles:

- **Equality & Inclusion:** Inclusive decision-making processes go hand in hand with ensuring adequate representation of diverse communities and perspectives. It is necessary to consider the social and economic impacts of AI, especially in light of the key societal challenges that this technology may even be intended to address. With the speed of scale and rate of change, the risk of leaving behind entire communities becomes crucial (e.g., faster chips and functions may require bandwidth and Internet connectivity that are not available for entire populations to access). When things go wrong, AI has the potential to harm marginalized communities the most.

- **Protection of Human Agency:** AI solutions should be designed as co-pilots of humans, enhancing rather than replacing our agency. In past de-skilling models, humans needed to understand a task to make it more efficient and teach it to other humans. With AI, humans must understand tasks to teach them to machines. This requires off-skilling and re-skilling in ways that must keep humans at the helm of decision making and supervision, not merely as a step in a larger process. Human insight cannot be fully replaced by machines and must be present throughout the entire process of training data, running algorithms, and interpreting the results.

- **Privacy, Security & Fairness:** While there are different ways of approaching security and privacy, it is necessary to ensure resilient systems and identities. Companies and organizations are being increasingly rated on trust and motivation. Users and customers

want to know that their data is secured responsibly, and they want to maintain their individual sovereignty. Ethical AI developments should safeguard individual rights and liberties based on a sense of sovereignty.

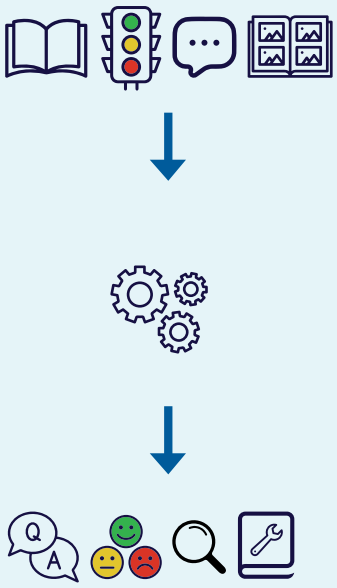
- Governance & Accountability: Trust is fundamental for AI, alongside a notion of a dynamic social compact that adjusts with new issues at the technology progresses. Trust frameworks should be founded upon governance and interoperability considerations. They should reflect a broad understanding of the collective benefits relative to any risks of AI. Shared values, responsibilities, and roles point to the importance of continued collaboration among stakeholders. While companies may have different priorities for models and governance approach (e.g., depending on the size of the company), it is beneficial to define a roadmap and strategy with specific principles to prioritize.
- **Managing AI Risks:** An adequate approach to risk assessment and mitigation will reduce misuse and unintended consequences. Understanding risk implications, as a starting point from the design of any AI model, can lead to better assessing the full tech stack behind each use case from an ethical perspective. AI agents, for instance, can learn and run models that embed risk considerations alongside the benefits they offer.

FOUNDATION MODELS

Foundation models are tools that are trained on substantial amounts of data to carry out a wide range of activities, enhancing business intelligence and any of the use cases in the section above with increasing accuracy. Their adoption has exploded in recent years, as have the amount of foundation models available for the public to use, which are now in the hundreds. With larger industry players creating new models consistently, there are also gravitational pulls toward economies of scale. Models may be open to the public on any device, or alternatively they may require login via software and subscriptions for enhanced tasks. They vary widely in architecture, approach to processing data (e.g., autoregressive, autoencoding, encoder-decoder, multimodal, retrieval-augmented, sequence-to-sequence), and outputs (e.g., text-to-speech or vice-versa, text-to-visual).

Figure 3: How Foundation Models Work

Data inputs (e.g., text, signals, speech, images)



Various outputs

Data Processing for a wide range of activities				
Program writing: using natural language to generate code	**Image Captions:** Describe and classify images	**Image Generation:** using natual language	**Parsing Data:** extracting data from images	**Classify text:** Based on entities, parts of speech, or other text categories
Q&A: Answering natural knowledge questions using knowledge base	**Writing assistant:** Corrects writing and grammar	**Summarize:** Drawing key concepts from text	**Math & Code:** Solving basic math & programming problems	**Translation:** From one language to another
Explaining Code: Describing code functionality in natural language	**Sentiment Rating:** Provides sentiment analysis and rating from text (happiness, warmth, etc.)	**Chat:** Mimics human conversation to enhance service delivery (e.g., chat bots)	**How-to manual:** Directions to complete a task (e.g., recipes, etc.)	**Search:** Provides search functionality
Natural Language Processing: Enhancing communication across languages and systems, including more natural human to computer interactions, and powering machine translation	**Content Creation:** Creates text or other content based on prompts (e.g., job description, ad, product description)	**Image and Video Analysis:** Object detection in security cameras, analysis of medical imaging, generation of special effects in video content	**Scientific Discovery:** Accelerating scientific research by analyzing massive datasets, identifying hidden patterns and relationships effectively (e.g., drug discovery, climate change research, materials science)	**Automation:** Automating any repetitive tasks, to free up time for more complex work to be performed by humans

The most common foundation models are featured below, and a full landscape of these tools can be accessed in Annex 2.

Table 2: Overview of Selected Foundation Models

Foundation Model	Provider	Description	Access
GPT (Generative Pre-trained Transformer) series	OpenAI	Multimodal LLMs, with a proprietary model, to process knowledge and language patterns from various Internet sources, with vast scope of training data.	Open
BERT (Bidirectional Encoder Representations from Transformers)	Google	Machine Learning framework used by Google to understand context from search queries using Natural Language Processing, processing knowledge and language patterns from various Internet sources,	Closed
Llama	Meta	Autoregressive LLMs to recursively generate and predict text, using data from publicly available resources, with an open-source model	Open
BLOOM	BigScience	Multilingual autoregressive LLM to support open science initiatives, accelerating AI-driven insights	Open
Claude	Anthropic	"Constitutional AI" principle to align models to enterprise needs, with strong language capabilities and context windows, to focus on larger and more complex models	Open or limited (depending on the version)
Bedrock	Amazon Web Services	Generative AI capabilities for application building, model alignment, governance, and security within the Bedrock ecosystem.	Limited
Gemini	Google DeepMind	Offers multimodality and interconnectivity with Google Cloud. Commercially available multimodal LLM with multilingual capabilities	Open or Limited (depending on the version)
DBRX	Databricks	Pre-trained model to build applications, and carry out governance and security tasks, with support services for users to fine-tune it.	Open
Nemotron	Nvidia	Multilingual and multimodal capabilities for enterprise solutions of Nvidia customers.	Open
Granite	IBM	Capabilities for enterprise needs and governance structures, offering robust insights into the training data used, to mitigate risk of unlicensed content.	Limited
Phi	Microsoft	Processing real and synthetically generated content, enabling the use of small datasets and curated content, aligning model behavior to needs of enterprises.	Open
Cohere Command	Amazon Web Services	Business-friendly models to support knowledge based on retrieval-augmented generation (RAG), with multilingual capacities and specific optimizations.	Limited
Mistral AI	Mistral AI	Internationally-focused open-weight models allowing access for developers to modify internal structure. Strong core language capabilities with an approach of "mixture of experts" enable higher accuracy with fewer computing resources	Open

While traditional AI models, are more narrow and built from scratch, foundation models can be pre-trained, providing developers with a solid starting point to build applications, which in turn make them more likely to outperform traditional models. They can contribute to the democratization of AI by lowering barriers to entry.

Foundation models are versatile and can be fine-tuned in many ways, making them much more flexible and adaptable. They often experience ongoing training, with constant new version releases. By fine-tuning data into narrower datasets to carry out specific tasks, foundation models also make new AI application development faster, more efficient, less expensive, and reliant on less compute power.

Recent trends point toward smaller models, with reliable data as sources and results. Specified tasks point to pre-trained data and processes, that may be domain-specific or general in their approach. For instance, an LLM educated on image analysis, healthcare data, translation, etc. can be adapted to specific use cases and applications. Foundation models can also be supplemented with organizational data. Even micro-foundation models can be built as specialized generative AI solutions to for domain-specific tasks, such as sustainability issues. They can decrease costs, capitalize on the opportunities of AI democratization, and preserve sovereignty of data.[4]

The context in which foundational models operate, and any relevant standardization practices, are also key. Topic domains (e.g., healthcare, finance, insurance) can provide insight to better understand and design models and datasets. Blockchain technology can be useful for applying metrics to these models (e.g., subject focused), or general adaptations for specific sectors (e.g., issues like data ownership, incentives for decentralized AI, etc.).

Blockchain can optimize foundation models

Blockchain technology can help optimize both existing foundation models and new models that being built. There are implications of the data sets on which the foundation models are trained. It is important to have previously trained data, from legitimate sources. Otherwise, if there are no checks and balances on open models, the data may include information from unwanted sources such as the leaked data or other data on the dark web, children's data, etc. Blockchain technology can also help reduce biases from pretraining models on concepts like gender, skin color, etc. The evolution of LLMs, for instance, this can have implications on the validity and ease of compromising data. Once models are trained, they cannot be untrained or "forget." Therefore, tainted models with unwanted data can become a major liability for any companies and organizations using them. This is especially concerning because we don't fully understand the third-party implications or risks that may come from their use.

Even though the intent of foundational models is automation, the quality, coherence, and relevance of the outputs generated by these models need to be assured. Blockchain can enable different parts of the process to be carried out with greater trust. This way, it is the entire process, more than just the outcome, that becomes validated (e.g., guaranteeing a smart contract has executed a process, or that other steps have been followed through).

Blockchain can benefit foundation models in the following ways:

1. Data Sourcing & Data Quality: Provenance of data, ensuring adequate data sourcing and quality, especially the quality of unlabeled data
2. Training: Recording approaches to processing data
3. Outputs artifacts: Monitoring and evaluating functions, results, and their implications
4. Inference: Recording how models are utilized to produce outputs
5. Incentivization: Providing a layer to compensate contributors providing data or compute resources that power the process supporting decentralized AI functions

Foundation Models as Digital Assets

The entirety of a foundation model, from input datasets to formation and output artifacts, can be recorded as a digital asset, such that the full process of carrying out any activity can be recorded on a blockchain. The evolution of LLMs, for instance, can have implications on the validity and ease of compromising data. With widespread deployments across multiple foundation models, there are constant updates on their capabilities, such that their features are always evolving. This makes strategic model performance benchmarking crucial, especially ensuring the benchmark is unknown to the model for the process to be effective.

From a governance perspective, timestamps can identify the latest version of the model or its underlying data, to maintain consistency of results. An earlier version of a model may not be aware of the latest relevant data, such that asking both an earlier version and the latest version of a foundation model to perform an activity may lead to different results. Blockchain enhances governance of data, AI projects, and processes. Digital assets linked to foundation models can be version governed across their full lifecycle.

Foundation models represented as digital assets can also be treated as assets of an entity and better protected or commercialized. For instance, investors with ethics-based frameworks may make more informed decisions when foundation models have the level of certifications and security mechanisms that blockchain technology can provide.

Importance of Standards

Standards point to metrics of reliability for inputs and outputs of AI models. Many sets of technical standards have been established by several bodies, which all demonstrate similar principles. Below are key considerations for standards, followed by actual developments toward AI standards:

Table 3: Considerations for AI Standards

Consideration	Importance
Privacy & Security	Priority issue for industry-specific use cases, such as financial services, where AI can draw insights from user activity. Data ownership is a key consideration, especially in the context of decentralized AI, and a potential need to clarify open access (e.g., licensing models like Creative Commons, IP implications, etc.).
Data Provenance	Specifying and vetting data sources, ensuring reliable data and quality data. This includes trustworthy data utilized by oracles or certified third party data sources. Data provenance should be aligned with data preferences (e.g., real vs. synthetic, 1st party vs. 3rd party, reliance on ground truth derived from lived human experience).
Unbiased	Ensuring adequate representation of relevant populations of users in training data
Transparency	Clear and available information on how data is used, explainability on what a model is and is not supposed to do, in a way that is understandable to humans, and adequately informing users on the reliance of AI for applications
Inclusion	Facilitating equal access to AI solutions, so as not to contribute to the digital divide
Ethical	Responsible AI uses to prevent harm, mindful of social impact (e.g., AI in the context of global migrations)
Aligned with Human Values	Human-centered AI developments, aligned with values to ensure human wellbeing and existence on earth
Accountability & Trust	It is important for AI solutions to function adequately and consistently. Good practices include: 1. Governance 2. Controls and tests 3. Human feedback in maintenance and reinforcement learning, to ensure realistic results 4. Validation of processes 5. Iterative learning and training, enhancing databases and knowledge base 6. Benchmarking best practices (e.g., ensuring benchmark is unknown to model to remain valid) 7. Retesting and maintenance 8. Monitoring and evaluation Countermeasures specific to: 9. Model drift, where models' performance may decline over time 10. Hallucinations, where algorithms may invent wrong results 11. Scalability challenges in the context of technical advances and considerations on their adequate use (e.g., data sharding or off-chain data storage solutions).
Human direction and feedback	AI should remain under human control
Risk Management Frameworks	Process-oriented and outcome-oriented risk assessment measures and mitigation, clarifying who is accountable when things go wrong

Table 4: Progress on Global AI Standards

Standards Body/ Entity	Standards & Principles Developments
International Organization for Standardization (ISO)	ISO/IEC 4200: AI management system standard, providing guidance for a methodical approach for businesses to balance innovation and governance while managing risks. This standard can help organizations address AI challenges such as performance evaluations and risk assessments, ethics, transparency, and continuous learning. ISO Technical Committees under ISO/IEC JTC 1/SC 42 convene several working groups in ongoing discussions on AI related topics.
European Committee for Standardization (CEN) & European Committee for Electrotechnical Standardization (CENELEC)	CEN-CLC/JTC 21: Technical committee analyzing existing standards for AI, with the objective to produce deliverables relevant for the European market and society, in conjunction with the EU's laws, policies, principles, and values.
Consumer Technology Association (CTA)	Several projects delivering AI standards focused on definitions and basic characteristics, security, and trustworthy AI systems.
IEEE	IEEE P7000: Runs multiple standards projects under the AI Standards Committee, focusing on technological and ethical considerations for AI development including governance, computational developments, machine learning, algorithms, and use of data. These projects are producing "ethical specifications" for AI.
International Telecommunication Union (ITU)	Several projects to discuss AI and its role to increase efficiencies for the realm of telecommunication and ICT systems, with a focus on sustainable development and AI for good.
National Institute on Standards and Technology (NIST)	NIST published A Plan for Global Engagement on AI Standards, under the NIST Trustworthy and Responsible AI (NIST AI 100-5) group, discussing priority topics and the need for standardization, in addition to a roadmap for an AI Risk Management Framework. It aligns AI standards initiatives with US regulatory developments and strategies, including the US Government National Standards Strategy for Critical and Emerging Technology.
European AI Office	General-Purpose AI Code of Practice: Providers of general-purpose AI models may rely on codes of practice to demonstrate compliance with EU AI Act obligations until harmonized standards are published.
United Nations	Several initiatives focusing on AI ethics, mainly the UN Principles for Ethical Use of AI in the UN System. The High-level Advisory Body on AI to the UN Secretary-General focuses on Governing AI for Humanity and related principles.
UN System Chief Executives Board for Coordination (UNCEB)	Several initiatives around governance, ethics, capacity building, policies, and uses across the UN system.
United Nations Economic Commission for Europe (UNECE)	Focus area on AI in the context of innovation, financing infrastructure, energy, smart cities, and trade – under the UNECE-hosted Centre for Trade Facilitation and Electronics Business (UN/CEFACT).
United Nations Educational, Scientific, and Cultural Organization (UNESCO)	AI Ethics hub, with focus areas including overall AI ethics, education, and inclusion. The group's Four Core Values include i) human rights and human dignity; ii) living in peaceful societies; iii) ensuring diversity and inclusiveness, and iv) environment and ecosystem flourishing. UNESCO also launched an open consultation on AI governance.

As companies and organizations work to adhere to best practices for AI, as outlined by the standards and considerations above, they can benefit from taking specific proactive measures to ensure compliance with relevant standards. Additionally, by strategically leveraging blockchain technology, they can enhance the trustworthiness and effectiveness of AI solutions. Below are some potential actions to consider:

1. **Data Validity Methodologies**: Approaches to ensure that data is valid and properly scored based on its quality or adequacy (e.g., drawing on multiple, unconnected data sources can increase confidence that data points are valid). This validation should occur before providing outputs that could have negative effects from inadequate data.
2. **Data Validity Practices**: Developing practices to assess the validity of data, such as a scoring system based on the percentage of ground truths of human experience incorporated into an AI model.
3. **Clarification of Unacceptable Data**: Establishing clear guidelines for when data is not allowed, and determining approaches to assess when data is not fit for its intended purpose.
4. **Data Suitability Understanding**: Businesses should be aware of both the potential and the limitations of data, especially when not all data is fit for its intended purpose.
5. **Data Sourcing and Validation Measures**: Defining measures for sourcing and validating data, processes, and outcomes throughout the entire lifecycle of AI.
6. **AI Ethics Impact Assessment**: Conducting AI Ethics Impact Assessments and reviews throughout the lifecycle of AI models—from design, through usage, to retirement.
7. **Blockchain Metrics**: Defining appropriate metrics for the use of blockchain technology, including smart contracts, in AI applications.
8. **Governance of Decentralized AI**: Developing adequate practices for decentralized AI systems to ensure proper governance, consensus, and balance of power.
9. **Responding to Deepfakes and False Media**: Establishing swift and effective measures to detect and respond to deepfakes and false media content.
10. **Addressing Inadequate Data**: Creating mechanisms to stop the use of AI algorithms that rely on inadequate data, or, if possible, quarantining or destroying such algorithms.
11. **Transparency Levels**: Determining the appropriate level of transparency in AI systems, including how and when to disclose data and decision-making processes.
12. **AI Governance Principles**: Defining principles and strategies for AI governance (e.g., having AI experts at the executive level, addressing personalization and localization concerns, and ensuring data science skills among business leaders and decision makers).
13. **Alignment with Human Values**: Establishing an approach to ensure that AI systems align with fundamental human values, such as fairness, privacy, and equity.
14. **Reinventing Processes for Equality**: Designing processes to preserve equality and optimize both human and machine capabilities, ensuring that AI is a force for positive change.
15. **Mitigating the Digital Divide**: Implementing measures to detect and mitigate factors that could widen the digital divide or cause social isolation.
16. **Developing Digital Skills Equitably**: Promoting the equitable development of human capacities for the digital age, alongside investments in basic digital infrastructure to ensure last-mile access.
17. **Adapting AI Models to Local Contexts**: Ensuring AI models are adapted to local norms, practices, and cultural nuances in the contexts in which they will be deployed.
18. **Contextualizing Datasets**: Developing measures to clarify the relevance of datasets based on context (e.g., jurisdictional issues for legal datasets, ESG datasets for sustainability applications). Ensuring datasets used in large LLMs are consistent and up-to-date to avoid conflicts that could lead to confusion or misinterpretation.

19. **Contributing Data in Decentralized AI**: Establishing guidelines for contributing data within decentralized AI models, ensuring fairness and accuracy.
20. **Monitoring Ethical Adherence**: As companies and organizations implement ethical AI practices, defining key performance indicators (KPIs) to monitor adherence to ethical principles and establishing clear methods for measuring these KPIs.
21. **Optimizing Blockchain for AI Trust**: Identifying the optimal timeframe and approach for integrating blockchain technology into AI projects to enhance transparency, security, and trust.

AI REGULATION

While regulatory developments specific to AI today are in early stages, it's imperative to shape the norm of doing things right. AI is becoming front and center in international convenings, including G7 and G20 Summits, and other regional convenings globally. There is ample consensus that regulation needs to be speedy and flexible, given the pace and nature of technological change. Regulation also needs global alignment to minimize regulatory arbitrage, and regulation must aligne with human values of wellbeing. Regulatory approaches around the world range from horizontal regulation, applicable to all AI developments, or vertical regulation, applicable to specific applications or sectors. Horizontal regulations often come from central governments and are at this point in earlier stages of development.

Certain jurisdictions have set a precedent in their progress toward regulatory frameworks that have influenced other jurisdictions. This can contribute to harmonization of rules. There is optimism that the US and EU approaches, as major jurisdictions, are evolving toward increasing regulatory alignment. There are also trends toward regional harmonization, as in the African Union case, or the Latin American case which largely follows the EU model.

Jurisdictions with more flexible and clear regulations are expected to attract innovations. As regulatory developments for AI continue to take shape, and as AI solutions continue to converge with blockchain capabilities with the intent of responsible and more effective AI, innovators will need to adhere to requirements for AI in the context of other regulations, including those focused on blockchain and digital assets that are also developing in parallel and are generally at more advanced stages globally relative to AI regulations. GBBC has an i**nteractive regulatory map of such regulatory developments for blockchain and digital https://gbbcouncil.org/gsmi/assets**.

Table 4: Regulatory Developments in Selected Jurisdictions

Country/ Region	Regulatory Focus	Status
Africa: The development and regulation of Artificial Intelligence (AI) in Africa are primarily guided by the African Union ("AU") and the African Union Development Agency ("AUDA"), which together represent 55 member states. The general consensus is that AI regulations in Africa are adopting a horizontal approach, similar to the European Union's GDPR. Key AI-related issues in Africa include data privacy breaches, algorithmic bias, and a lack of cybersecurity measures. In response, African nations are developing AI policies that prioritize ethical guidelines, data protection regulations, and capacity-building initiatives to address these challenges.		
On February 29, 2024, AUDA published a draft policy ("the AU Draft Policy") outlining a framework for AI regulation by member states. This framework provides recommendations for the standards and practices for building, testing, and benchmarking AI systems. It also suggests the establishment of regulatory oversight bodies within the framework. On August 9, 2024, the African Union Executive Council published the Continental AI Strategy. The strategy advocates for a more unified national approach across the public and private sectors of AU member states to navigate the evolving AI landscape, while also strengthening regional and global cooperation. Its goal is to position Africa as a leader in inclusive and responsible AI development. The Continental AI Strategy categorizes AI-related risks into the following four areas: **1. Environmental risks** **2. System-level risks** (e.g., bias, privacy, and personal data protection) **3. Structural risks** (e.g., gender equality, job displacement, the AI divide, and more) **4. Risks to African values** (e.g., the spread and manipulation of AI-generated misinformation, disinformation, and hate speech; subversion of Indigenous Knowledge and African cultural heritage; and more) Although it is somewhat challenging to determine the exact level of acceptance of the AU Draft Policy and the Continental AI Strategy, the alignment of national AI strategies with these policy documents is promising. It suggests the potential for a more unified approach to AI policy development across the continent. Status: Regional AI Strategy in place, Pending regulatory developments		
Mauritius	Mauritius was the first to lead the way in Africa on AI with the publication of the Mauritius Artificial Intelligence Strategy in 2018.	AI Strategy in place, Pending regulatory developments
Kenya	by Kenya's Distributed Ledgers Technology and AI Task Force Report was published in 2018.The country's existing National ICT Policy also acknowledges the need to pay attention to current trends in big data, AI, and machine learning as emerging technologies. The Kenya National Digital Master Plan 2022-2032 also calls for a National AI Strategic Plan to be devised.	AI Strategy in place, Pending regulatory developments
Egypt	National Egyptian AI Strategy developed by the Egyptian National Council for Artificial Intelligence (NCAI)	AI Strategy in place, Pending regulatory developments
South Africa	Draft National AI Plan including AI policy plan released in April 2024.	AI Strategy in place, Pending regulatory developments

Nigeria	National AI Strategy released in August 2024	AI Strategy in place, Pending regulatory developments
Asia-Pacific: Rapid regulatory developments in the region, with AI guidance and regulations, with regulators and policymakers revising existing frameworks to evaluate their relevance to AI-related risks, or proposing new rules. Priorities center on promoting AI uses and developments. Certain jurisdictions like China, South Korea, and Taiwan are taking steps toward AI-specific regulations, which are mostly in early stages. Other jurisdictions like Australia, Japan, Singapore, India, Hong Kong, Thailand and Vietnam are taking steps toward non-binding high-level principles and guidelines. **Status:** Regulatory developments underway at different stages in different countries.		
China	China has been the most active jurisdiction shaping new rules on AI, with a multifaceted approach that includes AI regulations, national standard, and guidance. They country's approach to regulating AI is characterized by a delicate balance between fostering technological innovation and ensuring societal oversight, security, and privacy. Key principles guiding these regulations include data protection, algorithm transparency, content control, security, and social stability. Specific areas targeted by Chinese regulations include recommendation algorithms, deep synthesis technology, generative AI, and broader cybersecurity concerns. For instance, the Administrative Provisions on Recommendation Algorithms in Internet-based Information Services (2022) mandates platforms to disclose their algorithm principles and prohibits the spread of harmful content. The Administrative Measures on Deep Synthesis in Internet-based Information Services (2023) regulates deepfakes, requiring labeling of generated content and prohibiting their use for illegal activities. The Interim Measures on the Administration of Generative Artificial Intelligence Services (2023) sets guidelines for generative AI, focusing on cybersecurity, data privacy, and content control. China's broader Cybersecurity Law (2017) also applies to AI, requiring data localization, imposing cybersecurity obligations, and providing for government oversight. Further details on the regulations (elements, implementation, and enforcement include): 1. Administrative Provisions on Recommendation Algorithms (2022) This regulation aims to ensure transparency, accountability, and user control in the use of recommendation algorithms. Platforms are required to disclose the principles and logic behind their algorithms, preventing them from spreading harmful, false, or discriminatory content. Additionally, users must be provided with options to customize or opt out of algorithm-based recommendations. The government has implemented enforcement mechanisms to monitor compliance and impose penalties on non-compliant platforms, while industry associations have developed guidelines and best practices for algorithm transparency and user protection. 2. Administrative Measures on Deep Synthesis (2023) This regulation seeks to address the challenges posed by deepfakes and other forms of manipulated content. It requires deep synthesis service providers to label generated content and prohibits their use for illegal activities, such as defamation or fraud. The government has invested in research and development of deepfake detection technologies and has collaborated with international organizations to address the global challenge of deepfakes. Enforcement measures include fines, suspension of services, and criminal prosecution for violations.	Existing regulations in place, in addition to national standards and guidance. Iterations and further developments in progress.

	3. Interim Measures on the Administration of Generative Artificial Intelligence Services (2023) This regulation establishes guidelines for the development and use of generative AI, focusing on ethical considerations, data privacy, and content control. Generative AI services must comply with cybersecurity and data privacy laws, avoid generating harmful content, and disclose information about their training data and algorithms. The government has been working with industry stakeholders to develop guidelines and best practices for the responsible use of generative AI. Enforcement measures include fines, suspension of services, and criminal prosecution for violations. 4. Cybersecurity Law (2017) This broader cybersecurity law applies to AI and other technologies. It requires data localization, imposes cybersecurity obligations on network operators, and provides for government oversight. The government has been actively enforcing the Cybersecurity Law, conducting inspections and imposing penalties on non-compliant entities. Additionally, the government has been working to raise awareness of cybersecurity risks and promote best practices among businesses and individuals.	
Singapore	Singapore introduced the National AI Strategy (NAIS) 1.0 in 2019 and, in December 2023, released an updated version (NAIS 2.0) developed through collaboration with various stakeholders. Singapore is taking a sectoral approach, with individual ministries, authorities, and commissions publishing guidelines and regulations. The NAIS 1.0 framework primarily aimed at expanding the AI ecosystem and developing National AI projects. In contrast, NAIS 2.0 takes a more comprehensive approach, moving away from the 1.0 focus on flagship projects to a broader system approach. This shift reflects Singapore's ambition to establish itself as a leading AI world power, with excellence and empowerment as its primary goals. NAIS 2.0 identifies and details: The NAIS 2.0 outlines (i) 15 key actions distributed across three systems: Activities Drivers, Communities, and People and Infrastructure. These actions form the backbone of the strategy, guiding Singapore's AI development and regulation efforts. (ii) The strategy also identifies 10 enablers, such as industry, research, infrastructure, talent, the regulatory environment, and international partnerships. These enablers are crucial in fostering a conducive environment for AI development and ensuring the strategy's success. (iii) Building capabilities in data services and Privacy-Enhancing Technologies (PETs). The strategy proactively identifies and details the potential risks associated with AI, spanning concerns around model quality and fair use to fears around the loss of control and existential risks of AI models (NAIS 2023, pp. 54-55). Mitigation strategies: (i) engaging with all perspectives. (ii) enhance our understanding of the risk landscape. (iii) ensure that AI systems are well-developed, reliable, and resilient (ensure the model development process is unbiased, accurate, and aligned to human values). (iv) preventing AI models from being used maliciously and securing them against adversarial attacks. (v) Benchmarks and testing. (vi) Ensuring development of regulatory framework, guidelines, and continuously updated laws.	AI Strategy in place, Pending regulatory developments

Taiwan	Taiwan's emerging AI regulatory environment is shaped by a strategic focus on leveraging its robust hardware industry to bolster growth in high-value AI applications. This effort is encapsulated within the framework of the "Five Trusted Industry Sectors," which includes AI, semiconductors, and next-generation communications, aimed at fortifying Taiwan's role in global supply chains and aligning with democratic partners. The draft AI Basic Act, introduced to guide the development, application, and regulation of AI technologies, emphasizes principles like sustainable development, data governance, transparency, fairness, and accountability. The act aligns with international standards seen in the U.S., EU, and Singapore, advocating for a balanced approach that fosters innovation while ensuring safety and fairness. The draft proposes a risk-based regulatory framework similar to the EU AI Act, categorizing AI applications by risk levels and promoting innovation through mechanisms like regulatory sandboxes. Additionally, it seeks to establish accountability mechanisms, including certification, testing, and requirements for foreign AI products entering the Taiwanese market. Potential content regulations focus on preventing harms like bias, discrimination, and misleading information from AI applications, suggesting that further laws might be introduced to mitigate risks associated with machine-generated content. The act also emphasizes data protection through "data protection by design and by default," which could shape future amendments to Taiwan's Personal Data Protection Act (PDPA). Moreover, it stresses the importance of intellectual property rights in AI training data usage, echoing positions held by the U.S. on copyright considerations. While the draft's open comment period concluded on September 15, 2024, it remains in the legislative process. The government's efforts reflect a desire to align with global standards while tailoring regulations to Taiwan's unique needs, balancing innovation and regulation. This regulatory framework aims to support AI developers and users while addressing issues like liability, insurance, and the workforce impacts of AI deployment. The legislation also addresses emerging challenges, such as those posed by deepfake technology and AI-generated content, suggesting a proactive approach to mitigating potential risks. Overall, Taiwan's AI regulatory strategy seeks to position the country as a leader in AI technology while maintaining safety, fairness, and international collaboration.	Draft AI Act released, Regulatory developments in discussions

European Union: European Union: The EU AI Act, the world's first law focused on artificial intelligence, is part of a wider package of policy measures that including the AI Innovation Package and the Coordinated Plan on AI. The act establishes a comprehensive legal framework with the objective of ensuring safety and fundamental rights to individuals and businesses with respect to AI.

The EU AI Act establishes a risk-based approach where AI applications are assigned to three categories: Minimal risk, High risk, and Unacceptable risk. Activities with minimal/no risk are generally permitted with no restrictions, and activities with generally minimal "transparency risk" are permitted but subject to transparency/information obligations. Activities with "high risk" are permitted subject to compliance with AI requirements and other assessments (e.g., medical software run by AI), and activities with "unacceptable risk" are prohibited. The latter would be considered banned applications of AI, such as social scoring systems run by government. In addition, the EU AI Act requires clear and transparent disclosures to users of chatbots and other automated systems that their interaction is with a machine.

Developers and deployers of AI are subject to specific obligations and requirements that include:

i) Ensuring compliance with regulations and being prepared to demonstrate such compliance as requested
ii) Compliance with restrictions on the basis of high-risk AI activities
iii) Relevant conformity assessments
iv) Maintenance of adequate logs and documentation
v) Registration with EU wide centralized database

Non-compliance with the EU AI Act could represent fines of up to 7% of global annual turnover of companies.

While the EU AI Act came into force on August 1, 2024, most of the provisions will take more time to be enforced, and full enforcement is expected to take place on August 1, 2027.

Status:
Regional AI law in force, pending full enforcement of provisions

Latin America: Several countries are developing different legislative projects to regulate AI, where most are influenced by the European Union's approach. However, the initiatives are at different stages and lack clear regional coordination, which creates additional challenges for coherent and effective regulation.

Status:
Regulatory developments in discussions at different stages across different countries

Argentina	The proposals seek to establish a legal framework for the ethical use of AI, guaranteeing the protection of human rights, privacy and security, in addition to promoting innovation and international cooperation. Several initiatives have been presented in 2023, but none have yet been discussed in Congress.	Regulatory developments in discussions
Brazil	The laws focus on establishing ethical principles and guidelines for inclusion, sustainability, privacy protection, and transparency. In addition, they seek to promote public-private collaboration in research and development to make the country competitive. Brazil is the Latin American country with the most legislative projects on AI, being debated in the Senate and in the Temporary Commission on AI (CTIA).	Regulatory developments in discussions
Chile	Chile has legislative projects in progress. Proposals include amending the Penal Code to penalize the use of generative AI in telephone fraud or violation of sexual privacy.	Regulatory developments in discussions
Colombia	Regulation is sought to oversee the development of AI and mitigate associated risks. A proposal is underway to create a regulatory authority specialized in AI.	Regulatory developments in discussions
Peru	Peru is the first country in Latin America with an approved law on AI (Law No. 31814 in 2023). The AI law promotes the ethical, transparent and responsible use of AI, with risk-based safety standards	AI Law approved
Uruguay	Participatory process and creation of national strategies for the responsible use of AI, with an emphasis on ethics and responsibility. Uruguay is making progress in AI governance with the adherence to the UNESCO Recommendation on the Ethics of AI in 2023	Regulatory developments in discussions
Mexico	Mexico has a number of legislative proposals on AI. The country is seeking to modify the Penal Code to sanction the misuse of AI in the violation of sexual privacy	Regulatory developments in discussions

United States & Canada: Currently there is no comprehensive AI regulatory framework in either the United States or Canada. There are a number of bills in discussion, and regulators are increasingly acknowledging the importance of sensible regulations for this technology.

Status: Regulatory developments in discussions

Canada	Canada has made relatively slow progress toward reaching an agreement on an AI regulatory framework. Bill C-26 — the Critical Cyber Systems Protection Act — is currently at its third reading and is progressing slowly. Canada is also four years into its efforts to modernize its data privacy regime with Bill C-27, the Digital Charter Implementation Act. However, there is growing doubt that the proposal will pass before the next federal election, expected in October 2025.	Regulatory developments in discussions

	The Standing Committee is continuing a clause-by-clause review of Bill C-27, with a long list of amendments still to be considered. This includes the Artificial Intelligence and Data Act (AIDA), which is unlikely to come into force before 2025. While major tech companies have expressed support for the objectives of Bill C-27, AIDA still requires further work. There is a growing consensus to remove AIDA from Bill C-27, in order to establish clear rules that will enable businesses to confidently deliver AI products and services. The goal is to expedite the creation of a legal framework that fosters responsible AI development. Canada is also continuing efforts to modernize the Personal Information Protection and Electronic Documents Act (PIPEDA), which forms part of the broader effort to pass Bill C-27. This underscores the urgent need to update privacy laws and establish a regulatory framework for responsible AI development in Canada. One of the most significant unresolved issues is how to regulate open-source AI. Many of the proposed regulations are challenging to implement, both from a technical and a political standpoint.	
United States	The US approach to AI regulation is sector dependent and rules-based, with no statutes and a state-by-state approach. At a US-wide level, there is an increasing federal focus on AI, with significant expected developments for 2025. The only legislation in place is at a state level,[5] with New York, California, and Wyoming having established very specific rules. California has had significant activity around the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act (SB 1047). It is complex to define the concept of "trustworthy AI" which much of the US rhetoric refers to. This concept raises questions like "is it about the inputs, outputs, or transparency of the model?," or "what features does it specify?" Therefore, it can be challenging in codifying anything values based, just like it can be difficult to keep up with a moving target give the rapid developments in the space. There has been a reliance on case law, often from decades prior, in relation to AI issues. This may still work if the concepts are the same. For instance, companies may be sued for wiretapping when chatbots record user information to optimize their algorithms without informing users. Case law in relation to AI at this point has relied on the Fair Use Doctrine as a backstop, allowing the use of copyrighted materials in certain circumstances without permission. At a federal level, the comprehensive US Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence was released after years of hearings and focused conversations on AI, setting a clear direction toward AI-specific regulatory developments. It establishes a government-wide approach toward responsible AI development and deployment. It set in motion over 100 deliverables and catalyzed activity across US agencies, calling for increased coordination among them. It acknowledges the need to complement efforts and better understand AI before moving more aggressively forward with regulatory developments. The Executive Order recognizes the rapid pace of technological developments and the need to act. Once the expected deliverables are finalized, legislative activity is expected in the following session alongside continued hearings. Congress is expected to take action, as it has been ramping up engagement in a bipartisan way with government actors and stakeholders in the space. There is still a perception of a knowledge gap as a barrier that needs to be addressed, which is more generational than partisan. Key takeaways from Congress's conversations with the AI industry thus far include the	Regulatory developments in progress

	importance of preserving the decentralized nature of AI, addressing concerns over concentrations of power, single points of vulnerability, and security. The Congressional AI Caucus, with the objective of educating policymakers on the economic, technological, and social impacts of AI and supporting innovations that benefit Americans, is expected to ramp up its activities in 2025. The US has also released an AI mandate for federal agencies issued in March 2024, in the form of guidance issued by the Office of Management and Budget (OMB) to advance responsible acquisition of AI at a government level (OMB M-24-10). This is the first set of government-wide binding requirements for US agencies to implement measures for risk management, governance, and innovation in their acquisition and use of AI. The National Science Foundation (NSF) has also set measures to support AI developments and risk assessments, under the concept of trustworthy AI. There have also been multiple recent amendments to multiple US AI bills, including the Future of Artificial Intelligence Innovation Act of 2024, the AI Advancement and Reliability Act, the GUIDE AI Act. Overall, the US is moving toward a regulatory regime that focuses on innovation and extracting value for individuals, while ensuring consumer protections. Key issues include lessons learned from early Internet developments, in support of open systems as opposed to closed systems, which points to decentralized AI models. This implies open access and use, as well as agency over one's data. There is support for democratized access, affording opportunities at a greater bandwidth.	

United Kingdom: The UK has established guidelines on AI, with a policy aimed at fostering innovation while ensuring responsible governance. This approach is part of a broader, outcome-focused strategy underpinned by two key principles: adaptivity and autonomy. The strategy is primarily built on the National AI Strategy (2021), a 10-year plan designed to support the transition to an AI-enabled economy. It aims to ensure that AI benefits all sectors and regions, aligns with the UK government's objectives of fostering innovation, and safeguards core values while protecting the public through progressive initiatives.

This led to the development of the Pro-Innovation Regulatory Approach (2023), which is guided by five key principles:

1. Safety, Security, and Robustness
2. Transparency and Explainability
3. Fairness
4. Accountability and Governance
5. Mechanisms for Contestability and Redress

The approach, led by the Department for Science, Innovation, and Technology (DSIT), largely reflects the original proposals and supports practices that can foster safe, ethical AI development across various sectors. It positions the UK as a global leader in artificial intelligence, focusing on promoting innovation, regulating AI responsibly, and encouraging international cooperation for sharing information, ensuring interoperability, and advancing governance.

The policy framework also prioritizes the safe, ethical deployment of AI for the benefit of society. It establishes ethical guidelines through organizations such as the Centre for Data Ethics and Innovation (CDEI) and the Office for AI, which collaborates with the Office for Science and Technology Strategy (OSTS) to explore how AI can contribute to the UK government's strategic goals, while ensuring that AI aligns with core values such as privacy, fairness, and inclusivity.

While AI offers significant benefits, a key challenge for the Labour government will be addressing public concerns, particularly around regulating AI companies and AI-generated content. Unlike the previous Conservative administration, which somewhat delayed regulation to protect innovation and avoid stagnation, Labour has signaled a more proactive approach. In its manifesto, the Labour Party committed to introducing binding regulations for companies developing the most powerful AI models, reflecting a stronger focus on managing AI risks and ensuring alignment with the government's strategic objectives.

Further support for this strategic alignment comes from the AI Foundation Model Taskforce (2023), which focuses on advancing foundational AI models, such as large language models, and developing safe, reliable AI tools for commercial use. This will enhance the UK's position in the global AI landscape.

Status: Guidelines, policy, and national strategy in place, with regulatory developments underway

FUTURE OUTLOOK

Businesses and organizations are increasingly incorporating AI into their operations and cultures to remain competitive and relevant in the future. While AI will not replace humans, it is expected that human activities using AI will outperform those that do not adopt the technology. Human intervention and input remain essential in ensuring that AI is used effectively.

International and cross-stakeholder cooperation is crucial to ensure that AI benefits humanity in safe, inclusive, and ethical ways. Standards, best practices, and regulations are important steps toward achieving the global coordination needed to deploy AI at scale responsibly. Both guardrails to address risks and incentives to promote the growth of responsible AI models are essential. The role of blockchain technology is becoming increasingly central in advancing trusted AI solutions, especially with the growing emphasis on decentralized AI. In all cases, it is imperative for stakeholders to consider, in addition to AI outcomes and outputs, the broader implications of the technology on human lives.

It is therefore important to think beyond immediate use cases and production goals and address more strategic issues:

- What broader problem is AI solving?
- What are the outcomes of AI, and how do they impact humans?
- What incentives should be used to create responsible AI models?
- What controls and tests are essential?
- How do we address unintended consequences, such as inaccurate conclusions, hallucinations, or other erroneous facts that algorithms may "make up" due to their lack of lived human experience and emotion?

Moreover, while AI innovations continue to develop at a rapid pace, and regulatory frameworks and standards are being established to ensure trust, several open questions remain:

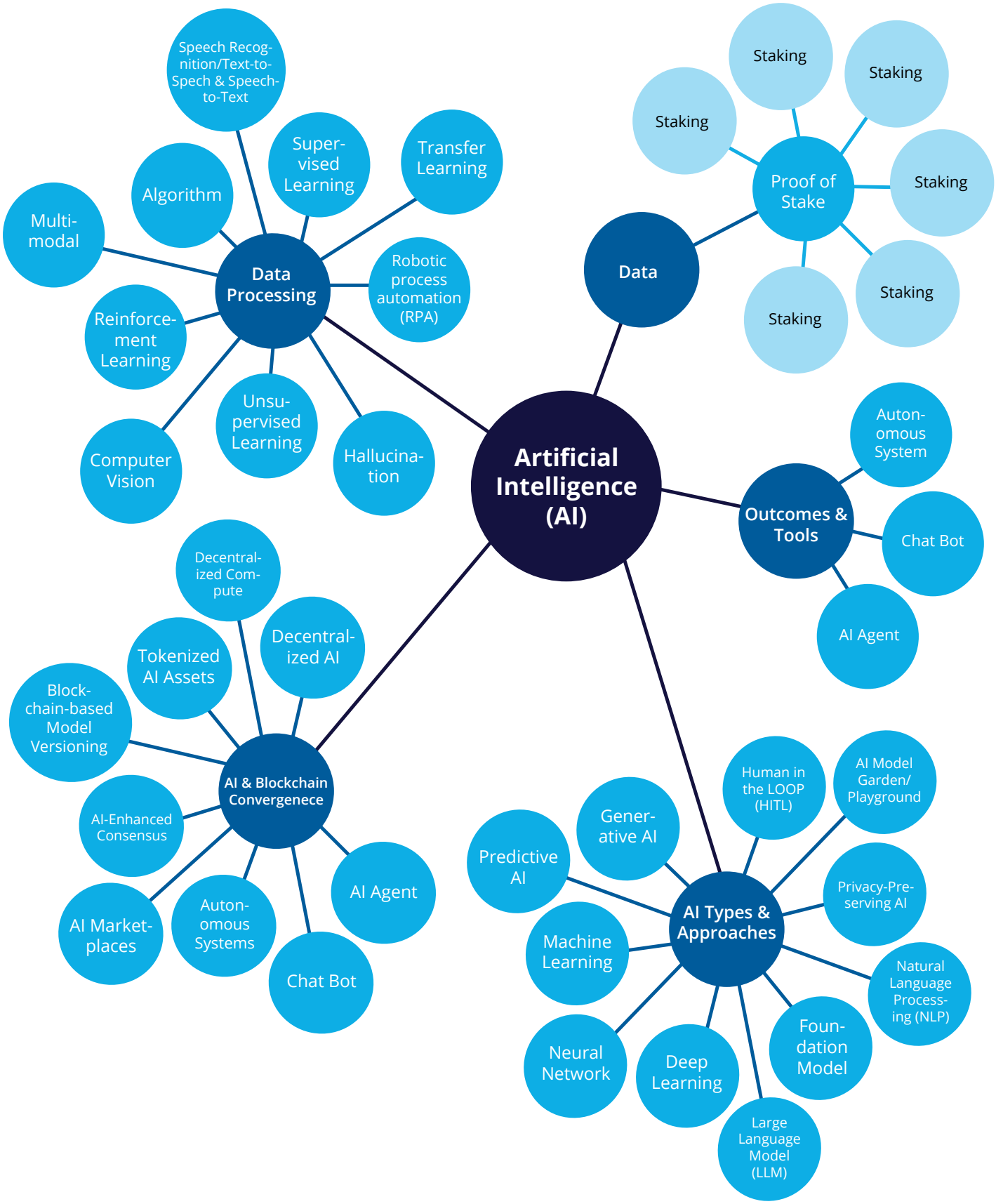
1. **Backward vs. Forward Looking AI:** When data is generated after events and circumstances have occurred, as is often the case, AI can become more backward-looking than forward-looking. How can we ensure that AI training is designed to anticipate future outcomes rather than merely reflecting past data?
2. **Incentive Structures and Data Attribution:** How should incentive structures and payment models be tailored to encourage individuals and entities to contribute data? Additionally, how should entities handle the attribution of data?
3. **Intellectual Property and Data Security:** Where should the line be drawn between intellectual property rights for data and the need for creative freedom to allow innovative solutions? How should this be managed in cases where users do not give explicit consent to have their data recorded or used (e.g., AI notetakers for virtual calls, chatbots, etc.)?
4. **Regulating Unsecured AI:** How should unsecured AI systems, in particular, be regulated to mitigate risks?
5. **Cross-Jurisdictional Regulation:** What regulatory framework should apply when different parties are in different jurisdictions, particularly when AI systems span multiple regions with varying legal requirements?

Looking ahead, responsible AI must be deeply connected with human input and insight. It is crucial that humans remain in control, not just as a "human in the loop" in part of the process, but throughout the entire lifecycle of AI—from design and training data to algorithms and final interpretation. Fortunately, current AI auditing practices, often based on if/then logic, are largely in line with existing relevant regulations.

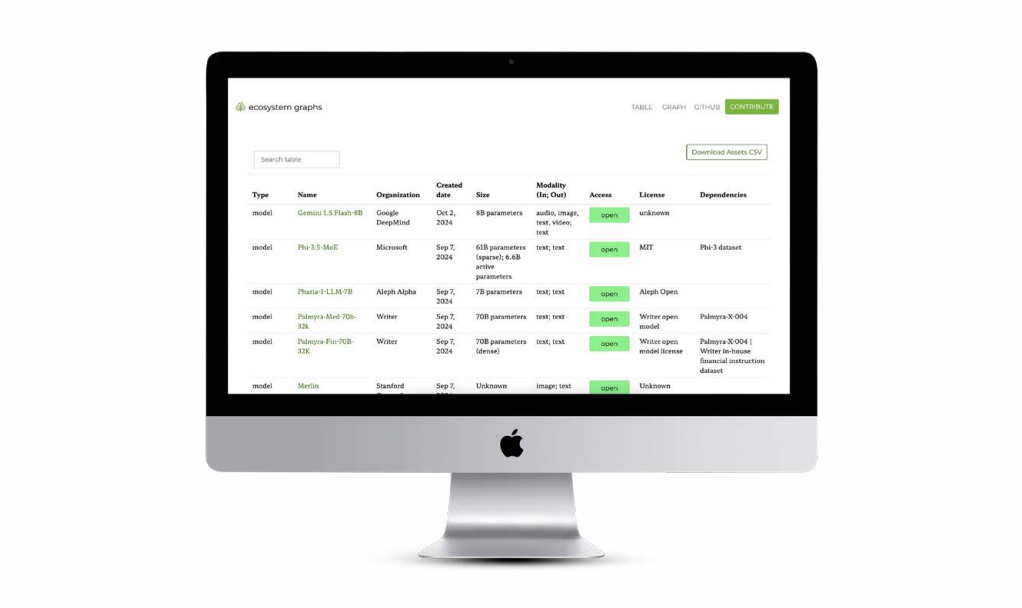
In the realm of AI, errors often arise from misinterpretations or conclusions drawn out of context. Only humans possess lived experiences—rich, subjective insights that serve as the ground truth for AI models. By digitizing our physical and lived experiences, we can provide AI with reliable data to stay on course. Data that is interpreted by third parties, derivative data, synthetic data, and some types of metadata are more distanced from the original source and are more likely to misrepresent the truth.

Thus, in a world increasingly dominated by AI, humans as "data laborers" will play a critical role in providing the human-grounded truths that enable AI models to course-correct, ensure accuracy, and remain relevant. Ultimately, knowledge is power, and blockchain technology can provide a layer of verified knowledge that is a game-changer for trustworthy AI. Audit trails for verified information will serve as a key risk mitigation measure. If the global community continues to take AI risk mitigation seriously—drawing lessons from the early days of the internet—we can pave the way for the next wave of innovation that benefits humanity.

Annex 1: Taxonomy of AI terms (builds on GSMI 4.0)



Annex 2: Landscape of Foundation Models: https://crfm.stanford.edu/ecosystem-graphs/index.html?mode=table



Annex 3: Considerations for a Risk Assessment Approach Model

Status of Concern	Categorize as “no issues”, “low issues” or “high issues”
Code	Assign code for monitoring purposes
Risk	Name risk
Methodologies to Identify/Assess risk	Define what actions must be taken to properly detect, assess, and mitigate risk
Control Activity	What has to be done to mitigate risk
Who Performs the Control?	Assign staff involved in risk mitigation and their roles
Control Frequency	Establish periodic reviews (e.g., daily, weekly, monthly, quarterly)
Format to Perform Control	Define approach (automated, manual, assessment, multiple appraoches)
Preventive or Detective	Identify relevant policies/regulations in relevant jurisdictions and their requirements
Directionality	Conclusions of the assessment: Identification and evaluation of risk, and implications
Mitigation Measures Taken	Identify actions taken to mitigate risk, and any remaining measures to be taken

SECTION VIII

DECENTRALIZED FINANCE (DEFI): OPPORTUNITIES, RISK CONSIDERATIONS, AND KEY PRINCIPLES FOR GROWTH

INTRODUCTION

Decentralized Finance (DeFi) is a new trend in commerce that has emerged from the onset and maturation of decentralized networks and blockchain technology. At first DeFi focused on ways to leverage blockchain's programmability, autonomously functioning code to :decentralize" financial activities. This initial foray into traditional finance sought to disrupt and replace the institutions that have traditionally been integral to financial services. As the rise of tokenization expands to encompass various asset types, DeFi has travelled beyond its financial roots, paving the way for innovation across a broad range of financial and commercial markets. This shift brings exciting possibilities, such as enhanced liquidity, broader access to global markets, and entirely new forms of value exchange. However, it also introduces challenges, including regulatory uncertainties, risks of technical vulnerabilities, and the potential for market manipulation.

What exactly defines this new trend, and how might its opportunities and risks shape the future of finance and commerce?

This paper explores the meaning of DeFi, and presents a taxonomy of DeFi concepts, as well as a set of common principles and standards to address the novel issues that DeFi presents. Based on those principles, the paper then proposes a mapping of potential risks and mitigation measures for different types of participants in the DeFi space, followed by a regulatory commentary to identify gaps where there may be no principles or regulatory clarity to address issues of concern that DeFi may raise. Throughout the paper, we identify several common misconceptions about DeFi, and attempt to dispel them with simplified explanations that provide context and clarity.

This paper also seeks to identify what matters most to DeFi protocols for their activities to be legitimized and scale, while recognizing the frenetic pace of DeFi developments. It raises open questions, and provides recommendations for considering the future of DeFi, which forms an approach toward a DeFi playbook.

The reader is encouraged to keep in mind several core themes while reading this paper

First, decentralized blockchain networks arguably remove the need for intermediaries, but that does not mean that intermediaries cannot participate nor does it mean that intermediaries may not eventually become a necessary or practical part of DeFi in the future.

Second, DeFi protocols that utilize decentralized blockchains are automatically global, which means that by design anyone with an internet-connected device can participate. This global access and participation greatly expands the size of the markets but also means that local laws and regulations might be overlooked, or worse, that conflicts between different sovereign laws, standards, and expectations will likely increase.

Third, with fewer or no intermediaries, decentralized blockchains and associated protocols rely heavily and sometimes exclusively on infrastructure (software, hardware, and communication). In traditional markets, both financial services and broader commerce, such infrastructure has not typically been subject to much, if any regulation. Drives to change this paradigm just because transactions in assets happen on or through this infrastructure will often involve a fundamental rethinking of long-held legal and regulatory concepts.

Fourth, in a world built entirely on software, the code becomes of paramount importance because it functions autonomously such that it cannot be stopped or the results of its execution changed. This is not necessarily an argument to regulate the development and deployment of software, but it points to the difficulties associated with determining how to regulate DeFi and reminds us that software suffers from imperfections. Creating incentives to encourage people to code and test carefully and thoroughly, and to solve these imperfections, seem worthy goals.

DEFI OVERVIEW

The DeFi movement often points to a new paradigm for financial services, which can be automated and recorded on a decentralized blockchain. It results from the use of software and emerging technology to facilitate direct, point-to-point value exchange between counterparties, and removal of third party intermediaries. Composable financial services can be carried out through automated transactions enabled by smart contracts that use digital assets including stablecoins as the form of currency.

It is not clear that a universally adopted definition of "DEFi" exists yet. While definitions and common understanding are still evolving, the industry has made progress toward a functional meaning of DeFi.

Let's start with the foundations in the very name:

- **Decentralized:** no single point of failure, no single source of truth, no single authority capable of or responsible for making changes to data
    - This is a natural continuation of trends towards greater automation, leveraging developments in computing, the internet, and global connectivity
- **Finance:** traditional financial services activities such as trading, lending, deposit-taking, custody but with tokenized assets

DeFi does not exclusively involve financial instruments because any asset or bundle of rights can be tokenized and subjected to the functionality of a traditional financial instrument or transaction.

...which lead us to a starting DeFi-nition:

Take traditional financial services activities such as trading and lending, distill them into their component rules and processes, and convert them into self-executing code on decentralized

networks accessible to anyone with an internet-connected device such that any tokenized asset can be utilized on them.

Layering on, "DeFi commonly refers to the provision of financial products, services, activities, and arrangements that use distributed ledger technology (DLT), including self-executing code referred to as smart contracts DeFi aims to operate in a disintermediated and decentralized manner, eliminating some traditional financial intermediaries and centralized institutions, and enabling certain direct investment activities."[1] (IOSCO)

Misconception 1: "DeFi is the opposite of TradFi (Traditional Finance)"

Reality: Rather than attempting to do away with TradFi, DeFi signifies a move towards straight-through processing and universal access to markets with enhanced efficiency and inclusivity, including the ability to subject non-financial assets to those markets. While DeFi arose outside of TradFi and proposes alternative ways to solve problems, including some of the longstanding problems and risk associated with intermediaries (such as counterparty risk), its aim is to make marketplace processes as simple as possible by automating them and removing the need for intermediaries. DeFi also enables integration with TradFi using features like smart contracts, tokenization, and decentralized lending features. DeFi does not remove third parties altogether but allows them access through smart contract integrations. In many cases there can be an integration with an existing centralized TradFi player. For instance, as banks are integrated with a central stock exchange and need its approval to allow trading in traditional assets, they would need to follow a similar process to allow clients who choose to use them to access new protocols. Similarly, for DeFi protocols to integrate tokenized versions of traditional assets, there would need to be at least some integration with traditional players and central exchanges. With tokenization presenting opportunities for markets and liquidity, from event tickets and art to private credit, intellectual property and beyond, innovative business models will have to adapt to these changes.

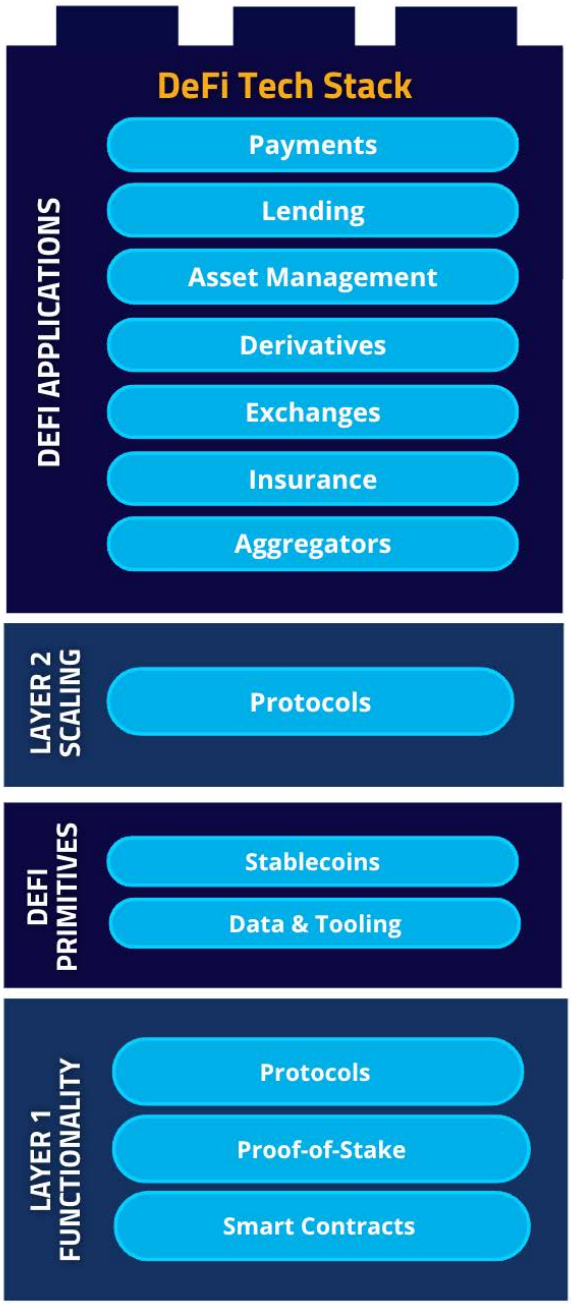
How does this work?

DeFi essentially takes the concept of a traditional financial services activity, such as exchange trading or lending, and breaks it down into basic components. It then recreates that activity in a way that shifts several core traditional functions from centralized market intermediaries to allow individual participants to conduct the activity on their own, on a peer-to-peer basis. Any individual with an Internet connection can access existing DeFi applications or build new ones using open-source code. This open structure has generated a truly global liquidity pool deposited by participants, with which an increasing amount of financial and commercial trading activities are taking place, all by means of automated systems that permit peer-to-peer interactions between counterparties.

DeFi can be envisioned as a "tech stack" that starts with a decentralized blockchain layer on which everything else is built, a Layer 1 comprising basic protocols that allow for the deployment of smart contracts, which create the rules for automating transactions and activities. Operating from the

smart contract layer, DeFi primitives include data, tooling and tokenized assets for composable functionality. With these tools, a wide range of DeFi applications can be built. The full listing of DeFi terms and definitions can be found in the taxonomy in Appendix 1.

FIGURE 1: DEFI TECH STACK



Composable financial primitives can be used to build products with a plug and play architecture. Key features include:

- Protocols define sets of common rules for each financial function
- Total Value Locked (TVL) as the total value of digital assets deposited into DeFi protocols, indicates liquidity, user engagement, and market sentiment
- Liquidity pools combine deposits of digital assets to enable trading
- Automated Market Makers (AMM) provide liquidity management and asset pricing mechanisms
- Flash loans enable borrowing and returning funds within a single automated transaction
- Proof-of-Stake is generally the consensus mechanism to process transactions effected on the protocol, in addition to other consensus mechanisms

It is important to note that DeFi has been developed without an official, or legally agreed definition, nor have the risks been clearly defined. Clarity has yet to be established with respect to ways DeFi should fit within the world of regulated activities, especially for financial services. Yet there are certain principles that its participants have established as foundational for DeFi, which can advance common understanding and also help to define and address risks.

Misconception #2: "DeFi is all about financial markets and financial instruments and is not accessible to all"

Reality: A participant can use any type of token in a DeFi protocol, so long as it is of a configuration, such as ERC20, recognized by the protocol. Layer 1 tokens, governance tokens and memecoins are some examples, as are tokenized stocks, event tickets and trading cards. All assets can be used in DeFi because the software does not differentiate based on the nature of the asset. DeFi essentially allows any activity involving the decentralized trading of assets over blockchain technology, allowing the possibility of activities that are not related to financial instruments but any asset or item tokenized using blockchain technology.

For instance, the regenerative finance (ReFi) movement, considered an offshoot of DeFi, proposes an alternative financial system centered on inclusivity, transparency, and responsibility relative to society and the environment to create net positive effects through regeneration. Another example that can morph into DeFi can be the emerging Decentralized Physical Infrastructure Network (DePIN) trend, which enables a blockchain-based network using cryptocurrency incentives to create and maintain physical infrastructure.

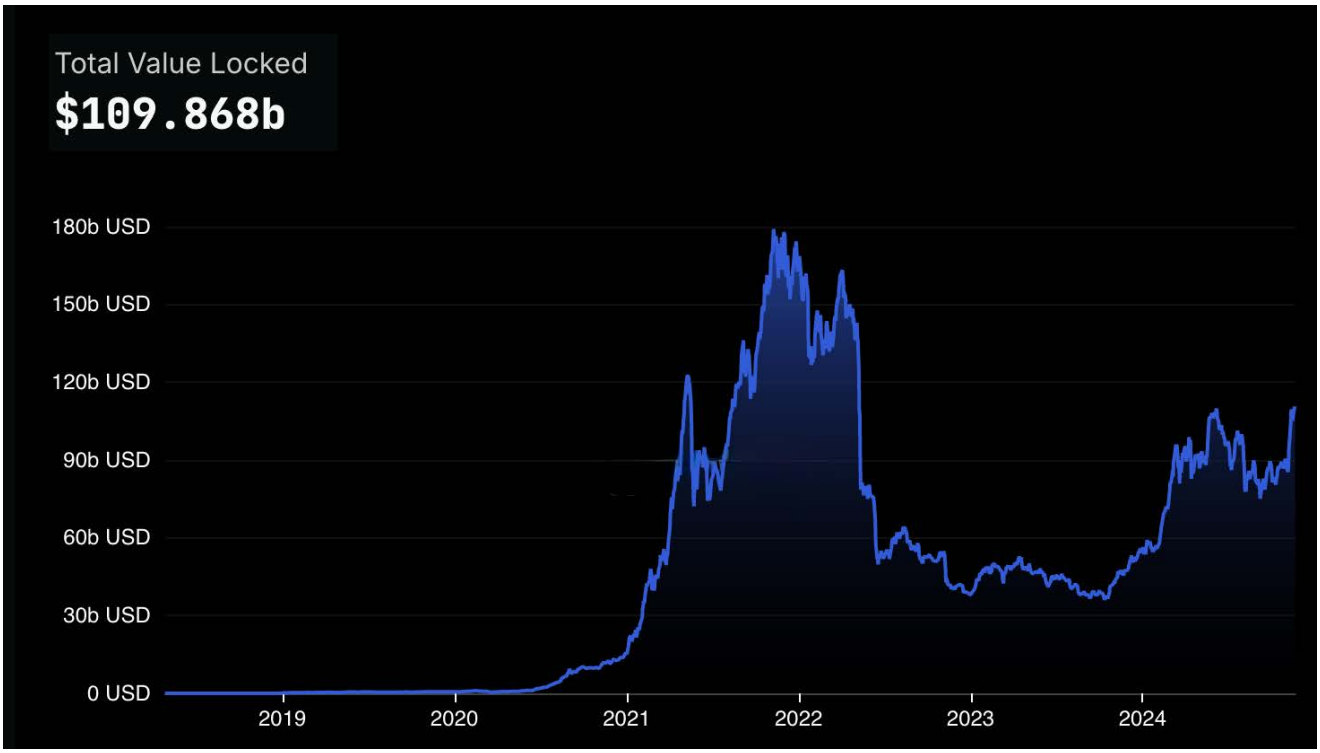
Misconception #3: "Smart contracts are real contracts and are safe because they are automated"

Reality: Smart contracts are nothing more than self-executing code. They are not inherently legally binding contracts, although they could be depending on the facts and circumstances. Moreover, they are not smart in the sense that they do not foresee variations or context apart from the conditions built into them to execute a transaction automatically. They do not account for unforeseen or unanticipated future events that could affect the technology's function or the participants' needs. Therefore, there will always be potential gaps and loopholes, scenarios that smart contracts will "miss" or not account for. It is in the time stamping element on which the safety of smart contracts can be relied.

Smart contracts also have a series of vulnerabilities, including operational risks (e.g., insufficient backup, lack of critical system safeguards, poor governance), technological risks including unintended technological (e.g., vulnerabilities in the code, human mistakes in coding, issues with oracles or sources of information they rely on), cybersecurity risks, and fraud and manipulation (e.g., nefarious code, backdoors). The code may have vulnerabilities to being controlled, and human mistakes may be difficult to reverse if funds are sent to the wrong recipient. Few people may have the technical ability to understand its function or the risks that could be fatal to its functioning.

Who uses DeFi?

FIGURE 2: TOTAL VALUE LOCKED IN DEFI PROTOCOLS



Source: DeFi Lama, Nov 20, 2024 - https://defillama.com

Total Value Locked has increased over the years and normalized following an initial hype. While most early DeFi users have been institutional and professional investors seeking excess returns , early users of DeFi in crisis situations where traditional financial systems have failed are showing real opportunities for financial inclusion. DeFi user growth has been especially significant in emerging markets, with Latin America leading, followed by Sub-Saharan Africa and Eastern Europe respectively. DeFi can reduce barriers to entry, especially for financial services like secondary trading and funding, helping to democratize alternative assets and scale innovations to make Web3 infrastructure more mainstream.

Steps to Scale

In order to achieve the opportunities that DeFi promises, so including the democratization of finance, there are a number of challenges to address and milestones to achieve in its early stages. Finding solutions to these challenges and getting closer to capitalizing on existing opportunities are represented as milestones below:

Functionality

To effectively reach these milestones, it is imperative that the technology functions effectively and securely for all stakeholders. From a technical perspective, an increasing array of tools are being developed to enable DeFi to fulfill its potential. Many of these innovations are driven by partnerships aimed at fostering coordinated progress, relying heavily on shared experiences. These efforts often integrate multiple emerging technologies and establish connectivity with traditional banking infrastructure. Incorporating human-centric design and behavioral analytics, with a focus on diverse populations, will further enhance user experience. Understanding the needs of end users is crucial, particularly as these solutions evolve to serve unbanked and underbanked populations, as well as globally distributed users.

FIGURE 3: DEFI MILESTONES

Interoperability

Interoperability is essential to performing seamless settlements, as the DeFi space often requires exchanging assets of value across chains. Otherwise, when this is not possible beyond a single DeFi protocol, there may be a need to utilize traditional methods. In the traditional approach, one can call upon the example of customers using Visa or Mastercard to settle payments across various systems globally. The DeFi space has achieved collaboration between participants with alliances, public blockchain systems, and secure mechanisms to transact across chains such as bridging technologies. While there are multiple ways to resolve this interoperability need, fragmentation stil exists and a need to ensure an entirely seamless flow of transactions. Moreover, as we move to a multipolar financial system with multiple centers of major activity, it becomes even more important for all participants globally to be in alignment for settlement. Some ways interoperability is being addressed include:

- Decentralized Compute: Blockchain technology can distribute computing power in a secure manner across multiple nodes, enabling networks to rely on multiple servers or data centers to support parallel processing and enhance scalability. This can also make use of underutilized resources at a global level.
- Artificial Intelligence: AI can automate procedures, improve security, and enhance decision making in DeFi. For instance, AI algorithms can detect patterns and predict trends using large data sets, helping investors make better informed decisions.

- API exchanges: Allowing connectivity from API to API, these tools are reducing costs while improving scalability and discoverability for direct-to-consumer applications. They also facilitate rapid deployment of digital solutions to underserved markets. They depend on harmonization around rules, with programmable rules engines that determine data sharing between APIs, and linking protocols to exchange data and facilitate execution.

Privacy and Security

Developers are exploring the use of Privacy-byDesign as a default security feature.

- Zero-knowledge proofs and other tools help manage information sharing by making only necessary information available as needed.
- Sovereign cloud solutions are being designed and launched to provide cloud computing environments that protect data and metadata in compliance with local laws within a particular jurisdiction.

Governance

From a governance standpoint, DeFi has introduced community-driven decision-making structures through the use of Decentralized Autonomous Organizations ("DAOs"). When properly deployed, and at scale, voting and polling, with the use of governance tokens, is meant to ensure stability, efficiency, and agreement on a wide range of topics. Responsible governance and environmental accountability at the Layer 1 level can trickle down throughout the DeFi ecosystem. Governance mechanisms are still not standardized across the ecosystem and there are many challenges associated with various governance models. When governance undermines decentralization, various risks arise.

IN THE ABSENCE OF REGULATION, RISK MANAGEMENT

Most major jurisdictions lack clear regulatory frameworks for DeFi. Policy makers and regulators do not have a ready toolkit for how to regulate autonomously functioning code that allows all asset types to trade together on a peer-to-peer basis (that is, without intermediaries). These three core features of DeFi stand in contrast to traditional market and regulatory paradigms in most of the world. In fact, DeFi often looks and behaves much more like general commerce (which may offer a more appropriate lens for analysis), than financial regulation.

Nor does the laissez-faire approach to software, hardware and communications technologies provide an easy paradigm for activities involving trading, lending, creation of commodity and other derivatives in a mixed asset, automatic and unintermediated commercial environment. As a result, legislators and regulators are still grappling with how to regulate and where regulation is needed.

Without regulatory clarity or a useful toolbox, how should participants act? We propose active, informed risk management. The following sections lay out the different participants and activities core to various types of DeFi protocols and seeks to identify the associated risks. There is a lot of ground to cover and different participants will make their own judgments about what is important to them. Undoubtedly, some will glide along in blithe ignorance, simply happy to ride the waves of the markets and bear all the attendant risks of markets that hopefully function in accordance with their

mandates. Others will want a walled garden so they can ensure that they are doing business only with appropriately checked counterparties on software that has been subject to extensive testing (which might not even be DeFi) and regulatory compliance.

Participants will fall across the spectrum. This paper does not seek to mandate answers or provide guidance on where liability and responsibility should lie. Rather, it lays the foundation for thinking about risk and therefore perhaps about regulation.

As a result, popular considerations and obligations that are broadly recognized at law for intermediaries may not clearly apply for software developers and infrastructure providers, These considerations and obligations point to certain common principles:

- Consumer protection
- Market integrity, addressing market manipulation and fraud
- AML/CFT measures
- KYC best practices
- Security and privacy
- Compliance

What follows are the breakdown of activities and risks.

DEFI ACTIVITIES AND RISK ASSESSMENT APPROACH

There are different categories of participants in the DeFi universe. Some are already regulated, either under traditional regulatory regimes or newer, cryptoasset-specific regulatory approach like Europe's Markets in Crypto-Assets Regulation. Others are not subject to direct regulation. In order to better identify DeFi risks, it is important to begin with identifying what constitutes a DeFi activity, for which we propose a categorization of DeFi activities that have arisen across traditional and non-traditional spheres of financial services. The aim is to identify activities that can be considered true "DeFi" services, to address the question of what makes something "DeFi" in nature. Each category below specifies examples of platforms offering a range of DeFi services, or allowing their customers to access DeFi services.

Note that the actual peer-to-peer individual users are not included as a category or within any category, but they can have significant impact on DeFi in a variety of ways, not least because they provide liquidity and trading interest. They can also be responsible for manipulations and gaming, as well as hacks and other exploits. Because there are multiple laws about these kinds of bad actions, we do not cover them separately in the risk assessment.

One unique aspect about DeFi is the market forces and economic realities that drive demand for, and creation of, solutions to perceived problems. Because the code is usually open source and anyone can launch a protocol that fixes issues, market participants can react almost in real-time to create more fairness, predictability and efficiency when something is identified.

This analysis proposes a high-level approach toward identifying and mitigating risks for DeFi activities across different categories. These risks may range from financial, operational, consumer protection, and regulatory risks. The examples below identify risks, obligations, and issues specific to these categories of services involved in the DeFi ecosystem, as well as mitigation measures.

Category 1: Traditional Regulated Entities

As Centralized Finance (CeFi) dips its toes into DeFi, traditional regulated entities have already begun using DeFi on behalf of clients or providing clients with access to DeFi protocols. For those already regulated entities, an approach toward risk assessments for DeFi services can start with referring to existing standards and how they apply to traditionally regulated entities. The entities listed below have clearly defined responsibilities mandated by regulation or industry standards. If they are to successfully adopt or use DeFi, they need to figure out how those responsibilities apply in the DeFi context of autonomously functioning code. For instance, major global banks assisting clients to access DeFi protocols are expected to assume responsibility for some aspect of connecting them, especially when it involves retail clients. When it comes to risk, it is important to consider that there is a difference between centralized and decentralized technologies, and a difference between tokenized financial instruments and other asset types.

TABLE 1: RISK MANAGEMENT APPROACH FOR TRADITIONAL REGULATED ENTITIES

Type of Entity	DeFi Functionality Offered/Considered	Considerations/obligations for Customers	Risks	Mitigation Measures
Fund Managers & Asset Managers	• Trading tokens and investing as part of money management • Improving the flexibility of accessing decentralized asset investments and sophisticated financial solutions • DeFi ledgering that provides greater transparency into assets' performance	• Regulatory compliance, where there may be regulatory restrictions for fund managers. Rules on custody requirements may also make it difficult to participate in DeFi. • Standards, as defined by jurisdiction	• Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Insurance policies • Data insurance capabilities to safeguard data • Recovery mechanisms • Centralize KYC • Participation in, or use of, counterparty risk mitigation tools
Brokerage Firms	• Trading and other DeFi activities that can improve liquidity • Considering becoming swap dealers	• Regulatory compliance with functional regulators • Duty of care, acting in the best interest of clients • Separation of customer assets and other requirements may make it difficult for brokerage firms to offer DeFi swap services • Sanctions and AML compliance	• Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Insurance policies • Data insurance • Recovery mechanisms
Market makers and liquidity providers	• Liquidity provision	• Though acting as a market counterparty, they should maintain market integrity standards • Registration in certain jurisdictions	• predatory trading • Sanctions Violations • AML and Fraud	• strong internal policies and procedures
Central Banks	• Research and pilots on DeFi implications for enabling transactions in the traditional financial system	• Research and pilots on DeFi implications for enabling transactions in the traditional financial system • Adhering to central bank mandates • Preparation measures for crisis management	• Technical risks • Monetary losses • Data breaches	• Extensive research, piloting, and testing of blockchain-based financial infrastructure

Category 2: Registered Legal Entities Offering Digital Asset Services

Legal entities offering digital asset products and services are subject to obligations specified by the jurisdictions in which they are registered to operate. These entities include businesses considered to be crypto-native, offering products and services tailored for the digital asset industry, without directly operating a DeFi protocol. For instance, centralized digital asset exchanges, trading utilities and custodians (including custodial wallet providers) may provide their clients access to DeFi protocols, by trading the assets of, or on behalf of clients in DeFi protocols or providing gateways to such trading. Other entities may provide the basic tooling utilized by DeFi protocols, such as stablecoins.

While these businesses may already provide customers with digital asset opportunities, such as efficiencies for trading alternatives in private markets, DeFi provides opportunities for these customers, adding value to their existing offerings. As these entities increase their engagement in DeFi activities, they should have responsibilities with respect to their customers just as for their other client offerings.

The jurisdictions where the entities are registered and/or licensed may provide stringent or lax requirements for their operations, which can have implications on their overall reliability and risks. On the other hand, these businesses may also be operating without formal licenses, and as such be outside the purview of any regulation. In many cases, it will be important to better define what these services mean in the DeFi ecosystem, and how these entities should envision their obligations to their clients.

Table 2: Risk Management Approach for Registered Legal Entities Offering Digital Asset Services

Type of Entity	DeFi Functionality Offered/ Considered	Considerations/ obligations for Customers	Risks	Mitigation Measures
Crypto exchanges	• Trading • Staking Services • Self Custody Wallets	• Best practices around product offerings • Risk mitigation programs • Liquidity and market integrity best practices	• Counterparty risk is introduced upon leaving a DeFi platform • Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Transaction monitoring and sanctions screening
Brokers and trading platforms	• Trading	• Best practices around product offerings • Risk mitigation programs • Secure and adequate functioning backend, especially with respect to data management • Liquidity and market integrity best practices	• Counterparty risk is introduced upon leaving a DeFi platform • Monetary losses • Data breaches • Scaling concerns for smaller platforms (e.g., queries, volume, and throughput)	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Transaction monitoring and sanctions screening

Custodians and Wallets	• Custody of tokens • Wallets may allow access to other DeFi services	• Safeguarding funds	• Monetary losses, especially stolen customer funds • Data breaches • Sanctions Violations • AML and Fraud	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Best practices for safeguarding funds (e.g., segregation of funds) • Insurance and recovery mechanisms • Transaction monitoring, sanctions screening, counterparty analysis, and enhanced KYC processes
Market makers and liquidity providers	• See above	• See above	• See above	• See above
Tokenization Platforms	• Tokenization of assets • Trading • DeFi reduces barriers to entry for adoption of tokenized assets	• Compliant infrastructure • Access controls and permissions	• Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Sanctions screening
Stablecoin and other Token Issuers	• Providing currency used as a key DeFi asset, allowing users to engage in DeFi activities such as lending, borrowing, and yield farming	• Providing currency used as a key DeFi asset, allowing users to engage in DeFi activities such as lending, borrowing, and yield farming - Adequate reserves and transparency • Integration with DeFi platforms using tokens as currency	• Monetary losses • Data breaches • Sanctions Violations • AML and Fraud • Collateralization or reserves risks	• Transparency and Risk Disclosures • Registration and licensing to ensure regulatory compliance • Transaction monitoring and sanctions screening • Processes to assure satisfactory reserves

Category 3: DeFi Protocols (truly decentralized per the definition above)

DeFi protocols operate as decentralized platforms, providing applications and services that have arisen and operates outside the purview of traditional regulation or agreed upon obligations. These are interfaces and pure technology providers, in a decentralized context where no single entity or authority is responsible for events taking place, in keeping with the definition presented at the beginning of this paper.

By removing intermediaries, DeFi protocols shift trust from third parties to the protocol itself. A new layer of smart contract risk, which is essentially programming risk plus the risk of "gaming" the system, arises when relying on purely automated functionality. Access also depends on how protocols are set up, which can have implications on risk. The nature of digital assets being exchanged over DeFi platforms also has implications on risk, as do common utilities utilized, such as the availability of data or interoperability mechanisms, including bridge technologies.

Defi protocols raise the question of whether there is there anyone "running the shop" who should have clear obligations to users and/or who should be regulated. While the applications themselves and the software developers behind them may not be regulated, there still need to be risk assessment considerations for these purely technology-enabled DeFi activities as suggested below. In this context, risk will depend on the activity in question. For instance, smart contracts have programming risks and other vulnerabilities. Websites may have flaws that allow bad actors to steal private keys to take control of funds. Moreover, for smaller businesses developing digital solutions, up-front costs and necessary integrations can present risks when there is uncertainty in the market, such as attempting to bank the unbanked.

An important subcategory of this section comprises DAOs, which play a critical role in the DeFi space when introduced for governance. DAOs may not be legal entities in the traditional sense and yet can have a certain level of responsibility associated with a DeFi protocol. Even while operating outside of clear regulatory obligations, the creation of clear roles and responsibilities that should be considered. While most jurisdictions have not yet devised ways of categorizing DAOs, the US State of Wyoming has developed in its laws two different versions of DAO structures. One is similar to a traditional limited liability company ("LLC"), and the other resembles an unincorporated association. The contours of each type are yet to be fully explored. Certain proposed legislation in the U.S. Congress also has sought to address certain requirements for DAOs (e.g., taxation). And, at least U.S. courts are beginning to recognize DAOs as "general partnerships," which (unfortunately for DAO participants) imposes joint and several liability for the acts of the DAO upon each and every DAO participant equally. This "general partner liability" could create significant challenges for the future adoption of DAO approaches to activities that carry significant risk exposure.

Table 3: Risk Management Approach for DeFi Protocols

Type of Entity	DeFi Functionality Offered/Considered	Considerations/ obligations for Customers	Risks	Mitigation Measures
Layer 1 Protocols	• Smart contract layer on which to build DeFi applications • Sets of common rules enabling composable financial services and governance • Essential functions like security and settlement	• Technical functionality • Security and privacy • True Decentralization	• Technical failures • Monetary losses • Data breaches • Consolidated control that is not fully and practically decentralized	• Code and security audits • Best practices for programming • Full divestment of protocol control by founders and creators
DeFi Applications in general	• Wide range of alternative financial services	• Technical functionality • Security and privacy	• Technical failures • Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Code and security audits • Best practices for programming • Implement next generation RegTech solutions to assure mitigation of Sanctions, AML, and Fraud risks

Decen-tralized Exchanges (DEXes)	• Exchange services	• Liquidity	• Technical failures • Monetary losses • Data breaches • Sanctions Violations • AML and Fraud	• Code and security audits • Best practices for exchange services • Implement next generation RegTech solutions to assure mitigation of Sanctions, AML, and Fraud risks
Lending Services	• Alternative lending mechanisms	• Responsible and fair lending	• Technical failures • Monetary losses • Data breaches • AML/Fraud • Sanctions Violations	• Code and security audits • Best practices for lending services • Implement next generation RegTech solutions to assure mitigation of Sanctions, AML, and Fraud risks
Bridges	• Interoperability solutions	• Effective transaction recording and verification	• Data breaches • Cross-chain jurisdictional compliance violations between Layer 1s • AML and Fraud • Sanctions Violations	• Code and security audits • Insurance • Recovery mechanisms • Best practices for privacy & security
Layer 2	• Scaling solutions, freeing up space at the L1 level for essential functions	• Offloading transaction execution	• Technical failures • Monetary losses • Data breaches	• Depend on the solutions provided
DAOs	• - Decentralized governance and decision making	• Ensure truly decentralized decision-making power • Mechanisms to overrule single voters	• Technical failures • Monetary losses • Data breaches • Unequal representation of individual participants, leading to information asymmetries and abuses • Concentrations of power in voting and other decision making structures • General Partnership Liability for violations of law	• Enable mechanisms similar to traditional corporate accountability structures • Warn participants of general partnership liability exposure

Misconception #4: The risk of criminal activity is higher in DeFi because there is no AML/KYC

Reality: Theft and fraud, with bad actors engaging in illicit and criminal activities, occur in both DeFi and TradFi. In DeFi, security protocols can be put in place, including AML/KYC and other compliance measures, to provide safe ways of exchanging funds. These measures are particularly important when removing intermediaries, and when integrating tokenized traditional assets with DeFi protocols. In some cases, data may be collected and made accessible only to regulators upon request. That said, this area remains subject to development and discussion. We expect developments here in the coming years. Insights drawn from tracking and tracing technologies have shown a relatively low (or at least comparable) incidence of money laundering in the space. While the data reveals growth in illicit funds sent into DeFi protocols, alongside a reduction in illicit services, this is in the context of DeFi's overall growth in market size. On the other hand, the transparency of fund flows in DeFi makes it harder to obscure fund movements.[4]

Category 4: Sandboxes, Free Zones, and Other Government-Sponsored Innovation Centers

Several governments are taking part in the DeFi space by providing sandbox environments for testing. Many innovations need to go through a sandbox for testing, as registration and licensing services, laws, regulatory frameworks continue to evolve for the DeFi space. These testing environments may also become an informal path for regulators to familiarize themselves with DeFi innovations. The aim is to ensure compliance in the use of smart contracts, algorithms, and processes at the settlement layer, transaction layer, and value/messaging layer while adopting new software.

Table 4: Risk Management Approach for Sandboxes, Free Zones, and Government-Sponsored Innovation Centers

Type of Entity	DeFi Functionality Offered/ Considered	Considerations/ obligations for Customers	Risks	Mitigation Measures
Sandboxes	• Testing environment and pre go live safety checks • Workshops and Incubation programs with security reviews	• Alignment with laws and regulations • SDKs to support safe testing and innovation • Ensuring balance of speed, security, and ease of use • Reviewing open-source environments and projects • Ensuring audited code	• Providing undue regulatory advantages to participants at the expense of the broader market	• These entities themselves are intended as mitigants for risks
Participating Entities	• Testing a wide range of DeFi functionalities	• Passing regulatory reviews as precursor for acceptance • Maintaining regulatory compliant operations	• Likelihood of operating in breach of rules within testing environment	• Seeking registration and licensing • Participation in sandboxes • Key partnerships

Category 5: DeFi Supporting Services

As a creature of the decentralized internet and blockchains, a range of supporting services have emerged to ensure smooth functionality, though not always accountability or responsibility. Attempts to regulate these support service providers would generally contradict the traditional "hands-off" approach to them by policy makers.

Table 5: Risk Management Approach for DeFi Supporting Services

Type of Entity	DeFi Functionality Offered/ Considered	Considerations/ obligations for Customers	Risks	Mitigation Measures
Certifiers & Assurance Providers	• Supporting services to ensure practices follow relevant compliance checks	• Certifications that DeFi activities are following compliance checks • Reviews of safety measures including analytics, insights, tracing, and due diligence practices • Transparency on nature of endorsements • Disclosures of 3rd party reviews	• False assurance, inaccurately miscalculating or failing to consider risks	• These activities themselves are intended as mitigants for risks
Decentralized file storage	• Supporting services	• Technical functioning • Security and privacy • Disclosures of 3rd party hosting data	• Technical failures • Data breaches	• Code audits • Best practices for data security, data hosting, backup mechanisms, and recovery mechanisms • Insurance
Layer 1 validators	- Ensure correct functioning of the underlying blockchain	• Under current legal and regulatory regimes, validators conduct this activity in accordance with the built-in consensus mechanism, which should be designed to ensure fidelity through Byzantine Fault Tolerance	• Technical failures • Failures of the consensus mechanism to be truly Byzantine Fault Tolerant	• Code, security and other audits
Internet infrastructure providers	- Providers and developers of software, hardware and cloud services, communications protocols, ISPs, market data providers, oracles	• Under current legal and regulatory regimes, infrastructure providers have few requirements and often are able to escape liability entirely, except when their actions amount to fraud or other types of willful misconduct such as theft	• Technical failures	• Security and other audits • System redundancies and back-ups

REGULATORY CONSIDERATIONS

With respect to regulatory risks and expected regulatory requirements, many open questions remain stemming from DeFi's core of automonous functioning, multi-asset, peer-to-peer nature and how associated activities would properly fit into existing regulatory regimes and expectations. Given that that DeFi protocols and platforms are regulated more by the market than by supervisors and have arisen outside the purview of regulatory supervision, a proper risk assessment seems foundational to any eventual requirements policy makers might seek to impose.

For centuries, the government has regulated intermediaries, not the individuals that design them, or the direct counterparties in peer-to-peer interactions. The implicit assumption is that individuals and counterparties would be in danger of third parties doing them wrong. Regulated activity, therefore, is designed to include the intermediaries all along the chain of custody based on traditional models. Yet DeFi presents a new model that essentially eliminates the traditional players that governments would regulate. Annex 3 below lists regulatory developments globally for DeFi thus far.

As an alternative, the space can start with a self-governance perspective, with structured standards and rubrics for adequate risk assessment and mitigation measures. These standards have made progress identifying best practices that, in the context of several enforcement actions against DeFi protocols in the last few years, could make many DeFi protocols more acceptable to regulators.

Misconception #5: All DAOs are fully decentralized and autonomous

Reality: DAOs come in all shapes and sizes, with their founders making decisions about how they function that may result in an organization that is not truly decentralized or autonomous, or indeed is (as a functional matter) fully centralized. It depends on the architecture and how tokens are distributed, as well as the voting process and other elements of governance. Moreover, few people may in fact read the smart contract behind a DAO, which can become a seemingly black box. Similarly, they may not fully understand their potential exposure to the "general partnership" liability described above. Reread the definition of decentralized at the start of this paper for a framework to think about whether a DAO is decentralized.

DAOs may have a treasury of funds separate from the voting group, which votes on different issues with tokens. If a single entity or a few entities hold a majority of tokens or control decisions in any other form, they essentially have decision making power regardless of how other token holders may vote or what they want. If there are no rules for minimum voting periods, or minimum timeframes from when a vote passes to when a decision is executed over a smart contract, decisions may be determined easily by a few or a single player when not everyone has had the time to vote. If the mechanisms to overrule a single entity casting a majority vote, decentralization may be a mirage.

In fact, litigators have in some rare cases recovered funds from unwilling DAOs. In these cases, these DAOs were not fully autonomous. When one person is the majority token holder, litigation can force them to pay for injustices using traditional measures and standard legal principles.

CONCLUSION

DeFi does not fit comfortably within existing frameworks because it involves autonomously functioning code with transaction finality, multiple asset classes and no central authority or gatekeeper. Peer-to-peer activity is paramount. It also currently suffers from a lack of clear definitions, categorization of actors and activities, and standardization. One might argue that all these features are actually good. They show creative disruption and experimentation on an unprecedented scale, which will drive markets and commerce to better, more global solutions.

On the other hand, just like blockchains provide certainty and predictability, it might be important for DeFi to accomplish those goals. To that end, below is a repository of open questions that the space is addressing, followed by a set of recommendations and considerations for DeFi developments moving forward. The goal at this point is not to specify regulation, which would lead to a jurisdiction specific analysis at too preliminary of a stage, but instead to point to areas that standards might cover. The implications of these questions, considerations and recommendations can then point to specific needs such as new legislation or regulatory developments, new interpretations of such, or necessary exemptions, new sets of expectations, or new technologies (e.g., decision makers investing in analytics solutions tailored for the space).

Open Regulatory Questions for DeFi

1. What constitutes a true DeFi activity?
2. How do DeFi activities fit into existing regulated activities, if at all?
3. For those DeFi activities that may not fit into existing regulations, what are the regulatory expectations for them, and can DeFi protocols satisfy them?
4. What is the appropriate role of government and regulation in a context where there are no intermediaries? Does current law address this effectively in any way?
5. Is having an intermediary sufficient to require regulation? To whom should this point, and what does it mean to remove intermediaries?
6. Should any DeFi protocols, or any elements of protocols (e.g., Dexes) be treated as intermediaries?
7. What makes a financial intermediary, especially for the purposes of being held liable as such?
8. How should regulation address data subjects and counterparties when there are no intermediaries?
9. Who should be held responsible when something goes wrong in the context of no intermediaries?
10. What functionalities should DeFi participants ensure in order to be considered acceptable by regulators and prevent enforcement actions?
11. Should the same principles apply for all DeFi participants, or should there be different rules for different participants?
12. How should regulation address DAOs? Should they be considered legal entities in relation to the law?
13. How to deal with potential “general partnership liability” for DAO actions and activities?
14. What should risk assessments for DeFi entail?
15. What considerations and obligations to customers should DeFi participants be required to have?
16. Should regulators stay out of or lean into regulating the industry?
17. What are the implications of imposing penalties on direct participants (individuals and counterparties), as opposed to exchanges, mixers, and other services?

18. Should an interface providing access to regulated activities (e.g., wallet to access DeFi protocols and make trades) be considered an intermediary and be regulated? Should protocols that provide access to those interfaces be regulated for doing so (e.g., wallet providers)? Where will that end up, if we regulate all layers of access?
19. Should contract participants follow rules to be considered eligible to carry out a transaction? Should a transaction involving an ineligible contract participant be allowed in any circumstance?
20. Should smart contracts be regulated as brokers for carrying out order routing activities, etc.?
21. What new changes does DeFi bring, how do they affect markets, and what would be the implications if DeFi were to scale?
22. Does fully a permissionless and trustless system truly exist, and should it?

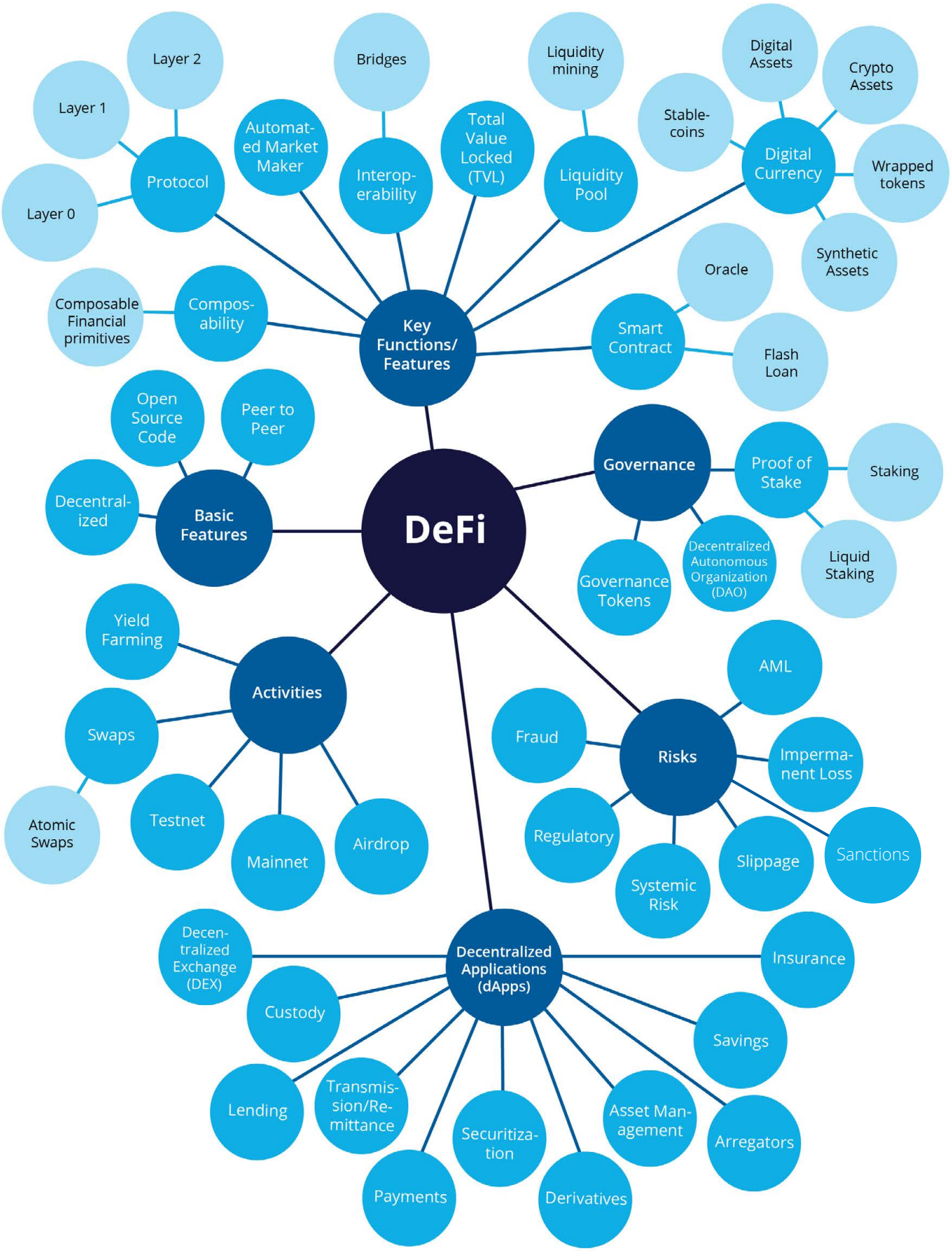
Recommendations and a Skeletal Playbook for DeFi

1. Providing clear definitions in this ecosystem is imperative as a first step to define roles and responsibilities for DeFi players.
   a. There may be a need to define the necessary elements of a DAO in order to merit that name.
   b. A definitional exercise will help the space to identify and approach entities, or subcategories of such, that should or should not be covered by rules
2. Define what standards should be in place for DeFi, and what categories of activity they should apply to, as a precursor for regulation
   a. Define what categories of DeFi activities should be subject to specific standards and best practices, in the absence of regulation at this point
3. Consider that DeFi players, including DAOs, may have a certain level of responsibility will require a certain amount of regulation and what determines when that level is met. a. To determine DeFi players' considerations and obligations to customers, understand what part of the protocol is in question (e.g., smart contract executing transactions, website customers use to access smart contract).
   b. For specific issues (e.g., IP, tax schemes, etc.), consider the actual allocator in a project.
   c. Consider the scope of traditional players and legal entities participating in DeFi, and their regulatory requirements.
   d. Assess the relevance of existing regulations (e.g., regulations for issuance of assets, residence/jurisdiction of defi users, KYC requirements to trade in tokenized assets, etc.)
4. Acknowledge that the activity makes the cases, considering the particular facts and circumstances rather than making sweeping claims. Tokens are separate from the entities and activities using them.
5. If DeFi services replace traditional financial services and processes, they must also be effective at protecting the markets they serve. Define measures for effective AML, protections against fraud, sanctions compliance, and other existing safeguards
6. Implement risk assessments for all types of DeFi activities, identifying the topics they would address and the expectations they give rise to.
7. Consider measures for governance and dispute resolution across categories of DeFi activities
8. Consider services for AML/KYC, verifications, and consumer protection measures.
   a. For instance, protocols may require participants to use secondary digital identity solutions to prove they are not bankrupt, not in a sanctioned country, and have not been convicted of a crime.
   b. Zero knowledge proofs can ensure privacy, and the data can be validated by a legitimate external entity (e.g., US Customs), providing a credentialing solution that any DeFi protocol could accept.

c. This can be operationalized as a layer on which DeFi protocols can function, as an example of harmonizing regulatory technology on top of DeFi solutions. Consider finding ways to obtain legal immunity for using these methods and tools in a DeFi environment.

9. When DAOs are not in reality as decentralized or autonomous as intended, consider a need for broader agreement on DAOs' responsibilities and proper functioning.
   a. Voting and decision making power should not be concentrated in the hands of a few players or a single player.
   b. Assess if a DAO is fully decentralized and autonomous, or partially so, and define an approach accordingly
10. Define the entities that should be held responsible when things go wrong, and solve the "general partnership liability" problem.
11. Define the regulatory risks and consider an iterative process toward legislative and regulatory developments.

Appendix 1: DeFi Taxonomy



Annex 2: Standards and Principles for DeFi and Tokenization

When it comes to basic functionality:

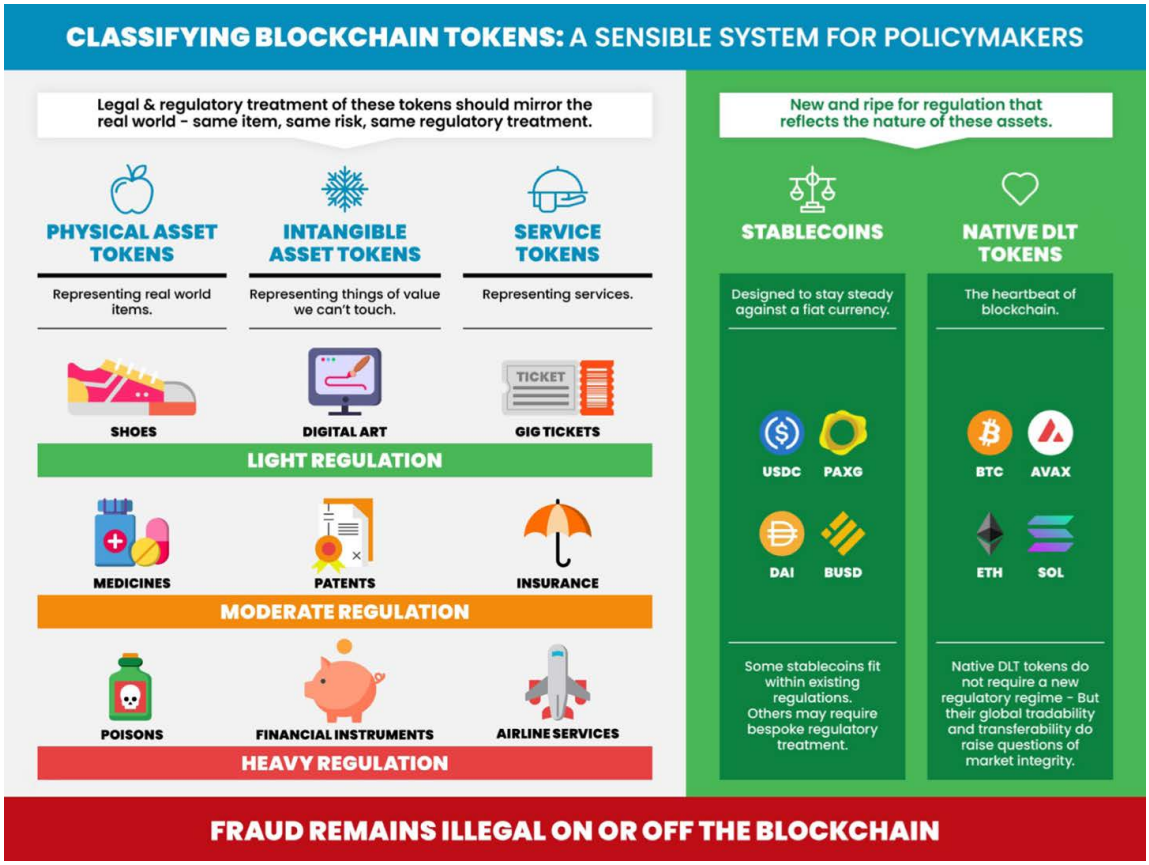
- Quality Management: ISO 9000 is a family of standards for quality management systems. They provide guidance and tools to ensure protocols and services meet external requirements for quality improvement consistently.

There have also been initiatives to develop principles addressing issues presented by the broader blockchain and digital asset space, which are relevant to DeFi, and also principles specific to the DeFi ecosystem.

The recommendations to the US Commodity Futures Trading Commission (CFTC) Global Markets Advisory Committee (GMAC) by the Digital Asset Markets Subcommittee (DAMS) in March of 2024 proposed a Digital Assets Classification Approach and Taxonomy[5] acknowledging that ***"The features of a Digital Asset include, but are not limited to, how the asset: (1) is issued; (2) holds value, (3) confers rights, (4) has fungibility, (5) can be redeemed, and (6) is recorded in books and records. The Subcommittee has endeavoured to define these features below. Digital Assets in this classification have at least one or more of the features captured in the categories, but it should be noted that there may be features developed in the future that have not yet been contemplated at this time. Similarly, not all Digital Assets classified here, have all these features. This is therefore intended as a starting point designed to support regulators and policymakers to take a use case driven approach to evaluate which types of regulations should apply to which type of assets. As these assets evolve and new ones are created, this classification will need to be evolved."*** Digital assets and their various forms are defined and categorized as follows:

Digital Asset Type	Instrument Type	Instrument
Money & Money-Like Digital Assets	Central Bank Digital Currency	General Purpose of Retail CBDC
	Central Bank Digital Currency	Wholesale CBDC
	Bank Deposits	Tokenized Deposits
	Bank Deposits	Deposit Tokens
	Reserve Backed Digital Currencies	Reserve Backed Digital Currencies
	Stablecoins	Stablecoins
Financial Digital Assets	Tokenized Security	Digital Twin
	Security Token	Digital Native
	Tokenized Derivative	Digital Twin
	Derivative Token	Digital Native
Alternative Digital Assets	Tokenized Alternative Asset	Digital Twin
Cryptoassets (e. g. cryptocurrucies)	Platform Cryptoassets (e.g. Bitcoin Ether)	Non-redeemable digital native token with no rights conferred by the issuer (if any)
	Other Cryptoassets (e.g. meme coins)	Non-redeemable digital native token with no rights conferred by the issuer (if any)
Functional Digital Assets	Functional Digital Assets	Cannot be exchanged for value, provides owner with a specific utility
Settlement Controllable Electronic Record	Settlement Token	Solely to transfer or record ownership or perform other middle/back-office financial functions

Another approach to classification of tokens proposed by Owl Explains[6] and published in the International Journal of Blockchain Law[7] is as follows:



"Core Principles for the purpose of setting minimum standards and best practices for the conduct of centralized digital assets businesses that handle customer (or user) digital assets and funds"[8] include:

- Strong Governance and System of Checks and Balances
- Protection of Customer Assets
- Enterprise Risk Management and Stress Testing
- Liquidity Reserves
- Proper Books and Records
- Annual Independent Audit

The "Proposed Information Guidelines for Certain Tokens Made Available in the United States"[9] include proposed guidelines for:

- Token offering and sale information
- Material participants
- Governance
- DLT Technology
- Token information
- Financial information
- Risk factors
- Exhibits

Gibraltar has also released 10 principles for DLT:[10]

1. Honesty and Integrity
2. Customer Care
3. Resources
4. Risk Management
5. Protection of Client Assets
6. Corporate Governance
7. Cybersecurity
8. Financial Crime
9. Resilience
10. "A DLT Provider must conduct itself in a manner which maintains or enhances the integrity of any markets in which it participates."

Guidance for smart contracts

- Smart Contracts: OpenZeppelin has ample guidance for smart contracts on GitHub, as a library for secure smart contract development[11]
- The Smart Contract Primer co-authored by several law firms and TradFi industry groups provides a comprehensive look at the technology of smart contracts and some of their use cases[12]

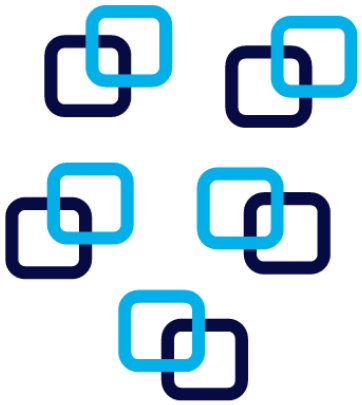
IOSCO: Final Report with Policy Recommendations for Decentralized Finance (DeFi)[13]

- Recommendation 1 - Analyze DeFi Products, Services, Activities, and Arrangements to Assess Regulatory Responses.
- Recommendation 2 - Identify Responsible Persons.
- Recommendation 3 - Achieve Common Standards of Regulatory Outcomes.
- Recommendation 4 - Require Identification and Addressing of Conflicts of Interest
- Recommendation 5 - Require Identification and Addressing of Material Risks, Including Operational and Technology Risks.
- Recommendation 6 - Require Clear, Accurate, and Comprehensive Disclosures.
- Recommendation 7 - Enforce Applicable Laws.
- Recommendation 8 - Promote Cross-Border Cooperation and Information Sharing.
- Recommendation 9 - Understand and Assess Interconnections Among the DieFi Market, the Broader Crypto-Asset Market, and Traditional Financial Markets.

Additional academic and governmental resources can be found on the EU Crypto Initiative DeFi webpage and the Owl Explains DeFi webpage.

SECTION IX

DIGITAL IDENTITY AND BLOCKCHAIN: USE CASES, DIGITAL PUBLIC INFRASTRUCTURE MODELS, AND KEY PRINCIPLES FOR GROWTH



EXECUTIVE SUMMARY

Digital Identity systems are essential for services that empower individuals to securely prove their identity and access a wide range of public and private services. Within a dynamic data economy built around data exchange, digital identities must work seamlessly across national boundaries and jurisdictions, be interoperable and resilient, and enable individuals to govern their digital identity.

A robust digital identity is a necessity and a catalyst for innovation. It paves the way for transformative use cases in decentralized finance, social services, healthcare, and other domains. The emergence of the need for a high-assurance digital identity in many countries is a testament to its potential. The current state of affairs in these use cases is plagued by data duplication, low data quality, loss and leakage during service delivery, loss of benefits, exclusion, and forgery of digital identity. A robust digital identity can address these issues and unlock possibilities.

INTRODUCTION

It is essential to highlight that digital identities are not limited to individuals. Businesses also use digital identities to establish bona fide relationships and exchange verifiable information. While the term "digital identity" implies a transformation from traditional forms of identification and authentication (such as printed ID cards, passports, etc.), there is much confusion around the definition of the term itself.

The Wikipedia entry[1] for the term describes it as

*"A **digital identity** is data stored on computer systems relating to an individual, organization, application, or device. For individuals, it involves the collection of personal data that is essential for facilitating automated access to digital services, confirming one's identity on the internet, and allowing digital systems to manage interactions between different parties. It is a component of a person's social identity in the digital realm, often referred to as their online identity.*

While this term is reasonably complete, it needs more insights into the capabilities of a digital identity. The UK government has published a UK Digital Identity Attributes and Trust Framework document where it defines a digital identity[2] as

"a digital representation of a person acting as an individual or as a representative of an organisation. It enables them to prove who they are during interactions and transactions. They can use it online or in person."

For this document, we will consider a digital identity to be

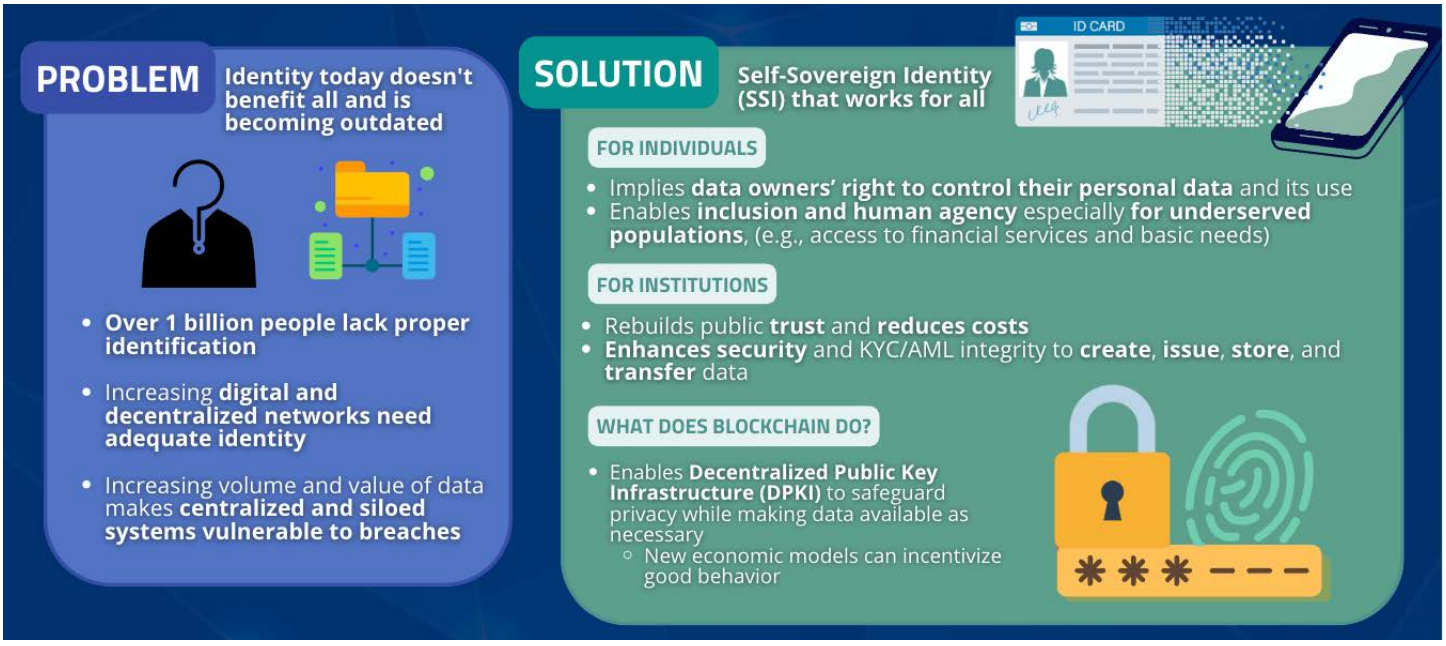
"A digital representation that enables people, organizations and things to present trustworthy data when interacting digitally."

Digital trust company Sezoo[3] published this definition in the paper "Trustworthy digital identities as a foundation for digital trust"[4]

(PART 1) DIGITAL IDENTITY & USE CASES: WHAT IS THE NEED FOR DIGITAL IDENTITY?

A fact often highlighted in any discussion around digital identities is that nearly a billion people do not have any verifiable identity or other legal documentation. The absence of such papers significantly encumbers, especially for underrepresented and marginalized communities, the ability to access services, seek employment, or discover ways to improve their way of life. In a digitally connected world that depends on digital transactions, the absence of trustworthy digital identities leads to exclusion and exploitation. It exacerbates the magnitude and consequences of a digital divide between those with access and those without access to networks of productivity. A foundational digital identity presents a form of "root of trust" that can be recognized by other entities and stakeholders in an ecosystem. Such recognition also establishes the acceptance of the assertions made by the individual through the digital identity they consent to share, which allows access to participate in the economic, legal and political aspects of the ecosystem or network.

Figure 1: The need for Digital Identity



The digital transformation of society has led to explosive growth in transactions that depend on reliable and trustworthy data exchange. Access to such high-trust data is now essential to the value-creation system. Therefore, data bound in some form to reliable digital identities is a critical component for governance, business and regulatory functions. The various use cases of digital identity demonstrate a fundamental need to create, issue and manage reliable digital identities, which offer the holders/principals/subjects the capability to mitigate the risks emanating from poorly designed data flow systems, and even data security breaches.

(1.1) FORMS OF DIGITAL IDENTITY

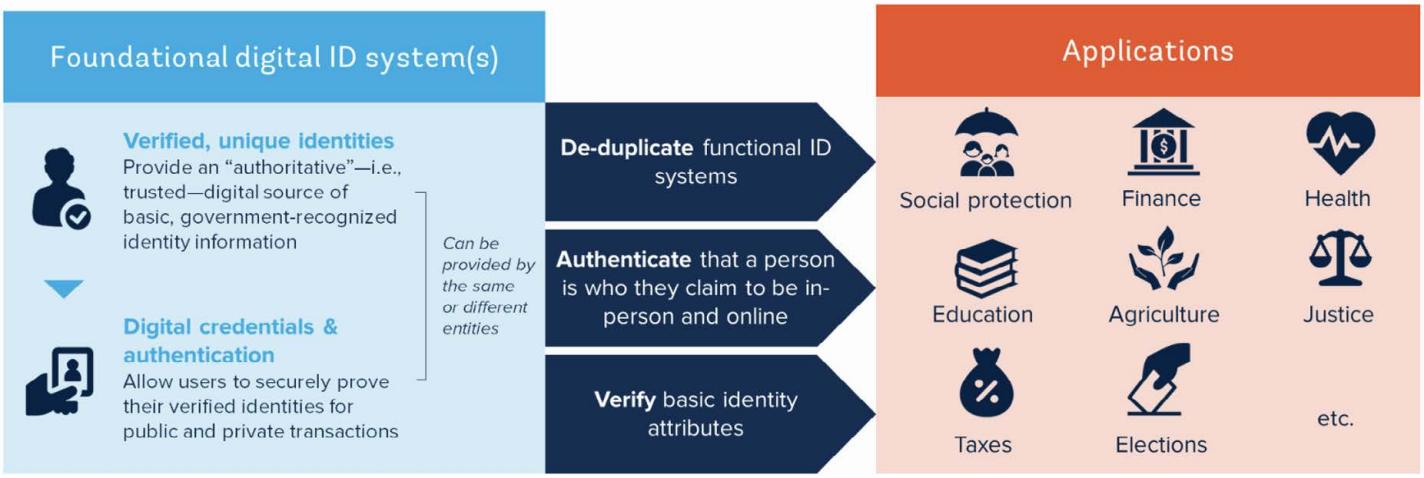
Digital identity refers to the use of data, represented and utilized as a digital identifier, identify an individual or entity. These identifiers can refer to the following broad categories:

1. Persons (Personal Identity)
   - **Definition:** This refers to an individual's unique identity used in the digital world for various personal activities.
   - **Usage:** For social media interactions, personal communications, and accessing non-work-related online services.
   - **Examples:** Social media profiles, email accounts, user IDs for personal apps. This also includes digital versions of government-issued IDs (e.g., e-passports, digital driver's licenses, national ID cards).
2. Employees of the Company / Organization
   - **Definition:** The digital identity assigned to an individual by their employer, representing them as part of an organization.
   - **Usage:** For accessing company systems, conducting business tasks, and collaborating on projects.
   - **Examples:** Work email addresses, employee ID numbers, login credentials for work platforms.
3. Legal Identities (Legal Entity Identifiers - LEI)
   - **Definition:** A unique, standardized code that identifies businesses and organizations in financial and legal transactions.
   - **Examples of LEI in Use:**
     i. **International Trade:** A shipping company uses its LEI to facilitate cross-border transactions, ensuring compliance with global trade regulations.
     ii. **Banking:** A financial institution verifies the LEI of a corporate client before opening a business account.
     iii. **Investments:** An asset management firm uses LEIs to identify counterparties in securities transactions.
     iv. **Tax Reporting:** A multinational corporation includes its LEI in regulatory tax filings to comply with international standards.
     v. **Regulatory Compliance:** A startup registers for an LEI to participate in financial markets and report transactions to regulators like the European Securities and Markets Authority (ESMA).
4. As Internet of Things (IoT)
   - **Definition:** Digital identities associated with connected devices and machines that communicate over the internet.
   - **Usage:** For device authentication, remote control, data sharing, and security management in smart environments.
   - **Examples:** Smart home devices, industrial IoT devices, wearable tech with unique device identifiers.

When it comes to individuals, digital identity can also take several forms and attributes, of which we highlight the most common below:

Foundational Identity: This refers to the general concept of a basic identifier, generally at a national level, that can be used to access a wide range of services offered by the public and private sector, and also engage in related transactions. A foundational identification system is to manage the identity data for the general population, providing credentials to serve as proof of identity to access such services and transactions. Increasingly, foundational identity systems are adopting digital formats.

Figure 5. Potential role of a foundational ID system



Source: https://id4d.worldbank.org/guide/types-id-systems

Derived Identity: In some cases, where a state-mandated national ID has yet to be slowly rolled out, bank IDs have become repurposed to provide a set of high-quality digital identifiers that can be linked to and integrated into many other services. These services do not have to be banking-related; many non-banking use cases have also emerged building on the basic digital identifiers provided by banks. In some cases, the interactions and transactions of the ID holder provide a good proxy for the notion that a derived ID can be attested and certified by external or third parties. Therefore, derived identity can serve as a proxy for a foundational identity that may not exist.

Biometric Identity: The unique biological characteristics of individuals can be used to verify their identity. These attributes can be biological characteristics (e.g., fingerprints, iris scans, facial recognition, veins, and shapes of body parts like ears, hand geometry, or even odor or DNA attributes) or behavioral attributes (e.g., voice, signature, keystroke patterns, or patterns in gestures, walking, or other movements). Biometric authentication is invoked when a select number of unique biological traits are used to verify a person's identity. In some digital identity systems, especially those related to high-trust and high-assurance data exchange use cases, the user enrollment workflow also includes registering biometric information. Many of the largest identity projects include a biometric component.

Biometrics may be considered more accurate than other forms of identity because they are inherently tied to the individual. Biometric characteristics, as opposed to passwords and other

codes, are very difficult, or nearly impossible, to duplicate, lose, or share for use among multiple persons. Many national identity and immigration or border crossing records rely on biometrics. Security is of utmost importance for this form of identity because any personal data stolen through a breach would be nearly impossible to reverse. As opposed to changing a password, we cannot change the shape of our fingerprint. Therefore, the risks and overall downside of biometric identity (e.g., violation of privacy rights, high costs, invasive format) in many cases may not make this form of identity worthwhile because they may not be outweighed by the benefits.

Self-Sovereign Identity (SSI): The main challenge with a digital identity has always been to implement it safely and correctly. This usually means that the digital identity protects the holder's privacy, does not lead to exclusion, and functions in a way safe enough to prevent unwanted surveillance by correlating usage patterns of the digital identifier. Over time, self-sovereign identity (SSI) principles[6] have provided a working framework for designing, deploying, and managing a digital identity system where identity holders have the power and sovereignty over their own identities. These principles focus on the digital identity holder's agency, autonomy, and integrity.

Figure 2: 12 Principles of SSI from the Sovrin Foundation

CANADA'S DIGITAL SELF-SOVEREIGN IDENTITY FRAMEWORKS

In recent years Canada has led in the adoption of SSI based approach to digital identity and the creation of a regulatory framework which enables user-centric approach to the governance of such identifiers.

A digital identity would simply be the electronic equivalent of physical documents one already has. With the digital identity, the holder would be able to do things like:

- Claim social benefits
- File your taxes
- Access your health records
- Open a bank account
- Buy a home

Digital ID in Canada is protected by The Privacy Act, The Digital Charter and a Policy of Government Security Directive on Identity Management.

The Canadian government is in the planning stages of rolling out a country-wide digital identity program. https://ised-isde.canada.ca/site/innovation-better-canada/en/canadas-digital-charter-trust-digital-world

Digital credentials allow people and businesses to access services online without having to go to a location in person, send sensitive information through mail, or remember another username and password. Enabling individuals and businesses to prove their identity and share verified information through digital means.

This approach is built around offering security, efficiency, convenience for the holder of the digital credentials. However, as this is an emerging technology landscape there are downsides to rapid adoption in the form of enabling robust cybersecurity, ensuring inclusiveness and equity through accessibility features, managing privacy and the overarching reliance on technology through the digital transformation process.

Digital ID generally offers greater protections from ID theft and leaks of sensitive info in boosting privacy. But concerns include data collection, who can access this data and how it's used, as well as location tracking, and questions around potential for government tracking.

The Privacy Act and the Digital Governance Council of Canada standardized framework (PCTF) define a duty of care that citizens, clients and customers should expect while using modernized digital services. This defined duty of care puts people's benefits at the center while enabling adopters to verify their practice, and trustmark to validate data integrity and security.

The Digital Identity and Authentication Coalition of Canada DIACC has produced a shared European and Canadian perspective on digital identity policy principles to maximize benefits for people. Comparing digital identity approaches to inform policy development and support interoperability efforts. More information is available about this approach https://diacc.ca/2022/11/02/policy-design-principles-to-maximize-people-centered-benefits-of-digital-identity/

Directive on Identity Management https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16577 is supported by two guidelines and one standard:

Guideline on Defining Authentication Requirements https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=26262;

Guideline on Identity Assurance https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30678;

Standard on Identity and Credential Assurance https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32612

The west coast Province of British Columbia now has a digital identity, the BC Services Card. The service provides cardholders the ability to prove their identity to access government services in-person and online using a physical or digital BC Driver's Licence and Services Card. DID will not be mandatory, other forms of physical ID may still be used.

The City of Vancouver is spearheading the use of digital credentials to reduce the need for manual verification steps in permitting and licensing services. Digital credentials are issued by recognized authorities to the BC Wallet mobile app where the information is encrypted and secure. Work is underway to further explore applications, including Digital Business Licences, Digital Certificate of Qualification, Digital Home-Owner Credential.

(1.2) DIGITAL ID AND BLOCKCHAIN

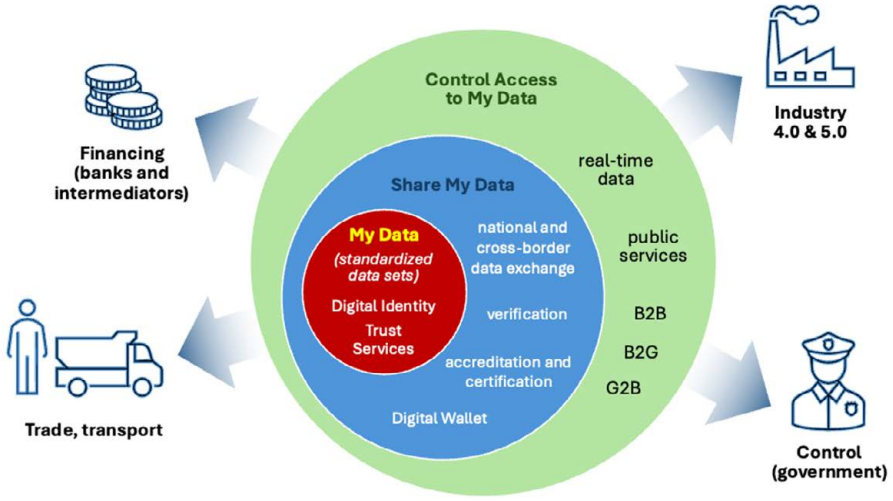
Blockchain, a technology usually more recognised for cryptocurrency moorings, has been pivotal for the adoption of SSI models. It has expanded access to underserved communities and enhanced the privacy and security of personal information. More importantly, it has empowered the holders to have more control over their data, enabling a significant shift in the digital landscape of activities.

Today, we see digital identities becoming the focal point of discussion when designing digital transformation policies globally, including those spearheaded by member states in the EU, and a wide range of programs currently developing and rolling out national ID projects in countries such as Bhutan[7]. The Modular Open Source Identity Platform (MOSIP)[8] project has enabled the implementation and adoption of digital identity as an open-source Digital Public Good (DPG)[9]. This approach has lowered the cost of digital identity deployment and encouraged many more countries to pivot toward creating the necessary business, legal and technical frameworks for successful digital identity rollouts.

In many cases, good biometric technology is a key binding element to digital identities, especially doing so in a manner that enables the person to have more agency, control, and autonomy.

DIGITAL ID CAN BE A CORNERSTONE OF A REAL-TIME ECONOMY

Digital Identity is fundamental to an ecosystem where economic transactions, processes, and activities occur in real-time or near real-time, as facilitated by blockchain technology. This is enabled by digital technologies and instantaneous data flows, allowing businesses, governments, and individuals to interact and make decisions with minimal latency. Key characteristics include automation, integration of systems, and immediate processing of payments, reporting, and other economic activities. Digital identity is a cornerstone of the Real-Time Economy, as it facilitates seamless, secure, and efficient transactions.



(1.3) FORMS OF DATA

Just as there are several forms of digital identity, there can also be several forms of data utilized to create digital identities. Each form of data can also facilitate certain kinds of identifiers. Therefore, digital identity use cases are often tied to a particular form of data.

Different forms of data can be used to achieve distinct use cases through a digital identity...

Less information → Extensive information

	1 Deterministic data	2 Probabilistic data	3 Self-managed data
Overview	• First party data that is trusted and true. • Deterministic data relies upon identity attributes that act as unique identifiers to create a match between one or several pieces of personally identifiable information.	• Predictive insights that are inferred from behavioral events across a wider range of data sets. • Statistical modeling is generally used to assess the probability that the data matches a specific person	• Individual (usually consumer) created data that provides the user with increased control and autonomy of verifiable credentials.
Scenario examples *Deep dive next page*	• Credit and financial identity • Data aggregators • Business and entity verification • Identity verification	• User-generated content management • Identity graphing and resolution • User and entity behaved analytics • Biometrics	• Identity wallets • Password managers • Master data management • Decentralized ID and verifiable credential management
Type of information requiered	• Legal name • Government issued ID number • Biometric data • Data verification data	• Usage patterns (i.e., statistical data) • Geolocation data • Social media activity and engagement	• Credentials and certifications • Nationality • User-generated profile information

... With each type of data category enabling a series of unique use cases

1 Deterministic data

- Credit and financial identity
- Data aggregators
- Business and entity verification (KYB)
- Identity verification (KYC)
- Identity proofing
- Regulatory compliance transaction monitoring
- Background screening
- Document verification
- Mobile identity and device intelligence
- eID and Civil IDs
- eSignature

2 Probablistic data

- Identity graphing and resolution
- Personal and signals based intelligence
- User and entity behaved analytics
- Fraud detection and prevention
- Biometrics

3 Self-maanged data

- Master data management
- Privacy, data protection, and consent
- Identity governance and administration
- Workforce IAM
- Customer IAM
- Privileged access management
- Authentication
- Machine identity
- Password managers
- Identity wallets
- Decentralized ID and verifiable credential management

FORMS OF DATA AFFECT ACCESS TO DIGITAL IDENTITY

The form of data that a given digital identifier comprises can have a fundamental impact on the use cases that it can facilitate, through which persons can be authenticated to the extent that they can be matched to records of digital identifiers. Self-managed data, for instance, can be flexible and take several forms. Deterministic data refers to an exact value (e.g., Identity card number) that leaves no margin of error in matching a person to an identifier. On the other hand, biometric data uses a probabilistic mechanism to match a person to an identifier (e.g., fingerprints). The patterns detected on a biometric record (e.g., past fingerprint image) may have a margin of error with respect to the biometric information provided by the person in real time (current fingerprint image capture). Therefore, there must be a tolerance value that must be considered.

ADDITIONAL CONSIDERATIONS FOR BIOMETRIC IDENTITY

Biometrics are being gradually introduced at scale, such as at border checkpoints, thus intersecting with traveler experience and a broad range of activities in which such identities are used. Many of these interactions primarily include Facial Recognition Technologies (FRTs). Implementations must keep current with the work underway at the National Institute of Standards and Technology (NIST),

under the Face Recognition Technology Evaluation (FRTE), among many related initiatives and standards underway, which are meant to ensure the accurate and measurable quality of biometric data readings such as FRTs.

At the moment a person opens an online account, the identity verification process involves a form of device binding to the credentials utilized, ensuring the device acting on behalf of a person is actually owned by that real person and not someone else claiming to be that individual. An essential driver of binding biometric information during digital identity enrollment is the capability to use a mobile device-centric user experience during the data exchange stage. The Digital Identity Guidelines from NIST[10] (800-63-4, available for public comments until 7th October 2024) include a comprehensive set of aspects around the management of risks and determination of impact levels around the measures of risks for enrollment into a digital identity service.

ETHICAL CHALLENGES FOR BIOMETRIC IDENTITY: COMPLIANCE, SECURITY, AND TECHNICAL CONSIDERATIONS

A recent case highlighting the importance of ethical considerations has been the emergence of projects like WorldCoin, and subsequently the Orb project, which have become highly controversial in providing technology to capture biometrics to build reusable digital identities. After a high-profile rollout that was deemed to be non-compliant with local regulatory requirements, many countries have decided to revisit this approach and stopped further citizen enrollment using WorldCoin technology.

WorldCoin implementations didn't consider the legal requirements in the countries where they launched operations, leading to heavy regulatory scrutiny and investigations. There is sufficient research[11] [12] [13] that acquiring biometric data and enabling binding requires regulatory approvals and oversight. An important lesson learned from the response of various national governments to the approach adopted by WorldCoin is that a launch at a global scale must be compliant in all jurisdictions in which operations are to take place. This requires strategic considerations around security, both with respect to data and the applications themselves.

Another ongoing challenge with using biometric technology for identity binding during the enrolment process of creating a digital identifier is creating adequate guardrails against unintended consequences[14]. Since biometric technology- based authentication is often the first option for enabling access to the services, selecting good failsafes is crucial. Biometrics are a powerful tool, but they only work adequately if robust security measures can be ensured, given the magnitude of potential downsides (e.g., identity theft compromises uniquely personal information that cannot be replaced).

Moreover, biometric authentication which requires fingerprinting, for instance, can also become a barrier when there is a fingerprint mismatch or fingerprints can no longer be read with sufficient accuracy by the hardware used. Robust management of biometric data, preventing such data being accessed at rest or in transit, and ensuring secure encryption technology is essential for adopting biometric based digital identity workflows[15]. Given the level of digital literacy in a given population, it is essential that workflows which depend on biometric technology provide ways to record informed consent, protect the privacy of the holder and prevent data misuse.

EXAMPLES OF BIOMETRIC IDENTITY SOLUTIONS

Digital identity, with biometric components designed adequately, can lead to empowerment of underserved communities, while also allowing for cross jurisdiction exchange of data and services, spanning a wide range of activities and aspects of daily life.

- **Economic Community of West African States (ECOWAS) Biometric National Identity Card (ENBIC)** - The ENBIC[16] is expected to facilitate movement and business transactions among women and other vulnerable individuals in the border communities between Senegal and Guinea Bissau. The ECOWAS Commission intends to expand this offering to other member countries.
- **Electronic/Digital Civil Registration and Vital Statistics System (e-CRVS) Project** - The National Population Commission launched the e-CRVS[17] in partnership with the United Nations Children's Fund (UNICEF/WARCO) and the World Health Organization (WHO). The West and Central Africa region, and UNICEF Regional Office (WCARO) have also significantly advanced the digitalization of community health information systems across nine countries: Benin, Burkina Faso, Central African Republic (CAR), the Democratic Republic of the Congo (DRC), Liberia, Mali, Niger, Nigeria, and Sierra Leone.
- **The Ethipia Digital ID for Inclusion and Services Project (FAYDA)** - The World Bank financed the Ethiopia Digital ID for Inclusion and Services Project[18]. Fayda is built on the Digital Public Good platform MOSIP.
- **Digital Zambia Acceleration Project (DZAP)** - Funded by the World Bank this project also seeks to speed up Zambia's digital infrastructure development and improve Internet access and connectivity.[19] The goal is to promote inclusive access to the Internet and digital services.
- **Democratic Republic of Congo (DRC) Digital Transformation Project** - This project , also financed by the World Bank, aims to improve access to affordable and high-quality broadband connectivity, in addition to digital services, especially solutions with a high impact, and digital skills that are relevant to key industries.[20]

(1.4) NOTABLE USE CASES FOR DIGITAL ID

- **Humanitarian Assistance** - Digital identity of beneficiaries has increased access to aid funding for many and provision of funding in emergency situations, especially for unbanked populations. It also eliminated many bottlenecks that arise when attempting to make payments through different channels.
  – The United Nations High Commissioner for Refugees (UNHCR) has developed, in collaboration with the Stellar Organization "Stellar Aid Assist"[21], a blockchain-based application that enables the deposit of stablecoins[22] (USDC) into refugees' digital wallets. The application is equipped with biometric capabilities and mandates the provision of a government-issued ID or/ other forms of acceptable digital identification to ensure the authenticity of the beneficiary.
  – GBBC GIving, in partnership with the World Food Programme Innovation Accelerator, has developed the Food for Crisis joint initiative to track and trace donor funds, from donor to beneficiary, with blockchain technology and digital twins. Funds are traced using digital identifiers, and beneficiaries can also be validated with digital identifiers.
- **Environmental Impact** - Digital identifiers for workflows are also used to generate environmental impact. Digital identifiers of carbon credits enable a mechanism to create a marketplace for tokens enabling trade, exchange and burning. The use of blockchain technology can greatly improve trust and transparency in carbon markets.,

– The World Bank funds initiative[23] Carbon Assets Tracking System (CATS)[24] for low-carbon emission and emission tracking is an example. Of an emission reduction transaction registry.
– GBBC's InterWork Alliance has also developed an approach to a Carbon Emissions Token (CET) Protocol, using the Token Taxonomy Framework as a standard to define and guide the tokenization of emissions. The objective is to strengthen reporting of emissions with common guidance, specifications, and best practices of tokenizing carbon emissions.[25]

- **Farming and Agriculture** - Verified identities of farmers can greatly enhance their access to digital solutions.
  – With the support of a consortium of partners convened by USAID's Feed the Future Program, AgriFi provides rural farmers with digital extension and financial literacy workshops, increasing access to digital solutions. AgriFi is built on a unique blockchain infrastructure called ToroNet, specifically designed to solve real-world problems at scale. Toronet[26] aims to revolutionize farmers' market engagement and sovereignty by leveraging digitalization and smart contracts to create fairer, transparent, connected, and inclusive agricultural markets[27]. The project leverages the full power of tokenization, including zero-knowledge proof KYC technologies, to enable the creation of a digital yet verifiable business profile for farmers, solving the problem of access to capital, inputs, and offtake, all in one place. Aggregate lending pools powered by smart contracts enable farmers to get funded while providing industry-standard insurance and KYC solutions. The money from the lending pools can only be used by farmers to purchase the inputs needed for their crops. At the end of the harvest cycle, the off-takers sell the produce and credit the smart contracts that distribute the revenue to all parties involved.
- **Decentralized Finance (DeFi)** - The optimal function and scaling of DeFi will depend largely on a blockchain-based model of digital identity of participants that is decentralized and self-sovereign. This can provide the right balance between the need for anonymity and the right identifiers to ensure participants are legitimate actors. Individuals can have the burden of proof, providing their information voluntarily. In a self-managed approach, the type of data provided by individual participants can be the differentiating factor. An external party would have to certify the data provided by the individual. Regulatory developments and industry discussions are still underway regarding the role of central authorities and other key stakeholders in an ecosystem that seeks to preserve privacy and anonymity, while also defining adequate rules and requirements.
- **Global Identity Systems and Standards** - Data on individuals and entities can be utilized to carry out verifications, and then white list models to facilitate access to trust services. The importance of privacy preserving zero-trust architecture can be key in these scenarios. Common standards can also define best practices
  – The Legal Entity Identifier (LEI) is a 20-character, alpha-numeric code based on the ISO17442 standard developed by the International Organization for Standardization (ISO). The LEI uniquely identifies legal entities globally. It contains key reference information about the entity (e.g., its local registration number and registration authority, legal name, legal address, parent/child entity relationships, etc.), enabling clear and unique identification of legal entities globally. All users can access all the LEI reference data via the GLEIF website for free as an open database.

LEI COMMON DATA FILE FORMAT

- https://www.gleif.org/en/about-lei/common-data-file-format/current-versions/level-1-data-lei-cdf-3-1-format#
- https://www.gleif.org/en/about-lei/common-data-file-format/current-versions/level-2-data-relationship-record-rr-cdf-2-1-format#

- The Global LEI System is managed by the Global Legal Entity Identifier Foundation (GLEIF), established by the Financial Stability Board of G20 in 2014 as a Non-for-Profit Swiss Foundation. The Global LEI System is overseen by the Regulatory Oversight Committee of more than 65 regulators and 19 observers from 50 countries. Regulators mandate the LEI in global financial transactions. Currently, over 2.6 million entities in 200+ jurisdictions have LEIs.

(PART 2) DIGITAL PUBLIC INFRASTRUCTURE (DPI)

Large-scale deployments of digital identity projects mandate digital infrastructure development, maintenance, and operation. It is essential to consider this, as the state is often the primary sponsor and driver of digital identity initiatives. With technology advancements using public and private cloud infrastructure, it is now possible to design, build, and operate the necessary technology components that interplay to provide a robust consumer experience for digital identity and services associated with digital identity.

In recent years, the Digital Public Infrastructure (DPI) approach has found considerable success and adoption while designing the infrastructure for digital identity efforts. While there is no commonly accepted definition of "Digital Public Infrastructure", enough conceptual commonalities exist to help sponsors and stakeholders.

WHAT IS DPI?

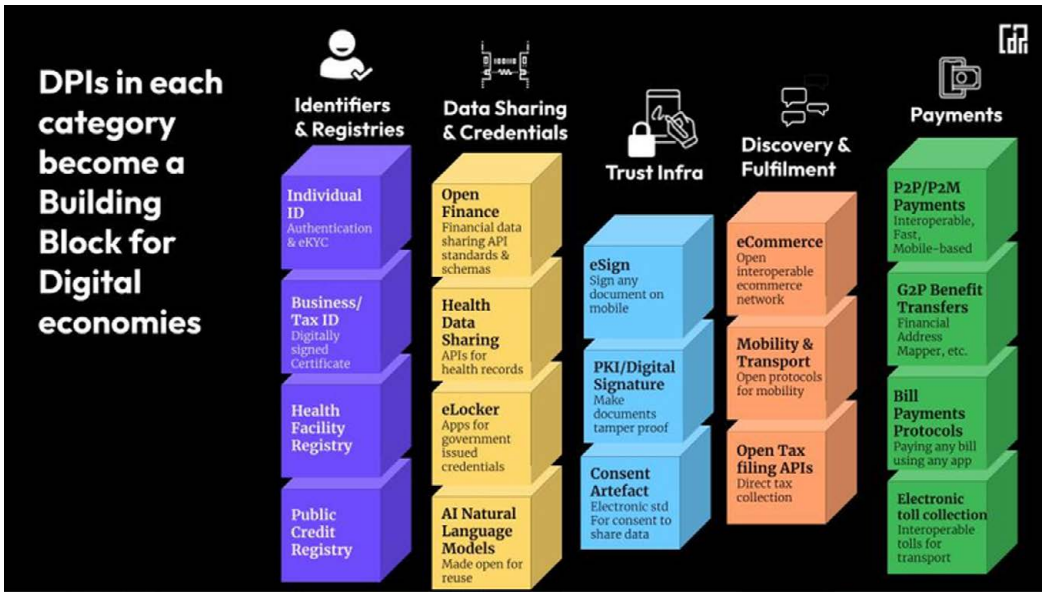
The Centre for Digital Public Infrastructure[28] mentions that **digital** does not require smartphones or connectivity to scale, **public**-minded yet still crafted to drive private innovation exponentially, and **infrastructure** is not just an app, a platform or a solution but a minimalist approach to build at a national scale.

According to the Centre for Digital Public Infrastructure:

Digital Public Infrastructure is an approach to solving socio-economic problems at scale, by combining minimalist technology interventions, public-private governance, and vibrant market innovation.

Common examples include the Internet, mobile networks, GPS, verifiable identity systems, interoperable payments networks, consented data sharing, open loop discovery and fulfillment networks, digital signatures, and beyond.

This perspective considers that digital public infrastructure (DPI) has core elements such as identifiers and registries, data sharing, credentials and data models, signatures and consent, discovery and fulfilment, and payments. These building blocks span all activities that emerge as possibilities for a robust and scalable digital identity deployment.



While specific digital identity projects can be open-source and can be a digital public good (DPG - like the open-source MOSIP infrastructure introduced above), the overall technology design which makes a good digital identity worthwhile is Digital Public Infrastructure (DPI). In the design pattern of DPI, the more traditional approach of "platforms" is transformed into "networks". This ensures that several interconnected and interoperable digital ecosystems can emerge using open standards, open-source software, open protocols and open networks.

The DPI approach fully uses digital identifiers and data registries, data exchange and processing (including AI/ML), trust infrastructure, digital payments and discovery and fulfilment. These are the building blocks, and blockchain and digital identity are the essential, foundational components of a DPI.

(2.1) DIGITAL IDENTITY AND REGISTRIES

Digital identities become meaningful and valuable when the holders can reuse, exchange, or share them to access various services. The data-centric dynamic economy is designed around the consent-based exchange of digital identities and metadata. The digital transformation from legacy systems to digital ones underscores the need to have "trust". This implies that relying parties can easily verify the digital identity using some authentication.

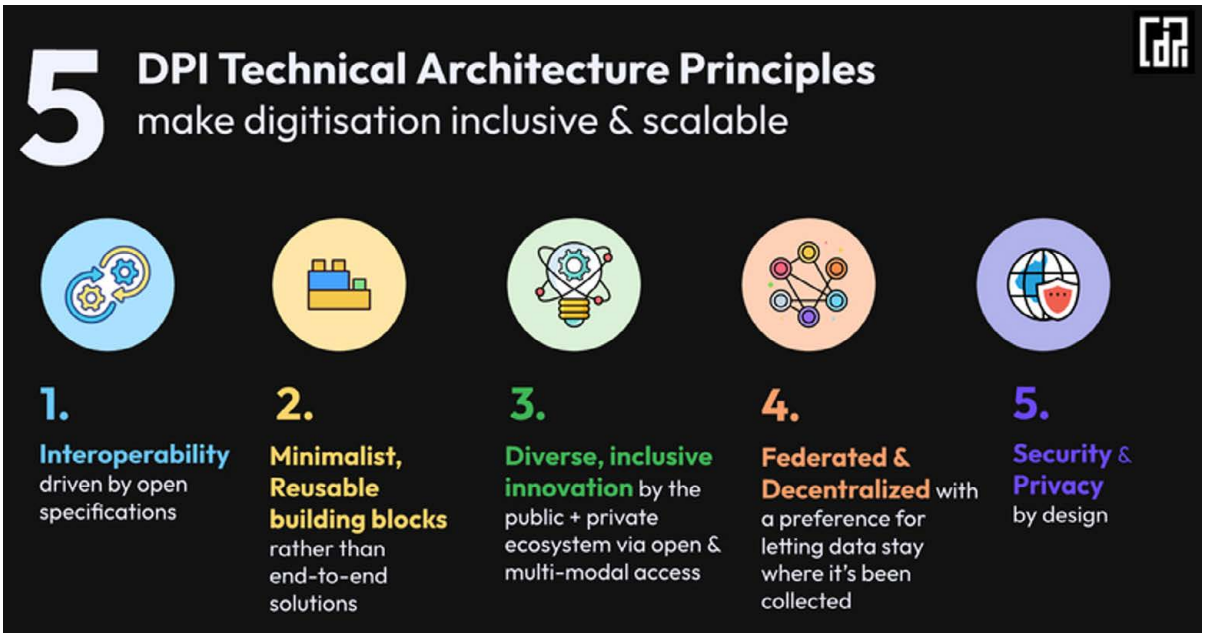
Additionally, as digital identities become more commonly used across sectors, it implies that issuers of digital identities maintain a registry of such digital identifiers. In some instances, such registries are publicly available, driven by the needs of the sectors and digital ecosystems. In other cases, these registries can be private or accessible only to authenticated and authorized entities. These decentralized digital registries, which contain digitally signed data, are a crucial driver to high-trust, low-cost consumption of digital identities for various purposes (such as authentication, KYC flows, civil registries, entity registries, etc.).

Many countries are adopting the DPI pattern when transforming services and building data registries, such as civil registries (of births and deaths), registries of attestors and notaries, and so forth. Some leading examples emerge from Brazil, Australia, Singapore, Switzerland, and others.

(2.2) PRINCIPLES OF DIGITAL PUBLIC INFRASTRUCTURE

Considering the emergence of Digital Public Infrastructure (DPI) as a preferred playbook or approach to deploying digital identity solutions, it is essential to examine some fundamental principles. Without a widely understood and commonly accepted definition of DPI, the principles provide a foundation for reviewing the merits of any digital identity infrastructure as a DPI.

The Centre for Digital Public Infrastructure has identified five principles that ensure digitization is inclusive, equitable, fair, and scalable. These principles are explained in the illustration below.



Digital identity systems should also demonstrate additional values that ensure they are designed to be user-centric and aligned with the requirements of the jurisdiction where the systems operate. Such values should include:

- Being human-centric to prevent unintended consequences or harm
- Focusing on informed consent to ensure that technology overreach is prevented
- Empowering innovation growth and fostering the UN Sustainable Development Goals

Digital Strategy of New South Wales (NSW)

For example, the government of New South Wales (NSW) announced a Digital Strategy[29], which focuses on delivering inclusive and secure digital services to improve residents' lives. The strategy is built around five missions:

- Accessibility - making digital services inclusive and accessible for all people in NSW
- Productivity - using digital transformation to advance service delivery
- Trust - sustainable digital infrastructure to build trust in government services
- Resilience - to deploy infrastructure that is resilient for emergencies
- Digital Skills - to uplift the digital capability in the public sector workforce

NSW has decided to create a NSW Digital ID and a NSW Digital Wallet to enable individuals to prove their identity while engaging in secure and safe digital data exchange. The enrolment workflow for

the NSW Digital ID requires two or more ID documents, a mobile number and an email address. The image/photo verification flow uses a selfie to match against an existing photo.

(2.3) DPI AS A BLUEPRINT FOR DIGITAL IDENTITY

Digital Public Infrastructure using modular, reusable components enables a blueprint that can be easily adopted and adapted to the needs of any given use case, or even a nation seeking to implement a digital identity system. This flexibility has resulted in improved economics, as many open-source projects can easily fit into the technology requirements of a DPI focused on extensible digital identities.

DPIs that adopt open standards and protocols can incubate an ecosystem of digital services that includes private and public sector participants. Adopting open standards is essential to achieving the stated goal of interoperability, particularly data interoperability, as successful scaled DPI deployments of digital identity depend on extensive data exchange systems being established.

Digital Public Infrastructure Model in the United States
The U.S. Digital Public Infrastructure has evolved over the years, and with the support of advanced technologies, the US was able to successfully link individual IDs (for e.g. Social Security Numbers (SSNs) and International Tax Identification Numbers (ITINs) issued by Homeland Security Department, and Internal Revenue Service, respectively) with nationwide repositories and databases to allow individuals to be identified, authenticated, and authorized to access basic digital ID services such as Financial Institutions / Banking system, housing, taxation, education and healthcare.

Legal entities and corporations selling and trading activities are also governed by different government identification mechanisms, such as Tax IDs and Employer Identification Numbers (EINs) issued by Internal Revenue Service, with the former being used to oversee movement in employment activities, and the latter to monitor transactions and for tax reporting purposes.

U.S. Customs and Border Protection (CBP) is one of the key agencies that regulates movement of persons, goods and products. It applies diverse and sophisticated technologies in key airports and customs ports to scan persons, goods and products using their digital ID and permit details. Some of the advanced technologies that CBP adopts include Persistent Surveillance; Mobile Surveillance; Cargo Gamma Ray and X-ray Scanners, and Biometric ID technologies. The CBP initially started at exploring the wider capabilities of DLT, and then diverted its attention to working on resolving the global interoperability challenge between various systems. As a result, CBP had recommended to the World Wide Web Consortium (W3C) two standards on interoperability: Decentralized Identifiers and Verifiable Credentials that were accepted by W3C as official web standards.[30] [31]

Digital Public Infrastructure Model in Italy: A European Case.
The Digital Public Infrastructure model adopted in Italy is a good example of how digital transformation using strategic imperatives results in the availability of impactful nation-scale systems.

Italy's digital transformation is driven by several strategic initiatives and infrastructure investments aimed at modernizing the country's economy and addressing its current digital gaps[32].

Italy's digital transformation push aligns with the European Union's broader objectives, including the Digital Agenda for Europe and the Recovery and Resilience Facility (RRF). Italy has earmarked

significant funds from the EU recovery funds to close the digital divide, modernize public administration, and promote innovation across industries. The National Recovery and Resilience Plan (PNRR), a key policy initiative, allocates billions towards digital transformation, with a focus on:

1. Digital infrastructure development (e.g., fiber optics, 5G networks, cloud platforms).
2. Industry 5.0 technologies such as AI, IoT, and robotics to modernize manufacturing, logistics, and other sectors (sustainability, ESG)
3. Encouraging small and medium enterprises (SMEs) to adopt digital tools to improve their operations

The European Digital Identity (EUDI) Regulation will revolutionize digital identity in the EU by enabling the creation of a universal, trustworthy, and secure European digital identity wallet. A digital identity guarantees all citizens a single authentication method and access to all digital services provided by public administrations and accredited private entities in Italy and Europe. The identification tools used to access online services are the SPID (Public Digital Identity System), the Electronic Identity Card and the National Service Card.[33]

Italy's digital infrastructure expansion is essential to enabling new technologies:

1. Fiber optic networks: Italy has been lagging behind other European countries regarding broadband coverage, but it's now scaling up investments to expand fiber-to-the-home (FTTH) networks, aiming to cover underserved areas and rural communities. Companies like TIM (Telecom Italia) and Open Fiber are leading in this area.
2. 5G networks: Italy has been rolling out 5G infrastructure, which will unlock opportunities for new services, including smart cities, connected vehicles, and advanced IoT applications.
3. Data centers and cloud computing: The Italian government is also investing in national cloud computing infrastructure, including the development of public-sector cloud solutions to support the digitalization of public services. This infrastructure will help Italy manage the growing demand for data processing, storage, and security.
4. Cybersecurity: As digital adoption increases, cybersecurity is a critical area of focus. Investments in secure infrastructure and cybersecurity solutions are being prioritized by both public and private sectors.

Incorporating Digital Public Goods (DPGs) alongside Digital Public Infrastructure (DPI) is highly relevant to the evolving digital landscape in Italy. Like many countries, Italy is leveraging digital tools and open technologies to foster innovation, improve public services, and support the United Nations' Sustainable Development Goals (SDGs). DPGs, which include open-source software, open data, AI models, open standards, and content, are playing a growing role in Italy's digital transformation.

- Italy's IO app is a prime example of a digital public good. It is an open-source platform that provides citizens with a unified interface to interact with public administration services. It allows access to a variety of public services like digital identity (SPID), digital certificates, and payments (PagoPA), fostering transparency and improving the accessibility of public services.
- PagoPA is another key open-source platform that modernizes how citizens interact with public administration for payments. It supports financial inclusion and facilitates transparent, efficient digital payments, which helps in advancing SDG 16 (Peace, Justice, and Strong Institutions).
- SPID (Public Digital Identity System). This is Italy's national digital identity system, which is interoperable and designed to enable citizens to access public and private services securely. The

SPID system is based on open standards and helps promote digital inclusion and accessibility, aligning with SDG 9 (Industry, Innovation, and Infrastructure).

Italy's Industry 5.0 plan incentivizes businesses to adopt advanced digital technologies to increase automation, efficiency, and competitiveness. Key opportunities include:

1. Cloud computing: As companies shift to cloud-based solutions, the demand for platforms that offer scalability, flexibility, and security has surged. Italy's cloud market is growing rapidly, driven by both SMEs and larger enterprises adopting Software as a Service (SaaS) and Infrastructure as a Service (IaaS) solutions.
2. Artificial Intelligence (AI) and Big Data: Italian companies and public administrations are increasingly adopting AI for automating processes, enhancing customer service, and making data-driven decisions. AI applications in sectors like healthcare, finance, and manufacturing are also growing.
3. Internet of Things (IoT): Italy is becoming a leader in IoT technologies, especially in the manufacturing sector, where connected devices help optimize production processes, predictive maintenance, and supply chain management.
4. Cybersecurity: The rise in digitalization increases vulnerability to cyber threats. Italy is expanding its investment in cybersecurity frameworks to protect both private and public institutions.

Regulations: The initiative to enhance Italy's public administration systems through investments in a national hybrid cloud infrastructure, referred to as the "Polo Strategico Nazionale" (National Strategic Hub), is a significant step towards modernizing Italy's digital ecosystem[34].

The primary aim of the Polo Strategico Nazionale is to ensure that all public administration systems, datasets, and applications are hosted in highly reliable data centers. This includes a focus on:

1. Security: Protecting sensitive government data from cyber threats
2. Performance: Ensuring quick and reliable access to services for citizens and businesses
3. Scalability Allowing for future growth and increased demand for digital services
4. Interoperability: Ensuring that different systems and datasets can work together seamlessly within the European framework
5. Energy Efficiency: Promoting sustainability through efficient energy use in data center operations

The investment in the Polo Strategico Nazionale represents a transformative effort to modernize Italy's public administration through a robust, secure, and efficient cloud infrastructure. By focusing on high standards of quality, security, and interoperability, Italy aims to create a resilient digital framework that will enhance public services and meet the growing demands of its citizens. This initiative not only addresses immediate needs for modernization but also positions Italy to thrive in the increasingly digital future, leveraging data as a strategic asset.

The Italian government has taken significant steps to promote Open Data by making public administration data accessible, reusable, and transparent for its citizens. These initiatives align with global trends towards openness and transparency in governance and are aimed at fostering innovation, accountability, and civic participation.

- Dati.gov.it is the official national portal for open data in Italy. Launched by the Agency for Digital Italy (AgID), this platform provides centralized access to datasets from various public administrations. It encourages the reuse of public data by developers, researchers, businesses, and citizens to foster innovation and create services that benefit society.

- OpenCoesione is an open data initiative focused on the transparency of public spending in Italy, particularly in projects funded by EU cohesion policy funds. The platform offers detailed information on how these funds are allocated, which projects they support, and the progress and outcomes of these projects.
- Italy has adopted a National Strategy for Data and Artificial Intelligence (AI)[35], which underscores the importance of open data in driving AI development and fostering innovation. By making public sector data open and accessible, the government aims to enable the development of AI solutions that can support public administration, healthcare, transportation, and other sectors.

Italy is an active member of the Open Government Partnership (OGP), an international platform for domestic reformers committed to making their governments more open, accountable, and responsive to citizens. As part of its OGP commitments, Italy has launched several open data initiatives aimed at enhancing public sector transparency and fostering citizen participation. The OGP action plans regularly focus on open data efforts, encouraging collaboration between public authorities and civil society to maximize the impact of open data on governance and public service delivery.

(2.4) UNLOCKING THE POTENTIAL OF DIGITAL IDENTITY THROUGH DPI GLOBALLY

Digital Identity projects developed using the DPI pattern have recently unlocked tremendous potential and created socio-economic opportunities. The table below provides an at-a-glance view of the impact from a region-specific view. Many use cases below utilize open-source technologies, such as X-Road - an open access software that facilitates unified and secure exchange of data across organizations.

Table: DPI and Digital Identity in selected jurisdictions

Country	DPI	Regulation	Primary Use Cases	Digital Identity	Digital Identity Regulations	Digital Identity Use Cases
Argentina	Argentina has made progress toward online government services with a single citizen-focused portal that consolidates solutions that were previously dispersed across systems.	While several laws and presidential decrees have been issued to reinforce digital services, the major guiding policy is the country's Digital Agenda. It defines policy goals toward digital government	Government services are still undergoing digital transformation.	The government of Argentina and the city of Buenos Aires have announced[36] the adoption of a QuarkID-based digital identity protocol to issue, manage, and exchange verifiable records. This is the first government-backed deployment of a decentralized identity model. The city of Buenos Aires is also adopting a blockchain-based SSI protocol within its digital identity app.	Argentina's Digital Signature Law is meant to regulate the use and legal validity of digital and electronic signatures, clarifying the conditions in which they are acceptable, as well as use of authentication methods and identity data used.	Records include such as civil registry records, proof of income, and learning and education credentials.

Brazil	The PIX instant payment system is one of the main DPI platforms in the country, with more than 100 million users. At the regional level, X-Road DPI infrastructure has been implemented in states such as Mato Grosso and Amapá.	Brazil has a legal framework for digital payments and has developed a robust digital authentication and data protection framework using PKI.	PIX has facilitated financial inclusion through instant payments, supporting social programs such as Auxílio Emergencial, which allowed the rapid opening of digital bank accounts.	The Gov.BR system has registered more than 150 million digitally authenticated users, facilitating access to public services.	The country has implemented personal data protection laws and has a PKI infrastructure for electronic signatures.	Gov.BR allows citizens to access more than 4,500 digital services, including authentication for opening bank accounts during the pandemic.
Chile	Chile has implemented a single authentication system for public officials, allowing secure access to various databases, including health databases.	The country has implemented regulations on data interoperability and advanced electronic signatures to support data exchange between agencies.	The interoperability system facilitates the efficient delivery of social services and data management between different government areas.	Digital authentication at the government level facilitating secure access to public services.	Chile has legislated on advanced electronic signature and interoperability of services, allowing for greater integration between agencies.	Digital identity is used to access government platforms that provide health, social assistance, and other essential services.
Colombia	Colombia has implemented X-Road to improve secure data exchange between government agencies and has used this platform to verify the beneficiaries of assistance programs.	The country has developed interoperability and digital authentication regulations, focusing on personal data protection.	During the pandemic, Colombia used X-Road to verify the eligibility of beneficiaries of social programs such as “Ingreso Solidario”, improving targeting and reducing fraud.	Colombia has implemented digital authentication to verify the identity of beneficiaries of social programs, such as “Ingreso Solidario”.	Colombia is strengthening its regulatory framework around the protection of personal data and interoperability of services.	The digital identity system was crucial during the pandemic because it used multiple databases to verify the eligibility of social program beneficiaries.

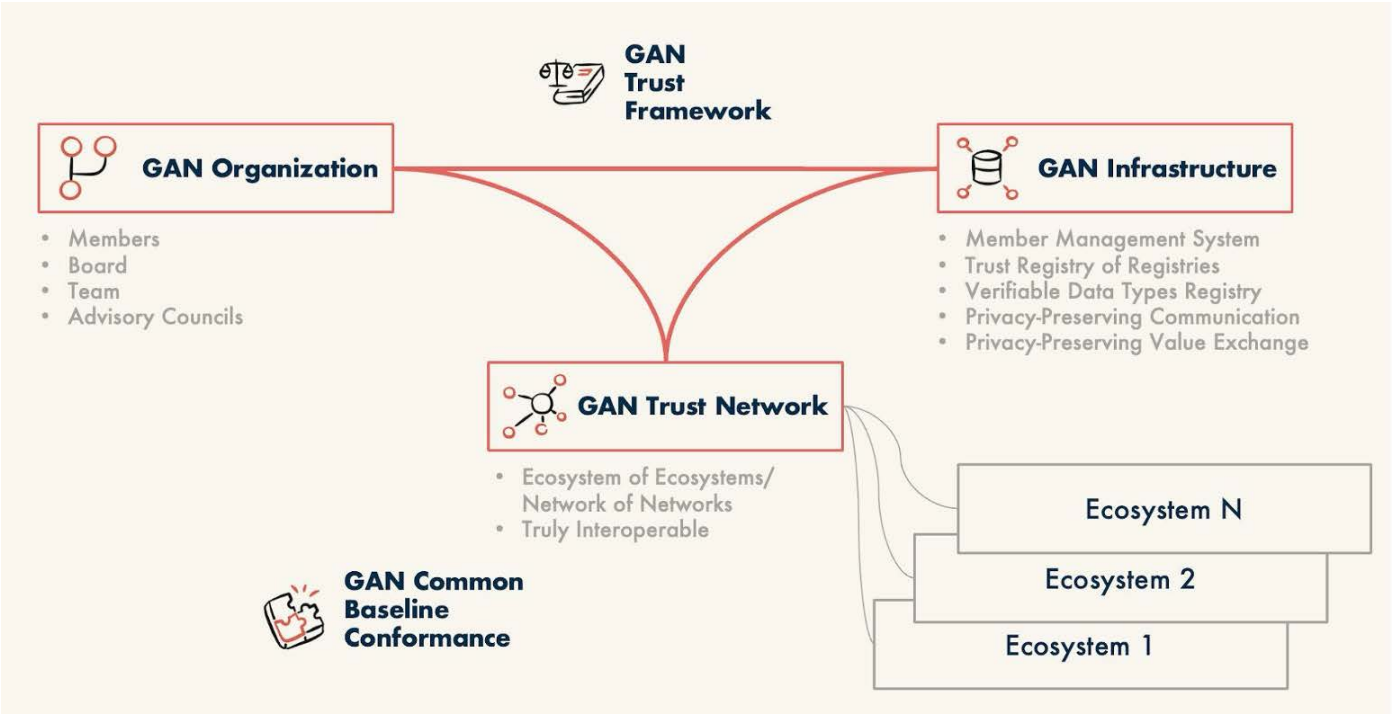
El Salvador	El Salvador has adopted X-Road through the Tenoli platform, allowing data exchange between government agencies. Moreover, as Bitcoin was made legal tender, a new class of DPI was announced to grant citizens access to USD and BTC, enabling holdings, sending, and receiving funds while prioritizing financial inclusion, interoperability and international trade.	El Salvador is working on regulations to strengthen interoperability and digital authentication within the public sector.	The Tenoli platform facilitates data interoperability between government agencies, improving efficiency in service delivery.	El Salvador is developing its digital identity system, which will allow authentication in public services, together with the Tenoli platform.	In the process of creating a regulatory framework that supports digital authentication and advanced electronic signatures.	Tenoli allows user authentication across multiple government agencies, facilitating the provision of services to citizens.
Estonia	Using the open-source data-sharing protocol X-Road, Estonian service providers can share user data in a secure way while still allowing changes to be recorded on the blockchain. This form of digital public infrastructure allows the government to provide its services more efficiently, securely and conveniently to citizens, forming the concept of a digital society e-Estonia. The unified platform allows citizens to see everything from their tax dues to their drivers license renewal date in one place. While the data is owned by each individual party, it is shown and made available to the user in a unified interface. When someone pays their taxes, renews their license, or buys a new house, that change is recorded by the tax authority, DMV, or Property registry, and that update is recorded on the blockchain. Because the update was recorded on blockchain, if there is ever a corruption or dispute about the data the DMV has, for example, the blockchain reference can be used to validate or invalidate truth from the timestamped event record.	Estonia became the first country to implement blockchain technology in its digital government services in 2012, and has leveraged it as a backbone of digital public infrastructure since. One of the key enabling factors of innovation in Estonia was their early adoption of bold regulation around digital services, such as the Principles of Estonian Information Policy. Establishing cornerstone legislation like the Digital Signature Act in 2000, which was updated in 2016, the requirements and protocols required for a Digital Signature to be legally binding were clear before any scaled infrastructure was established. This clarified technological requirements or uncertainty for new software providers or legacy businesses looking to provide legally binding services online. Similar such legislation in the EU such as Open Banking law and GDPR have consequently become pillars of directional clarity for the evolution of digital infrastructure.	As a layer of immutable data record, citizen activities interacting with public services including healthcare, land titling, taxes, and more, are all time stamped and recorded on a blockchain. The integration of x-roads and blockchain enable user-friendly and cohesive interaction points for citizens to access government services digitally.	All Estonians have access to a state-issued digital identity, the e-ID card. Alongside, the country has also offered a digital wallet to enable secure identification, digital signatures, and document storage on mobile devices.	The Identity Documents Act requires all residents, citizens or non-citizens, living permanently in Estonia to possess an identity document which includes a digital identity	The e-ID card is the cornerstone of Estonia's model of an e-state, embracing digital governance at its core, and all the services it provides digitally.

Guatemala	The Guatemalan government has committed to implementing a complete DPI system within the next five years as part of the "50 in 5" initiative[37].	Guatemala is developing legal frameworks for interoperability and digital authentication, including using advanced electronic signatures.	The system under development seeks to enable interoperability between agencies, facilitating the secure exchange of information.	The country is working on implementing an interoperable digital identity system to improve access to public services.	Guatemala is developing legal frameworks for digital authentication and interoperability of services.	Digital authentication will facilitate citizen access to multiple government platforms, allowing identity verification across various services.
Mexico	Mexico has implemented the instant interbank payment system (SPEI), which has been expanded with the CoDI platform for mobile payments.	The country has regulations on personal data protection and a framework for interoperability through PKI, applicable to both the public and private sectors.	SPEI and CoDI have transformed digital payments in Mexico, facilitating financial inclusion through interoperable platforms.	They are used for authentication in payment services and access to government platforms.	Personal data protection laws and a PKI infrastructure support the use of digital identity in Mexico.	Digital identity is essential for using CoDI, enabling instant payments and facilitating the integration of financial services.
Uruguay	Uruguay uses a centralized platform, managed by AGESIC, that facilitates data interoperability between government agencies.	Uruguay has an advanced regulatory framework for data interoperability and digital authentication, supported by its PKI infrastructure.	The "ID Uruguay" system allows citizens to access public services through a unique digital identity, improving service delivery digital identity.	The "ID Uruguay" system allows citizens to authenticate themselves to access public services digitally.	Uruguay has an advanced regulatory framework around digital identity, supported by its PKI infrastructure.	Digital authentication facilitates citizens' access to a wide range of public services, simplifying government procedures.

(PART 3) REGULATORY CONSIDERATIONS

Regulatory interventions are an essential driver for the wider adoption of digital identity. Robust frameworks for data governance, privacy, and citizen services provide the impetus for innovative approaches to reusing digital identity data.

In the last two years, many countries have introduced regulations along these lines, with the intent of enabling the efficient delivery of citizen services through digital public infrastructure. Organizations such as the Global Acceptance Network (GAN)[38], which focuses on enabling a sustainable layer of decentralised digital trust infrastructure, have also given this issue attention[39].



Approaches such as the one illustrated above envision the presence of public directories. This, in turn, implies the need for a decentralized directory protocol[40] - developed as part of the Finternet. The DeDi Protocol offers a standardized, open-source specification that can be integrated into existing or new systems. It aims to unify diverse implementations, ensuring interoperability and trust across the ecosystem.

In this section, we will introduce three examples of regulatory frameworks of digital identity and digital wallet systems, the Bhutan NDI, UAE framework, and EU eIDAS initiative. These are meant to present examples of how focused improvements in the regulatory environment have resulted in better infrastructure, standards, and deployments being made available to citizens.

UNITED ARAB EMIRATES

The Federal Authority for Identity, Citizenship, Customs & Port Security (ICP) is the main administrator of ID, customs authorities and border security services across the UAE. The Authority was established in September 2004 as ""Emirates Identity Authority"" under Federal Law No. (2) for the year 2004 to establish the "Population Register and Emirates Identity Card Program", which

included recording personal and vital data for all population in the state and keeping them in electronic databases in coordination with the competent authorities, and issuing the Emirates ID Card for each individual to be registered and to contain the Emirates ID number, readable data and data stored on an electronic chip, which can be used in all entities."

On the other hand, the main regulation governing Know Your Customer (KYC), Customer Due Diligence (CDD), Enhance Due Diligence (EDD), and Simplified Due Diligence (SDD) activities is Federal Decree Law No. 20 of 2018 on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT). To enable better execution of the law, the UAE Government has issued Cabinet Decision No. 10 of 2019, which provides further guidance on compliance expectations for KYC AML and CFT requirements. The Central Bank of UAE (CBUAE) has also issued "Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations" detailed guidelines for financial institutions for better understanding and clarity on the application of KYC, CDD, EDD, and SDD requirements.

It is also important to note that there are other KYC regulations that may be established by regulators located across the UAE (e.g., Abu Dhabi Global Markets, Virtual Assets Regulatory Authority, and a large number of other authorities); however, all these regulations are separate and do not contradict the spirit and approved direction of the aforementioned Federal laws.

Drivers for Digital Identity:

1. 1. ICP is the main custodian/driver for adopting Digital ID services specific to affirming persons and organizations legal status in the UAE, and customs and borders protection and security, and has established proper governance, controls and systems for these purposes and is constantly improving those to enable the transition to a highly efficient and effective ecosystem that caters to the needs of the millions living and organizations transacting in the UAE.

   Moreover, it gauged the interest of many semi-government and private sector entities in adopting Digital ID services to identify and verify persons and organizations. ICP also works with local agencies and departments that are focused on achieving digital enablement, and integration happens between its systems (e.g., UAE Pass) and local government agencies and departments' web applications.

2. CBUAE is the main custodian/driver for adopting Digital ID services specific to identifying, verifying and affirming persons and organizations financial diligence status (KYC, CDD, EDD, and SDD). It does so by ensuring all banking and financial sector actors comply with federal laws, decisions and regulations. Local regulatory authorities provide their Digital ID services while aligning with the expectations and requirements set forth by federal laws and overseen by the CBUAE.

BHUTAN NDI INITIATIVE[41]

The Kingdom of Bhutan launched a national digital identity[42] system in 2023 adopting SSI as a design pattern with which to develop a nation-scale digital trust ecosystem. Adopting the "Digital Trust Ecosystem Building Blocks" model proposed by the Trust Over IP Foundation (ToIP), the Bhutan NDI[43] includes trust registries, trust enabling systems, governance and ecosystem parties who participate in the system. The NDI Act of Bhutan[44], 2023 provides the overarching governance for the digital trust ecosystem.

It is important to understand that given the wide ranging impact of the NDI project, the stakeholders included the Department of Civil Registration and Census, the Department of Immigration and other agencies. The VCs issued as part of the project cover foundational digital identities and permanent address credentials as well as permits issued for tourism, residency and other purposes. The "trust registries" (NDI Trust Registry and Verifiable Data Registry) are enabled through the inclusion of a vLEI (Verifiable Legal Entity Identifier) issued to trusted parties. With organizations from a cross-section of institutions being involved in the NDI effort, the value is unlocked through the wider acceptance network achieved by including academic institutions, BFSI sector, Telcos and others.

At present the set of verifiable data which can be presently issued, exchanged and verified include foundational ID, permanent address credential, academic credential, employment related information, mobile number, driver's license, vehicle ownership etc. The NDI initiative also enables the creation of self-attested credentials which can be presented during eKYC workflows.

REGULATORY APPROACHES IN THE EU

EU eIDAS 2.0 Regulation

eIDAS 2.0 represents a significant upgrade to the European Union's electronic Identification, Authentication, and Trust Services (eIDAS) regulation. This enhancement aims to refine and expand cross-border digital identity solutions and trust services, allowing citizens and businesses to securely access a wide range of public and private services across the EU.

By enhancing trust services and website authentication, eIDAS 2.0 ensures that transactions across European Union Member States are secure and legally recognized, promoting greater trust, interoperability and reliability in digital interactions.

The three pillars of the regulation are the following:

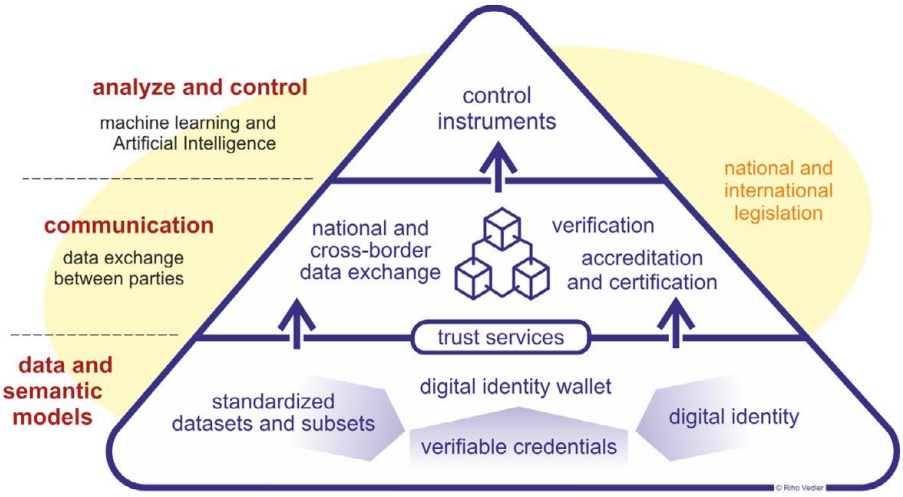
1. eID Schemas. Allows individuals to prove their identity digitally when accessing services. Each EU member state establishes these schemes and can vary in implementation but must comply with eIDAS standards for cross-border recognition. The eIDAS framework defines three levels of assurance for eID schemes:
   a. Low: Suitable for low-risk transactions, offering basic security.
   b. Substantial: Provides a higher level of security and is suitable for moderately sensitive transactions.
   c. High: Offers the highest level of assurance for high-risk or sensitive transactions, such as financial services.
2. EUDI Wallet. A secure, digital identity wallet solution enables citizens and businesses to store and manage their personal information, credentials1, and documents (e.g., ID, driver's license, banking details) in one place. It allows users to authenticate themselves and access online (trust) services across the EU, including cross-border services, without needing multiple logins or paper documents.
3. Trust Services. The legal framework is built upon acceptance, mutual recognition and equal conditions. Digital services that ensure the security, authenticity, and legal validity of electronic transactions.

In summary, key components include trust frameworks, legal recognition, a common set of rules and eIDAS cross-border standards, and legal recognition across Member States.

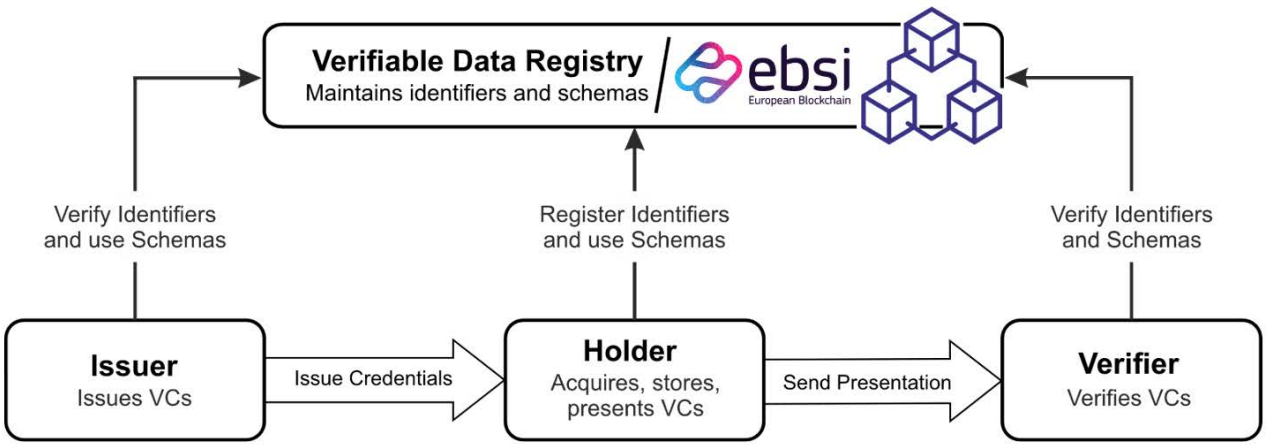
Categories of qualified trust services

- Electronic (digital) Signatures. An electronic way for a person to agree to a document or data. Qualified Electronic Signatures hold the same legal weight as handwritten ones.
- Electronic Seals. Like a traditional business stamp, it can be used on electronic documents to ensure their origin and integrity.
- Timestamps. Connects an electronic document, like a purchase order, to a specific time, proving the document existed then.
- Electronic Certificates. Electronic certificates that show your customers that your website is safe and reliable. They confirm the website is connected to the certificate holder and help prevent data phishing.
- Electronic Registered Delivery Services enable users to send data electronically. They offer proof of sending and delivery, safeguarding companies from loss, theft, damage, or unauthorized changes.

Technical infrastructure



Verifiable Credentials Data Exchange Model 2.0 and EBSI



This model developed by the W3C promotes trust data exchange (for B2C, B2B, B2G, and C2G), privacy, and data sovereignty, ensuring compliance with GDPR, Interoperable Europe Act and other regulatory frameworks. By EBSI supported verification service based on 'Zero Trust Architecture.

EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE AND BLOCKCHAIN NOTES

European Blockchain Services Infrastructure (EBSI) complements eIDAS 2.0 by enabling trusted, blockchain-based digital transactions, while EUDI ensures seamless identity verification. Together, they enhance secure cross-border digital interactions.

The EBSI comprises a peer-to-peer network of interconnected nodes running a blockchain-based services infrastructure. Each European Blockchain Partnership (EBP) member – the 27 EU countries, Norway, Liechtenstein and the European Commission – will run at least one node.

The infrastructure is made up of different layers, including:

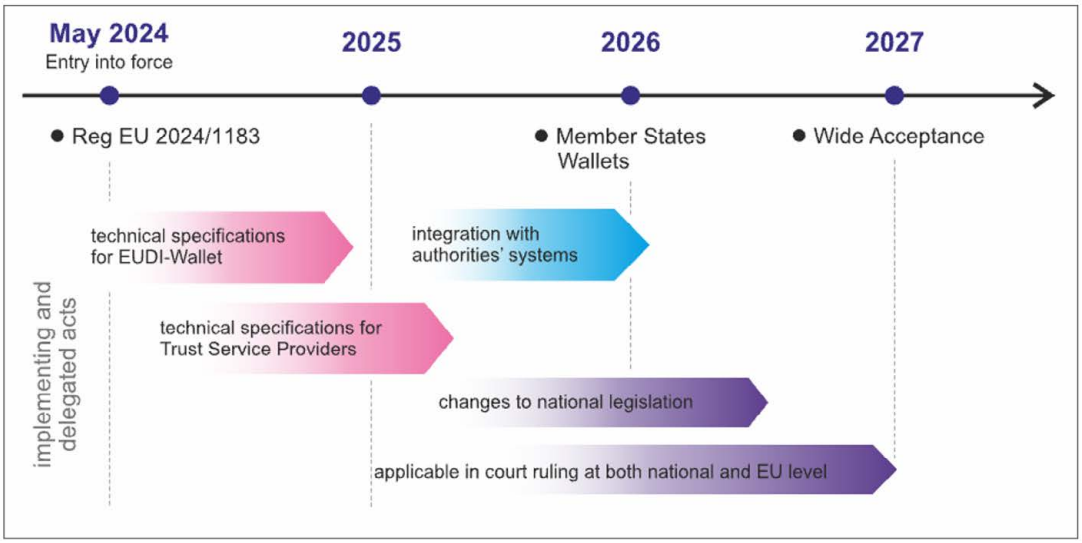
- a base layer containing the basic infrastructure, connectivity, the blockchain and necessary storage;
- a core services layer that will enable all EBSI-based use cases and applications;
- additional layers dedicated to use cases and specific applications.

POSSIBLE SERVICES TO BE DEVELOPED[45]

Generic relevant regulatory areas: AI, Environmental, Social & Governance (ESG), commercial registers, cybersecurity, consumer protection, competition law, customs, data protection & data regulation, Digital identity, Batteries/Digital product passports, Trade finance
Sector specific relevant regulatory areas: Automotive, cryptoassets, energy & utilities, education, financial markets, government, healthcare, media, retail, trade & logistics

- **Logistics, trade and trade finance.** eIDAS 2.0 with trust services (electronic signature, eSeal, etc.) enables seamless cross-border transactions by verifying identities, signing documents electronically, and securing data exchanges. This fosters smoother supply chain operations, efficient customs processing, and more secure trade finance, driving increased trust and transparency across these sectors.
- **Financial Services.** Speed up account opening by reusing existing verified identities. Improve KYC and fraud protection through richer identities.
- **Licenses.** Digital documents, such as identity and health documents, driving licenses, vehicle registration and voter cards, are always kept and carried in the safest and most convenient place possible.
- **eGovernment.** Increases efficiency and reduces manual processes by reducing in-person appointments. Automate data exchange between government agencies.
- **Travel & Hospitality.** Digitalize customer check-in and registration. Speed up processes and reduce manual labor through increased automation.
- **Mobility.** Automate customer onboarding and speed up driver license verification. Benefit of a European standard that works for various markets.
- **Telecommunications.** Speed up registration for prepaid cards by using existing verified identities. Improve fraud detection through richer identities.
- **eHealth.** Store health information and access other relevant information. Increase efficiency and effectiveness through reduced data handling and GDPR compliance.

Implementation indicative timeline



Source: DigitalTrade4.EU

eIDAS 2.0 was adopted by the European Parliament in February 2024 and is already published in the Official Journal of the EU. It entered into force on 20 May 2024.

- Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework https://eur-lex.europa.eu/eli/reg/2024/1183/oj

EU Member States must implement trust services within 24 months after the implementing legislation is adopted.

RELATED ACTS (EUDI WALLET)

Status: The public feedback period has ended (09 September 2024). After approval by the European Parliament, they will be published in the Official Journal of the European Union.

1. **Trust framework** [link]
   It aims to ensure that the electronic notification system established by the European Commission acts as a secure and transparent communication channel for exchanging information between the Commission and the Member States.
2. **Protocols and interfaces to be supported** [link]
   It aims to ensure the proper implementation of protocols and interfaces crucial for the effective operation of the wallets.
   By supporting common protocols and interfaces, the wallets can guarantee:
   - successful issuance and presentation of identification data and electronic attestations;
   - successful data sharing between wallet units; and
   - efficient communication with relevant parties.
3. **Integrity and core functionalities** [link]
   It aims to lay down rules to ensure that Member States provide wallets that are interoperable and can be used for all their intended purposes. For example, the wallets should enable:

- secure online cross-border identification for a wide range of public and private services;
- sharing of electronic attestations; and
- issuance of electronic signatures.

4. **Person identification data and electronic attestations of attributes** [link]
   It aims to ensure the smooth lifecycle management of both personal identification data and electronic attestations, covering issuance, verification, revocation and suspension. This guarantees that users' personal identification data and electronic attestations are issued to the wallet and can be disclosed to relevant parties.
5. **Certification** [link]
   This initiative aims to lay down the requirements for certification of the conformity of European Digital Identity Wallets. Where Member States cannot use European cybersecurity certification schemes based on Regulation (EU) 2019/881 or if such schemes are not sufficient, they must establish national certification schemes to supplement them. These schemes must, for instance, specify the competence requirements and an evaluation process.

RELATED ACTS (TRUST SERVICES)

Status: To be published 1 quarter 2025 to public feedback.

1. **Cross-border identity matching [link]**
2. **Security breaches [link]**
3. **Registration of relying parties [link]**
4. **Verification of electronic attestation of attributes [link]**
5. **List of certified wallets [link]**

(PART 4) RECOMMENDATIONS

Digital ID systems are making the leap from merely a digital identifier to a multi-purpose reusable set of identifiers that have significant impact on the lives of individuals and the workflows of organizations. To ensure that new technologies and capabilities are introduced while continuing to offer the benefits of a fair, equitable, secure and inclusive digital identity, it is important to examine the recommendations below.

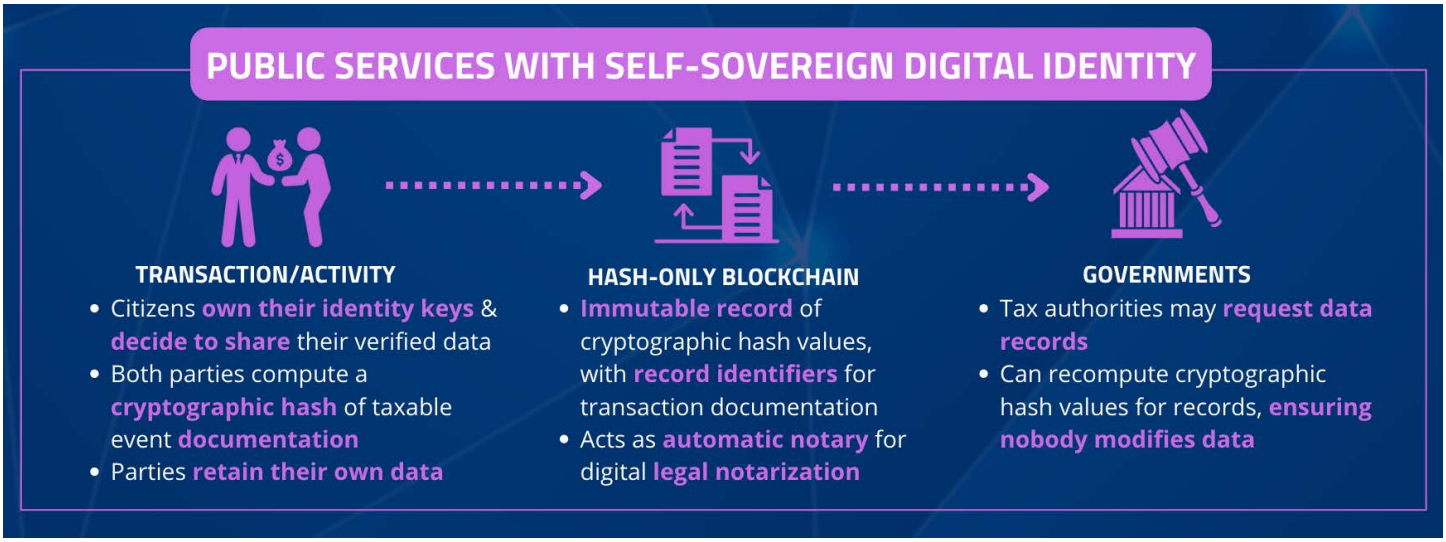
Recommendations for impact-driven Digital ID systems

- Adopt a Privacy-by-Design Approach
  - Incorporate privacy protections into the digital identity system from the outset, ensuring minimal data collection and anonymization where possible.
  - Allow users to control their data, with options to consent to sharing and revoke access at any time.
  - Encrypt sensitive information both at rest and in transit to prevent unauthorized access.
- Ensure Universal Accessibility and Inclusivity
  - Design the system to accommodate people of all abilities, including those with disabilities, low literacy levels, or limited technical skills.
  - Provide multilingual support and alternative offline registration options for individuals in remote or underserved areas.
  - Make participation voluntary and offer alternative forms of identification for those who opt out.

- Develop Robust Legal and Regulatory Frameworks
  - Establish clear laws that govern data protection, user rights, and the accountability of system operators.
  - Create mechanisms for independent oversight and redress in cases of misuse or grievances.
  - Define clear penalties for data breaches and misuse by government or private entities.
- Promote Interoperability and Open Standards
  - Use open standards to ensure the system can integrate with existing public and private services.
  - Enable cross-border recognition of digital identities for international travel and trade while maintaining national sovereignty over data.
  - Allow flexibility for future upgrades to keep pace with technological advancements.
- Implement Advanced Security Measures
  - Use multi-factor authentication to verify identity securely.
  - Employ biometric data cautiously, ensuring it is stored securely and used only for authentication purposes.
  - Conduct regular security audits and simulate potential attack scenarios to strengthen the system against threats.
- Address Digital Divide Challenges
  - Provide affordable and widespread access to necessary technology, such as smartphones or biometric devices.
  - Partner with local organizations to educate communities about the benefits and use of the digital identity system.
  - Invest in infrastructure improvements to support reliable internet connectivity in rural and remote areas.
- Foster Public Trust and Awareness
  - Engage communities through public consultations to ensure their needs and concerns are addressed in the system's design.
  - Be transparent about how the system works, what data is collected, and how it is used.
  - Run public awareness campaigns to inform citizens about the system's benefits and security measures.
- Guarantee Non-Discrimination and Equity
  - Conduct impact assessments to identify and mitigate risks of exclusion or bias in the system.
  - Avoid embedding discriminatory algorithms or practices that could marginalize vulnerable populations.
  - Ensure equitable treatment regardless of socioeconomic status, gender, ethnicity, or geographic location.
- Enable Decentralized and Federated Models
  - Explore decentralized digital identity architectures to reduce reliance on a single central authority and enhance resilience.
  - Use federated systems to allow individuals to use a single ID across multiple domains without risking privacy or security.
- Monitor, Evaluate, and Evolve the System
  - Set up mechanisms for continuous monitoring and evaluation to identify issues and areas for improvement.
  - Incorporate feedback loops to adapt the system based on user experience and technological developments.

Regularly update the system to incorporate advances in security, privacy, and inclusivity.

By adhering to these recommendations, policy makers, bureaucrats, technologists and other stakeholders can collaboratively develop a digital identity system that is fair, equitable, secure, and inclusive, fostering trust among users and contributing to societal advancement.



(PART 5) CONCLUSION

As societies globally continue to embrace digital transformation, digital identity systems are poised to play a central role in enabling secure access to services, fostering economic growth, and promoting social inclusion. These systems are evolving beyond mere identity verification to becoming dynamic platforms that integrate with a wide range of public and private services, from financial inclusion and healthcare to cross-border mobility and e-commerce. The trajectory of digital identity systems points toward greater interoperability, decentralization, and personalization, making them a cornerstone of modern digital economies.

Emerging trends indicate a growing emphasis on privacy-enhancing technologies (PETs) such as zero-knowledge proofs and decentralized identifiers (DIDs). These innovations aim to balance the dual imperatives of data security and user convenience, empowering individuals to control their digital identities while minimizing exposure to privacy risks. Additionally, artificial intelligence and machine learning are expected to refine the efficiency of identity verification processes, ensuring faster and more accurate authentication.

The integration of digital identity systems with blockchain technology is a promising development, offering immutable record-keeping and enhanced transparency. Furthermore, the rise of global standardization efforts suggests a future where digital identities can facilitate seamless cross-border interactions, unlocking new possibilities for international trade, migration, and cooperation.

However, this bright future comes with significant challenges and risks. One major concern is the potential for digital identity systems to exacerbate existing inequalities. Without equitable access, marginalized populations could face further exclusion from essential services. Similarly, the misuse of personal data, whether through data breaches or unwarranted surveillance, threatens individual privacy and public trust. Biometric data, while secure, raises ethical questions and must be handled with utmost care to avoid misuse.

Cybersecurity remains a persistent risk as attackers target digital identity infrastructures. Sophisticated cyberattacks could undermine the reliability of these systems and erode user confidence. Additionally, poorly designed or biased algorithms in identity verification could perpetuate discrimination, undermining efforts to create fair and inclusive systems.

The success of digital identity systems will depend on collaboration between governments, private entities, civil society, and international organizations. By working together, stakeholders can create systems that are not only secure and efficient but also inclusive and empowering. The opportunity to transform lives is immense—providing people with a digital identity can unlock access to opportunities, reduce barriers to participation, and drive innovation across sectors.

While challenges and risks are inevitable, the future of digital identity systems holds immense promise. By embracing a people-centric, privacy-preserving approach, these systems can serve as powerful tools for progress, bridging gaps and enabling a world where everyone has the opportunity to thrive in the digital era.

SECTION X

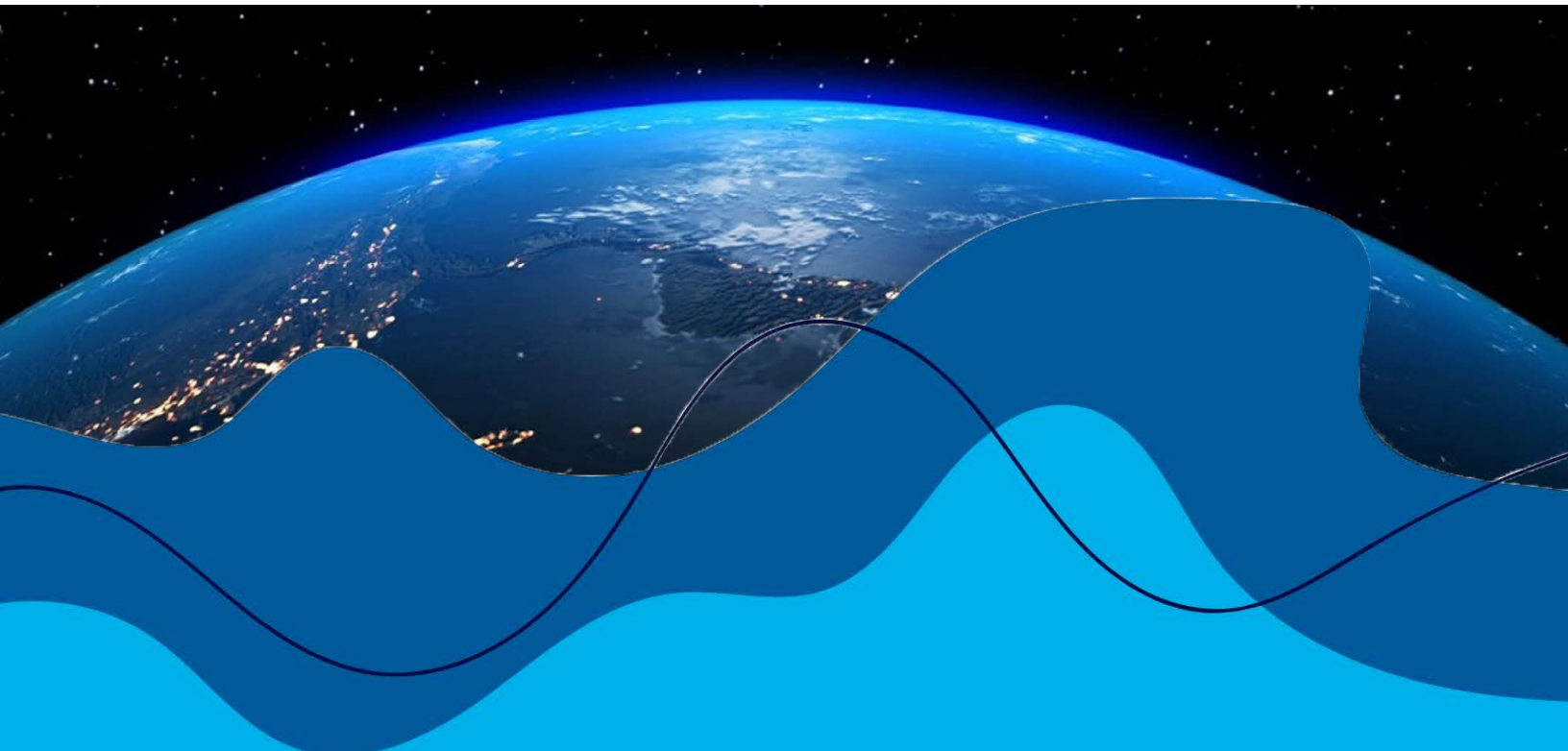
THE FUTURE OF GLOBAL SUPPLY CHAINS

GSMI 5.0 SUPPLY CHAIN – VISION

Our focus for GSMI 5.0 Supply Chain is from the International Space Station (ISS), e.g., from space. At this level, there are no companies, industries, or borders, and data knows no geographic borders. And yet, our standards entities have been built for centuries around just these items. The future of global supply chains is from this view, which will require harmonized, interoperable, and open standards, and will be a global digital ecosystem that seamlessly and instantly moves trillions of data elements around the world daily. The challenge? How do we get key stakeholders up to this level, so we can either:

1. Closely and quickly work to align the existing international standards entities currently each focused in their own lane, or,
2. Create a new digital trusted end-to-end and future-proof ecosystem.

We must simplify the processes of shipping, tracking, delivering, and returning goods, and we need to make it easy to use for all stakeholders and make financial sense. Today's systems, that are the best we have come up with so far, result in capital locked up, pollution, waste, delays, and vast resources, and they simply weren't designed at the truly global (ISS) level. This journey starts with harmonization and interoperability, which leads us to 'open' data standards, which leads us to



'digital' (including blockchain/Web3) and all of those are connected by centuries of network effects of trade, industrialization, and globalization that predict the inevitability of this outcome.

GSMI 5.0 SUPPLY CHAIN – EXECUTIVE SUMMARY

We believe that the future of global supply chains must depend on machine-verifiable (paperless) proofs to ensure the authenticity, legality, and origin of shipments. Achieving this vision requires standards that serve everyone—individuals, organizations, and nations—regardless of their size.

The purpose of this document is to evaluate the current landscape of global supply chain standards, assess our progress, and chart a path forward.

In our research, we identified over four hundred major standards organizations worldwide, collectively responsible for more than 60,000 published standards. While the volume of standards is not an issue, the challenge lies in understanding how they relate to each other, and determining which standards provide the best pathways toward inclusive and frictionless global supply chains.

A key initial contribution of this document is the distillation of over nine hundred data elements related to global shipments, drawn from the broad landscape of existing supply chain standards, into forty-eight fundamental data elements that capture the essential movement information. This simplification marks an important first step in harmonizing the data elements across standards. While key to pointing out the need for harmonization, it also became apparent that any such review of tens of thousands of standards in an attempt to harmonize would fail.

However, by pulling back out to the space level, our analysis focused on seventeen standards bodies that meet the World Trade Organization's (WTO) six criteria for global standards entities: transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and inclusion of developing countries. We evaluated these organizations based on their mission, industry focus, membership, number of published standards, and funding model. Our recommendation is to concentrate efforts on the ten standards organizations that provide open standards for digital documents, at no cost.

Data elements must be digital, so we also envision how digital identity, digital twins, sensors, blockchains and artificial intelligence can technically enable trusted and paperless global supply chains

BRIEF REVIEW OF GSMI 4.0 – SUPPLY CHAIN (2023)

To start, we used a simplified supply chain use case, where an everyday individual – let's call her Maria – ordered a gift online and, because it delivered late, had to figure out how to return it. With this initial Supply Chain effort, we started with an intentionally simplistic and normal example of something most people can do:

> ***'Maria ordered a birthday present online.'***

Unfortunately, the problem was that item arrived after the birthday party and Maria was thrown into the deep end of the global supply chain pool as she had to navigate trying to return it. What started as a simple example of a routine online purchase unfortunately turned into a late delivery, a

missed birthday gift, and then a return process that required navigating the complicated process of returning an international shipment.

What most people don't see in their everyday purchases is that when an item is initially purchased, there can be close to 50 steps to get that item from the website, across a border, to the point of delivery, and, as it turned out in our example, the reverse of that to get the item returned.

The working group then worked through the various modes of transportation, types of commerce, parties involved, data exchange, documentation, and, finally, the critical nature of the proxies of trust that have been used in these processes since trade began thousands of years ago.

Hundreds of data elements were identified involving the movement of goods, which were distilled down to about four dozen data elements most frequently used for global movement of goods, like shipper, receiver, broker, etc. Then, where possible, those items were mapped to their corresponding standards quickly pointing out that the standards could come from many different entities, and, in some cases, an entity pointed to another standards entity, making clear the case for harmonized standards in global commerce.

In this context, the International Chamber of Commerce (ICC) Digital Standards Initiative (DSI) has released Key Trade Documents and Data Elements (KTDDE), having published a parallel effort designated as the Minimum Data Elements. The standards body ASTM F49 also has a Committee for Essential Data Elements and has active work items that addressing the collection and normalization of common terms.

Table 1: Essential Data Elements for Global Movement of Goods

	Data Element	Description	Stan-dard	Free Form	Standard	Entity	WCO	DSI	OCB	CO	CI
1	Air Waybill/ Tracking #	Shipping document used for air cargo shipment that serves a contract between shipper and the airline, outlining the details of the shipment.	X		IATA 600a	IATA				X	X
					IATA 600b	IATA					
2	Broker	Intermediary who facilitates trade by negotiating transactions between buyers and sellers. In shipping, a customs broker assists with customs clearance.		X	UNTDED 3036	UNECE	X				
3	Buyer - Name	Entity or individual purchasing goods.		X	EDIFACT 3035	UNECE			X		

4	Buyer - Adress	Address for the entity or individual purchasing goods.		X	UNTDED 3164	UNECE			X		
5	Buyer - Trader ID (e.g., EORI)	Identifier of a party to which merchandise or services are sold.	X		EORI	EU			X		
6	Carrier	Organization or individual responsible for transporting goods from one location to another, such as an airline, shipping company or trucking company.		X	EDIFACT 3035	UNECE				X	
7	Commodity code (HS - Harmonized System code)	Standardized code from the Harmonized System used to classify products based on their nature and intended use.	X		WCO HS Code	WCO	X	X	X		
					UNTDED 7357	UNECE					
8	Consignee - Name (Buyer)	Entity or individual to whom the goods are being shipped or delivered.		X	UNTDED 3036	UNECE	X	X		X	X
9	Consignee - Address (Buyer)	Address of the entity or individual to whom the goods are being shipped or delivered.		X	UNTDED 3164	UNECE	X	X		X	X
10	Consignee - Contact info (Buyer)	Contact information of the entity or individual to whom the goods are being shipped or delivered.		X	UNTDED 3412	UNECE	X			X	X
11	Consignor/ Shipper - Name (Seller)	Entity or individual who is shipping or sending the goods.		X	UNTDED 3036	UNECE	X		X	X	X
12	Consignor/ Shipper - Address (Seller)	Address of the entity or individual who is shipping or sending the goods.		X	UNTDED 3164	UNECE	X		X	X	X

13	Consignor/ Shipper - Contact (Seller)	Contact information of the entity or individual who is shipping or sending the goods.		X	UNTDED 3412	UNECE	X		X	X	X
14	Country code/ Country of origin	Code representing a specific country.	X		ISO 3166	ISO	X	X	X	X	
					EDIFACT 3207	UNECE					
15	Country of export	Country from which the goods are being exported.	X		ISO 3166	ISO			X		X
					EDIFACT 3207	UNECE					
16	Country of manu-facture	Country where the goods were produced or manufactured.	X		ISO 3166	ISO					X
					EDIFACT 3207	UNECE					
17	Country of ultimate destination	Country where the goods are ultimately intended to be delivered or used.	X		ISO 3166	ISO					X
					EDIFACT 3207	UNECE					
18	Currency	Medium of exchange used for financial transactions	X		ISO 4217	ISO	X		X		
					EDIFACT 6345	UNECE					
19	Dimension	Size, measurements, or physical attributes of a product of package, such as length, width, and height.		X	UNTDED 6168	UNECE	X		X		
20	Export Reference #	Unique reference number or code associated with an export transaction for tracking and documentation purposes.		X	Free form	NONE					X
21	Exportation - Date (YYYY-MM-DD)	Date on which the goods are officially exported from one country to another.	X		ISO 8601	ISO					X
					UNTDED 2380	UNECE					

22	Exporter - Name	Entity or individual responsible for shipping goods from one country to another.		X	UNTDED 3036	UNECE			X	X	X
23	Exporter - Address	Address of the entity or individual responsible for shipping goods from one country to another.		X	UNTDED 3164	UNECE			X	X	X
24	Exporter - Contact info	Contact information of the entity or individual responsible for shipping goods from one country to another.		X	UNTDED 3412	UNECE			X	X	X
25	Full description of goods	Detailed and comprehensive description of the products being shipped, including their characteristics, quantity, and specifications.		X	UNTDED 7008	UNECE			X	X	X
26	Goods Passport ID (GPID)	Unique identifier or code for tracking and tracing specific goods.		X	Open Customs Blockchain	OCB			X		
27	Gross Weight (kg) / Total weight	Total weight of the goods, including their packaging and any other materials.		X	Int'l System of Units (SI)	ISO		X		X	X
28	HS Subheading Code (Commodity Code/ Binding Tariff Reference ID)	More detailed level of classification within the Harmonized System, providing a specific code for certain types of products.	X		WCO HS Code	WCO			X		
					UNTDED 7140	UNECE					
29	Importer	Entity or individual responsible for bringing goods into a country from another.		X	UNTDED 3036	UNECE	X				

30	Invoice - Number	Unique identifier for the commercial invoice associated with a shipment.		X	UNTDED 1004	UNECE	X	X	X		
31	Manufacturer	Entity or individual responsible for producing or manufacturing the goods.		X	UNTDED 3036	UNECE	X				
32	Net Weight/ Net Mass	Weight of the goods after deducting the weight of packaging and other materials.		X	Int'l System of Units (SI)	UNECE			X		
33	Owner	Legal entity or individual with ownership or legal rights over the goods.		X	UNTDED 3036	UNECE					
34	Payer	Entity or individual responsible for making payments related to the shipment, such as freight charges or customs duties.		X	UNTDED 3036	UNECE	X				
35	Pieces/ Number of packages	Quantity of individual items or packages being shipped.		X	UNTDED 7224	UNECE				X	X
36	Preferential origin	Country where the goods qualify for preferential tariff treatment under a trade agreement.		X	ISO 3166 EDIFACT 3207	ISO UNECE			X		
37	Quantity (# of items)	Number of amount of a specific item or product being shipped.		X	ISO 7372 UNTDED 6060	ISO UNECE			X		X

38	Seller - Name	Entity or individual selling the goods.		x	UNTDED 3036	UNECE			x		
39	Seller - Address	Address for the entity or individual selling the goods.		x	UNTDED 3164	UNECE			x		
40	Seller - Trader ID (e.g., EORI)	Identifier used in the EU for economic operators engaged in international trade, including importers, exporters, and customs agents. The EORI is a unique code assigned to facilitate customs procedures and ensure smooth and efficient trade within the EU.	x		UNTDED 3036	EU			x		
41	Sequence number	Unique numerical or alphanumerical identifier used for tracking and reference purposes.		x	UNTDED 1050	UNECE			x		
42	Ship date	Date on which the goods are shipped or dispatched.	x		ISO 8601	ISO				x	
					UNTDED 2380	UNECE					
43	Terms (F.O.B., C&F, C.I.F.)	Standardized trade terms that define the responsibilities and obligations of the buyer and seller.	x		EDIFACT 4053	UNECE	x				x
					INCOTERMS	ICC					
44	Total invoice value	Total value of the goods as indicated on the Commercial Invoice (CI).		x	ISO 4217	ISO	x	x	x		x

45	Transport document number	Unique identifier associated with the document used for shipping and transporting goods.		X	UNTDED 1004	UNECE		X			
46	Type of packaging / Handling Units	Specific packaging or packaging materials used to contain and protect goods during shipping.		X	EDIFACT 7065	UNECE	X	X			X
47	Unit of measure	Standard unit used to express the quantity or measurement of goods, such as kilograms, liters, or pieces.		X	Int'l System of Units (SI)	UNECE					X
48	Unit value	Value of a single unit of a product (e.g., the cost per kilogram or per item).		X	ISO 4217	ISO					X
					INCOTERMS	ICC					

Key Words

- **WCO - World Customs Organization**
- **DSI - Digital Standards Initiative**
- **OCB - Open Customs Blockchain**
- **CO - Certificate of Origin**
- **CO - Certificate of Origin**

"While thousands of years of trade have led us to the global supply chain of today, blockchain and emerging technologies are leading us to a future where paperless trade can become a reality, transforming industry and regulatory processes, and entire industries. That is why GBBC's BITA initiative has come to fruition, bringing together major global logistics and transportation stakeholders to thoughtful adoption of Web3 innovations toward a new generation of global commerce that can finally adopt an "International Space Station" view. BITA is working as a global harmonizer for open data standards in global commerce."

INTERNATIONAL SPACE STATION VIEW ON STANDARDS

In the process from buying to shipping to payment for any item, there are vast amounts of documentation exchanged. Standards are meant to facilitate global commerce through harmonization of processes. There are over four hundred major standards organizations worldwide, when combining international (about 10-20), regional (about10-15), national (about 160 – many are National Representative bodies of International Groups), and industry specific (several hundred). Just from the international standards entities, we have approximately 60,000 published standards. It is important to note, we are not lacking for published standards. We are lacking in harmonized, interoperable, and open standards with a truly global, particularly a global commerce, focus. We are also lacking in the language, or data-organization that can harmonize standards.

We will later discuss the definition of a standard, and the six principles set by the World Trade Organization (WTO), as requirements for global standards entities. Out of the vast landscape of standards bodies, the working group identified that there are currently less than twenty standards organizations that rise to that WTO level, meaning that they can be considered to meet the six principles for global standards. These are the entities we will review and compare in later sections. Those entities represent more than 150 years of 'standards' development, during which the world has continually evolved, including massive changes in technology. One thing immediately clear is that each of those entities has done excellent work, and they were each created for a specific reason, staffed by committed leaders in the industry.

When it comes to global harmonization, there historically has been little focus on overlaps at that International Space Station level. The goal at hand is to align silos of the standards world in support of open, interoperable, and harmonized global standards for international commerce.

With this review, it is also becoming clear that there are a couple of splits taking place in the international standards arena:

- There is a division between 'legacy,' (paper/document) vs. 'digital' (post-document), e.g., for global commerce, the 'legacy' could be thought of as the rear-view mirror, and the 'digital' could be considered the windshield.
- There is also a division between fee-based standards entities and those entities which have opened their standards for use by all. As we explore the need for harmonization, it leads us to the critical importance of 'open' (non-fee-based) standards. For true harmonization, interoperability, integration, speed, and reduced friction in global commerce, what will scale globally is open standards.

Once we get to 'open,' this really becomes a discussion about 'digital,' which is to say, a post-document (paperless) global supply chain. Many systems today utilize AI-enabled Optical Character Recognition (OCR) solutions to digitize documents and data entries While helpful to automate, simply translating a data element from a paper document into a digital format might be a step in the right direction, it doesn't connect directly to the source of that data. When data elements from existing documents can be identified down to the source, we will evolve beyond the dozens and hundreds of movement documents we have used for millennia as proxies for trust, and then we can rethink (digitalize) the processes. Once we digitize, we also get to things like digital identity, blockchain, sensors, AI and other existing and yet-to-be-developed critical emerging technologies that will transform global supply chains in the future. Open is also achieved by a decentralized, shared environment of digital data called blockchain.

Standards are an important piece of streamlining global commerce; however, there are other key components that have brought us to this point and will take us forward. Standards propel a 'network effect' which is also a key part of this discussion. Network effects have been seen before in many ways, from the earliest days of trade to the Industrial Revolution, to Globalization in the 20th Century, to now the Digital Revolution and beyond. The role we all play in embracing the global nature of what got us here, and the key impact of technology moving forward, is critical. From the space viewstandards, technology, and emerging governance models, along with existing government and regulatory components, must work for all parties, public and private, large, and small, and they must be both open and interoperable.

HISTORICAL PERSPECTIVE: WHAT IS A 'STANDARD'?

Standards have been around since the Egyptians (~3000 BCE), they exist in every aspect of our society and is it inevitable that we must work together on open, harmonized, and interoperable standards for global commerce to continue to scale with emerging digital technologies. The discussion of 'Standards' is the first specific reference of 'network effect,' but we will revisit it in other areas of this work.

Just to put a definition out there for context for this effort, standards are a formalized set of guidelines, technical specifications, or established criteria designed to ensure consistency, safety, quality, and interoperability across a given activity, product, or process.

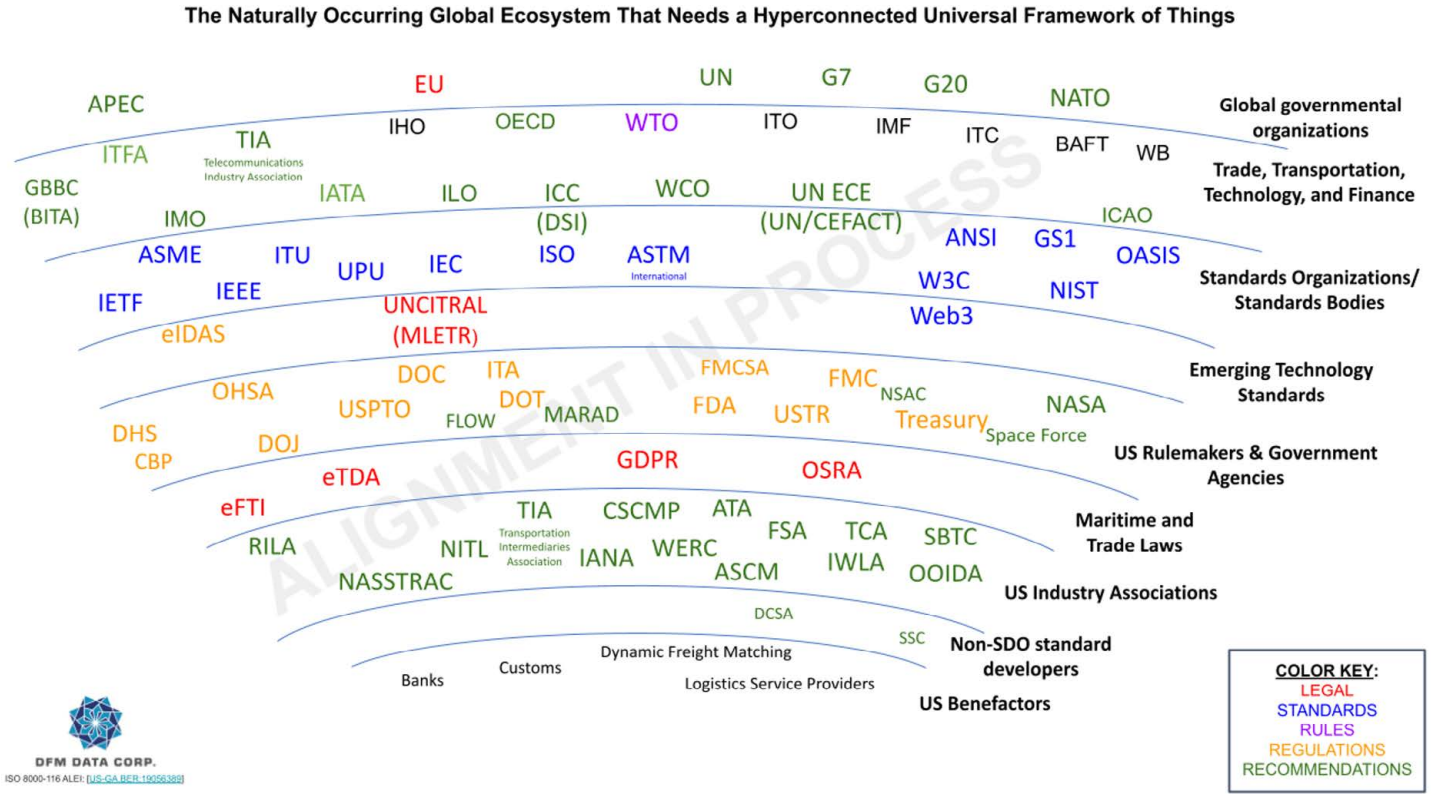
One of the earliest standards was in Egypt thousands of years ago and was the length of the forearm from elbow to the tip of the middle finger, called a 'cubit,' and it helped to standardize construction of the pyramids and other things in ancient Egypt. As society and technology developed, we then saw standardization of commercial transactions, weights, and measures in Babylon (~1750 BCE), road construction in Rome (~500 BCE), quality standards by guilds in Europe (12th century), and the metric system in 1799. By the mid 1800's, we saw standards for railroad track width, and the early 1900's brought us airline and automotive industries and standards, and now we chronologically overlap with the current International Standards Development Organizations (ISDO).

Of the group of ISDO's we will review, the International Telecommunication Union (ITU) was established in 1865, and then we see the Universal Postal Union (UPU) in 1874, and, over the next century or so, the others in our review were established including the International Standards Organization (ISO) in 1947, all the way to UN/CEFACT in 1996. Multiple entities like these were established during and after WWII (ICAO-1944, IATA-1945, ISO-1947, IMO-1948, WCO-1952).

Standards have always reflected the time, measuring the length of a typical arm – cubit – in ancient Egypt, to increasingly sophisticated uses around railroad track width 150 years ago, to safety and interoperability, to currently envisioning a document-free (paperless, digital) global supply chain. The network effect is such that each additional user makes the network more valuable to all existing users, and the associated reduction in friction leads to the inevitability of open and interoperable standards for the global supply chain on the horizon.

STANDARDS LANDSCAPE TODAY

The international standards community has spent a great deal of time mapping the various standards globally, as well as effective governance models to coordinate standards bodies. Below is a standards map referred to as 'The Onion,' produced and developed through collaboration in the DFM Data Corp Transport Unit Identifier (TUID) Working Group. This shows the various layers of standards entities and gives us a visual sense of these entities along with our International Space Station analogy. We will be focusing on the international standards entities in the third layer from the top (Standards Organizations/Standards Bodies) and those entities just above that line.



- Like a view from the ISS, this graphic starts at the global organizations level with ITFA, EU, G7, G20, WTO, UN, and NATO, which leads us to trade, transportation, technology, and finance entities.
- We then get down to our current focus area of International Standards Development Organizations, such as IEEE, ISO, etc.
- Next is Emerging Technology Standards, and then we get to additional layers around US Rule makers & Government Agencies, Maritime Laws, US Industry Associations, and Non-SDO Standard Developers in the US.

Even with this graphic doing its best to categorize these key entities, it is still apparent that each of these entities was created separately, over the last 150 years, all with acronyms we may or may not be familiar with, and this is an incredibly fragmented discussion around standards. Each of these entities tried to make sense (through standards) of an industry or country or type of movement (Customs, etc.), or other segments. They are all excellent examples of 'Best in Class' over the last 150 years, but at the ISS level, we see dozens of these across industry and geography with little to no common focus around open and interoperable global movement, such as what we currently see in e-Commerce (B2C, Business-to-Consumer) examples. We saw this extremely fragmented view at its worst during the Covid pandemic where a product wasn't on the shelf, or ships were stuck at a port, etc., which exaggerated the already elevated levels of friction (documents, resources, delays) to move products across borders. What we need is a global commerce focus on standards, and not just any one industry or segment, and it must embrace harmonized, interoperable, and open digital standards. Some international standards entities created after WWII are a snapshot of what supply chains looked like 75 years ago, prior to the 'digital' discussion, or even the internet.

KEY INTERNATIONAL STANDARDS DEVELOPMENT ORGANIZATIONS

The six **WTO/TBT (Technical Barriers to Trade)** principles required for global standards entities, which encompass what a standard should convey, are the following:

1. **Transparency:** All essential information regarding current work programs, as well as proposals for standards, guides, and recommendations under consideration and progress reports on the work programs, should be accessible to all interested parties.

2. **Openness:** Membership of an international standardizing body should be open on a non-discriminatory basis to relevant bodies of at least all WTO members.

3. **Impartiality & Consensus:** All relevant bodies should be provided with meaningful opportunities to contribute to the development of international standards, guides, and recommendations. The procedures should not give privilege to, or favor the interests of, any particular supplier, country, or region.

4. **Effectiveness & Relevance:** International standards need to be relevant and effectively respond to regulatory and market needs, as well as scientific and technological developments.

5. **Coherence:** In order to avoid the development of conflicting international standards, it is important that international standardizing bodies avoid duplication or, or overlap with, the work of other international standardizing bodies.

6. **Development Dimension:** Constraints on developing countries' effective participation in standards development should be addressed. The development dimension should be taken into consideration in the development of international standards.

Using these principles as a reference in addition to the Onion graphic above, a deeper dive into the key International Standards Development Organizations relevant for global supply listed is illustrated below. These organizations are listed in chronological order of when they were established.

Collectively, they represent approximately 60,000 standards, or the equivalent (ILO 'conventions,' UN/CEFACT 'recommendations' included).

With the goal of identifying common concepts across standards, the working group assessed the purpose of these standards in terms of what they are meant to accomplish, along with the portion of "movement" covered by them, based on the common data elements identified for all physical shipments (e.g., import/export, customs, sellers/buyers, point of origination, point of destination, etc.), industry focus, and level of adoption as defined by global presence and number of standards. Importantly, these standards entities were analyzed based on whether they offer freely available or open-source standards, as opposed to a more traditional model of selling access to standards for a fee. This led to an assessment of alternative revenue models for those entities that make their standards freely available. Standards setting entities were also categorized for being traditional document-based or digital-first.

Table 2: International Standards Development Organizations Reviewed

Organization	Year Esta-blished	Mission/ Purpose	Industry	# of Members	# of Standards	Fee-based or Open Standards	Document or Digital-based Standards	Link
ITU - International Telecommunication Union	1865	Coordinate global telecom standards, spectrum management	Telecommu-nications	193 Member States	4,000+	Open	Document, Digital	ITU
UPU - Universal Postal Union	1874	Foster the global postal system	Postal services	192 Member States	~200	Open	Document	UPU
ASME - American Society of Mechanical Engineers	1880	Advance engineering standards and practices	Engineering, (Mechanical)	~90,000	~600	Fee	Document	ASME
ASTM International - (Originally, American Society for Testing and Materials International)	1898	Develop and deliver voluntary consensus standards	General Idustry	30,000+	~12,800	Fee	Document	ASTM

IEC - International Electrotechnical Commission	1906	Develop international standards for electrical and electronic technologies	Electro-technology	~170 countries	~10,000	Fee	Document	IEC
ILO - International Labor Organization	1919	Promote labor standards, decent work, and social protection	Labor & Employment	187 countries	190 conven-tons	Open	Document	ILO
ICC - International Chamber of Commerce	1919	Develop international business standards and promote global trade	Global trade	100+ countries	~100	Fee	Document	ICC
ICAO - International Civil Aviation Organization	1944	Develop and enforce international civil aviation standards	Aviation	193 countries	~12,000	Fee	Document, Digital	ICAO
IATA - International Air Transport Association	1945	Represent and serve the airline industry through standards	Aviation	~300 airlines	~100	Open	Document	IATA
ISO - International Organization for Standardization	1947	Develop and publish international standards for a wide range of industries	General industry	167 countries	~24,000	Fee	Document	ISO

IMO - International Maritime Organization	1948	To set standards for the safety, security, and environmental performance of international shipping	Maritime	175 countries	60 Conventions	Open	Document	IMO
WCO - World Customs Oganization	1952	Develop global customs standards for the international trade	Customs	183 countries	Multiple	Open	Document	WCO
IEEE - Institute of Electrical and Electronics Engineers	1963	Foster technological innovation and excellence	Electrical, electronics, IT	~425,000	~1,300	Fee	Document	IEEE
GS1 - (Originally, Global Standards 1)	1973	Develop global standards for business communication	Retail, supply chain	115 national chapters	~150	Fee	Digital	GS1
IEEE - Institute of Electrical and Electronics Engineers	1963	Foster technological innovation and excellence	Technology	~425,000	~1,300	Fee	Document	IEEE
GS1	1974	Develop global standards for business communication	Supply Chain	115 National Chapters	~150	Fee	Digital	GS1

IETF - Internet Engineering Task Force	1986	Develop voluntary internet standards	Internet	Open community	~1000	Open	Digital	IETF
OASIS - Organization for the Advancement of Structured Information Standards	1993	Promote the development of open standards for the global information society	Information Technology	~600 organizations	~150	Open	Digital	OASIS
W3C - World Wide Web Consortium	1994	Develop open web standards	Web Technology	~450 Members	~500	Open	Digital	W3C
UN/CEFACT - United Nations Centre for Trade Facilitation and Electronic Business	1996	Develop trade facilitation recomm-endations and e-business standards	Trade facilitation	~60 counties	Multiple recomme-ndations	Open	Digital	UN/ CEFACT

INITIAL TAKE-AWAYS:

- Ten of the seventeen entities analyzed have 'open' standards.
- Seven of the seventeen entities are 'digital-based' standards, and six of those seven have open standards.
- Chronologically, all but two that are digital (5 of 7, all since 1971) are the most recent entities established (GS1-1973, IETF-1986, OASIS-1993, W3C-1994, UN/CEFACT-1996). There are two exceptions:

1. ITU, which started in 1865 with telegraph and related document-based standards, but as the technology advanced in the 1980's, started developing digital-based standards, and,
2. ICAO, which started in 1944 in the civil aviation standards space with document-based standards around regulatory and operational aspects of aviation, but in the 1990's started developing digital standards for digital navigation systems, e-passports, etc., and now their standards are both document-based and digital-based, according to the type of standard.

- The most recent four standards entities established chronologically (IETF-1986, OASIS-1993, W3C-1994, UN/CEFACT-1996) have standards that are both open and digital.

There are two recent items of note where we are starting to see some early alignment between more than one of these entities. In July 2024, UNECE (the parent organization of UN/CEFACT) and the ICC Digital Standards Initiative (DSI) called on the industry to accelerate the adoption of globally interoperable standards essential for achieving digital trade worldwide. In August 2024, ISO, IEC and ITU announced the coordination of publishing a monthly document that lists all work items from the three organizations including updates on the projects and timelines from the technical committees' work (link).With the major global standards entities discussed above, which set the basis for harmonization from their large scope and global adoption, there has also developed a hierarchy in the standards setting world. Generally, standards setting bodies that cover a broader range of data elements across the journey of movement from origin to destination, set a point of reference for other smaller and more narrowly focused standards setting initiatives. In a traditional model where standards are made available for purchase, those organizations that purchase standards are expected to commit to following those standards. In addition, auditors and certifiers who validate other organizations' compliance with standards must also purchase these same standards.

On the other hand, models that offer open-source standards may be more dynamic, providing tools for end users to configure data elements based on their own needs (e.g., different shipment types). Open-source standards may also increase users' ease of adopting standards across the supply chain:

- Sellers may assign common data elements to product at the point of export, which customs authorities may refer to at the point of entry
- Initial sellers' compliance with a standard facilitates compliance at the level of resellers, labeling companies, and larger marketplaces
- Open-source standards may also facilitate auditing and verification processes to ensure compliance with the standard, reducing the risk of manipulation of information or erroneous classification
- Global standards that are openly available will facilitate compliance across complex supply chains.[1]

When standards are made freely available, revenue models may also shift toward charging for additional documentation or services, different forms of membership fees, or public funding. This points to the shifting trend in standards models introduced above, which is taking place and will be essential for harmonizing and scaling tech-based solutions for global supply chains. This trend favors open-source rather than fee-based standards models, with digital-first (post-document) rather than paper-based models.

HARMONIZATION/INTEROPERABILITY

The initial models of standards as we know them started in Egypt, and in the thousands of years since then, standards have dramatically expanded in many ways, to include geography, industry, and technology. Yet, for the most part, once a standards entity exists it stays in its lane, so if the focus is customs, or aviation, etc., that tends to remain the focus. This has worked extremely well to map out and develop key standards in many fields as outlined in the entities we reviewed, but it doesn't account for the world of today from the International Space Station viewpoint. That is why we started this GSMI 5.0 Supply Chain effort with a view from space as our default position. Rather than building each entity out one step and one standard at a time (essentially, process improvement), looking at the global view makes it apparent that all of this will have to come together (breakthrough

thinking) to truly lean into the digital world that exists today and tomorrow, and that leads us to harmonization and interoperability. The sooner we align on the inevitability of this global view, and what that means for harmonization and interoperability, the sooner we can all work together to accelerate into that space for the benefit of a much more streamlined global supply chain.

Currently, much of the world moves at the physical speed of items, be that by water, rail, road, air, or a combination of those (multi-modal), including the paper documents we use as proxies for trust like Commercial Invoice, Bills of Lading, etc. However, critical emerging technologies promise a future where the key trusted elements from those documents we have used for millennia will move digitally and at the speed of data, and well ahead of the physical items they represent. One example would be that customs agencies and others in the supply chain could access secure data from trusted sources (verifiable credentials, etc.) to analyze and optimize that data, and, under some set of circumstances, could significantly reduce or even eliminate the traditional 'port of entry' concept, since these are known items from trusted sources. That single example helps envision the transformative nature of this technology to completely rethink global supply chains.

To accomplish that, we must bring the standards entities together at that ISS level view, so we accelerate harmonization of standards and interoperability of processes. That means aligning different standards to ensure they are compatible and can work together globally, which is essential in a world where businesses and supply chains routinely operate across borders. Where we can reduce friction across borders, we all win, and global commerce can significantly speed up. Interoperability is the goal here, where different systems, products, or services can exchange and use information seamlessly. Harmonization ensures that various local or industry-specific standards don't become isolated silos but are a part of a larger, integrated global system.

Harmonized, interoperable standards create smoother, more scalable global systems and reduce compliance costs for businesses, accelerating participation in global trade.

INTERNATIONAL COOPERATION AND REGULATORY PROGRESS

Regulatory developments today are also favoring progress toward global harmonization of standards for digital trade. Legislation may be needed to ensure support of standards, with adequate educational resources and frameworks in place to facilitate adoption. For example, the United Nations Commission on International Trade Law (UNCITRAL), which operates as a subsidiary of the UN General Assembly, has adopted a Model Law on Electronic Transferable Records (MLETR), which introduces a legal framework to allow electronic documentation to be adopted instead of paper-based documentation. Legislation related to logistics at a national level, in turn, must align with MLETR as an international framework.

The aim of MLETR is to facilitate paperless trade, through a legal environment that supports the recognition of electronic documentation as legally valid when functionally equivalent to the paper-based version of such documentation. The aim is to facilitate and expand the adoption of electronic documents at a domestic and international level. This requires supporting the increasing acceptance and use of emerging technologies including blockchain, with capabilities such as smart contracts, and data capture from Internet of Things. MLETR promotes the acceptance of electronic formats for documents including bills of lading, bills of exchange, promissory notes, and warehouse receipts, which are equivalent functionally to other transferrable formats. It recognizes the benefits of digitalization over paper-based processes for trade including faster processing, increased

security, sustainable practices in going paperless, and facilitation of inclusion for small and medium enterprises.

The international community will benefit from continued efforts to advance harmonization and interoperability, including:

- Calls to action for global adoption of unified standards for digital trade
- Open-source repositories of key trade documents, data elements, and reference data models for global transportation
- Development and maintenance of a business standard that can be applied at a national and regional level across administrations and industries
- Open-source data sets to be used for global regulatory developments supporting digital trade
- Legislation may be needed to ensure support of standards, with adequate educational resources and frameworks in place to facilitate adoption

OPEN STANDARDS

Harmonized and interoperable global data standards are necessary, are a huge step forward, and are both a grand aspirational goal and a necessity. However, back to our view from space, harmonized and interoperable data standards are just one step in the inevitable journey to create and optimize the global economy and global supply chains of the 21st century, and beyond. The next step for scale is the need for open data standards.

Traditional standards models were built around B2B (Business-to-Business), with a cost of entry for memberships, access, contributions to standards development, etc. At that time, there was little effort to focus on what is now known as e-Commerce (B2C), which generally refers to the online sale and shipment of items of minimal value, and which is currently a revenue engine in many economies. Even some Customs agencies currently have lesser requirements for that low-value **(***di minimis*, for example, <$800 USD) product to be imported, though that is starting to change. While all the entities reviewed are government agencies or 'Not-for-Profit,' all do have a revenue model. All seventeen entities generate their revenue in multiple ways, including charging for the use of their standards, membership fees, consulting services, sales of publications, training, etc., and UN agencies are funded by member states. However, those with open standards (10 of 17) do not charge for the use of their standards and gain their revenue in other ways.

While, viewed through multiple centuries of evolution, the current international standards entities each helped us get to where we are today, current and future types of commerce (B2B, C2C – Consumer-to-Consumer, aka, Peer-to-Peer, etc.) and digital and decentralized technology drive the inevitability of international movement standards needing to be open. The result will reduce friction and cost across borders, and will function as an accelerator for global commerce, to include the speed of movement. The earlier customs example where, based on trusted data moving ahead of the physical movement and approved to cross a border and resulting in no port of entry is a good indication of the difference between current processes compared to what will be much quicker global movement across borders. Current 'fee-based' standards function as 'toll gates' for global commerce activity, and while they have helped us get to where we are today, charging for standards won't help us realize the 'breakthrough thinking' moving forward of truly optimized movement at the global level.

The shift to B2C, C2C, etc., puts those membership models at risk. Where previously paying for a standard could be considered 'the cost of doing business' for large entities, increasingly, not only with the shift to B2C/C2C but also with technology advances allowing for decentralized, trusted, and more inclusive models, legacy standards entities may face the choice between becoming obsolete or transitioning to an open model for their standards to stay relevant. Charging a large entity for the use of standards may have worked for a period, but a current or future small start-up or lone entrepreneur is unlikely to be able to afford that, effectively suppressing growth globally in that type of small business. The vast majority of global businesses and employers are small and medium enterprises, and standards are essential to access global markets and increase competitiveness. Of note, IATA (est. 1945) and WCO (est. 1952) have each opened their standards recently, both of which used to be fee based, so precedence has been set.

Open standards are a key accelerant in this process. They democratize access to global trade and digital ecosystems, allowing small, medium, and large enterprises to participate without artificial barriers.

THIS IS REALLY A 'DIGITAL' DISCUSSION

Digitization of Data Elements for Movement

Now that we have harmonized, interoperable and open data standards for global movement, we finally get to the key point, which is digitizing key data elements for traditional movement documents and other key processes. This is literally -the- moment in human history where, since the start of what we originally called 'trade' (~3,000 BCE), physical items (clay tablets, papyrus, parchment, and, finally, paper) have been used as proxies for trust, moving forward the future of the global supply chain is digital. Yes, of course, there will still be physical movement, but by creating trusted and secure digital data elements surrounding that movement, we now move into a paperless (post-document) global supply chain. The ability for those key data elements about a shipment to move ahead of the physical shipment and at the speed of data will transform everything we know of global movement in all modes (water, rail, road, air, multi-modal). Once those data elements are digitized, we can and will completely rethink (digitalize) those processes, reinventing many aspects of how global supply chains operate.

When we now think of a 'digital' global supply chain, it creates a portal into multiple current and emerging technologies that will be equally transformative in this space, including digital identity, blockchain, sensors, AI, etc.

Digital Twins

An example of the value of digitization is a 'digital twin,' which is a virtual representation of an object or system designed to reflect a physical object accurately. For example, it can represent a physical package and track its trajectory, providing real-time data on the status of any given shipment. It also spans the object's lifecycle, is updated from real-time data, and uses simulation, machine learning and reasoning to help make decisions. By digitizing that data, all aspects of that physical item can be broken into distinct processes, from manufacture to movement, to sale, to resale, and so forth, and can therefore be tracked and managed accordingly, potentially into micro data and/or revenue streams.

The signed feature of blockchain capabilities, through verification, adds trust to the process. Digital twins of real-world assets are signed and verified, preserving the attributes of what makes each

digital twin unique, while providing digital connectivity to an inherently physical process of global movement of an item.

Digital Identity

As we digitize key data elements in a trusted and secure manner, one of the initial next steps will be what some consider the next 'Holy Grail,' which is digital identity. 'I am who I say I am,' sounds straightforward, but when hundreds of millions of shipments are moving globally every day, determining data points such as who created the product, from which part of the world it was created, whether forced labor was involved (forced labor=yes/no), who sold the product, who bought the product, and other key areas, can be challenging without digital solutions. It is a huge opportunity for data points tied to these processes digitally, as they are generally currently done using documents. Once digitized, current and emerging technologies can analyze and optimize that data to enhance informed decision making, such as creating predictive models (What will happen?) and prescriptive models (How can we make that happen?).

Now we get to the Customs example where those dots can be connected and, because of the hundreds or thousands of previous shipments from the shipper, that entity can be both known and trusted, or not trusted if unknown. The same goes for recurring movement to the receiver, and the dots can connect, with global scalability. Customs agencies, including U.S. Customs, are accelerating into this space, and they are also working across borders with their peers, the goal of which will be to create a true 'single (clearance) window' for movement, starting with verifiable credentials. Critical to all of this work will be that definitions such that 'identity' (and other examples in this paper – blockchain, etc.) are defined the same way by all standards entities, and not only in the eye of the beholder, or based on decades of work based on previous generations of technology.

Key terms in this space are 'DID' (Decentralized Identifier), which represents an entity (person, shipment, product) and 'VC' (Verifiable Credential), containing information or claims that can be cryptographically verified. A DID identifies who/what something is, while a VC states what we know about it. The next iteration of the ACE (Automated Commercial Environment) platform for U.S. Customs (ACE 2.0) is in development, and will be credentialed, so this is coming much sooner than later.

Back to the importance of open standards in support of B2C/C2C commerce, in regions where traditional identity is lacking, digital identities provide a means for micro-entrepreneurs to enter the formal economy, participate in global supply chains, and access financial services. By providing a verifiable credential (identity), even small entities can engage in cross-border commerce with large corporations, reducing barriers to entry. Globally, that will lead to authentication, trust, scalability, cross-border compatibility, unified systems, inclusion, fraud prevention, and smart contracts using blockchain.

As digital identities evolve, the concept of self-sovereign identity, where individuals or organizations have full control over their digital identity without relying on a central authority, is gaining traction, which could further enhance trust and autonomy in global supply chains.

In this context, many global entities have substantial data that can be used to identify and validate companies and individuals operating across global supply chains, ensuring that a given entity is in fact a trusted shipper, etc. With established common standards, there can be multiple ways to identify these users and certify them as trusted entities. With better solutions on common identifiers, traceability can be improved as well as trust. For example, the Global Legal Entity

Identifier Foundation (GLEIF) has established a Legal Entity Identifier (LEI),), recognized as ISO 17442 standard, which has been accepted as a trusted and viable commercial option in many aspects of the global supply chain, such as supporting an e-bill of lading model. This standard defines the basic reference data or a set of attributes that serve as the most essential components of identification for legal entities in financial transactions.

Blockchain, Sensors, and AI

The concept of blockchain has been envisioned for years, and many have just wanted to immediately jump into that space as a revenue model. But rather than a single company simply using blockchain, we go back to the ISS view from space, which is, for blockchain to scale it will take a pro-competitive global village, a 'coopetition,' where increasing opportunities for all stakeholders become an incentive even for traditional competitors to engage more securely in collaborative ways. Agreement to adopt common data language, driven by a semantic ontology, as well as adoption of standards, interoperability, and harmonization, are examples of such collaborative behaviors.

Scaling this globally is pro-consumer. We will all have to play in that space, and no single company will be able to put a logo on it for their exclusive use. Now that we are at the 'digital' discussion for global commerce, blockchain, even if not yet fully mature, is both a feasible, and inevitable outcome, but foundationally it will take this truly global approach.

Where authenticity (provenance, pedigree) matters, blockchain and Web3 will be transformative. 'What is the true source of that data, or that product,' and 'can that be proven' become significant changes for global supply chains using current and emerging technologies, with data recorded immutably on a ledger of verified records. Those entities, to include Customs agencies, can then use AI and other analytics and optimization tools to significantly streamline their operations, reducing friction across borders (documents, resources, delays), and speeding up global supply chains. Essentially, data recorded and shared over blockchain-based ledgers can be validated as trusted inputs going into AI algorithms to draw patterns and support better informed decision making.

Finally, sensors/IoT devices are very complementary to this entire discussion since sensors can capture the physical world and digitize the results (location, temperature, humidity, shock, light, etc.). Where desired, data from a uniquely identified sensor could be memorialized onto a blockchain for security and for immutable retention. Where certainty matters, at the highest levels, such as chemotherapy medicines and other similar healthcare scenarios, the combination of blockchain and sensors, with that data analyzed and optimized by AI, provides all stakeholders a clear sense of the future of global supply chains. As blockchain is becoming increasingly scalable and due to technological advances (e.g., interoperability mechanisms, sharding, side-chains, etc.), it is now feasible to use near real-time IoT sensor data for the majority of supply chain ecosystems. It is important to define what IoT data logs may not need to be kept on chain, to optimize business value for space utilized, while keeping real-time IoT sensor readings accessible on chain.

CREATING A NETWORK EFFECT

Standards are an important piece of streamlining global commerce, however, there are other key components and areas that have brought us to this point and will take us forward into a truly digital global supply chain. This is a network effect discussion, where the value or utility of a product, service, or system (in this case, global commerce) increases as more people adopt it. Historically, each era added network effect inertia and an expanding focus on greater geography, to the ISS view we have today:

- **Early trade** – Geography, natural resources, cultural/social exchanges
- **Development of trade routes/empires** – Maritime innovations, colonial expansions
- **Industrial revolution** – Technological advancements, mass production
- **20th century: Globalization** – Multilateral agreements, containerization
- **Digital revolution / The Information Ag**e – Digital communication, e-Commerce, supply chain digitization
- **Current / emerging trends** – Global standards, interoperability, ethical trade, sustainability

While we are currently focused on harmonized, interoperable, and open data standards, which are foundational to the transition to digital global supply chains, it is important to note that this could be considered inevitable based on the network effects and the value creation that was started thousands of years ago, and has continued to grow and expand to the global focus of today.

The sooner we focus on the global level, the sooner we accelerate adoption of those harmonized, interoperable, and open data standards, increasing value for all. This network effect not only accelerates the growth of global supply chains but also facilitates the continued expansion of international trade. As more entities digitize and rethink (digitalize) their processes, to include digital identity, blockchain, AI, etc., the overall value of the global supply chain network increases, leading to faster, more efficient, and more resilient trade. Encouraging the participation of all stakeholders, beyond suppliers and tier-1 stages of the supply chain, will create a network effect that can be a gamechanger in terms of visibility, traceability, and trust.

A PRACTICAL LOOK AT THE RESULTS OF HARMONIZED, OPEN STANDARDS AND EMERGING TECHNOLOGY

When data standards are harmonized, they allow for frameworks to be developed that define a business problem and show how this data and these technologies can be used to solve it. Standardized data allows for more efficient exchange of information and comparability between data from different parties.

Tokenization

Tokenization is the result of breaking down such an item into its digital representation, through the creation of one or more unique 'tokens,' representing digital value. The token uses a non-human readable format, the data is cryptographically secure, is stored in a cloud data vault, and can only be decrypted with the appropriate key (e.g., rules). The tokenization process is highly customizable by those issuing or transacting with the tokens, including whether sensitive business information is included. So, based on the preference of asset owners and token issuers, a token representing a shipment of penicillin may have the property of the drug shipment, but would not have the cost or the name of the end purchaser, and smart contracts can enforce specific rules around data access. Other considerations for tokens may be whether this is a private or public blockchain, or data access and privacy considerations (e.g., restricting data only to crucial stakeholders and not to all sub-contractors along the supply chain).

Frameworks

Work is underway to create blueprints of supply chain use cases through the lens of tokenization and blockchain projects, and some entities are using these blueprints to build frameworks for use case implementation. These groups include GBBC, BITA Standards Council (BITA), and the InterWork

Alliance (IWA), which have convened working groups to outline tokenization standards and frameworks. Focus areas include supply chain, carbon emissions tracking and tracing, and voluntary ecological markets and carbon credits.

The IWA maintains the Token Taxonomy Framework (TTF), the purpose of which is to clearly define innovative technology concepts and terms in the context of new tokenization use cases/scenarios. TTF provides definitions that have clear and well-understood requirements for properties and behaviors that are implementation-neutral for developers to follow and standards organizations to validate against. The taxonomy from TTF serves as underlying foundational data structure for reporting and disclosures.

The framework establishes a base Token Classification Hierarchy, driven by metadata, which is simple to understand and use, and which enables the generation of visual representations of classifications and modeling tools to view and create token definitions mapped to the taxonomy.

A Blockchain Supply Chain Use Case

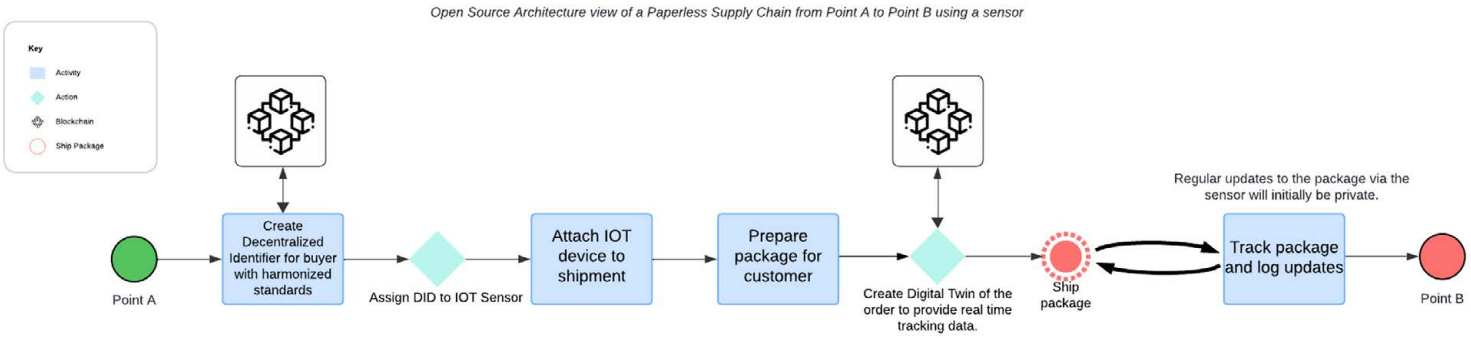
In this harmonized, interoperable, open, and digitized supply chain that is on the near horizon, foundational use cases for movement are already being created. In the following example, BITA is contemplating the following challenge using a 'crawl, walk, run' methodology for a blockchain solution, e.g., 'crawl' would be the initial technical effort to prove out the concept. 'Walk' adds features, and 'run' would be full use of the technology and use case. While this looks fairly simple, it represents a significant portion of the global supply chain of today and tomorrow:

- 'Point A to point B, across a border, with a sensor.'

So, 'crawl, walk, run' for that scenario may look like this in a few key areas:

	CRAWL	WALK	RUN
PHYSICAL MOVEMENT	Point A to point B, across a border, with a sensor. Private.	Multiple border crossings.	Provenance data exceeding the bounds of a single package.
SENSOR	Unique identity, full cell to prove out concept, use global standards.	Step down from cell device - still verify all required items, etc.	Potentially step down to lesser device - still all verifications.
PRIVACY	Full closed/private, participants only, private blockchain server.	Still private, but increased amount of public auditability.	Public? Blockchain given access controls based on permissions.
IDENTITY	Some kind of private key (registered with biz ID database).	Develop and deliver volunIncrease the # of private key parties. Verifiable credentials.	Multiple Align with global open interoperability & other standards.

In the Privacy area (and other areas, as applicable), all laws must be followed (EU-GDPR, as an example), but likely all items that are known to be 'public' would be identified up front, with the remainder considered 'private,' and adjustments could be made moving forward, as applicable. As this develops, other use case frameworks will be created that will move the 'paperless supply chain' vision forward, paving the way toward a blockchain-based supply chain as traditional signing of physical "paper" documents transitions toward digital verifications, with real-world implementations that will benefit all stakeholders.



THE GLOBAL SUPPLY CHAIN OF 2035 AND BEYOND

To create a speculative outlook on what future supply chains might look like using current trajectories we need to consider multiple factors, including, history, network effects, current and emerging technologies, and economic, environmental, and social trends. This is a 'breakthrough thinking' exercise, which gets us to a point on the horizon (let's call it our 'True North'), rather than the outcome 'process improvement' would provide, based only on previous and current small iterative steps.

We start with the ISS view which, by then, includes harmonized, interoperable, open, and digital standards, and interoperable digital ecosystems will result in trusted data flowing freely across borders and industries. When, in combination with sensors (as applicable), we know where everything is, we won't need as much, which will impact inventories. And, in combination with 3D printing/additive manufacturing and predictive analytics around procurement, not only will we more efficiently fulfill orders, but those products will also be closer than ever to the receiver, reducing shipping times, in addition to the global efficiencies previously discussed for international movement.

Smart contracts, potentially with the use of AI agents, will securely automate transactions and ensure compliance with global standards instantly. In an underlying financial supply chain comprised of all transactions involved, payments can also be made more seamlessly, and both businesses and customers can benefit from advances in financial supply chain, based on the impact of automated payment flows instructed by smart contracts and related to supply-chain events.

Supply chains will be fully decentralized, powered by blockchain or similar technologies that ensure transparency, traceability, and trust without centralized intermediaries. Every transaction, from production to delivery, will be securely recorded, enabling real-time verification of every step in the supply chain. AI will drive decision-making across the supply chain, optimizing everything from procurement to logistics in real-time, and advancements in robotics and autonomous vehicles can further maximize efficiencies. Unlike what we experienced during the Covid pandemic; predictive analytics will anticipate disruptions before they occur.

Every participant and product in the supply chain will have a unique identity, which will ensure authenticity, reduce counterfeiting, and enhance consumer trust. Supply chains will also be designed to minimize environmental impact, with many operations achieving carbon-neutral (or even carbon-negative) status. We are already starting to see Digital Product Passports (DPP) that will track an item from cradle to grave and create a circular economy. Renewable energy, sustainable materials, and zero-waste processes will be standard. Also, the ethical treatment of workers and the responsible sourcing of materials will be non-negotiable. All of this will lead to consumers, empowered by transparency, demanding higher standards of ethics and sustainability, and companies will comply, or risk being excluded from the market. To no surprise by now, regulations will be globally harmonized, interoperable, and open, to facilitate seamless international trade. Also, robotics, drones and automation will each play a key role globally.

In summary, the global supply chain of ten years from now t and beyond will be a highly integrated, intelligent, and adaptive system. It will balance efficiency with sustainability and, with the digital foundation built in the coming years, will utilize advanced technologies like AI, blockchain and further emerging technologies to create a seamless flow of goods and services across the globe. Driven by network effects, these supply chains will be more resilient, ethical, and responsive to the needs of both consumers and the environment. In this future, the supply chain is not just a logistical network but a complex, self-regulating ecosystem that evolves with the world around it.

CONCLUSION & CALL TO ACTION: A UNIFIED VISION FOR GLOBAL SUPPLY CHAIN STANDARDS

As we stand at the threshold of a new era in global commerce, the challenges, and opportunities before us are immense. From the vantage point of the International Space Station, Earth appears as a singular, interconnected system, underscoring the need for unity and collaboration in shaping the future of our global supply chains. The transition from fragmented, localized or industry-level standards to a future of harmonized, interoperable, and open systems is not just an economic imperative but a call to action for international standards entities and stakeholders worldwide.

For over a century, current day standards organizations have been foundational in facilitating trade and innovation. However, in the digital-first era, the traditional, siloed approaches must give way to a new paradigm of global collaboration, a pro-competitive ‘coopetition’ approach. No single entity can address the complexities of the evolving supply chain alone. We must break free from sector-specific approaches and work together to create open, digital definitions and standards that transcend industries and borders, fostering interoperability (e.g., between blockchain-based systems and existing systems used to manage data and processes along global supply chains) and supporting the digital identity of goods and services. Through this process, we must normalize how we consume data so that we can develop, build, and support a global supply chain (including reverse logistics

for returns) that is less impacted by hurdles or challenges that we face today. This is a collective responsibility that requires a global coalition. Initiatives that will help advance this goal include:

- Facilitating the transition toward a harmonized global system that can better link different platforms
- Promoting engagement across standards entities in a forum that supports dialogue on harmonization
- Promoting engagement with tech communities to support alignment with standards
- Identifying gaps, pain points, and ways to facilitate new model alignment
- The clear establishment of scope for these efforts, so that 'scope creep' doesn't stall or stop critical progress for success

The time is now for international standards development organizations and all other stakeholders to align in a concentrated push toward the development of these harmonized and interoperable standards. By doing so, we will accelerate the creation of a truly global supply chain that is faster, more resilient, and equitable, capable of meeting the demands of the 21st-century economy, and beyond. Inspired by the global view from space, we must build a future where the movement of goods and services is seamless, sustainable, and powered by open, collaborative standards. With that focus from the ISS view, let us begin the work together to build the harmonized, interoperable, and open standards and infrastructure that will power the commerce of the future and benefit all stakeholders.

SECTION XI

ADVANCING BLOCKCHAIN SOLUTIONS FOR SUSTAINABILITY AND SUSTAINABLE BLOCKCHAINS

INTRODUCTION

We need standards on sustainability:
Core sustainability frameworks point to a broader context of governance, social, and environmental factors that innovations must address to ensure lasting global impact. As developers focus on building innovations that will bring forward the use of blockchain technology to address global sustainability issues, it is fundamental to have a common adherence and understanding on standards. Standards provide resilience for projects, ultimately ensuring innovations are deployed in a responsible and truly impactful manner as they are intended.

This report addresses those activities at the intersection of blockchain technology and sustainability goals. It starts with covering a basic taxonomy of authority bodies and basic applicable rules, followed by a discussion of ways blockchain can advance sustainability projects, and finally a discussion on how the blockchain space itself is taking measures to operate in a sustainable manner.

I. TAXONOMY

Often regulatory frameworks and reporting requirements are crucial for businesses, organizations, and individuals to adopt sustainable practices and undergo necessary behavioral changes in a coordinated way. Entities operating at the intersection of blockchain technology and sustainability are bound to navigate the complex and evolving landscape of regulatory requirements for blockchain technology, and in addition, be compliant with requirements covering their sustainability practices.

It is important to consider the landscape of global authorities setting standards, best practices, and regulatory obligations, in addition to the data and requirements around reporting and disclosures. Public-private partnerships can be fundamental to guiding and establishing reasonable and measured obligations, especially at a global level. There is still a need to address and harmonize fragmented systems and approaches.

Below is a taxonomy of sources of legal, regulatory and quasi-legal authority related to climate and sustainability. In the context of identifying these, it is useful to cover those authorities with the greatest influence globally, having comprehensive coverage of those that affect the greatest number of entities recognizing that each entity will be subject to climate and sustainability rules not included here.

Table 1: Sources of Authority for Sustainability

Level of Authority	Relevance	Examples
Legislation	Legislation takes the form of enacted rules. Its importance is its durability and permanence. This is the realm of authority with the least flexibility for interpretation and change. In the United States, for example, it is harder to pass legislation than issue regulations; but once passed, these laws and statutes are much harder to challenge in courts.	Statutes can cover different jurisdictional levels, ranging from; - Supranational level covering multiple nations (e.g., European Union) Statutes can cover different jurisdictional levels, ranging from; - Supranational level covering multiple nations (e.g., European Union) - National rules (e.g., US federal agencies like the Securities and Exchange Commission) - Political economy levels, where rules apply only to the domain where a specified political economy may have jurisdictional authority (e.g., US states) - Regional authorities (e.g., multistate bodies that regulate how electricity is managed) - Bilateral and multilateral treaties (e.g., MOUs between jurisdictions, acting as contracts among countries to take certain actions)
Regulation	Regulations are pursuant to statutory authority as defined by legislation. They comprise rules with a similar legal effect as legislation, but regulations can be more easily revised or abandoned. Usually government agencies take regulatory actions, often becoming implementing agencies to ensure compliance with the rules put forth. These agencies issue nimble rules that can be enforced quickly, sometimes with severe penalties. The only recourse people may have to resist these rules may be in court, which would be expensive and risky. There may be ample space for interpretation, and the drivers to assist people in compliance may be more behavioral.	Regulations can span federal (country-level), state, or local rules, They include policies, standards, and rules that businesses, organizations, and individuals are obliged to follow. For instance, environmental regulations may limit power plant emissions. Financial regulations may impact the operations of financial institutions from banks, credit unions, insurance companies, etc. Employment regulations may set minimum wages, protections against child labor, and licensing requirements.
Guidance	Guidance is pursuant to regulatory authority. Guidance documents make no enforcement promises. It is assumed that if entities follow the rules announced through guidance, then there will be no enforcement actions against those who conform to their dictate. Due to the fact that guidance has room for interpretation, certain entities may be deemed to be non-compliant even when doing their best to remain in compliance.	Guidance may be announced by industry sector. In some domains, laws and regulations may be too broad, such that guidance from agencies becomes more relevant for the regulated community to take actions (e.g., US Food and Drug Administration setting documentation to submit for different purposes). If entities are considered to be non-compliant with these rules, there is a risk of being sued (e.g., SEC enforcement letters to blockchain and digital assets startups).

Quasi-Regulatory: International bodies	International bodies tend to work with governments to enforce treaties and other international rules. Representatives of various nations and supranational entities come together to attempt to set rules and standards.	Governments can work with international organizations like the United Nations to enforce global treaties and rules. The United Nations Framework on Climate Change (UNFCCC) has established the main international agreement on climate change.
Quasi-Regulatory: Voluntary Standards Bodies	Industry bodies and professional associations can set rules at a sub-legal level, which can be presented as voluntary standards and frameworks for a variety of activities. These quasi-regulatory voluntary standards bodies represent a wide array of different types of distributed geographical, industry, and technical expertise, creating common rules and inviting relevant stakeholders to follow them. These organizations are not backed up by government power, so they are not in a position to enforce their system of rules and standards with government authority. Instead, they rely on the voluntary consensus of the community as authority. They are considered, nevertheless high reputation organizations, and it is in the best interest of entities operating in a given industry to follow their standards where relevant, as a stamp of legitimacy. While there is no obligation to follow their rules, often stakeholders do choose to follow them, giving these organizations de facto power that may resemble that of legal authorities. These standards bodies can be highly influential in establishing authorization of methodologies, protocols, and instruction sets. The aim of these rules can be to preempt regulatory action to follow. If industry-focused bodies can show that their standards are widely adopted, government agencies may then be compelled to utilize those standards as a default premise to set regulatory requirements. If a significant portion, or a majority, of an industry adopts a voluntary standard by consensus, then any ensuing regulatory developments that may contradict this standard would be very difficult to enforce. In this way, consensus-based standards bodies can be a way for industry to take part in shaping the rules it will be held subject to. Moreover, to extent relevant conditions may apply, consensus-based standards bodies can merge or collaborate with regulatory bodies a to take advantage of safe harbors.	International standards bodies (e.g., ISO, ASTM, UL, accounting standards), may have a level of authority that is not considered legal and does not come directly from governments yet is still considered mandatory to operate in a certain way. Industry-focused groups also include voluntary standards-setters focused on environmental space at an international level (e.g., International Sustainability Standards Board), standards bodies focused on a specific environmental activity (e.g., Verra, Gold Standard, EcoRegistry for carbon markets), or standards operating at a country level (e.g., US voluntary consensus standards as defined by the Department of Energy).

Data disclosures ensure transparency and accountability for stakeholders. Hence, several accounting frameworks for sustainability have arisen in the context of the importance of sustainability accounting, which involves the collection, analysis, and reporting of social and environmental impacts of businesses. Sustainability frameworks and requirements set a path toward companies to manage risks, monitor progress toward net-zero and other sustainability goals, and ultimately raise their reputation and brand image.

Particularly in development sectors, it can be difficult to track activity on the ground when there are various systems in use, especially when there is still a need for basic infrastructure to move beyond manual systems and adopt blockchain solutions. There is still a need for technical integrations and capacity building, but standards and requirements can help pave the way toward necessary measures and compliance.

Below is a mapping of major global, or globally relevant, requirements for sustainability. While these frameworks range from mandatory to voluntary, and span several jurisdictions, there still may remain inconsistencies in reporting due to different requirements, and actions are being taken toward consolidation and harmonization.

Table 2: Global Sustainability Requirements and Standards

Requirement	Description	Jurisdiction
EU Corporate Sustainability Reporting Directive (CSRD)	Under this European sustainability reporting program, companies are mandated to disclose standardized and comprehensive data on their environmental, social, and governance (ESG) impact. Sustainability reporting is put on par with financial reporting.	EU, with global implications
EU Green Deal	Composite of over 12 regulations related to sustainability	EU, with global implications
EU Emissions Trading System (ETS), and other ETS around the world	Establishes a "a cap-and-trade" system that sets a limit (cap) on total greenhouse gas emissions permitted for certain sectors, and allowances for emitters that can be bought and sold. This creates an economic incentive to reduce emissions, such that entities that pollute less can sell their unused allowances in this marketplace. Out of a larger number of active emissions trading systems, the EU ETS is the oldest and most impactful by size and scope (e.g., German ETS with carve outs for the auto industry, UK ETS modeled after EU with carve outs for certain industry interests), dwarfing the size of other voluntary and compliance markets around the world. Most of these markets don't allow voluntary offsets issued in other contexts to be integrated into their systems, with few exceptions (e.g., South African ETS may permitting certain exceptions).	EU (or other jurisdiction specified), with global implications

Paris Agreement	Legally binding climate change international treaty, which was adopted in 2015 and came into force in 2016, and falls under the United Nations Framework Convention on Climate Change (UNFCCC). This is the first instance where all nations agree to cooperate at scale on climate action. This involves countries working to adapt to the impacts of climate change, reducing emissions, strengthen commitments, and provide climate financing for developing nations. The goal is to limit global warming to significantly below 2°C over pre-industrial levels, in addition to taking all possible actions to limit temperature rising below 1.5°C over pre-industrial levels. Article 6 of the Paris Agreement allows countries to collaborate for the reduction of carbon emissions. This involves the growth of carbon markets, standards, and registries. As Article 6 comes into force, voluntary carbon markets may surpass the size of the EU ETS.	Global
US Securities and Exchange Commission (SEC) Climate Disclosure Rule	The SEC Climate Disclosure Rule requires public companies to include climate-related disclosures in their annual reports and registration statements. Companies must specifically disclose data that can materially impact their core businesses and investor decisions. The purpose of this rule is to provide investors with standard information to guide them in making informed decisions related to identifying investment opportunities and risk management. These disclosures include climate-related risks and related governance actions, financial effects of extreme weather or natural conditions, greenhouse gas emissions, assessment and management of climate-related risks, and actions taken to account for such climate-related risks.	United States, with global implications
Carbon Disclosure Project (CDP)	International carbon disclosure reporting program to incentivize companies, including suppliers and business relationships, to disclose their emissions and other climate-related information to key stakeholders and investors.	Global
Supply Chain Due Diligence Laws	Laws like the EU Corporate Sustainability Due Diligence Directive (CSDDD), Germany's Supply Chain Due Diligence Act, the UK Modern Slavery Act, Australia's Modern Slavery Act, the EU's Forced Labor Ban, and the US Tariff Act of 1930, set requirements mandating companies to assess and address the environmental (e.g., transition plans) and human rights risks across their supply chains. Even the suspicion of forced labor in a shipment can jeopardize it being mandated to be sent back. These requirements are meant to ensure companies can prove they are taking action to prevent these risks.	Specified jurisdictions, with global implications
California's Climate Disclosure Bill	This law sets requirements for climate disclosures for companies with over $ 1 billion in annual revenues doing business in the US state of California.	US state of California, with global implications
Benefit Corporation (B-Corporation) Structure	The B-Corporation establishes a scoring framework applied to sustainability and governance practices. This provides a certification granted to a for-profit company for meeting high social and environmental standards, especially with respect to transparency on practices and outputs, accountability, governance structure, and workforce.	Global

International Sustainability Standards Board (ISSB)/ Sustainability Accounting Standards Board (SASB) / Task Force on Climate-Related Financial Disclosures (TCFD) Recommendations	The International Financial Reporting Standards (IFRS), which set a global standard for accounting rules and financial reporting to ensure consistency and comparability, has released the IFRS Sustainability Disclosure Standards, which are developed and approved by the International Sustainability Standards Board (ISSB). SASB sets standards that specify sustainability information disclosures that are financially material across 77 industries. These standards are being integrated at the level of the International Sustainability Standards Board (ISSB). TCFD recommendations provide guidance on information that companies should disclose on financial risks related to climate change. TCFD recommendations are also being integrated at the level of ISSB.	Global
Global Reporting Initiative (GRI) Standards	GRI is an international independent standards organization that provides a modular framework including universal, sector-specific, and topic-focused standards meant to reflect global best practices for sustainability reporting. These standards are a tool for businesses, governments, and other entities to better understand and reflect their impacts related to climate change, human rights, and corruption issues.	Global
Science Based Targets Initiative (SBTI)	Provides standards and guidance for climate action specific to certain industries, with the goal of enabling a net-zero economy and embracing innovation to drive sustainable growth. These best practices are based on scientific research and guide companies and organizations to set and meet ambitious emissions reduction targets.	Global
Integrity Council for the Voluntary Carbon Market (ICVCM) principles	Principles to incentivize rules on what comprises a high-quality carbon credit, with ethical and environmental validity considerations for minting carbon credits. ICVCM takes responsibility for ensuring carbon credit quality on the supply side, ensuring the integrity of carbon credits.	Global
Verra	Verra's Verified Carbon Standard (VCS) program validates and credits greenhouse gas emissions. Projects and programs that register with VCS, after completing a development and assessment process, are issued unique carbon credits authorized for trading in global carbon markets.	Global
"Blue Sky" Campaign	Air pollution reduction through stricter emissions standards and fostering reliance on cleaner sources of energy.	China, with global implications
Ecodesign Regulations	Rules like the European Ecodesign Directive, which was significantly expanded into the Ecodesign for Sustainable Products Regulation (ESPR), as part of the Sustainable Products Initiative, and the 2020 Circular Economy Action Plan, are mandating the adherence to sustainable design principles for companies' products. These principles are aimed to minimize environmental impacts throughout the lifecycle with elements like circularity, responsible energy usage, minimizing waste, resource efficiency, and other sustainable practices. The US (e.g., Energy STAR certification for energy efficiency), Japan, South Korea, Brazil, and India are also increasingly considering and putting in place ecodesign principles.	Specified jurisdictions, with global implications

Regulations	Rules that protect biodiversity are being set across jurisdictions, including the US Endangered Species Act of 1973 which prohibits commercializing endangered species and requires recovery plans to protect critical habitat areas. Biodiversity offsetting policies also require entities to compensate for any negative impacts of their activities on biodiversity by preserving, restoring, and enhancing biodiversity elsewhere. France, for instance, has required biodiversity disclosures and vigilance plans for companies with over 500 employees. These companies must set plans to identify biodiversity risks, carry out ecosystem impact assessments, and describe mitigation actions. In addition, international biodiversity treaties include the Convention on Biological Diversity (CBD), the Convention on Migratory Species (CMS), and the Convention on International Trade in Endangered Species (CITES). Finally, the Taskforce on Nature-related Financial Disclosures (TNFD) has established recommendations for companies and organizations to report and take action based on nature- related impacts, risks, and opportunities.	Specified jurisdictions, with global implications
Greenwashing Prevention	Rules and requirements from governments and industry bodies are underway to address deceptive environmental marketing and misleading sustainability claims by companies and organizations. This requires transparency and greater accuracy in messaging about environmental practices (e.g., making specific claims, with supporting evidence, and verifications). These rules also support companies to establish an anti-greenwashing strategy. Anti-greenwashing regulation includes the 2024 EU Directive on Green Claims, the UK Green Claims Code, the Australia Green Claims Code, components of the US SEC Climate Risk and Emissions Disclosure Rules, and similar approaches in Canada, France, and South Korea.	Specified jurisdictions, with global implications

II. BLOCKCHAIN TO ADVANCE SUSTAINABILITY GOALS

Emerging technologies including blockchain can greatly help address climate change concerns and facilitate compliance with increasing sustainability requirements. Blockchain provides a toolset to solve business problems in ways that are in compliance with regulations and environmentally friendly best practices. These solutions are increasingly relevant as nation-states are taking steps to comply with the Paris Agreement commitments and turning to technology to assist them to tackle the most complex and urgent issues of taking climate action, ensuring transition plans, and reducing emissions.

Moreover, the ability to implement these technology tools depends on legal, regulatory, and voluntary standard landscapes where companies and organizations are operating. The legal context could bring challenges that blockchain technology can help overcome, becoming a tool to support competitive advantages by facilitating compliance with requirements. Reporting, which has largely focused on carbon emissions, can be difficult to accurately calculate across direct Scope 1 to indirect Scope 3 emissions, and subsequently report to the public. Emerging technologies including blockchain can help with this task, in the context of standardized reporting mechanisms still in development.

Foundational Issues for the Circular Economy:

In the context of climate change, land-system change is one of several planetary boundaries where humanity is living outside of a safe operating space. Changes in the use of land, largely from forests

to agricultural land, have affected climate by altering the carbon dioxide level concentrations, and impacting biodiversity, freshwater, and Earth's surface reflectivity. Earth's biggest systems that trap carbon (forests/rainforests/soil) are no longer trapping as much as necessary. Risks to humans range from health, natural disasters and extreme weather, and impacts on infrastructure.

Permacultures, for instance, introduce an ethical and holistic, ethical approach to land management and settlement that draws on natural ecosystem dynamics that are inherently localized. The goal is to improve sustainability practices and reduce waste, while increasing efficiency and transparency of supply chains, and verifying that resources are adequately sourced, managed, and recycled or repurposed. Blockchain technology can track data to ensure effective mitigation practices, with an unprecedented level of transparency to monitor short- and long-term impacts. NFTs and incentive structures that affect bottom lines can further advance a range of best practices to combat climate change and its effects. Ultimately, blockchain technology can record data, impact, and align incentives toward responsible use of resources at a local level, even as granular as micro communities or individuals.

Sustainable Housing: There is opportunity to utilize localized resources to build multi-family units, such as wood from trees that get replanted with sustainable considerations. Blockchain technology can ensure the provenance of materials, ensuring responsible sourcing, ecosystem conservation practices, and guaranteeing that there is no deforestation impact.

Food Supply: Localized, and even hyper-localized resources can support the circular and local economy with fewer emissions. Incentivizing local supply and demand can ultimately reduce costs, benefitting small and medium businesses and consumers. This can improve levels inclusion especially in the context of global food shortages. Blockchain technology can track these circular economies, including local supply chains and validating responsible agricultural practices (e.g., use of chemicals and pesticides). This transparency and efficiency can help ensure adequate stable food supplies to meet the needs of a given community, ultimately bringing more integrity into the food industry. An added benefit would be that shorter shipment times and a shorter shelf life prior to consumption preserves higher nutritional density and can support health outcomes. Incentive structures can also be created for activities like composting, to support further local food production.

Waste Management: Waste to energy systems, where waste produced by a household can be utilized to produce power, can provide monetary benefits for households and be verified with blockchain and tokenized assets. Incentive structures can also reward households that demonstrate more sustainable behaviors with their waste, such as NFTs or other tokens to enable additional purchases or other benefits. IoT technologies including sensors can detect areas where waste is being managed more responsibly

Water Usage: Much like with carbon markets, blockchain technology can facilitate water trading as an exchange of water rights, or allocations, between buyers and sellers. Blockchain can be useful to make trading activity more efficient, helping match buyers and sellers, increasing competition to lower prices. Added transparency can addresses concerns over provenance issues and improve trust. Moreover, as wastewater can be treated and reutilized to support a permaculture, tracking and tracing mechanisms can enhance the validity, scalability, and impact of these processes.

Renewable Energy: Today, consumers usually have one major choice to purchase power from state-run utilities. Other choices, such as co-location of solar farms or owning solar panels, are

often distant second choices, and access to wholesale markets to purchase power from several generators can be very limited. Blockchain can facilitate a transition away from dependence on a small number of massively produced fossil fuel sources, to reliance on numerous renewable energy sources, each of which can be small in its production capacity.

Blockchain technology can be an effective accounting system for grid management for renewable energies, with the necessary pricing flexibility to adapt to changing supply and demand dynamics. Tokenization can facilitate local energy production and trading, so that individual households can benefit economically from excess energy sales. Competitive markets for energy can permit buyers to bid on offerings by sellers. Blockchain technology can make these markets more efficient and transparent, enhancing opportunities for individuals to competitively bid for electrical generating capacity as buyers on wholesale markets (e.g., deregulated energy markets in some US states), or purchase energy in retail markets, allowing for price negotiations for renewable rates. Microgrids are also increasing in popularity, with opportunities to provide energy back into the main grid (e.g., powering electric vehicles).

With blockchain, Pricing can be made more transparent based on the competitive landscape, energy projects' characteristics, and aspects like scope and cost. Smart contracts can limit credit risk and collateral requirements, putting funds on escrow and ensuring delivery of energy upon payment. Certificates of origin of energy, as well as renewable energy certificates (RECs) can also be validated by, unbundled, and sold separately in marketplaces. Access to energy subsidies can also be facilitated in relevant jurisdictions that authorize RECs, especially for cases where renewable energies may be more expensive (e.g., off-shore wind). Incentive structures enabled by blockchain can also provide tools to significantly increase sales, tracing, and reporting of renewable energies. Finally, blockchain can facilitate the implementation of legal orders with partial oversight over energy markets that align incentives toward renewable capacity production.

Selected Examples of Blockchain Solutions for Sustainability

Blockchain technology can benefit sustainability initiatives with transparency of data, tokenization, and advancing the interests of the Global South.
[please add visual logo for each of these 3 attributes in () for each of the examples below]

Satva Trust – Carbon Data for Global Shipping (Data Transparency)

Satva Trust is a technology company that leverages AI and machine learning to provide independent, auditable, and consistent data on fuel consumption and carbon emissions in the global shipping industry. Their platform offers unique insights that help stakeholders, including banks, insurers, and shipowners, make better business decisions by assessing risks associated with fuel use and emissions performance.

Satva Trust ensures data transparency and traceability using the blockchain, enabling users to compare their emissions performance with peers globally and price lending or insurance products based on emissions performance. This innovative approach supports the shipping industry's decarbonization efforts and promotes sustainable practices.

Plastic Bank – Transparency for Recycling (Global South, Data Transparency, Tokenization)

Plastic Bank is a social fintech company that aims to tackle plastic pollution and poverty by incentivizing the collection of plastic waste. They support the Global South through their operations

in regions with high levels of plastic pollution and poverty, such as the Philippines, Indonesia, Brazil, and Egypt. They establish collection branches where community members can exchange plastic waste for money and social benefits, such as grocery vouchers, health insurance, and life insurance. This approach helps to alleviate poverty while cleaning up the environment.

Plastic Bank uses blockchain technology to ensure data transparency and verification that allows for traceability and accountability, ensuring that every piece of plastic collected is tracked from collection to recycling. Plastic Bank's tokenization process involves converting physical plastic waste into digital tokens, which can be tracked and verified on the blockchain. This ensures that the plastic waste is properly accounted for and that the social and environmental impacts are transparent and measurable.

Ava Labs – Sustainable Blockchain (Tokenization, Data Transparency, Global South)
Ava Labs, creators of the Avalanche blockchain platform, are promoting sustainability by offering an energy-efficient network which reduces environmental impact of networks run on this technology. Unlike traditional proof-of-work systems that consume large amounts of energy, Avalanche uses an innovative consensus mechanism called repeated random sub-sampling to validate transactions. This solution has significantly lower energy usage compared to networks like Bitcoin. For instance, a 2022 study highlighted that Avalanche's proof-of-stake network uses a minuscule fraction (0.0005%) of the energy consumed by Bitcoin's network.

The platform enables tailored tokenization, allowing real-world assets to be represented digitally on the blockchain. This capability enhances transparency in data sharing and makes transactions more efficient. This can be particularly beneficial for countries in the Global South, as they open up access to decentralized financial services and create new economic opportunities.

In addition, Ava Labs offers AvaCloud, a no-code, customizable platform that lets users develop blockchain solutions tailored to their needs without requiring advanced technical skills. This accessibility encourages innovation in areas like renewable energy trading, tracking carbon credits, and creating transparent supply chains, which can contribute to sustainability efforts globally.

Hedera – Sustainable Blockchain (Tokenization, Data Transparency, Global South)
Hedera Hashgraph is advancing sustainability through its energy-efficient ledger technology and by facilitating the tokenization of environmental assets. To this end, Hedera uses the Hedera Guardian, an open-source tool that standardizes and streamlines the creation and management of digital assets used for carbon credits and renewable energy certificates.

The Guardian simplifies the process of developing ESG assets by incorporating policy templates and automating data collection and verification, often integrating with IoT devices. This enhances transparency and ensures compliance with regulatory standards, reducing the risk of fraud in environmental markets.

Facilitating and streamlining of the management of environmental assets help organizations efficiently trade and track these assists on Hedera's network. The platform is globally accessible, and its open-source nature means that it can be adopted by emerging markets in the Global South, thus aiding these regions in participating in global sustainability initiatives and attracting investment for environmental projects.

Ripple Impact – Sustainable Blockchain (Global South, Tokenization, Data Transparency)
Ripple Impact is using the XRP Ledger (XRPL) to support sustainability and foster economic development. The XRPL operates on an eco-friendly consensus mechanism that avoids energy-intensive mining, thus maintaining high efficiency without compromising security or decentralization.

One of Ripple's significant contributions is in the space of cross-border payments. Traditional international money transfers can be costly and slow, affecting over 272 million migrants worldwide who rely on remittances. Ripple's technology offers a solution by enabling faster, more reliable, and more affordable transactions through their network. This is particularly important for individuals and economies in emerging markets, enabling greater connectivity, and ease of cash transfers on a safe and accessible platform.

The XRPL also supports applications such as CBDCs and NFTs, which can promote financial inclusion and create opportunities for economic growth when implemented effectively.

BTG Pactual – Nature-Based Solutions (Global South, Data Transparency)
Brazilian financial institution BTG Pactual's Timberland Investment Group is leading efforts in Latin America to restore and reforest land, using advanced technologies to support sustainability. Partnering with Meta, they are employing open-source data and artificial intelligence models developed with the World Resources Institute to monitor forests. These tools allow for detailed mapping of tree canopies, even identifying individual trees on a global scale. Making this data publicly available enhances transparency and can aid various stakeholders in their efforts to advance in carbon markets and reforestation efforts.

The aim of the project is to generate carbon removal credits by addressing deforestation in critical regions, rehabilitating degraded lands and their biodiversity. Due to accurate monitoring, BTG Pactual can ensure precise carbon accounting, thus strengthening the credibility of carbon markets - a feature essential to their functioning and growth.

Beyond environmental restoration, the initiative supports local communities, by creating jobs and encouraging sustainable economic activities such as honey production, which benefits from the restored ecosystems. By combining technological innovation with sustainable practices and supporting structures for the emerging bioeconomy, the project combines action for environmental and social SDGs within the Global South.

Algorand - Digital Health Passport: (Data Transparency, Global South)
Algorand Foundation's India initiative has collaborated with Lok Swasthya SEWA to launch a Digital Health Passport based on the AlgoBharat blockchain technology. This innovative solution aims to enhance healthcare access by providing secure, immutable records of verified health credentials. The Digital Health Passport allows users to quickly access critical health benefits and social safety net programs while also helping SEWA Shakti Kendras scale services based on individual household requirements. This initiative particularly benefits working women and their families, promoting economic empowerment and self-reliance.

The Algorand Digital Health Passport utilizes blockchain for transparent data management. By creating immutable records of health credentials, it ensures data integrity and security, complying with India's new Personal Identifiable Information regulations. This use case advances the interests of the Global South by improving healthcare access and empowering women workers in India.

Hyphen - Trust in Carbon Markets: (Transparent data, Global South)
Hyphen collaborated with LI-COR to develop a revolutionary technology for greenhouse gas (GHG) monitoring in carbon markets. This collaboration integrates LI-COR's eddy covariance flux measurement systems with Hyphen's proprietary atmospheric-based digital monitoring, reporting, and verification (aMRV) software. The result is a robust hardware-software combination that automates the entire process of issuing high-quality carbon credits. This solution offers real-time, precision quantification of GHG fluxes across various sectors, including nature-based solutions, agriculture, oil and gas production, and waste management.

This use case leverages blockchain for transparent data by providing real-time, accurate quantification of GHG fluxes. The solution enhances the integrity of carbon markets by improving transparency and trust through automated, blockchain-based processes. While not explicitly mentioned, this technology could potentially benefit the Global South by providing more accurate and trustworthy carbon credit verification for projects in developing countries.

Nuklai - Smart Farming: (Transparent data, Tokenization, Global South)
Nuklai, an on-chain smart data platform, has collaborated with peaq, a layer-1 blockchain for decentralized physical infrastructure networks (DePINs), to improve AI and data monetization capabilities for DePINs, beginning with Farmsent, a global Web3 marketplace for farmers. This integration aims to leverage data from over 400,000 devices within the peaq ecosystem to provide quality datasets and industry insights for smart farming. With more than 160,000 farmers registered, Farmsent leverages blockchain technology to streamline the food supply chain by cutting costs, enhancing transparency, and eliminating middlemen.

This use case relies on blockchain for transparent data and tokenization, by creating decentralized product passports (DePPs) that record and verify the journey of agricultural products. It also incorporates tokenization through the potential for data monetization opportunities within the ecosystem. The initiative advances the interests of the Global South by empowering small farmers, enhancing food security, and providing valuable insights for a more data-driven agricultural future.

AgroWeb3 – Sustainable Agricultural Ecosystem (Global South, Data Transparency, Tokenization)
With the support of the Inter-American Development Bank, AgroWeb3 is a project built on the LACChain blockchain, to develop an ecosystem that relies on verifiable digital credentials, specifically for managing activities with economic and environmental assets for smallholder farmers across developing countries. The aim is to improve transparency and accountability for food systems, in a way that ensures financial inclusion and empowers smallholder farmers by facilitating their access to the digital economy.

AgroWeb3 enables market linkages, improves visibility of supply chains, and facilitates funding – particularly microcredit access for farmers to scale their operations. Smallholder farmers can be more engaged and active decision makers, and greater beneficiaries of economic activity, across the agricultural value chain. Blockchain technology facilitates transparent tracking of agricultural produce in ways that support fair trade and increase buyers' trust. Decentralized identity solutions for farmers can enable greater access to financing and a wide range of services, particularly with a self-sovereign model in which they can own and monetize their data. Farmers can also participate in carbon credit markets to boost their income for adopting sustainable practices.

III. NET ZERO APPROACH FOR BLOCKCHAIN

As blockchain technology is being utilized to help other sectors meet sustainability requirements, the blockchain space itself must address these issues as an industry. It is important to consider that using blockchain as a solution to advance sustainability goals in other sectors also brings tradeoffs, defined by the energy use and sustainability factors of the blockchain being utilized. Just like in any other industry, the blockchain space also has to address sustainability requirements, especially as defined by carbon emissions and reporting requirements. Addressing these issues is also subject to legal, regulatory, and other requirements, which are important to determine and comply with as the space matures.

In most cases, blockchain activities can couple initiatives to decarbonize their activities over time with tokenized carbon credits to address residual emissions. Yet as for calculating past emissions, and current emissions for reporting purposes, there is a significant amount of nuance.

Layer 1 blockchains, which refer to the foundational level of blockchain architecture on which other applications are built, must determine the costs and utility tradeoffs, and make sure they are addressing sustainability concerns. Reducing and controlling emissions is a way to prevent these technologies from expanding sustainability issues across the broad array of applications that are built on them. While the Bitcoin network has been known to utilize significant amounts of energy with its proof-of-work validation mechanism, Ethereum got past this issue when it transitioned from proof-of-work to proof-of-stake and reduced an estimated 99.9% of emissions. Therefore, it is important to consider that not all blockchains utilize the same consensus mechanisms, which leads to different sustainability issues across their respective networks.

Industry communications and messaging on sustainability have yet to be made clear across the blockchain space; yet there has been significant progress. Several blockchain networks, for instance, that have positioned themselves for enterprise use, have also developed energy efficient operations and ambitious net-zero goals.

Ensuring the sustainability of blockchain technology as an industry starts with a clear methodology to measure environmental impacts across blockchain networks. This points to the need to ensure the data to be collected, reported, and monitored. When it comes to carbon emissions, which are the major concern, it is important to consistently define what activities comprise direct and indirect emissions according to generally accepted and standardized convention:

- Scope 1: Direct emissions from operations owned and controlled by an entity.
  - For blockchains, in most cases there are very few, if any direct emissions. In some cases, however, there may be emissions resulting from direct operations at the miner level. If Bitcoin have ownership of their power generation in terms of equity and operational control, then they produce Scope 1 emissions. Miners may purchase their source of energy to generate the electricity that powers their mining activities. In this case, the power generation is part of the miner's assets.
- Scope 2: Indirect emissions from energy purchased by an entity.
  - For blockchains, Scope 2 is essential, as it is where most of the action is with respect to emissions. The bulk of these emissions are Scope 2. It points to activity at the node level, referring to the electricity purchased (not controlled at the source) to power operations. Nodes

utilizing computational electricity to run a network make up the core source of emissions for the entire blockchain and digital assets space.
  - Geographical insight on nodes is important, as depending on the energy grid utilized and the emissions associated with it, a node in Africa may not have the same emissions per transaction as a node operating out of North America. Electric grid coefficients for different countries, at a subnational region,or at the utility level, can be utilized to measure this data at increasingly granular levels.
  - It may also be important to understand the supply and real estate related to carbon emissions. The buildings and physical infrastructure where energy is generated may have an impact on emissions. This can be estimated with insight on embedded emissions in building materials, though it may not always be relevant.
- Scope 3: Indirect emissions across an entity's value chain.
  - For blockchains, this can refer to the emissions of a chain that builds on a separate main chain, a Layer 1. Layer 1 emissions flow through to Layer 2 that runs on a Layer 1, as purchased goods or services, which can be accounted for as Scope 3 in the value chain. Yet questions remain on how to calculate the exact portion of Layer 1 emissions to allocate to Layer 2 activities and consider Scope 3 emissions for that very Layer 2.

Table 3: Net Zero Approach for Blockchain Networks

Chain	Consensus Mechanism	Approach to Scope 1 emissions	Approach Approach to Scope 2 emissions	Approach to Scope 3 emissions
Ethereum - pre merge	Proof-of-Work	function of miners producing energy in-house (trivial)	nodes providing their computational electricity to run a network	Portion of energy from sidechains & other activities on separate chains that runs on Ethereum
Ethereum - post merge	Proof-of-Stake	function of miners producing energy in-house (trivial)	nodes providing their computational electricity to run a network	Portion of energy from sidechains & other activities on separate chains that runs on Ethereum
Bitcoin	Proof-of-Work	function of miners producing energy in-house (trivial), in addition to a potential special case where a historical portion of Scope 2 may be considered Scope 1	nodes providing their computational electricity to run a network	Portion of energy from sidechains & other activities on separate chains that runs on the Bitcoin blockchain
Sidechains / Layer 2	Proof-of-Stake - aligned with that of the main Layer 1 chain on which side chain runs, considered as purchased good or service	function of miners producing energy in-house (trivial)	Sidechain nodes running sidechain network	Layer 1 emissions flow through to Layer 2 as purchased goods/services within Scope 3. Portion of Layer 1 emissions goes to Layer 2's S3

Digital assets have certain unique characteristics that can present challenges for consistent measurement and reporting of emissions. Existing measurement frameworks don't necessarily incorporate how emissions can and should be measured as starting point. When considering emissions per transaction, these can generally be considered Scope 2 or Scope 3, depending on the design of a network and the nature of its operations. The vast majority of blockchain digital asset operations will interplay between Scope 2 and Scope 3 in different ways, where one chain's Scope 2 can be another chain's Scope 3 emissions. It is necessary to have accurate accounting for all these activities.

It is important to define what net zero means in the context of a given blockchain network and its operations, given the wide array of issues encountered on reporting emissions, and potential actions to take to address those issues.

- **Measurement:** Blockchain enables increased granularity when it comes to emissions and activities (e.g., automating emissions analysis and data stored on chain). . Moreover, insights extracting data recorded on blockchains can also be used for emission metrics.

- **Reporting:** Voluntary standards and reporting frameworks can be adopted by blockchain providers, which can demonstrate adherence to existing requirements for climate reporting in addition to climate impact investing initiatives. Yet there may still be gaps in how standards are written and how emissions are generated by blockchain networks, such that there may be a possibility to make claims that are not supported by real world impacts.

- **Regulatory Requirements:** As financial entities are being required to report on emissions (e.g., EU MiCA regulation establishing emissions reporting requirements for financial companies, Greenhouse Gas Protocol and its approaches, standards), decisions to purchase digital assets are increasingly tied to regulatory drivers to understand the nature of underlying emissions.

There are several approaches to calculate a network's emissions, and existing methodologies have achieved a certain level of standardization to calculate and measure emissions:

- Cambridge Center for Alternative Finance - Bitcoin & Ethereum Emissions Calculations: https://ccaf.io/cbnsi/cbeci/ghg/methodology

- Climate Action Data Trust: https://climateactiondata.org/how-blockchain-technology-addresses-the-double-counting-of-carbon-emissions/

- Crypto Carbon Ratings Institute (CCRI): https://carbon-ratings.com/dl/whitepaper-mica-methods-2024

- Rocky Mountain Institute: https://rmi.org/wp-content/uploads/2022/02/principles_for_blockchain_based_emissions_reporting.pdf

- Societe Generale: https://www.sgforge.com/wp-content/uploads/2023/11/SGF_Carbon-footprint-report_2023-11-20.pdf

- South Pole: https://www.southpole.com/blog/accounting-for-the-climate-impacts-of-cryptocurrency

While these methodologies are a good starting point, there may still be gaps, especially when it comes to sidechains - blockchain networks that connect to a separate main blockchain yet operate independently from it – or a wide range of activities that are built on different Layer 1 protocols. Open questions remain, numbered below, followed by recommended considerations for moving forward in the space:

Open Questions:

1. Should each node have its own location-based emission factors to consider for Scope 2?
2. While there are global trajectories, it may be unclear how a new sector like blockchain, and the various network operation designs, can fit into those trajectories
3. For blockchains that benefit from the emissions reductions from the Ethereum Merge, can they take credit for future emissions that didn't occur?
4. Are there any privacy issues that should be taken into account when utilizing geographical insight on nodes for the purpose of calculating emissions?
5. What additional activities is a Layer 1 chain enabling in other sectors, and how can the chain's activities be utilized to help transition to net zero across the value chain?
6. How does a change in one place of the value chain flow through the blockchain and digital assets space as a whole, and how should emissions be calculated and allocated to the designated stakeholders adequately?
7. How can these changes fit within a normal net zero trajectory, to align with broader emission reduction goals?

Recommendations/Considerations:

1. Define sustainability-focused activities for the sector as a whole, to facilitate better net-zero alignment
2. Develop a more granular approach to metrics, to confront increasing greenwashing concerns.
3. Optimize systems & controls around performance assessments in addition to methodologies.
4. A sector wide approach to metrics should also consider data at a granular level in addition to high level data.
5. Refer to existing reporting frameworks and methodologies available for reporting on emissions, providing granular data to the extent possible.
6. If emissions are avoided (e.g., building on a more energy efficient system, or benefitting from the Ethereum Merge's reduction in emissions), consider if that can be considered a part of a net zero strategy
7. Consider to what extent activities outside the blockchain and digital assets space may play in the discussion of net zero alignment and transition plans
8. Identify additional activities beyond mining and transactions that may have an impact on emissions. Reducing emissions in additional activities in exchange for value from mining or transactions may be beneficial.
9. Identify these additional core activities that can create value in chains, and can be used to allocate emissions fairly across participants.
10. Define what the technology is being used for, and implications for offsetting approaches for Scope 3.
11. Consider a consistent approach for measurement and reporting in cases where one chain's Scope 2 is another chain's Scope 3 emissions.
12. Define how existing methodologies for calculating emissions can fit into existing net zero pathways and identify gaps. Define to the extent possible where gaps may potentially align with requirements for emissions reporting.

13. Be transparent regarding prior practices on emissions calculation, especially if different from current approaches, explain progress and evolution of calculations, and disclose additional issues that need to be considered.

CONCLUSION: A FRAMEWORK FOR BUILDING AND MAINTAINING A SUSTAINABILITY PROOF BLOCKCHAIN ECOSYSTEM:

The development of any blockchain enabled sustainability application requires a careful thought around the key success factors that helps cement its posture and capability to navigate and overcome historical challenges, and particularly inaccurate accounting and reporting of carbon and gas emissions and decarbonization efforts.

A framework that considers the following key aspects can be beneficial for a developing sustainability proof blockchain ecosystem:

1. **Transparency:** despite the blockchain promise and reality of operating on distributed ledger technologies, making it tamper proof and transparent by design, there are still ways to avoid full transparency. For example, for certain hybrid models sourcing and collecting data may involve manual ways such as feeding data initially on spreadsheets, and then transferring those to the sustainability blockchain application either manually or using AI which may present a risk of loss or evasion of fully reporting on sustainability data. Therefore, mechanisms that allows for a comprehensive identification of the key sources of information, value and inputs that the blockchain users, beneficiaries, regulators and investors can rely on to understand how emissions and decarbonization data is collected, captured, synthesized, processed, reported and disseminated to the concerned stakeholders is fundamental. This also requires recognizing the importance of adopting some of the world's leading sustainability standards and frameworks, while noting the necessity for customization according to the specific circumstances of the applications working environment. For example, places where weak communication infrastructure and services exist may require sustainability blockchain applications be capable to operate with hybrid connectivity modes to ease the collection and capturing of emissions and decarbonization data on chain.

2. **Trust:** building upon the transparency by design outcomes, a reliable and trusted route is possible if the data infrastructure is built in an accessible way that showcase the emissions and decarbonization journey from start to end to the concerned stakeholders. Moreover, devising a clear set of metrics throughout this journey becomes crucial for the concerned stakeholders, as it will act as a benchmark for measuring progress and improvement in achieving sustainability targets over the long run.

3. **Accountability:** assigning clear roles and responsibilities for teams and professionals involved in the emissions tracking and decarbonization process is paramount for identifying sources of issues and bottlenecks that requires immediate attention and resolution, as well as identifying opportunities for enhanced levels of streamlining, tracking, reporting, recognizing and incentivizing sustainability efforts and activities.

4. **Verifiability:** maintaining a solid governance, authentic and provenance rich environment over the data sets managed by sustainability blockchain applications and its surrounding ecosystem of enablers and partners, underscores the importance of operating on an open-source manner, or at least deploying measures that ease access by regulators and qualified assurance providers, to verify emissions and decarbonization tracking and reporting activities.

5. **Global South:** adopting blockchain enabled sustainability applications provides an ideal path to accelerate progress and growth for developing and emerging economies, especially most vulnerable populations that have missed on transformative technologies that arouse with the internet 1.0, 2.0 and 3.0, or been and continue to be affected significantly by physical infrastructure erosion, deforestation, loss of human potential and natural resources due to adverse events, including wars, climate change and increase in dumping practices.

SECTION XII

INDIA COUNTRY SPOTLIGHT

1. EVOLUTION OF BLOCKCHAIN IN INDIA

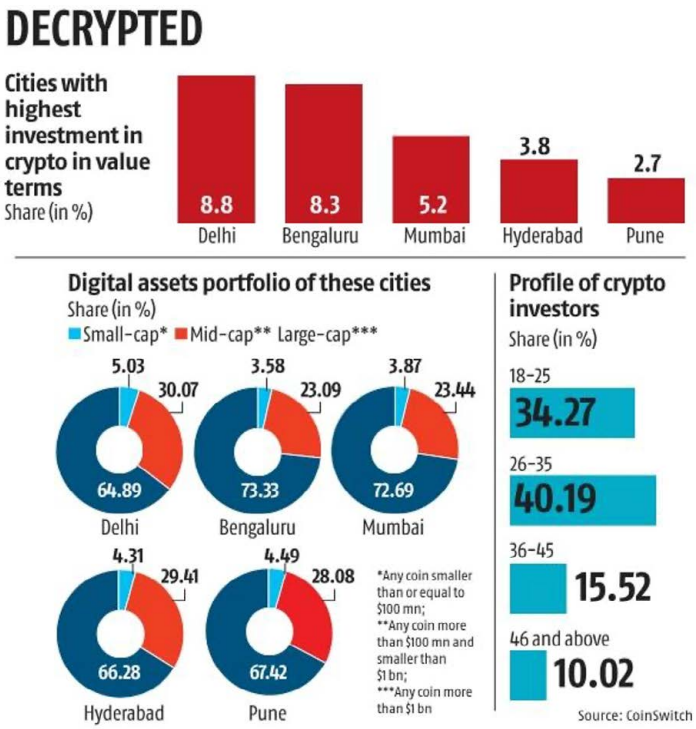
1.1. Market Overview and Key Milestones in Blockchain Adoption[1]

India is poised to emerge as a global leader in blockchain and Web3 technologies, driven by rapid adoption and a thriving startup ecosystem. According to a white paper unveiled at the 'Entrepreneur Web3 Summit' in Bengaluru, the Indian blockchain market is projected to grow from $0.28 billion in 2019 to $4.3 billion by 2025, reflecting a staggering compound annual growth rate (CAGR) of 47.3%. This growth is fueled by applications across financial services, supply chain management, and government initiatives. Notably, India is home to 1,203 blockchain-based financial startups, including prominent players like Hike, CoinDCX, CoinSwitch, IndiGG, and Vauld. International funds have already invested over $500 million in the Indian start-up and blockchain ecosystem

The momentum extends to the broader Web3 space, which is expected to grow from $0.0049 billion in 2022 to $1.1 billion by 2032, at an impressive CAGR of 57%. India's adoption of cutting-edge technologies such as decentralized finance (DeFi) and non-fungible tokens (NFTs) mirrors this trajectory. The NFT market alone is projected to expand from $3.3 billion in 2021 to $27 billion by 2028, with a CAGR of 61.6%. Additionally, India ranks first among 151 countries in the 2024 Global Crypto Adoption Index by Chainalysis, highlighting its leadership in digital assets. The digital assets market is further expected to grow by 6.58% annually from 2024 to 2028, reaching a volume of $726.2 million. With approximately 450 Web3 startups among 8,700 globally, India's ecosystem is evolving rapidly, signaling significant opportunities for innovation and economic transformation in the coming years.

India's cryptocurrency landscape is marked by a vibrant and youthful investor base. According to a report by cryptocurrency exchange platform CoinSwitch, the country boasts over 19 million cryptocurrency investors, with nearly 9% of them being women. The majority of these investors, approximately 75%, fall within the 18 to 35 age group, reflecting the strong interest among younger demographics.

In 2023, Dogecoin emerged as the most popular cryptocurrency in India, accounting for 11% of the total invested value in the crypto market, followed by bitcoin at 8.5% and Ethereum at 6.4%, showcasing the diverse preferences of Indian investors.



1.1.1. Timeline and Development Phases[2]

Early Stage

India's initial engagement with blockchain technology was marked by increasing Bitcoin awareness, laying the foundation for broader exploration. Companies like Unocoin and Zebpay pioneered cryptocurrency exchanges, showcasing blockchain's transformative potential. Financial applications gained momentum with initiatives such as BankChain and research efforts by the Institute for Development and Research in Banking Technology (IDRBT), focusing on banking innovations. Meanwhile, the Reserve Bank of India (RBI) maintained a cautious but keen interest, acknowledging blockchain's prospects while carefully monitoring its development within the financial sector.

Growth and Adoption

India's blockchain journey reflects significant strides in innovation, collaboration, and regulatory foresight. Initial efforts saw blockchain-based land registry systems piloted in Panchkula and trade finance solutions tested in diverse settings. NITI Aayog, the government's policy think tank, played a pivotal role in exploring blockchain's potential for public governance through pilot initiatives.

Entrepreneurial activity surged with startups like Polygon and WazirX, while increased banking engagement and the establishment of the Hyperledger India Chapter fostered collaboration. Indian projects gained global recognition, especially in areas of DeFi and NFTs, along with witnessing increasing participation from corporations such as TCS and Infosys integrating blockchain into their operations. Reserve Bank of India also initiated pilot projects for a Central Bank Digital Currency (CBDC).

Enhanced cooperation between educational institutions and blockchain enterprises is fostering innovation and skilled talent development. A few examples include:

- TimesPro, in collaboration with IIT Delhi, iHub Divyasampark (IIT Roorkee), and the India Blockchain Alliance, has developed cutting-edge courses on Web 3.0 technologies like blockchain, cryptocurrencies, and NFTs. These programs aim to provide modern, interactive learning experiences with certifications issued by participating IITs.
- AlgoBharat initiative by the Algorand Foundation, has to date (2024) onboarded over 60 universities across India to integrate Algorand-based curricula and projects.
- Kalp Decentra Foundation (KALP) and the Birla Institute of Management Technology (BIMTECH) have signed a Memorandum of Understanding (MoU) to establish a Blockchain Learning Centre at BIMTECH's campus.

These initiatives highlight the growing integration of blockchain technology into Indian academia, preparing a new generation of technologists well-versed in advanced blockchain systems.

Policymakers have demonstrated a concerted effort towards creating a supportive regulatory environment for blockchain technologies, aiming for a balance between innovation and consumer protection. For instance, the Government of India has launched the National Blockchain Framework (2024), to foster research and application development. The Government of Telangana released a draft Blockchain Policy outlining the framework of the blockchain ecosystem in 2019, which aimed at creating an ecosystem for promoting research, innovation and industry collaboration. Hosted in collaboration with NITI Aayog, the Governments of Telangana and Goa, in addition to Nucleus Vision, the first International Blockchain Congress was aimed at bringing thought-provoking conversations on blockchain for next-generation services, developing blockchain applications, blockchain technologies for government, and putting in place regulations and guidelines. The dialogue between blockchain enterprises and regulatory bodies continues to evolve, reflecting the government's intent to harness the benefits of blockchain while remaining focused on mitigating potential risks.

1.1.2. Future Projections and Trends[3]

- Regulatory Evolution: As the government refines its approach to blockchain technologies, clear regulations are anticipated to emerge, which could further fuel the market's growth.
- Technological Advancements: Continued innovation in blockchain could lead to more efficient systems, lower costs, and new applications in sectors like healthcare, education and agriculture.
- Programs like the first-ever Web3 Startup Lab at T-Hub, sponsored by the Algorand Foundation, focus on supporting accelerating blockchain innovation across different verticals and increasing access to the necessary tools for founders to take their solutions to market.
- The PwC India Blockchain Lab in Kolkata, established in 2017, drives innovation by integrating advanced blockchain solutions. It helps organizations harness the potential of distributed ledger technology to foster growth and embrace disruptive advancements.
- Investment Inflow: With regulatory clarity and continued growth, both domestic and international investors appear eager to increase their participation, supporting the expansion of the blockchain ecosystem in India.
- Community & Talent Pool: Increasingly more courses and training resources are being deployed to support blockchain ecosystem growth.

1.2. Cryptocurrency in India: A Tale of Ambivalence

India presents a fascinating dichotomy when it comes to cryptocurrency. Millions of Indians actively trade and invest in digital currencies, driven by the promise of innovation and high returns, fueling a burgeoning crypto community. It is driven by a dynamic ecosystem led by exchanges like WazirX, CoinDCX, and CoinSwitch, which have democratized access to cryptocurrencies and influenced regulatory discussions through active policymaker engagement. This success has spurred a surge in crypto investments and inspired a wave of startups exploring blockchain applications in DeFi, NFTs, smart contracts, and tokenization, supported by a tech-savvy user base eager to embrace innovative financial solutions. Venture capital inflows are fueling this growth, with investors recognizing the potential of India's large, digitally connected population.

However, regulatory bodies are cautiously crafting policies to address concerns like market volatility, consumer protection, and potential misuse, striving to balance innovation with security. Practical challenges, such as inadequate infrastructure and hesitant traditional financial institutions, limit everyday use, confining cryptocurrencies to investments. Yet, with a vibrant entrepreneurial ecosystem and evolving regulations, cryptocurrencies are poised to transition from speculative assets to integral financial tools.

2. NATIONAL INITIATIVES AND GOVERNMENT FLAGSHIPS

2.1. Integrating Blockchain Technology into National Strategy[4]

The National Strategy on Blockchain Technology, unveiled by the Ministry of Electronics and Information Technology (MeitY) in 2021, marks a significant commitment by the Indian government to integrate blockchain technology into its digital infrastructure. This strategy is not merely about adopting new technology but is aimed at transforming public services through enhanced transparency, security, and efficiency.

MeitY aims to advance blockchain adoption across sectors by focusing on creating a robust ecosystem through fostering research & development, establishing a clear regulatory framework, and enhancing capacity building. The national strategy seeks to integrate blockchain into public services and governance, positioning India as a global leader in blockchain technology.

The strategy emphasizes robust research and development (R&D) to address key challenges in blockchain technology, including scalability, interoperability, security, and privacy. It prioritizes designing scalable consensus mechanisms, improving transaction throughput and smart contract security. Furthermore, capacity building is a core component of the national strategy. The government is investing in education and training programs to prepare the workforce for the upcoming technological shifts. This includes specialized courses in blockchain technology and its applications, aimed at both new students and existing professionals.

2.2. National Blockchain Framework[5]

MeitY, envisioning a future of trusted digital platforms, has launched the National Blockchain Framework (NBF) to foster research and application development. The initiative aims to enable transparent, secure, and reliable digital service delivery to citizens, aligning with the Government

of India's commitment to leveraging cutting-edge technology for public benefit. It seeks to position India as a global leader in blockchain technology while encouraging the proliferation of developed solutions for global adoption.

The research focuses on improving security, privacy, and performance. Key advancements include the implementation of Zero-Knowledge Proofs (ZKP), Attribute-Based Encryption (ABE), indigenous Certification Authorities (CA), and Software Security Modules (SSM). Other efforts involve enhancing smart contract security, developing security audit checklists, and optimizing performance through parallel smart contracts and scalable protocols. Interoperability across blockchain applications is also a priority, ensuring seamless integration and robust fault tolerance.

2.2.1. Vishvasya-Blockchain Technology Stack[6]

The Vishvasya Blockchain Technology Stack is designed to provide Blockchain-as-a-Service (BaaS) through a geographically distributed infrastructure, supporting various permissioned blockchain applications. By fostering trust through innovative distributed software architectures, it enables consensus on shared states and establishes a single source of truth. The BaaS model ensures robust security across blockchain components while addressing adoption challenges faced by stakeholders such as infrastructure providers, smart contract developers, and application developers. Vishvasya's key features include rapid end-to-end development and deployment of permissioned blockchain applications, ready-to-use, security-audited Blockchain containers for production setups, and blockchain-specific security audit guidelines and best practices. The geographically distributed infrastructure spans across three data centers at Hyderabad, Pune, and Bhubaneswar. This innovative platform is the result of collaborative efforts by the Centre For Development of Advanced Computing (C-DAC), the National Informatics Centre (NIC), the Institute for Development and Research in Banking Technology (IDRBT) Hyderabad, the Indian Institute of Technology (IIT) Hyderabad, the International Institute of Information Technology (IIIT) Hyderabad, and the Society for Electronic Transactions and Security (SETS) Chennai, developed with support from MeitY.

2.2.2. NBFLite[7]

NBFLite is a blockchain sandbox platform, specifically designed to support startups and academia in rapid application prototyping, research, and capacity building.

2.2.3. Praamaanik[8]

In the ever-evolving digital landscape, ensuring the security of mobile devices from malicious applications and counterfeit customer support has become critical to protecting personal data and preventing financial losses. Praamaanik, powered by the National Blockchain Framework, addresses this challenge by leveraging blockchain technology to verify the authenticity of mobile applications. Through this system, designated representatives upload mobile apps, and their unique details are securely recorded in a blockchain ledger, creating an immutable record. Citizens can authenticate mobile apps seamlessly using the M-Kavach 2 mobile security application, ensuring trust and safety.

The platform offers several key features that enhance its utility and impact. These include maintaining a tamper-proof ledger of mobile app fingerprints, providing a single source of truth for

app authenticity, and delivering a robust solution to combat counterfeit and malicious applications. Additionally, Praamaanik fosters user confidence with its streamlined process for recording app fingerprints, ensuring ease of use, and simplifying access to genuine customer support services.

2.2.4. National Blockchain Portal[9]

The National Blockchain Portal has been designed as a comprehensive resource hub to support the National Blockchain Framework initiative. Built on a robust Content Management System, the portal offers a wealth of information, including the latest blockchain news, articles, success stories, events, conferences, and updates on education and training. This centralized platform keeps users informed about emerging blockchain trends and advancements, fostering awareness and collaboration within the ecosystem.

The portal's coverage spans a wide array of topics, including success stories, technical resources, national and international events, workshops, conferences, and a curated list of blockchain startups. It also provides access to education and training materials, along with publications and patents, ensuring users stay informed and engaged with the latest developments in blockchain technology.

The platform is further enhanced by several key features designed to improve user experience and participation. An integrated AI-powered chatbot offers quick answers to queries, while a crowdsourcing option allows users to contribute content. Managed content roles—such as "User," "Reviewer," and "Admin"—ensure the portal remains dynamic and well-maintained. Additionally, a subscription feature enables users to receive regular updates, keeping them connected with the latest portal content. By combining rich resources with interactive features, the National Blockchain Portal serves as a vital tool for India's blockchain ecosystem.

2.3. Central Bank Digital Currency (CBDC) Pilot Launch by RBI[10]

The Reserve Bank of India (RBI) launched a pilot project for the Central Bank Digital Currency (CBDC) in 2022. The digital rupee is intended to enhance payment efficiency, reduce transaction costs, and improve financial inclusion while maintaining the stability of the traditional banking system.

The pilot was launched for a CBDC in both Wholesale and Retail segments. The Wholesale pilot, termed the Digital Rupee - Wholesale (e₹-W), was introduced on November 1, 2022, with its primary use case being the settlement of secondary market transactions in government securities. This initiative aims to enhance the efficiency of the inter-bank market by reducing transaction costs and eliminating the need for settlement guarantee infrastructure or collateral to mitigate risks. The Retail pilot, called the Digital Rupee - Retail (e₹-R), was launched on December 1, 2022, within a closed user group comprising selected customers and merchants.

The e₹-R, a digital token representing legal tender, is issued in denominations equivalent to physical currency and distributed through banks. Users can transact via digital wallets provided by participating banks, enabling Person-to-Person (P2P) and Person-to-Merchant (P2M) transactions. Like cash, the e₹-R ensures trust, safety, and settlement finality, but does not earn interest and is convertible to other forms of money. Initially, the retail pilot involves eight banks in phases: State Bank of India, ICICI Bank, Yes Bank, and IDFC First Bank in the first phase, followed by Bank of Baroda, Union Bank of India, HDFC Bank, and Kotak Mahindra Bank. The RBI plans to gradually expand the scope of these pilots to include more banks, users, and locations based on the feedback received.

As of June 2024, both retail and wholesale CBDCs (e₹-R & e₹-W) in India have witnessed a number of customers rising to 5 million, from 1.3 million a year earlier, and the number of merchants increasing to 420,000 from 300,000.

2.4. Centre of Excellence in Blockchain Technology[11]

The National Informatics Centre (NIC), established in 1976 under MeitY, serves as the technology partner of the Government of India, providing ICT and eGovernance support to Central and State Governments. To advance blockchain adoption, NIC has established a Centre of Excellence in Blockchain Technology (CoE-BCT), envisioned as a coordinated, interoperable ecosystem for fostering blockchain innovation. The CoE aims to enhance understanding and implementation of blockchain technologies, offering a platform to develop, test, and deploy innovative solutions for government projects. By collaborating with global experts, the CoE will lead the development of blockchain systems from proof of concept to production, driving research-led initiatives to address complex governance challenges and improve service delivery. Additionally, the CoE seeks to promote blockchain adoption across public and private sectors, ensuring solutions meet modern technological standards in a secure and trustworthy manner. By leveraging blockchain's potential for trust, transparency, and efficiency, NIC aims to foster transformative applications that enhance government operations and citizen engagement, emphasizing evidence-based solutions to ensure cost-effectiveness and service improvement. The NIC launched a new website to highlight its blockchain initiatives, which hosts up to 7.93 million documents.

2.5. India's Call for Global Collaboration: The G20 Story[12]

At the G20 Summit, India advocated for a global framework on cryptocurrencies to address their transformative potential and associated risks. A key highlight was the call for swift implementation of the Crypto-Asset Reporting Framework (CARF), which standardizes tax reporting for crypto transactions and ensures automatic information exchange between jurisdictions. This will enhance transparency and prevent concealment of crypto transactions, including those involving foreign exchanges.

2.6. Regulatory mandates

2.6.1. Regulatory Measures for Curbing Spam with Blockchain Integration[13]

The Telecom Regulatory Authority of India (Trai) has urged MeitY to take decisive action against the rising wave of spam and phishing communications occurring on over-the-top (OTT) apps like WhatsApp and Telegram. While Trai and the Department of Telecommunications (DoT) have been implementing measures to curb spam calls and messages that often facilitate financial fraud, OTT platforms fall under MeitY's regulatory purview, creating a gap in oversight for these newer communication channels.

In a recent meeting of the joint committee of regulators, Trai officials emphasized the need for MeitY to address this issue collaboratively. Trai has already implemented measures such as a blockchain-based distributed ledger technology (DLT) platform for telecom operators to manage and regulate commercial traffic effectively. However, this solution does not extend to OTT communication channels, leaving them outside its scope of enforcement.

To strengthen protections against spam, Trai recently directed telecom operators to block messages containing unverified URLs, OTT links, APKs (Android application packages), or call-back numbers starting October 1. Entities like banks and e-commerce platforms must whitelist their information with telecom operators, who then integrate it into their DLT systems. Only messages that match this registered data are allowed to pass through, ensuring an additional layer of security for users. Trai continues to advocate for a joint regulatory framework to comprehensively address spam across both traditional and digital communication platforms.

2.6.2. Anti-money laundering (AML) provisions[14]

India has introduced anti-money laundering (AML) measures targeting cryptocurrency platforms and virtual digital asset (VDA) transactions to enhance financial transparency, curb criminal activities, and prevent terrorist financing. These provisions bring cryptocurrency trading, safekeeping, and related financial services under the ambit of the Prevention of Money Laundering Act (PMLA), 2002, marking a significant step in regulating the digital asset sector.

The federal government issued a gazette notification mandating intermediaries dealing with VDAs, including crypto exchanges, to implement robust "know your customer" (KYC) protocols for all users. These entities, now classified as "reporting entities" under PMLA, must also notify the Financial Intelligence Unit India (FIU-IND) of any suspicious activities. Additionally, they are required to maintain detailed records of all transactions, especially those involving cash amounts exceeding INR 1 million (US$12,191), for at least five years. Transactions closely related within a month that cumulatively exceed this threshold must also be documented.

The directive specifies that various VDA-related transactions are now subject to PMLA compliance. These include exchanges between VDAs and fiat currencies, transactions between different VDAs, VDA transfers, safekeeping or administration of VDAs, and financial services related to the issuance and sale of VDAs. This comprehensive approach underscores India's commitment to fostering a transparent and secure digital asset ecosystem.

3. UNLOCKING THE POTENTIAL: USE CASES OF BLOCKCHAIN TECHNOLOGY ACROSS INDIA

3.1. Blockchain-based Solutions[15]

A variety of blockchain-based solutions have been developed or are currently under development in collaboration with prominent government organizations in India. These include the Security Printing & Minting Corporation of India Limited, Cotton Corporation of India Limited, Forensic Science Laboratory, Sardar Vallabhbhai Patel National Police Academy, Central Board of Secondary Education, Ministry of Justice, Ministry of Consumer Affairs, and the Unique Identification Authority of India. In addition, partnerships with state governments such as Karnataka, Puducherry, Andhra Pradesh, Chhattisgarh, Assam, Telangana, and Jammu & Kashmir aim to create and deploy innovative blockchain applications across various domains.

Key blockchain applications being implemented include e-Stamp solutions, judiciary-focused applications, service-level training record management for IPS officers, and forensic systems. Other notable projects encompass Praamaanik for verifying mobile app authenticity, consent management frameworks, IoT device security, cotton bale identification and tracking, and several document

management solutions such as domicile certificate chains, caste certificates, property chains, and education certificate chains. Furthermore, initiatives like agricultural produce tracking and inspection systems for childcare institutions are enhancing transparency and efficiency in critical sectors.

3.2. State-Driven Initiatives

Several Indian states are actively leveraging blockchain technology to modernize governance and public service delivery. This adoption underscores a widespread recognition of blockchain's capabilities to foster transparency, enhance security, and streamline operations across various sectors of governance.

3.2.1. Tamil Nadu: Nambikkai Inaiyam's Digital Identity and Service Delivery[16]

Tamil Nadu Nambikkai Inaiyam is a state-wide blockchain infrastructure project launched by the Tamil Nadu government in 2023. The project aims to create a secure and transparent platform for government services, enabling efficient and fraud-resilient workflows. Key features of Nambikkai Inaiyam include the use of blockchain technology to secure and verify government documents, such as land records, academic certificates, and e-Sevai certificates. This platform is expected to benefit citizens by providing them with easy access to government services and ensuring the authenticity of official documents.

3.2.2. Maharashtra and Karnataka: Digitizing Land Records[17]

These states are at the forefront of using blockchain to digitize land records. The primary objective is to ensure greater transparency in land transactions and prevent common frauds associated with land sales and ownership disputes. The blockchain ledger provides an immutable record of land titles, making it nearly impossible to tamper with data.

- **Problem:** Land records in these states have long been plagued by issues of transparency and security. Traditional paper-based systems are prone to errors, fraud, and corruption. This leads to disputes, delays in property transactions, and overall inefficiency in the land administration process.
- **Solution:** Blockchain technology offers a robust solution to these challenges. By digitizing land records onto an immutable, decentralized ledger, it ensures transparency, security, and efficiency in land transactions.

Karnataka's Bhoomi Project: It has successfully digitized over 120 million land records. This initiative has reduced land disputes by 70% and boosted land revenue collection by 20%. By integrating blockchain technology, the project ensures transparency, security, and immutability of land records, while smart contracts automate processes like land registration and mutation, further enhancing efficiency and trust in the system.

Maharashtra's Land Records Modernization Project: The key focus of the initiative is to streamline land registration, mutation, and property tax collection, leading to a significant reduction in fraudulent land transactions and faster property registration processes. By leveraging blockchain technology, the system creates tamper-proof digital records of land ownership, enabling real-time tracking of land transactions[18]

3.2.3. Punjab: Transforming Agricultural Supply Chains[19]

The focus here is on revolutionizing agricultural supply chains. Blockchain technology helps in tracking the provenance of agricultural products, ensuring fair pricing mechanisms, and improving the overall efficiency of the supply chain. For farmers, this means better access to markets and a more transparent system of pricing their produce.

- **Problem:** The agricultural supply chains in these states face numerous challenges, including lack of transparency, inefficient logistics, and unfair pricing. Farmers often struggle to get fair prices for their produce due to intermediaries and information asymmetry.
- **Solution:** Blockchain technology can revolutionize agricultural supply chains by providing greater traceability, transparency, and efficiency.

Punjab's Agricultural Reforms: This initiative focuses on enabling direct farmer-to-consumer sales by reducing the role of middlemen, resulting in fairer pricing for farmers, improved quality control, and reduced food wastage. By leveraging blockchain technology, it establishes a decentralized platform where farmers can sell their produce directly to consumers. Smart contracts automate payments and ensure timely settlements, enhancing trust and efficiency in the agricultural supply chain.

3.2.4. Rajasthan and Uttar Pradesh: Streamlining Government Services[20]

These regions are adopting blockchain for a broader spectrum of applications. Projects include blockchain for enhancing citizen services, streamlining healthcare and educational offerings, and improving the efficiency of tax collection systems. These initiatives are designed to simplify interactions between the citizens and the government, reducing bureaucratic inefficiencies, and ensuring a higher degree of data integrity.

- **Problem**: These states face challenges in delivering efficient and transparent government services. Bureaucratic hurdles, corruption, and lack of digital infrastructure hinder the delivery of essential services to citizens.
- **Solution:** Blockchain technology can streamline government processes, enhance citizen services, and improve governance.

Uttar Pradesh: The Uttar Pradesh government has approved 109 research projects worth Rs 140 million to utilize AI and blockchain technology for various applications. These include early cancer detection, posture correction systems, assistive technology for the disabled, and renewable energy solutions. The government aims to leverage these technologies to address pressing societal issues and drive innovation in the state.

Rajasthan's Electronic Health Records (EHR) on Blockchain: This project has enhanced patient privacy, with secure data sharing and streamlined healthcare delivery. Blockchain integration ensures data integrity, transparency, and auditability of health records.

The state-specific initiatives described above demonstrate a growing recognition of blockchain's potential to improve transparency, security, and efficiency in government operations. By implementing blockchain solutions across various sectors, these states are working towards creating a more transparent, accountable, and citizen-centric governance ecosystem. Among these, the state of Telangana leads the way in blockchain adoption and in building the blockchain ecosystem.

3.3. Telangana: A Blockchain Pioneer

"India's blockchain journey is a testament to our commitment to innovation and technological leadership. The nation's rapid adoption of blockchain across governance, finance, and enterprise solutions demonstrates our potential to set global standards in building secure, efficient, and transparent ecosystems." – Jayesh Ranjan, Special Chief Secretary, ITE&C Department, Government of Telangana

Telangana is particularly noteworthy, leading the way, not only in blockchain adoption but also in fostering a supportive ecosystem for blockchain innovation. The Telangana government is committed to the adoption of blockchain technology. Telangana's Emerging Technologies Wing has been at the forefront of blockchain innovation, promoting transparency, trust, and efficiency across various sectors. The government's blockchain initiatives have the potential to transform several sectors, including government, finance, supply chain, and healthcare.

The state has formulated a policy framework based on four main pillars: to develop a talent pool supporting infrastructure, to promote research and innovation, to enable collaboration, and to build a robust web3 community. The state conceptualized the Blockchain District, aimed to create the world's best blockchain technology ecosystem, in collaboration with the Government of Telangana, C-DAC, Industry (Tech Mahindra), and Academia (IIIT-Hyderabad).

The state also set up a blockchain accelerator called T-Block Accelerator in partnership with the industry - Tech Mahindra. It is a four-month-long accelerator program for blockchain startups. T-Block selects promising blockchain startups, providing them with mentorship, technical support, and networking opportunities to accelerate their growth.

This provides a controlled environment for Web3 use cases to navigate the regulatory space in India. This initiative comprises 17 partnerships between Government bodies, Industries, Regulators, Lawyers, Investors, and Academia. The potential shortlisted Web3 startups were in the field of sustainable finance, digital asset trading, DeFi (Agriculture & Micro, Small & Medium Enterprises - MSMEs), SocialFi & Tokenization. This initiative also identifies the roadblocks faced by startups to establish themselves in India within the regularity space, in addition to providing recommendations for legal and regulatory modifications to Indian regulations/policies.

The Telangana government is at the forefront of India's blockchain revolution, publishing a Technical Guidance Note on Asset Tokenization. It provides a comprehensive recommendation for stakeholders to navigate this emerging domain, fostering innovation and growth in the blockchain ecosystem.

The Government of Telangana has successfully implemented over 12 blockchain pilot projects across various departments, showcasing diverse use cases. Key implementations include securing educational certificates, tracking and traceability for agricultural goods like gunny bags and seeds, First Information Report (FIR) management in police records, vehicle life cycle management (VLM) at the Regional Transport Office, and blockchain-based property registration systems. Another notable initiative, StreeNidhi, leverages blockchain to build credit histories and provide credit ratings

for Self-Help Groups. Future projects in collaboration with departments such as Energy and Gram Panchayats aim to develop blockchain-based systems for carbon credit trading, while the Excise and Police Departments plan to enhance tracking and traceability in the liquor supply chain and distillery products. These initiatives highlight Telangana's commitment to leveraging blockchain for transparency, efficiency, and innovation.

3.3.1. Telangana State Blockchain Framework

"In Telangana, we have embraced blockchain as a cornerstone of our digital transformation strategy. By fostering collaboration between the government, industry, and startups, we are creating a vibrant ecosystem that drives impactful solutions and establishes the state as a leader in emerging technologies." – Ramadevi Lanka, Director Emerging Technologies Wing, ITE&C Department, Government of Telangana

Implementing blockchain technology in public services often involves complex processes and the collaboration of multiple stakeholders. The government in consultation with the industry, is working towards making Hyderabad the Web3 hub of India. Taking a giant leap in this direction, the Government of Telangana has conceptualized India's first Blockchain District. This one of its kind initiative will aim to put all blockchain companies based out of Hyderabad in a strategically advantageous position globally. While the **Blockchain District** acts as an anchor around which the blockchain ecosystem will develop, the **Telangana State Blockchain Framework** sets the strategic direction and is based on four main pillars:

1. **Developing Talent Pool:** The Telangana State Blockchain Framework fosters a skilled workforce by collaborating with industry and academia to provide blockchain education and training programs. It also supports research, innovation, and infrastructure development to create a conducive environment for blockchain adoption. Additionally, it promotes collaboration and community building to drive blockchain adoption across various sectors.
2. **Supporting Infrastructure:** To foster blockchain innovation and adoption, the Telangana State Blockchain Framework will provide shared infrastructure and resources. This includes subsidized office space for startups, international collaboration to attract investment and knowledge exchange, a sandbox environment for testing blockchain solutions, and cloud computing services to enable Blockchain-as-a-Service offerings.
3. **Promoting Research & Innovation:** The Telangana State Blockchain Framework aims to foster innovation and research in blockchain technology by encouraging collaborations between industry and academia, attracting global talent, funding research programs, supporting startups through incubators and accelerators, and organizing events to facilitate knowledge sharing.
4. **Enabling Collaboration and Building Community:** The Telangana State Blockchain Framework aims to foster collaboration and community building by raising awareness, supporting developer communities, showcasing local successes globally, creating online platforms for networking, joining industry organizations, organizing events, and providing mentorship and support to startups.

3.3.2. T-Chits

T- Chits introduce a blockchain-based system for administering chit funds, a saving and borrowing instrument akin to mutual funds, in the state. The solution helps in preventing fraud in the system and protects retail customers who may be more vulnerable to scams. T-Chit's success is such that it is finding takers of its technology in neighboring states like Tamil Nadu, Karnataka and Andhra Pradesh. *Since its rollout, the Hyderabad-based startup has had a massive impact: it has facilitated savings of over $2.1 billion and more than 1 million subscribers per annum in the State alone.*

Context: "Chit", a traditional yet unique financial instrument, which combines both saving and borrowing option in a single transaction, has become a household name in southern India for ages. Many SMEs from lower and middle-income groups have chosen Chit Funds for their capital and saving needs.

Problem: Both the central and state governments regulate Chit Funds. These entities have an enormous task of managing a huge number of transactions, in addition to enforcement involving loads of paperwork being exchanged between parties. For Chit Fund companies, often plagued by brand image, many unregistered businesses have been sprouting. For subscribers, in a distributed economy, a Chit Fund can play a key role as a complement to other financial instruments/services provided both from the government (SME loans, Free education, Health, etc.) and private financial entities like Banks, non-banking financial companies (NBFCs), and Insurance companies.

Solution: There is a need to enable this quasi-banking industry and rebuild trust into the system, not just by digitizing current processes but also by leveraging next generation technologies. T-Chits have enabled all the application processes, reporting activities and many other operations on a cryptographically secure, permissioned, distributed ledger, smart contract based blockchain.
Tech Stack:

- UI Framework: Angular 4, HTML5, CSS 3.0, PWA, JavaScript
- J2EE framework: Spring Boot, Hibernate, JPA, Flowable BPM
- Database: MySQL, Mongo DB, Couch DB Blockchain IBM Hyperledger Fabric
- Browsers supported: Chrome (for POC)
- Cloud: AWS (Amazon Web Services)

3.3.3. E-Voting

Telangana with C-DAC, conducted India's first smartphone-based e-voting pilot in the Khammam district. The project utilized blockchain to secure votes, ensuring transparency and preventing tampering. It aimed to enhance voter accessibility and explore the potential of technology in elections. Some of the important issues that are addressed while implementing remote e-Voting are as follow:

a. Correct Voter Identification

- **Problem:** Prevent proxy voting and ensure only eligible voters to cast ballots
- **Solution:** Utilize Real-Time Digital Authentication of Identity (RTDAI)
- **RTDAI Features:**
    - o Liveness detection: verifies a real person took the selfie (not a photo)

- o Demographic matching: compares facial features in the selfie with the voter's Electors Photo Identification Card (EPIC) photo
- o Deep learning-based image comparison: identifies discrepancies between photos even with significant changes

- **Benefits**: Proven success in Telangana's Pensioner Life Certificate program with high accuracy

b. Voter Registration

- **Challenge**: Streamline registration for remote e-Voting
- **Solution:** Mobile app registration with user information and selfie submission.
- **Registration Steps:**
  1. Enter name, voter ID, and upload a selfie
  2. Liveness detection and photo matching with EPIC card details occur
  3. Upon successful verification, a transaction ID is sent via SMS and email
- **Expected Success Rate:** 90-95% of voters based on past experience
- **Alternatives for Non-Registered Voters:**
  - o Traditional EVM voting at polling stations
  - o Online or in-person resubmission of details at government centers
- **Security Measures:**
  - o Phone number and International Mobile Equipment Identity (IMEI) number used for registration are tagged to the voter ID
  - o Voting allowed only from the registered mobile phone
  - o One phone can't be used for more than two registrations to prevent proxy voting

c. Server Redundancy

- **Challenge:** Ensure system availability and data integrity in case of server failure.
- **Solution:** Dual server setup in active-active mode
- **Server Locations:**
  - o One set in Ministry of Urban Affairs & Development (MAUD)
  - o Another set in the State Data Centre (SDC)
- **Benefits:**
  - o Every transaction gets recorded in both locations
  - o Enhanced redundancy and data protection

d. Leveraging Existing Expertise

- **Challenge:** Identify qualified entities to develop and implement the solution
- **Solution:** Collaborate with experienced providers and researchers
  - o Potential Partners: National Securities Depository Limited (NSDL) – Indian central securities depository, K-Fintech, Right2Vote.in (e-voting experience), IITs (research expertise), startups specializing in blockchain, encryption, and data security
  - o Crucial Requirement: Enhance data security protocols of existing solutions to meet stringent e-Voting standards

Tech Stack:

- o **AI and Machine Learning:** For liveness detection, biometric matching, and demographic verification

- **Blockchain:** For immutable record-keeping and transparency
- **Encryption:** For secure data transmission and storage
- **Cybersecurity Tools:** For protecting the system from cyberattacks
- **Mobile App Development:** For a user-friendly interface for voter registration and voting
- **Server Infrastructure:** For hosting the e-voting platform and ensuring high availability

3.3.4. Seed Traceability

Telangana is indeed at the forefront of utilizing blockchain for seed traceability. To prevent disbursement of spurious seeds in the agricultural value chain, a blockchain based seed traceability solution was implemented. This initiative aims to enhance transparency, prevent adulteration, and ensure the quality of seeds distributed to farmers.

Process Cycle: The solution involves tracking the journey of seeds from the producer to the farmer. Growers provide verified data about seed production, which is recorded digitally using QR codes. Seeds are then packed and containerized with QR-mapped information, and the distributor onboards them into their inventory management system. Distributors scan for GRN (Goods Received Note) and sell to retailers, who receive SMS notifications upon sale. Farmers can scan the QR code on the seed packet to view the seed's quality, source, and origin, with SMS notifications provided in the local language for better accessibility. This traceability solution ensures transparency and accountability in the seed supply chain, allowing farmers to make informed decisions and trust the quality of the seeds they purchase.

Deployment Landscape: The solution involves two private Seed Production Companies (SPCs) and one government SPC, with approximately 300 seed-producing farmers. The system has enabled the traceability of over 250 metric tons of seeds across two major crops, paddy and cotton. The solution has been implemented across 4 distributors and 9 retailers, reaching approximately 200 seed-buying farmers. This traceability initiative ensures transparency and accountability in the seed supply chain, benefiting all stakeholders from producers to farmers.

Impact:

- **Seed Producing Farmers and Aggregators:**
  - Benefit from managing farm activities and detailed farm mapping
  - Can track the seed journey from sowing to harvest, adhering to the package of practices
- **Seed Producing Companies:**
  - Achieve (Stock keeping Unit) SKU-level traceability with QR codes, enabling better inventory management and efficient production and processing
  - Benefit from an integrated supply chain approach
- **Distributors and Retailers:**
  - Implement container and SKU-level tracking
  - Improve inventory management and operational efficiency
- **Crop Producing Farmers:**
  - Reduce distress and save lives by ensuring the quality and source of seeds
  - Improve productivity by tracing the seed journey

3.3.5. Stree Nidhi

Stree Nidhi in Telangana State is playing a great role in alleviating poverty and helping to enhance the financial status of poor women who are part of Self-Help Groups (SHG), with timely and

affordable credits. Over the years, Stree Nidhi has created a niche in the sphere of microfinance with its low-cost credit delivery. The success of Stree Nidhi Telangana in delivery of low-cost funds to borrowers in need has already attracted national attention and is being implemented in several states across the country. PoST is a Blockchain-based solution to empower poor women, especially the unbanked and underbanked population. *The Loan disbursement and repayments of StreeNidhi for all the 150,000 members will be recorded on a blockchain platform. The Pilot phase will include 150,000 SHG members of the Rajanna District of Telangana.*

Problem: Stree Nidhi's system faced several challenges, both technical and functional. Technically, the system lacked data security, was highly dependent on vendors, lacked transparency, and had high maintenance costs and inadequate performance. Functionally, the system relied heavily on manual work for accountancy, depended on bank loans, and lacked member-level information, including credit history. This hindered the ability to incentivize or disincentivize members based on their financial behavior.

Solution: Stree Nidhi now has an enhanced system for their operational needs, developed based on blockchain technology, which ensures greater transparency, enhanced data security, increased efficiency, and reduced maintenance costs. This system helped Stree Nidhi to significantly reduce operational expenses, while enabling SHG members to leverage their credit history to access other financial products like micro-insurance from external providers.

Tech Stack

- Ethereum Blockchain
- Dharma Protocol
- Java
- ReactJS

3.3.6. Telangana Web3 Regulatory Sandbox[22]

The advent of Web 3.0, powered by blockchain technology, is ushering in a new era of decentralized internet, empowering users and shifting focus from centralized entities. However, the emerging regulatory landscape poses challenges for firms and consumers operating in this space. To address this, the Government of Telangana launched a Web 3.0 Regulatory Sandbox. This initiative aims to create a conducive environment for Web 3.0 startups in India, not only to encourage them to operate within the country but also to assist them in navigating the complex regulatory terrain. By providing a controlled environment for testing innovative products, the Sandbox seeks to foster innovation while ensuring consumer protection and regulatory compliance.

The Execution team is comprised of a Governing Council and an Operations team. The Governing Council is responsible for making the executive level decisions for running the sandbox. The members of the Governing Council have representation from the State government, industry experts, lawyers, academia, VC firms, and other domain experts.

The first cohort of the Sandbox includes eight startups working on sustainable finance, digital asset trading, DeFi for agriculture, DeFi for MSMEs, Social-Fi, real estate tokenization, and media IP registration. The State has Studied regulations, laws, and licenses of different countries to make recommendations for central government reforms.

3.3.7. Asset Tokenization: Technical Guidance Note[23]

This note suggests a path forward on the technical nuances to be considered during tokenization of assets, as well as how the standards around it could be formed. It also sets forward an approach that could be incorporated for any company or startup that wants to pursue the path of asset tokenization. This document could work as a ready reckoner for anyone who wants to tokenize any assets in the State of Telangana. It can serve as guidance for all the projects which are being built within the region and can enable them to get a suggestive pathway. This report also intends to provide guidance to other government agencies that want to look into tokenization.

3.3.8. Corporate Initiatives in Blockchain by Fostering Innovation and Building

Partnerships
The Telangana IT Department has forged partnerships with Tech Mahindra, ISB, HYD DAO, Polygon, Devfolio, Ryze Labs, IBC Media, BITFURY, nagarro, InnoHat Systems, Lukka, Algorand Foundation, ChitMonks, SEQUOIA, Woodstock, European Crypto Initiative, World Economic Forum, International Financial Services Centres Authority (IFSCA), Coinbase, Evident, dygnify, TRST01, Casper, Avalanche, Bharat Web3 Association, and Indian Blockchain.

Innovation
Ripple's University Blockchain Research Initiative (UBRI) has established a partnership with IIIT Hyderabad to conduct in-depth research on blockchain technology and its practical applications. Bitfury and the Indian School of Business (ISB) have also joined forces to advance blockchain education and research in India, aiming to cultivate a skilled workforce and drive innovation in the blockchain industry.

3.3.9. Web3 Community in Telangana: A Hub of Innovation and Collaboration

Telangana has firmly established itself as a leading hub for Web3 innovation in India, driven by groundbreaking events and the initiatives and Collaborations. The state gained international recognition by hosting the **International Blockchain Congress** in 2018, a platform that brought together global industry leaders. To further its mission, Telangana launched the B**lockchain Capacity Building Program**, aimed at educating students and faculty on blockchain fundamentals. Additionally, the **ETHforAll Hackathon** provided an experimental playground for young innovators to explore blockchain and Web3 technologies.

- **Hyderabad DAO: Building the Web3 Ecosystem:** As the most active Web3 developer community in Telangana, Hyderabad DAO has been instrumental in nurturing talent and fostering collaboration with over 2,000 members. The DAO organizes a variety of activities, including monthly blockchain meetups, university sessions, Faculty Development Programs (FDPs) to train educators in blockchain technology and curriculum development, and hands-on blockchain bootcamps that guide participants from foundational knowledge to deploying decentralized applications (DApps)

- **Representation at Global Web3 Conferences:** Hyderabad DAO has showcased Telangana's blockchain initiatives on prominent international platforms, including DevCon (Ethereum Foundation), ETH India, ETH Bangkok, India Blockchain Week (IBW), Token 2049 Singapore, and the Google Cloud Web3 Conclave. These engagements have solidified Hyderabad DAO's reputation as a significant contributor to the global blockchain ecosystem.

- **A Track Record of Success:** Over the past 2.5 years, Hyderabad DAO has hosted **50+ events** in collaboration with **30+ global blockchain companies and protocols**, solidifying its position as India's most active Web3 community. Its mission is clear: to establish Hyderabad as the **Web3 Capital of India**, leveraging the city's renowned technological capabilities and innovative spirit.

- **Global Partnerships**
  Hyderabad DAO has established prominent partnerships including: Aleph Zero, Arweave, Binance, Cosmos, Cardano, Polygon, Shardeum, Polkadot, StarkNet, Reef Chain, Nervos, Algorand, TON, Aurora, Filecoin, StackOS, LBank, OmniFlix, dYdX, Hypersign, Hyperlane, Timechain Labs, Router Protocol, Graviton, Concordium, CoinDCX, Farcaster, Huddle, etc. These collaborations aim to create greater opportunities for local developers and innovators, ensuring Telangana remains at the forefront of the Web3 revolution.

4. INDUSTRY-LED BLOCKCHAIN USE CASES IN INDIA

Industry-led blockchain use cases in India showcase how sectors like finance, healthcare, supply chain, and governance are leveraging blockchain technology to enhance transparency, efficiency, and trust in operations.

4.1. Tokenization

One of the biggest players in the ecosystem, Polygon is driving innovation in cross-border payments with real-time settlement through stablecoins. It has also enabled Flipkart to tokenize and list vouchers on a marketplace, contributing to the growth of e-commerce. Additionally, it is advancing real estate fractionalization through tokenization via the REET mechanism, allowing properties to be converted into equity. In the gold sector, it is enabling gold tokenization and blockchain-based borrowing solutions

4.2. Authenticity and Transparency

4.2.1. Astrix

This solution is utilizing blockchain technology to introduce authentication and transparency into ticketing in the live event industry. This platform represents a significant shift from traditional ticketing systems by introducing a fraud-proof, blockchain-based solution that provides real-time updates and an enriched event experience.

Transforming the Ticketing Experience

- **Fraud-Proof System:** The inherent decentralization and cryptographic security of blockchain enables Astrix to offer a ticketing solution that is virtually immune to fraud. Each ticket issued is a unique, NFT that can be traced and verified on the blockchain, ensuring that counterfeit tickets are virtually nonexistent.
- **Real-Time Updates:** Astrix leverages the blockchain to provide instant updates across the network. Ticket buyers and sellers can receive immediate confirmation of transactions, changes in event details, or any updates directly related to their purchased events. This level of responsiveness enhances customer satisfaction and streamlines event management.

- **Secondary Marketplace and B2B Discovery Platform:** In addition to primary ticket sales, Astrix enables a secondary marketplace that will allow ticket holders to resell their tickets while providing artists and/or event organizers the ability to cap the price charged on that secondary sale. Furthermore, a B2B discovery platform is being developed to connect event organizers with service providers, thereby enriching the event planning ecosystem and creating more value for all stakeholders.
- **Enhanced Event Experience:** The Astrix platform further enhances the overall event experience by integrating digital collectibles, exclusive content, and interactive engagement opportunities directly linked to the event.

Through these innovations, Astrix is setting a new standard for how events are ticketed, attended, and experienced. Astrix is using blockchain not only to ensure authentic and secure ticket sales, but also to enhance the connectivity and interactivity of the live event industry.

4.2.2. LW3

From verifying the origin of Assamese Tea to the reverse tracking of EV batteries, LW3 is utilizing blockchain technology to revolutionize product tracking and traceability through several key mechanisms:

- **Smart Contracts Automation:** LW3 utilizes smart contracts to automate and enforce compliance with sustainable practices and quality standards at each step of the supply chain. This automation not only speeds up transactions but also ensures they are completed without errors and in accordance with predefined rules.
- **Traceability:** LW3 introduces its 'Phygital Product Passport,' a digital certificate that tracks each product from its origin to the consumer. The passport records detailed information – such as the date of harvest or the initial purchase all the way to your kitchen table or to the drop off for recycling – on the blockchain, providing a tamper-proof and accessible log that can be crucial for regulatory compliance, consumer trust, and operational auditing.
- **Embedded Finance:** LW3 is integrating embedded finance into its platform, allowing for instant financial transactions that can support refunds, deposits, or pay-outs to different stakeholders in the supply chain.

LW3's blockchain solution in logistics exemplifies how technology can be leveraged to empower both consumers and producers. This approach not only can authenticate the origin and journey of a product, but also aligns with global sustainability goals by ensuring that materials like batteries are responsibly recycled and reused, reducing environmental impact and promoting resource efficiency.

4.2.3. Women Development & Child Welfare (WDCW)

Avalanche partnered with the Telangana government to develop a blockchain-based solution for the WDCW department. This initiative ensures the transparent and trustworthy delivery of direct benefits to individuals in need.

4.3. Digital Identity

Digital identity solutions powered by blockchain technology are particularly crucial in India, where proving identity can be a significant barrier to accessing essential services for low-income populations. Blockchain offers a secure, decentralized, and tamper-proof platform for

digital identities, facilitating greater inclusivity and access to services. Initiatives that illustrate the application of blockchain in digital identity solutions in India include the SEWA Digital Health Passport and the Mann Deshi Credit Scorecard solution.

Both the SEWA and Mann Deshi initiatives described below showcase the power of blockchain-based digital identity solutions to transform access to healthcare and financial services. These solutions promote inclusion while empowering individuals with ownership and control over their personal data. This approach is particularly effective in bridging the gap for those who have traditionally been underserved by conventional systems, driving forward socio-economic empowerment and equity.

4.3.1. SEWA Digital Health Passport for Healthcare Identity

Lok Swasthya Self-Employed Women's Association (SEWA) recently launched the Digital Health Passport, a blockchain solution designed to improve health access by providing a secure and immutable record of verified credentials, on the Algorand blockchain protocol. The digital passport enables SEWA members and their households to more efficiently enroll in critical health benefits and social safety net programs to provide secure, paperless, and cashless service delivery. This platform ensures that women, especially those from marginalized communities, have secure and easy access to their health records, enabling:

- **Secure Storage and Access:** Individual and household data is stored securely on the blockchain, providing women with control over who can access their information and when.
- **Efficient Health Service Delivery:** With access to their verified documents and personal data, women can more efficiently enroll in critical health and other safety net programs.
- **Enhanced Privacy and Compliance:** The solution adheres to strict data privacy standards, ensuring that personal health information is managed in compliance with national regulations.
- **Economic Empowerment:** The solution not only improves healthcare access but also fosters economic empowerment and self-reliance among women. This is a core goal of India Stack, which seeks to empower all Indians by providing them with tools to access various services seamlessly.

4.3.2. Mann Deshi Credit Scorecard Solution

The **Mann Deshi Foundation** is leveraging blockchain to offer digital identity solutions aimed at financial inclusion. This initiative focuses on providing women entrepreneurs and small business owners in rural areas with digital identities that facilitate access to banking and financial services:

- **Facilitating Financial Transactions:** With a secure digital identity on the blockchain, women can easily open bank accounts, apply for loans, and access other financial services that were previously out of reach due to lack of formal identification.
- **Building Credit Histories:** The blockchain platform allows for the recording of financial history as well as educational and professional experience, helping women build a credit history that can improve their eligibility for future borrowing from other banking institutions.
- **Targeted Programming:** With enhanced information on their clientele, including on their work and educational history, Mann Deshi Foundation will be able to better target training resources to increase financial literacy and borrowing success.

4.3.3. Senior Citizen Identity Verification System

Avalanche, in partnership with the Karnataka government, is developing a proof-of-concept (PoC) for a senior citizen identity verification system on the Avalanche blockchain. This solution aims to streamline age verification and facilitate direct access to government benefits.

4.4. Supply Chain Management

Blockchain technology is revolutionizing supply chain management, from manufacturing to cross border shipment. Companies like ARVO, Autom Axis, and Anveshak are at the forefront of deploying blockchain solutions that address various challenges within the supply chain, from quality control in manufacturing to inefficiencies in documentation processes.

4.4.1. ARVO: Enhancing Traceability and Authenticity

ARVO specializes in providing traceability and authenticity solutions for sectors heavily reliant on supply chain integrity, such as automotive and pharmaceutical industries. Utilizing a combination of artificial intelligence (AI), internet of things (IoT), and blockchain technology, ARVO ensures that products are genuine and traceable throughout their lifecycle. This includes:

- **Real-time Tracking:** Leveraging IoT devices, ARVO provides real-time data on the location and condition of products as they move through the supply chain.
- **Authentication at Every Step:** Using AI, ARVO analyzes patterns and anomalies to detect potential counterfeiting at various stages of the supply chain.
- **Immutable Records:** Blockchain technology records every transaction and movement, creating a tamper-proof ledger that all parties in the supply chain can trust.

4.4.2. Autom Axis: Revolutionizing Trade Documentation

Autom Axis contributes to supply chain efficiency with its FDP Connect solution, which digitizes the bill of lading. This crucial document underpins many global trade operations that have traditionally been prone to inefficiencies and fraud risks when handled in paper form. FDP Connect offers:

- **Digital Efficiency:** The Autom Axis digital format bill of lading document eliminates delays, lost documents, and entry errors associated with paper processing.
- **Enhanced Security:** Blockchain integration ensures that each digital bill of lading is secure and verifiable, reducing the risk of fraud and unauthorized alterations.
- **Global Accessibility:** Stakeholders from any part of the world can access and verify the authenticity of the bill of lading in real-time.

4.4.3. Anveshak: Advancing Traceability in Biofuels and Green Hydrogen

Anveshak introduces a novel application of blockchain technology using a mass balance model to trace sustainable energy sources such as biofuels and green hydrogen. This approach is critical for industries transitioning towards green energy solutions, which require rigorous documentation of the origin and lifecycle impacts of these energy sources. Anveshak's solution provides:

- **Accurate Sustainability Tracking:** Ensures that claims regarding the sustainability of biofuels or green hydrogen are verifiable and based on accurate, real-time data.
- **Mass Balance Traceability:** Utilizes a mass balance approach to track the input and output of sustainable materials throughout the supply chain, ensuring that the environmental impact is accurately recorded and reported.
- **Regulatory Compliance:** Helps companies comply with stringent regulations governing renewable energy credits and carbon emissions.

These companies are setting new standards in supply chain management, leveraging blockchain's inherent capabilities to enhance transparency, security, and efficiency. Their innovations not only solve existing challenges but also pave the way for more sustainable and ethical business practices across industries.

4.4. Microfinance and Inclusion

Blockchain technology is helping make significant strides in microfinance and financial inclusion. **FilmFinance** and **Miniland** are two unique startups from India that highlight the diverse applications of blockchain in facilitating economic empowerment and access to financial services. Both initiatives showcase how blockchain is being utilized to enhance financial inclusion and microfinance opportunities. FilmFinance introduces a new way for individuals to participate in film financing, while Miniland provides innovative solutions for land ownership that can help bridge the wealth gap. These solutions not only foster economic empowerment but also ensure that financial systems are more inclusive, transparent, and efficient.

4.4.1. FilmFinance: Empowering Film Industry Stakeholders

FilmFinance leverages blockchain to transform how investments in the film industry are managed. This platform allows for the secure fractional tokenization of films and web series, enabling:

- **Democratization of Investment:** By offering fractional ownership through tokens, FilmFinance opens up investment opportunities in the entertainment sector to a broader audience.
- **Transparent and Secure Transactions:** The transparent and secure nature of transactions recorded on blockchain provide investors with confidence in the integrity of their investments.
- **Smart Contract Execution:** The use of smart contracts automates the distribution of profits and royalties, ensuring that investors receive their due returns efficiently and without dispute.

4.4.2. Miniland: Revolutionizing Land Ownership and Transactions

Miniland focuses on the tokenization of land, a revolutionary approach that enhances transparency and accessibility in real estate transactions. This platform provides:

- **Simplified Land Ownership Transfers:** Tokenization allows for the seamless transfer of land ownership without the cumbersome bureaucracy typically associated with real estate transactions.
- **Enhanced Access to Capital:** By tokenizing land, property owners can unlock the value of their assets more easily, accessing capital by selling fractional interests in the property.
- **Increased Market Efficiency:** The blockchain-based system reduces fraud, lowers transaction costs, and speeds up processes, making real estate markets more efficient and accessible.

4.5. Sustainability

4.5.1. Sow & Reap

It is pioneering climate tech and finance company based in Hyderabad, is making significant strides to support farmers and other rural residents in their adoption of sustainable technologies. Collaborating with scientists and technical partners, Sow & Reap is utilizing digital monitoring, reporting, and verification (dMRV) technologies to support carbon credit generating projects that span renewable energy and AFOLU (Agro-Forestry and Land Use). Blockchain helps provide immutable records and transparent reporting of dMRV data to generate higher value carbon credits that help incentivize practices with a proven record of mitigating climate change.

4.5.2. Terano

Based out of Delhi, Terano is at the cutting edge of environmental and financial technology, utilizing blockchain solutions to transform the management and trading of carbon credit assets. Key aspects of Terano's blockchain-based solution include:

- **Tokenization of Carbon Credits:** By converting carbon credits into digital tokens on a blockchain, Terano significantly enhances their liquidity, allowing for easier and faster trading, while also opening the market to a broader range of investors.
- **Reduced Costs:** The reduced need for intermediaries in a blockchain-based solution reduces transaction costs, making the carbon credit market more accessible and financially viable for more businesses.
- **Enhanced Risk Management:** With every transaction recorded on a secure, immutable ledger, blockchain reduces the risk of fraud while enabling more accurate tracking of carbon credit origins and ownership.
- **Comprehensive Carbon Management Tools:** Terano provides businesses with precise tools to measure, reduce, and report emissions. These tools help businesses not only comply with regulations but also optimize their carbon usage and reduce environmental impact strategically.

By tokenizing both traded and non-traded carbon credits, Terano aims to enhance the transparency and security of these assets while also improving their liquidity and management efficiency. This innovative approach enables businesses to turn their environmental responsibility into a profitable and strategically advantageous endeavor.

4.6. Securing the Blockchain Ecosystem

In the rapidly evolving blockchain ecosystem, security remains a paramount concern, especially with the increasing adoption of NFTs, digital financial assets, and decentralized applications (dApps). **SecureDapp** and **David's Protocol** are at the forefront of addressing these security challenges.

Together, SecureDapp and David's Protocol provide comprehensive security solutions that address both the operational and financial risks within the blockchain ecosystem. These efforts are crucial for the continued growth and maturation of blockchain technologies, making the ecosystem more secure and appealing to a broader audience.

4.6.1. SecureDapp

This solution is dedicated to strengthening the security framework around decentralized applications by focusing on:

- **Preventive Security Measures:** SecureDapp implements advanced security protocols to safeguard dApps from vulnerabilities from their development phase through to their operational stage.
- **Comprehensive Protection:** The company offers a suite of security tools designed to detect and mitigate potential threats in real-time, ensuring the integrity and reliability of dApps.
- **Building Trust:** By securing dApps against a wide array of cyber risks, SecureDapp plays a critical role in building trust among users and developers, which is essential for the widespread adoption of decentralized technologies.
- **Community and Developer Support:** SecureDapp provides ongoing support and resources to the developer community, empowering them with the knowledge and tools needed to create secure applications.

4.6.2. David's Protocol

It addresses the financial risk aspects of blockchain investments, particularly in the realm of NFTs and digital financial assets. It offers tailored insurance solutions to mitigate risks associated with these investments, enhancing investor confidence through:

- **Tailored Insurance Coverage:** David's Protocol provides specialized insurance products that protect against losses from fraud, theft, and other specific perils that threaten digital assets.
- **Risk Management:** The protocol employs a strategic approach to risk assessment, helping investors understand potential vulnerabilities and how best to protect against them.
- **Enhancing Market Stability:** By offering insurance, David's Protocol contributes to the overall stability of the digital asset market, encouraging more secure and responsible investment practices.
- **Investor Education and Support:** David's Protocol also focuses on educating investors about the importance of insurance in managing risks associated with blockchain investments, offering detailed consultations and support for those looking to secure their digital assets.

4.7. Trading

Avalanche supports impactful Web2 and Web3 projects through grants, investments, and innovation, fostering entrepreneurship and aiding Web2 companies in transitioning to Web3 on Avalanche. Some of their support initiatives include

4.7.1. Growfitter

This solution offers an incentivized wellness platform designed to motivate users to adopt an active and healthy lifestyle. With over 2 million app users, it provides a gamified solution for trading digital assets, tokens, brand NFTs, and real-world assets (RWA) on the Avalanche blockchain. Growfitter has partnered with 100+ premium brands, including Puma, Jockey, Gillette, Sandbox, and more, to deliver engaging and rewarding experiences. By incorporating unique NFT games, a ticketed raffle system, and fitness challenges, Growfitter makes digital asset trading both accessible and enjoyable. The platform anticipates achieving 128,000 daily active users (DAUs), further strengthening its position as a leading wellness and blockchain solution.

4.7.2. TradeX

This solution is an innovative online trading platform that allows users to invest or trade based on predictions about real-world events. Users can speculate on outcomes in areas such as politics, economics, and weather, leveraging their opinions to influence trading decisions. Positioned in the B2C FinTech, Media, and Entertainment segments, TradeX also offers a Loyalty Program that enables users to earn additional rewards. With a goal to onboard 2 million users across India and the APAC region, TradeX is poised to revolutionize event-based trading and user engagement.

4.8. Certifications

4.8.1. IEEE – Certificate Issuance

In collaboration with IEEE, Avalanche has implemented a solution for issuing and verifying certificates on the Avalanche blockchain. This system provides tamper-proof and verifiable credentials for individuals who complete courses with the organization.

4.8.2. Digital Public Goods (DPG)

Avalanche is working with a United Nations agency to integrate Digital Public Goods (DPG) on blockchain. This initiative enables users to receive blockchain-based certificates for completed tasks, which can then be presented to governments for direct benefits like employment or subsidies

4.9. Education and Skilling

Avalanche India is actively promoting blockchain awareness and community building through meetups, workshops, and events across India, including Tier-1 cities like New Delhi and Bangalore, as well as Tier-2 cities like Indore. Its workshops and hackathons at top universities such as IITs and Centurion University of Technology and Management (CUTM) to educate students on blockchain development, attracting over 300 registrations and 250+ in-person attendees on average. Additionally, Avalanche hosted a community game launch in Delhi, showcasing “Off The Grid,” a high-graphics, blockchain-based AAA game, highlighting the transformative potential of Avalanche-powered technology in gaming.

Polygon’s Web3 Made in India tour is set to engage developers, entrepreneurs, and students across India through seven Guild events and campus collaborations with experiential learning platform Reskill. Polygon aims to deliver hands-on blockchain education to students at 50 colleges, with cohorts of 50-100, culminating in micro-hackathons to showcase their dApps. Additionally, Polygon is partnering with Pesto Tech to help Web2 developers transition to Web3, aiming to build a network of skilled developers for future blockchain innovation

4.10. Bharat Web3 Association (BWA)

India is on the brink of a digital transformation, with the Web3 revolution poised to reshape the nation's economy, governance, and society. With its decentralized, transparent, and user-focused approach, Web3 is unlocking unparalleled opportunities for growth, inclusivity, and empowerment. Our latest report, the Web3 Compendium, highlights over 400 Web3 firms, showcasing the dynamic entrepreneurial spirit and innovation of Indian pioneers. From decentralized finance (DeFi) and blockchain infrastructure to NFTs, the Metaverse, decentralized autonomous organizations (DAOs), and custody wallets, Indian companies are leading the way in leveraging Web3 technologies to create transformative applications and services - Dilip Chenoy, Chairman, BWA

The Bharat Web3 Association (BWA) is an industry body representing leading members of India's Web3 ecosystem. Its members include prominent infrastructure providers such as Polygon; Virtual Digital Assets (VDA) exchanges like CoinDCX, Coinbase, and CoinSwitch; gaming platforms such as Hike; and other Web3 innovators like Liminal and KoinX.

BWA is committed to strengthening India's Web3 ecosystem by raising awareness, conducting research, establishing industry standards, and fostering indigenous talent. Aligned with initiatives like Atma Nirbhar Bharat, Start-Up India, and Digital India, it emphasizes the transformative potential of Web3 to contribute significantly to India's economy and technological progress. Through its internal subcommittees, BWA formulates focused strategies in areas such as policy, compliance, and partnerships to drive innovation and ensure a structured approach to Web3 adoption.

Key partnerships include working with the Government of Telangana on Web3 regulatory sandbox, collaborating with Maharashtra on State Skills University, and engaging with global entities like Blockchain Australia, Blockchain Association Singapore and the European Crypto Initiative. It engages with regulators and industry players to create comprehensive reports and foster a conducive environment for Web3 growth. This includes Consumer Protection Guidelines, AML Compliance under PMLA regulations, and the recently released Web3 Compendium, with more than 400 Web3 based firms operating in India recorded. Articles by BWA leaders and members have been published in various publications, including Economic Times, Business World, and Financial Express.

5. CHALLENGES IN BLOCKCHAIN ADOPTION

5.1. Technical Challenges: Scalability, Security, and Integration

India's blockchain journey faces hurdles in scalability, security, and integration. The technology's inherent limitations in processing high transaction volumes and maintaining privacy need to be addressed. Ensuring data security and preventing vulnerabilities is crucial. Seamless integration with existing systems, interoperability requirements such as standardizing data formats, protocols, and APIs, along with rigorous testing, is also essential for broader adoption.

5.2. Navigating Compliance Challenges

India's current regulatory landscape presents significant challenges for startups operating in the emerging technology sectors. The absence of clear and comprehensive frameworks in several areas is hindering innovation and driving businesses to seek more favorable jurisdictions. Some are mentioned below:

- Financial Services and Cryptocurrencies: A comprehensive regulatory framework for digital lending, clear cryptocurrency regulations, and streamlined AML (Anti-Money Laundering) processes are essential for India's fintech ecosystem. Startups face increased compliance costs due to stringent AML regulations, leading to higher operational expenses and reduced profit margins.

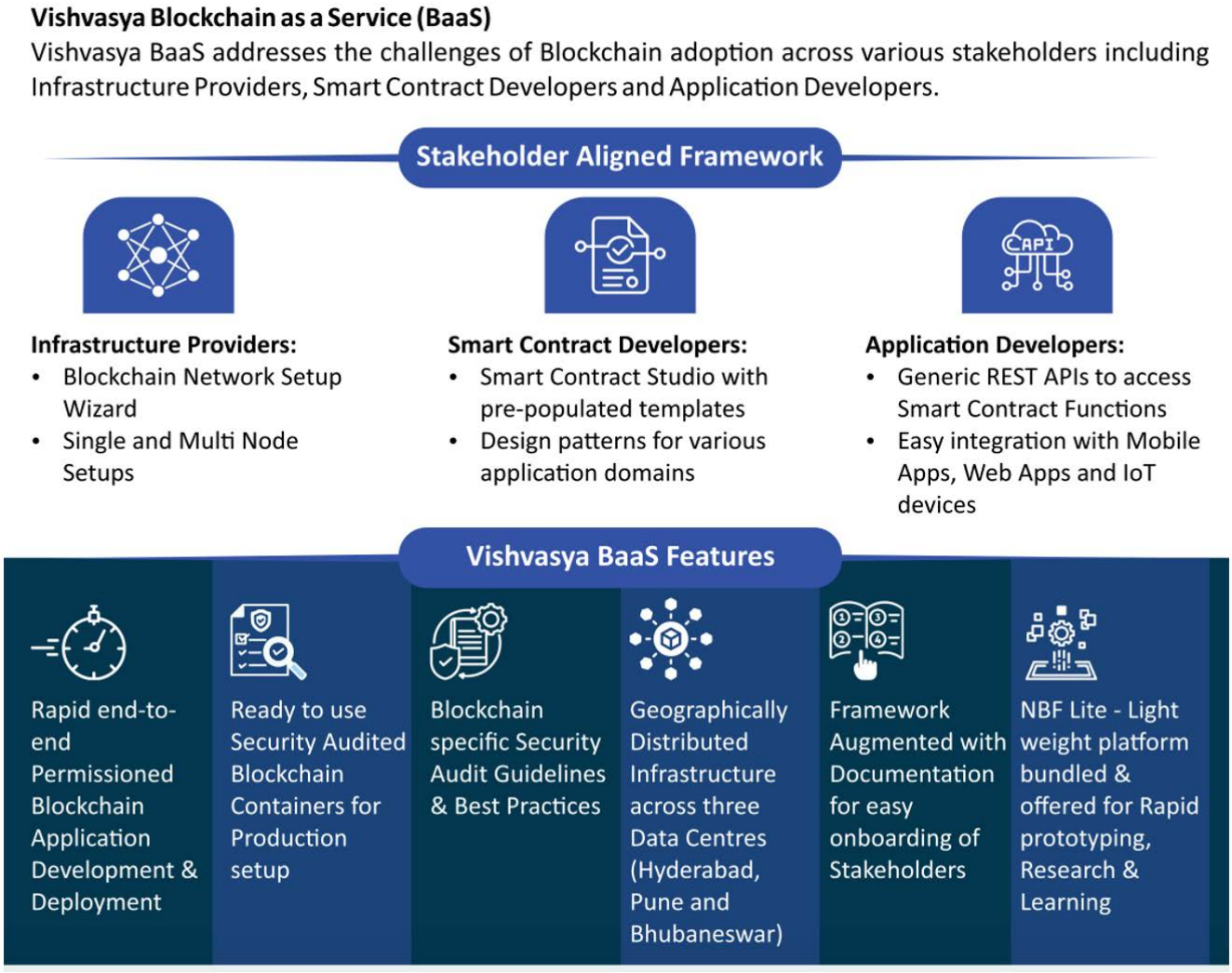
- India requires standardized carbon credit verification (Environment, Social & Governance) to promote sustainable business practices for carbon offset blockchain projects and attract green investments. Robust risk management frameworks and clear regulations on electronic signatures are needed to support business growth and operations in India.

5.3. Market Adoption Barriers: Awareness, Trust, and Education

Widespread adoption of blockchain in India is hindered by factors such as low awareness, trust issues, and inadequate education. Many people are unfamiliar with the technology and its benefits. Building trust in decentralized systems is essential. Moreover, there's a need for comprehensive education and training programs to equip individuals and organizations with the necessary knowledge and skills.

6. APPENDIX

Vishvasya: National Blockchain Technology Stack - Enabling trust in digital systems



Full details here: https://static.pib.gov.in/WriteReadData/specificdocs/documents/2024/sep/doc202494387501.pdf

SOURCES:

1. https://www.business-standard.com/markets/cryptocurrency/india-has-over-19-million-crypto-investors-with-75-youth-report-123122200814_1.html, https://economictimes.indiatimes.com/tech/technology/indian-web3-industry-to-reach-1-1-billion-by-2032-report/articleshow/98632635.cms?from=mdr
2. https://www.statista.com/outlook/dmo/fintech/digital-assets/india
3. https://tracxn.com/d/explore/blockchain-in-financial-services-startups-in-india/__RaWEWQGswGy0BjCoE4i4pXwnHxjnwRwm42Zpug4d-os/companies
4. https://community.nasscom.in/communities/blockchain/web-30-investor-market-india-calling#:~:text=In%202021%2C%20international%20funds%20invested,to%20data%20shared%20by%20Tracxn

5. https://it.telangana.gov.in/wp-content/uploads/2022/12/Telangana-Blockchain-Framework.pdf
6. https://www.expresscomputer.in/news/the-1st-international-blockchain-congress-creates-the-largest-blockchain-event-in-asia/27605/
7. https://education.economictimes.indiatimes.com/news/bimtech-and-kalp-decentra-foundation-announce-strategic-collaboration-to-establish-blockchain-learning-centre/112643092, https://ciso.economictimes.indiatimes.com/news/iits-prepare-for-web-3-0-future-to-offer-crypto-blockchain-nft-courses/94143882
8. https://www.pwc.in/consulting/technology/emerging-tech/blockchain-lab.html
9. National Strategy on Blockchain, MeitY, 2021: https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf
10. National Blockchain Framework Brochure, MeitY, https://static.pib.gov.in/WriteReadData/specificdocs/documents/2024/sep/doc202494387501.pdf, Press Information Bureau; C-DAC, https://pib.gov.in/PressReleasePage.aspx?PRID=2051934
11. PIB launch 2022 - https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883
12. RBI's currency and finance report: https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RCF29072024D5F1960668724737AD152F783DB63F10.PDF
13. Forbes India: https://www.nic.in/emergings/centre-of-excellence-for-blockchain-technology/
14. Livemint https://www.livemint.com/money/personal-finance/what-g20-decided-on-crypto-and-foreign-assets-11694453267825.html
15. https://www.india-briefing.com/news/cryptocurrencies-in-india-to-be-subject-to-anti-money-laundering-aml-compliance-27354.html/
16. https://tnega.tn.gov.in/page/36
17. https://landrecords.karnataka.gov.in/Service2/
18. https://igr.karnataka.gov.in/new-page/Block%20Chain/en
19. https://www.deccanherald.com/india/karnataka/karnataka-to-use-blockchain-for-property-registration-934862.html, https://mahabhumi.gov.in/
20. https://indianexpress.com/article/cities/mumbai/maharashtra-to-protect-property-e-registration-agreements-with-blockchain-technology-8135241/https://agri.punjab.gov.in/
21. https://agriwelfare.gov.in/Documents/DPR_Punjab.pdf
22. https://www.magzter.com/stories/Computer-Mobile/Express-Computer/Rajasthan-Leads-Indias-First-Government-Blockchain-Implementation?srsltid=AfmBOop6OlWsyWYmnTa5ZgBf9758GBT9haE03PDBfa6zi7NzFhVwHrjA
23. https://invest.up.gov.in/wp-content/uploads/2023/10/Uttar-Pradesh-Government_091023.pdf, https://web3sandbox.telangana.gov.in/

CONTRIBUTORS:

1. Jayesh Ranjan, IAS: Special Chief Secretary for Information Technology, Electronics & Communications (ITE&C) and Industries & Commerce Departments of Government of Telangana.
2. Lakshmi Eswari, Senior Director & Centre Head, Centre For Development of Advanced Computing (C-DAC)
3. Sukriti Govil, Consultant, Emerging Technologies Wing, ITE&C Department, Government of Telangana
4. Ragini Laskar, Consultant (YCP-Auctus), ITE&C Department, Government of Telangana
5. Anil Kakani, VP & India Country Head, Algorand Foundation
6. Nikhil Varma, Technical Lead – India, Algorand Foundation
7. Aishwary Gupta, Global Head of Payment, Polygon Labs
8. Kamakshi Arjun, BD Lead India - Enterprises & Institutions, Ava Labs
9. J. Siv Ram Shastri, Co-Founder, Hyderabad DAO
10. G. Rohan Reddy, Co-Founder, Hyderabad DAO
11. Diana Barrero Zalles, Head of Research and Sustainability, Global Blockchain Business Council
12. Rama Devi Lanka, Director of Emerging Technologies Wing, Officer on Special Duty, Information and Technology Department, Government of Telangana, India

ENDNOTES

AI & BLOCKCHAIN CONVERGENCE:

1. https://www.key4biz.it/wp-content/uploads/2023/03/Global-Economics-Analyst_-The-Potentially-Large-Effects-of-Artificial-Intelligence-on-Economic-Growth-Briggs_Kodnani.pdf
2. https://www.nytimes.com/2023/05/23/business/ai-picture-stock-market.html
3. https://www.linkedin.com/pulse/ais-blindspot-blue-ocean-innovation-represents-brigitte-piniewski-md-1xhac/
4. https://www.prnewswire.com/news-releases/the-neuralfabric-generative-ai-platform-pioneers-micro-foundation-models-to-decrease-costs-ensure-data-sovereignty-and-democratize-ai-302075181.html
5. https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation

DECENTRALIZED FINANCE (DEFI):

1. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf
2. https://www.chainalysis.com/blog/2021-global-defi-adoption-index/
3. https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/
4. https://www.chainalysis.com/blog/2024-crypto-money-laundering/#:~:text=In%202023%2C%20illicit%20addresses%20sent,obfuscating%20the%20movement%20of%20funds.
5. https://www.cftc.gov/media/10321/CFTC_GMAC_DAM_Classification_Approach_and_Taxonomy_for_Digital_Assets_030624/download
6. https://www.owlexplains.com/en/
7. https://assets.ctfassets.net/eynrhjw8vyk9/6rJQPJfWcdGgp3MYBEndOd/1ccd9500c4ce4dd4939b44ee044a2171/Owl_Explains_-_IJBL_Volume_VIII.pdf
8. https://global-dca.org/core-principles/
9. https://global-dca.org/wp-content/uploads/2024/10/Information-Guidelines-for-Tokens-Available-in-US-FINAL-Oct-20-2024-1.pdf
10. https://www.gibraltarlaw.com/insights/post/102il0f/dlt-regulation-in-gibraltar-the-ten-principles/
11. https://github.com/OpenZeppelin/openzeppelin-contracts
12. https://www.steptoe.com/a/web/gVYaEV4B1drh8mne29DBvC/gfma-gdf-smart-contract-primer-report-2024.pdf
13. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf. One shortcoming of the IOSCO report is its failure to recognize that DeFi allows all asset classes to transact, not just financial instruments. The IOSCO report also lacks a definition of "decentralized" and does not differentiate between protocols that call themselves DeFi even though they are not decentralized. Notwithstanding these and other deficiencies, the IOSCO report's recommendations provide a solid set of reference points for approaching DeFi.

DIGITAL IDENTITY AND BLOCKCHAIN:

1. https://en.wikipedia.org/wiki/Digital_identity (accessed on 14th October, 2024)
2. https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2#what-are-digital-identities (accessed on 14th October, 2024)
3. https://www.sezoo.digital/
4. https://www.linkedin.com/posts/sezoo_trustworthy-digital-ids-as-a-foundation-for-activity-7240235397006442497-hCrj/ (accessed on 20th October, 2024)
5. Umar Bashir Mir, Arpan K. Kar, Yogesh K. Dwivedi, M.P. Gupta, R.S. Sharma, Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India, Government Information Quarterly, Volume 37, Issue 2, 2020, 101442, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2019.101442
6. https://sovrin.org/principles-of-ssi/ : Principles of Self-Sovereign Identity published by The Sovrin Foundation (accessed on 14th October, 2024)
7. https://www.bhutanndi.com/ : Bhutan NDI (accessed on 14th October, 2024)
8. https://mosip.io/ : MOSIP (accessed on 14th October, 2024)
9. https://www.digitalpublicgoods.net/ : Digital Public Good Project (accessed on 14th October, 2024)
10. https://pages.nist.gov/800-63-4/ (accessed on 7th October, 2024)
11. https://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf
12. https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf
13. https://www.ibia.org/download/datasets/5741/IBIA%20Ethical%20Use%20of%20Biometric%20Technology%20FINAL.pdf
14. https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf
15. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure/
16. https://www.iom.int/news/west-africa-moves-towards-biometric-identity-cards (accessed on 2nd November, 2024)
17. https://nationalpopulation.gov.ng/press-release/launching-of-the-national-geospatial-data-repository-the-digital-civil-registration-and-vital (accessed on 2nd November, 2024)
18. https://projects.worldbank.org/en/projects-operations/project-detail/P179040 (accessed on 2nd November, 2024)
19. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099090424093523075/p505094127c43207b1a297190f5dac37edb (accessed on 2nd November, 2024)
20. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099061523065541763/p18049509fb3f3000b48602cc780351af2 (accessed on 2nd November, 2024)
21. https://stellar.org/case-studies/unhcr
22. https://stellar.org/blog/thought-leadership/one-year-of-stellar-aid-assist
23. https://www.worldbank.org/en/news/press-release/2024/05/21/global-carbon-pricing-revenues-top-a-record-100-billion
24. https://www.worldbank.org/en/news/factsheet/2024/11/12/carbon-markets
25. https://gbbcouncil.org/wp-content/uploads/2023/11/CET-Protocol-IWA-November-2023.pdf
26. https://toronet.org/agrifi-2/
27. https://toronet.org/wp-content/uploads/2024/06/Toronet-Whitepaper.pdf

28. https://cdpi.dev/ (accessed 10th November, 2024)
29. https://www.nsw.gov.au/media-releases/digital-roadmap-drives-innovation-and-delivers-for-communities (accessed 10th November, 2024)
30. https://publicsafety.ieee.org/topics/high-tech-border-security-current-and-emerging-trends
31. https://www.cbp.gov/border-security/along-us-borders/us-border-patrol-technology
32. https://www.trade.gov/country-commercial-guides/italy-digital-economy
33. https://www.agid.gov.it/en/intervention-areas/digital-identity
34. https://www.italiadomani.gov.it/en/Interventi/investimenti/infrastrutture-digitali.html
35. https://www.agid.gov.it/en/news/the-italian-strategy-for-artificial-intelligence
36. https://blockworks.co/news/buenos-aires-id-ethereum-zksync (accessed 14th November, 2024)
37. https://50in5.net/
38. https://gan.foundation/ (accessed on 12th November, 2024)
39. https://identifinity.net/what-is-the-global-acceptance-network-gan-and-do-we-need-it-e4fc2147ee0b (accessed on 12th November, 2024)
40. https://github.com/finternet-io/dedi (accessed on 12th November, 2024)
41. https://www.bhutanndi.com/article/bhutan-s-national-digital-identity-embodies-the-king-s-vision-of-a-digitally-connected-prosperous-society_3a777c24-8891-480b-9b02-e583ba1565da
42. https://parliament.bt/uploads/topics/16920885498838.pdf
43. https://www.bhutanndi.com/company/vision-mission
44. https://parliament.bt/national-digital-identity-act-of-bhutan-2023
45. https://digital-strategy.ec.europa.eu/en/library/european-blockchain-sandbox-best-practices-report

SUPPLY CHAIN:

References:

- FACT SHEET: Implementing the National Standards Strategy for Critical and Emerging Technology
- U.S. Government National Standards Strategy For Critical And Emerging Technologies (USG NSSCET): IMPLEMENTATION ROADMAP
- Enabling Standards Development Through Public-Private Partnerships – Prepared by the American National Standards Institute (ANSI)
- The Standards Alliance: Phase 2 (SA2)
- NIST Awards $15 Million to ASTM International to Establish Standardization Center of Excellence

Endnotes:

1. With this motive, NIST awarded a grant to ASTM International for a Standardization Center of Excellence for Critical and Emerging Technologies

INDIA:

1. CoinSwitch, https://www.business-standard.com/markets/cryptocurrency/india-has-over-19-million-crypto-investors-with-75-youth-report-123122200814_1.html, https://economictimes.indiatimes.com/tech/technology/indian-web3-industry-to-reach-1-1-billion-by-2032-report/articleshow/98632635.cms?from=mdr, Statista - https://www.statista.com/outlook/dmo/fintech/digital-assets/india, Tracxn - https://tracxn.com/d/explore/blockchain-in-financial-services-startups-in-india/__RaWEWQGswGy0BjCoE4i4pXwnHxjnwRwm42Zpug4d-os/companies, https://community.nasscom.in/communities/blockchain/web-30-investor-market-india-calling#:~:text=In%202021%2C%20international%20funds%20invested,to%20data%20shared%20by%20Tracxn
2. https://it.telangana.gov.in/wp-content/uploads/2022/12/Telangana-Blockchain-Framework.pdf https://www.expresscomputer.in/news/the-1st-international-blockchain-congress-creates-the-largest-blockchain-event-in-asia/27605/ https://education.economictimes.indiatimes.com/news/bimtech-and-kalp-decentra-foundation-announce-strategic-collaboration-to-establish-blockchain-learning-centre/112643092, https://ciso.economictimes.indiatimes.com/news/iits-prepare-for-web-3-0-future-to-offer-crypto-blockchain-nft-courses/94143882
3. https://www.pwc.in/consulting/technology/emerging-tech/blockchain-lab.html
4. National Strategy on Blockchain, MeitY, 2021: https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf
5. *National Blockchain Framework Brochure, MeitY, Press Information Bureau; C-DAC*
6. *National Blockchain Framework Brochure, MeitY, Press Information Bureau; C-DAC*
7. *National Blockchain Framework Brochure, MeitY, Press Information Bureau; C-DAC*
8. *National Blockchain Framework Brochure, MeitY, Press Information Bureau; C-DAC*
9. *National Blockchain Framework Brochure, MeitY, Press Information Bureau; C-DAC*
10. *PIB launch 2022 - https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1882883*
    RBI's currency and finance report https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/RCF29072024D5F1960668724737AD152F783DB63F10.PDF
11. *National Strategy on Blockchain, MeitY, 2021, Forbes India https://www.nic.in/emergings/centre-of-excellence-for-blockchain-technology/*
12. *Livemint*
13. https://economictimes.indiatimes.com/industry/telecom/telecom-news/trai-pushes-meity-to-act-strongly-to-curb-spam-phishing-on-ott-apps/articleshow/113104092.cms?from=mdr
14. https://www.india-briefing.com/news/cryptocurrencies-in-india-to-be-subject-to-anti-money-laundering-aml-compliance-27354.html/
15. *National Blockchain Framework Brochure, MeitY, Press Information Bureau; C-DAC*
16. https://tnega.tn.gov.in/page/36
17. https://landrecords.karnataka.gov.in/Service2/, https://igr.karnataka.gov.in/new-page/Block%20Chain/en, https://www.deccanherald.com/india/karnataka/karnataka-to-use-blockchain-for-property-registration-934862.html
18. https://mahabhumi.gov.in/, https://indianexpress.com/article/cities/mumbai/maharashtra-to-protect-property-e-registration-agreements-with-blockchain-technology-8135241/
19. https://agri.punjab.gov.in/, https://agriwelfare.gov.in/Documents/DPR_Punjab.pdf
20. https://www.magzter.com/stories/Computer-Mobile/Express-Computer/Rajasthan-Leads-Indias-First-Government-Blockchain-Implementation?srsltid=AfmBOop6OlWsyWYmnTa5ZgBf9758GBT9haE03PDBfa6zi7NzFhVwHrjA, https://invest.up.gov.in/wp-content/uploads/2023/10/Uttar-Pradesh-Government_091023.pdf

21. https://web3sandbox.telangana.gov.in/
22. https://web3sandbox.telangana.gov.in/
23. https://it.telangana.gov.in/wp-content/uploads/2023/12/Technical-Guidance-Note-on-Asset-Tokenization.pdf