GSMI UPDATE

GLOBAL STANDARDS MAPPING INITIATIVE 4.0

NOVEMBER 2023

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 4.0

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 4.0, GBBC is profoundly grateful for the active participation of **100+ contributors from 75+ entities** spanning government, corporates, startups, nonprofits, and academia, who also took part in **6 specialized working groups**. 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.

GBBC and its partners released the first version of GSMI in 2020 (GSMI 1.0) to highlight the most relevant topics for this emerging industry. This included an interactive map of regulatory developments across 185 jurisdictions, a legal and regulatory report, a technical report cataloguing outputs from over 30 technical standard-setting bodies, a taxonomy of concepts for blockchain and digital assets, and a list of industry consortia.

In response to insights and feedback from the initial release, GBBC later partnered with 130 leading institutions, including over 200 participants across 9 topic-specific working groups, to release GSMI 2.0 as an expansion and continuation of the initial work.

The findings, key insights, and action-oriented guidance proposed by the working groups were captured in an initial series of reports covering the role of blockchain technology for the green economy, taxation, derivatives, and other topics. GSMI 2.0 further updated the interactive map of regulatory developments to contain 187 jurisdictions, further developed the repository of technical standards bodies to include 37 entities, and added to the taxonomy to include 182 terms. Finally, GSMI 2.0 introduced a new catalogue of accredited academic institutions offering a combined list of 300+ blockchain courses.

GSMI 4.0 continues to update and add to the repository of resources with the most relevant updates in the fast-changing environment in which blockchain technology and digital assets are developing. As new themes and stakeholders become relevant, existing ones continue to mature.

For the regulatory map, the team expanded the content and made it more user-friendly, covering **230 jurisdictions** & **6 international regulatory bodies**, while introducing a new filtering features by key issue. GSMI 4.0 also expanded the taxonomy to include 350 terms, including multiple definitions for blockchain and digital assets terms 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. The technical standards section was made more comprehensive to include **63 bodies advancing standards**, characterized as globally or regionally-focused standards setters, associations, and regulators setting standards for various aspects of the industry.

GSMI 4.0 also 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 4.0 releases 4 in-depth reports as the output of 4 working groups focused on specific areas where blockchain technology can have significant opportunities to develop. These reports blockchain in the context of **Convergence with Artificial Intelligence**, **Digital Identity**, **Supply Chain**, and **Sustainability**. In addition, in collaboration with key stakeholders, GSMI produced a **Country Spotlight on Brazil**, covering the current status of developments in blockchain and digital assets in the country.

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.

We would like to thank our many partners, members, and supporters who worked tirelessly and enthusiastically over the past months to produce GSMI 2023, version 4.0, including:

Working Groups

SUPPLY CHAIN
CO-CHAIRS

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

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

SUSTAINABILITY
CO-CHAIRS

DAVID FORTSON
Director, Blockchain x Climate (BxC); Chief Executive Officer and Founder, LOA Labs

BLAKE GOUD
Chief Executive Officer, RFI Foundation

DIGITAL IDENTITY
CHAIR

SANKARSHAN MUKHOPADHYAY
VP, Customer Experience, Dhiway

TAXONOMY
CO-CHAIRS

BRYONY WIDDUP
Partner, Hogan Lovells

MICHAEL WECHSLER
Adjunct Lecturer, City University of New York (CUNY), Queens College

TECHNICAL STANDARDS
CO-CHAIRS

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

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

AI & CONVERGENCE
CHAIR

JENNY CIEPLAK
Partner, Latham & Watkins

Partner Programs

2023 IFC-MILKEN INSTITUTE CAPITAL MARKETS SCHOLARS

GABRIELA SHIBATA
Head of Cash Equities Products at Brazilian Stock Exchange and OTC (B3)

ABROR MIRZO OLIMOV
Deputy Director, Monetary Operations Department at Central Bank of Uzbekistan

GSMI 4.0 FELLOWS

JOSEPH HAAR
Queens College, CUNY

ISHRAQ HUDA
Queens College, CUNY

Thank you to our team of contributors representing over 70 organizations:

A100X, ACIFMA, Abstract srl, AIGC Chain, Alfonso Govela Thomae, Avanade/Accenture, Ava Labs, Babesta, Blockchain Laboratories, BLKF, Brazil Crypto Report, Brazil Stock Exchange (B3), BTG Pactual, BxC, Central Bank of Brazil, Central Bank of Jordan, Central Bank of Uzbekistan, Citizensbank, Clifford Chance, Climatecoin, Code Green, Daphne Liu, Digital Token Identifier Foundation, Dino Dell'Accio, DLA Piper, EBRD, FedEx, First National Bank of Omaha, Florida Institute of Technology, Forest Stewardship Council, George Washington University, HBAR Fund, Heifer International, Hogan Lovells, Home of Blockchain.swiss, Hyperledger, Identity Woman, KAIST, Kismetrics, KlimaDAO, KPMG, Landis & Co., Latham & Watkins, Leadingbit, Lexicon of Sustainability, Liongate Bahamas Limited, LOA Labs, Loxley Graham, Makki ElFatih, Mercury Strategies, Nataliya Dyka, Oliver Wyman, OpenID Foundation, Paravella, Paul Hastings, Punchline Audio Authentication, Queens College, City University of New York, Rainforest Partnership, Real Variable, RecycleGo, RFI Foundation, Salesforce, SBI Digital Assets, State of Pennsylvania, Summer Graham, TerGo, Tokeny, Truist, Tunisia Ministry of Education, U.S. Blockchain Coalition (USBC), University of Arkansas, University of Wyoming, UPS, Yield App, YNBC, Zumo.

Special thanks to the GBBC team for their contributions:

- Diana Barrero Zalles
- Greg Buron
- Tristen Dague
- Riley Fay
- Michele Hubbard
- Sierra Lewis
- Paul Rapino
- Sandra Ro
- Jackson Ross

SECTION II

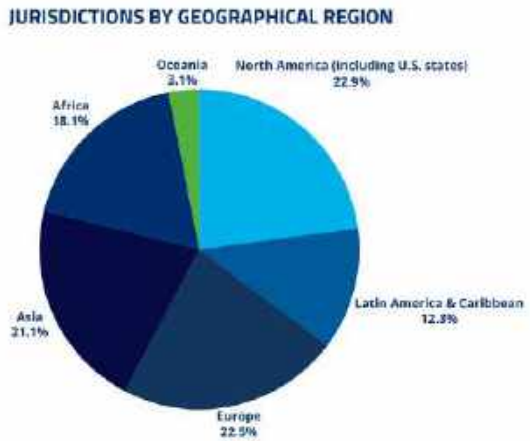
LEGISLATION AND REGULATORY DEVELOPMENTS

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. The growth of this technology can benefit greatly with increasing regulatory clarity, a harmonized approach across jurisdictions, and a balance that will support innovation in a way that fosters inclusion without forsaking security and protections for consumers and investors.

The road ahead continues to be paved. Instances of excessive hype, irregular activity outside the purview of regulation, and resulting losses have highlighted the need for adequate regulation time and time again. Government bodies are increasingly taking part in discussions and assessments for regulatory requirements, regulatory sandboxes are facilitating testing environments, and enforcement actions and case law are setting new precedents for the legal treatment of this technology.

GSMI 4.0 includes 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 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. Among the major issues of focus for regulatory developments, the most common ones have been selected and quantified in the diagram.

ACCESS THE MAP



SECTION III

TAXONOMY

In order to foster the level of collaboration across stakeholders necessary for scale, it is essential to operate under a common language. As the space develops at lightning speed, where definitions can evolve at the pace of 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 Taxonomy includes **350+ terms** specific to blockchain and digital assets, categorized as essential terms, non-essential terms, and sector-specific terms. Terms considered essential to blockchian and digital assets have been further categorized 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 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.

This taxonomy is meant to be an interactive resource, where users can pick a definition from the landscape of sources listed in the drop-down menu for each term. It is also meant to be a dynamic resource that will evolve over time as the space continues to develop.

At the core of the GSMI taxonomy is the acknowledgement that global innovators creating solutions to address society's toughest challenges need globally accepted standards to facilitate impactful and responsible cross-border innovation. This work builds on materials and knowledge from prior shared taxonomies, and in highlighting industry-specific concepts, emphasizes the tangible ways that this technology can transform our everyday lives.

Moreover, often regulatory clarity follows advances in collaborative developments resulting in applications that work well across stakeholders, where a shared acceptance of best practices is built on common terminology and understanding. Taxonomy is imperative for harmonized global regulatory developments which are fundamental for scale and credibility. Regulators around the world have produced taxonomies to classify digital assets, as well as definitions preceding statutes, as part of comprehensive frameworks in development that are tailored for this space. This resource is meant to be utilized as a resource to support such efforts.

Finally, we welcome recommendations and additional resources that will enable us to further refine the quality and scope of this effort.

VIEW THE LIST OF TAXONOMY

SECTION IV

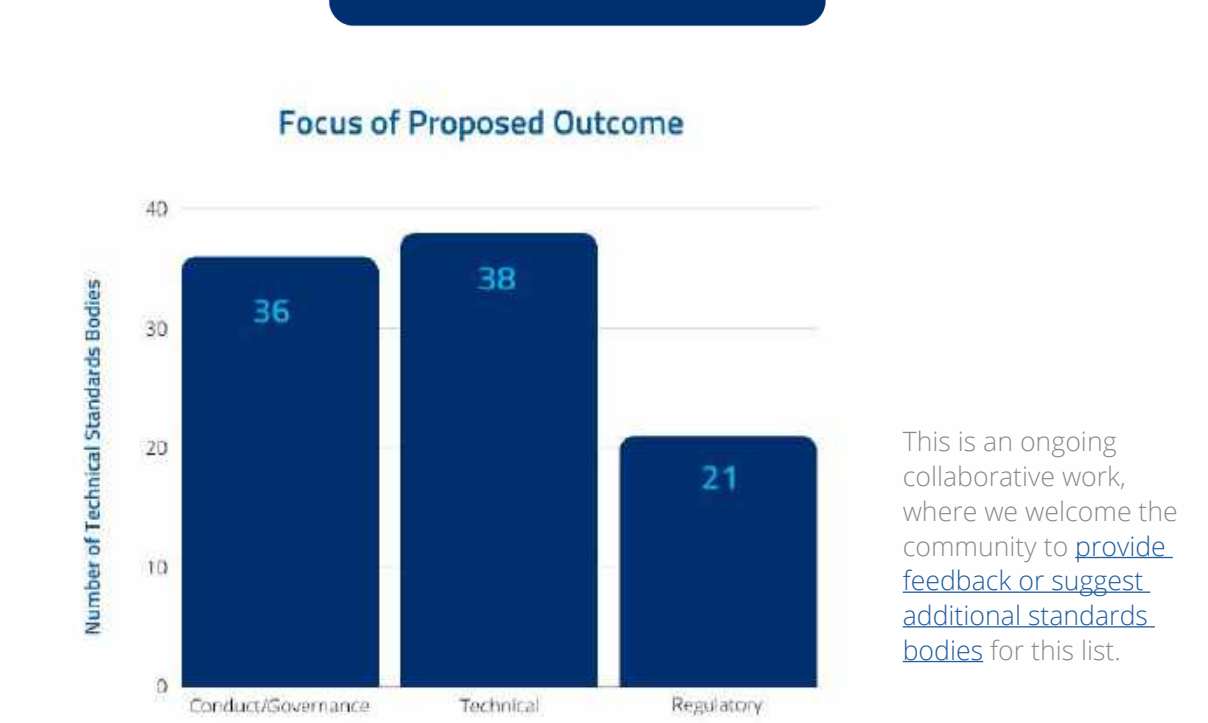
TECHNICAL STANDARDS

Technical standards for developments in blockchain and digital assets, as in any new technology, are fundamental to ensure safety, reliability, and further innovation. 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 **63** 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.

We worked to make it easier 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.

ACCESS TECHNICAL STANDARDS



This is an ongoing collaborative work, where we welcome the community to provide feedback or suggest additional standards bodies for this list.

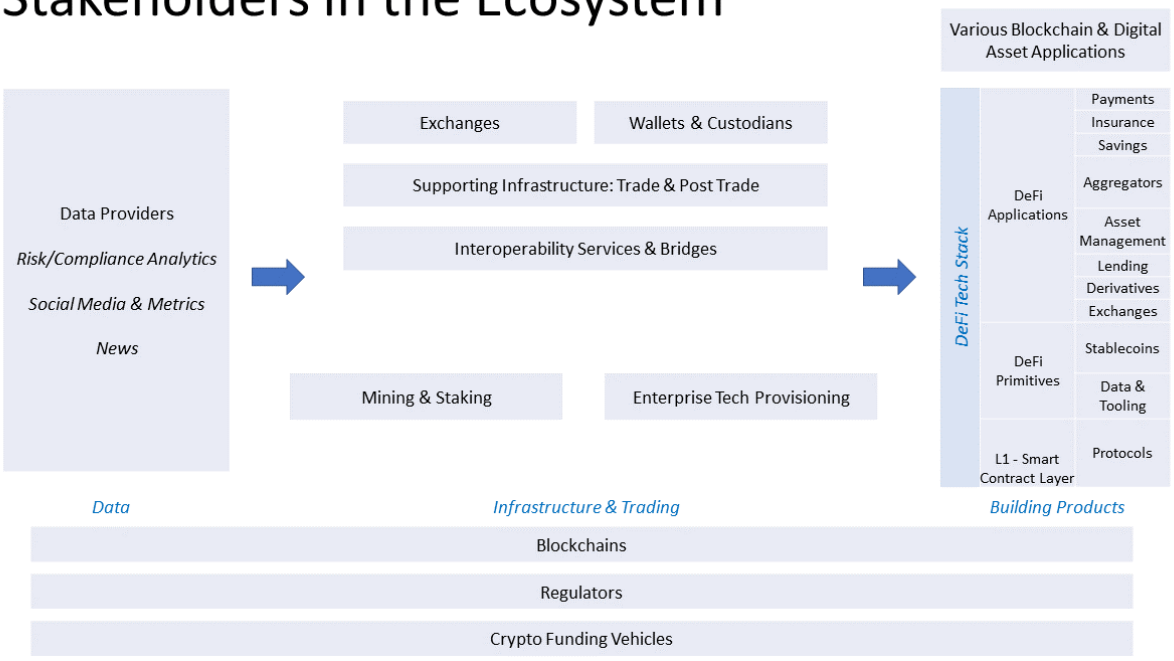
SECTION V

BLOCKCHAIN AND 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 4.0 offers a continually updated global mapping of this landscape, with key stakeholders and their interactions, as summarized in the diagram. GSMI 4.0 also provides access to the full list of **2,000+** players, and welcomes further suggestions from the community. We are in the early innings of this multi-trillion dollar industry, with many more developments underway and innovations to come.

ACCESS THE COMPLETE LANDSCAPE

Stakeholders in the Ecosystem

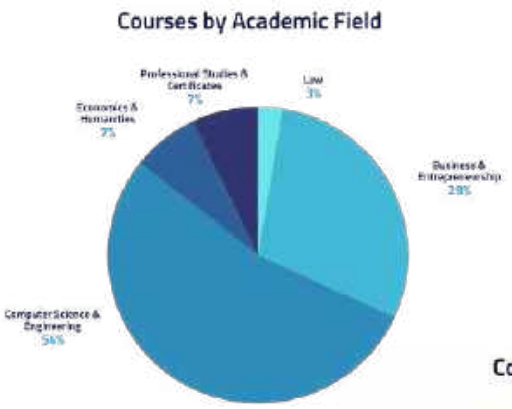


SECTION VI

UNIVERSITY COURSES

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 LIST



SECTION VII

ARTIFICIAL INTELLIGENCE (AI) & CONVERGENCE

AI & CONVERGENCE OVERVIEW

What is AI?

Artificial Intelligence (AI) refers to the use of technology to simulate human cognitive functions, enabling computers and machines to perform tasks such as problem-solving, decision-making, understanding and producing natural language, recognizing patterns, and adapting to changing environments.

Human-machine interactions can be direct, where humans engage with AI interfaces, or indirect, where AI systems work behind the scenes to enhance productivity or decision-making.

AI can take advantage of and create synergies with other new technologies. For example, blockchain can record data, which may someday be utilized by AI to draw patterns and help make informed decisions based on validated data. AI is also used for monitoring transactions in both decentralized finance and high frequency trading in traditional financial products. Cryptocurrencies can be used to pay for AI processing power. Internet-of-things tools and sensors can provide vast amounts of data that are necessary for AI training and processing. Cloud technology, with its vast processing power, is used by many AI models and applications.

This working group will discuss the major facets of the AI landscape today, reviewing the main considerations for companies and organizations seeking to deploy AI innovations to take into account, discussing a select number of use cases for AI today, and the policy implications of such uses.

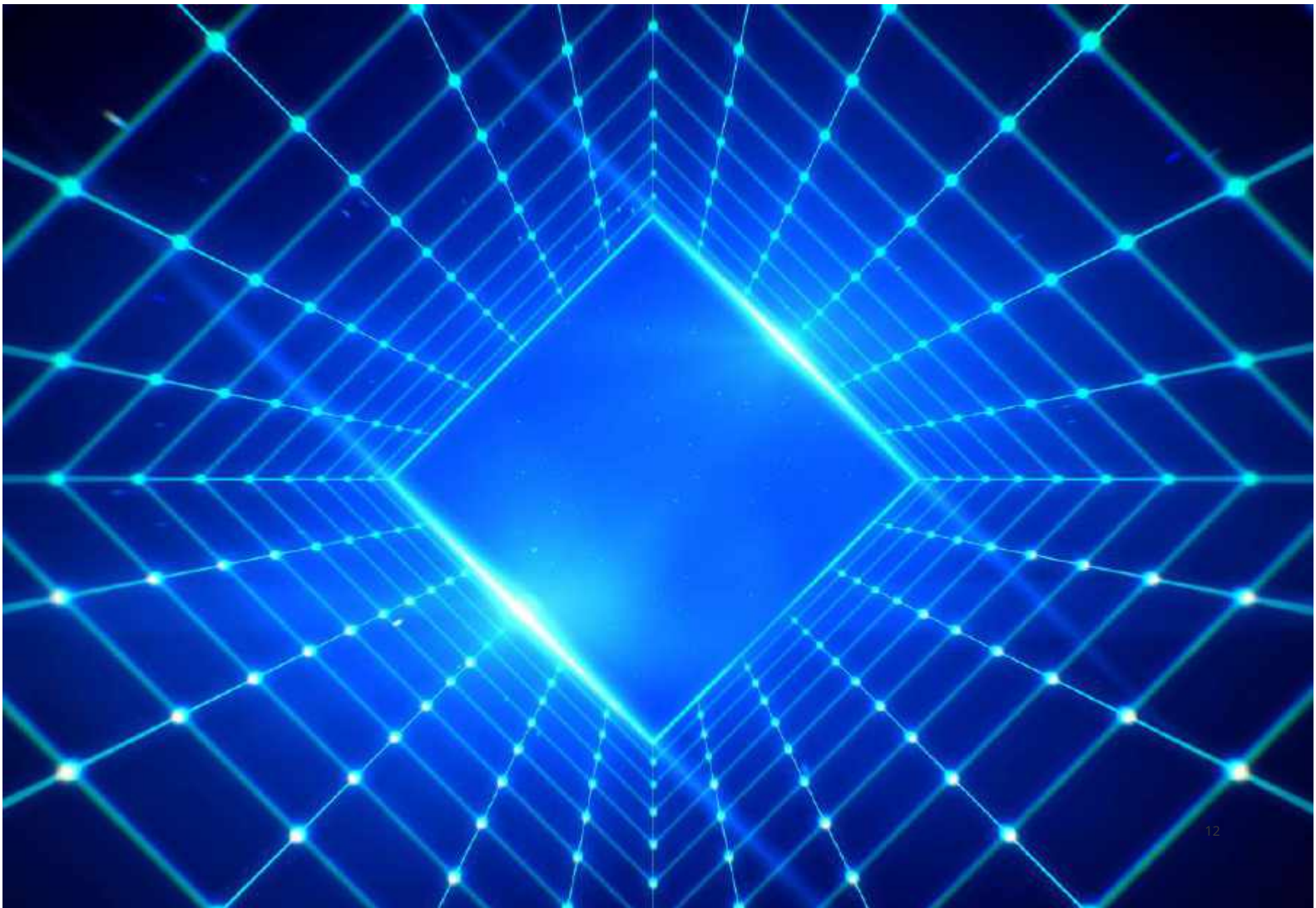
Opportunities for AI

With the rapid expansion of AI across industries, AI has become a disruptive force that is reshaping how businesses operate and how individuals interact with machines. This new field is full of possibilities, such as:

- **Automation -** AI can automate repetitive tasks, improving efficiency and reducing human error.
- **Data Analysis -** AI can analyze vast datasets quickly, enabling data-driven decision-making in various domains.

- **Personalization -** AI can tailor user experiences, such as content recommendations or product suggestions, based on individual preferences and behaviors.
- **Innovation -** AI can drive innovation by enabling the development of new products, services, and solutions that were previously unattainable, through automation of testing or generation of new formulae.
- **Improved Decision-Making -** AI can provide insights and predictions to assist human decision-makers in various fields, from healthcare diagnostics to financial forecasting.
- **Enhanced Safety -** In industries like transportation, AI-powered systems can enhance safety through features like autonomous driving and predictive maintenance.
- **Content Creation -** AI algorithms can be utilized to create content in literature, art, and a range of human activities. For instance, Creative Commons uses generative AI for content creation, in ways that support its mission to support open access to education and creative works, which can be shared and built upon legally based on its licensing.[1]

AI is ultimately an enabler of technological solutions in human-centered and social contexts. It enables a wide array of human-machine interactions with multiple possibilities, roles, and functions. AI can help address the most complex problems facing humanity, with adequately defined parameters, dimensions, and values to include in the algorithms on which it runs.



Risks of AI

It is important to remember that AI systems do not actually "reason." in the same way that human beings do, which requires emotional associations and logical cognition. AI models merely "think" in the sense that they perform processes that require decision making based on datasets and information, and thus they mimic a narrow part of human thought processes. For instance, both AI software and human "thinking" can come up with a word that rhymes with another word based on an existing dataset of vocabulary from which to choose similar sounding words.

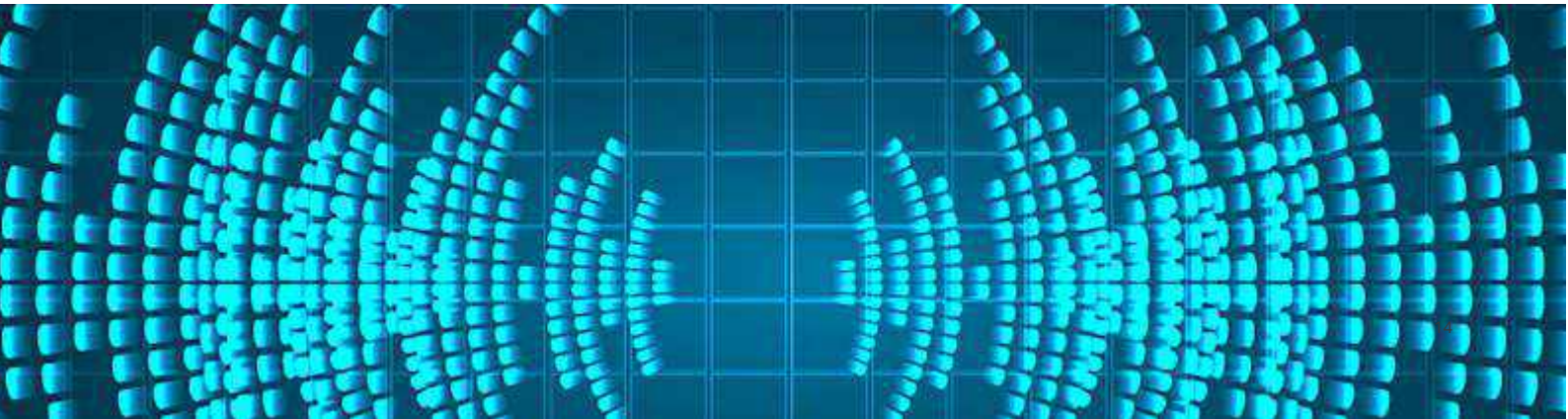
> On the other hand, AI does not have and cannot mimic human reasoning, as logical cognition and emotion are inherently human qualities. When asked why blue is a beautiful color, while humans may answer with an emotional association of the color to a bright blue sky, or a feeling or mood, an AI model would answer based on its past dataset.

It is also humans that program the information and datasets that go into AI systems, which can contain emotionally-driven biases or other unwanted implications, which are then perpetuated as AI uses predictive models to "think" of which information from the given dataset is relevant to determine a given action. AI models are predictive, taking in vast amounts of data to recognize patterns and predict the next sequence in the pattern, which data elements are anomalies, or what should be the result from a series of prompts. An AI model makes predictions based on the data that is used to train it, and eventually it learns from its interactions with human users. Therefore, its predictions will not have any inherent moral code or guidelines unless those are built into the system.

Moreover, AI models may experience hallucinations, where responses generated based on data inputs produce false or misleading information presented as facts. AI models, such as language models or image generators, may make predictions or produce outputs that incorrectly extrapolate on their training data, or are not fully grounded on their data inputs on which they rely.

AI therefore can have unintended consequences when unchecked. The complexity and lack of human oversight of AI systems can perpetuate unwanted behaviors and influence decisions with negative consequences for individuals, businesses, and human civilization. AI presents a series of risks such as:

- **Lack of Transparency -** AI systems and models can be complex and therefore hard to interpret, which makes decision-making processes and their underlying logic opaque.
- **Concentration of Power, Inequality, and Bias -** When AI relies on biased training data or algorithms, it can amplify and perpetuate societal biases. AI developments can disproportionately benefit wealthy individuals and corporations, aggravating the wealth gap and opportunities for social mobility. Concentration of processing power and data can not only increase social and economic inequalities when AI developments are dominated by a small number of large entities (e.g., corporations and governments), but also can have geopolitical effects. Concentration of models could have a wide range of unintended results, such as herding, and will also create single points of failure. In addition, concentration of market power could lead to monopolistic practices.
- **Lack of Privacy -** AI often collects and analyzes significant amounts of personal data, which needs to remain private and secure.
- **Ethical Issues -** Moral and ethical values embedded into AI systems can present significant ethical dilemmas, particularly in the context of decision-making processes with major consequences for people's lives.
- **Lack of Security -** Increasingly sophisticated AI models also raise security risks, including potential misuse. Hackers and bad actors can make use of AI for cyberattacks, bypassing security measures, and exploiting system vulnerabilities. Moreover, AI-driven autonomous weapons also can come into the hands of rouge nations and non-state entities, which further raise concerns given the potential loss of control by humans in critical decision making. A resulting AI arms race can promote rapid and unchecked development of AI with harmful consequences.
- **Concentration of Power -** Concentration of processing power and data can not only increase social and economic inequalities when AI developments are dominated by a small number of large entities (e.g., corporations and governments), but also can have geopolitical effects.
- **AI Dependence and loss of human connection -** If society becomes over reliant on AI systems, it can lead to a loss of creative initiatives, critical thinking, and human intuition, which are not only key to preserving human cognitive abilities but also for addressing the most pressing issues and human flourishing. Moreover, dependence on AI-driven communications and interactions could hinder levels of empathy, social skills, and human connection.



- **Job Displacement -** Automation driven by AI across industries can weaken the power of human workers and lead to job losses, especially affecting low-skilled workers.
- **Legal and regulatory challenges -** New legal frameworks and regulations are fundamental to address the novel issues posed by AI developments, such as liability and intellectual property rights, while protecting the rights of all citizens.
- **Manipulation and Misinformation -** The spread of AI-generated false content, such as deepfakes, can manipulate public opinion. Disinformation can threaten democracy and promote authoritarian political leadership (e.g., facist currents, ultranationalist ideologies, oppressive centralized autocracies, etc.) by influencing public discourse, spreading fake news, and undermining social trust. Extremist groups, criminals, and rogue states can manipulate groups of people for economic and political interests.
- **Existential Threats -** An artificial general intelligence (AGI) that surpasses human intelligence on various functions can present long-term concerns including a threat to our very existence, especially because AI may not be aligned with human interests, priorities, and values.
- **Super-Dominant AI Platforms -** A significant potential danger from large-scale AI systems is the creation of super-dominant AI platforms such as OpenAI, especially widespread platforms with the level of reach of Google, Microsoft, etc., that will have a vast technological advantage due to heavy investments into data and hardware. This can perpetuate a tech oligarchy at the expense of human well-being.

In the worst-case scenario, the risks of unchecked AI can threaten to worsen wealth inequalities, weaken human agency, and even threaten human existence.

Blockchain Convergence and Opportunities

Blockchain technology can add a layer of trust for AI developments, which could draw patterns and guide informed decisions based on validated, immutable, and open data records.

- **Visibility on Algorithms -** The features of blockchain technology add a layer of transparency into AI developments, which can be fundamental to ensure safe and reliable outcomes, and ultimately safeguard trust. When people can comprehend the reasoning and processes with which an AI system arrives at conclusions and outcomes, greater trust and adoption can follow.

- **Transparency on Data Provenance -** Blockchain technology can provide transparency into the source of data sets, helping identify risks of biased, or narrowly focused data sources. A blockchain can document and validate relevant input data from an adequately identified and anonymized source, such as clinically and medically relevant patient data that an AI tool can rely on to identify cancer cells.

  Blockchain's promise in validating data provenance can address the inherent biases that can be present in AI filtering models. This can alert the need to make use of diverse training data sets and unbiased algorithms to ensure fairness in outcomes. Transparency, particularly with respect to data provenance, can also help identify false content in order, to preserve the integrity of information in our digital age.

- **Transparency on AI Outcomes -** Blockchain technology can also provide transparency into the uses and outcomes of AI, such that accurate records of AI-driven decisions and uses recorded on an open ledger can be preserved for monitoring and evaluation of results. For instance, both the use of an AI tool to show "yes/no" regarding whether medical imaging shows the presence of cancer, as well as the following decision to take measures accordingly, can be recorded accurately on a blockchain. The analysis based on the results can also be documented immutably and preserved.

  Therefore, blockchain technology can provide a transparent lifecycle of data sources, uses, and results. It can validate the provenance data going into AI tools, as well as the provenance of the output of AI tools, and track the success of outcomes based on AI-driven decisions. With better controls in place enabled by transparency regarding input data and outputs, it can be more feasible and realistic to determine the effectiveness of AI tools and reduce the risk of relying ineffective or under-performing tool.

- **Data Privacy and Security -** In addition to transparency, blockchain technology at the intersection of AI can also improve privacy protection mechanisms, which can safeguard the privacy of individuals while ensuring security and dependability of data. A range of privacy protecting techniques including data encryption, and fully-anonymized data sets, can greatly improve trust for functions such as authorization management, access control, data protection, network security, and scalability.[2]

- **Decentralization to address power concentrations -** Decentralization can prevent concentration of power and single points of failure, adding resilience and trust. Decentralized and collaborative developments toward AI are fundamental to avoid concentrations of power in AI that can further existing inequalities. On the other hand, decentralized AI developments can contribute toward inclusive relationships and economies.

- **New processes to preserve equality -** AI in convergence with blockchain technologies can also reinvent processes, such that automation doesn't lead to job losses where the same functions are replaced by machines. On the other hand, in decentralized economic interactions with new peer-to-peer possibilities and governance, more jobs can be created than those eliminated, while preserving inclusion and equality.

A BRIEF TAXONOMY

The field of AI is vast and encompasses various subfields, techniques, and applications. In that sense, a taxonomy is essential to provide a structured framework for organizing and categorizing these diverse elements. It helps researchers, educators, and policymakers to establish a common language and terminology for discussing AI concepts, methods, and technologies. This standardization enhances communication and understanding among individuals and organizations involved in AI research and development. This working group has also begun preparation of an AI taxonomy.[3]

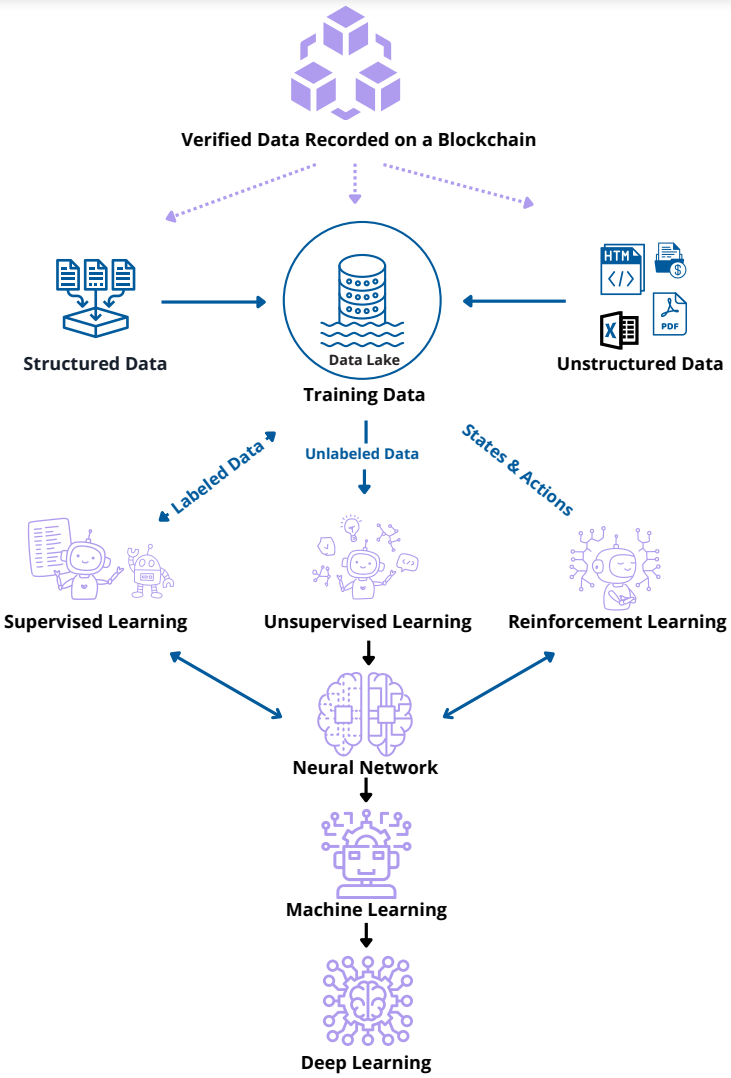
Figure 1: Generative and Predictive AI are two alternative functions

Much of AI perception today focuses on Generative AI, that is, models that are trained to generate new original content based on natural language input. Some Generative AI is in the form of chatbots, which generate responses to user input in a way that mimics predictive text, but in a much more powerful way. Other types of Generative AI allow users to describe a desired output in normal everyday language, and the model can respond by creating appropriate text, images, sounds, videos, or even code output. Yet there is much more to AI than just generative models.

What this paper refers to as "predictive AI" is a method of data analysis which recognizes patterns and analyzes those patterns to make predictions about future outcomes using historical data combined with statistical modeling, data mining techniques and machine learning. This allows for prediction of trends and risks, identification of anomalies, and categorizing of data.

Different use cases for AI call for different models, where those models may be generative, predictive or a combination of both.

Figure 2: How AI functionalities come together



AI functionalities demonstrated above can be seamlessly integrated with blockchain technology, which can serve as the immutable trusted record on which AI models source their data. Sourcing inputs from decentralized ledgers can also address the risks of power concentrations to better safeguard fairness, equality, and human freedom. Data originating from records on a blockchain can add a layer of auditability and validation for accuracy, and ultimately greater trust in the AI models.

USE CASES

When assessing new AI tools generally, companies and organizations must assess their own understanding of the technology and how it can be used to further business goals in compliance with law and with the organization's goals. Each new use will require an evaluation of the AI model in the context of the organization's overall operations and proposed use. This paper provides an overview of certain use cases and matters that should be considered when adopting AI tools for these uses as examples of how organizations should consider implementing such tools. However, there are certain considerations that will be applicable to almost all AI uses. General considerations for AI implementations include the following:

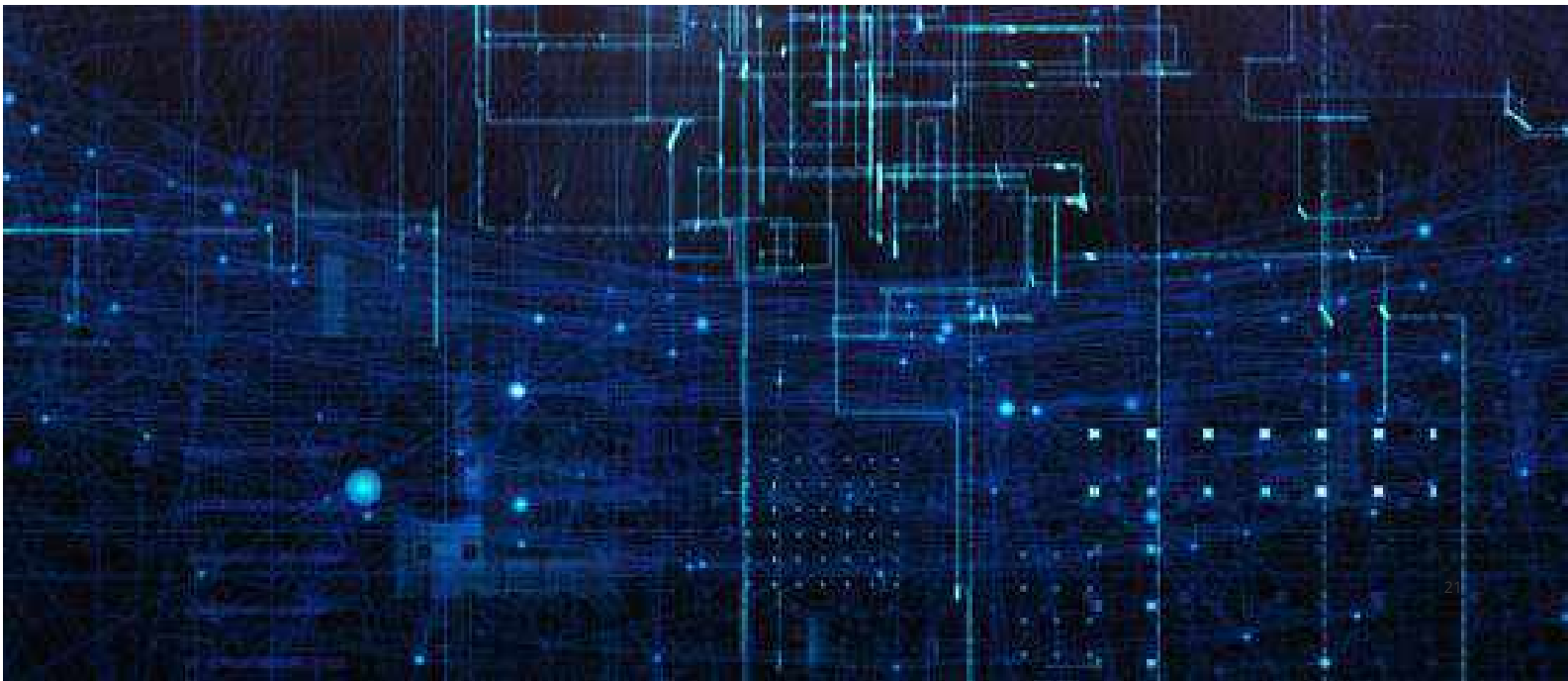
- **Regulatory Compliance -** Each organization implementing an AI tool should assess its regulatory posture with respect to how that tool will be used. The use cases listed below are sector-specific examples of how organizations operating in different industries might consider the use of a new AI tool. However, generally applicable regulations and policies such as anti-discrimination, sanctions, and data privacy will be relevant to all uses.

- **Protection of Intellectual Property -** Generative AI tools can create new intellectual property – but whether this property is protected under applicable laws, and the rights the user of the tool has to newly created property, should be considered. In addition, use of protected intellectual property as inputs or training data creates infringement risks.

- **Safety Considerations -** Depending on the specific applications, safety can be a paramount concern. For AI-powered systems, particularly those in sectors like autonomous vehicles, healthcare, or manufacturing, assessing and ensuring the safety of the technology is critical. This includes rigorous testing, validation, and verification processes to minimize the risk of accidents, injuries, or other adverse outcomes caused by AI failures. Other types of AI tools must also take safety into account – for example, chatbots, especially those targeted to vulnerable audiences, need to be assessed to ensure that they do not produce harmful content. AI tools should be subject to regular testing and audits to detect and mitigate biases, errors, and unintended consequences[4].

- **Data Privacy -** Organizations must assess how an AI tool will use and store data in order to ensure compliance with data protection regulations such as GDPR or HIPAA. In addition to restrictions on sharing and use of personal data, the GDPR grants its subjects the right to not be subject to decision based solely on automated processing which produces legal/significant effect, subject to certain exceptions.

- **Information Security -** Organizations should implement strong cybersecurity measures to protect AI and blockchain systems from attacks (robustness), including encryption, multi-factor authentication, and intrusion detection systems. Ensure that AI tools are secure and free from vulnerabilities that could be exploited by malicious actors.
- **Concentration Risks -** AI tools can also create risks associated with a lack of robustness, alignment and/or controllability of strong AI systems. The upcoming UK AI Safety conference will focus on this. So is the Global Partnership on AI (GPAI) mandated by the G7 to look at AI and in particular generative AI safety solutions (G7 Hiroshima AI Process).
- **Interoperability -** Evaluate how AI and blockchain solutions will integrate with existing systems and technologies within the organization. Compatibility and interoperability can be critical for successful implementation.
- **Data Governance:** Establish robust data governance practices to maintain data integrity, quality, and traceability throughout the AI and blockchain lifecycle.[5]
- **Ethical and Moral Considerations -** Organizations seeking to implement AI tools must consider the moral ambiguity and ethical questions that AI can pose. Although government regulatory frameworks are expected to develop and eventually guide AI implementations with these ethical and moral considerations at the core, these regulatory developments are not likely to be drafted in the time needed to ensure the right safeguards today. Therefore, in absence the of comprehensive regulatory frameworks for AI as of now, organizations should evaluate how launching AI tools can raise ethical and moral uncertainties. They should also adapt to these risks accordingly, or to the extent possible take steps to minimize the risks.



Major AI Implementations Today

The below use cases are illustrative examples of how companies and organizations might consider the implementation of a new AI tool.

FINANCIAL/FINTECH USE CASES

I) Anti-Money Laundering/Know Your Customer (AML/KYC)

The methods currently employed by financial institutions to achieve compliance with Anti-Money Laundering ("AML") and Know-Your-Customer ("KYC") requirements tend to involve human review of transactions and customer identification materials, which injects inefficiency and human error into this important but costly function. Predictive artificial intelligence can materially improve these manual processes by allowing for a rapid and efficient review of large data sets via automated processes that mitigate the inaccuracy of manual human review to achieve more accurate results at a fraction of the cost. The large sets of data reviewed by an artificial intelligence can then be stored centrally via blockchain technology, allowing for ease of access to the results of such review as well as the data underlying those results. Combined with advances in digital identity, use of artificial intelligence for AML and KYC applications promise new levels of efficiency and accuracy.

However, financial institutions employing artificial intelligence to automate review of transactions and customer identification should ensure that some level of human review remains in place with respect to both the results produced by such review and the explainability of the decisions made by any artificial intelligence involved in these processes. Financial institutions should also consider how the models they employ are being trained and deployed, and how any data inputs to the model, or outputs from the model, are shared outside of an organization to ensure compliance with data privacy and confidentiality obligations with respect to customer and transaction data processed by the model.

I.I) AML AND KYC REQUIREMENTS FOR FINANCIAL INSTITUTIONS

The **Currency and Foreign Transactions Reporting Act of 1970** (the "Bank Secrecy Act") details the AML requirements imposed on financial institutions. At its core, the Bank Secrecy Act requires that financial institutions maintain records of all cash purchases of negotiable instruments, file reports of all cash transactions in excess of USD$10,000 per day, report any suspicious transactions indicative of money laundering or other criminal activities, and maintain a security program of policies and procedures designed to ensure compliance with Bank Secrecy Act requirements.[6] FDIC-supervised financial institutions are subject to additional reporting requirements in connection with any known or suspected criminal activity in connection with transactions conducted through such institutions.[7]

The **Financial Crimes Enforcement Network** ("FinCEN") promulgated the Customer Due Diligence Requirement for Financial Institutions (the "CDD Rule"), effective as of July 2016,[8] which requires certain financial institutions to identify and verify the identity of their customers, a process that has come to be known as "Know-Your Customer" or "KYC."

At its core, compliance with the CDD Rule's KYC requirements imposes on qualifying institutions the obligation to identify and verify the identity of customers and of customers' beneficial owners, to understand and develop respective risk profiles, and to conduct ongoing monitoring of suspicious transactions and customer identities.[9]

The compliance programs implemented by financial institutions today largely comprise a high degree of manual individual review of large sets of customer information and volumes of transactions on a daily basis. The manual nature of these processes, and the amount of customer information and transaction data requiring review, has produced an inefficient system whereby substantial time and effort is devoted to providing KYC information to financial institutions, validating the KYC information provided by customers, and subjecting large numbers of transactions to several layers of review and escalation as appropriate.

Unsurprisingly, these compliance efforts result in large costs (both financially and temporally) borne by financial institutions and by customers who may lack the sophistication and resources to effectively understand and meet the information requests they receive. The process further opens the door to inaccuracies resulting from human error and the large volume of data available; false positives and false negatives are bound to occur, especially in light of the growing sophistication of money laundering techniques and the proliferation of blockchain-based transactions in cryptocurrencies.

I.II) HOW CAN AI HELP?

Given the core issues with AML and KYC compliance today, it should come as no surprise that **AI can make a substantive impact on the speed, efficiency and accuracy of AML and KYC reviews.** Machine learning models can be trained to allow for rapid review of large data sets, and to screen customer and transaction data against a broader and more comprehensive list of data points (e.g. sanctions list, media, internal data points, watchlists etc.) improving accuracy and reducing human bias in review (though consideration should be given to bias in machine learning models as well, as discussed below) of transactions.

Furthermore, **AI can assist in expediting customer onboarding** by extracting and validating structured data in an automated and efficient manner, and reliably comparing them against trusted data sources for validation, significantly reducing costs associated with one of the most labor-intensive aspects of KYC. Furthermore, the ability to store and access KYC using blockchain technology can provide an ever-growing secure and robust source of data that can be used across institutions to reduce redundancy in process and lower costs for financial institutions.

I.III) CONSIDERATIONS FOR FINANCIAL INSTITUTIONS SEEKING TO UTILIZE AI IN AML AND KYC COMPLIANCE FUNCTIONS

While AI can substantially improve the efficiency and efficacy of AML and KYC compliance processes, financial institutions seeking to automate such processes through the use of AI should implement robust policies and procedures designed to ensure careful consideration and monitoring of the incorporation of AI into such processes. Such programs should require a balanced approach by an institution that includes careful human review of both inputs to and outputs from an AI model at critical points in the AML and KYC compliance processes and routine reviews of random samples of data reviewed by an AI model to validate any recommendations made by the model with respect to such data. Firms should additionally require that any AI technology it uses allow for sufficient explainability as to its conclusions so that firms have sufficient recourse for instances of claimed false positives.

Financial institutions seeking to employ AI models in AML and KYC compliance processes should also carefully monitor all information fed into the model, whether for model training or for model decision-making purposes. To the extent any outputs from an AI model might be made available outside of the firm, information fed into the model should exclude any confidential information of the firm and of its customers to ensure compliance with both confidentiality obligations and applicable data privacy requirements imposed on financial institutions.

II) AI KM – Financial Services Consumer Banking Fraud Detection and Prevention

Wherever financial services providers enable consumer transactions, the risk of fraud is a central issue that must be addressed and mitigated. The rise of technology-enabled digital payments has created an arms race between increasingly prevalent fraudsters, and financial services providers utilizing sophisticated tools to detect and deter fraud. Artificial intelligence has accelerated this trend: **predictive AI** has empowered financial services providers to better detect fraud in real time, allowing them to decline potentially fraudulent transactions before they are processed, while **generative AI** is now enabling fraudsters to more efficiently and more effectively fight through these defenses. In this section we will explore the use of AI in consumer transaction fraud detection and protection, outlining the current technological landscape and how this may evolve going forward.

II.I) HISTORY OF FRAUD DETECTION TECHNOLOGY

The increasing prevalence of digital payments in today's economy has invited an uptick in consumer banking fraud. According to the Federal Trade Commission, in 2022 consumers reported losing approximately **$8.8 billion** to fraud—up more than **30%** from 2021. (link). Fraudsters who once needed physical access to credit or debit cards to perpetrate fraud can now target a wide variety of security vulnerabilities across a breadth of digital payment and e-commerce platforms. Historically, financial services providers have taken rigid, rules-based approaches to detecting and preventing payments fraud. For instance, attempted payments would be flagged as potentially fraudulent based on geographic location, payment amount, payment time, or other pre-determined limits. Such legacy systems had critical inherent shortcomings: they failed to adapt to changing spending habits of consumers over time without costly and time-consuming manual updates, and they could be learned (and avoided) by practiced fraudsters. These shortcomings led to high rates of false negatives, as a high volume of fraudulent transactions slipped through the cracks.

The early adoption of AI-enabled fraud detection tools helped financial service providers level-up in their efforts to deter fraud. In many ways, the questions involved and the data sets available to such financial services providers are ideally suited to the application of predictive AI, making use of pattern recognition across large data sets. Whether any given transaction is fraudulent can be predicted with relative confidence based on how well it fits into past patterns of payments known to be legitimate. Banks already had large volumes of prior transactions data—including pre-labelled fraudulent transactions data derived from legacy manual and rules-based fraud detection efforts—on which they could train AI models. Furthermore, financial services providers could effectively lean on their customers to provide additional reinforcement learning for predictive AI models in the form of real-time email and text message-based suspect transaction validation. Thus, once the underlying technology sufficiently matured, it was comparatively (relative to other applications in other industries) easy for financial services providers to deploy in the name of fraud detection.

II.II) ISSUES ARISING IN ADOPTION

That is not to say early adoption of predictive AI in the fraud detection space was without issue. Heightened monitoring of large data sets by generalized predictive AI models has shifted the most common source of fraud detection error from false negatives to false positives). This problem was likely compounded by the low risk tolerances of many financial services providers, who, when determining their desired sensitivity of fraud detection AI models preferred to err on the conservative side of enhanced caution. Said differently, financial services providers may have realized the asymmetric cost-benefit balance of false positives, and calibrated their fraud detection models accordingly: in the era of near instantaneous text messages compounded with the low risk tolerance of many financial services providers transaction validation, the cost to consumers of false positives (measured in seconds of inconvenience) is small compared to the cost to financial services providers (measured in dollars lost processing fraudulent transactions) of false negatives. Additionally, more heavily data-driven approaches to fraud detection have raised questions related to cybersecurity and privacy, as some critics question how much data is worth sharing in the name of deterring fraud. Questions of potential bias, transparency, and fairness linked to the black box nature of underlying AI models likewise abound. Clearly there remains much room for improvement in the way financial services providers design, train, deploy, and calibrate AI based fraud detection tools in the consumer financial services space.

II.III) LOOKING TO THE FUTURE

Looking forward, we foresee two main avenues for improvement of the use of AI in consumer financial services fraud detection. The first represents a change in degree from existing applications, and is likely to occur in the near term. As financial services providers gain access to more consumer data and more processing power, they will be better able to tailor fraud detecting AI models to narrower subsets of consumers—or perhaps even individual consumers—yielding more accurate analyses of each transaction in the context of the corpus of those consumer's transactions history. Incorporating an individual's cell phone location data into predictive AI models, for example, could drastically improve such models' ability to predict the validity of a transaction. Today, some companies (e.g., Sardine) are even going far beyond this and checking against how a phone is being held, and other data that can greatly impact fraud detection.

However, financial institutions will need to keep in mind the privacy implications of using such data and whether additional disclosures need to be made or whether new consents will be required. In addition, firms will need to consider whether use of new information leads to biased or unreliable results, by for example penalizing customers whose travel schedules suddenly change.

The second expected change represents a change in kind from existing AI applications, and is likely to take longer to develop. Financial services providers may look beyond supervised learning AI models based on pre-labeled data and towards unsupervised models, and use of unstructured data, to expand the scope of fraud detection capabilities and reduce the need for human input. Generative AI could enable financial services providers to analyze unstructured data and interact more meaningfully with clients—improving efficacy along the way.

III) AI Standards – Credit Decisions

Traditionally, lenders had only limited data to determine the creditworthiness of an individual, such as debt, income, and loan payment history. AI and "big data" have exponentially expanded the factors available to inform credit decisions, allowing lenders to issue loans to "credit invisibles," or those without extensive debt, income, or loan payment history. However, this new data also risks exposing lenders (and companies providing such data) to increased regulatory oversight. This section highlights the legal considerations when using "big data" in credit decisions, and provides a few suggestions to ensure companies do not inadvertently expose themselves to greater legal risk.

III.I) WHAT TYPES OF DATA ARE USED IN CREDIT DECISIONS?

In the realm of credit decision-making, there is an ongoing and notable shift from traditional methods to a technologically-driven, data-rich approach. This transformation is facilitated by the integration of AI and the increasing availability of alternative data sources. The traditional or "classic" data that is utilized when determining an individual's creditworthiness includes factors such as their FICO score, debt levels, income, and credit history (including credit card usage, auto and personal loans, and mortgages, among others). These inputs have long been the cornerstone of credit assessments, providing a snapshot of an individual's financial stability and reliability.

However, the advent of AI and the vast amount of data generated in our increasingly digital world have opened the doors to an array of new data sources for credit assessment. This expanded dataset includes education information, address stability, rent and utility payment history, online shopping activity, browsing history, and even inferences drawn from this data, such as detecting signs of marriage infidelity.

Social media activity, phone apps downloaded, standardized test scores (like SAT), GPA, field of study, job history, geolocation data, payday loan usage, bank account balances, student loan debt, and even smartphone usage patterns, such as the time of day calls are made, the length of phone calls, texting frequency, text length, phone make and model, phone contact organization, Wi-Fi networks used, mobile wallet balances, and phone battery level trends are all now on the radar of AI-assisted credit assessment. In some cases, even one's friends and contacts, along with their credit and personal information, can be considered. Type of computer used and email domain are additional data points that can be of influence.

While this extensive array of data offers the potential for more accurate credit assessments, it raises substantial privacy concerns. For example, recent polls indicate that **96%** of respondents are opposed to the use of social media data for credit risk assessment.[10] The broad spectrum of data inputs noted above is certain to raise eyebrows from a privacy standpoint, as it essentially opens up individuals' personal lives to be evaluated in creditworthiness assessments. The ethical implications of this vast data collection and its use in determining an individual's creditworthiness are profound, and they underscore the necessity of robust data protection and privacy regulations.

There are also significant legal considerations under the **Fair Credit Reporting Act** (FCRA). The FCRA governs credit reporting agencies, which play a vital role in credit decisions. As data aggregators provide increasingly detailed "profiles" to employers, creditors, and similar entities for the purpose of informing credit decisions, there is a growing risk that these aggregators could be categorized as "credit reporting agencies."[11] In such a scenario, they would be subject to the full scope of the FCRA, including its stringent requirements for data accuracy, consumer rights, and dispute resolution. This legal dimension raises questions about the regulatory framework and potential consequences for the industry.

III.II) ECOA: DISCLOSURE & DISCRIMINATION

Under the **Equal Credit Opportunity Act** (15 U.S.C. §1691) ("ECOA"), creditors are mandated to furnish a written statement to applicants outlining the specific reasons for taking adverse actions, such as refusing a loan application. These reasons must not only be relevant but also accurately represent the factors that the creditor genuinely considered or assessed in their decision-making process. It is crucial to note that no factor deemed a primary basis for the adverse action can be omitted from the disclosure. The Consumer Financial Protection Bureau (CFPB) has emphasized that "creditors cannot justify noncompliance with ECOA based on the mere fact that the technology they use to evaluate credit applications is too complicated, too opaque in its decision-making, or too new."[12] This underscores the importance of transparency and accountability in the use of technology for assessing credit applications, ensuring fair treatment for all applicants under the ECOA.

III.III) ECOA: DISCRIMINATION

The **Equal Credit Opportunity Act** (ECOA) serves as a fundamental safeguard against discrimination in credit transactions. The ECOA explicitly forbids creditors from engaging in discriminatory practices against credit applicants based on several criteria, including race, color, religion, national origin, sex, marital status, age, the receipt of income from a public assistance program, or the exercise of any right under the Consumer Credit Protection Act.

However, with the advent of AI-driven credit models, some of the data points considered in these models can sometimes act as proxies for characteristics such as race, religion, or sex. Consequently, the weight and scoring applied by AI-driven credit models may inadvertently result in proxy discrimination, where "the predictive power of a facially-neutral characteristic is at least partially attributable to its correlation with a suspect classifier," potentially undermining the core principles of ECOA.[13] This issue raises important questions about fairness and bias within the framework of AI-assisted credit assessment.

III.IV) DODD-FRANK: UNFAIR ACTS OR PRACTICES[14]

Under the **Dodd-Frank Wall Street Reform** and **Consumer Protection Act of 2010** (124 Stat. 1376) ("Dodd-Frank"), it is unlawful for any provider of consumer financial products or services to engage in any unfair, deceptive or abusive act or practice ("UDAAPs"). The CFPB is tasked with protecting consumers against such UDAAPs. Any entity that determines creditworthiness when issuing loans would quality as a provider of consumer financial products, subject to CFPB jurisdiction. Under Dodd-Frank, an act is "unfair" when (i) it causes or is likely to cause substantial injury to consumers; (ii) the injury is not reasonably avoidable by consumers; and (iii) the injury is not outweighed by countervailing benefits to consumers or to competition.

A company that uses AI-driven algorithms to make a credit decisions may inadvertently commit an "unfair" act under Dodd-Frank because (i) a denial to credit could cause substantial injury to consumers, (ii) without access to the model, the injury would not be avoidable by the consumer, and (iii) depending on the accuracy of the model, might not be outweighed by countervailing benefits to consumers.

The crux of the issue turns on prong (iii). On the one hand, AI-driven credit decisions may increase access to credit to "credit invisibles", or those without a traditional credit score (i.e., one driven by debt, income, and assets, as noted above). On the other hand, such tools may also exacerbate discriminatory results in credit decisions (e.g., through proxy discrimination, as noted above).

III.V) DODD-FRANK: AVM RULES[15]

Federal agencies recently proposed rules that require banks, when using automated valuation models ("AVMs") in mortgage decisions, to adopt policies/procedures designed to, among other things, (i) ensure a high level of confidence in the estimates produced by AVMs; (ii) promote compliance with applicable nondiscrimination laws; (iii) avoid conflicts of interest, and (iv) protect against the manipulation of data. If credit issuers cannot understand or articulate their model outputs, then banks risk noncompliance with these (proposed) rules.

AUTONOMOUS VEHICLES USE CASES

Autonomous vehicles (AVs) represent a transformative approach to transportation, leveraging advanced sensors, artificial intelligence, and connectivity to operate without human intervention. These vehicles are expected to bring about new transportation use cases influenced by factors such as the type of cargo, ownership models, and operational environments. While the potential of AVs is vast, achieving true autonomy, where no human intervention is required under any circumstances, remains a challenge. The integration of technologies like 5G, edge computing, and vehicle-to-everything (V2X) communication will be pivotal in realizing the full potential of AVs in the future.

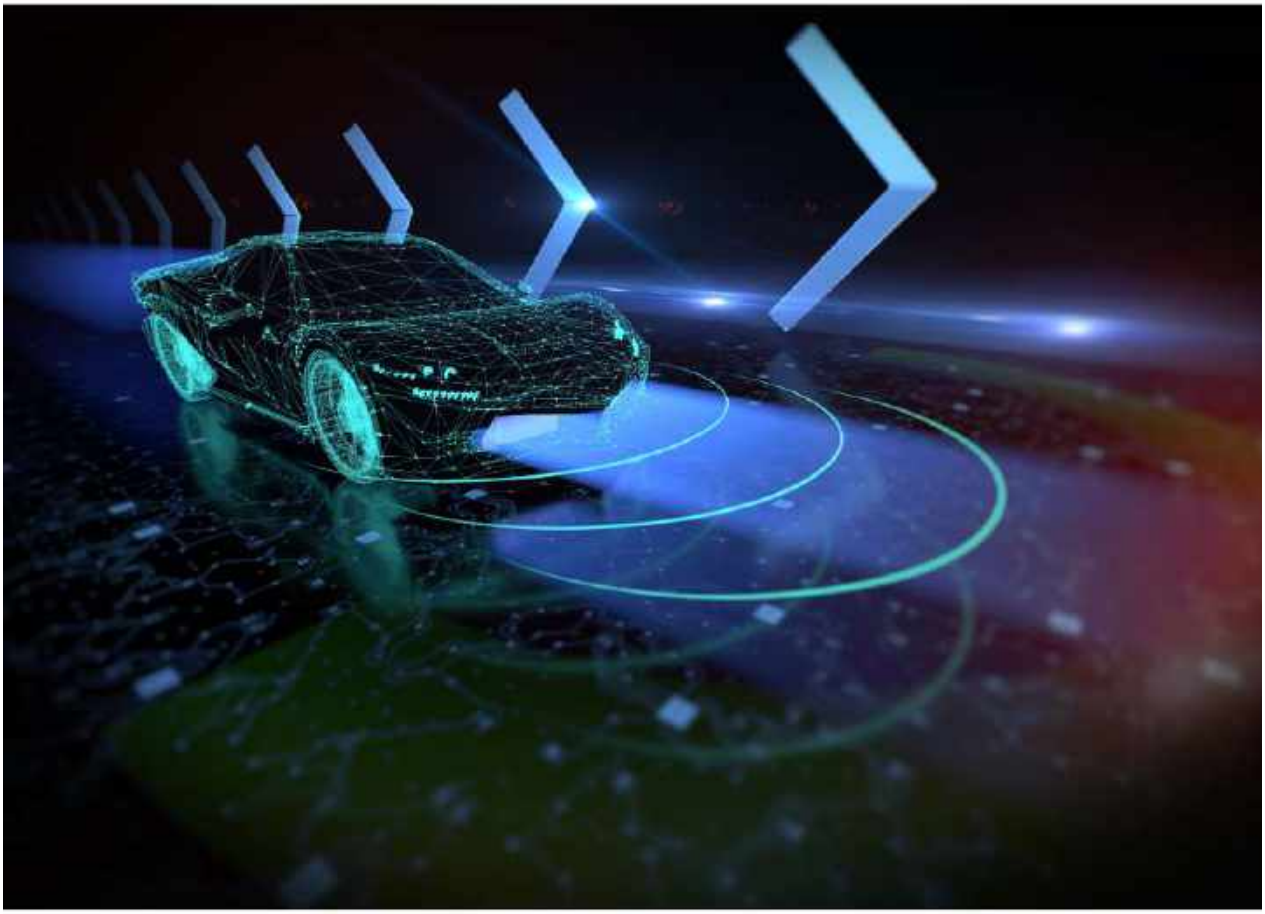
Autonomous vehicles can be much more widely interpreted to include drones (air and sea), as well as any other vehicles equipped with computer vision and AI. Equipping any vehicle with vision and AI-based interpretation will change not only land and air transport but also manufacturing with robots and armed conflicts. A fundamental aspect of AI is to build machines that can simulate humans in their operations in physical spaces – such as factories or office functionalities taking place out of new physical spaces.

AI, particularly predictive AI, has the potential to enhance the benefits of computer vision based on massive data and tailor-made hardware from cameras to sensors and AI chips. Computer vision and AI will let machines and vehicles operate and interact with our real-world physical environment. Many US AI companies are investing significantly in this sector.

Companies and organizations venturing into the realm of autonomous vehicles (AVs) are making significant strides in both technology development and deployment. Here are some notable examples: Microsoft, Alphabet, Baidu, General Motors Company, NVIDIA, Tesla, Ford, Aptiv PLC, Luminar Technologies, Pony.ai, and others.

Companies and organizations looking to implement autonomous vehicle (AV) technologies should consider several critical factors. **The potential of autonomous driving (AD) to transform transportation, consumer behavior, and society is vast**. However, to realize the consumer and commercial benefits of AD, auto OEMs and suppliers may need to develop new sales and business strategies, acquire new technological capabilities, and address concerns about safety. Challenges such as object detection, decision-making, and handling edge cases are paramount. Furthermore, testing and validation in the AV realm will require a paradigm shift. Instead of relying solely on physical testing, companies will need to adopt software-based simulations and virtual testing methods to ensure the safety and reliability of AV systems. As the technology evolves, addressing these concerns will be crucial for the mass adoption and success of AVs in the market[16].

In addition, companies and organizations delving into the realm of autonomous vehicles (AVs) must be attuned to the regulatory landscape, and necessary safeguards required across various jurisdictions. The adoption of AVs hinges on global regulations that favor both testing and development, ensuring the safety of all road users. Regulatory bodies, such as the United Nations Economic Commission for Europe (UNECE), alongside several countries, are striving to refine a global regulatory framework that addresses the multifaceted challenges posed by AVs. The overarching goal is to strike a balance between innovation and safety, ensuring that as AVs become more prevalent, they do so in a manner that instills trust and confidence in the public.



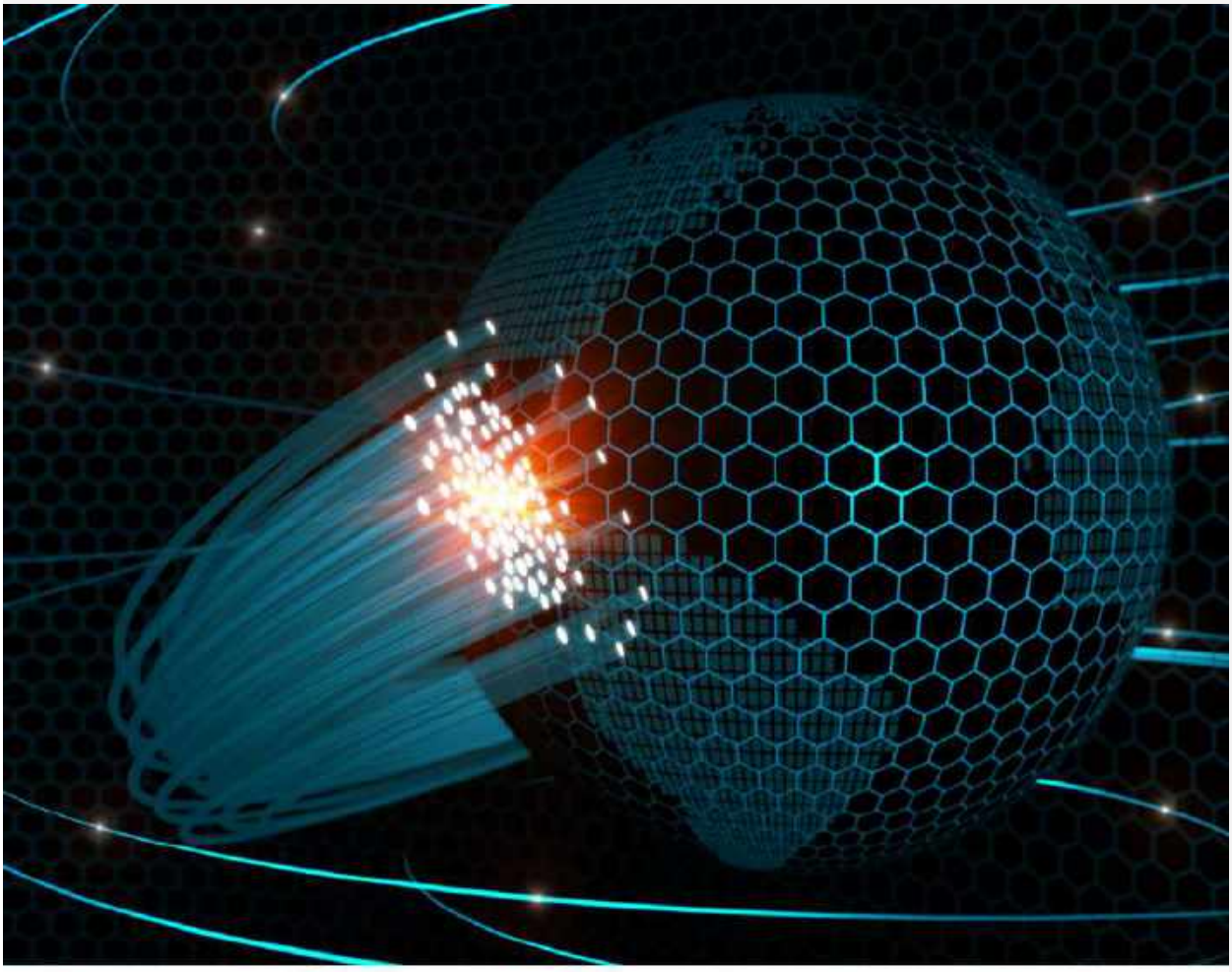
McKinsey's report *"Global Autonomous Vehicles Regulatory Growth Opportunities"* offers insights into testing and deployment regulations for autonomous vehicles in **27** countries, covering regions like Europe, Asia-Pacific, and North America, including China. In addition, the US and EU have held consultations on the matter.

Among these countries, Germany, China, and Japan are among the early actors at the forefront of crafting a regulatory framework conducive to the evolution and deployment of AVs. Germany, a hub for several automotive powerhouses, has a national strategy[17] in place, which intends to set international standards automated and connected driving systems to perform their functions safely and reliably, across national boundaries, while ensuring clear regulation for rights to individual mobility data. The country is diligently working to expand these frameworks for broader applicability. China, another early player in AV testing, has not only implemented comprehensive road safety laws covering driverless vehicles but also facilitated local governments to introduce their bespoke regulations. At the national level, Chinese authorities have rolled out Regulations on the Administration of Road Testing of Autonomous Vehicles[18], a pivotal step to foster transportation innovation and ensure the safe integration of AVs on roads. Japan also adopted provisions for automated driving[19] in April of 2023, to ensure safe and early deployment of automated driving systems in accordance with the existing safety frameworks.

GOVERNMENT & POLICY USE CASES

The government's place is not in the development of AI, but in providing governance to allow public servants to use it to better serve their constituencies. The integration of AI in various sectors, especially government, presents multifaceted challenges and opportunities. Traditional forms of service provision, policy-making, and enforcement are undergoing rapid transformations with the introduction of AI technologies. Governments worldwide are recognizing the potential of AI to revolutionize public-sector ecosystems, but this also brings forth complexities in terms of implementation, transparency, and accountability. The expanding use of AI in governance can significantly alter the dynamics of public service delivery and decision-making processes.[20] In the United States, the state of Ohio has explored using a large language model (LLM), an AI program that can perform tasks such as recognizing and generating text.

AI, especially when deployed in public governance, can inadvertently introduce biases and discriminatory decisions. Policymakers are increasingly focused on the risks associated with AI technologies making discriminatory decisions, similar to human biases. These biases can stem from the data sets on which AI models are trained or from the algorithms themselves. There have been instances, particularly with facial recognition software, where misidentification of individuals, especially those in minority groups, has raised concerns. To address these challenges, there's a pressing need for policies that ensure AI systems are transparent, fair, and free from biases. A report from the National Institute of Standards and Technology (NIST) emphasizes the importance of mitigating biases through appropriate representation in AI data sets and rigorous testing and validation of AI systems.[21]



Immediate assessment regarding AI implementation must include current use of AI as well as automation intelligence by the organization, to understand what is already being utilized and the processes that govern them. Once an audit is completed, a governance structure should be put in place with leadership from across the government and organization, with particular attention paid to representatives from the procurement space that will have to acknowledge and plan for a new element to procuring artificial technology. The structure should include core values by which every new artificial intelligence tool must abide, a mandate for the governing body to create a regulatory process for internal use, and a direction to design updated procurement processes allowing for the accurate procurement of AI technology.

Drawing parallels with AI, other technological advancements in the past have also posed challenges that required regulatory and policy interventions. For instance, the internet's advent brought about issues related to data privacy, cybersecurity, and digital rights. Over time, governments and organizations established frameworks and guidelines to address these concerns. Similarly, AI's integration in public governance can benefit from lessons learned from these previous technological shifts. Policymakers can look at successful regulatory models from other tech domains and adapt them to the unique challenges posed by AI. By doing so, they can ensure that AI is harnessed responsibly and ethically, maximizing its benefits while minimizing potential harms.

POLICY IMPLICATIONS OF USE CASES

From a policy perspective, it is important to consider the ways AI raises complex issues, including ethical issues, and ways to address them. Policymakers are beginning to evaluate measures than need to be taken to address the risks and novel issues that AI poses. For instance, the US White House released a pioneering and very comprehensive policy statement with the "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"[22] that attempts to respond to the entirety of treats and corresponding challenges posed by AI. The states of Pennsylvania and Virginia have also produced executive orders on AI. AI policies have also been envisioned in Japan, China, and India.

With respect to security and privacy, applicability of data protection regulations and safe data handling practices are key. To safeguard against security threats, particularly at a geopolitical level, governments and organizations internationally must agree on best practices for AI developments and deployments, with underlying international cooperation toward global norms and regulations.

Policies and other initiatives should also promote economic equality with AI developments – including reskilling programs for sow skilled workers, promoting social safety nets, and fostering inclusive AI developments that can enable more equal opportunities that can combat economic inequalities rather than aggravate them.

Moreover, many of the proposed measures by policymakers to address AI risks can also be relevant for blockchain developments such that, in convergence with AI, can support innovation to benefit human civilization.

Importance of Principles & Standards

In the immediate term, principles, globally agreed upon regarding AI, offer a softer approach that sets the stage for more hard core policies to be enforced in the future. For example the OECD AI Principles were adopted in 2019 by member countries, followed then by an adoption by the G20, giving them a global reach with the 2 AI super powers (US and China) agreeing on them. Principles contain Ethical considerations to ensure that the use of these technologies aligns with societal values and does not result in discrimination, bias, or harm to individuals or groups.

In addition, voluntary standards, can be made obligatory through later regulations. For AI, the standards bodies the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers Standards Association (IEEE) are actively working on developing standards around development and deployment of AI tools, such as IEEE's seminal work on Ethically Aligned Design.

FAT/ML, or Fairness, Accountability, and Transparency in Machine Learning, is an interdisciplinary field of research and practice that focuses on addressing ethical and social concerns related to machine learning and artificial intelligence (AI) systems. FAT/ML encompasses several key principles and areas of focus:

- **Fairness -** This aspect of FAT/ML aims to ensure that machine learning algorithms and AI systems do not discriminate against or unfairly disadvantage certain groups of people. Fairness concerns often involve issues related to bias in data, algorithmic decision-making, and the potential for reinforcing or exacerbating existing societal inequalities.
- **Accountability -** Accountability in FAT/ML refers to the ability to trace and attribute decisions made by AI systems to specific individuals or entities. This involves understanding how decisions were reached, what data was used, and who is responsible for the outcomes. Accountability mechanisms help establish transparency and ethical responsibility.
- **Transparency -** Transparency involves making AI and machine learning models more understandable and interpretable. This is important for both technical experts and non-experts to comprehend how algorithms work, what factors influence their decisions, and how to assess their behavior.
- **Privacy -** FAT/ML also considers the protection of individual privacy in the context of AI and machine learning. It involves implementing measures to safeguard sensitive and personal information, ensuring that data is used responsibly and in compliance with data protection laws and regulations.
- **Robustness -** Ensuring that AI systems are robust to adversarial attacks and unexpected inputs is another aspect of FAT/ML. Robustness measures aim to prevent AI systems from making incorrect or harmful decisions when faced with unusual or malicious inputs.

FAT/ML often intersects with discussions about regulation and policy development for AI and machine learning. Researchers and policymakers work together to establish guidelines and rules that promote fairness, accountability, transparency, and ethical behavior in AI applications.

Government Actions and Public LLMs

Regulatory Clarity

Governments must help provide clear and up-to-date regulations and guidelines for the responsible use of AI and blockchain. This clarity will in turn help organizations make informed decisions and comply with the law. The issue is that AI is a very fast moving field while laws and regulations are slow, adding to that the lack of comprehension by policy makers of the impact of these systems and how they operate. A robust regulatory framework is paramount. This includes clear guidelines on testing protocols, safety standards, data privacy, and interoperability.

Open Source vs. Closed Source

The choice between open-source and closed-source LLMs depends on the specific use case and requirements. Open-source models promote transparency and collaboration but may require more effort to customize and maintain. Powerful Open-source models could also be used for nefarious reasons and that is why many are suggesting a graduation approach to decide what model should be open or close and for what purpose, which user, etc. Closed-source models offer proprietary features and support but are by definition less transparent.

Public LLMs

Governments may consider encouraging or supporting the development and use of public LLMs for various purposes, such as legal research, content generation, and more.

Monitoring and Oversight, Collaboration

Governments are looking at establishing mechanisms for monitoring AI and blockchain implementations, especially in critical sectors like healthcare, finance, and transportation, to ensure compliance with regulations and ethical standards. Governments should also facilitate collaboration between industry stakeholders, academia, and civil society to develop best practices, standards, and frameworks for AI and blockchain governance.

CONCLUSION

AI raises complex issues, especially as a technology enabler in social contexts with increasing levels of nuance. Therefore it is critical to consider the impact of AI on human society and well-being. In order to comprehend the impact of AI and promote its adoption in ways that are beneficial for human civilization, cooperation among stakeholders is key – an effort that will likely be driven by standards and regulation. Now more than ever, cooperation among stakeholders is essential to advance harmonized regulations for coordinated and constructive AI innovations that will benefit humanity. Agreement on standards, conditions, and parameters will shape the future of AI and its impacts.

There is a need to balance technological development while preserving the integrity of human interactions, in order to maintain our well-being and flourishing. AI developers and researchers must engage in robust testing, validation, and monitoring of AI systems to identify and address any issues and unintended consequences before they escalate. The AI community must also promote safety research, ethical guidelines, and transparency, in particular for artificial general intelligence developments, such that they can serve humanity's best interests rather than posing serious threats.

In this context, we believe that blockchain technology has an important role to play in the development of responsible AI. Blockchain can secure, source, and verify data provenance, for a future landscape of AI that is made more trustworthy. Blockchain serves as a risk mitigation tool, with a transparent ledger and audit system that support an unprecedented level of effective and trustworthy record keeping. Blockchain-based identification mechanisms can address many of the privacy concerns that arise from Machine Learning. Digital rights will be a foundational piece of this.

We hope to spur the first major body of work to explore the convergence of blockchain and AI, with continued collaborations and discussions toward responsible innovation.

SECTION VIII

COUNTRY SPOTLIGHT: BRAZIL

OVERVIEW

Brazil is developing into an increasingly mature, developed, and very attractive market for digital assets and blockchain technology, and arguably among the most overlooked. Adoption has been expanding at an increasing rate that is worthy of notice in terms of speed and size (e.g., increasing size of crypto investments, disclosures of holdings and transactions to the tax authority, and projects advancing financial innovation with blockchian and digital assets). This is a market of high volumes in size that is worth considering to bring to the forefront of discussions in the space.

With increasing trade volumes and significant activity for both retail and institutional investors, Brazil has become a critical market for many of the world's largest cryptocurrency exchanges. For example, the country has been one of Binance's largest markets globally since 2020. Other global exchanges such as Coinbase, Bitget, Huobi, OKX, and Crypto.com have also begun servicing Brazilian customers via integrations with the local instant payment system Pix, and have also been engaging in regulatory discussions. This trend i salso consistente with claims from Consensys that Brazil has the second-most Metamask downloads of any country in the world, trailing only the US. Moreover, many blue chip companies over time have been moving their operations to Brazil.

Fintech in Brazil is fertile ground for blockchain & digital assets deployments – with caveat in payments

Financial technologies in Brazil have already attained a significant presence, setting the stage for promising implementations in blockchain and digital assets. Brazil has a history of fostering fintech developments aiming to promote competition, enhance the efficiency of Brazilian financial markets, and ultimately foster financial inclusion by increasing the availability of financial products and sources of financing for the broader population. Brazil's ecosystem of fintechs is also quite diversified, as they operate in several market segments: credit, payments, financial management, loans, investments, private financing, insurance, debt negotiation, etc. These solutions are at the moment making use of technological innovations both within the traditional banking system as well as distributed ledger technology (DLT) and cryptoassets.

Brazilian regulatory bodies in collaboration, including the country's central bank, operating along the lines drawn by the governmental agenda, have assessed the potential impacts of these innovations on existing operations conducted within the Brazilian financial and payment ecosystems.

Some fintech segments fall under the regulatory scope of the Securities and Exchange Commission of Brazil, the Comissão de Valores Mobiliários (CVM),[23] and Superintendency of Private Insurance (Susep).[24] Other segments are included within the regulatory scope of the Banco Central do Brasil's (BCB) [25] – particularly credit and payments.

In order to support ongoing innovation in the financial ecosystem, in May 2018, Central Bank launched the Laboroatory for Innovation in Fiancial Technology (Lift) — a virtual environment that allows the collaboration between regulators, academia, market participants, technology copanies, and startups — aiming toward promoting knowledge sharing and technological innovation. The Lift initiative is jointly run by by the Central Bank and the National Federation of the Central Bank's Civil Servants Associations (Fenasbac). The role of tech companies is to support ideas selected to the take part in the program.

These initiatives have made the vibrant Brazilian fintech ecosystem fertile ground for continued financial innovation. In 2020, the launch of Pix, the Brazilian instant payments system, allowed enterprises to connect through a single rail, and the resulting adoption has been much higher than originally anticipated.

PIX BY THE NUMBERS

107%
in transactions

2.9 billion Pix transactions in December 2022, against 1.4 billion in December 2021, an **increase of 107% in just one year**

67%
in transactions

R$1.2 trillion was the total amount transferred in December 2022 against R$718 billion registered in December 2021, **an increase of 67%**

93% of transfers made by individuals are worth up to **R$200.00**

71.5 million users included with Pix (**35% of the Brazilian population**)

133M
individuals use Pix

133 million individuals and 11.9 million merchants use Pix, as of December 2022, representing **77% of the adult population**, and **67% of merchants** with current relationship on the national financial system

Ultimately, the Central Bank's policies toward advancing Pix, and in support of open finance, have set the stage for a friendly environment with respect to financial innovation in Brazil, so much so that crypto innovations for payments already face a competitive landscape because of the high rates of penetration and the population's satisfaction with Pix. There is a very high penetration of neobanks, with Nubank as an example having experienced very fast adoption. The population has come to trust and openly adopt financial innovations in general, which influences their level of openness to experimenting with blockchain and digital assets developments. In this context, crypto and blockchain innovations emerge as a new stream that can scale as it comes together to converge with existing fintech solutions.

There is increasing energy and interst in digital assets on the coat tails of the Cental Bank's Drex project to launch a CBDC, which is further attracting investors focusing on Brazil due to the attractiveness of the financial ecosystem on which a tokenized Real would operate. It is expected that these innovations, offering solutions beyond a mere alternative to Pix, that can gain significant traction. Ethereum in Brazil ran a Drex focused hackathon, and there is increasing excitement on tokenization efforts expanding on the Drex platform.

RISE OF BLOCKCHAIN & DIGITAL ASSETS IN BRAZIL

Increasing Crypto Trading

A total of **US$3.8 billion**[26] in overall crypto trading volume was reported during July 2023. This number is roughly equivalent to the monthly average of **US$3.9 billion**[27] reported for the prior months of the year. For context, the highest volume ever reported was **US$5.2 billion**[28], which came during the peak of the last crypto bull market in May 2021. Bitcoin and Ether remain the preferred non-stablecoin crypto assets for investors, with average monthly volumes of **US$226 million**[29] and **US$49.7 million**[30], respectively. These numbers are down significantly from the bull market of 2021, when bitcoin averaged **US$1.1 billion**[31] and Ethereum **US$308 million**[32] in monthly volumes. Bitcoin's market share for 2023 has been in the single digits, versus 40-50 percent during the bull market.

According to the *2023 Geography of Cryptocurrency Report* from Chainalysis, Brazil slipped from 7th to 9th place with respect to strength of its crypto market, but it still maintains the top spot out among all Latin American countries. This ranking seems consistent with Brazil's ranking as the ninth-largest economy in the world. For the 12 month period for June 2022 through June 2023, Brazil received approximately **US$80 billion** in cryptocurrency value, with the overwhelming majority of that volume coming in transaction sizes of larger than **US$1 million**. A positive trend identified in the report is that small and large retail transaction volume remained strongly consistent throughout the 12 months studied. Given that this was an extremely volatile and difficult period for the crypto industry, the consistency of these transactions demonstrates a longer term faith in the technology's value proposition. DeFi and peer-to-peer technology usage in Brazil has proven to be significant as well, though adoption was down slightly year-over-year. The report states:

> "The data paints an optimistic picture for the Brazilian crypto market. Even in crypto winter, the so-called "middle class" of high-value crypto traders, along with basic retail users, stuck with the asset class."

Figure 1: Brazil monthly transaction volume by transfer size, Jul 2022 - Jun 2023 (Source: Chainalysis)

In addition, there are currently **19** domestic and international brokerages offering crypto trading services to Brazilians, as tracked by the domestic website Livecoins.[33] These exchanges have been moving an average of **US$7.2 million**[34] per day worth of trades. Several other banks and fintechs offer crypto brokerage services as well, including Nubank, PicPay, Mynt (from BTG Pactual) and, until recently, XP Investimentos and PicPay. Many other traditional finance institutions are expected to apply for VASP licenses once the regulatory and licensing framework is released by the Central Bank.

Other marque name Web3 companies and service providers have been aggressively eyeing the market and establishing a solid presence include Ripple, BitGo, Fireblocks, Metaco, Ramp, and Zero Hash. Outside interest from service providers is expected to increase significantly as more banks and traditional finance institutions increase their digital asset infrastructure. Leading Web3 protocols also have significant community presence in the country, including Polkadot, Near, Algorand, and Cardano.

Retail markets

While inflation is largely under control in Brazil at the moment, the memories of hyperinflationary environments still ring true for many residents - particularly those over the age of 30. For retail investors, there are not many alternative investments available for preserving wealth. Capital markets in Brazil are not very deep, there are very few investors on the B3 stock Exchange relative to the country's entire population. Arguably, may be even easier to buy crypto than a treasury bond in Brazil.

It is also difficult to access dollars and other hard currencies - even though Brazilians on the aggregate would prefer to keep their funds in dollars rather than in the local currency, the Real. Brazilians also tend to view the value of the Real in relation to the US Dollar, such that even if inflation remained flat, the average Brazilian would feel richer or poorer if there were to be a notable increase or decrease of the Real's value against the US Dollar.

With the exeption of payments where there is an existing system with widespread adoption on existing rails, crypto as an investment and trading alternative becomes even more attractive for a retail population does not have easy access to many other investment options, as opposed to the accessibilty of crypto. Outside of crypto, it is also difficult to gain exposure to US Dollars, which are particularly attractive in Latin America due to their credibility and price stability relative to local currencies in the region, which have experienced drastic historical price fluctuations and massive inflation episodes.

Record amounts of users reporting crypto trades are partially driven by a younger Brazilian population where demographic factors of age, socioeconomic factors, and fintech adoption have contributed to openness to crypto. Stablecoins and bitcoin are proving to be an option that many retail investors turn to as a means to protect wealth, or merely to access dollars. There is no definitive estimate of the total number of crypto holders and users in Brazil, but there are a variety of respectable estimates that place fall within the **5 million** and **15 million** range. This amounts to between **3** and **7** percent of Brazil's total population of **214 million**.

According to the most recent data from the Receita Federal, Brazil's tax authority, **4.1 million** citizens reported crypto transactions during the month of July 2023.[35] This figure is the highest since the agency began tracking this information in August 2019 and represents a **173 percent** increase from **1.5 million** in July 2022 and a **1,200 percent** jump from **315,000** in July 2021.

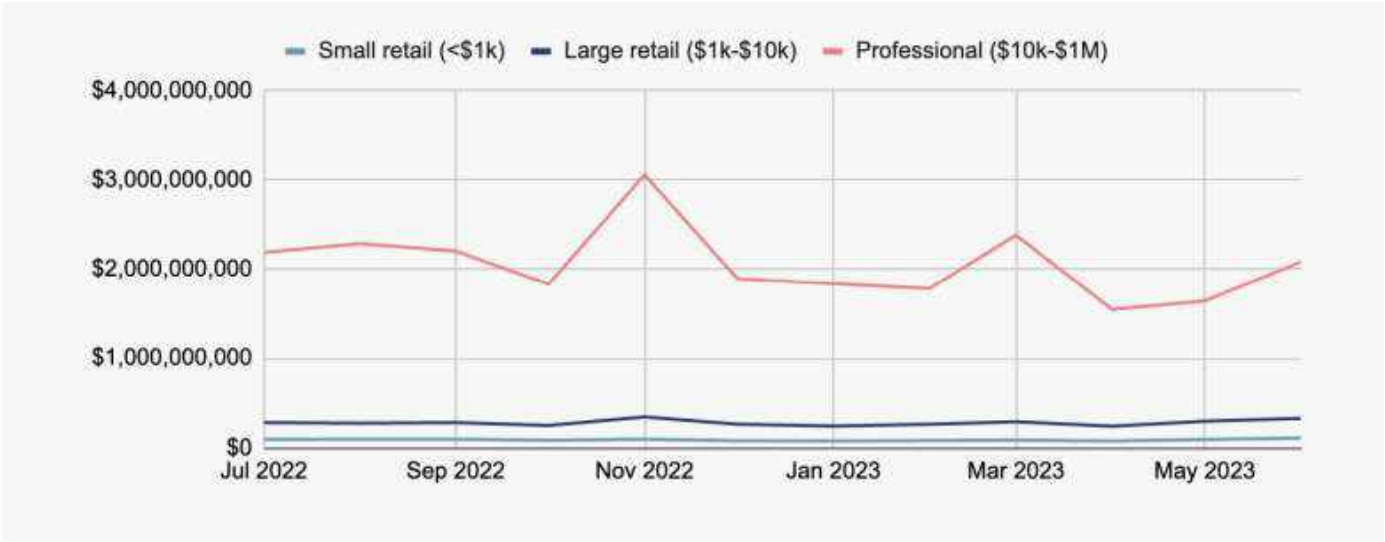
Institutional markets

The Brazilian Securities and Exchange Commission approved regulation No. 175, in which Investment Funds are allowed to invest up to **10%** of their net worth in crypto assets.[36] After a series of postponements due to other factors affecting the funds industry in Brazil, this new Resolution CVM 175 has come partially into force on October 2nd, 2023 to regulate investment funds in the country. Most changes proposed have entered into force, although a few changes are expected to come into force in 2024.

During the month of July 2023, a total of **92,000 businesses**[37] declared crypto assets on their balance sheets to the Receita Federal, another a record number for the regulator. This figure compares to **33,000** in July 2022 and **7,600** in July 2021. While the exact nature of these companies is not disclosed in these statistics, nor is the reason for holding and transacting in cryptocurrency, there are indications that these companies are, at least for the most part, investment firms or asset managers invested in Brazil's many cryptocurrency ETFs or private crypto funds, and thus obliged to report these holdings and transactions to the Receita Federal.

Moreover, insights on Brazil's cryptocurrency market from the most recent *Geography of Cryptocurrency Report* by Chainalysis indicate that the country possesses the characteristics of a more mature, developed North American or European market. This is largely due to the strong institutional and professional investor presence in the market, as measured by on-chain transactions and exchange order book data.

Figure 2: Retail and professional-driven transaction volume in Brazil, July 2022-June 2023 (Source: Chainalysis)



Evolving regulation to support crypto markets

To address the growing crypto market, Brazilian regulatory authorities have also taken steps to provide regulatory clarity and oversight. Overall, growing crypto adoption is leading to reporting requirements for exchanges, equivalent to requirements for local fintechs.

It should be noted that the increasing figures of crypto market activity take into account the transactions that are being reported to Brazil's tax authority Receita Federal. Investors, both retail and institutional, must report their holdings and trades on crypto exchanges, and exchanges also must report customers' trading information to Receita Federal for tax reasons.[38] Reporting of crypto holdings and trades takes place using the regular federal earnings tax form. For monthly transactions that surpass the threshold of **R$35,000**, entities must pay capital gains taxes.

While citizens are obliged to report these transactions, reporting rates may still vary significantly but have been trending upward in recent years as more citizens become familiar with the process and the requirements. Domestically-headquartered brokerages are required to automatically report transactions of their customers to the agency. Overseas exchanges are not obliged to report on behalf of their customers, though customers are still required to report these transactions themselves. In that context, the growing figures for volumes and unique users recorded in Brazil should be interpreted as a result of growing interest in digital assets and increased compliance with reporting requirements.

The Brazilian CVM has also issued regulations related to cryptocurrency products and trading, contributing to a more structured environment for market activities. In 2019, the CVM issued regulations related to cryptocurrencies, particularly Initial Coin Offerings (ICOs). These regulations require companies conducting these activities to register with the CVM and provide specific information to investors. In October 2022, the Brazilian Securities and Exchange Commission published a guidance[39] consolidating its understanding and guidelines about the definition and regulation of crypto assets in Brazil and their relationship with the securities market.

It is imortant to note, however, that crypto has not gained significant popularity thus far as a means of payment or infrastructure for transactions – a trend likely also attributed to the regulatory framework that has been supportive of financial innovation and has paved way to the existing and widespread payments system Pix. Brazilian residents have already adopted and trust Pix as a predominant payments use case.

Crypto ETFs

Crypto ETFs in Brazil have also gained popularity largely among retail investors. Brazil is the second country after Canada to approve a crypto ETF, and the first in Latin America. Currently, there are **13** cryptocurrency-related ETFs available in Brazil. Given that many investors gain access to crypto through ETFs, a resulting assessment is that ETFs actually contribute in growing the crypto market in Brazil.[40]

The landscape of cryptocurrency exchange-traded funds (ETFs) in Brazil has witnessed significant growth since the Brazilian Securities and Exchange Commission approved the first crypto ETF to be listed on the Brazil Stock Exchange (B3), Hashdex Nasdaq Crypto Index ETF (HASH11), on April 4th, 2021. This is the world's first crypto-based ETF, available to accredited non-US investors at the time of its launch. The Brazil Stock Exchange listed its first bitcoin ETF, QR Capital's bitcoin ETF, in June of 2021.

Managed by Hashdex, a pioneer in the field, HASH11 set a precedent for the Brazilian market, marking a new era in crypto investments. This ETF, like others that followed, offered investors a more structured and regulated way to gain exposure to cryptocurrencies, without the complexities and risks associated with direct purchases and storage of digital assets.

As of today, the total market capitalization of crypto ETFs in Brazil stands at **US$438 million**.[41] ASH11 remains a dominant player, contributing over **US$1.4 million**[42] to the daily trading volume of around U**S$1.9 million**.[43] This dominance underscores Hashdex's pivotal role in shaping the Brazilian crypto ETF market. Furthermore, the presence of multiple ETFs from Hashdex and QR Capital in top ETF lists highlights the competitiveness of this landscape, where a few key players are leading the market.

Interestingly, traditional financial institutions are also entering this space, as evidenced by Itau, one of Brazil's top banks, launching its own crypto ETF, BITI11. This move by a mainstream financial player not only legitimizes the crypto market but also broadens the options available to investors.

Additionally, BTG Pactual integrated cryptocurrencies to its investment app for customers, allowing them to buy and hold crypto without additional custody or management fees. Moreover, the regulatory environment in Brazil is notably advanced, allowing for ETFs based on derivatives and crypto spot ETFs to be launched. This regulatory openness has been crucial in fostering a diverse and dynamic ETF market, enabling investors to choose products that align with their risk appetite and investment strategies. The combination of innovative ETF offerings and a supportive regulatory framework positions Brazil as a significant player in the global crypto investment landscape.

Figure 3: Data on Crypto ETFs (Source: B3)

Stablecoins

As the regulatory environment in Brazil has progressed, providing greater clarity for businesses, the development of new products that foster innovation and advance the Brazilian market has been gaining momentum. Post-pandemic, the number of Brazilian investors has grown significantly, adding **8 million investors** - **5%** of the population - from 2021 to 2022, leading to an increased pursuit of new products and opportunities across capital markets. Diversification stands as a cornerstone of investment, and the Brazilian market has made substantial advancements in expanding the array of financial products available to domestic investors.

In this context, stablecoins can play a relevant role when facilitating access to traditional markets' assets through blockchain, as they serve as the vehicle for transacting these assets on a decentralized network.

Surging usage of stablecoins is one of the most significant trends in the Brazilian market for 2023. Stablecoin transactions saw a total volume of **US$3.3 billion**[44] for the month of July 2023, roughly **86 percent** of total crypto volume. This is a notable increase in stablecoin volume, from **US$2 million**[45] registered in July 2022, which comprised **77 percent** of total volume for that month. Brazil has reached among the highest volumes of Tether activity in terms of transactions, as recorded by government statistics.[46] For July 2023, USDT-paired transactions comprised **US$3.2 million**[47] of total stablecoin volume (**82 percent** of total volume), while USDC comprised **US$172 million**[48] in volume.

Interestingly, the average size of a transaction involving USDT was registered at **US$13,500**,[49] whereas the average size for USDC was **US$4,300.**[50] This tracks with the broader trend witnessed over the first half of the year, where the average USDT transaction size has been **US$14,800**[51] and the average USDC transaction was **US$3,100**.[52] These data points suggest that USDT has been the preferred stablecoin for larger institutional traders and commercial enterprises, whereas USDC has become the primary option for retail users and investors looking for exposure to dollars as a store of value.

Of note is also the relatively strong adoption of a Brazilian Real-pegged stablecoin called BRZ, which is issued by Transfero Group. This coin has one of the largest market caps among stablecoins that are not pegged to the US dollar. Prior to November 2022, BRZ was averaging between **US$102 million** and **US$200 million**[53] in monthly trading activity, largely due to its popularity with traders. A significant portion of BRZ's liquidity was on the FTX exchange, however, so when the exchange collapsed a significant portion of BRZ's liquidity also declined.

Leveraging blockchain technology and aiming to enhance its product offerings, BTG Pactual Group, Brazil's largest investment bank, also issued a stablecoin pegged to the U.S. dollar, the BTG DOL. This is the world's first dollar-backed stablecoin from a bank.[54] This constitutes a significant move towards the tokenization of money markets in Latin America. This milestone not only signifies the advancement of institutional initiatives in Brazil but also reflects the rise in crypto adoption in the Brazilian market.

Digital Identity Solutions

Brazil is rolling out a National Identity Card project, a digital identity solution using blockchain technology, drawn by the features of immutability and decentralization to enhance security and reliability. [55]The national data processing service Serpro has launched a private blockchain, the b-Cadastros platform, on which on-chain identification documentation is issued.

Blockchain technology is deemed to be critical for protecting personal data and preventing fraud, providing citizens with a more secure digital experience. Local governments have also stated that blockchain technology can help target organized crime, facilitate collaboration among government sectors, and simplify citizens' access to public services while streamlining administrative records. The ability to securely exchange data among the Federal Revenue and government departments can be a gamechanger according to the announcement of the project.

This solution is launched initially in the **3** states of Rio de Janeiro, Goiás, and Paraná.[56] The Brazilian government announced that over **214 million** Brazilians would adopt blockchain technology for digital identity in the near future, and eventually the rollout is expected to be nationwide. This is consistent with Brazil's efforts over the last few years to unify identity issuance across all its **26** states.

PIER: Blockchain to exchange information among regulators

Initiatives to foster blockchain adoption have taken place in the Brazilian government prior to many other countries, particularly to channel the benefits of this technology to enhance data sharing. One early example is the network built to exchange information among Brazilian regulators in the financial sector. This is especially relevant as blockchain adoption in financial services has been expanding across the country, and that financial innovation is further supported through the Brazilian Securities and Exchange Commission's recent regulatory sandbox launch.

The Platform for Infromation Integration Among Regulated Entities, or Plataforma de Integração de Informação entre Entidades Reguladas (PIER) was created to facilitate information exchange between the Brazilian Securities and Exchange Commission, the Central Bank of Brazil, and the Private Insurance Superintendence (Susep).[57] PIER interacts with various information systems across these three regulatory institutions, comprising a vast integrated database that includes data on sanctioning actions; participants and their administrators, administrators' curricular information, and the controls and corporate participation of regulated entities and their administrators. Authorized users may query information regarding any specified regulated entity, and more than one topic may be searched simultaneously.

The introduction of blockchain technology to facilitate this information exchange has greatly improved the quality of information security on the platform. Through this technology, the platform records data about its use, mitigating undue access to available information and the history of consultations already carried out. Blockchain adoption for PIER also significantly reduces compliance costs for market participants by avoiding unnecessary redundancies in information requests from common regulated entities. This in turn reduces bureaucracy and speeds up the availability of information.

Brazil Blockchain Network

Brazilian government agencies are working together, since early 2022, to create the Brazil Blockchain Network (RBB) to serve as a backbone for the blockchain environment in the country. RBB is a public non-profit that aims to enhance government connectivity, helping to prevent fraud and corruption, while optimizing the provision of digital services to citizens.

This effort is yet another measure to encourage the adoption of blockchain technology in public administration, which is expected to propel future uses in a variety of activities. The aim is to increase security in public administration acts and contracts. Public administration bodies and private institutions of public interest can participate in the RBB initiative in order to create, strengthen, and foster an innovative ecosystem utilizing blockchain technology.

This implementation is part of the ongoing digital transformation strategy implemented across several sectors of the Brazilian government (BNDES national development bank for economic development, Maranhao state, etc. – refer to stakeholders),[58] expected to foster numerous future applications much like the Internet did since the 90's. RBB encourages institutions to leverage their initiatives and enables the adoption of blockchain technology by public institutions and institutions serving the public interest.

Taxation Solutions

RIO DE JANEIRO

According to a decree published on Oct. 11, 2022,[59] the city of Rio de Janeiro announced its intent to allow the use of cryptocurrencies to make Real Estate Tax Payments, through third-party service providers, starting in 2023.[60] This move would position Rio as the first Brazilian city to accept digital assets for tax payments. It is expected that taxpayers would be able to make these payments using several cryptocurrencies, and that their use for tax payments in other matters may be approved in the future. The decree also states that companies wishing to provide cryptocurrency payment services as third-party service providers must be registered with the city and comply with the requirements set forth by the Brazilian Securities and Exchange Commission (SEC).

BCONNECT: INFORMATION SHARING ACROSS COUNTRIES – MERCOSUR TAX BODIES

The Southern Common Market, a South American trade bloc denoted as Mercosur for its Spanish abbreviation, is comprised of 5 sovereign member states (Argentina, Brazil, Paraguay, and Uruguay)[61] that are now connected through the blockchain network bConnect, which was launched for use in October of 2020.[62] Mercosur tax bodies have adopted this blockchain based system to share information. Bconnect was bulit on Hyperledger Fabric by Brazil's Federal Data Processing Service (Serpro), the country's state-owned IT service, which serves the Federal Tax Service of Brazil and the Brazilian Internal Revenue Service.

The bConnect platform aims to validate the authenticity and security of customs data shared between the Mercosur countries.[63] This tool enhances the agility and security of information exchange regarding foreign trade, particularly registration information on companies certified by the Federal Revenue Service as Authorized Economic Operators (OAS) which benefit from facilitated of customs procedures, both in Brazil and abroad.[64] The purpose of bConnect since its lauch has been to meet an international need for automating the exchange of customs data from OAS across countires, which previously was carried out largely over e-mails sending this data in the form of spreadsheets extracted from each country's respective systems. Additional plans include expanding this network to facilitate information sharing from customs declarations.

VASP Regulations Expected in 2024

Brazil intends to continue fostering enabling legislation in support of developments in blockchain and digital assets in the country. [65] In December 2022 Brazil enacted a legal framework for virtual assets ("Marco Legal das Criptos") through Law No. 14,478/22, which was approved, enacted, and entered into force in June 2023.[66] This framework provides guidelines for reguatory activities conducted by VASPs, while also stating that the crimes of fraud, money laundering, and other financial crimes with virtual assets would fall within the corresponding exiting frameworks.

This framework also replaces and formalizes a number of prior regulatory developments. The Central Bank and the Brazilian Securities and Exchange Commission are the designated regulators, with the Central Bank designated as the competent authority to regulate, authorize, and supervize the activities of virtual asset service providers (VASPs) operating in the country.

Under its new mandate as regulator overseeing the space, the Central Bank is expected to release an update to this regulatory framework for VASPs in 2024.[67] It has released public consultations on regulation of the space during 2023, requesting feedback from the market, on issues such as consumer protection, disclosures, and risks of decentralize governance, to incorporate into the upcoming framework. Once licensing requirements are underway, the expected outcome aims to attract entrepreneurial activity and foster innovation within the country. The Brazilian president has emphasized the importance of coordinated action with other regulators, notably the Brazilian Securities and Exchange Commission, for adequate oversight of activities in the space.

DREX: THE RISE OF CBDCS IN BRAZIL

Objectives

The discussion about the issuance of a Central Bank Digital Currency (CBDC) in Brazil has gained prominence over the last few years, broadening the general understanding that monetary authorities' financial stability mandate also comprises promoting innovation in payment methods. Authorities recognize that the accelerated digital transformation underway in the global economy makes financial innovation a requirement to ensure competitiveness in the future. Hence, ensuring financial stability is closely related to promotion of financial innovation, especially as it relates to improving financial inclusion.

After having systematically followed relevant discussions regarding digital assets and innovation in money since 2016, and also having conducted targeted relevant research initiatives on the matter, the Central Bank of Brazil (BCB) began to seriously consider issuing a CBDC in August of 2020, through internal discussions and discussions with its international peers. CBDC development is at the moment a work in progress, intended to be launched alongside the upcoming regulatory framework in the near future.

The aim of the Central Bank deepening financial inclusion in Brazil, democratizing the population's access to services, such as investments, financing and insurance. The intent to develop a CBDC falls within the Central Bank's vision of "financial democratization," which is the ultimate objective of its Agenda BC#.[68] Financial democratization consists in improving access to financial markets, low long-term interest rates, and better financial services to benefit the general population. Launched in 2016, the Agenda BC# is the Central Bank's strategic work agenda to tackle structural issues facing the national financial system through technological innovation. With this project, the Central Bank is pushing the market toward financial innovation and further blockchain adoption.

In this context, the possibility of the Central Bank issuing the Brazilian Real in digital format has been considered with the following objectives in mind:

- Keeping up with the dynamism of the technological evolution of the Brazilian economy;
- Increasing the efficiency of the retail payments system;
- Contributing to the emergence of new business models and other innovations based on technological advances;
- Favoring Brazil's participation in regional and global economic scenarios, while increasing efficiency in cross-border transactions.

CBDC project begins

In light of the success of Brazilian instant payments Pix, the Central Bank began to consider further possibilities of imlementing digital assets technology. The quick spread of decentralized financial transactions, conducted over blockchain ecosystems with the use of various digital assets as tokens, was perceived as an opportunity to apply such technologies to further modernize the Brazilian financial system. Based on the results of the Central Bank's working group on CBDCs established in August 2020, alongside advancing internal discussions on the topic, the path was forged toward building the conditions for issuing the Brazilian Real in digital format.

The Central Bank made a number of announcements throughout 2021. In 2022, in light of the accelerating development of the digital economy, the Central Bank promoted the discussion of possible uses of its CBDC through the LIFT Challenge Real Digital – a virtual laboratory to enable a collaborative environment to evaluate use cases and technological feasibility of the digital currency issued by the Central Bank. As a result, a prototype comprised of 9 different projects was developed in LIFT Challenge, with their results currently available as reports published on the LIFT home page.[69]

Drex CBDC Project & Features

In August of 2023, the Central Bank's CBDC project was given an official name and logo: the "Drex Platform," alluding to the initials of "Digital Real" and the name of the existing payments tech solution Pix.[70] One important aspect of the Drex Platform is that, under the proposed architecture, the Central Bank will maintain its partnership with the private sector in providing liquidity to the market, through the coexistence of the CBDC, or wholesale Drex, with private digital currencies, retail Drex, issued by regulated institutions through the transformation of demand deposits and payment account balances into digital currency in the Drex Platform. Such regulated private digital currencies will serve as the basis for building digital financial services and will play on the Drex Platform the role that stablecoins currently do in public chains.

To access the Drex Platform, the financial user will need an authorized financial intermediary, such as a bank, cooperative or payment institution. This intermediary will transfer your money (specifically, balances on demand deposits and payment accounts) to the user's digital wallet on the Drex Platform, to enable transactions with digital assets. As is already the case with Pix, the population's access to intelligent services on the Drex Platform will occur through an app offered by their financial service provider – such as a bank, a credit union, fintech, or payment institution.

The objectives trough the Drex platform will be carried out through a platform that operates with digital assets and smart contracts, among other functionalities, facilitating the provision of more efficient and secure financial services and products. Hence the smart services of the Drex platform will be carried out through smart contracts, which can be adapted to the convenience of customers, and can allow financial transactions to be completed when all conditions are met, adding security to all parties. The benefits of these technologies, to be used with Drex, will be offered to a larger base of citizens without exposing their businesses to the uncertainties of an unregulated financial environment.

Programmability functions – available in the crypto asset ecosystem and across web3 – are recognized for their potential to expand financial inclusion. The standardization of protocols involved in financial transactions and the interoperability of solutions integrated into the Drex Platform – apart from the reuse of protocols and composability of financial services – reduce the cost and time of developing new financial products, enhance access and transparency, while freeing the entrepreneur to focus on specific aspects of their business model.

Risk Management

All actions undertaken by the Central Bank support the perception that, in the absence of a decentralized infrastructure that has the central bank currency as a settlement asset and that is compatible with transactions with tokenized assets, users of tokenized financial services are exposed to integrity and market risks, which could compromise the financial stability. Moreover, if financial instruments that are traded in traditional markets are tokenized and traded on decentralized ecosystems as well, then there arises the risks of pricing mismatches and market fragmentation.

Regulators have taken significant steps to ensure consumer protection, especially data protection and privacy at scale. They have deployed significant resources toward these protections, as well as systems which reveal this topic is not taken lightly.[71] Brazil has also enacted its own dat privacy law, the Lei Geral de Proteção de Dados or General Data Protection Law in English (LGPD), with purpose of protecting every natural person's fundamental rights of freedom and privacy, alongside the free development of a personality.

Drex alignment with regulatory objectives

Thus, the Drex Platform is being developed to democratize access to the benefits of the digital economy, bringing more efficiency and security to financial transactions, by allowing various types of secure financial transactions with digital assets and smart contracts to be available to the population. Those may be the building blocks for new or improved financial services, and upon those new or improved business models.

In this scenario, the Central Bank concluded that the adoption of a DLT infrastructure for Drex would allow a high degree of auditability, traceability and transparency, guaranteeing the necessary tools for its supervision and regulation, at the same time in which it fosters the incorporates new technologies and the development of new businesses models with the potential to meet the population's demand for natively digital means of settlement, similar to those available in the crypto assets ecosystem.

To deepen the internal debate on asset tokenization – considering the technical aspects of the registration, custody, trading, and settlement activities of financial assets in DLT infrastructures –, the Central Bank established a working group at the end of 2022. Several round tables were held with representatives of the financial market, which resulted in virtual seminars with the themes "Market Operators" – June 2023; "Market Infrastructures" – July 2023; "Identity and Compliance" – August 2023; and "Sustainable Assets" – September 2023.

Initial Testing & Next Steps

To operationalize the development of a unified testing platform for Drex, the Central Bank established rules and procedures for the operation of the Drex Platform Pilot Project, the Drex Pilot, as Resolution 315/2023 - Central Bank. On the one hand, the group of Pilot participants is kept small and menageable to be efficient. On the other hand, the Central Bank established the Drex Forum, in March 2023, with the aim of providing transparency about the implementation of Drex, in addition to favoring broader society's participation in the process. The Drex Forum is a communication channel with market agents and entities representing institutions regulated by the Central Bank, as well as other interested sectors of society. Two virtual Drex Forum plenaries have already been conducted, in June 2023 and September 2023.

The Drex Pilot is, therefore, a testing platform for operations with Brazilian digital currency. At the current testing stage, the BC is evaluating the benefits of programmability and privacy guarantees that can be assured by the Drex Platform, a multi-asset environment based on the Hyperledger Besu open-source platform, in where simulated operations with digital assets are being conducted.

To participate in this testing environment, the Central Bank received **36** applications from individual companies and consortiums of companies. Based on the criteria established in the Drex Pilot Regulation, 16 proposals were selected, comprising a total of more than **70** firms involved in the Pilot. The construction of this testing environment began in March 2023 and its first testing phase is planned to be completed in May 2024.

After the current testing phase planned to be concluded on May 2024, assuming that the privacy concerns will be clarified by then, the Central Bank will open another call for use cases to be deployed on the resulting platform, so as to incorporate the population in the testing environment by the end of 2024 or the beginning of 2025.

TOKENIZATION

Tokenization gaining popularity

Tokenization involves the conversion of rights to an asset into a digital token on a blockchain. Stakeholders recognize that the tokenization and trading of real-world assets is an important next step for a blockchain integrated economy. Regarding the tokenization landscape in Brazil, both neobanks and banks are getting heavily involved in the trend to tokenize and trade assets in Brazil. Tokenization in general is a part of financial players' strategy to enter the blockchain and digital assets space (e.g., tokenizing fixed income, stocks, currencies, real estate, etc.).

As the market evolves and new tools for accessing tokenized products emerge, the adoption curve is expected to steepen. In Brazil, the anticipated launch of "Drex" is eagerly awaited by the market, as it will serve as a tool for the settlement of digital assets, further facilitating Brazilian investors' access to blockchain-registered assets. Tokenization initiatives using the same rails as Drex set to ensue at an accelerating pace. Stakeholders are already exploring strategies to tokenize and experiment with the possibilities, and evaluate the opportunities.

Regulatory Support

New advancements in the provision of an infrastructure for a regulated DLT, as well as regulatory clarity, create a promising environment for innovation in the financial sector. The Central Bank is currently coordinating a working group that is expeted to produce a detailed report on the tokenization of financial assets and securities. Major financial institutions are developing and testing new application in partnership with Brazilian regulators, improving digital assets' efficiency while contributing for the development of a legal framework.

Bolsa OTC Brasil is a great example of this collaboration, a project primarily focused on the tokenization of private credit instruments (CCBs, CCIs, and CCCBs) with a goal to test issuance, distribution, and settlement improvements through blockchain technology. Approved by the Central Bank at the end of 2021, this initiative originated from the LIFT (Financial and Technological Innovations Laboratory) program, which initially selected 8 projects to offer financial products on the platform. Notably, big financial institutions like Bradesco have utilized its infrastructure, tokenizing a CCB issuance in a transaction worth BRL **10 million** in January 2023.

Tokenization in Brazil's banking sector

Brazilian banks in particular looking to enable the tokenization of as many assets as can be made feasible. In February 2023, there was a successful completion of the first tokenization of a security by a traditional Brazilian bank, BTG Pactual, under the project named "ReitBZ". Backed by real estate in Brazil, ReitBZ was issued in the Cayman Islands to distribute the token for international investors. Launched in May 2019, the project raised **BRL 23 million** and distributed a total of **BRL 4 million** in dividends to its shareholders, yielding an average return of **137.5%** over Brazil's basic interest rate during its tenure. The project successfully tested an international distribution of a tokenized real-world asset, and the use of digital wallets for dividends' payments in digital currencies.

Another notable development in this realm is the recent collaboration between Itaú, one of the largest banks in Brazil, and the digital assets company, Liqi. Together, they have issued the first RWA token of TIDC (Credit Rights Tokenized Investment). This move signifies the growing acceptance and integration of tokenized assets in mainstream banking and underscores the potential of blockchain technology in revolutionizing the financial landscape.

Tokenization across sectors in a Regulatory Sandbox Environment

The Brazilian Securities and Exchange has launched a Regulatory Sanbox where a number of promising tokenization projects are being developed. This has promoted significant progress in Brazil's tokenization sector encompassing the stock market. The regulatory sandbox has already approved projects involving issuance, public distribution and trading, in an OTC market, of securities issued or represented by tokens on blockchain networks, such as SMEs' stocks and bonds.[72]

For instance, BEE4, a tokenized stock trading platform currently in CVM's sandbox, held its inaugural trading session in September 2022, with a daily trading volume of **BRL 332,000**, surpassing the company's projection by **50.9%**. Leveraging this technology, Eletron Energia, a company specializing in energy optimization with an estimated total project value of BRL 162 million, is also set to conduct a tokenized IPO in January 2024. The anticipated minimum capital raise is BRL 3.33 million, and the company will be the fourth to embark on a tokenized IPO journey, following Mais Mu, Plamev Pet, and Engravida.

Tokenization in Carbon Markets

In the realm of carbon credits, as the demand for carbon emission offsets surges among major corporations, the carbon credit market is projected to be worth approximately **USD 50 billion** by 2030, as per the "ESG Under Pressure" report by Reuters. Tokenization can enhance both the transparency of asset conditions and their liquidity, democratizing access to this market and playing a pivotal role in its growth. Taking advantage of the huge potential to generate carbon credits in Brazil, Ambipar, a leader in environment management in Brazil, has built a company called Ambify with the goal of tokenizing and distributing carbon credits in Brazil.

CONCLUSION

For all the developments stated above, Brazil is positioning itself to be a country with significant market opportunities in blockchain and digital assets, and it arguably may be the most overlooked crypto market in the world. The population is willing to take risks and try new technologies, which lowers the hurdle for crypto adoption.

The Drex ecosystem is establishing itself not just as a platform to send tokenized national currencies back and forth, but also as a backbone for a much more widespread tokenized financial system. These developments, with the active collaboration of regulators, are being designed to positively affect the lives of everyday Brazilians in many ways. The cost of doing business remains high in Brazil, largely driven by intermediating transactions. Hence the cost reductions and increased efficiencies of blockchian related projects can be among the most value adding in the world if structured correctly, with much value to be generated across the Brazlian society. Standardization and composability of financial services over blokcchian platforms can significantly lower the bar for fintechs to enter the market.

Finally, there is a strong angle toward inclusion across the innovation and transformation initiatives leading up to the expected VASP framework. Stakeholders, particularly regulators, recognize that financial markets will change fundamentally, as well as the importance of keeping risk management in check. Therefore the high emphasis on supporting blockchian projects has been to provide better financial services for the population, and open the market for new fintech companies to provide their serivices in the country. In many ways, Brazil can be considered a case study in responsible government-promoted innovation

SECTION IX

DIGITAL IDENTITY

EXECUTIVE SUMMARY

In the last years, the ecosystem around digital identity and digital identifiers has seen a rapid and significant set of announcements, activity and adoption. This is reflected through pilot projects, production deployments and governments announcing extensive funding into creating the technology infrastructure and ecosystem necessary to incubate innovative approaches using digital identifiers. However, this growth has faced a fair number of challenges. The topic of digital identity is complex, and when these have been ignored, they have caused significant harm to consumers leading to reduced trust in the process. There have also been instances where the digital identity ecosystem has enhanced the level of tracking, surveillance and violation of privacy. However, the critical challenge has been the technology methods needed to design, build, implement, and maintain the infrastructure required to offer services that consume digital identifiers. Governments, systems integrators, developers, and rights activists have struggled to form a robust understanding of how open standards-based digital identity can be a way to realizse the UN SDGs.

This report is meant to focus on a number of challenging topics in this domain. It is being published as many organizations undertake similar exploratory examination and evaluation of the technology standards, domain models, and approaches. The GBBC convened a working group of experts with deep experience in digital identifiers as a critical component of digital transformation. Technology in this sector can moves faster than any documentation, and the group fully acknowledges that work on digital identity will involve continued engagement and developments.

INTRODUCTION

In any discussion around digital identity and digital identifiers, it is essential to note that nearly 1 billion people do not have legal and verifiable identity documents — the absence of such documentation results in their inability to access various public or private services. As digital identity's issuance, circulation, and exchange increase, the public and private systems that issue such IDs must be designed to respect foundational rights. Moreover, as the world is becoming more digitized, lack of identity in the digital realm can have major implications on inclusion and lifestyles, potentially aggravating the digital divide between those with access and those without access to networks of productivity and exchange to conduct activities.

Digital identity is fundamental to meet many of the UN Sustainable Development Goals (SDGs) in pursuit of reducing global inequalities. Specifically, SDG 16 on Peace, Justice, and Strong Institutions sets a target to provide a legal identity for all, including a birth registration. Otherwise there is an increasing risk of leaving entire communities disenfranchised and cut off from means of human flourishing. Advancing digital identity also requires advancing data protection, and the most promising models are inherently people-oriented. Yet in this context, there have been several approaches to digital identity, with multiple design considerations, opportunities, and risks. While there have been several approaches in development, it is fundamental to "get it right," in the sense of providing adequate identity that is also secure.

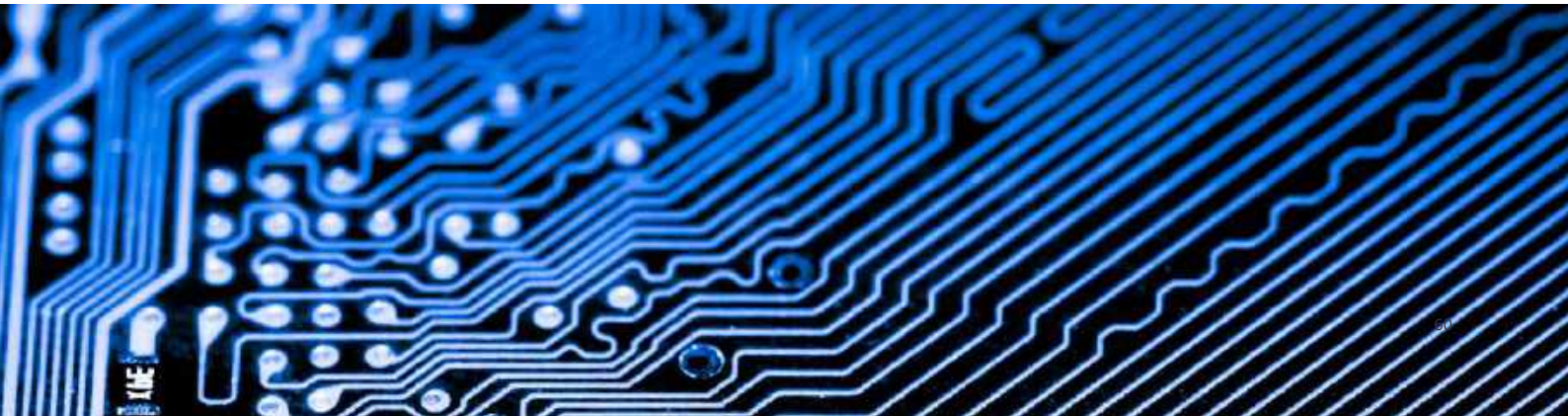
Policymakers, regulators, governments, and other stakeholders often bring their definition of digital identity and digital identifiers. This report will define identity as <insert the definition and citation>. A digital identity may entail one or more attributes associated with the individual. The process of creation and issuance of the digital identity conveys a level of assurance necessary for the ID to be used in different workflows.

When poorly designed and implemented digital identity systems can exacerbate the topics of exclusion, surveillance, and harm - designers and implementors often grapple with the challenge of adopting the best practices, standards, and technology frameworks, which could result in better outcomes for everyone. Today, sizeable digital identity systems, which include foundational IDs such as national IDs, functional IDs such as birth and death registration records, pension systems, etc, are no longer in prototype design or pilot stage - they have gone live. This presents a fundamental challenge for future implementations, as the insights and knowledge from the ongoing deployments will be used to improve and innovate incrementally.

Digital identity systems often build upon and extend existing foundational components. While this expedites the drafting of necessary changes to regulations and workflows, it also highlights the need to focus on data quality. Digital ecosystems require digital identifiers with a high level of assurance to create trustworthy interactions. These data exchanges go a long way in mitigating the risks associated with such systems. This report examines the ongoing and emerging challenges and concerns around digital identity using the identity life cycle. This lifecycle is imagined to comprise a set of processes, including registration and enrollment, issuance, use and management. Each of these processes helps bring to light some of the complex topics associated with digital identity and audit, risk management and standards.

Digital identity systems have emerged and demonstrate a set of archetypes. These system archetypes are called Centralized, Federated and Decentralized . Each archetype has specific strengths and challenges, and while this report will not provide any comparison among these systems, it is necessary to state that the discussion around digital identity will draw from the ongoing efforts around the decentralized archetype.

As this report intends to guide and aid designers of digital identity systems, it provides a set of technical and non-technical considerations that can be read as recommendations. These considerations have been put together with the intrinsic understanding that digital IDs should empower humans and not contribute to curtailing their rights in any manner.



CHALLENGES OF DIGITAL IDS

Backdrop

The design, development and deployment of digital identity systems bring forth complex challenges because the approach needs to consider a set of hard problems. These challenges range from synchronization and reconciliation issues of identities across disparate systems as well as being able to design robust portable IDs that do not inadvertently aggravate the digital divide. In this context, it is important to note that digital systems are relatively new. They were first created following World War II, and the earliest mainframe computers were adopted by government and industry in the 1960s. Accounts for different users were created, and these evolved over time to support employees in enterprises accessing their accounts to do their work across different applications and computers.

Many systems in enterprise and government were used to track information about people who are customers (who buy things from businesses) and citizens or residents (who pay into pension schemes and pay taxes). These people did not have their computers, but information about them lived inside these enterprise systems.

The paradigm of how to manage an employee identity in an enterprise system is widespread, and it makes sense for that context. An employer hires an employee to do work inside their enterprise. To do that work, the enterprise gives them an identifier within the context of the enterprise. To use that identifier, the employee establishes a shared secret (password) with the enterprise, and when they assert they are in control of a particular identifier, they are prompted to provide the shared secret and if they succeed in sharing that with the enterprise they are authenticated into the enterprise.

The commercial service providers in the early days of the first commercial services (like AOL, Compuserve, Prodigy) that people subscribed to used the model that employer-employee systems had - they allowed people to claim identifiers within their name spaces and then authenticate to those services and interact on the internet. This model continued with common web-mail providers like Hotmail (now MSFT), Gmail and Yahoo.

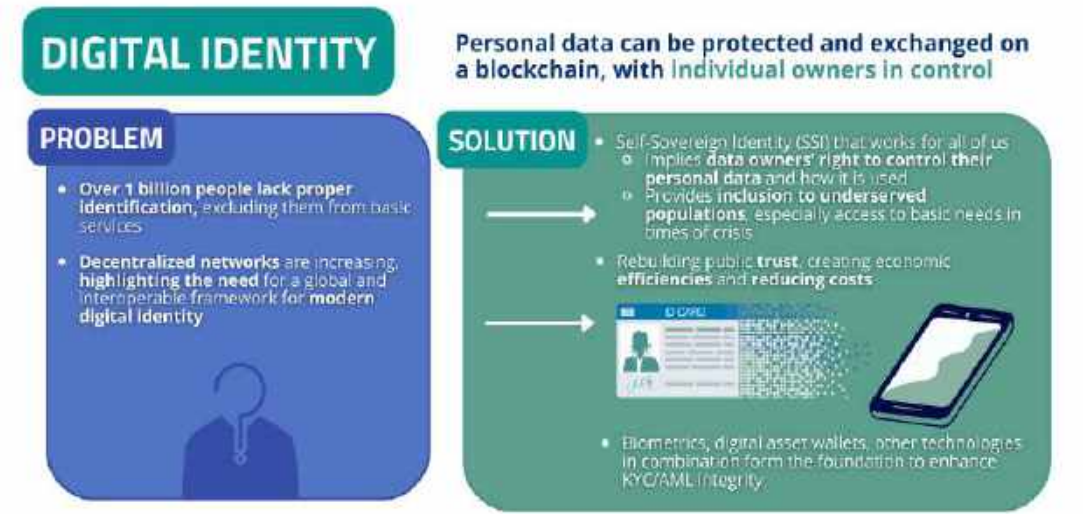
This is called the two-party model. It has an identity provider (who controls an identifier) and a relying party. For an individual to use an identifier from one service at another service (relying party), they must prove it to the relying party by authenticating to them. Tokens are exchanged between these two parties. This model of identity provider and user or employee, to whom an identifier is assigned and can be revoked by the identity provider, does not align with individual autonomy and rights that we experience daily as we move about the world in other roles outside of being “an employee.” We should therefore not have a general-purpose digital identifier revocable by another party like a government or commercial entity that, in the fundamental design of the architecture, has power over us.

There has been a significant amount of work in the last few years by a community that has aimed to change this two-party paradigm, where there is "control over an identifier" in either a private namespace or a global registry namespace, to a model where people could create and control their identifiers. This effort spawned the Decentralized Identifier standard at the World Wide Web Consortium (W3C). Identifiers only go so far in solving identity challenges, especially ones that are very long and not humanly readable numbers. What matters to people and organizations is more information about the very people and organizations - key attributes and information. This is where work on the three-party or direct presentation model arose, where individuals are put at the center of any transaction related to identity information in a three-party model. Where issuers issue credentials (a blob of signed attributes) to holders (individuals or businesses), and then the holder can choose what relying parties (or verifiers) they want to involve, as many times as they want to, and the issuer of the credential and the verifier of that credential do not connect or talk. Hence, the three parties.

Commonly understood challenges

One of the often-quoted aspects of the challenges with digital identities is the number of individuals who do not possess any formal verifiable documentation establishing their identity and associated rights. This presents a growing challenge in addressing the inequity and denial of rights globally. Sometimes, digital identity systems are also not designed to be equitable, secure, and portable. These systems hinder the ability to use digital identity for access to services or benefits, with the holder of the ID being able to govern and manage their data.

Today, digital identity-centric systems are required as an integral part of many workflows. These range from user onboarding and KYC (Know Your Customer) flows to fraud prevention systems, electronic commerce marketplaces, delivery of healthcare and telemedicine, travel and hospitality industry, education and learning, financial services, gig economy and peer-to-peer services, etc. Delivery of citizen services by governments is one of the largest use cases of using digital identity to manage access to services for taxes, permits and document workflows.



This report will discuss specific details of the challenges in a later section. It is important to mention that an emerging discourse in digital identity and digital identity systems is the need to make them "people-oriented" and "consumer-centric". This approach enables the design and development to focus on the rights of the holders of the digital identities.

For instance, the short introduction to the UN Joint Staff Pension Fund project is provided below as an aid to conceptualize some of the complexities and the methods by which good design can help create digital trust ecosystems that are impactful, respectful of rights, and enable the delivery of services.

An Example - The UN Joint Staff Pension Fund

The United Nations Joint Staff Pension Fund (UNJSPF) supports 84,000 beneficiaries located in 192 countries. As required by its Regulations and Rules, each year, UNJSPF needs to verify the proof-of-existence and location of those receiving benefit payments through a process referred to as the "Certificate of Entitlement" exercise. For more than **70** years, this process has been conducted using a paper form and relying on **192** postal services, involving printing tens of thousands of pieces of paper, handling and processing physical mail, and sometimes multiple interactions between the beneficiaries and UNJSPF.

In 2020, COVID-19 caused widespread disruptions to postal services, negatively impacting the Certificate of Entitlement exercise. The challenge for the UNJSPF was to modernize this process and find an innovative, reliable, and environmentally sustainable solution. A digital identity solution was created to address this challenge, with a system called the "Digital Certificate of Entitlement (Digital CE)", which offers a secure and user-friendly mechanism to verify the existence of retirees and beneficiaries for the continuation of benefit payments and generates traceable, unalterable, and independently auditable evidence.

The Digital CE is a sustainable initiative, as it reduces the use of paper and global postal services. It is an application that can be loaded on mobile phones, tablets, or computers, and on average, it requires about 30 minutes to complete the initial enrollment in the first year and only 5 minutes the following years.

Aligned with the United Nations Secretary-General's vision of a digital UN, the Digital CE is part of implementing the UNJSPF strategic plan and Information and Communications Technology investment in simplifying client experiences and modernizing the Fund's services.

Compared to the paper-based proof-of-existence solution, the Digital CE application offers retirees and beneficiaries a much faster, more secure, and easier way to validate their identities and locations to meet the requirements for continued benefit payments. After downloading the application on their smartphones or tablets, they can enrol in the app in a few easy steps by filling out some personal information and taking pictures of themselves. Once enrolled, they schedule an in-person video appointment with the Fund's Call Centre to complete the identity verification process.

DESIGN AND TECHNOLOGY CHOICES

In designing the Digital CE application, the project team put clients' needs at the heart of the process and focused on simplifying the client experience. Adopting a human-centred approach, the product development team identified retirees' and beneficiaries' needs at the outset, considering the disparity in geographical location, technological ability, mobile device availability, and internet connectivity. The team used an iterative approach to build multiple proofs of concepts and ran a pilot incorporating user feedback from beneficiaries to improve product usability and design.

The project team explored new technologies to develop a user-friendly and cost-effective solution. Biometric technology, such as facial recognition, was used to authenticate beneficiaries' identities. Project team members worked hard to perfect the facial recognition functionality and improve the application's user-friendliness. After assessing existing off-the-shelf solutions, they built a custom-made biometric facial recognition solution to deliver better results. The solution is now being incorporated into other innovation plans involving digital identity within the United Nations System. In addition, the Digital CE application incorporated emerging geolocation technology that can capture beneficiaries' physical locations to validate their places of residence. The application also embedded blockchain technology to have a traceable, immutable and independently auditable record of the certification process.

Retirees and beneficiaries can complete their annual Certificate of Entitlement exercise entirely using the digital application, even offline, without the need to print or sign any paper. The solution also eases the burden on the Fund to manually process tens of thousands of paper forms to validate beneficiaries' identities and locations. Hence it has contributed to increased efficiency in the validation process of the Certificate of Entitlement. Considering the environmental impact of the end product, the project team designed and delivered a solution that is environmentally friendly and sustainable. The employment of a digital solution prevents thousands of paper and postal mail per year, with a target population of 84,000 retirees and beneficiaries having to fulfill this requirement. It only marginally impacts the general use of mobile phones and tablets, as it requires downloading the app and, on average, 30 minutes maximum to complete the initial enrollment, and only five minutes the following years.

PRINCIPLES OF DIGITAL IDENTITY

Any discussion around digital identifiers and digital identity needs to acknowledge the potential risk of creating unintended consequences, harms, and biases through poor design choices, poor technology implementation, and poor compliance with regulatory requirements. Sometimes, a poorly constructed regulatory framework for governance also contributes to the harms resulting from deploying such IDs. It is also essential to be aware of the fact that many digital identity systems are designed to be the next generation of IDs in an ecosystem which already has a form of identifiers. Thus, these legacy systems include a set of governance and operational rules, legal frameworks, and workflows that have worked for non-digital or analog systems.

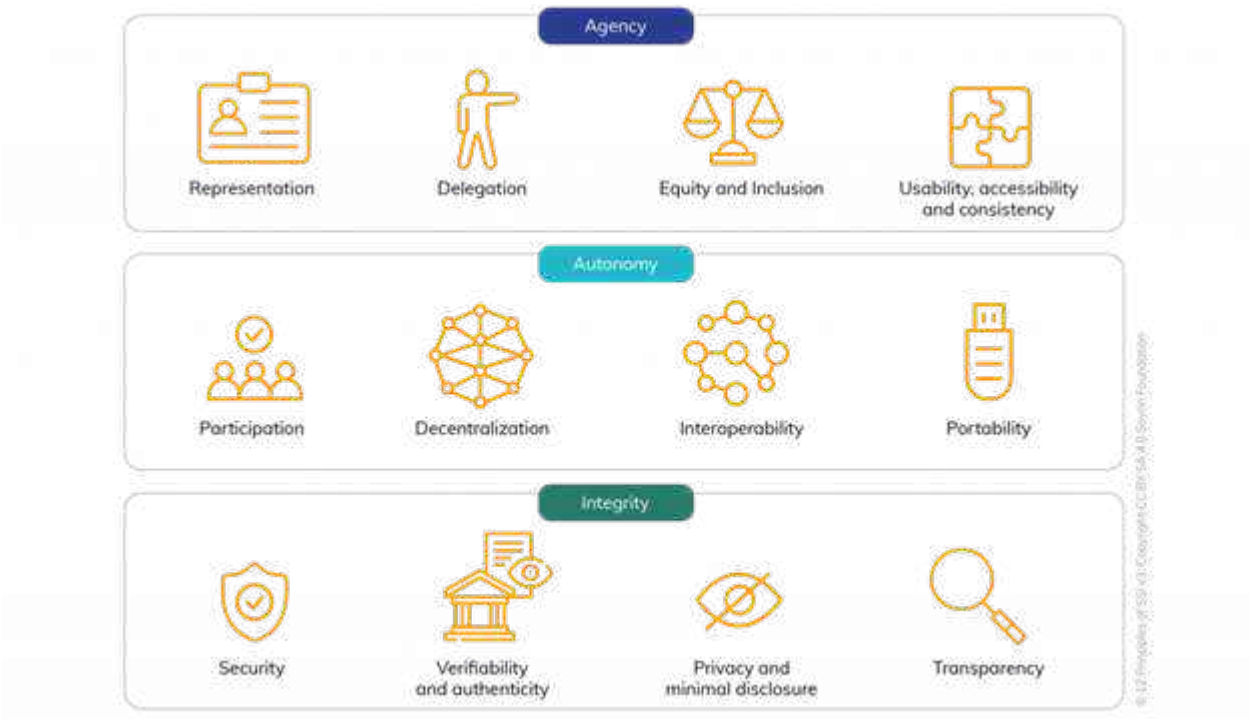
If digital identity systems are to make the expected impact, it is necessary to frame a set of principles to help design, evaluate, and assess the emerging technology patterns in digital governance. Some of the recent work in the domain of digital identity and principles come from organizations are listed below:

- **The Sovrin Foundation:** Sovrin has published[73] *The Principles of Self-Sovereign Identity (SSI)* as a set that has been organized to provide a human rights-based perspective in the context of digital identity and identity rights of holders, with the ultimate goal to enable humans to exercise their rights to work, study, and travel, while having freedom of choice and being protected.

- *Human-Centric Digital Identity for Government Officials*[74] published by the **OpenID Foundation** as a nonprofit standards body advancing identity and security specifications, with the objective of helping billions of customers, across millions of applications, to assert their identity

- The **OECD** Privacy Principles [75]which focus on collection limitation, purpose specification, security safeguards and accountability among other factors.

Figure 1: 12 Principles of SSI (Source: Sovrin Foundation)



DIGITAL IDENTITY LIFECYCLE AND STANDARDS

Digital Identity Lifecycle

As new approaches to digital identities go into production, it is important to note that such identifiers create opportunities for advancing inclusion, privacy and agency over one's data. Digital identities help the holders of such identifiers to make claims about specific attributes. The digital identity has a lifecycle[76] which includes registration, issuance, exchange, and management flows. The entire lifecycle is the basis of enabling various use cases in different digital ecosystems to be designed around digital identities and the access to various services offered through exchanging such identities.

Each stage of the lifecycle includes specific tasks and activities made possible by adopting specifications, standards and guidelines.

It is important to highlight that not all stages of the lifecycle will have the same level of assurance - this is determined by the governance framework of the digital trust ecosystem where the digital identifiers are issued and the purpose. Assurance levels can be thought of as the equivalent of confidence and trust in the specific digital identifier based on the process through which the identifier was issued.

Important Standards and Specifications

Digital identifiers are issued and managed within a specific digital ecosystem. This means that the lifecycle of digital identifiers is influenced by the jurisdictions in which these are managed as well as the legal, regulatory and technical requirements in that particular jurisdiction. It is important to be mindful of this situation as often a wide range of standards, specifications and recommendations are involved in the production and circulation of digital identifiers. If these standards, specifications and recommendations are incompatible with each other, then the notion of interoperability, wider verifiability and trustworthiness breaks down. While it is impossible to list all possible standards and specifications related to digital identifiers, it is important to mention a few which are relevant to the concept of their significance in the digital identifier lifecycle.

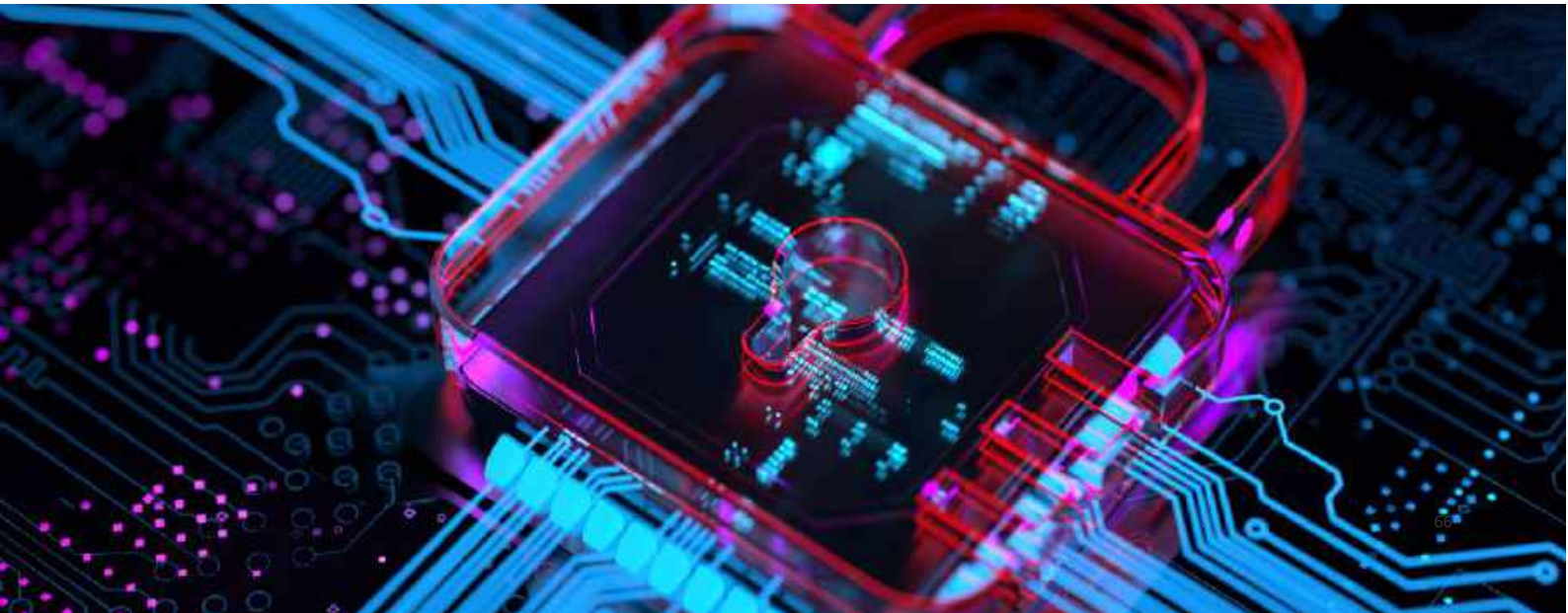
The production, management and exchange of digital information is intimately linked with the available data governance and data protection regulations.

The section on Principles of Digital IDs indicates some of the principles recommended to be adopted while designing digital identifier workflows. Additionally, there are standards and specifications which are necessary for good digital identifiers to be instantiated. Such standards include, but are not limited to the following:

- **ISO/IEC 29100** Privacy Framework
- **ISO/IEC 29134:2017** (Guidelines for privacy impact assessment)
- **ISO/IEC 29184:2020** (Online privacy notices and consent)
- **Blinding Identity Taxonomy**[77] from the Kantara Initiative Information Sharing Interoperability Work
- **NIST SP 800-63 Digital Identity Guidelines**[78] (includes 800-63-4, 800-63A, 800-63B and 800-63C)
- **Overlays Capture Architecture (OCA) Specification**[79] from the Human Colossus Foundation
- **Verifiable Credentials Data Model**[80] from the W3C

Digital Identifiers also include the topic of Risk Management and in later sections a few recommendations are provided for this aspect.

It is also important to note that there is an entire world of biometric standards that is beyond the scope of this paper. Biometrics in the form of photographs have been used for a long time on identity documents. Knowing the current best practices for creating templates and sampling against those biometrics is important while creating the regulatory framework and technical architecture for digital identifiers.



Standards Development Communities

A wide range of global standards power the technology designs which enable the digital identifier lifecycle. Standards Development Organizations (SDOs) and communities work to ensure that the process factors in regulatory and privacy requirements, and that it also addresses the topics emerging from preventing harm. Some of the notable SDOs and communities are listed below.

ISO	ISO (International Organization for Standardization)[81] is an independent, non-governmental international organization with a membership of 169 national standards bodies.
W3C	World Wide Web Consortium (W3C)[82] has been an international multi-stakeholder community where member organizations, a full-time staff, and public work to develop open web standards together across key stakeholders.
IETF	The Internet Engineering Task Force (IETF)[83], founded in 1986, is the premiere standards development organization (SDO) for the Internet. The IETF makes voluntary standards that are often adopted by Internet users, network operators, and equipment vendors, and it thus helps shape the trajectory of the development of the Internet. But in no way does the IETF control, or even patrol, the Internet.
Open ID Foundation	Founded in 2007, the OpenID Foundation (OIDF)[84] is a global open standards body committed to helping people assert their identity wherever they choose. It is a global vibrant community where identity peers and thought leaders convene to craft the identity ecosystems of tomorrow.
ToIP	The Trust Over IP (ToIP)[85] Foundation was launched in May 2020 with 27 original founding member organizations. It was gestated over the previous year as a confluence of multiple efforts in the digital identity space, verifiable credentials, blockchain technology, and secure communications spaces by people who saw the need to converge and create an interoperable architecture for decentralized digital trust.
DIF	DIF[86] is an engineering-driven organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interoperability between all participants.
Open Wallet Foundation	The OWF[87] aims to set best practices for digital wallet technology through collaboration on standards-based OSS components that issuers, wallet providers and relying parties can use to bootstrap implementations that preserve user choice, security and privacy.
MyData	MyData[88] is a human-centric approach to personal data management, which combines industry need for data with digital human rights.

Kantara Initiative

Kantara Initiative, Inc[89] is an international ethics based, mission-led non profit industry 'commons'. Kantara's Mission is to grow and fulfill the market for trustworthy use of identity and personal data in pursuit of its Vision to see equitable and transparent exchange of identity and personal data for mutual value. Kantara's members are spread across continents and countries around the globe.

Human Colossus Foundation

The Human Colossus Foundation (HCF) [90]is a Swiss-based independent non-profit organization (IDE: CHE-441.741.202) working globally to create and foster the development of critical infrastructure for a data-agile economy, coined the Dynamic Data Economy (DDE).

The eSSIF-Lab

The European Self-Sovereign Identity Framework Lab (eSSIF-Lab)[91] views itself as an ecosystem of parties that work together to make existing (and new) Self-Sovereign Identity (SSI) technology into a scalable and interoperable infrastructure that businesses can use very easily for negotiation and execution of (business) transactions with other organizations and individuals alike, as further described in the eSSIF-Lab Vision.

The above list is not exhaustive. It presents a small snapshot of the various organizations, communities and bodies engaged in the work of creating robust technology designs and recommendations which can be adopted by organizations attempting to implement digital identifiers as part of enhancing the experience of the consumers.

Introduction to Digital Wallets

The digital revolution has seen an increased focus on the digitalization of several aspects of human life. Facilitated by incredible developments in the financial industry, wallets and conversations about wallets have transformed from a visually bulky leather pouch filled with precious stones, coins, banknotes and identification documents to versatile, functional and accessible digital wallets.

While most would associate digital wallets with electronic wallets that hold digital assets (essentially the digitalization of the traditional wallet), the past couple of years have brought interesting progress by both governments and private sector developers towards the creation of a functional digital wallet that private persons can use to store, manage and even share their personal data.

Variations of digital wallets have been introduced in countries like the Faroe Islands, India, Monaco, Thailand and the United Arab Emirates, allowing their citizens and residents to benefit from either a simple repository of immediately accessible personal data, whether for identification as is the drivers' license in the UAE or for having access to the financial system by simply scanning a QR code in Thailand.

The digital wallet concept has also raised the bar and intensified conversations around sovereignty, security and privacy issues concerning personal data. Interoperability, user-centric ergonomics, and global and personal security are factors that regulators and developers understand are and will be differentiating factors for long-term, sustainable solutions.

DESIGN CONSIDERATIONS

Technical Considerations

The technical considerations involved in the design of a robust digital identifier infrastructure follow from the Principles of Digital ID. It follows that with a human-centric approach to design the individual holder of the digital identifier must be at the critical element when examining competing design approaches. This leads to the following requirements as a necessary component in design

- Consent-based approach to the exchange of data
- Transparency in the acquisition, processing and exchange of data
- Selective disclosure of information unless required by local regulations
- Adoption of open standards in the design of systems to enable interoperability
- Handling of guardianship and dependent relationships to enable inclusivity, equity and representation
- Capability to address both onboarding and offboarding of consumers at end of natural lifecycle

In addition to the above requirements, there are two additional overarching guidelines which influence the technical choices and technology adoption. These are:

- **Security and resilience:** Digital identity systems should be secure and resilient to attacks. This means that they should be designed to protect personal data from unauthorized access, use, or disclosure.
- **Privacy by design:** Digital identity systems should be designed with privacy in mind. This means that they should minimize the amount of personal data that is collected and stored and that they should use privacy-preserving technologies.

Non-Technical Considerations

ETHICS

The UN Roadmap for Digital Cooperation [92]was adopted by the UN General Assembly in June 2020. The Roadmap laid down a vision for the responsible and inclusive development and use of digital technologies, and ethical principles on digital identity formed a key pillar of the Roadmap.

These principles are intended to guide the development and moral use of digital identity systems globally and in a way that respects human rights, promotes inclusion, and is devoid of bias that would disadvantage any ethnic or socio-economic group. Since there are only regional pockets where compliance standards, mandates and penalties exist, the recommendation included developing and advocating a shared and globally acknowledged set of ethics compliance parameters that would be set by federal mandates and or legally binding and enforced via local government agencies. These parameters are intended to be revisited annually to reflect changes in the pace of adoption and or applications of Blockchain technologies—impacting both public and private sectors. These parameters are thus empathic, based on principles of protecting human rights, freedoms and preferences to control an individual's personal information and its access and data repurposing.

The ethical compliance principles include but are not limited to

- **Human rights and inclusion:** Digital identity systems should respect and promote human rights, including the right to privacy, the right to non-discrimination, and the right to access essential services.
- **Proportionality and necessity:** Digital identity systems should be proportionate to the risks they intend to address and not be used unnecessarily or excessively.
- **Transparency and accountability:** Digital identity systems should be transparent and accountable to the public. This means that people should be able to understand how their data is being collected, used, and shared and that there should be mechanisms to hold those who control digital identity systems accountable for their actions.
- **Human-centered design:** Digital identity systems should be designed with the user in mind. This means that they should be easy to use and understand and meet the needs of all users, including those with disabilities.
- **Multi-stakeholder participation:** The development and use of digital identity systems should involve various stakeholders, including governments, businesses, civil society organizations, and individuals. This will help ensure that the systems are designed and used fairly, inclusively, and beneficial.

GOVERNANCE AND POLICY

There is significant variability in the pace of governance and compliance standards adoption by regions of the world related to digital identification. The European Union's General Data Protection Regulation (GDPR) – is the most advanced in documenting requirements for the processing and sharing of personal data. Currently, in Asia and the Americas, the federal government and private consortia are collaborating to propose nationwide data security laws and mandates. The increasing occurrences of data theft and digital data privacy in healthcare are critical drivers for building regulatory frameworks and enforcement mechanisms to deal with data security, data governance and incidents of data breaches.

Governance and policies in the future must manage across several gaps:

1. development of a consent ontology model;
2. development of a methodology for monitoring fairness on the blockchain;
3. resolution of the contradiction between auditing and obfuscation;
4. development of a methodology for tracking controllers in the blockchain; and
5. integration of the different-purposed technical solutions without conflicts.

With a few emerging deployments of digital identities using blockchain technology to create data anchoring, it is necessary to know the status of data protection approaches when blockchain is involved. Standards Development Organizations (SDOs) such as the ISO have published documents on this topic. However, there are a limited number of references related to various compliance requirements of the blockchain (ISO/TR23244:2020 provides a set of cursory guidelines for personal data protection applied to the blockchain). Since digital identities come with privacy and security risks – what adds complexity is the fact that compliance requirements will need to be auditable—taking into consideration individual rights to control the sharing of personal information.

In governance and policy-making, the two additional essential elements are

- **Regulating Verifier Collusion:** Regulators might require access to blockchain source code(s) to build data monitoring to analyze transactions and price trends to detect tacit collusion. This practice, while well-intentioned, also creates ethical concerns about what aspects of the transactions are private matters. Moreover, if this information falls into criminal hands, it could be misused for unethical purposes, including black mail or other personal reputational damage.

  Further, the unique digital identity verifier (signature) cryptographic encryption methods are not standard and require enforcement against fundamental privacy rights violations, secrecy of communications, and unauthorized or illegal use of personal information.

- **Data Broker Industry:** Data brokers or information brokers collect data and create profiles of individuals which may introduce discrimination risk and lead to harassment involving unsolicited contact based one's profile characteristics or personas. Compiling, aggregating, and selling data for marketing and other practices raises clear ethical concerns for privacy and discrimination based on race, age, and other data characteristics which may be accurate or inaccurate.

Automated Governance

Automated governance of digital identities (human or machine) relates to access and approvals rights and detection of permission discrepancies, including passwords - using business process workflows that are decentralized to manage and secure data with minimal error.

Automated governance must also protect human rights, ensuring consent, access, participation, dignity, and respect. Identity Governance and Administration (IGA) systems automate the provisioning, management, and administration of user identities and password rights today.

There is no standardized or verified national or international system for digital identity authentication and authorization compliance. There are, however, guidelines for industry best practices and innovation for surveilling user activities.

There are ethical implications today, which can lead to 1) deepening societal inequities, 2) jeopardizing data security, and 3) eroding privacy through new avenues of surveillance.

Currently, Identity Governance Access (IGA) frameworks and tools help somewhat with the management of the lifecycle of digital identities, as software platforms that control data access within an IT environment). These solutions help monitor compliance requirements and security objectives, but with minimal monetary fines and reprimands. This is a critical area for policy development and education that balances cyber threats and human privacy.

The Chartered Society of Forensic Sciences

The Chartered Society of Forensic Sciences, based in the UK, is the only international professional organization focused on global standards for blockchain data movement.

Blockchain forensics uses data analysis to monitor potential criminal activity on a blockchain – the ethical implication is whether this private data, often associated with crypto transactions, for example, can be exploited. Specifically, the metadata and smart contracts are accessible to internet service providers and law enforcement agents.

There is accelerated innovation related to new forensic software on computers, personal digital assistants (PDAs), and mobile devices. There is an increased demand for ethical standards provisions.

In both the UK and the US, Chartered Forensic Scientists focus on digital forensics to analyze forgery and data manipulation on blockchains. Although no consistent or standard regulations exist today, federal governments use existing statutes for compliance and ethics.

A note on risk management

Like any other technology infrastructure, digital identity systems are also subject to attacks. Hence, the design, development and deployment of such systems should include a systematic way to identify risks and design policies and technical requirements to mitigate such risks. While standard risk management approaches and models are well understood, domain-specific recommendations are also available to enable auditors to provide better inputs to such systems.

Provided below are some recommendations and observations related to the management of digital identity systems, surface areas of attacks and handling data governance to prevent the risk of data breaches. The last topic is almost always covered by data governance regulations available at the jurisdictional level.

US/GAO Key Audit Recommendations on Digital Identity

- Develop a comprehensive strategy for digital identity management. This strategy should include a clear vision of how digital identity will be used across governments and specific goals and objectives. It should also identify the roles and responsibilities of different agencies and stakeholders.
- Implement strong authentication and access control measures. This includes using multi-factor authentication, requiring users to provide passwords and codes from their phones to access sensitive systems and data.
- Protect personal identifiable information (PII). This includes encrypting PII when it is stored or transmitted and limiting access to PII to authorized personnel.
- Educate users about digital identity risks and best practices. This includes teaching users how to create strong passwords, spot phishing emails, and report security incidents.
- Monitor and evaluate the effectiveness of digital identity security measures. This includes conducting regular security assessments to identify and address vulnerabilities.
- With particular regard to the use of biometrics, the GAO has raised concerns about the security of biometrics because data can be spoofed or stolen and used to impersonate someone else. Accordingly, the GAO recommended US Agencies carefully consider biometrics' risks and benefits before implementing them for digital identity verification. In particular, the GAO recommended that US Agencies implement strong identity-proofing processes to verify the identity of individuals seeking access to government systems and data. These processes should include multiple authentication factors, such as passwords, security questions, and biometrics.

The Institute of Internal Auditors (IIA)

The Institute of Internal Auditors (IIA)[93] is an international professional association that provides guidance, education, and resources to internal auditors. The IIA guides digital identity in its Auditing Identity and Access Management Global Technology Audit Guide (GTAG).[94] The GTAG defines identity management (IDM) as "the set of processes and technologies used to establish and maintain the identities of individuals and systems and to control access to information and systems."

The GTAG identifies three key objectives of IDM:

- **Identity proofing:** The process of verifying the identity of an individual or system.
- **Authentication:** The process of verifying that an individual or system is who it claims to be.
- **Access control:** The process of granting or denying access to information or systems based on identity and authentication.

The GTAG recommends that internal auditors review the organization along the following aspects:

- Risk appetite for identity-related risks.
- IDM policies and procedures.
- IDM controls.
- IDM training and awareness programs.
- IDM incident response plan.
- Identity proofing processes to ensure that they are effective in verifying the identity of individuals and systems.
- Authentication processes to ensure that they are effective in verifying that individuals and systems are who they claim to be.

Information Systems Audit and Control Association (ISACA)

The Information Systems Audit and Control Association (ISACA) is an international professional association focused on information technology, assurance, security, and governance.

The ISACA *"Audit Program on Identity and Access Management"*[95] guides how to assess the effectiveness and efficiency of IAM processes and controls, identify gaps and weaknesses, and provide recommendations for improvement.

"The Importance of a National Digital Identity System" states that the creation of a national digital identity system (NIDS) would provide a centralized repository of identity information that can be used to verify the identity of individuals and organizations and improve the security and efficiency in a variety of ways, such as by reducing fraud, streamlining government services, and making it easier to do business online. However, there are several challenges to implementing an NIDS, such as ensuring the security of the system and protecting privacy.

"The state of digital trust 2023", an ISACA global research report, identified the following best practices:

- **Several factors can erode digital trust.** These include data breaches, security incidents, and privacy concerns.
- **Organizations can build digital trust by taking several steps.** These include implementing strong security measures, protecting privacy, and being transparent about their data practices.
- **There is a growing need for international cooperation on digital trust.** As the world becomes increasingly interconnected, having common standards and practices for digital trust is important.

CENTRALIZED VS. DECENTRALIZED MODELS

While centralized digital identity models still retain a centralized repository of data, decentralized models focus on users' control of their own data. Interoperability in either case should be a prerequisite ensures equal access to platforms and services, so as to minimize inequalities.

Digital identity models that utilize blockchain technology can verify data records transparently and immutably, and deploy security enhancing tools such as zero-knowledge proofs and hashing to make data anonymous, pseudonymous, and conditionally available only to authorized parties upon request. These tools embed privacy considerations around selective disclosure and requirements. Maintaining individual control over personal data can be a major step toward preventing breaches and their harmful consequences. The following considerations should be taken into account for each model:

- **Biometric Data:** Biometric data includes unique physical or behavioral characteristics of an individual, such as fingerprints, facial features, iris scans, voice patterns, and even behavioral traits like typing patterns or gait. Biometrics provide a highly secure and difficult-to-forge method of verifying identity.
- **Personal Information:** This includes basic personal details such as name, date of birth, gender, and contact information. These attributes are commonly used for identification and verification purposes.
- **Authentication Credentials:** Authentication credentials are the means by which individuals prove their identity when accessing digital services. This includes passwords, PINs, security questions, and more advanced methods like one-time passwords (OTP), security tokens, or biometric authentication.
- **Consent Management:** Consent management involves obtaining explicit permission from individuals to access their personal data and use it for specific purposes. It's a crucial component for ensuring data privacy and compliance with regulations like GDPR.
- **Blockchain and Distributed Ledger Technology:** Blockchain can be used to securely manage and verify digital identities. It provides a tamper-proof and decentralized way to store identity-related information, enhancing security and transparency.
- **Multi-Factor Authentication (MFA):** MFA combines multiple authentication methods to increase the security of access to digital services. This might involve something the user knows (password), something the user has (a physical token), and something the user is (biometric data).
- **Single Sign-On (SSO):** SSO allows users to access multiple services using a single set of login credentials. It improves user experience and reduces the need to remember multiple passwords.
- **Identity Providers (IdPs):** Identity providers are entities that manage and verify digital identities. They play a key role in authentication and authorization processes, often using standards like OAuth and OpenID Connect.
- **Privacy Controls:** Privacy controls enable individuals to manage the sharing and exposure of their personal information. This ensures that users have control over who can access their data and under what circumstances.

USE CASES

Private and public sector implementations of digital identity can greatly improve access to services, and thus improve levels of equality and well-being for all citizens.

ACCESS TO BANKING/FINANCE

Identity verification is one of the most critical components of banking and impacts most areas of banking including account opening, KYC, credit card applications, loan originations, high-risk transactions, account closures access to services, and various other banking products. The current state of identity verification methods is ad hoc and inconsistent in most cases, resulting in friction for customer experiences and reconciliation efforts for bank employees.

Digital identity, on the other hand, enables secure and frictionless customer experiences while integrating various lines of businesses cohesively into using a single source of verification for KYC. Digital identity has several use cases in banking, including:

- **Digital identity services:** Digital identity services can help banks improve risk management through streamlined know-your-customer (KYC) processes, better fraud management, and improved protection of customer data against cyber threats. It simplifies how individuals interact with new banking products and helps banks reap tangible results such as cost reduction, better risk governance, customer profiling, paperwork reduction, and improved data management.
- **KYC automation:** Businesses often need to verify the identity of customers during onboarding or registration processes. Verified digital identity solutions streamline this process by automating identity verification, reducing manual work, and improving compliance with KYC regulations. Digital identity can allow banks to authorize identities and verify transactions in real time while streamlining the necessary customer due diligence procedures by using open banking to fetch and verify customer information. This use case is critical for smaller financial institutions that typically have limited resources for compliance operations.
- **Transaction monitoring:** Transaction monitoring is a requirement that lets payment service providers (PSPs) detect unauthorized or fraudulent transactions by looking for anomalies in the data.
- **Financial management (FM) services:** Using open banking to aggregate financial information from different accounts and banks can simplify money management for consumers and businesses. FM services ranked high in Italy, Norway, the UK, and Spain – countries characterized by significant competition for the digital customer experience.
- **Financial Inclusion and Access to Banking Services:** Extending access to banking and financial services to underserved and unbanked populations by enabling them to establish a digital identity. Providing a foundation for individuals without traditional identification documents to participate in the formal financial system and access loans, savings accounts, and other financial products.
- **Fraud Prevention and Security:** Verified digital identity helps prevent identity theft, account takeovers, and fraudulent transactions. By verifying a user's identity through multi-factor authentication, biometrics, or other means, businesses can ensure that only authorized users gain access to sensitive information or perform critical actions. Verified digital identities can also improve the security of online banking, mobile payments, and online trading platforms. This reduces the risk of fraudulent activities and unauthorized access to financial accounts.

Digital identity can significantly improve efficiency in the private financial services industry in several ways. Private sector companies such as Visa, PayPal, and Mastercard are exploring various use cases as digital identity solutions could play a crucial role in enhancing security, convenience, and efficiency. Here are four use cases specifically relevant to private-sector companies:

Enhanced Cardholder Verification and Authentication

Visa, Mastercard, and other payment card companies can leverage digital identity to enhance cardholder verification methods. This includes using biometrics such as fingerprint or facial recognition to authenticate transactions, making payments more secure and convenient. Digital identity helps reduce instances of card fraud, as biometric data linked to a cardholder's account ensures that only authorized users can make transactions, protecting both the consumer and the financial institution.

Tokenization for Secure Online and Mobile Payments

Visa and Mastercard have introduced tokenization services that replace sensitive card information (e.g., card numbers) with unique tokens for online and mobile payments. Digital identity securely links these tokens to the cardholder, ensuring that only the legitimate cardholder can use these tokens for transactions. This protects against card-not-present fraud and enhances payment security in the digital realm.

Personalized User Experiences and Loyalty Programs

Digital identity data allows companies like Visa and Mastercard to gain insights into cardholders' spending behaviours and preferences. By analyzing this data, these companies can offer cardholders personalized promotions, discounts, and loyalty programs, enhancing their overall customer experience and incentivizing card usage.

Secure Mobile Payments and Digital Wallets

Facilitating secure and convenient mobile payments by enabling users to link their digital identity to their mobile devices. Enhancing the security of digital wallets and mobile payment apps through biometric authentication methods like fingerprint or facial recognition. One such use case is using a consumer's digital identity as a key for payment execution. This has already eroded the value of plastic cards by enabling the use of a consumer's digital identity as a key for payment execution. Another use case is the use of virtual cards, such as PayPal Key, which hides the real details associated with your payment account, providing an extra layer of protection against fraud and identity theft while you shop.

E-commerce

Online retailers can enhance user trust by implementing verified digital identity for customer accounts and transactions. This can help prevent fraud, reduce chargebacks, and provide a seamless shopping experience.

OTHER BASIC SERVICES

- **Healthcare and Telemedicine:** Verified digital identities can be used to securely access electronic health records, telemedicine services, and other healthcare-related platforms. This ensures that only authorized individuals, such as patients and healthcare providers, can access sensitive medical information.
- **Government Services:** Verified digital identities can simplify interactions with government agencies and services. Citizens can securely access and submit documents, apply for permits, pay taxes, and access public services online.
- **Travel and Hospitality:** Verified digital identities can expedite airport security processes, hotel check-ins, and car rentals. Travelers can use their digital identity to authenticate themselves and access various services quickly.
- **Education and e-Learning:** Online learning platforms can use verified digital identities to ensure the authenticity of students, prevent cheating, and protect intellectual property. This is especially important for online certification and degree programs.
- **Cybersecurity and Access Management:** Enterprises can enhance their cybersecurity posture by implementing verified digital identities for employee access to corporate networks, systems, and sensitive data. This reduces the risk of unauthorized access and data breaches.
- **Supply Chain and Logistics:** Verified digital identities can improve supply chain transparency and security by ensuring that authorized personnel access sensitive information and make critical supply chain decisions.
- **Digital Voting and Civic Engagement:** Verified digital identities can enable secure online voting and civic participation, making it easier for citizens to engage in the democratic process while preventing voter fraud.
- **Gig Economy and Peer-to-Peer Services:** Platforms in the gig economy can use verified digital identities to establish trust between service providers and customers, ensuring a safe and secure environment for transactions.

In summary, digital identity solutions are changing how financial institutions verify their consumers' identities, providing various advantages, including higher security, efficiency, and a better client experience. From adopting blockchain technology to using digital identity for inclusive growth and the evolution of business models, companies are finding new and innovative ways to leverage this technology to improve their customers' security, convenience, and efficiency.

RECOMMENDATIONS

While the scope and focus of this paper is not designed to put forward wide-ranging recommendations on digital identities, governance frameworks, and digital trust ecosystems, there are opportunities to enumerate specific recommendations because more jurisdictions are finding it necessary to implement a form of digital governance by introducing digital identities, linking services, and enabling an "update once" approach to data modification and exchange. If the ease and convenience of access to services are built around digital IDs, then it is necessary that the lifecycle of such identifiers can provide all the promised benefits.

Robust and sustainable digital trust ecosystems require high-quality digital IDs. In addition, technology designs, information technology architectures, and network protocols are some of the ways in which these governance requirements are translated into implementation details . It is also important to consider that technological innovations provide an acceptable compromise between what is possible and what is required by the regulations and laws. Digital IDs also function in cross-border transactions, thus bringing in more complexities and challenges among the various jurisdictions.

Below is a summary of the recommendations for governance authorities, system designers, implementors and operators of digital ecosystems, which include digital identities. These recommendations are not binding but provide guidelines to adopt and include in digital trust ecosystems.

- Design human-centric digital IDs aligned with the Principles of Digital ID
- Enable transparency to make systems explainable to the consumers
- Anticipate and design policies to mitigate the risks from harms
- Advocate for regulatory environments which provide protections from erosion of principles

An additional recommendation is to examine, evaluate and assess the emerging innovations in technology such as Generative AI, Large Language Models (LLMs), Synthetic Content Creation flows - all of which are capable of eroding the level of assurance of digital identities. The threats inherent in these technologies need to be thoroughly evaluated, and safeguards built into digital identity systems to prevent bypassing any existing protection mechanisms and guardrails.

Digital identities should be useful, fit for purpose, inclusive and secure . These are not new or novel requirements but must be in place to prevent the exploitation of data enabled by certain forms of digital identity. It is also necessary to be cognizant of the fact that popular messaging applications also enable the creation of portable digital identities, often bound to a combination of mobile phone numbers and mobile hardware. While such inexpensive and portable digital identities facilitate communication between individuals, there has not been extensive research on the security of the platforms enabling the creation of such digital identities, or the secure management of the same. It can be noted that individuals' activities using these platforms leave "breadcrumbs", or activity trackers, such that their personal information may not remain as private as expected or desired. Such digital identities, if found to be weak or weakly managed, can lead to data breaches, exploitation, and other harms.

CONCLUSION

A growing number of digital identifiers are issued, exchanged, and managed, with the intention of enabling better access to services for consumers. While digital identifier systems have the potential to impact consumers positively, there have been ongoing discussions about the possibility of harm originating from poorly designed systems. The worldwide standards for digital identity have a direct impact on the protection of human rights. This makes it uniquely significant that all the stakeholders focus on the necessary components of a digital identifier system to have a long-term impact. The growing number of secure, interoperable systems can unlock services such as financial inclusion, access to healthcare, and inclusion in other services. While the compliance requirements will evolve, it is necessary to be mindful of the pace of innovation and shifts in markets alongside changes in geopolitics. Bias or unfairness in the design criteria of digital identity and using and categorising personas can be inequitable - profiling or targeting people in discriminatory ways.

Whether intentional or not, such systemic bias has implications that may be difficult to identify, correct or equalize quickly or without debate once agreed upon.

Innovations in technology are essential to ensuring that the digital IDs being put into circulation align with the principles highlighted in this paper. The idea that digital IDs will be able to protect privacy, enable agency, and promote inclusion must be upheld and protected from being misused through poor design choices. The topic of privacy is enormous and an emerging field - and like the governance frameworks, regulations and technology enabling privacy, it is impossible to acquire a deep understanding of the topic. All the stakeholders in a digital trust ecosystem, including digital IDs, have the responsibility to examine the innovation, research and development to create guardrails against the possible misuse and abuse of the technology infrastructure powering digital IDs.

The standards-making work is necessary to create robust systems that ensure interoperability, scalability, compliance, and human-centricity. This is complemented by ethical compliance requirements built around principles and values which take into consideration the uniqueness of culture, such as language and social norms. Today, large digital identifier systems are being deployed as "Digital Public Infrastructure" (DPI), thus enabling more deployments to develop a shorter development cycle. These deployed systems should focus on consistent user experience, improved digital ecosystem governance frameworks, and sound approaches to managing personal data aligned with both legal requirements and security best practices.

International cooperation and harmonization are key. The long-term impact and consequences of digital identity systems should be carefully considered. Changes in technology, policies, and societal norms can affect how digital identities are used and interpreted over time. As for cultural sensitivity, digital identity systems should also respect cultural differences and avoid imposing a single standardized identity framework that might not resonate with all individuals, for the sake of preventing disparities and biased access to services. As for the role of government and corporate entities in managing or safeguarding digital identities in any form, the centralization of digital identity data can lead to concentrated power in the hands of governments and corporations. Ensuring checks and balances are in place to prevent abuse of this power is crucial.

Effective and secure digital infrastructures are key to moving beyond fragmented digital solutions toward broader digitization and accelerate the growth of a digital economy in a way that fosters inclusive social and economic development. As global initiatives continue to work toward access to digital identity for all, in support of the SDGs, individual governance and empowerment are at the center. While individuals can have multiple identifiers, it is the individuals themselves who matter. Safeguarding individuals' wellbeing through universal access to a digital identity that is effective and secure can greatly advance social and economic inclusion, for better outcomes.

ADDITIONAL READING

1. Blockchain for Digital Identity and Credentials | IBM. (n.d.). Retrieved September 23, 2023, from https://www.ibm.com/blockchain-identity
2. Tuchen, M. (n.d.). Council Post: How Digital Identity Can 'Amazonify' The Financial Services Industry. Forbes. Retrieved September 23, 2023, from https://www.forbes.com/sites/forbestechcouncil/2022/08/05/how-digital-identity-can-amazonify-the-financial-services-industry/
3. Importance of Digital Identity in US Banking Revolution. (2022, April 1). DIRO Original Document Verification Technology. https://diro.io/us-digital-banking-revolution-importance-of-digital-identity/
4. The top 5 open banking use cases for European bankers. (n.d.). Retrieved September 23, 2023, from https://tink.com/blog/open-banking/top-uses-cases-survey-report/
5. RISK ANALYTICS FOR FRAUD PREVENTION: TOP USE CASES IN BANKING, https://www.onespan.com/sites/default/files/2020-10/OneSpan-WhitePaper-A4-Risk-Analytics-Fraud-Prevention_20200930_1.pdf
6. UN Roadmap for Digital Cooperation (June 2020) https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf (last accessed on Nov 7, 2023)
7. The Principles of SSI v3 published by the Sovrin Foundation https://sovrin.org/principles-of-ssi/ (last accessed on Nov 7, 2023)
8. Towards Better Ends by John Phillips on behalf of Sezoo https://www.sezoo.digital/resources/towards-better-ends/ (last accessed on Nov 7, 2023)
9. Digital Wallet Design for Guardianship by John Phillips on behalf of Sezoo https://www.sezoo.digital/resources/digital-wallet-design-for-guardianship/ (last accessed on Nov 7, 2023)
10. Digital ID At Last by David Birch https://www.linkedin.com/pulse/digital-identity-last-its-from-banks-david-birch-w9wbe/ (last accessed on Nov 7, 2023)
11. Principles of Dynamic Data Economy (DDE) v1.0 https://static1.squarespace.com/static/5ead4c8660689c348c80958e/t/62f288b25f9c364d7945e6eb/1660061875006/HCF+DDE+Principles+v1.0.0.pdf (last accessed on Nov 7, 2023)
12. The Domains of Identity: A Framework for Understanding Identity Systems in Contemporary Society by Kaliya Young
13. Standards-Based Digital Credentials: Flavors Explained: An Independent Review and Analysis https://consulting.identitywoman.net/standards-based-digital-credentials-flavors-explained (last accessed on Nov 7, 2023)

SECTION X

SUSTAINABILITY

EXECUTIVE SUMMARY

This report explores the benefits of blockchain technology and digital assets to address the world's most pressing and complex issues that call for prioritizing sustainability. It builds upon prior work focused on the decarbonization of upstream value chain emissions within the digital asset space, and now covers downstream value chain emissions measurement and finance for mitigation. Having addressed the negative impacts of blockchain on the environment with a prior report, now this working group explores positive contributions that blockchain can have to advance sustainability.

Blockchain technology can be deployed with promising outcomes in cases where there are sensors capturing data on climate factors (e.g., emissions, waste and pollution, weather patterns), as a means to measure, monitor, and evaluate the impact of climate mitigation activities. Blockchain technology can also integrate with IoT along digitized supply chains, to measure emissions, record data on responsible business practices, and improve outcomes. To place these solutions into context, this report takes a step back to assess the broader conditions that led to the imminent sustainability concerns the world faces today, and how new models of activity can break harmful cycles, where innovations in blockchian technology can emerge.

Fundamentally, this report discusses the ways our current economic systems have contributed to the situation at hand, and alternative economic models to address these issues including regenerative finance (ReFi), sustainable supply chains, and domestic resource mobilization. Covering real-world examples and use cases of blockchain and digital assets being deployed toward promising solutions, this report also serves as a guide on how these innovations can help companies and organizations meet increasing regulatory requirements for sustainability and make their own transition plans more realistic and effective.

OVERVIEW: IMPORTANCE OF SUSTAINABILITY

Increasing Focus on Sustainability

Sustainability has been an increasing focus area across sectors, impacting the decisions of business leaders, politicians, and all stakeholders concerned with the future of humanity. The UN Sustainable Development Goals (SDGs) call for collective and meaningful action by 2030, mobilizing not billions but trillions in funding from public and private sectors to address the world's most pressing needs. The Paris Agreement, a legally binding international treaty on climate change, also calls for climate change mitigation, adaptation, and financing, to limit the rise of average global temperatures to below 2°C above pre-industrial levels, and to take measures to remain below 1.5°C. Article 6 of the Paris Agreement acknowledges the role of voluntary cooperation across countries, to reach nationally determined emission reduction goals.

Institutions and corporations are realizing that disregarding sustainability has become a material financial risk that can significantly impact bottom lines, while customers are increasingly driving demand for sustainable products and services driven by increasing awareness of the risks for our society and generations to come. As for small and medium enterprises, many are either actively developing sustainability-focused innovations, or being pushed into adopting more sustainable practices through large corporates embedding their sustainability objectives and compliance requirements into their contracts with vendors and suppliers. Ultimately, regulators and standards setters are actively producing requirements for all stakeholders to adhere to.

Urgency of the problem: it's environmental and social

Climate change affects all of us, and it's expected to disproportionately impact marginalized and vulnerable populations with less economic resources, mainly in the Global South. This is why the "E" and "S" in ESG are closely related. With rising temperatures, extreme weather events, and oceans rising due to , an imbalance where snowfall no longer matches ice lost from melting ice caps, the effects on the future of humanity can be major. . These issues can bring major global concerns and aggravate the complex global issues we are already facing today (e.g., migration crisis, hunger crisis, geopolitical conflict, increasing wealth gap perpetuated with rising food and energy prices and inflation).

Researchers have established and quantified nine planetary boundaries, as conditions within which humanity can adequately operate and maintain its well-being. Crossing any of these boundaries is expected to cause irreversible changes, with major consequences for humanity. As of today, six of the nine limits have been breached (climate change, biosphere integrity through biodiversity loss and extinction of species, freshwater change, land system change, biogeochemical flows, and introduction of novel entities), one is close to being breached (ocean acidification), and only two may remain well within the constraints (atmospheric aerosol loading, which has not been

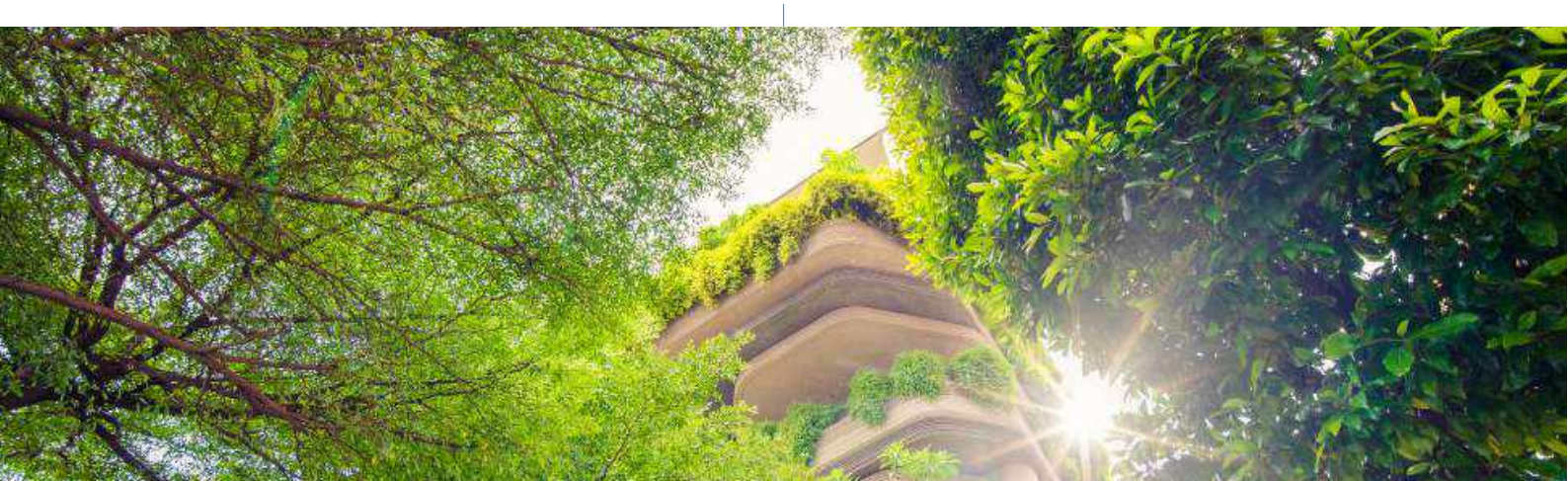


Figure 1: The nine planetary boundaries and their status

quantified, and ozone depletion).[96]

1. CLIMATE CHANGE

2. CHANGE IN BIOSPHERE INTEGRITY (BIODIVERSITY LOSS AND SPECIES EXTINCTION)

3. STRATOSPHERIC OZONE DEPLETION

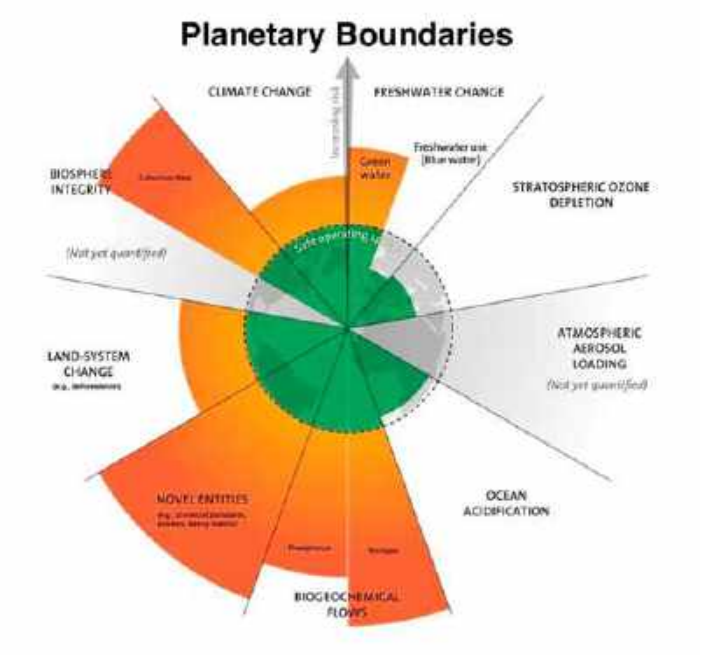
4. OCEAN ACIDIFICATION

5. BIOGEOCHEMICAL FLOWS (PHOSPHORUS AND NITROGEN CYCLES)

6. LAND-SYSTEM CHANGE (FOR EXAMPLE DEFORESTATION)

7. FRESHWATER USE

8. ATMOSPHERIC AEROSOL LOADING (MICROSCOPIC PARTICLES IN THE ATMOSPHERE THAT AFFECT CLIMATE AND LIVING ORGANISMS)



9. INTRODUCTION OF NOVEL ENTITIES

The expected melting of the **110 tons** of ice from the Greenland ice cap alone can cause oceans to rise by **10.6 inches** (27 cm), affecting **600 million** people living in coastal areas and costing trillions of dollars. With other factors at play, the ocean could rise up to **30.7 inches** (78cm), and with further ice caps melting (Himalayas, Alps, Antarctic) and continued global emissions, the rise in oceans can be multi-meter and affect billions of people with floods.[97]

Financing for sustainability

Urgent and effective climate action can have a dramatic impact in reducing potential future damage. Limiting rising temperatures by **1.5 degrees C**, as set out by the Paris Agreement, can bring down the total global cost of climate change by hundreds of trillions of dollars, cutting expected losses by more than half. Leading institutions have developed frameworks for sustainable investments, such as the UN supported Principles for Responsible Investment (PRI), which have gained significant traction since being introduced in 2005, having been adopted by many of the world's largest institutional investors such as BlackRock (signatory since 2008).

Over the last decade, there has been an explosion of funding going into sustainability-related investments, largely with a focus on climate finance. In 2023 alone, global sustainable funds attracted **$23.6 billion** and **$13.7 billion** in Q2 and Q3 respectively.[98] By now, the World Bank has issued USD $18 billion worth of green bonds since the first issuance in 2008, as a form of debt financing for sustainability initiatives to provide positive impact to societies.[99] According to the Reserve Bank of Australia, **$13 billion** in green bonds were issued in the first half of 2023 which is a record amount to date in the Australian green bond market.[100] Yet there is a wide spectrum of approaches, and the specific objectives have yet to be standardized, starting with a commonly agreed upon perception of the issues and the standardization of the data to measure, monitor, and evaluate impact.

The United Nations Framework Convention on Climate Change (UNFCCC) refers to climate finance as "finance that aims at reducing emissions, and enhancing sinks of greenhouse gases and aims at reducing vulnerability of, and maintaining and increasing the resilience of, human and ecological systems to negative climate change impacts,[101]" and the Climate Policy Initiative has produced a database of climate finance that provides guiding parameters and definitions for the private sector.[102]

While there is no concrete definition of climate finance as of yet, there is still a need for harmonized and actionable guidance on climate action. Common standards for project financing, reporting, and monitoring impact can greatly mitigate concerns of ineffective climate action, misaligned initiatives, and greenwashing. For instance, developed nations have reported financing projects to the UN and other international organizations as contributing toward national climate finance goals, when the true impacts toward sustainability have been minimal or even detrimental.[103]

Innovations in blockchain technology can advance sustainability:

The transparency and trust offered by blockchain technology can improve accountability, while the community-driven action that peer-to-peer relationships enable can propose new governance models (the "G" of ESG) to drive environmental and social impact. These models can facilitate a harmonized approach to climate action at scale, while democratized ownership can enable collective action starting from individuals and small entities. Digital transformation is fundamental to coordinate urgent global action addressing pressing issues like biodiversity loss, disaster displacement, energy grid deficiencies, and social and geopolitical strife. Blockchain and digital assets can greatly improve mitigation and adaptation efforts through greater integrity of data, real-time visibility on carbon emissions and sequestration, and cost-effective transactions.

These innovations can ultimately support a more sustainable and inclusive system of capital flows through built on a transparent accounting system, and are even forming the backbone of a regenerative economy that not only reduces emissions but deploys resources toward conservation and restoration of ecosystems, for a better future for humanity and the planet. The movement to mitigate climate change could create more opportunities that may increase chances for achieving higher rates of equality, especially for the most vulnerable populations. Restoration of environmental, social, and financial stability can bring a holistic series of benefits alongside monetary gains. Therefore, the movement to mitigate climate change is integrated with improving equality.

STATUS QUO & PROBLEMS

Existing business models, which traditionally have not been built with sustainability as a priority, are not being effective enough to address the sustainability concerns the world is facing today, many of which originate from numerous externalities of those business models themselves.

Currently, many sustainability-linked risks that affect businesses' bottom lines are not envisioned in their central market strategies or main profit and cost items, such that they become increasingly substantial yet still non-market costs. Many major global corporations suffered major losses and reputational damage when customers, activists, and interested stakeholders brought light to unsustainable practices that came from a narrow focus on their pure market strategy to maximize short term profits (e.g., Nike for hiring labor from sweatshops, Nestle for purchasing palm oil from plantations that depleted natural ecosystems, oil companies for not responding adequately to oil spills). Sustainability strategies within those very business models, without innovations that seriously rethink current processes, may only get us so far.

Extractive approach to commerce

Currently, the global economy has valued and paid for products in their extracted format, at the end of the supply chain, fostering a system of perpetual extraction of natural resources, largely in the Global South, production, consumption, and waste. With this economic model, most of the economic benefits favor large corporates in the Global North, while the impacts and risks sit in the Global South where capital chases low-cost labor and less expensive resources.

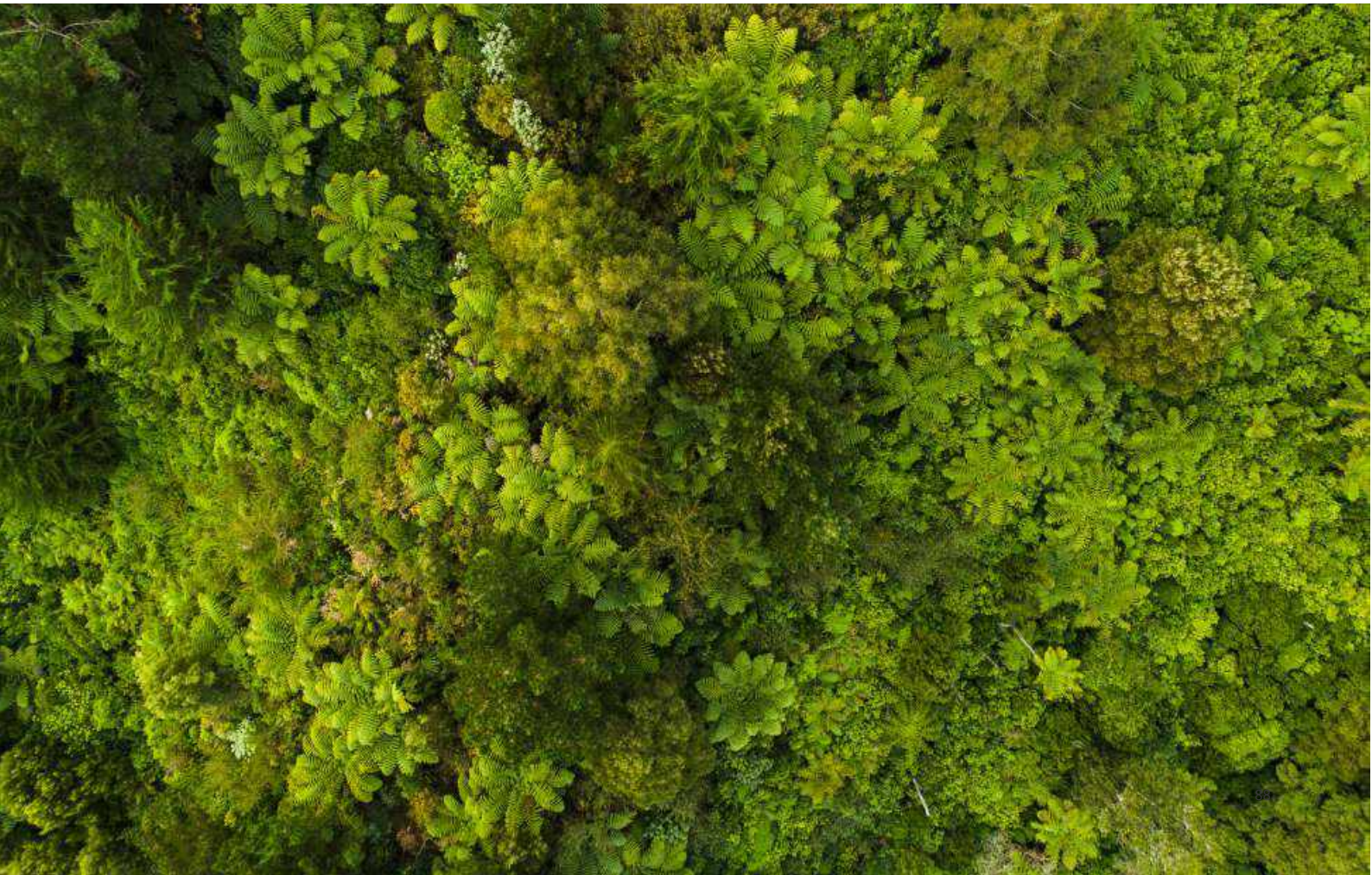
This extractive cycle, where the conservation of natural resources is not recognized as a central part of this (until we feel the effects as today), also shapes the commercial dynamics between the Global North, where the largest markets lie, and the Global South, where most of the resources are based to meet the commercial demands of the former. This view can be narrowly focused on short term profits, with several blind spots with respect to the importance of sustainability, not only to remain competitive, but to even allow the possibility of business practices to continue.

Figure 2: Extractive economic systems

Climate stress models, for instance, repeatedly underestimate the economic impacts of climate change, and there has been widespread criticism of climate stress tests (e.g., costs of carbon emissions can be estimated to be much higher than the US federally accepted estimate of **$51** per ton – affecting climate policy and outcomes).[104] Carbon Tracker research, for instance, recognizes that scenario modeling is important for financial institutions to assess the impact of climate change scenarios. However, many climate scenario models for financial services significantly underestimate the risk of climate change. As a result, budgets to deal with carbon impacts may be smaller than anticipated and necessary, while the risks may unfold more quickly than expected, leading to uncertainty and lack of predictability.[105] With this underappreciation of climate risks, underestimating the effects to the Global North in particular gives false confidence of the ability to 'raise the drawbridge' when the preceding issues hit with full impact.

Not enough funding for the Global South

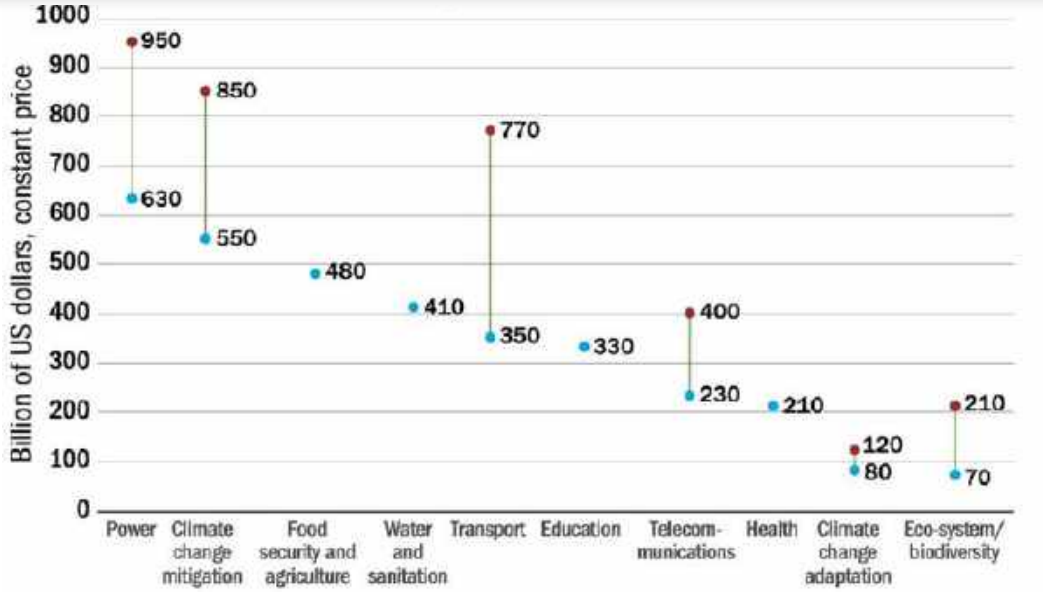
There are currently a number of blockages to funding in the Global South, which espeically impacts climate mitigation funding. While traditional finance has benefitted the extractive commercial approach, it has underinvested in the Global South where investments are most needed. In some cases, traditional capital flows absorbed and intermediated the resources needed to be mobilized domestically in the Global South, though both illicit fund flows and legal fund flows that avoided weak local institutions (e.g., sovereign funds, concealed flows). Often funds from the Global North to invest or pay for resources in the Global South go through financial centers in the Global North that take a cut (e.g., transaction costs, intermediaries), such that a portion of the funds directed toward the Global South get absorbed back to the Global North, and domestic markets in the Global South remain under-resourced.



As wealth created from extractive activities in the Global South often flows into financial centers in developed markets, even if a portion of resources are reinvested back into the Global South, they are often done so in hard currencies (e.g., dollars, pounds, euros), with high interest rates because of the high risk perception from hard currency lending to resource-dependent countries. Funding is also deemed to be in insufficient amounts because of perceived high risks and low credit ratings, which are at risk of being accentuated by the physical impacts of climate change in the Global South.

The United Nations Conference on Trade and Development (UNCTAD), which focuses on trade and development, estimates that in order to meet the SDGs by the designated time in 2030, SDG-relevant sectors in developing countries need total annual investments between $3.3 trillion and $4.5 trillion. There is an estimated financing gap of around $2.5 trillion per year, which represents the difference between existing funding and funding needed to be invested in the Global South.[106] Specifically climate finance needs of emerging & developing countries (ex-China) have been estimated at over **$2 trillion** per year through 2030, **90%** of which would have to be provided by private sources.[107] This is half or more of the **$4-5 trillion** per year needed globally.

Figure 3: Investment gap for developing countries in key SDG Sectors (Source: International Finance Corporation using UNCTAD estimates)



Challenges with risk mitigation

This perspective also factors into the approach in terms of mandating specific requirements that may not be feasible at a local level, or may push potential investors away from collaborative solutions that rethink the current systems, perpetuating portfolio biases toward the Global North. Traditional approaches to risk management in the financial sector have also created insufficient financial flows to address this issue. Investors already under-allocate toward the Global South, perpetuating the status quo (e.g., credit ratings, asset allocation model driven investments oriented around emerging market definitions or market cap weighting) and leading to persistent underinvestment. Moreover, the impact of the current debt crisis in many Global South countries post-Covid shows the likelihood of the underinvestment to continue or get worse.[108]

With respect to financial stability in the context of climate change, the Financial Stability Board found that cross-border lending may amplify climate-related risks in recipient countries, where the crystallization of physical risks may prompt abrupt and largescale withdrawals of foreign investments. In these developing economies, already existing macroeconomic vulnerabilities such as rapid exchange depreciation and wider capital outflows may aggravate the effects. On the other hand, contrary to many traditional risk management approaches, this research considers that for lending countries in the Global North, cross-border bank lending may diversify climate-related risks and would likely not led to material risk concentrations.[109] Yet a drawbridge approach for short term financing needs would also make sucking capital flows more likely in cases where the Global North would need needs capital most.

Moreover, risk mitigation measures have been pushing the burden of risk mitigation from the Global North to the Global South. For instance, passing policies preventing certain extractive activities due to their environmental impact in the Global South, without providing the funding for entities conducting those activities to make necessary changes, ultimately pushes the burden to the Global South. A policy that prevents cutting down all of a country's trees may force its stakeholders to adopt alternative activities with less economic rewards. This would merely recreate the same dynamics and resulting problems, and the status quo continues without an alternative workable model. Moreover, without global action and convenings requiring sustainability commitments, the mindset of regulators and decision makers has been to leave problems outside their borders, which can perpetuate a disposability mindset seeking low-cost labor or finding interchangeable parts elsewhere.

Imbalanced power dynamics

Despite having valuable natural resources, weak institutions and corruption in the Global South, coupled with weak domestic financial markets, form a detrimental combination that compounds the current cycle. As the Global South experiences value extraction toward the Global North, a disparate distribution of power dynamics and social design ensue. These power dynamics pose a number of challenges for the Global South's positioning in global commercial relationships, perpetuating current issues.

Weak institutions in many Global South countries may also repel financial resources and prevent them from being recycled domestically to address climate mitigation and adaptation. Weak institutions allow for counterfeiting and other forms of fraud within supply chains. The fact that payments from the import to export side get channeled back through the financial sector back to the Global North, and that a portion of those capital flows get lent back to the Global South in higher interest rates, often becoming more of a burden than a source of support, can also be attributed to weak domestic institutions.

There is a two-way problem with customers of financial institutions not currently being able to access data and its provenance within supply chains, and therefore not being able to provide climate financing resources to incentivize target-setting and progress reporting down the supply chains. Legal and commercial barriers to information sharing may interrupt data flow and sever the path for financial resources to travel down to the Global South. These data flow challenges create further problems, where what is happening on the ground (e.g., with primary commodities) and how information makes its way to people may not fully reflect itself in the price of final products. Therefore prices would not reflect whether a product is sustainably sourced and produced across the entire supply chain – a key aspect that consumers are willing to pay for. These legal data sharing limits create barriers that technological innovation alone will not solve.

Inefficient supply chains

The inherent imbalance of power from the extractive approach to commerce has also impacted resource allocation in supply chain agreements between the Global North and the Global South. Moreover, supply chains cast light on the imbalance of power and disparities, highlighting the contrasts between the Global North and the Global South. Moreover, lack of resilience makes supply chains vulnerable to disruption. The bottlenecks and delays experienced during the Covid pandemic are indicative of these issues, where lack of traceability aggravated supply chain concerns.

In the food sector alone, one-third of all food produced globally for human consumption is either wasted or lost – amounting to 1.3 billion annual tons, and worth $1 trillion. This wasted food could feed 2 billion people, more than two times the number of undernourished individuals, and the food wasted in developed nations amounts to the entire net yearly food production in sub-Saharan Africa. Moreover, if all wasted food were a country, it would be the third largest carbon emitter after the United States and China. While 40% of these losses occur after harvest and processing in developing nations, for industrialized nations over 40% of food waste occurs at retail and consumer stages of the supply chain.[110]

For the United States, nearly 40% of all food is wasted, amounting to **119 billion pounds** of food each year, which equates to 130 billion meals and over **$408 billion in food** thrown away. of food are wasted, equating to 130 billion meals and over thrown away.[111]

The problems with supply chain waste are vast and complex, and they can be boiled down to a few key issues:

- **Wasted resources:** The production and distribution of goods often results in the waste of raw materials, energy, and water.
- **Pollution:** Manufacturing and transportation can also generate air, water, and land pollution.
- **Deforestation:** The clearing of forests to make way for agriculture and other development is a major source of greenhouse gas emissions.
- **Social and economic inequality:** The extraction and processing of resources often takes place in developing countries, where workers are often paid low wages and work in dangerous conditions.
- **Greenhouse gas emissions:** If food waste ends up in landfill it produces methane, a potent greenhouse gas. The global food system emits around one-third of total greenhouse gas emissions, and food waste causes approximately half of this.[112]

These problems are exacerbated by the fact that the global supply chain is highly complex, with goods often traveling thousands of miles before they reach consumers. This makes it difficult to track and manage waste, and it also makes it difficult to hold companies accountable for their environmental and social impacts.

The combination of consumer willingness to pay more for sustainable products, and lack of verification of supply chain practices, leaves open the possibility of greenwashing by consumer-facing companies. It also produces an outcome where more of the value from the sustainability premium remains in the Global North and doesn't reach all the way down the supply chain to producers of primary inputs.

Environmental costs are also transmitted through supply chains to the most vulnerable communities. Companies are facing up to US$120 billion in costs from environmental risks in their supply chains within the next 5 years, and on average, supply chain GHG emissions are estimated to be 11.4 times as high as operational emissions.[113] Broader than supply chains, value chain emissions, which include activities to provide value to customers throughout the customer journey, are often 90% of an organization's entire carbon footprint.[114]

Current financing is either insufficient or has the wrong lens – hence most supply chain financing goes to areas we don't need. While supply chain finance overall amounts to **$7.3 trillion**, most of it is in the form of traditional letters of credit, guarantees, etc. which are generally not the type of supply chain financing of most relevance for these purposes. Finally, rather than keeping financial resources in the Global South, they are often exported to low-return savings accounts in financial centers in the Global North and returned with much higher return expectations.

Undervalued Natural Capital

Much of the problem facing our current economic model originates in our relationship with what we value in our natural capital. The value of natural capital is currently not able to be rewarded except through the traditional extractive model, and while voluntary carbon markets (VCM) have emerged as a vehicle to channel funding toward conservation and natural capital, they have faced major existential credibility issues because of the challenges in providing evidence to funders on actual impact, and payments going in the other direction.

Existing models of economic growth value resources in their extracted form, while undervaluing the benefits provided by natural capital. Now that the issue of climate change and nature loss is impacting the world at large, the response is a mandate to turn back to the inputs to the problem. Yet failing to recognize the costs required to do so (e.g., valuing natural capital assets, compensating for loss and damage, social and developmental costs accrued throughout extractive model duration) creates hesitancy or barriers to transparency and traceability. Early implementations of voluntary carbon markets, for instance, have collapsed due to undervaluing natural assets and lack of transparency.

Extractive models have separated the stock and flow of resources, undervaluing the stock of natural capital assets which have a particularly high concentration in the Global South (e.g., land under the stewardship of indigenous people). Monetary value is assigned only to the flow of extracted resources and commodities. Because the economic rewards for this value are only realized when resources are extracted or harvested, there is a pressure to do so because of the need to address high rates of poverty in many of these regions.

While **50%** the global GDP depends on natural capital assets (natural resources and biodiversity that can serve as raw materials for production),[115] the sources of essentially all supply chains are renewable and non-renewable natural resources. The global supply chain turns that natural capital, often from the Global South, into GDP that is quantified reflected economically toward the end of the supply chain. Undervaluing or not valuing natural capital assets at all, further perpetuates existing inequalities, shortage of financial resources in the Global South, and the risk that they'd lose access to financial resources in the future when climate risks materialize.

A "resource curse" occurs where countries that have an abundance of natural resources experience less economic growth, less democratic governance, and overall lower development outcomes relative to countries with fewer natural resources. The impact of these commercial dynamics on export sectors stunts domestic economic growth, paired with additional troubles in other sources of financial resources, such as voluntary carbon markets, which despite being designed to invest in natural capital and support the Global South, have experience major credibility issues and lack of trust. This contributes to others crises driven by volatility of natural capital assets in the current model. Ultimately, exporting countries have difficulty developing other parts of their economies beyond the exporting their natural resources and feeding into the extractive commercial model and its implications.

SOLUTIONS: RE-EVALUATE OUR ECONOMIC MODELS

It's hard to conceive true improvements in the common good (economic, social conditions, climate, overall justice especially for the poorest among us) - without considering innovation in support of wellbeing. Emerging tech like blockchain can be a conduit to facilitate these better relationships, through inclusive models of exchange and win-win situations that benefit all.

The fact that six of the nine planetary boundaries have now been transgressed, as stated earlier, calls for an urgent, and simultaneous implementation of multiple solutions that bring drastic changes to existing commercial models. Solutions lie in rethinking our current economic models, providing financial resources that are widely shared and not eroded by transaction costs from intermediaries, or diverted to those parties who control the opaque channels used in data, capital, and resource flows.

Role of blockchain based solutions

Blockchain, as an immutable ledger that is visible to all cannot be changed by any network participant, provides transparency and data integrity into sustainability initiatives. It can be used to create a more transparent, efficient, and secure supply chains. This can help to reduce costs and improve efficiency, as well as identify and address potential problems, anticipating before they occur and taking action accordingly. Transparency can also address counterfeiting and other forms of fraud, while making it easier to track and trace goods.

Finally, blockchain technology can be used to reduce the environmental impact of activities across their supply chains, while tracking and measuring progress towards sustainability goals. For instance, tokenization of assets can help to track the provenance of goods and materials, ensuring and proving that they are sourced from sustainable and ethical suppliers. This can reduce the risk of fraud and ensure that companies are meeting their sustainability commitments. It can also reduce instances of greenwashing.

The assumptions going into climate stress tests also need to be more realistic for both qualitative and quantitative aspects of climate change scenarios, and better anticipate risk drivers, impacts, and areas of uncertainty. Blockchain and data integrity can also have a role in developing more realistic assumpitons, and ultimately more credible net zero and transition plans.

Need a new model of generative relationships

We need to attract investments toward building traceable and transparent systems designed to overcome climate risks through an equitable and reciprocal relationship between the Global North and the Global South, rather than an extractive, hands-off approach. Data can draw light to the problems, helping companies monitor and measure impacts, and evaluate effective solutions. For instance, many blockchains offer climate friendly ledgers that run on energy-efficient proof-of-stake mechanisms, such that climate mitigation solutions built on their platforms can provide useful data records for the use cases at hand, in a way that produces minimal carbon emissions.

When Ethereum transitioned from a proof-of-work validation mechanism to a proof-of-stake mechanism, all of the applications built on it dramatically reduced emissions, and it was reported that the entire Ethereum blockchain eliminated over 99% of its carbon footprint overnight. In additon to low-carbon proof-of-stake models, many blockchains have further allocated additional resources to carbon offsets. In the case of Ethereum, additional funds toward carbon offsets are meant to reverse the environmental footprint of past operations during the period when it relied on proof-of-work. In the case of Algorand, an intentional decision to commit additional funds to carbon offsets are meant to create a climate-positive footprint that goes beyond its basic carbon neutral operations in order to have a positive environmental impact. Ripple has also committed to net zero by 2030, having taken proactive measures committing funds toward carbon offsets that make net zero more likely by 2028. Ripple's XRP Ledger has positioned itself as a public blockchain that is among the fastest, low energy, and carbon neutral.

These endeavors, which originate at the governance level of blockchain platforms, trickle down across all activities and applications built on them and can create a culture of environmental consciousness that shows how it is possible to embrace innovation while having a positive impact on the planet. Blockchain technology can deliver the most promising solutions with respect to sustainability when there's a dual system of data integrity and payment flows to rebuild the stock of natural capital assets, which can also compensate for loss and damage embedded in extractive economic activities. Valuing natural capital assets by assigning funds to their preservation is an important source of climate change mitigation.

Overall, generative relationships between producers and buyers requires an upgraded approach during a time of climate crisis, adjusting relationships between the Global North and the Global South to bring climate resilience. Meeting both company and consumer demand requires a more equal distribution of wealth. Given that impacts of climate risks are felt more in the Global South where most of the resources originate, we need to work together to find ways that innovative solutions including blockchain technology can better ensure critical production lines, compensation structures, and incentives are better distributed to players in the system.

We need to shift away from short term goals for company bottom lines, which can be problematic for both the Global South and the Global North. Economic development in less wealthy nations is convenient also for wealthier nations through better products, trade relationships, opportunities, and peace through commerce, and also better alignment and coordinated progress toward global goals such as the Paris Agreement, SDGs, etc. Rather, by building toward longer term generative relationships that maintain ecological balance and harmony between human civilization (e.g., societies & economies) and the planet, the "pie" of opportunity can expand toward more win-win situations.

These conditions can support the longer term health and distribution of supply chains, where blockchain solutions can support a model where value can travel alongside data. We need to ensure security and proper data management. This way we can effectively push toward sustainability and net zero, and even net positive operations. Blockchain technology has the potential to build models that create inclusion, benefiting all parties involved.

Figure 4: Regenerative, Sustainable, and Circular Economy

Inclusive finance

There is a need for financing models where benefits can reach inclusive levels, where blockchain has the potential to contribute. Simply put, it will not be possible to flow finance into emerging and developing countries in the volumes and with the speed required through current mechanisms alone. There will need to be three major and interrelated changes where blockchain has demonstrated potential to ensure fund flows toward sustainable outcomes at scale.

Inclusive finance can be sustained through mechanisms that support regenerative financial models, sustainable supply chains, and domestic resource mobilization in the Global South.

1) REGENERATIVE FINANCE (REFI) FOR NATURAL CAPITAL - ReFi often considered an offshoot out of decentralized finance (DeFi, proposes a new model of a financial system focused on inclusivity, transparency, and mutually beneficial commercial relationships. The benefits of these commercial exchanges should expand to both society and the environment, by integrating financial practices with sustainability. This involves responsibility relative to society and environment, and ultimately aims to create net positive effects through regeneration of natural resources.

ReFi proposes an alternative to traditionally extractive commercial relationships, especially between the Global North and the Global South, such that value and capital flows can allow economic benefits to remain in the Global South where much of the resources we rely on originate. Emerging technologies such as blockchain are fundamental to ensure the data transparency and reliable accounting systems on which ReFi is designed to operate.

A regenerative economy supported by ReFi consists in an economic system that goes beyond merely generating financial returns, but focuses on ensuring and restoring social well-being, economic prosperity, and environmental well-being through restoration, renewal, and sustainability of resources. The circular economy, with a holistic view of value, is fundamental to a regenerative economy, which lies in contrast to traditional economic models based on extraction, consumption, and waste.

Restoration of environmental, social, and financial stability bring a holistic series of benefits alongside monetary gains. Therefore, the movement to mitigate climate change is integrated with improving equality. ReFi recognizes the value of resources in the Global South and ensures that its population is adequately remunerated, as opposed to traditional systems where value is placed on production and end products after extraction of raw materials from the Global South.

ReFi has found acceptance in the blockchain/digital assets ecosystem, with models of decentralized finance (DeFi) leveraging transparency, low-cost transactions, and global liquidity pools with immediate settlement to facilitate access to financial services for unbanked and underbanked communities. The openly available data on the blockchain ensures a level of transparency that can allow a granular level of impact measurement, monitoring, and evaluation that is also secure and immutable (e.g., dMRV).

Tokenization allows representations of value to be exchanged on a blockchain, benefitting from low cost transactions with immediate/close to immediate settlement. This can revolutionize carbon markets, renewable energy accounting systems, and access to alternative financial services for underserved communities (e.g., DeFi).

2) SUPPLY CHAIN FINANCING –

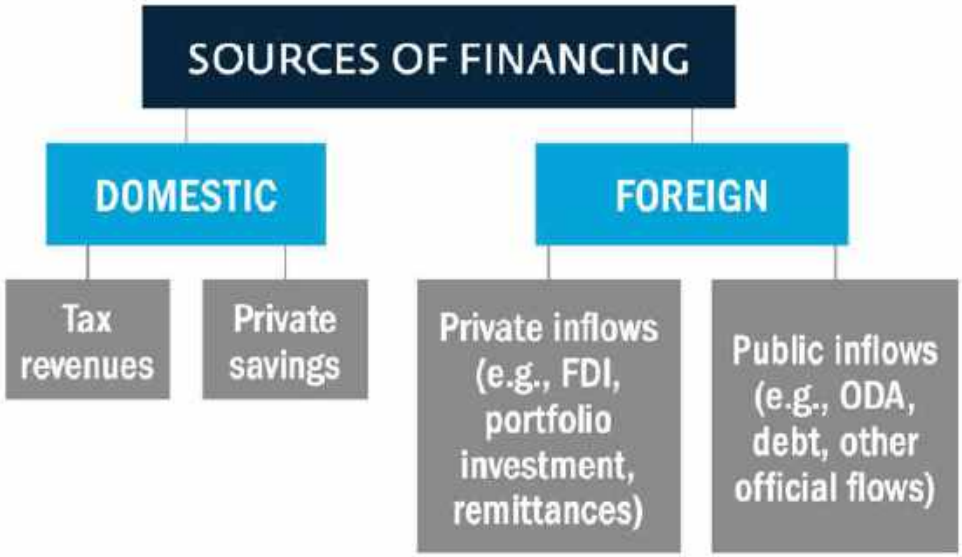
Supply chains are a major economic link between the Global North and Global South by connecting the pathway of value transfer across all points of exchange, where equal or unequal relationships can be perpetuated through the dynamics of capital flows in exchange for goods. Supply chain finance is connected to other financial activities, making it critical to advance sustainable practices with respect to voluntary carbon markets, compliance markets, certifications, consumer finance, and all areas of market activities.

If supply chains can support increasing resource flows toward the Global South and equitable governance, they can become a systemic disruption point with ripple effects throughout the ecosystem. Therefore revising current models of economic activity supported by supply chains can be key to driving equitable solutions.
Blockchain technology can both facilitate access to global markets through peer-to-peer, inclusive, and low-cost transactions, while also recording data on sustainable practices across supply chains. Ensuring trust and access to data can support companies' claims to end consumers, who want more sustainable products and are willing to pay more for them, regarding their labor practices, emissions generated from production and transportation of goods, and other indicators about the sustainability of their supply chains.[116]

Embedding supply chain finance with technology for resource distribution toward climate resilience is key to ensure trust and effectiveness. Blockchain technology can bring light to gaps along the supply chain where there may be difficulties meeting sustainability goals, especially upstream closer to the points of extraction of raw materials where there can be little visibility, so as to facilitate a targeted course of action.

The volume of supply chain finance enabled by blockchain has been estimated at $16 billion in 2021, with a yearly growth rate projected at 32%. This would account for only 0.2% of the total supply chain finance market today, indicating a significant opportunity.[117]

Figure 5: Potential sources of financing for the SDGs (Source: World Bank)



SHORT TERM SOLUTIONS - In the short term, even within the existing status quo, supply chains can be made more sustainable. As long as the traditional financing model continues, an alternative model to channel funding to the Global South consists in financing linked to sustainability performance at the base of the supply chain.

Although the problems facing our current economic model originate in the relationship of what we value in our natural capital, even within the status quo, supply chains can be made more sustainable. As long as the traditional financing model continues, another model to channel funding to the Global South is financing linked to sustainability performance at the base of the supply chain, supporting in-setting beyond merely off-setting.

Several applications of blockchain have focused on improving supply chain traceability, and there is a significant opportunity, largely untapped, in using data from traceability initiatives to provide supply chain financing where pricing is linked to sustainability practices. Often, these types of supply chain finance require transparency of supply chains, which may not be accessible for commercial, legal, or regulatory reasons, leading to gaps in the ability to trace sustainable practices back to the primary inputs. Despite lacking more robust data from across an entire supply chain, sustainability-linked supply chain finance focuses on sourcing sustainability certified inputs and the sustainability practices of Tier 1 suppliers. This works primarily by providing faster access to payment for suppliers who can meet sustainable sourcing requirements and who engage in sustainable operational practices.

Yet the benefits from this approach are likely to be more captured by Tier 1 suppliers who deliver final products, due to the lower capacity to validate and differentiate between different degrees of sustainability from sourced inputs from stages of the supply chain closer to the raw materials. If the objectives are improving supply chain practices and channeling funding towards suppliers of primary inputs who are more likely to be located in the Global South, then current practices are likely to only have limited efficacy.

EMERGING TECH-ENABLED SOLUTIONS -

On the other hand, pairing supply chain financing with supply chain traceability, including blockchain-based approaches within sustainability certifications, can enable greater transparency of data to validate sustainable practices among primary input suppliers, ultimately justifying financial incentives to reach them. This can have positive impacts even if sustainability-linked financing isn't extended all the way down the supply chain. Intermediate buyers, who may face working capital pressure from buying more expensive inputs, can be incentivized with better terms and alleviation of some working capital pressure through supply chain financing supported by the end buyer.

End buyers may also have an incentive to participate in this system for a number of reasons, including mitigating their supply chain due diligence regulatory risk, minimizing greenwashing risk related to failures within certification programs, or they may have stronger pricing power when they are able to demonstrate full traceability behind their sustainability claims. By alleviating working capital concerns of intermediate suppliers, greater traceability for sustainably-sourced inputs may enable suppliers to command a higher prices than they get using certifications that rely on manual processes. Intermediate suppliers may also have a similar rationale for partnering with financial institutions to offer sustainability-linked supply chain financing to their suppliers. If they do so, then the direct financial incentives of sustainability linked financing are provided more directly through their supply chain. In turn, this means less of the financial incentive for suppliers is reliant on the ability to get better prices for fully-traceable verification of sustainable sourcing practices.

Moreover, sustainable supply chain financing supports in-setting, which goes beyond merely offsetting and can be interpreted as a means for companies and organizations to buy themselves time as they devise ways to reduce emissions from their core operations. When early iterations of voluntary carbon markets have collapsed as a means for off-setting, many companies and organizations turned to the approach of reducing and avoiding emissions in their very operations through in-setting across the supply chain. In-setting becomes even more important as a long-term strategy that companies should aim toward, as they integrate sustainable practices into the core of their business models.

A generalized future model for sustainable supply chain financing:

Exchange of information for financing through a supply chain is portrayed below. This example uses a model where a financial institution offers sustainability-linked loans to the buyer and its suppliers, whose credit risk for the supply chain finance are more closely related to the credit risk of the buyer, adjusted by a margin related to their achievement of climate-related targets.[118]

In this process, the likely steps that will take place will be:

1. Financial institution works with the buyer on the basis of the buyer's credit risk and ESG-related risks to identify specific KPIs to measure financially material improvements from their suppliers that would mitigate specific climate-related supply chain risks.

2. Financial institution would make available a financing facility for the buyer priced on the basis of its current ESG risk, with discounts linked to supply chain and buyer's operational improvements to lower its climate risk exposure.

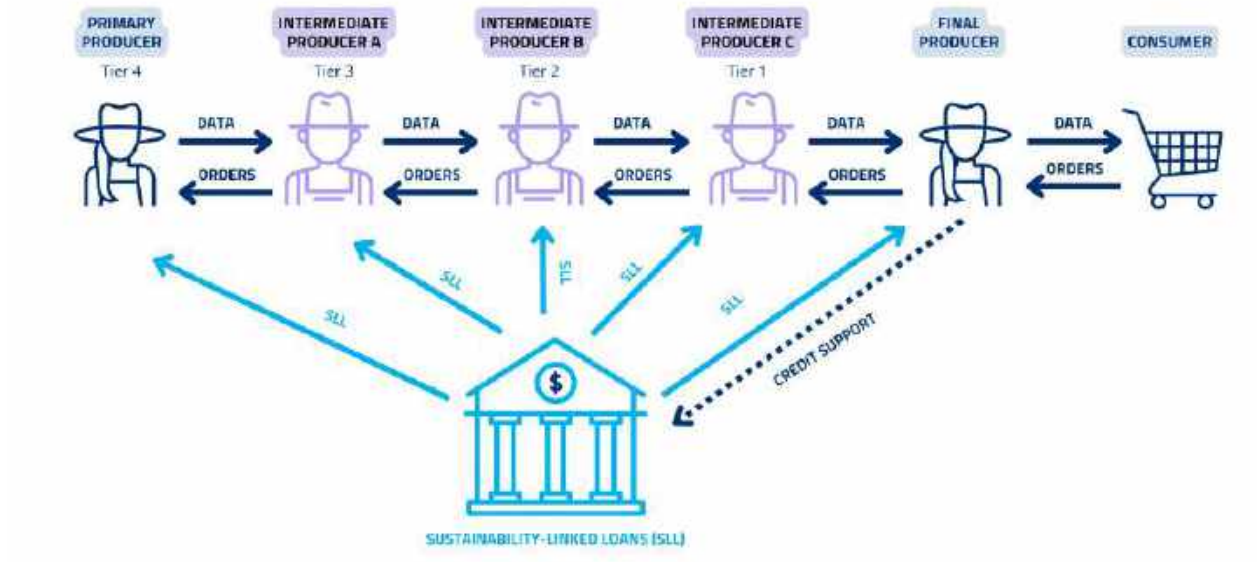
3. Buyer provides opportunity for its suppliers (as far as it can have visibility) to work with the same financial institution, for financing used to improve its cash flow related to the sales to the buyer (or Tier 1 direct suppliers, or Tier 2 or 3 indirect suppliers, respectively) conditioned on sharing the data with intermediate producers and the end buyer.

4. Suppliers work with the financial institution to develop KPIs specific to their business related to the overall KPIs relevant to the buyer to receive sustainability-linked supply chain finance, to receive access to financing at all / on terms that they may be unable to get on their own.

5. Suppliers and financial institution pass data to end buyer for their disclosures & audit / external assurance related to progress on their climate-related targets.

The GDF ESG working group was focused on upstream value chain emissions within the digital asset space. This working group covers downstream value chain emissions measurement and finance for mitigation.

Figure 6: Sustainability/ESG linked supply chain finance



As a flip side of the coin of environmental concerns being translated through supply chains, positive environmental impacts are also translated through supply chains. Supply chain financing linked to sustainability not only benefits input providers with financial incentives, but it is also beneficial for corporates. Blue chip companies like Google, L'Oréal, Walmart, Braskem and Toyota are among 150+ major buyers to call for transparency and action from suppliers to tackle sustainability risks. Cutting emissions also cuts costs. Suppliers in a Carbon Disclosure Project (CDP) survey that undertook activities that cut emissions by 619 million tC02e were able to save US$33.7 billion in the process.[119]

Reverse factoring, for instance, provides financing from the buyer to the supplier (where the interest rate charged could be linked to climate-related outcomes). Then Dynamic Discounting is set up to reward faster payments from the buyer to the seller with lower prices paid, and presumably there could be some step-up of higher prices paid conditional on achievement of climate-related KPIs where an automatic formula can adjusts prices depending on pre-agreed events. If the general use case is with speed of payment to supplier, there may be an easy addition of ESG or climate targets as well.[120] Buyer-led supply chain financing, where most sustainability-related financing is likely to occur, currently provides amounts to approximately $500 billion annually ($400 billion in reverse factoring, growing at a yearly rate of 15-20%, and $100 billion in dynamic discounting, growing at a yearly rate of 25-30%.

3) DOMESTIC RESOURCE MOBILIZATION -

One of the main ways blockchain has been used in lower income countries has been to address institutional weakness. In relation to climate finance in these developing economies, every dollar that stays in local markets is one fewer dollar that needs to flow from developed markets. Keeping resources generated by supply chains working within the Global South enhances domestic resource mobilization for sustainable investments that disintermediate offshore / financial centers.

For example, one of the exceptions to the norm of the status quo stated above is Malaysia, which proactively worked to build a domestic capital market as a government priority following its contrarian response to the Asian Financial Crisis in 1998.[121] In the years since, it has become a high-middle income country and aspires to become a high-income country between 2024 and 2028. The strength and development of its local capital market can be directly attributed to its greater domestic level of control over its natural resources.

Domestic resource mobilization is key for ensuring revenues to the Global South remain in the Global South. This is an area where other blockchain applications related to climate finance come into play if they can help mobilize resources at a local level that would otherwise be recycled through developed market financial centers and would then need to be attracted back to the Global South as "climate finance" if not retained domestically.

The cycle will be most effective if funds from developed market buyers and financial institutions are channeled into ReFi and projects connected to primary products within the global supply chain to meet buyers' regulatory compliance needs, in ways that result in financing that ends up staying in lower income countries. The only way to change the status quo perpetuated by extractive low cost labor and export for domestic resources in lower income countries is for financial flows to acknowledge value of natural capital assets. Sustainability-oriented supply chain finance can cut out the round trip of capital back to the Global North, while blockchain technology can validate the use of funds and increase transparency. This can help retain funds in lower income nations, which therefore can dramatically cut the costs of climate finance in the Global South.

This process of local retention of capital to strengthen domestic capital markets, which can be largely driven by supply chain financing, is a private sector complement to national carbon credit sales under the Paris Agreement. Both financing models bring financial resources within the Global South, which is particularly important as voluntary carbon markets face and related challenges. This is also complementary to the extent that national flows may support conservation and protection, while sustainable supply chain finance should provide additional financial incentives towards practices that put less pressure on depletion of natural capital.

USE CASES

Blockchain technology can provide a verified data layer, adding security, and trust to a wide range of sustainability-focused initiatives. It can integrate with other existing and emerging technologies to optimize processes through trusted accounting systems and efficient, cost-effective infrastructure for transactions. For instance, blockchain technology can record data captured by the Internet of Things in an immutable manner, and it can provide a reliable and decentralized source of data going into AI algorithms. A wide range of activities that already contribute to sustainability can rely on trusted data on a blockchain, alongside financial solutions provided by digital assets. For instance, unmanned aerial vehicles (UAVs) for asset inspections and maintenance, or other uses of drones from food delivery to emergency response, can be optimized. As for decarbonization, initiatives such as Carbon Capture, Use and Storage (CCUS),[122] where carbon emissions can be captured from the environment to produce materials such as concrete, plastics, and biofuels,[123] can also benefit from a trusted ledger across the lifecycle of inputs and materials. While many of these use cases have yet to be deployed at scale, solutions are already being built and tested.

- Creating new financial flows to support conservation and regeneration of natural capital
- Adding traceability to supply chains and linking them to supply chain finance from developed markets
- Developing sustainable capital markets in lower income nations to absorb and recycle funds from primary production

Below is a stakeholder mapping to identify Web2 and Web3 use cases, helping to identify market gaps that blockchain applications could fill. These solutions play a role to fit into developing Transition Plans for corporates and financial institutions – either as examples to follow or tools companies can use.

Web 2 models being optimized with blockchain

TRADITIONAL FINANCE & FINTECH:
Traditional finance use cases embracing sustainability include initiatives toward tokenization of green assets, sustainable finance, and green bonds. This intersection of finance transformation, digital finance, and ESG can take many forms. These use cases to demonstrate inclusive and green finance are already being deployed to overcome challenges that exist today. Green finance is increasingly embracing digital and tokenized bonds and loans. Blockchain could then also be used for verification that the green objectives claimed have been achieved. Data transparency within green finance and FinTech, including coding of assets against taxonomies including digital asset value chain emissions, can be of
great value.

Because of the costs involved in issuing bonds in general many smaller companies are effectively excluded from the green bond market. Such high transaction costs and minimum in-vestment size may make it especially difficult for emerging markets to support a thriving green bond market. Many companies will most likely struggle to find projects that are large enough to warrant issuing green bonds. This may lead to a lack of green projects for investors to invest in. Issuing tokenized bonds using blockchain is less costly, and more widespread adoption of the technology would perhaps open up the market for more projects to be financed in this way. Tokenization can also help issuers reach new investor bases by allowing companies to list their green bond on a cryptocurrency exchange in addition to a regular listing on a traditional marketplace.

Moreover, some of the problems associated with green bonds, such as greenwashing and lack of on-going verification may be tackled through regulatory and policy initiatives. However, it is possible, perhaps necessary, to use technology as a to enable and accelerate such efforts. While (blockchain) technology will not in and of itself help create consensus what constitutes a green activity and the criteria that should be used to measure such activities, it can be used to operationalise these definitions and goals. Using blockchain for issuing green financial products will also streamline and simplify the process. In addition to such efficiency gains, tokenization and smart contracts may also be used to increase transparency and to demonstrate alignment with regulatory developments for sustainable finance.

These products can also allow retail banking customers to participate in the green economy. A few examples of blockchain-based green bonds are below:

Green Bonds	SoBond is a platform for issuing digital bonds on a blockchain with a "Proof of Climate Awareness" feature that incentivizes participating nodes to improve their envoronmental footprint. SoBond was developed by Sweden's SEB and Credit Agricole CIB, and it can be applied for green or sustainability-linked bonds, where blockchain technology both makes climate finance more accessible. The European Investment Bank has for instance issued its first digital bond using the platform (Climate Awareness Bond – June 2023 – digital green bond on a blockchain platform).[124]
Evercity	Evercity has also launched a platform for green bond origination using blockchain.
Bank for International Settlements (BIS)	BIS developed Project Genesis 1.0, as a prototype for digital platforms for green bond tokenization.[125] This has moved to complete phase 2.0 involving HKMA, who want to issue green bonds.[126]
Hong Kong's SAR	Hong Kong's SAR Government **HK$800 million** offering is the first tokenized green bond issued by a government globally.[127]
Green Assets Wallet	Green Assets Wallet aims to scale the market for green investments that are credible, validated, and trusted, especially in emerging markets. Blockchain technology validates green investment claims and also provides immutable validation of impacts.
Fintech Players	Major fintech players like PayPal are prioritizing environmental sustainability initiatives at PayPal, aligning the company's net-zero objectives with their work in blockchain, cryptocurrency, and digital currencies.

SUPPLY CHAIN SOLUTIONS:

BNP Paribas CIB

BNP Paribas CIB[128] has developed a solution for traceable and green supply chain finance, which can incentivize data collection. Collection, validation and management of data are needed for supply chain due diligence & deforestation validation (e.g., palm oil, beef, wood coffee, cocoa, soya, rubber, and downstream products (furniture, leather, chocolate, charcoal, tires, printed paper) plus other commodities like maize and rubber, livestock other than beef, and waste & plastics).

The Forest Stewardship Council (FSC) International

The Forest Stewardship Council (FSC) International is integrating blockchain technology to enhance traceability and verification for products within the forestry sector. With the FSC Blockchain, FSC is establishing an immutable and verified ledger of trade transactions of wood and wood products (with volumes, species, and fundamental point-of-trade data), ensuring that their sources are sustainably managed and supporting FSC-certified companies with demonstrating compliance with regulatory requirements. The forthcoming version of the FSC blockchain platform is anticipated to enhance its analytical capabilities, providing insights such as trading partner analysis, origin verification, and broader sustainability metrics, such as supply chain efficiency and carbon footprints.[129]

DECARBONIZATION:
Mitigating the release of carbon into the atmosphere is the single most important factor to stop climate change; especially as the world generates 51B tons of greenhouse gases per year. Carbon markets can benefit from blockchain technology through interoperable global marketplaces, price discovery for offset quality, and emissions tracking across supply chains.

• Demia (formerly Digital MRV)	Solving the lack of trust in carbon and sustainability markets through an ecosystem of organizations developing standards and guidance for new digital infrastructure. Pilots in Copiulemu and Molina reflected to targets toward Paris Agreement goals in Chile and Canada.
TerGo	Provides solutions for individuals and companies to reduce their emissions, connecting them to carbon markets to purchase offsets and also providing a carbon calculator to measure and monitor their impact. Its mobile app can quantify and monetize sustainable actions, rewarding users for good behavior. With blockchain-based data management, Tergo is helping companies and their supply chains automatically track employee transportation emissions and supply chain emissions.
Zumo	Deploying blockchain technology to democratize access to sustainable finance for all. It offers an enterprise-focused digital-asset-as-a-service platform and a direct-to-consumer solution to help companies across sectors integrate solutions in digital assets sustainably.
EY OpsChain ESG	Offers a platform for trusted emissions and carbon credit traceability.
Hyphen Earth	Dedicated to institutionalizing and de-risking natural capital assets to improve certainty of environmental claims and value of carbon credits. It tracks greenhouse gas concentrations, fluxes, and observations from global to regional sources.

PUBLIC SECTOR CIRCULAR ECONOMY INITIATIVES:
Waste management and the circular economy through data collection can be great tools to create effective action. Blockchain technology is also being used for better reporting and accountability on the use of resources, and increasing efficiency in public services such as education. Other initiatives are integrating sustainability into national planning, with a focus on applying blockchain technology for various models aimed at achieving a circular economy.

RECYCLING:
Project TRACKCYCLE and RecycleGo are advancing a circular economy for recycling by embedding blockchain technology into the advanced recycling value chain, with the aim of providing a fully traceable and accurately labelled record of recycled materials, from the waste sourcing up to the use of recycled materials in new production streams.

Web3 native models

PARTNERSHIPS:
Consistent with peer to peer and decentralized governance concepts, sustainability initiatives in the Web3 ecosystem are gathering forces toward collaborative solutions. This is fundamental to deploy the technology under common standards, and interoperable platforms to allow for scaled solutions.

Blockchain x Climate (BxC)

BxC is an activist-to-industry network of global stakeholders working together to define and agree on common principles, shared understanding, and narratives to govern climate-related blockchain efforts. The goal is to design tangible and meaningful cross-chain and cross-industry initiatives and solutions to address climate change. It is largely a response to prior limited actions and siloed efforts in the climate space, which have contributed to a lack of trust. With a consolidated perspective, it is more feasible to work on real solutions, and create opportunities through collective actions.

Ethereum Climate Partnership

Ethereum Climate Partnership is a collaborative initiative to offset the Ethereum ecosystem's emissions prior to its transiton to proof-of-stake.

ReFi DAO

ReFi DAO is a decentralized autonomous organization that gathers players aroun d the world to share knkowledge and collaborate on regenerative finance developments.

NET ZERO & TRANSITION PLANS FROM WEB3 PLAYERS:
These plans can take several forms, depending on the focus areas of Web3 players across industries.

Ripple	In addition to having deployed a net zero plan by 2028 and deployed significant investments into carbon markets, Ripple has built a climate friendly Ripple Ledger on which further Web3 solutions can be deployed. Its acquisitions into market infrastructure can also be deployed for carbon markets. For instance, Ripple's acquisition of Metaco as a custody solution can allow users to custody tokenized carbon credits.
Zumo	In addition to having implemented its own net zero strategy, Zumo's Oxygen solution is being deployed to support companies transitioning to net zero. Oxygen allows companies to align their digital asset activities with ESG principles, calculating the electricity consumption associated with crypto activity and providing a solution for the procurement of renewable electricity to match this.
Algorand	Algorand has developed a carbon-positive footprint by running a carbon neutral platform that, in addition, funds further climate action.
Ethereum	Ethereum has reduced over 99% of its emissions by transitioning from proof-of-work to proof-of-stake.
Polygon	Polygon runs a carbon neutral platform, with the broader goal of driving the Web3 ecosystem to become carbon negative, having purchased additional carbon credits and supported overall sustainability initiatives as described in its Green Manifesto.

MARKETPLACES & INFRASTRUCTURE FOR BLOCKCHAIN-BASED CARBON MARKETS:
Web3 technology is being deployed to bring trust for carbon credits. Tokenizing natural capital with a social and ecological impact often includes the in support of indigenous land stewards.

Regen Network	Offers a blockchain-based fintech solution for ecological claims and data, at the intersection of remote sensors and blockchain technology to monitor ecological data. The platform offers tokenized carbon credits, a public ecological accounting system, and a registry where land stewards can sell directly to buyers globally.
Toucan Procol	Provides the digital infrastructure for tokenized carbon credits to operate.
Blockchain Laboratories	Provides a Web3 Software-as-a-Service infrastructure to support blockchain technology and digital assets solutions with a tripple bottom line. This is a tokenization platform for sustainability-minded projects including carbon markets.
LOA Labs	LOA Labs is an integrated product and marketing studio for Web3, focused on advancing use cases of blokchain with a positive impact, such as tokenizing social and ecological impact.
Thallo	Developed a blockchain-based infrastructure to revolutionize and democratize the process of buying, selling, and trading carbon offsets for individuals and businesses.
Reneum	Decentralized marketplace that aims to catalyze the energy transition through tokenized renewable energy credits on a platform accessible for businesses and individuals to offset emissions.
KlimaDAO	KlimaDAO built a carbon-backed digital token, with each token backed by a ton of verified tokenized carbon reduction or removal.
NFT Marketplaces	NFT marketplaces are also deploying funds into conservation in partnership with wildlife organizations and other ecological foundations. Revenue from NFT sales is deployed to supporting conservation, recycling activities, and biodiversity protection. ConservatioNFT and Plastiks are examples.
Powerledger	Deployed blockchain technology to streamline operations of decentralized renewable energy systems, enabling tracking, tracing, and trading of renewable energy.

SUPPLY CHAIN SOLUTIONS:

Triangle Digital	Triangle Digital uses blockchain for supply chain-related sustainability-linked loans [130]
Hedera	Hedera entered into a partnership with Guardian, in order to further credible carbon markets and other supply chains.[131] The aim is to enabe carbon accounting and tokenization for brands through blockchian networks to understand their carbon impact across the supply chain. In addition, they aim to support brands offering additional carbon reduction measures to achieve net neutrality and move towards carbon net positivity. They also leverage the technology to bring credibility and transparency across all activities and transactions. They also facilitate carbon reduction through the new online marketplace, powered by atma.io
HBAR Foundation	HBAR Foundation also partnered with FSCO, connecting to the Mastercard network.[132] They offer a payment trigger functionality that Continuity provides, which is a core component of FSCOs product offering on the Hedera network – the tokenization and financialization of Real-World Assets (RWAs) and events throughout the agricultural supply chain. As items move across locations, payments must be released only when their pre-approved conditions are met. For instance, if 250 2.5m x 6m shipping containers are received instead of 500 2.5m x 6m, the payment should not go through. If conditions are met, they should. Here, payment triggers combined with Internet-of-Things (IoT) devices automate this process, greatly improving efficiency. Historically, supply chain management has been opaque. By leveraging Hedera, FSCO also brings unprecedented transparency, providing rich data to financiers who need to calculate their credit-risk assessments.

HUMANITARIAN AID:

United Nations High Commissioner for Refugees (UNHCR)	One of the most recent and useful applications of blockchain to support sustainable finance initiatives for vulnerable populations is a first-of-its-kind integrated blockchain payment solution powered by the Stellar network and launched by United Nations High Commissioner for Refugees (UNHCR). Deployed in 2022 in a pilot phase designed for Ukraine, this payment solution is meant to be adapted in the future for worldwide adoption. It utilizes Circle Internet Financial's USD Coin (USDC), a stablecoin equal to one US Dollar in value, to disburse funds directly into recipients' digital wallets, which are downloadable onto smartphones, Recipients can safely hold their funds within Ukraine, and cross borders if needed, without having to carry cash.[133]
Algorand Foundation	Algorand Foundation has deployed its Kokua Wallet for humanitarian aid. Its HesabPay solution in Afghanistan also enables digital payments and relief funding with digital wallets that hold digital assets.

REGULATORY DEVELOPMENTS & VOLUNTARY INITIATIVES

With the view of meeting the Paris Agreement, regulation focused on environmental and social impacts is a key a driver of transition plans affecting non-blockchain native companies and organizations, which may consider blockchain solutions to facilitate data validation and transparency for reporting, as well as blockchain-native entities that would be subject to the same rules. Financial institutions face regulations about their sustainable finance claims, stress tests about their climate-related financial risks, disclosure requirements about climate, nature and other ESG risks. In addition, their customers also face regulatory requirements on climate-related disclosures and their sustainability practices, including requirements around supply chain due diligence and anti-deforestation requirements for primary inputs.

There has been a huge increase in regulations around sustainable finance and many of them relate to climate change. In this context, the European Union and several member states within the EU have been among the most aggressive in mandating specific due diligence requirements relating to supply chains and commodities whose production frequently leads to deforestation. Examples of regulatory developments include:

- In the blockchain and digital assets ecosystem, the comprehensive EU regulatory framework with Markets in Crypto-Assets Regulation (MiCA) has also set sustainability requirements.
- The EU's Corporate Sustainability Reporting Directive (CSRD) requires companies to report on the impact of their activities on the environment an dsociety, including audits of the reported information.
- The "Green New Deal" in the United States, reintroduced in 2021, calls for public policy to address climate change while achieving other social aims like job creation, economic growth, and reducing economic inequality, toward secure and sustainable future growth.
- The EU Taxonomy, which is fundamental to create alignment and trust in definitions around sustainability.
- The EU Green Bond Standard (GBS) was adopted on 5 October 2023, and is a voluntary standard that issuers may use to "label" their bond as green. The standard uses the criteria of the Taxonomy to determine if bonds are to be considered green
- The International Sustainability Standards Board (ISSB), an independent private sector entity that develops and approves IFRS Sustainability Disclosure Standards (IFRS SDS), provides a global baseline for sustainability disclosures that jurisdiction-specific reporting requirements may refer to and mandate.

.

Taxonomy-alignment could potentially be calculated automatically based on input data provided by the companies seeking alignment and the technical screening standards of the Taxonomy itself. Due to its highly technical nature, the Taxonomy should lend itself to coding. If a green bond is meant to finance a project developing new housing for instance, a smart contract could contain criteria for the materials to be used, and the way the materials have been transported to the building site. The information needed to determine whether the criteria have been met could (ideally) be collected via sensors in the physical world, or through manual recording and input. The energy efficiency of the finished building could be measured and recorded on a DLT database and made instantly available to the investors. If the issuer fails to deliver on agreed-upon metrics, such as achieving a specific Taxonomy-alignment percentage, this could trigger the smart contract to automatically execute a corresponding action, such as higher interest payments to the investors.

International organizations such as UN international energy agencies also play a role mobilizing efforts to create alignment, foster collaboration, define metrics and gaps, and calling to major stakeholders to action. Alongside international organizations, several voluntary disclosure bodies have also set standards to advance climate action. To make transition plans more effective, education is needed on the assumptions underpinning the models and their limitations, such as the AIGCC open letter to Asian banks,[134] the Exeter University / IFoA report,[135] which cite Carbon Tracker research and others.

Stronger stakeholder expectations for emissions disclosures, target and reporting on progress towards targets will make traceability a more important issue. Blockchain has both an opportunity and a responsibility to play a role in this process. First, it has the responsibility of improving its own emissions reporting, for its operations as well as relating to its financed and facilitated emissions, as addressed in the GBBC Digital Finance Guidance on ESG Reporting for Digital Assets.[136] Second, it has the opportunity of supporting better traceability and information integrity for operations across all sectors of economic activity, such as real economy supply chains.

In addition to regulatory requirements, standards setters and voluntary initiatives like the Science-Based Targets Initiative (SBTi) have been set up to provide frameworks for companies and financial institutions. Their framework provides a way for these entities to have emissions reduction and Net Zero claims validated in relation to their level of ambition compared to what is required to meet Paris Agreement targets or to limit warming to 1.5° C. Other voluntary frameworks such as the International Capital Market Association (ICMA) Green Bond Principles and the Climate Bonds Standard and Certification Scheme have also gained acceptance in the space, highlighting the importance of data to monitor and measure impact.

Within the crypto and digital asset sector as well, similar voluntary guidance exists for disclosing emissions based on the methodology published by the Crypto Carbon Ratings Institute (CCRI) and South Pole.[137] The sustainable finance digital assets working group at Global Digital Finance (now GBBC Digital Finance) compiled guidance for digital asset companies to set climate targets incorporating guidance for technology and finance sectors to include a wider range of value chains.

These requirements are designed to ensure that claims made about sustainability and climate change mitigation are accurate and not misleading, and that the intent of the regulations cannot be circumvented by outsourcing responsibilities to those who are not subject to the requirements.

Supply Chains

This topic is important in the context of many climate (emissions) risks being buried in supply chains and currently not visible, and that regulations (e.g., European Deforestation Regulation, EU Supply Chain Due Diligence Directive, etc.) are making this a topic of focus.

Beyond the scope of whether the targets meet the required level of ambition, there have also been issues in measurement of progress towards these targets. For climate targets in particular, the ability of companies to measure emissions in their value chains has been one of the weak spots in terms of validating whether targets have been met.

Currently, most regulations for financial institutions in particular either do not require value chain emissions (in the case of financed emissions) or allow for the use of proxy data for value chain emissions data (for example in the IFRS Climate Disclosure Standard S2 which is based on the Greenhouse Gas Protocol).

Greenhouse Gas (GHG) Protocol has also produced standards, guidance, tools, and training for businesses and government organizations to measure and manage emissions, including calculation tools for emissions. Updates to the GHG Protocol are likely to include clearer guidance for use of estimated proxy data.

Other regulatory requirements and voluntary disclosure standards like the European Sustainability Reporting Standard (ESRS) and Partnership for Carbon Accounting Financials (PCAF) increase the requirements for value chain and financed emissions over time beyond what is currently possible for most companies to comply with.

Many supply chain risks go down to the level of primary inputs, where either destruction, conservation or regeneration of natural capital assets will be important information for final producers / consumers, and information isn't currently easy to get from one end of the supply chain to another, and one of the barriers is financing for those within the supply chain to collect information and invest in improving their practices to meet buyers' expectations.

For example, the recently enacted European Sustainability Reporting Standards (Annex 1, Section 5.2, Paragraph 71) is for now allowing estimation and proxy for Scope 3 emissions in a reporting entity's value chain, which is likely to be tightened over time to require more data collection from within supply chains (there are stronger requirements for Scope 3 emissions disclosures for financial institutions who sign up to the Partnership for Carbon Accounting Financials (PCAF):

> "With reference to policies, actions and targets, the undertaking's reporting shall include upstream and/or downstream value chain information to the extent that those policies, actions and targets involve actors in the value chain. With reference to metrics, in many cases, in particular for environmental matters for which proxies are available, the undertaking may be able to comply with the reporting requirements without collecting data from the actors in its upstream and downstream value chain, especially from SMEs, for example, when calculating the undertaking's GHG Scope 3 emissions."

TRANSITION PLANS

Impact measurement is needed to make transition plans more realistic. We need to produce a trail of evidence, especially to make transition plans realistic. Blockchain provides the data and traceability to do this. This will also contribute to increasing trust across companies and organizations making claims of transitioning to Net Zero, and it will attract additional investments.

The connection between climate finance and companies making credible transition plans is quite direct. Important elements of creating a credible transition plan include a roadmap with actions needed, a capital allocation plan, governance for implementation of a transition strategy, independent monitoring, and progress reporting to show steps towards reaching interim targets.[138]

For many sectors where transition plans are especially relevant (e.g., high-emitting sectors), half or more of today's emissions are located in their upstream or downstream supply chains. Apart from a few sectors like transportation, shipping, and power generation, many high-emitting sectors like mining, oil & gas, agriculture and various forms of manufacturing have to mitigate either downstream or upstream emissions related to their suppliers or the use of their product. In either case, these Scope 3 emissions are created through the actions of suppliers or customers. A company has the ability to influence, through its choices, the behavior of these supply chain players (upstream), or may be subject to the priorities of others for whom they act as suppliers (downstream).

Access to financing is an important mechanism for influencing behavior across supply chains. However, in the context of a transition plan, as opposed to the case of corporate social responsibility programs, the objective isn't met merely by making financing available. Credibility of transition plans contains two elements:

1. Climate ambition, with a net zero target and ambitious trajectory to the objectives of the Paris Agreement
2. Robustness of ability to deliver, with an implementation strategy that enables tangible progress toward climate goals underpinned by consistent disclosures and monitoring

Having a science-based target can address (1) but does not guarantee (2). For the company's transition plan to be credible, there needs to be a cause-and-effect relationship between a company's provision of finance (e.g., directly or through an agreement with a financial institution) and resulting emissions reductions in its supply chain. The relationship needs to exist and must have data providing evidence that can be evaluated independently to demonstrate the capacity to deliver on the climate ambition in the transition plan. Supply chain traceability provided by blockchain technology, especially as it can underpin climate finance for suppliers, addresses a significant gap in the current ability to demonstrate the credibility of transition plans.

CONCLUSION

We must find ways to reverse the current paradigm where, for instance, it is only when a tree is cut that payments and rewards occur. We must collaborate across stakeholders to build systems that work to solve challenges first, and then apply multiple technologies within those new systems. Blockchain can be a tool to drive this change. As sustainability is becoming a strategy for competitiveness, more than merely a charitable aim, leveraging innovations like blockchain technology has shown that profitable business models can embrace net zero, and even climate-positive outcomes.

- This requires an acknowledgment that supply chains link global commerce and global finance together, even though there is often significant opacity throughout. Supply chains have developed in a way that is tied into an extractive economic model that benefits the Global North disproportionately over the Global South, undervalues natural capital and supports an unsustainable linear economy that produces high levels of waste. Blockchain has the ability to be additive to improving upon the status quo with a variety of business models.
- Certain approaches target the underlying extractive economic models, such as ReFi, and seek to value the stock of natural capital, such that markets can enable their participants to not only pay when resources are extracted. For supply chains, certain approaches that work link verified data together with financing of supply chains in order to improve the ability to support stages of the supply chain where mitigating emissions are needed, and make supply chain relationships more equitable.
- While many traditional approaches function adjacent to what happens with financial resources created from extraction and sale of resources, while both legal and illegal financial flows connected to resource extraction at the base of the supply chain often seek out developed market financial centers rather than being saved or invested domestically. This undercuts financial market development in these countries, helps weak institutions persist, which are often cited as the cause for the financial flight in the first place, and contributes to economic fragility of countries in the Global South. This is especially the case for those that are highly dependent on commodities and often subject to sharp boom-bust cycles where debt sustainability is a common concern.

Climate finance that brings or keeps more resources domestically can provide a counterweight to the economic cycles that have undercut countries' ability to generate sustainable development, let alone fund investments in climate adaptation. In these cases, blockchain provides a unique resource in contexts often characterized by weak institutions and low-trust markets with substantial leakage of financial flows connected to properly valuing natural capital assets and channeling supply chain climate finance toward conservation and regeneration of the planet, with positive outcomes for the people.

SECTION XI

SUPPLY CHAIN

EXECUTIVE SUMMARY

Most people didn't really focus on or even take note of what is referred to as the global supply chain until the Covid pandemic, when they weren't able to get goods that had always been available to them, virtually instantly. The global supply chain is actually made up of millions of entities that make, buy, sell, move, or, in the case of entities like customs organizations, even clear items to move out of or into a country. We will go more deeply into this throughout this document, but for now let's start with what would initially appear to be a very simple example:

Maria ordered a birthday present online

A **simple online order** can be much more **complex** than it appears.

- If it actually comes from a different country, it needs to clear customs.
- It may take much longer than anticipated to ship, so it wouldn't be delivered until after the birthday party.
- Because of the delay, she'd have to buy a replacement birthday present locally.
- Now she needs to work through the details to return the original present.

Now, a **simple online purchase** has potentially turned into an **ordeal** that is requiring Maira to jump into the details of **cross-border movement**.

- It took a dozen or more steps, and multiple entities, to get the shipment to Maria, which she had no visibility of.
- It also had to clear customs, which includes documentation she was unaware of.
- Now to return the birthday present and get her money back, she has to reverse a process she didn't know even existed.

Ultimately, stating that 'Maria orders a birthday present online' gets us to 50+ steps along the way, with multiple underlying processes and corresponding data points.: If and when she decides to return her order, a reverse supply chain process retraces all these steps, working through all the details of the same complex, multi-step, and multi-party process backwards.

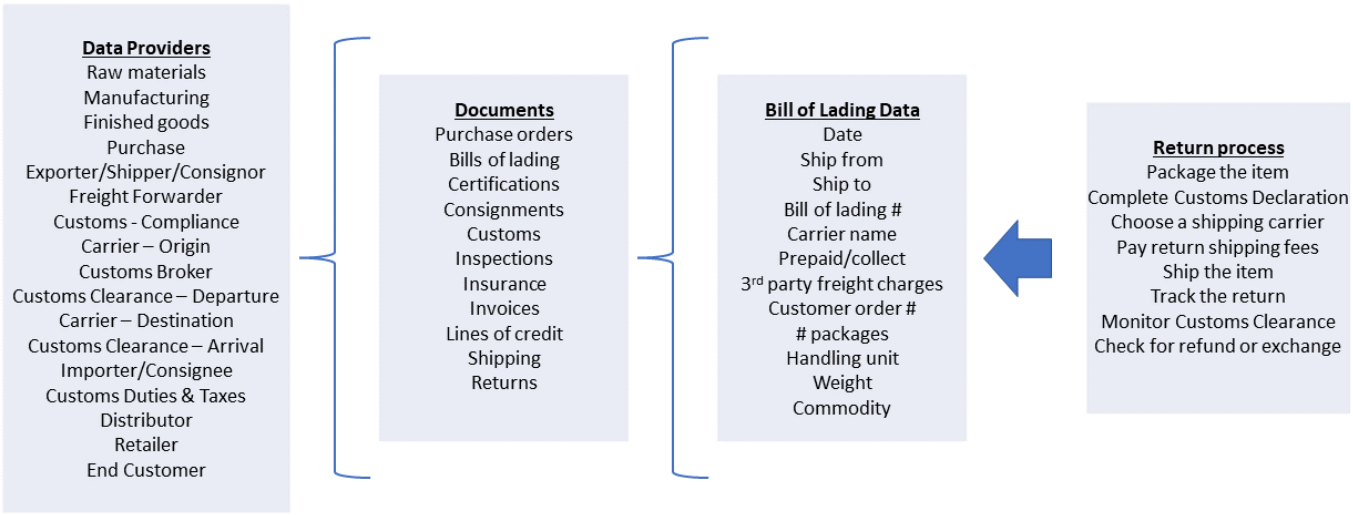


Figure 1: Complexity of today's global supply chain

As shown in the image above, the complexity of the global supply chain highlights a need for harmonization of processes and alignment of stakeholders. Beyond digitizing global supply chains, we need open-source standards to facilitate collaboration and reduce frictions. For digitization to scale we need a common data language and standards that all can use whether the largest companies, or the smallest.

This paper discusses the state of global supply chains today, defines the problems, and outlines solutions as enabled by emerging technologies to foster a Web3-enabled global commerce built on common standards. We feature specific business use cases of technology solutions, and ultimately emphasize the importance of common standards as a key underlying factor.

THE GLOBAL SUPPLY CHAIN

Global commerce involves multiple players, jurisdictions, and processes. The 'global supply chain' today refers to the intricate network of literally millions of interconnected organizations, processes, and resources involved in producing and delivering goods and services on a global scale. A typical example could span multiple countries and continents, with each participant playing a specific role in the production, distribution, and delivery of products to end consumers. This network of stakeholders collectively converts basic commodities or raw materials (upstream) into finished products (downstream) for delivery to end customers, with financial transactions and data being exchanged at each stage.[139]

Global supply chains encompass various stages and entities, including:

SOURCING	Acquiring raw materials, components, or services from suppliers around the world
MANUFACTURING	Transforming raw materials and components into finished products
DISTRIBUTION	Storing, transporting, and managing inventory throughout the supply chain
CLEARANCE BY REGULATORY AND CUSTOMS AUTHORITIES	Government agencies responsible for enforcing trade regulations, tariffs, and customs procedures, for both export and import into each country involved
RETAILING	Selling products to end consumers through various channels, such as physical stores, e-commerce platforms, and more

Every step of these processes has documentation to establish necessary checks and balances including movement, payment, and applicable Customs duties and taxes.

Global supply chains are essential for virtually all industries, enabling companies to access cost-effective resources, expand their markets, and optimize production processes. However, they also introduce complexities and challenges, such as logistical issues, regulatory compliance, and the need for risk management.

This all started with 'trade' by the Phoenicians, the Indus Valley trade, Egyptians, Silk Road, and Romans, as far back as 15,000 BCE ('Before Common Era'). Methods of movement were limited to the tools and innovations available at the time, including ships for maritime trade, overland caravans for land-based routes, and river transport, where applicable. The choice of transportation method depended on geographical factors, available infrastructure, and the nature of goods being traded. In the same way, supply chains today are shaped by the technology available which shapes all facets of the lifecycle of the physical movement of goods, records of those movements, and corresponding transactions.

Modes of Transportation

'Movement' of goods being traded gets us to 'mode' (initially, overland caravan or ship, and, later, rail, road, air, etc.), and as additional modes were developed, especially with highways and air movement, we quickly get to speed. Finally, once multiple speed options exist, and increased technology like the internet, deeper fragmentation has occurred to create Business-to-Business (B2B), Business-to-Consumer (B2C), and other similar areas of focus and types of commerce.

Global supply chains have been foundational to the millennia of human civilization, and they are continuing to evolve today with technology and innovation that enable different modes of transportation. Today, the main modes of transport are ship, rail, ground, and air, listed in order of speed. The most complex scenario actually includes multiple modes, known as intermodal or multimodal, in which two or more modes of transportation are involved to ship a package from its point of origin to its final destination.

- **Ship –** Ships are used for transporting goods over water, including oceans, seas, rivers, and canals. They are especially efficient for long-distance and bulk cargo transport. Ships typically are the slowest and least expensive mode.
- **Rail –** Rail transportation involves the movement of goods on railroad tracks using trains. It is known for its reliability and cost-effectiveness for land-based, long-distance transportation.
- **Ground –** Ground transportation includes movement by road (trucks and vehicles). It is versatile, used for both short-distance and regional transportation of goods on land.
- **Air –** Air transportation relies on aircraft to carry goods quickly over long distances. It is known for speed and is often used for high-value or time-sensitive cargo. Increasingly, drones will likely play a larger role in air transportation. Air is typically the fastest and most expensive mode.
- **Intermodal/Multimodal -** Intermodal shipping is the transportation of freight using two or more modes. The concept was brought about in the mid 20th century through the development of modern containerization. As standards were developed for container sizes and shapes, it scaled beyond ships to include rail and ground movement. Intermodal freight can reduce costs and handling on cargo, and is more eco-friendly, but is also much more complex due to multiple entities each having their own processes and requirements.

Figure 2: Modes of transportation

Types of Commerce

The notion of "business-to-business" (B2B) and "business-to-consumer" (B2C) in commerce began to gain prominence with the rise of modern industrialization and the development of mass markets in the 19th and 20th centuries. These distinctions became more pronounced as economic structures, trade practices, and technology evolved.

- **Business-to-Business (B2B) – Late 19th century onwards –** The growth of industrialization and the expansion of manufacturing industries led to increased trade between businesses. Companies began to specialize in producing goods and services for other businesses rather than solely for consumers.

- **Business-to-Consumer (B2C) – Late 19th century onwards –** With more significant distinctions in the mid-to-late 20th century, mass production, marketing and advertising strategies emerged, leading to the development of consumer markets. The advent of the internet and e-Commerce in the late 20th century further transformed various types of commerce, leading to even more distinctions in these categories.

- **Other categories –** Business-to-Government (B2G), Business-to-Business-to-Consumer (B2B2C), Business-to-Employee (B2E), Consumer-to-Consumer (C2C), Consumer-to-Business (C2B), Business-to-Government-to-Government (B2G2G – national level), Government-to-Government (G2G – international level), and Business-to-Business-to-Government (B2B2G – Traders/Regulatory), etc. have emerged with the increased sophistication of supply chains involving multiple parties.

Parties Involved

There are millions of entities involved in global commerce, across 200+ countries, conducting business in thousands of languages. In addition, each transaction requires multiple documents (could be up to 100 or more), making the end-to-end process extremely complex.

- **Manufacturers –** Produce goods and products for the global market, playing a central role in the supply chain by creating the physical items that are bought and sold.

- **Wholesalers –** Facilitate the distribution of goods by purchasing large quantities from manufacturers and selling them in smaller quantities to retailers, helping products reach a broader market.

- **Transport Companies –** Ensure the physical movement of goods across borders and regions, using various modes of transportation as defined above, to connect producers and consumers.

- **Logistics Providers –** Manage the movement and storage of goods, optimizing supply chains to ensure efficient, timely, and cost-effective delivery.

- **Financiers –** Provide the capital and financial services necessary for businesses to operate and expand globally, offering funding, loans, and investment opportunities.

- **Insurers –** Mitigate risks associated with global commerce, offering coverage for cargo, shipping, and other business risks to protect against potential losses.
- **Payment Providers –** Facilitate international financial transactions, enabling secure and efficient cross-border payments between buyers and sellers.
- **Retailers –** Sell products directly to consumers, offering a wide range of goods and services through various channels, including brick-and-mortar stores and e-Commerce platforms.
- **Regulators –** Oversee and enforce laws and regulations related to international trade, ensuring fair competition, consumer protection, and adherence to trade agreements.

Data Exchange

As the multiple stakeholders that make up the global supply chain convert basic commodities or raw materials (upstream) into finished products (downstream), and ultimately deliver them to end customers who will utilize them, data is exchanged at every stage. Flows of information include records of the trajectory of inputs and finished products, financial transactions, and personal information from customers and all stakeholders involved carrying out activities.[140]

The following image illustrates the flows of information, represented as arrows, between the typical parties involved in international commerce, as inputs become transformed into finished goods and transported from shippers to final consumers.

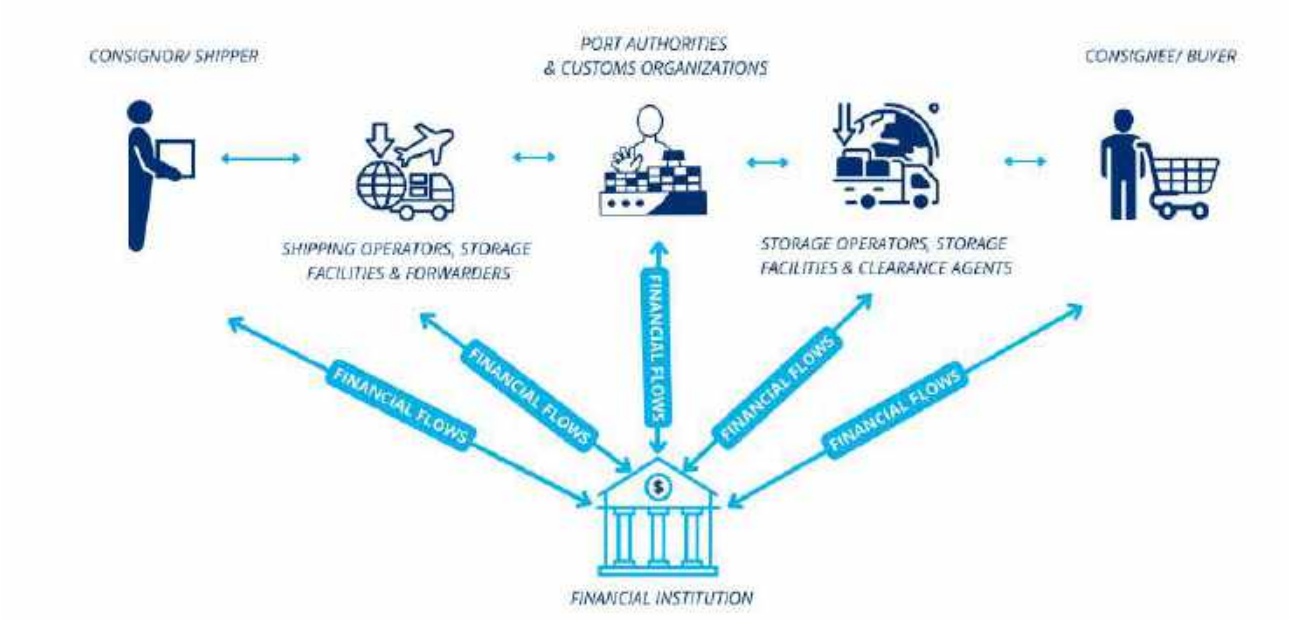


Figure 3: Data exchange across the supply chain

Documentation & Trust

A key part of the story of trade, leading to what we now think of as global commerce, is documentation, which emerged as a proxy to ensure trust. In the context of global digital trade, trust requires verifiable trust of the physical, financial, and informational exchanges. In all cases, trust requires the presence of a human subject (or a trustor) who forms a trust perception about an object trust (or trustee) in a specific context. A human may trust another individual, group, organization, or society; humans may also trust a thing, such as a policy or technology.[141]

Historically, all examples previously covered used some type of documentation for trade contracts, letters of credit, manifests, etc. By 3,000 BCE, the first customs and regulatory roles appeared in Mesopotamia. Since then, many of the underlying processes have been in place for as long as several thousand years, relying on a form of documentation to verify information.

Documentation, starting originally with clay tablets, and then papyrus, and and eventually paper, allowed some level of subjective 'trust' to be built into the movement of goods, such that, when something was being moved for the past several thousand years, the person/entity moving the items had some type of documentation to address custodianship, ownership, value, etc.

Today, current technologies are allowing us to digitize these traditionally document-driven processes, and digitalization and emerging technologies will allow us to completely rethink not only entire global movement processes, but how to significantly streamline those processes. These technologies will, for the first time, allow us to move from subjective trust to objective trust, where we know the true source of the data.

Current and emerging technologies allow virtually all paper documents to be replaced, and, once digitized, the data can be analyzed and optimized, significantly reducing delays that currently exist at borders and when changing hands between the many parties involved in global commerce.

Peer-to-peer technology, like blockchain, will allow digital 'trust' to be built into new solutions. Emerging technologies allow us to completely rethink processes that may have been used for millennia. The result will be significantly reduced friction (paper, delays, resources) in these processes, which across borders, has a major impact on global commerce. Increasingly, global supply chains are also expected to capture data to make sure goods were produced with fair labor practices and with environmentally sustainable practices.

PROBLEM & SOLUTION

Problem

Today there is no end-to-end visibility into the supply chain lifecycle. The magnitude of this problem can be seen with major global concerns such as undetected forced labor scenarios and mislabeled products that mislead consumers (e.g., murkiness in the beef supply chain, where not only the origin but also the nature of the product have been misrepresented). This section covers those undesired aspects of the global supply chain, from the past hundreds, and in some case thousands of years, in the context of the following: What failed in the past? What problems can be addressed? What are the implications?

Global supply chains today are not harmonized.

Virtually none of the processes in global commerce today were designed with a 'global' focus, so it should not be surprising that global supply chains are not harmonized. In this case, 'harmonized' means interoperable, with a common data language and open data standards. Lack of standardization causes myriad complexities and difficulties, where inconsistencies in formats and access to data lead to inefficiencies and unnecessary friction, including massive amounts of paperwork, resources, and delays. The world experienced this in real time during the COVID-19 pandemic, when many everyday products suddenly became unavailable and supply chains experienced massive bottlenecks.

DATA SILOS & INCONSISTENT DATA STANDARDS

With multiple stakeholders collecting massive amounts of data throughout the supply chain in disparate ways, a range of inefficiencies can be attributed to data silos and complexities of information flow. While data on physical and financial flows across every step of the supply chain remains inconsistent, it can be very difficult (if even possible currently) to create a holistic view of the end-to-end journey from raw material to finished product. Data silos and inconsistent data standards are estimated to cost the global supply chain **$1.1 trillion** each year.[142]

Inconsistent records across trading partners can also trigger disputes, while loopholes can enable counterfeit and sub-par products to slip through the supply chains. Missing paperwork and disparate records can also lead to assets getting lost or stolen, causing shipping containers to be delayed in ports, just as one example.

Moreover, data silos can hinder communication and collaboration across stakeholders. Not only do parties across the supply chain often create and store data in their own separate formats, they may also share it only with the next partner in the supply chain to create a limited "one step up, one step back" visibility that makes it very difficult to have a holistic view of the end-to-end trajectory of a product.

As a result, in cases where a retailer must respond to a food recall, for instance, the task of tracing produce on the shelves to the farmers who grew it can be a daunting task taking days or even weeks.

LACK OF TRUST

In order to build trust into the system, we operate in a complex, often cumbersome and document-laden process, in place for centuries, even millennia. Most of that trust has been artificially created within these processes as a system of documents and signatures, and, in some cases 'chain of custody' scenarios. Manual processes bring time consuming documentation and revisions procedures. Many of these processes and requirements have essentially been created as proxies for trust.

In only a small subset of the global commerce space, a single delivery carried out by a truck to fulfill a single invoice can involve hundreds of data elements. Moreover, additional charges for wait times, layovers, and specialized services (e.g., liftgate services, inside delivery, temperature-controlled services, handling of hazardous materials, unloading, etc.) can add to the amount and complexity of data far beyond basic shipping information and freight description.

Often customers dispute the charges presented to them by freight carriers. In the US transportation industry, which amounts to $8 trillion annually, an average of $140 billion in invoices are disputed daily, with disparate accounting records among different stakeholders.[143]

It is estimated that up to 38% of invoices are overpaid, as a cheaper alternative for enterprises than investigating unexpected charges. Other indications of lack of trust include disputes over the condition of freight and compliance with specialized requirements for certain supply chains, such as keeping items at the proper temperature throughout the entire route.

Counterfeiting in particular is a major concern. For instance, in 2019, the global fake foods market was estimated at $449 billion, or 2.5% of all global trade – greater than the entire economy of Ireland.[144] The COVID-19 pandemic further aggravated the concern of counterfeiting, particularly for vaccines. Counterfeit medicines have been on the rise globally, with nearly 6,000 pharmaceutical crime incidents recorded by PSI in 2021 – a rise in 38% from the prior year, and a new 20 year high.[145] In addition to counterfeit products as a concern, goods may be unsafe or contaminated.

Finally, vulnerability to fraud can lead to security concerns due to lack of transparency. This can lead to poor collaboration between partners in the supply chain, where incentives toward dishonest behavior may prevail. Unethical and unsustainable practices can also go unchecked.

OUTDATED PROCESSES

Digitization alone does not solve the underlying issues that come from outdated processes, which to lead to a wide range of inefficiencies. Friction in supply chains, caused by document-laden processes, is estimated to cost the global supply chain $1.2 trillion each year.[146] It is difficult to align incentives among stakeholders across common global supply chain processes (e.g., export clearance, import clearance), and also across industry-specific processes (e.g., batch traceability for pharmaceuticals).

The sheer number of intermediaries and lack of openly available, harmonized data can lead to significant logistical and operational challenges, alongside outdated and inconsistent infrastructure. The average international trade transaction involves dozens to hundreds of original documents, copies, and entities to send them to, often involving cumbersome manual processes.[147] Sourcing raw materials at a global scale, and shipping, and any stage along the supply chain becomes highly, and unnecessarily, complex.

Often delayed payments and verifications lead to a wide range of friction stemming from disparate and long reconciliation times, lack of clarity on how items are transported, and lack of data. The complexity of payments in shipping is best exemplified by the payment of truck drivers. One challenge facing ground transportation drivers is that they do not get paid until a shipment is delivered, and they may have to wait weeks, or even months, to receive payment. This creates cash flow challenges, so entire business models have emerged to pay these operators 70%-90% of their invoiced amount at an earlier point in time, which introduces yet another party in the process, with its own set of complex systems. Drivers can choose to be paid – albeit less than what they are owed

Figure 4: Each stakeholder faces a particular set of challenges along the supply chain

LACK OF INCLUSION & RESILIENCE

Foreseeable and unanticipated disruptions in the supply chain can have significant repercussions. The world immediately discovered just how fragile global supply chains were during COVID-19, and other examples could be natural disasters or other catastrophes. These systems can be far from resilient with seemingly minor events taking place to start a domino effect with major repercussions on the ability to deliver of essential products to those who need them most.

Global commerce, with its cumbersome processes and siloed data as it istoday, can make it very difficult to access global markets for small and medium enterprises, particularly in economically disadvantaged areas. This affects those players who would most benefit from accessing global markets. Roughly one in five adults, or around **1.7 billion** people in the world still do not have access to formal banking services, with women more likely to be unbanked than men. Lack of access to mainstream marketplaces can perpetuate global inequalities, which often fuel geopolitical conflict.

Solutions

With Web3/blockchain and emerging technologies, along with the desire and ability to create common and open data standards to reduce friction in existing processes, there is a – much – more efficient and digitized global supply chain in our future. This is not a process improvement exercise, where we are essentially trying to improve processes that in some cases are literally hundreds to thousands of years old. Today's emerging technology will allow us to completely rethink and reinvent existing processes, making life much easier for Maria making everyday purchases, as opposed to the state of supply chains today.

This section discusses the following key elements toward optimizing supply chains:

- Harmonization
- Common language and standards
- Trust through data
- Better processes
- Resilience

HARMONIZING GLOBAL SUPPLY CHAINS

Harmonization is at the core of every solution to address the issues mentioned in the section above, to reduce friction across the life cycle. This requires reimagining a new model for supply chains that are efficient and resilient.

The attributes of blockchain technology, in convergence with other emerging technologies, can have numerous benefits across several solutions that ultimately are pointed toward harmonizing supply chains at a global level. First, blockchain allows participants to store digital records of information, exchange that information directly among participants, and abide by common business rules (e.g., smart contracts, standards, etc.).

> **Interoperability** is key, where open data is fundamental for scale. A new model leveraging emerging technology can enable a pro-competitive coopetition to increase the available opportunities to all stakeholders with increased collaboration and alignment.

COMMON LANGUAGE AND SHARED OPEN STANDARDS

Consistency for the financial and physical movements of data is key. Shared records that blockchain technology allow can be revolutionary. The need for interoperability in the blockchain space goes beyond connecting multiple blockchains, but also implies the ability to integrate with existing systems. Shared data can streamline processes, reducing time and paperwork required do complete tasks. Open standards enable interoperability and ease of communication among devices and systems, toward more efficient use of existing resources.

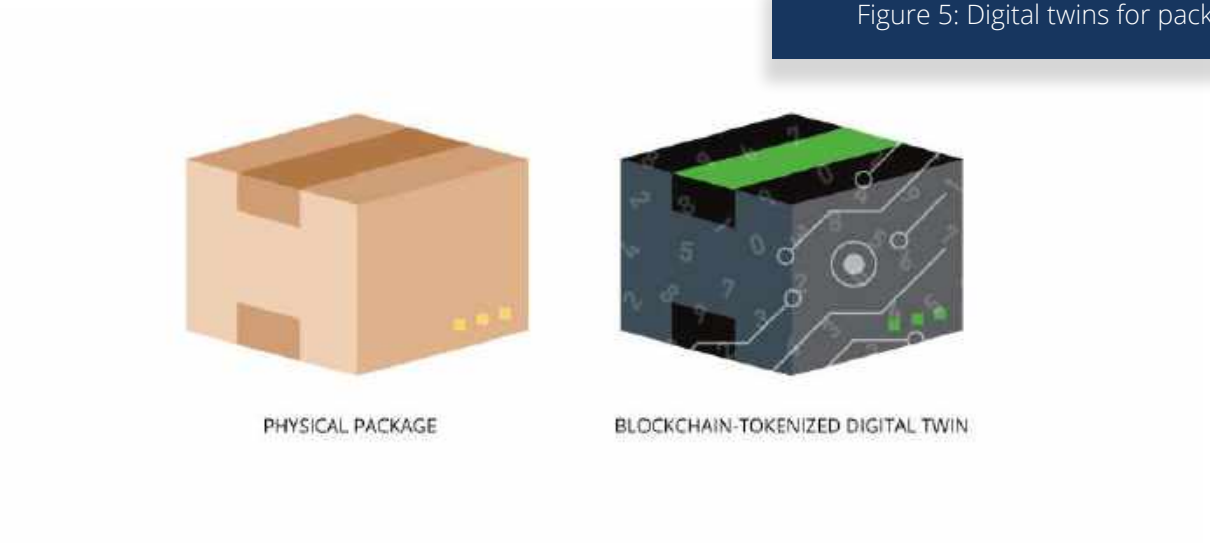
Open data can also enable a single source of trust for vendor verification, stakeholder authenticity, and authenticity of products. For instance, a public key infrastructure to verify digital signatures or zero-knowledge proofs can increase trust in authenticated evidence on physical and financial flows. In turn, developers of digitized solutions can also quickly adapt to changing circumstances and conditions, leading ultimately to faster development, better applications, and greater trust.

Shared invoices, for instance, can greatly reduce disputes. The disputed invoicing problems mentioned above in the context of truckers can be solved by creating one shared version of the invoice, managed with a smart contract, and integrated with IoT devices that can monitor the temperature and location of freight, as applicable. When freight carriers can move to a shared invoice managed with smart contracts using blockchain technology, which can connect to IoT data, invoice disputes can fall from as high as 70 percent to as low as under 2 percent. Invoices can also be finalized more quickly – such as within 24 hours instead of days, weeks or longer. Moreover, with costs reductions for both parties in a commercial exchange, relationships can also be improved.

Emerging technologies, such as blockchain, enable an unprecedented level of transparency, allowing an end-to-end view of the status of a shipment. The concept of a 'digital twin' will be used by industry to model opportunities in a number of areas, and, with tokenization, representations of data or value on a blockchain can be exchanged and new value created. Self-sovereign identity will also be foundational with these emerging technologies. 'I am who I say I am' is a dramatic improvement over legacy paper-driven processes.

As physical and digital worlds are colliding such that physical and digital information flows alongside in parallel, the opportunities of digital twins for global supply chains highlight how the information about a package may be as important than the shipment of the package itself.

Figure 5: Digital twins for packages



Current technology allows us to create a 'digital twin' of virtually anything, and in the context of the global supply chain, it becomes possible to essentially clone the data from all packages moving around the world, along with many other applications. There will still be a physical movement from point 'A' to point 'B,' but having a digitized version of that will streamline a wide range of activities, from crossing a national border to creating virtual supply chains where efficiencies can be modeled for improvement. All of this allows opportunities for analytics, optimization, and both predictive models ('What -will- happen?') and prescriptive models ('How can we -make- it happen?') to enhance and streamline existing, and, in some cases, archaic processes. Such a digitized process can significantly reduce friction across borders (e.g., paper, delays, resources, etc.). True paperless trade will transform global supply chains and customs processes, disrupting business models that are currently reliant on multiple 'middlemen.'

Figure 6: End to End Supply Chain Matrix Subset Example

EFFICIENCY WITH BETTER PROCESSES

Updating current models to harmonize global processes is the essence of the "true north" to which global supply chains are pointing toward, as enabled by emerging technology. Blockchain and emerging technologies allow us to completely rethink systems and processes that weren't originally built with digital/ paperless and trusted systems in mind. Processes centered on sharing open data and common standards are fundamental.

These processes will be redesigned with digitalization in mind, ensuring objective trust is built into future systems, not only significantly streamlining many of these processes, but also minimizing the friction that has always existed in these processes to date. A streamlined and paperless supply chain framework can provide a full end-to-end life cycle view of the whole supply chain, as well as subsets of the full lifecycle.

Technology allows users to hold a digital asset that represents value, and transfer the digital asset, as a replacement to the historical model of a paper data record. Digital records on a blockchain will consist of information captured in a standardized format. Transfer of information directly among different parties without intermediaries increases transparency and reduces costs, besides having the ability to verify information and authenticity of the publisher of information regarding the legitimacy of players involved and goods produced & shipped. Blockchain technology provides an opportunity to create seamless information exchange between various parties, where information and trust can be established. Peer-to-peer interactions can reduce costs and streamline processes, allowing feedback loops from top down and bottom up.

PUBLIC & PRIVATE MODELS FOR SUPPLY CHAIN LIFECYCLES

Broadly speaking, a private blockchain prioritizes controlled access and confidentiality among a select group of companies and participants in a network, while a public blockchain emphasizes transparency and trust across a broad network of participants. The choice between the two depends on the specific needs and objectives of the supply chain participants.

In a private (also known as a 'permissioned') blockchain, normally a consortium of companies involved in a specific supply chain (e.g., manufacturers, distributors, retailers, etc.) operates the network. They maintain control over who can participate and what data is openly visible. Each participant has a designated role, and sensitive pricing or proprietary information is kept confidential.

In a public blockchain, multiple stakeholders in a global supply chain use a shared, transparent ledger to track the movement of goods. Any participant can join the network, view the entire transaction history, and validate transactions. For instance, consumers can scan a QR code on a product and see its entire journey from the manufacturer to their hands. Benefits of a public blockchain include transparency, immutability of records, and decentralization.

To scale globally, the shared transparent ledger of a public blockchain must also address confidentiality while preserving the benefits of transparency.

Figure 7: Public vs. private models for supply chains

Public blockchains	Open to anyone to update and view with full access. For instance, a supply chain ledger for a retail brand would be viewable by anyone in the network.
Private blockchains	Permissioned model restricted to authorized set of participants to authorize updates and make changes. For instance, industry specific ledgers with payment contracts may restrict sensitive data. In the enterprise sector, ledgers may be shared between a parent company and subsidiaries with restricted access.

TRANSPARENCY

Transparency doesn't mean everything is visible to everyone in the network, or blockchain and emerging technologies would simply not scale because no one would (or should) share confidential information such as intellectual property, pricing information, etc. There are also laws such as the EU's GDPR (General Data Protection Regulation), which introduce obligations such as 'the right to be forgotten.' GDPR would require administrators to comply with requests such as making changes or even remove records from a ledger. If I have the right to be forgotten, how can that take place if the data on a blockchain is immutable? The answer is, it can't when sensitive or personal informational is recorded directly on the ledger. This is the same reason why private information will be kept behind a firewall. On a blockchain, when information is recorded in a pseudonymous format through encryption mechanisms, it can be made available upon request to authorized parties that receive an anonymized link to the underlying data.

Transparency in the reference around blockchain, Web3, and broader emerging technologies, means creating a trustworthy, accountable and visible environment for transactions and processes along the supply chain lifecycle. For public blockchains to scale globally, technologies like zero-knowledge proofs, permissioned data access, control mechanisms, and keeping private information off-chain will all likely play a key role.

TRADELENS

While blockchain and emerging technologies have the potential to be transformative for global commerce, not all are created equal. TradeLens is an early example of a deployment on a permissioned blockchain, launched by Maersk's GTD Solution division in collaboration with IBM. This was a business model attempt to digitize and simplify global supply chains through an electronic shipping ledger that would track cargo shipments from origin, ports, overseas locations, and, ultimately, final destinations.

While the business model did not work for multiple reasons (high costs, broad scope, significant system integrations and consulting services, and unwillingness among key players and competitors to share data they considered business sensitive), the belief is that a public version of a blockchain solution for supply chains can still scale with open data standards, and, assuming confidentiality can be managed, as discussed in the 'Transparency' section.

RESILIENCE

Transparency and open data also make supply chains more resilient, able to adapt and respond to unexpected events and disruptions, and able to recover from negative consequences by maintaining the continuity of essential operations and functions. Connectedness is key to resilience, and the attributes of blockchain technology can enable an unprecedented level of visibility into potential bottlenecks across the supply chain. Providing organizations in a supply chain with the ability to be predictive and proactive, rather than reactive, in terms of risk management, can greatly decrease the severity of an unwanted event before it happens. Ultimately this can save money, reduce the stress of managing these situations, and avoid compliance violations that can damage the reputation of companies and organizations.

In addition, a decentralized and peer to peer system can facilitate access to global markets and business opportunities for smaller businesses and less developed geographical regions, which would support their global competitiveness. Increased inclusion of entities can also mitigate the impacts of strained supply chains, providing additional access to suppliers.

REAL WORLD USE CASES

Successful real-world applications of blockchain technology for the global supply chain are already addressing the multiplicity of issues emanating from a lack of harmonized supply chains, connecting various disjointed steps along the way, and ultimately facilitating outcomes for everyday individuals like Maria above, who buy and sell items consistently.

Provenance (authenticity/pedigree) is key in this context, where the benefits of recording and sharing provenance data can provide tremendous value across industries. In a 2020 report, economists at PwC identified provenance as the top application of blockchain technology that is driving adoption and has the potential to yield the most economic value. The potential boost to global GDP by 2030 was estimated to be US$962 billion.

With reliable provenance data, organizations can also demonstrate that their products are environmentally friendly, and produced in a socially responsible way. This is increasingly relevant with upcoming forced labor compliance rules, where shipments will be halted at customs upon the mere suspicion of involving forced labor at any point across the supply chain.

These applications are deploying Web3 technology to connect multiple exporters and importers to participate in a larger connected ecosystem where commercial interactions can take place. A technology platform that can validate a shipment, including all its parts and inputs, can optimize and harmonize the process for all participants in this ecosystem – with benefits ranging from improved resilience, authenticity, security and privacy, and interoperability.

By increasing efficiencies, reducing costs, and expanding market opportunities, blockchain technology can foster coopetition among traditional competitors, where collaborative practices can improve outcomes for all entities, even traditional competitors, and can do so in a pro-competitive way, to the benefit of all.

Circular Economy with End-to-End Traceability: Battery Passports

Digital product passports (DPP) are being envisioned to establish and contribute to a circular economy. Early work in the EU revolves around battery passports, digitally documenting every step of the life of a battery, from raw material, through all the stages of the supply chain, and even throughout the lifetime of the battery's use, and ultimately connecting to ways to reclaim and recycle the product at the end of its lifetime. The battery passport work in the EU will become foundational for Digital Product Passports in many other areas and for the logic of a circular economy.

Better Economic Outcomes for Producers: Coffee and Cacao Supply Chain Traceability in Honduras

Provenance enabled by blockchain technology can serve to greatly improve economic opportunities for producers of basic commodities. As customers are increasingly demanding insight into the provenance of products, the ability to demonstrate who grew the coffee bean becomes a competitive advantage. Consumers value access to this data, and with it they are more willing to purchase finished goods where a fair portion of the profits go to the farmers who did the work.

For instance, smallholder coffee and cocoa farmers in Honduras are leveraging public and private blockchain infrastructure to enhance transparency and make informed business decisions. These farmers, who often operate at a significant loss and earn a mere fraction from the sale of coffee and chocolate in retail outlets, are now empowered by a traceability system that provides insights from farm to point of sale. Blockchain has allowed farmers and their cooperatives to upload lot, quality score, certification, and other provenance data. This transparency not only offers buyers a clear view of the product supply chain but also positions farmers to negotiate better prices. The intricate journey of coffee and cacao, from farmers to consumers, involves multiple intermediaries, often diluting the profit margins for the initial producers. However, with blockchain solutions, there's an authentic record of provenance, granting these smallholder farms a competitive edge in the market, and increasing the resiliency of commodity-based supply chains. This enhanced resiliency is crucial in mitigating risks such as market fluctuations, climate change impacts, and geopolitical tensions, thereby ensuring a more stable and sustainable supply chain for all stakeholders involved.

Efficiency for Global Customs Organizations

There are approximately 200 customs organizations around the world, which would greatly benefit from an efficient chain of custody and provenance for cross-border shipments and returns, with a resulting duty drawback. Customs organizations are also undergoing increasing pressure from growing small packet commerce to handle the regulatory export and import clearances and associated duties.

Transparent value reconciliation, which is a major initiative for several customs organizations, can reduce frictions where blockchain-based and other emerging technology solutions can benefit all participants in a network with authenticated, trusted information exchange. In addition, manifest reconciliation can also record areas of labor exploitation, resource waste, plundering the earth, and pollution of natural ecosystems. This is particularly relevant today given upcoming regulations on stamping out forced labor, sustainable sourcing, and overall responsible behavior. These solutions can also improve turnaround time for clearances, thereby reducing customs holds caused by missing information or data silos. Customs compliance scores recorded on blockchain networks can help importers evaluate alternate sourcing options to mitigate risks and enhance planning and execution, ultimately resulting in more resilient supply chains.

Ensuring Specified Conditions for Supply Chains: Global Pharma

In combination with sensors across a supply chain capturing data through the Internet of Things, blockchain technology can record that data immutably to verify that specified conditions required for certain supply chains have been met across the journey from production, shipment, and final sale and use by the customer. In global pharmaceutics, requirements for cold chains are often necessary to ensure medical products such as certain critical vaccines (e.g., Covid vaccines) are fit for use. One example would be the combined use of IoT sensors and blockchain technology, where a blockchain would record the sensor information about a cold chain shipment and permanently memorialize that data, confirming whether the temperature requirements have been met across the entire journey. This helps identify with certainty the instances where IoT sensors detect a breach in the cold chain. This process can help stakeholders identify a batch that is deemed no longer safe for use, and take actions accordingly. Smart contract functionalities can make an autonomous decision to return the faulty batch back to the shipper, based on proof and understanding that across the lineage of destination the cold chain was broken.

Streamlining Payment Processes: Invoicing

Blockchain technology enables open sharing of validated information among network participants. In the case of global freight, a single invoice for one truck to make one delivery can have up to 200 data elements. Besides the obvious shipping information and freight description, freight carriers add accessorial charges are added to the invoice along the way, such as charges for wait times and layovers. Other common accessorial charges can include liftgate services, inside delivery, temperature-controlled service, hazardous materials handling, and unloading services. The customer must review accessorial charges, which can lead to disputes when the customer expects costs to be lower than the freight carrier's charges. In addition to disputes over costs, disputes also arise pertaining to the condition of the freight, such as if the freight was kept at the proper temperature during the entire route. Across the U.S. transportation industry, for instance, an average of $140 billion worth of invoices are in dispute on any given day while partners attempt to reconcile disparate accounting records across firm boundaries. Up to 38% of invoices are overpaid because it's sometimes cheaper for enterprises to simply pay these invoices than to investigate unexpected charges.

The series of issues associated with disputed invoices can be solved by creating one shared version of the invoice, managed with a smart contract, and integrated with IoT devices that can monitor the freight conditions such as temperature and location. For instance, when Walmart Canada and its freight carriers adopted a shared invoice system managed with smart contracts using a distributed ledger connected to IoT data, invoice disputes fell from 70 percent to under two percent. This system also allows invoices to be finalized within 24 hours instead of days, weeks or longer. Finally, reduced costs as a result also improved commercial relationships for both parties.

STANDARDS

While multiple data elements and standards exist in global commerce, they don't exist at the International Space Station – that is, truly global – level. Existing standards cover different aspects of supply chains and blockchain technology, although there still exist gaps where standards are unclear or non-existent, and ultimately certain standards may overlap.

This points to the need for a "harmonizer" role where open standards can apply to the full data journey of elements across the entire supply chain. Global standards for open data, precisely in the context of supply chains, are what it will take to scale Web3 technologies consistently in a way that can transform global commerce. Standards are the underlying condition for harmonizing global supply chains, allowing the solutions outlined above to address the challenges that have faced global commerce for thousands of years. Standards also lower the hurdles to leveraging blockchain as an achievable solution.

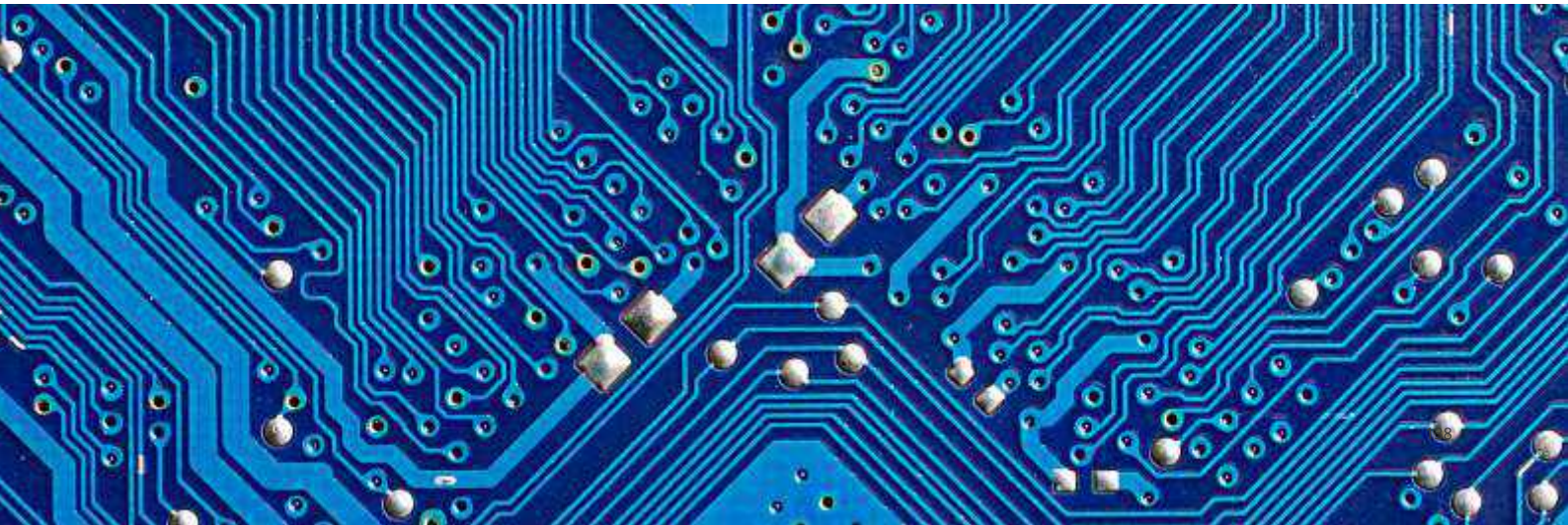
At the truly global International Space Station level, there is no individual company, no industry, and no borders. Data knows no geographic borders, but we don't yet have global standards to enable this vision. Global, pro-competitive, royalty-free, and open-source data standards must also apply to all players across the supply chain, which is key for scalability of Web3 technology solutions that are built on open data (e.g., digital twins). To optimize supply chain enhancements enabled by these innovations, open and interoperable standards provide a common data language to reinvent and redefine processes. Only then will global commerce accelerate to the speed of data.

The diagram below is a mapping of the existing standards as they are, an assessment of expected standards in development, and a gap analysis that identifies areas where there is still a need for standards. The resulting standards framework ultimately demonstrates a hierarchy of standards, where often standards bodies focused on certain aspects of the global supply chain draw their requirements from larger global standards bodies. For instance, many standards bodies dictating requirements on aspects of the supply chain, such as data elements on country of origin, ultimately point to requirements set by larger global standards setters such as the International Organization for Standardization (ISO).

Figure 8: Landscape of standards across supply chain data elements

			Type of element		Reference					
	Data Element	Description	Standard	Free Form	Standard	WCO	DSI	OCB	CO	CI
1	Country code/Country of origin	Code representing a specific country	x		ISO 3166 EDIFACT 3207	x	x	x	x	
2	x	x		x	x			x	x	x
3	x	x		x	x			x		
4	x	x		x	x		x		x	x
5	x	x	x		x			x		
6	x	x	x		x			x		
7	x	x		x	x				x	
8	x	x	x		x	x	x	x		
9	x	x		x	x			x		
10	x	x	x		x					x

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

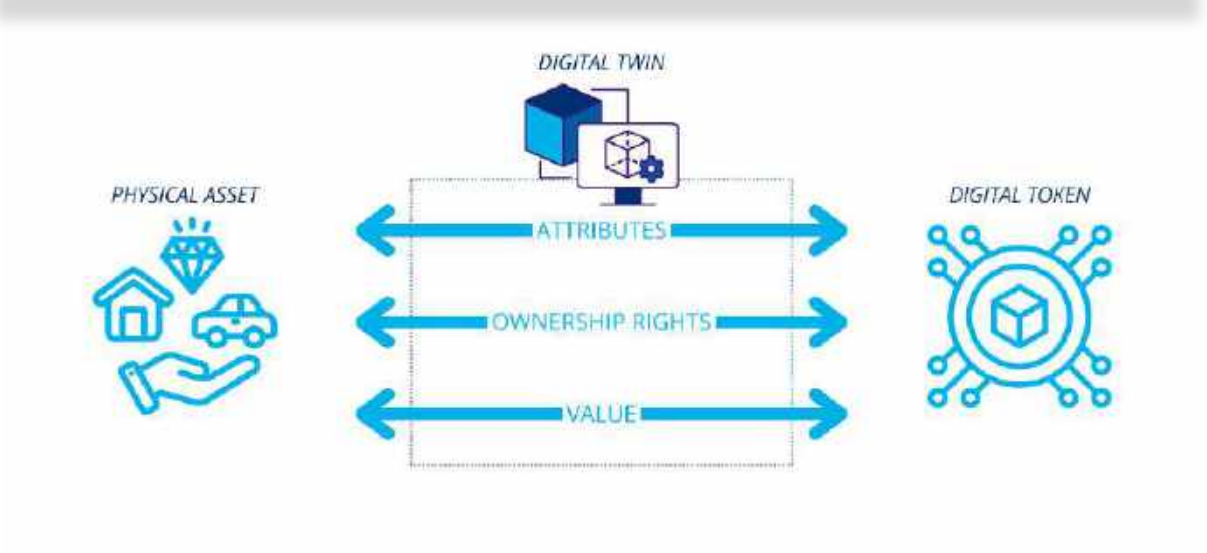


Examples

1. Tokenization allows for a digital representation on a blockchain of a real world asset that is not native to the blockchain. While this term has mostly been associated with a cryptocurrency token, a token is not a currency but a representation of any form of data, which functions as an "asset" (e.g., document, data files, historical tracking) . This digital representation is a key aspect of supply chain optimization using technology to efficiently transact at a global scale.

   GBBC's **InterWork Alliance (IWA)** has developed a **Token Taxonomy Framework** that has already produced a blueprint to develop open source, platform neutral tokenization standards to promote interoperability between disparate systems. With the shift to digitizing the supply chain ecosystem, adopting the needed data standards will be key to ensure token ("data") interoperability (e.g., cross-chain), while connecting legacy logistics systems to trigger token transfers for certain supply chain events. While the data standards will still be important, the tokens themselves will serve as a gate to the data recorded on a chain. Token standards can provide stakeholders with access to more industry-specific taxonomies. When the taxonomy and the underlying technical code for a use case are available to the community via open-source standards, they provide the blueprint that enables faster implementation of products and services.

Figure 9: Tokenization to trace supply chain packages through digital twins



2. For instance, **W3C's PROV-O**[148] open specification provides a foundation to implement provenance applications in various domains that can represent, exchange, and integrate provenance data generated by multiple parties, across different systems, and under diverse contexts.

3. The **Digital Container Shipping Association (DCSA)** has set a goal by 2030 of 100% adoption of standards-based electronic bills of lading for its members, contributing to end-to-end digitization.

4. The **Digital Standards Initiative (DSI)**, hosted by the **International Chamber of Commerce (ICC)**, has provided recommendations to harmonize digital trading standards to benefit businesses, governments, and individuals.[149] These standards are designed to ensure trust, where trust in global trade requires verifiable trust with respect to the physical, financial, and information exchange involved in the trade of goods and services, which ultimately depends on trust in legal, governance, and technology infrastructures underlying. [150]

Methodology

Due to the relatively short time between the announcement that BITA and GBBC had merged (July 2023) and the delivery date of GSMI 4.0 Supply Chain, the initial review of standards was limited. We will use the 4.0 version as our backbone/foundation moving forward, as we expand both the number of data elements included, and the number of standards entities and documents.

The initial 48 data elements included come from multiple sources, as explained below, and from business data element requirements, and are intended to form the backbone of future work as data elements and standards entities are added.

The one example above walks through the methodology:

- **Data Element –** Country Code/ Country of origin
- **Description –** Code representing a specific country
- **Type of standard**, e.g., an actual standard to be followed, or a free form entry
- **Identified standard(s) –** e.g., ISO, UN Trade Directory Code, WCO, etc.
- **Entities reviewed –** for the 4.0 version, this included World Customs Organization (WCO, Digital Standards Initiative (DSI), and Open Customs Blockchain (OCB)
- **Documents reviewed –** for the 4.0 version, this included Certificate of Origin (CO) and Commercial Invoice (CI)

This early work points out multiple observations, all pointing to the need for global harmonization, e.g., a common language, in global commerce:

- Some entities focus on specific forms or only customs, etc., and map their data elements that way, but we started with the business/movement/transportation side of this, e.g., what data elements are the most basic that are required to move a shipment from point 'A' to point 'B'? This list is likely in the hundreds, and BITA/GBBC/GSMI will continue to move forward with additional data elements and standards entities reviewed to make this more comprehensive and also to create a living, breathing list with applicable links.
- We quickly realize that not every data element has been identified by all entities, or exists on all forms, and we also quickly realize some data elements have a hierarchy of standards. In the country example shown, there is a UN EDIFACT number assigned (3207), but if you refer to that, it also points you to ISO 3166. There are numerous examples where multiple standards exist, or one standard points you to another standard, though, again no fully harmonized code.
- Other items above were simply reduced to an 'x' in appropriate cells just to further show the diversity of responses. The full list of 48 items, with all applicable responses, is included with this document for review.

This initial effort (GSMI 4.0 Supply Chain) points out that the more we can put into focus the full list of data elements, and a single standard, or multiple standards, or, likely, no standard, the more we can discuss with other like-minded open standards entities so we can agnostically align and harmonize these open standards results, to the benefit of all. One great example is that as recently as 2019, World Customs Organization (WCO) had proprietary standards, and as of 2023, those standards are now open.

CONCLUSION & BITA FUTURE OUTLOOK

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.

An effort to map, produce, publish, and implement open data standards harmonization for emerging technologies in the global supply chains is the "True North" guiding this initiative. Moving forward, the goal is to produce a living repository of standards documentation that is constantly updated (e.g., Wikipedia concept), to serve as an open-source standards foundation for emerging technology for global supply chains. These standards are meant to support future reference architecture for foundational use cases.

These standards will also serve as a roadmap to educate stakeholders and guide public and private models of that can shape a new era of commercial activity that can include a wider range of large, small, and medium enterprises and organizations from around the world to participate in connected, trusted, efficient marketplaces. New and efficient processes based on these standards can also enable point-to-point global commerce, addressing barriers that currently prevent individuals, for instance, to make purchases directly from manufacturers abroad.

CALL TO ACTION

The BITA initiative calls companies and organizations participating in the global supply chain to commit to collaborating on open source solutions.

Tomorrow, with emerging technologies deployed in harmonized and scalable ways underlying the processes involved in global commerce, Maria can make her daily purchases in a much simpler world. We expect most 10-year-olds today, as adults in the future, will want to know where the coffee they are drinking came from, if the clothes they are wearing are sustainably made, and many other details on the products they consume, which originate from data collected along global supply chains.

ANNEX A

MORPHOLOGICAL FRAMEWORK OF AI

The morphological framework below, based on Fritz Zwicky's "Morphological Astronomy," is a proposal to discuss and agree upon dimensions and conditions for AI implementations. This is a mind map of detailed categorizations and sub-categorizations of AI features based on structures, types, tasks, functions, and branches, to provide a broad structure that can be useful multiple stakeholders and facilitate collaboration.

ENDNOTES

AI & CONVERGENCE

1 https://creativecommons.org/2023/08/18/understanding-cc-licenses-and-generative-ai/
2 https://arxiv.org/pdf/2305.03928.pdf
3 Refer to taxonomy resources of GSMI 4.0, which includes a subset of definitions on AI
4 https://evals.alignment.org/
5 https://www.data4sdgs.org/
6 12 CFR Part 326 (https://www.ecfr.gov/current/title-12/chapter-III/subchapter-B/part-326); FinCEN (https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act#:~:text=Specifically%2C%20the%20regulations%20implementing%20the,might%20signify%20money%20laundering%2C%20tax)
7 12 CFR Part 353 (https://www.ecfr.gov/current/title-12/chapter-III/subchapter-B/part-353)
8 CDD Rules (https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions)
9 FinCEN (https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule)
10 https://www.consumer-action.org/news/articles/alternative_data_and_financial_inclusion_summer_2017
11 https://www.ftc.gov/business-guidance/blog/2012/06/speaking-spokeo-part-1
12 https://www.consumerfinance.gov/about-us/newsroom/cfpb-acts-to-protect-the-public-from-black-box-credit-models-using-complex-algorithms/
13 https://www.brookings.edu/articles/credit-denial-in-the-age-of-ai/
14 https://www.cfpaguide.com/portalresource/Exam%20Manual%20v%202%20-%20UDAAP.pdf
15 https://occ.gov/news-issuances/bulletins/2023/bulletin-2023-21.html
16 https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/autonomous-driving-disruption-technology-use-cases-and-opportunities
17 https://bmdv.bund.de/SharedDocs/EN/publications/strategy-for-automated-and-connected-driving.pdf?__blob=publicationFile
18 https://www.mps.gov.cn/n2254536/n4904355/c7787881/content.html
19 https://www.npa.go.jp/english/bureau/traffic/selfdriving.html
20 https://www.sciencedirect.com/science/article/pii/S0740624X21000137
21 https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/autonomous-driving-disruption-technology-use-cases-and-opportunities
22 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/#:~:text=It%20is%20necessary%20to%20hold,equity%2C%20and%20justice%20for%20all

COUNTRY SPOTLIGHT: BRAZIL

23 https://www.gov.br/cvm/en
24 https://www.gov.br/susep/pt-br
25 https://www.bcb.gov.br/en/about
26 R$ 18.5 billion as reported, converted to USD as of Nov 15, 2023
27 R$19 billion as reported, converted to USD as of Nov 15, 2023

28 R$25.7 billion as reported, converted to USD as of Nov 15, 2023
29 R$1.1 billion as reported, converted to USD as of Nov 15, 2023
30 R$242 million as reported, converted to USD as of Nov 15, 2023
31 R$5.5 billion as reported, converted to USD as of Nov 15, 2023
32 R$1.5 billion as reported, converted to USD as of Nov 15, 2023
33 https://www.mercadocripto.livecoins.com.br/corretoras
34 R$35 million as reported, converted to USD as of Nov 15, 2023
35 Month in which the most recent figures are available for this report
36 https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-0223.html
37 CNPJs according to reporting form
38 https://newsletter.brazilcrypto.io/p/episode-73-daniel-de-paiva-gomes#details
39 https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html
40 https://borainvestir.b3.com.br/
41 2.13 billion reais as of Nov 15, 2023
42 7 million reais as of Nov 15, 2023
43 9 million reais as of Nov 15, 2023
44 R$16.2 billion as reported, converted to USD as of Nov 15, 2023
45 R$10 billion as reported, converted to USD as of Nov 15, 2023
46 https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/criptoativos
47 R$15.4 billion as reported, converted to USD as of Nov 15, 2023
48 R$838 million as reported, converted to USD as of Nov 15, 2023
49 R$66,000 as reported, converted to USD as of Nov 15, 2023
50 R$21,000 as reported, conversted to USD as of Nov 15, 2023
51 R$72,000 as reported, converted to USD as of Nov 15, 2023
52 R$15,300 as reported, converted to USD as of Nov 15, 2023
53 R$500 million to R$1 billion as reported, conversted to USD as of Nov 15, 2023
54 https://www.prnewswire.com/news-releases/btg-pactual-launches-btg-dol-the-worlds-first-dollar-backed-stablecoin-from-a-bank-301789477.html
55 https://cointelegraph.com/news/brazil-rolls-out-blockchain-based-digital-id
56 The city of Buenos Aires in Argentina also announced a similar initiative that allows residents to access identity documents through a digital wallet: https://cointelegraph.com/news/buenos-aires-blockchain-based-digital-identity
57 https://www.ledgerinsights.com/brazil-central-bank-financial-regulator-blockchain-regtech/
58 https://exame.com/future-of-money/maranhao-primeiro-estado-rede-blockchain-brasil/
59 https://prefeitura.rio/cidade/carioca-podera-pagar-iptu-com-criptomoeda-em-2023/
60 https://www.cnnbrasil.com.br/economia/prefeitura-do-rio-autoriza-criptomoedas-para-pagamento-do-iptu-2023/
61 Mercosur also has 7 associate member states (Bolivia, Chile, Colombia, Ecuador, Guyana, Peru, and Suriname)
62 https://www.serpro.gov.br/menu/noticias/noticias-2020/aduanas-mercosul-conectadas-blockchain
63 https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/wco-wto-paper/2_brazil.pdf?la=en
64 https://www.digitalizetrade.org/projects/mercosur-blockchain-aeo-data-exchange
65 Refer to GSMI interactive regulatory map for full update of regulatory developments in Brazil
66 https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/brazil
67 https://finance.yahoo.com/news/brazils-central-bank-prepares-public-150826077.html
68 https://www.bcb.gov.br/en/about/bcbhashtag?modalAberto=about_agenda
69 https://www.bcb.gov.br/site/liftchallenge/en
70 https://cointelegraph.com/news/brazilian-cbdc-drex-official-name-and-logo

71 Therefore, while it was reported that a local developer discovered the Drex code could al low a central authority to freeze funds or reduce balances, it can be expected that regula tors are continuing to evaluate risks and establish safeguards.
72 https://www.gov.br/cvm/pt-br/assuntos/noticias/cvm-finaliza-primeiro-processo-de-admis sao-do-sandbox-regulatorio

DIGITAL IDENTITY

73 https://sovrin.org/principles-of-ssi/
74 Garber, E. and Haine, M. (eds) "Human-Centric Digital Identity: for Government Officials
75 OpenID Foundation, (September 25, 2023). https://legalinstruments.oecd.org/en/instru ments/OECD-LEGAL-0188
76 https://id4d.worldbank.org/guide/identity-lifecycle
77 https://docs.kantarainitiative.org/Blinding-Identity-Taxonomy-Report-Version-1.0.html
78 https://pages.nist.gov/800-63-4/
79 https://humancolossus.foundation/s/HCF-Overlays-Capture-Architecture-OCA-v1.pdf
80 https://www.w3.org/TR/vc-data-model/
81 https://www.iso.org/about-us.html
82 https://www.w3.org/about/
83 https://www.ietf.org/about/introduction/
84 https://openid.net/
85 https://trustoverip.org/about/about/
86 https://identity.foundation/
87 https://openwallet.foundation/
88 https://mydata.org/about/
89 https://kantarainitiative.org/about/
90 https://humancolossus.foundation/
91 https://essif-lab.github.io/framework/docs/essifLab
92 https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_ Digital_Cooperation_EN.pdf
93 https://www.theiia.org/en
94 https://iia.no/wp-content/uploads/2021/08/2021-Auditing-Identity-and-Access-Manage ment.pdf
95 https://www.isaca.org/resources/audit-programs/identity-and-access-management-au dit-program
96 https://www.stockholmresilience.org/research/planetary-boundaries.html
97 https://www.theguardian.com/environment/2022/aug/29/major-sea-level-rise-caused-by- melting-of-greenland-ice-cap-is-now-inevitable-27cm-climate

SUSTAINABILITY

98 https://assets.contentstack.io/v3/assets/blt4eb669caa7dc65b2/ blt7d329f330547f085/6537e909de6c442b29970d4d/Global_ESG_Q3_2023_Flow_Report_ final.pdf
99 https://treasury.worldbank.org/en/about/unit/treasury/ibrd/ibrd-green-bonds#:~:tex t=Since%202008%2C%20the%20World%20Bank,quality%20credit%20fixed%20in come%20product.

100 https://www.rba.gov.au/publications/bulletin/2023/sep/green-and-sustain able-finance-in-australia.html
101 History of climate finance evolution: https://unfccc.int/topics/introduc tion-to-climate-finance

102 Global Landscape of Climate Finance: A Decade of Data - CPI (climatepolicyinitiative.org)
103 Projects for financing a coal plant in Bangladesh, chocolate stores in Asia, and an airport expansion in Egypt have all been reported to the UN by developed countries as actions toward their national climate finance goals
104 https://www.rff.org/publications/journal-articles/comprehensive-evidence-implies-a-higher-social-cost-of-co2/
105 https://actuaries.org.uk/news-and-media-releases/news-articles/2023/july/04-july-23-emperor-s-new-climate-scenarios-a-warning-for-financial-services/
106 https://openknowledge.worldbank.org/server/api/core/bitstreams/5540a223-805b-5253-b0f3-3d72e78858ee/content#:~:text=In%20a%20recent%20paper%2C%20the%20IMF%20estimated%20that,sector%20grouping%20%28roads%2C%20electricity%2C%20and%20water%20and%20sanitation%29.4
107 https://www.imf.org/en/Blogs/Articles/2023/10/02/emerging-economies-need-much-more-private-financing-for-climate-transition
108 https://cepr.org/voxeu/columns/scaling-sustainable-finance-and-investment-global-south
109 https://www.fsb.org/wp-content/uploads/P231120.pdf "The difference between the nominal exposures of banking systems in these countries (blue bars in Graph 10, middle panel) and those weighted by the recipient countries' vulnerability to climate-related risks are relatively small, albeit with some exceptions. Cross-border bank lending might therefore play a role in diversifying, rather than amplifying, climate-related risks across a range of lending countries"
110 https://www.wfp.org/stories/5-facts-about-food-waste-and-hunger
111 https://www.feedingamerica.org/our-work/reduce-food-waste
112 https://www.carbonbrief.org/food-systems-responsible-for-one-third-of-human-caused-emissions/
113 https://www.cdp.net/en/articles/supply-chain/environmental-supply-chain-risks-to-cost-companies-120-billion-by-2026
114 https://www.carbontrust.com/value-chain-and-supply-chain-sustainability#:~:text=Up%20to%2090%25%20of%20an,downstream%20eg%20product%20use%20phase.
115 World Economic Forum. "Half of World's GDP Moderately or Highly Dependent on Nature, Says New Report," Press Release, 19 January 2020. https://www.weforum.org/press/2020/01/half-of-world-s-gdp-moderately-or-highly-dependent-on-nature-says-new-report
116 Simon-Kucher & Partners. "Recent Study Reveals More Than a Third of Global Consumers Are Willing to Pay More for Sustainability as Demand Grows for Environmentally-Friendly Alternatives," Press Release, 14 October 2021. https://www.businesswire.com/news/home/20211014005090/en/Recent-Study-Reveals-More-Than-a-Third-of-Global-Consumers-Are-Willing-to-Pay-More-for-Sustainability-as-Demand-Grows-for-Environmentally-Friendly-Alternatives
117 https://www.businessresearchinsights.com/market-reports/blockchain-supply-chain-finance-market-100093
118 https://miro.com/app/live-embed/uXjVMwv2SJs=/?boardAccessToken=xtg5sadEXp9JURDFR0lgK6wKXeq4SqwG&autoplay=true

119 https://www.cdp.net/en/articles/supply-chain/environmental-supply-chain-risks-to-cost-companies-120-billion-by-2026#
120 https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/accelerating%20winds%20of%20change%20in%20global%20payments/chapter-3-supply-chain-finance-a-case-of-convergent-evolution.pdf
121 https://www.bis.org/publ/bppdf/bispap113_m.pdf#:~:text=Financial%20market%20development%20in%20Malaysia%20after%20the%20Asian,dependent%20on%20the%20banking%20system%20for%20credit%20intermediation
122 CCUS is defined by the United Nations Economic Commission for Europe (UNECE) as "the process of capturing carbon dioxide (CO2) emissions from fossil power generation and industrial processes for storage deep underground or re-use"
123 Leading Oil & Gas players, such as ADNOC, have been early movers and have invested heavily in building the region's largest CCUS facilities, for example, Al-Reyadah established in 2016 and with a capturing capacity of 800,000 tons of CO2, and currently pursing one of its largest carbon capture projects in Habshan gas processing plant, that will result in additional storage of 1.5 million tones of CO2 per year.
124 https://www.ledgerinsights.com/eib-blockchain-digital-green-bond/
125 https://www.bis.org/about/bisih/topics/green_finance/green_bonds.html
126 https://www.ledgerinsights.com/hong-kong-green-bond-tokenized-blockchain/
127 https://www.ca-cib.com/pressroom/news/hong-kong-sar-issues-worlds-first-government-issued-tokenised-green-bond
128 https://cib.bnpparibas/supply-chain-finance-green-goals-for-payables/
129 https://www.cutter.com/article/forest-stewardship-council's-blockchain-verifying-material-trade-compliance-across-supply
130 https://bctriangle.com
131 https://rfid.averydennison.com/en/home/products-solutions/iot/faq-atma-io-hedera.html
132 https://www.hbarfoundation.org/blog-post/fresh-supply-co-fsco-payment-trigger-api-connects-hedera-to-mastercard-network
133 https://www.ukrinform.net/rubric-society/3636117-unhcr-launches-aid-payments-to-ukrainians-using-blockchain-technology.html#:~:text=UNHCR%20launches%20aid%20payments%20to%20Ukrainians%2%200using%20blockchain,is%20reported%20on%20the%20UNHCR%20website%2C%20Ukrinform%20reports.
134 https://www.esginvestor.net/live/asian-banks-underestimating-physical-climate-risk-aigcc/
135 https://actuaries.org.uk/news-and-media-releases/news-articles/2023/july/04-july-23-emperor-s-new-climate-scenarios-a-warning-for-financial-services/
136 https://www.gdf.io/wp-content/uploads/2022/11/Guidance-on-ESG-Reporting-for-Digital-Assets.pdf
137 South Pole & CCRI. Accounting for Cryptocurrency Climate Impacts. April 2022.
138 https://www.theacmf.org/images/downloads/pdf/ASEAN%20Transition%20Finance%20Guidance%20Version%201%20-%20FINAL%2017%20Oct%202023.pdf

SUPPLY CHAIN

139 (Harrison et al. 2014)
140 (Harrison et al. 2014)
141 Lacity, M., Schuetz, S., and Steelman, Z. (2023). IT's a Matter of Trust. University of Arkansas white paper: https://walton.uark.edu/departments/information-systems/files/bcoewhitepaper2023post.pdf
142 2022 Deloitte Report
143 https://www.computerworld.com/article/3454336/walmart-launches-world-s-largest-block

chain-based-freight-and-payment-network.html (Computerworld, 2019) - “Logistics and transportation is an $8 trillion industry and as much as $140 billion per day can be tied up in disputes or settlements between supply chain participants, according to Laurie Tolson, chief digital officer of GE Transportation.”

144 https://www.statista.com/chart/27289/global-trade-volume-with-counterfeit-goods-compared-to-gdp-of-selected-countries-regions/

145 https://www.statista.com/chart/30067/worldwide-counterfeit-pharmaceuticals-incidents/

146 2022 Deloitte report

147 Global Express – [source]

148 https://www.w3.org/TR/prov-o/

149 Key Trade Documents and Data Elements paper: https://www.dsi.iccwbo.org/_files/ugd/8e49a6_2d93b2f219cf404ab91bafd028e31fcc.pdf

150 Trust in Trade paper: https://www.dsi.iccwbo.org/_files/ugd/8e49a6_5a75a77950d7474da772bf9cfc2d985b.pdf

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

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

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland