GBBC
Global Blockchain
Business Council

STANDALONE REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 5.0
DECEMBER 2024

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

GBBC GSMI 5.0

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

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

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland

GSMI 5.0 IN-DEPTH REPORT

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

EXECUTIVE SUMMARY

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

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

PUTTING THE AI EXPLOSION INTO PERSPECTIVE

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

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

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

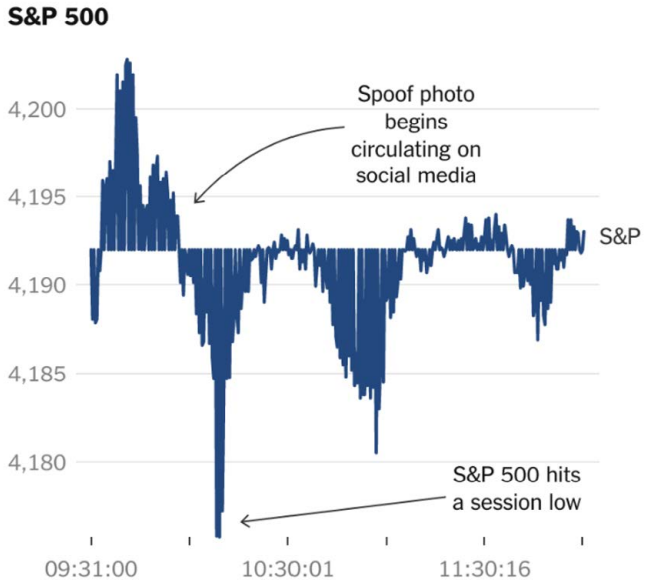
When AI solutions can maximize our possibilities to carry out and achieve any task, the point may not be to maximize activity and functionality alone, but to do so in the right way. Attention to responsible AI, from its very design and throughout its developments, can avoid significant monetary and reputational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

Better solutions & worse problems?

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

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

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



Source: Sentieo/AlphaSense • By The New York Times

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

Data Provenance

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

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

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

Data Quality:

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

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

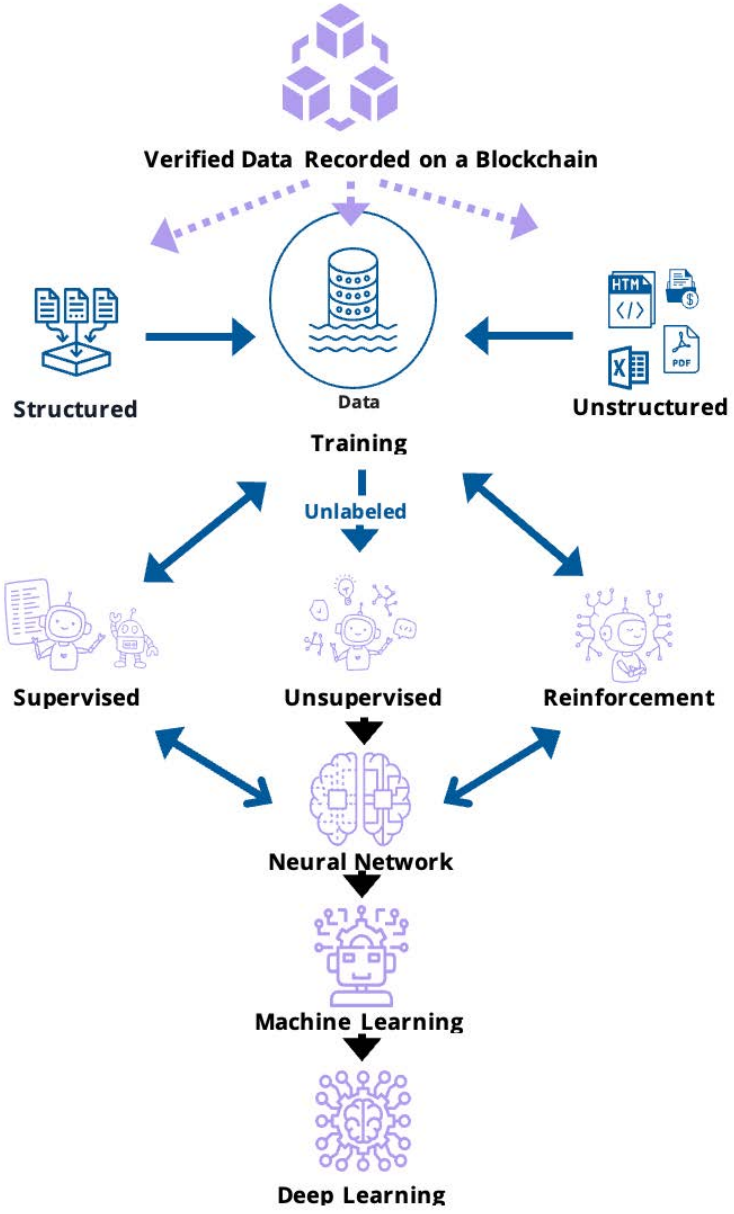
Furthermore, data quality can be regarded as a spectrum, starting with direct from source vs. interpreted data, 3rd party data, synthetic data, and beyond. Models are likely to be most reliable when they minimize the low-quality data used in training. This enables a future where humans become extremely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

Data Privacy & Security

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

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

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



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

Transparency on Processes & Outcomes

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

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

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

USE CASES OF BLOCKCHAIN & AI

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

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

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

Figure 3: Decentralized AI

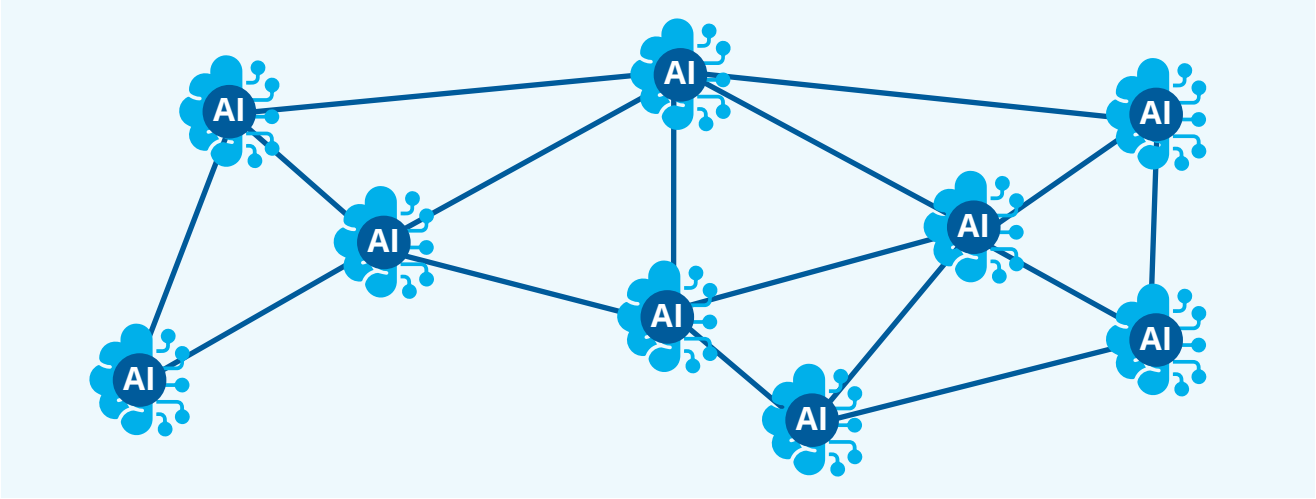


Table 1: Use Cases of Blockchain & AI Convergence

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

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

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

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

Ethical Considerations

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

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

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

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

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

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

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

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

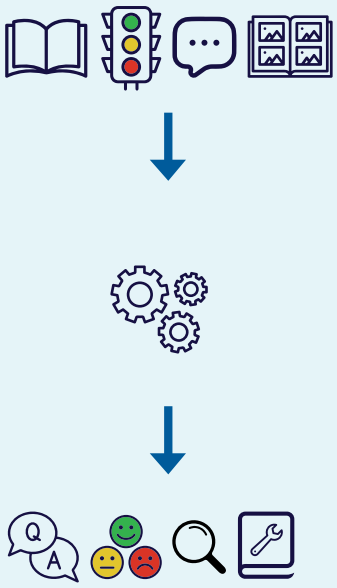
- Governance & Accountability: Trust is fundamental for AI, alongside a notion of a dynamic social compact that adjusts with new issues at the technology progresses. Trust frameworks should be founded upon governance and interoperability considerations. They should reflect a broad understanding of the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

FOUNDATION MODELS

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

Figure 3: How Foundation Models Work

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



Various outputs

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

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

Table 2: Overview of Selected Foundation Models

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

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

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

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

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

Blockchain can optimize foundation models

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

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

Blockchain can benefit foundation models in the following ways:

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

Foundation Models as Digital Assets

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

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

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

Importance of Standards

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

Table 3: Considerations for AI Standards

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

Table 4: Progress on Global AI Standards

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

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

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

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

AI REGULATION

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

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

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

Table 4: Regulatory Developments in Selected Jurisdictions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Status: Regulatory developments in discussions

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

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

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

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

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

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

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

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

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

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

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

FUTURE OUTLOOK

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

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

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

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

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

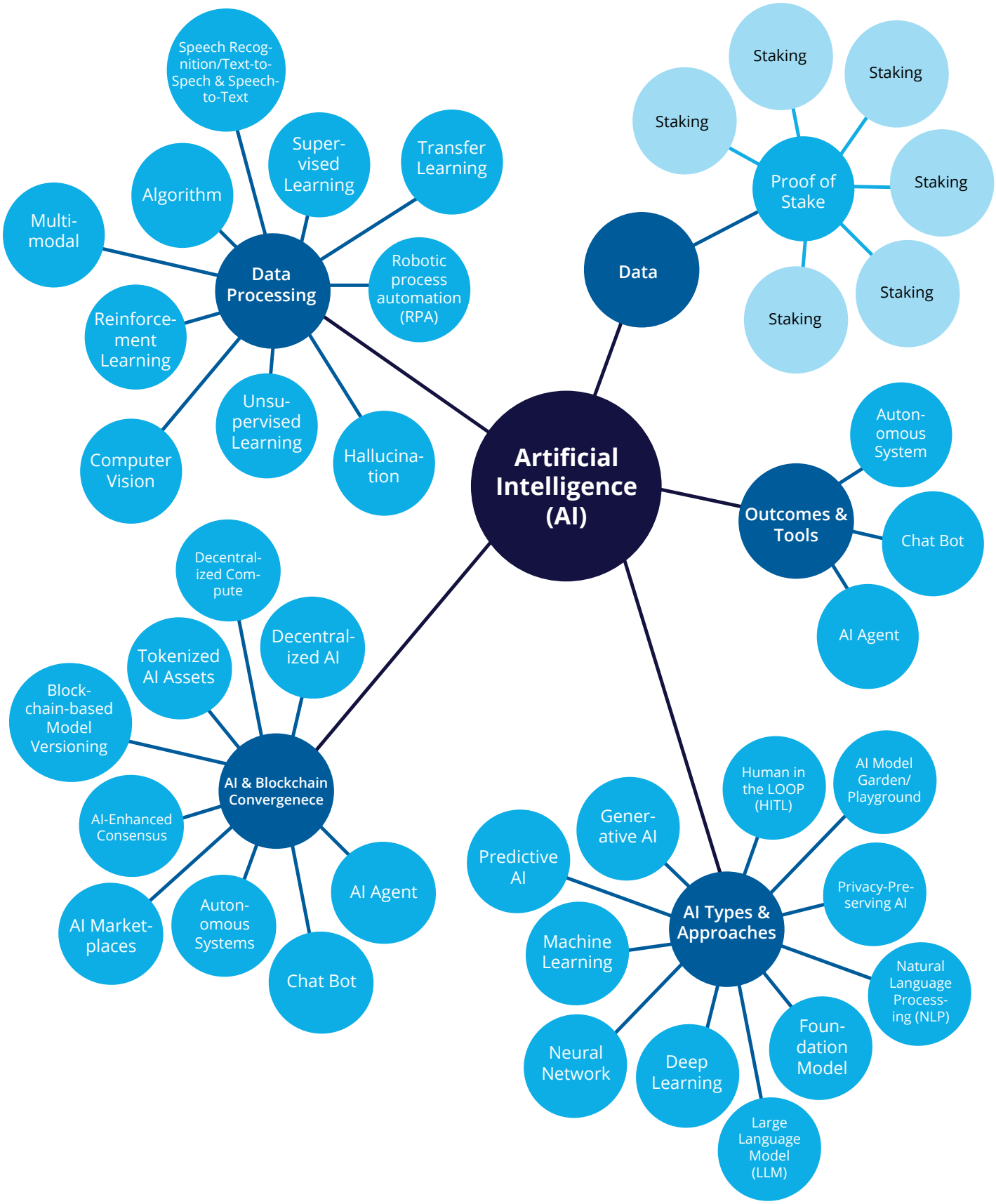
1. **Backward vs. Forward Looking AI:** When data is generated after events and circumstances have occurred, as is often the case, AI can become more backward-looking than forward-looking. How can we ensure that AI training is designed to anticipate future outcomes rather than merely reflecting past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

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

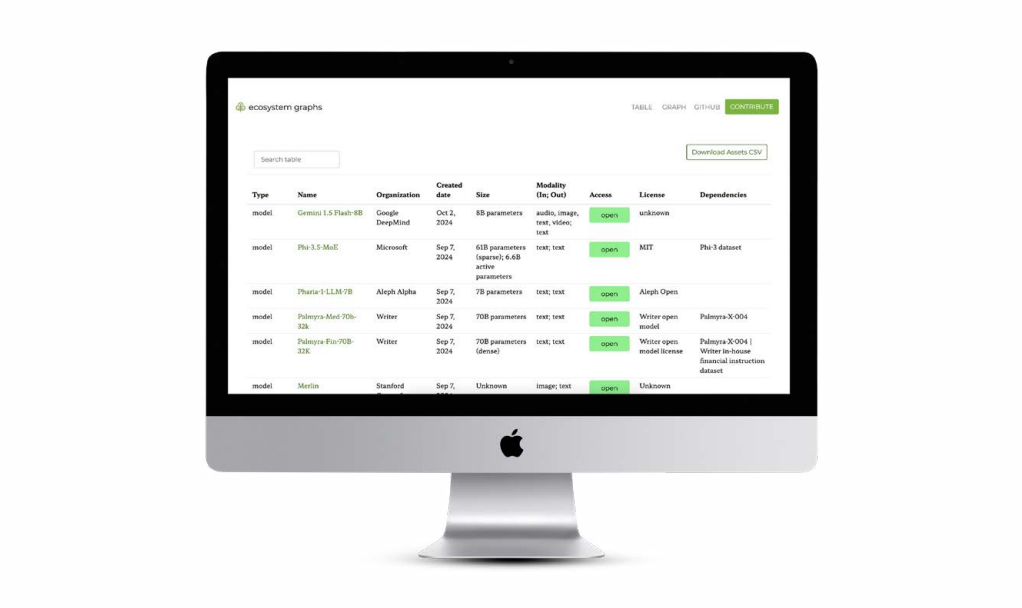
In the realm of AI, errors often arise from misinterpretations or conclusions drawn out of context. Only humans possess lived experiences—rich, subjective insights that serve as the ground truth for AI models. By digitizing our physical and lived experiences, we can provide AI with reliable data to stay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

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

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



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



Annex 3: Considerations for a Risk Assessment Approach Model

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

ENDNOTES

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

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

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

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland