THE DIGITAL ECONOMIST

Date of Publication | July 2, 2026

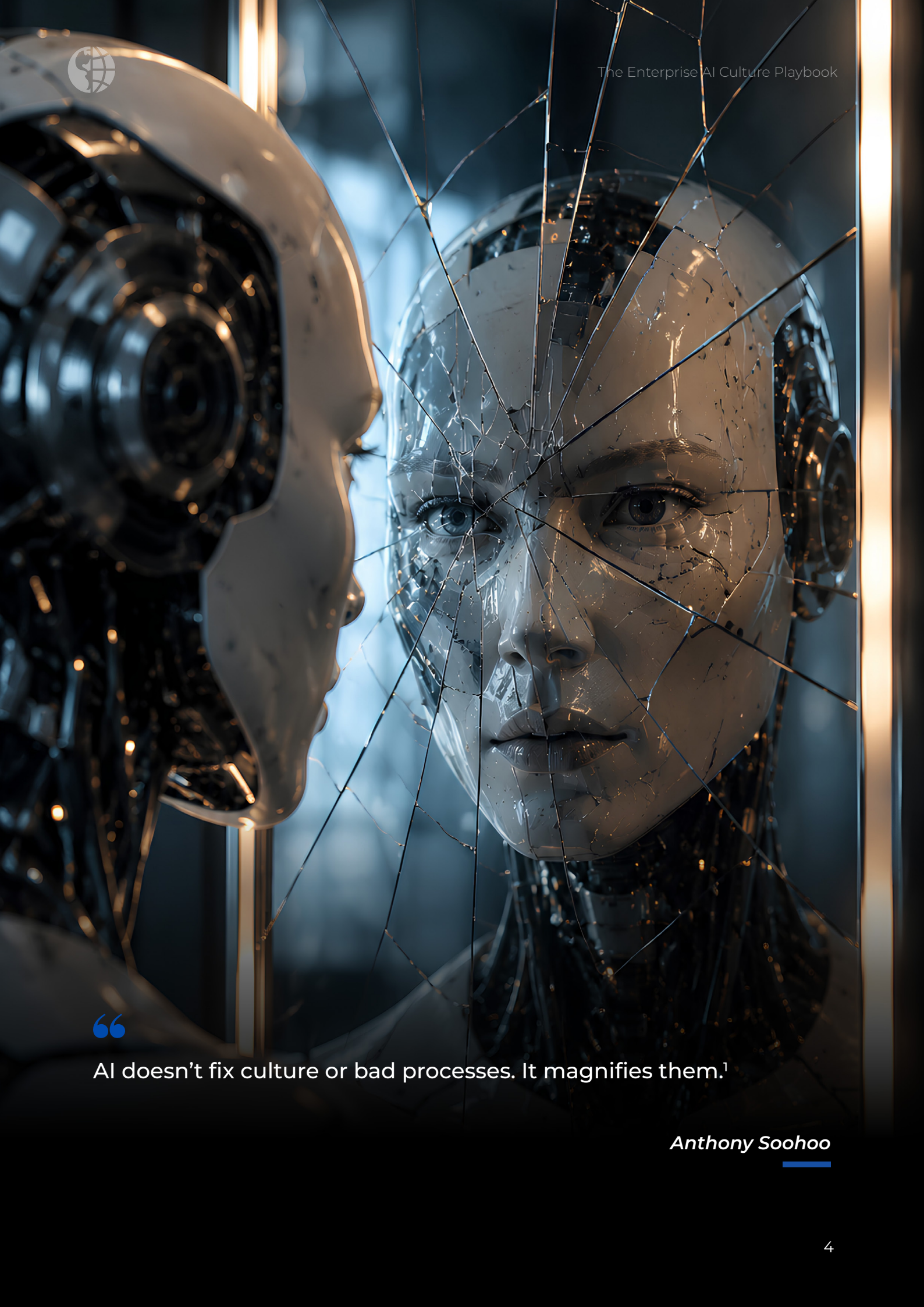
Position Paper

Dr. Maria Azua Himmel

AI and Blockchain: Balancing Risk, Value, and Accountability

AI GOVERNANCE | ENTERPRISE RISK | RESPONSIBLE INNOVATION

Table of Contents



> AI doesn’t fix culture or bad processes. It magnifies them.[1]

Anthony Soohoo

Executive Summary

Artificial intelligence and blockchain are reshaping how organizations make decisions, execute transactions, and establish trust. Together, these technologies create new opportunities for automation, transparency, and efficiency while introducing new forms of operational, governance, and accountability risk. This paper examines the systemic risks associated with current AI systems and explores governance approaches that support accountable oversight, sustainable value creation, and responsible deployment while preserving human agency.

This convergence is being driven by growing demand for immutable records, trusted verification, and distributed identity frameworks capable of securely enabling AI-driven automation. AI systems built on transformer architectures and large language models now demonstrate extraordinary capabilities in pattern recognition, insight generation, decision support, and autonomous execution. However, these systems still lack native mechanisms for immutable authentication, verifiable identity, and persistent auditability. Blockchain infrastructure provides capabilities AI inherently lacks, including immutable records, cryptographically verifiable identities, decentralized trust, and persistent audit trails. Tokenized execution layers can then leverage these capabilities to support real-time transactions, programmable controls, and transparent accountability. Together, they compress the distance between decision, execution, and accountability.[2, 3, 4, 5]

This compression creates a significant opportunity. AI can scale expertise, improve prediction, reduce process latency, and expand access to highly specialized capabilities. Blockchain can enhance transparency, strengthen auditability, support distributed verification, and enable new models of digital identity and asset ownership. In combination, these technologies can facilitate more efficient payments, more reliable recordkeeping, more secure autonomous-agent activity, stronger fraud detection, more inclusive financial infrastructure, and emerging tokenized asset ecosystems.[6, 7, 8]

The same convergence also introduces a new class of risk. Traditional governance models assume organizations have time to review, approve, reconcile, and remediate decisions. AI- and blockchain-enabled systems reduce those buffers. AI can generate actions at machine speed while blockchain-based rails can execute those actions with finality. As a result, the governance shifts from whether the organization can review decisions after the fact to whether it has embedded the right controls before automated action occurs.[9. 10. 11, 12]

The central thesis of this paper is that enterprises are entering an environment of accountability without direct control. Boards, CEOs, and senior executives remain accountable for outcomes produced by systems they may not fully observe, interpret, or stop in real time. This shift demands a different governance architecture, one that integrates data governance, model governance, identity management, permissioning, execution controls, auditability, and continuous monitoring.[13, 14, 15, 16]

The interviews conducted for this paper reinforce that this convergence is already underway. Anthony Soohoo, Chief Executive Officer of MoneyGram, emphasizes that AI magnifies existing culture and process quality rather than correcting underlying deficiencies. Kristen Schmidt, Chief Executive Officer and Co-Founder of UtopIQ, identifies unsecured AI infrastructure, inadequate agent-intake governance, the absence of immutable audit layers, overdependence on AI, and quantum-era risk as critical issues. Ryan McManus, independent director and technology governance advisor, underscores that innovation and risk management cannot be separated and argues that confining AI oversight to the audit committee creates structural governance risk. Phil Venables, a cybersecurity and enterprise risk leader, expands the discussion to include second-order effects, systemic dependencies, agent identity, sector-specific regulation, and the need to retool enterprise systems for an environment defined by speed and automation.[17, 18, 19, 20]

The paper concludes that responsible experimentation is essential. The objective is not to slow innovation but to enable it through a control architecture strong enough to sustain it. Organizations that lead in this next era will not be those that deploy AI or blockchain fastest in isolation. They will be those that successfully integrate speed, control, and trust into a coherent operating model.

> Every AI agent needs an identity, defined privileges, and an immutable record of its actions.[21]

> The real risks are not AI itself. They are the second-order effects from how businesses and society transform around its use.[22]

Phil Venables

1.

Framing the Convergence

The convergence of artificial intelligence and blockchain is one of the most consequential structural shifts facing modern enterprises. These technologies are no longer developing along separate innovation tracks. They are increasingly operating as complementary components of a new digital operating model: AI generates decisions and blockchain-based infrastructure executes, verifies, and records those decisions in near real time.[23, 24, 25]

Historically, enterprise systems were designed around separation. Decision-making, authorization, execution, settlement, reconciliation, and reporting occurred in distinct operational stages. In many organizations, this separation was not merely procedural but architectural. Enterprises intentionally fragmented infrastructure, duplicated systems, and compartmentalized processes to reduce correlated failure risk and limit the potential "blast radius" of cyberattacks or operational compromise. In some cases, this created a form of resilience through operational separation and infrastructure diversity. While these architectures introduced friction and operational complexity, they also created time for organizations to validate assumptions, escalate anomalies, review exceptions, correct errors, and reconcile accounts before outcomes became final. In highly regulated industries, these control windows became embedded within the implicit governance architecture.[26, 27, 28]

As AI-and blockchain-driven automation compress traditional control windows, market expectations for speed, transaction processing, and operational execution continue to accelerate. Organizations are increasingly deploying AI agents across financial transactions, operational services, and infrastructure environments to improve efficiency, responsiveness, and scale. However, many of these systems are being implemented without embedded trust, identity, and governance mechanisms capable of operating at machine speed. This creates the potential to amplify systemic and operational risk precisely as organizations become more dependent on autonomous decision systems.

For example, an AI system may detect a suspicious payment pattern, determine that a transaction exceeds established risk thresholds, initiate a hold on the transaction, notify relevant parties, and record each action through a blockchain-based audit infrastructure—all within seconds. The governance challenge is that the entire sequence of detection, decision, execution, and accountability may occur before a human has the opportunity to intervene. This example illustrates why AI-driven automation increasingly requires complementary trust infrastructure. As decisions and execution compress into machine-speed workflows, organizations need identity, permissioning, auditability, and tamper-resistant recordkeeping capable of operating at the same speed. Blockchain-based trust infrastructure can help provide those capabilities, making it increasingly relevant wherever autonomous systems are authorized to act, transact, and generate material operational or financial outcomes.[29, 30, 31]

AI systems can analyze data, generate recommendations, trigger actions, and increasingly operate through autonomous agents. Blockchain and tokenized infrastructure can execute transactions, transfer value, maintain immutable records, and provide distributed verification at speeds that bypass traditional layers of intermediation. When combined, the result is a tightly coupled system in which decision, execution, verification, and evidence of execution occur almost simultaneously rather than through sequential operational stages.[32, 33, 34]

This convergence creates a new accountability challenge for boards and executive teams. Directors and senior leaders remain responsible for enterprise outcomes even when those outcomes are generated by systems operating faster than human review and may not be fully explainable in real time. Governance models therefore cannot rely exclusively on retrospective review and periodic oversight processes. Oversight must increasingly evolve toward architecture-level governance, embedded controls, continuous monitoring, and resilient operational design.[35, 36, 37]

Anthony Soohoo captured the organizational dimension of this challenge in a simple but powerful observation.

This insight is central to the paper. AI does not automatically improve enterprise quality. It accelerates and scales the existing quality of data, processes, controls, culture, and leadership judgment. If a process is strong, AI may make it faster, more adaptive, and more scalable. If a process is weak, AI may amplify those weaknesses with equal speed. When those accelerated processes are connected to blockchain execution rails, the resulting outcomes may be externalized immediately and recorded permanently. [38]

The convergence also creates tension between AI's probabilistic decision-making and the corporation's need for deterministic accountability, explainability, and execution. AI systems make inferences based on continuously evolving data, statistical patterns, and probabilities. Their outputs may vary depending on training data, context, model drift, or changing environmental conditions. This lack of deterministic consistency creates challenges for auditability, repeatability, and accountability, particularly in highly regulated financial and operational environments where reconciliation and evidentiary integrity are fundamental. Blockchain systems, by contrast, execute predefined rules and record outcomes with finality. AI introduces adaptability while blockchain introduces immutability through distributed ledger architecture. Their combination can create extraordinary efficiency, but it can also produce systems that are unforgiving when data inputs, logic, permissions, or governance controls are flawed.[39, 40, 41]

As Phil Venables emphasized in our interview, mitigating these risks requires stronger identity and accountability frameworks for autonomous systems. His observation highlights an important shift in how organizations must think about AI risk.

The most significant governance challenges may not arise from the performance of a single model or system but from the broader organizational, operational, and market changes that occur as businesses increasingly depend on AI-driven automation. Understanding this distinction is essential to separating direct technology risks from the larger consequences of technology adoption at scale.

This distinction is critical for governance. First-order risks include bias, cyber vulnerabilities, hallucinations, unauthorized access, model drift, and operational errors. Second-order risks emerge when business processes, customer expectations, market structures, workforce development, and enterprise dependencies begin restructuring around AI-driven systems. The most material risks may not arise from a single model failure but from the emergent behavior of many agents, workflows, and interconnected infrastructures operating simultaneously at scale.[42, 43]

For boards and CEOs, this requires a more integrated oversight lens. AI cannot be governed solely as a model-risk issue. Blockchain cannot be governed solely as a digital asset issue. Together, they require an enterprise architecture perspective that connects fiduciary oversight, technology strategy, cybersecurity, operational resilience, compliance, disclosure, and human capital.[44, 45, 46, 47]

The objective of this paper is not to argue that convergence should be slowed. The convergence of AI and blockchain is already underway and will likely accelerate. The strategic question is not whether organizations should adopt these technologies but whether they can implement them responsibly and govern them effectively. The value created by this convergence is too significant to ignore or postpone. AI and blockchain can improve trust, reduce friction, enhance financial inclusion, accelerate security operations, enable programmable money movement, support resilient identity frameworks, and create more transparent records of automated activity. The challenge is whether organizations can build the governance architecture required to capture these benefits safely and sustainably.[48, 49, 50]

The central proposition is therefore clear: responsible convergence requires speed with control. Boards and executive teams should not view innovation and risk management as competing agendas. They should view governance as the architecture that enables innovation to scale safely.

> Current transformer models are fundamentally statistical systems.[51]

Phil Venables

2.

AI Decision Systems: Intelligence Without Full Explainability

Artificial intelligence has advanced rapidly because modern models can process vast quantities of data, identify relationships across complex inputs, establish patterns, and generate outputs that approximate reasoning across many domains. Transformer architectures, introduced in the foundational paper “Attention Is All You Need” in 2017, made it possible to scale pattern recognition and language-based inference through neural network architectures capable of processing entire sequences in parallel. This breakthrough now underpins many advanced AI systems.[52]

In enterprise settings, AI is increasingly used for fraud detection, credit and risk analysis, customer support, software development, cybersecurity monitoring, claims processing, supply chain forecasting, and operational optimization. These deployments create real value by allowing organizations to scale expertise, accelerate analysis, and improve consistency across large operating environments.[53, 54]

Yet the governance challenge begins with understanding what AI is and what it is not. Modern generative AI systems are powerful, but they remain probabilistic. They produce outputs based on relationships derived from training data and model architecture. They do not possess human judgment, business accountability, ethical reasoning, or contextual understanding in the way experienced professionals do.[55, 56]

Phil Venables stated the limitation directly: that limitation does not diminish the usefulness of AI. It clarifies the control requirement. The issue is not whether AI can be valuable. It clearly can. The issue is whether organizations understand where AI is reliable, where it is uncertain, and where it should not be authorized to act without additional safeguards.[57, 58, 59]

Anthony Soohoo frames one of the central tensions in AI governance as the widening gap between computational power and judgment. AI systems can process information, detect patterns, and generate outputs at extraordinary scale and speed, yet they still lack the contextual awareness, discernment, and practical judgment required for accountable decision-making in complex real-world environments.[60]

This observation highlights one of the most important governance asymmetries in AI deployment. Computational capability can operate at a scale far beyond human capacity while judgment may remain immature, context-dependent, or misaligned with enterprise objectives. A model may process more data than any human team, yet still fail to understand materiality, customer impact, ethical boundaries, regulatory sensitivity, or reputational consequences.[61, 62]

One of the central governance challenges associated with modern AI systems is the growing gap between computational capability and organizational accountability. Current large language models and transformer-based architectures operate through probabilistic inference, pattern recognition, and statistical prediction rather than deterministic reasoning or human judgment. As AI systems become increasingly capable of generating recommendations, making decisions, and executing actions, they do not acquire the judgment, responsibility, or fiduciary obligations that accompany human authority.

Figure 1 visualizes this governance gap and highlights why organizations must implement additional controls, oversight mechanisms, and accountability frameworks as AI adoption scales. As organizations increasingly rely on autonomous AI agents, governance architectures must therefore compensate through continuous monitoring, calibration, validation, drift detection, permissioning, and embedded oversight mechanisms designed to identify bias, operational anomalies, and model degradation before errors propagate at scale.

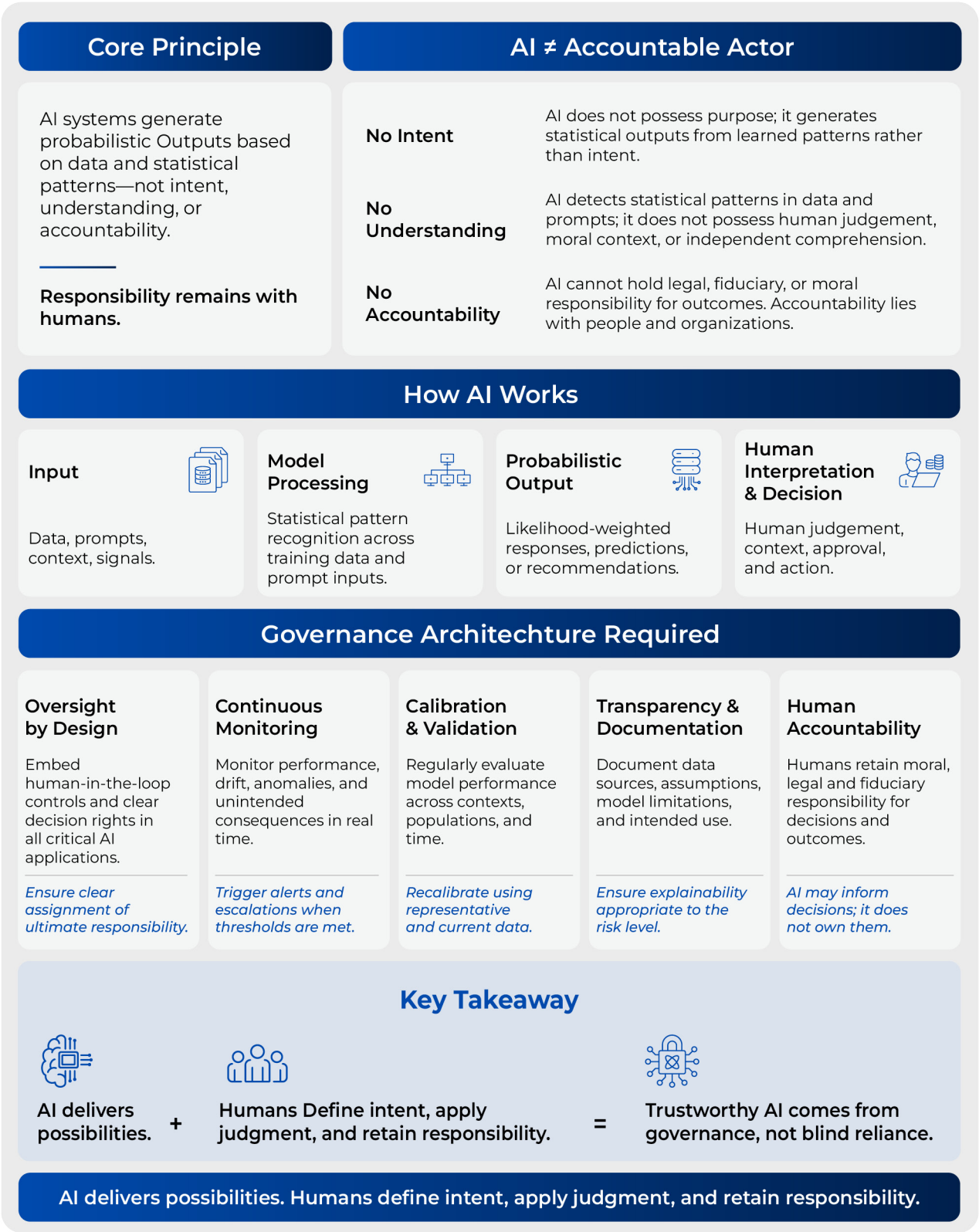


Figure 1. AI systems generate probabilistic outputs without agency or accountability, requiring governance, monitoring, calibration, and human oversight to ensure responsible use.

Three AI risks are especially relevant to the convergence with blockchain. The first is data dependency. AI systems inherit the quality, bias, completeness, and representativeness of their data. If training data reflects historic bias, incomplete controls, weak labels, or flawed business assumptions, the model may reproduce and amplify those weaknesses. This is particularly consequential in regulated environments such as financial services, insurance, healthcare, and energy.[63, 64, 65, 66]

The second is opacity. Many AI models cannot provide a simple, deterministic explanation for why a specific output was generated. Interpretability tools can help, but they do not fully eliminate the black-box concern. In a traditional advisory workflow, opacity may be mitigated by human review. In an autonomous workflow, opacity becomes more serious because the system may act before a human can interrogate the logic.[67, 68, 69]

The third is drift. AI systems can degrade as the environment changes. Market conditions, customer behavior, adversarial tactics, regulatory expectations, and data patterns all evolve. A model that was valid at deployment may become less reliable over time. This is why AI governance cannot be a onetime approval event. It must include ongoing monitoring, validation, recalibration, and escalation.[70, 71]

AI Capability	Associated Governance Challenge
Pattern recognition and prediction at scale	**Data dependency:** Biases may be amplified when training data is incomplete, unrepresentative, or of poor quality.
Rapid decision-making and automation	**Opacity:** Limited transparency and explainability of model outputs.
Continuous adaptation to changing conditions	**Model drift:** Performance may degrade over time as data and environments change.

Table 1. Strengths and Governance Challenges of Modern AI Systems

> Defenders have a structural advantage because AI performs best with context and data, and defenders have that context while attackers do not.[72]

Phil Venables

AI also changes the cybersecurity landscape. Venables observed that AI benefits both attackers and defenders, but that defenders may hold a long-term structural advantage because they have context and data.

This matters for boards because it reframes AI not only as a risk to be contained but also as a capability to be governed and deployed in defense of the enterprise. AI can identify vulnerabilities at scale, support red teaming, monitor anomalous behavior, assess software supply chains, and accelerate remediation. The governance question is how to ensure that these tools are themselves secure, validated, permissioned, and auditable.[73, 74]

Anthony Soohoo warns that AI does not repair flawed processes or weak operating models. When applied to an environment with poor controls, inefficient workflows, or unresolved structural problems, AI is more likely to accelerate and amplify those weaknesses than to correct them.[75]

This principle should be treated as a board-level deployment test. Before AI is placed into a workflow, management should be able to explain whether the underlying process is sound, whether the data is governed, whether decision rights are clear, and whether exceptions can be detected and escalated. AI should not be used to automate ambiguity. It should be used to scale disciplined processes.[76, 77, 78]

The implications for governance are clear. Boards and executives should require an inventory of AI use cases, classification by materiality, documented data lineage, model validation, human oversight thresholds, incident response protocols, and ongoing performance monitoring. In high-impact environments, AI governance should be connected to enterprise risk management, cybersecurity, compliance, audit, and strategy.[79, 80, 81, 82]

AI decision systems therefore create the first half of the convergence story. They determine what action should be taken. Blockchain and tokenized infrastructure increasingly determine how that action is executed, recorded, and settled.

> Blockchain allows for a more transparent ledger of how machines have made decisions and the logic which was involved in those decisions.[83]

> Innovation and risk management are not two separate things. The faster innovation moves, the more integrated governance must become.[84]

Ryan McManus

3.

Blockchain and Tokenized Rails: Execution Without Friction

Blockchain technology changes the execution side of the enterprise equation. At its core, blockchain is a distributed ledger that allows multiple participants to maintain a shared, tamper-resistant record of transactions. In financial and operational systems, this can reduce reconciliation friction, create stronger audit trails, and enable transactions to settle faster than legacy infrastructure permits.[85]

Tokenization extends this model by representing assets, obligations, rights, credentials, or payment instruments in digital form. Tokenized rails can support stablecoins, tokenized deposits, digital identity, programmable payments, and digital representations of financial and nonfinancial assets. These developments are particularly relevant for cross-border payments, custody, settlement, collateral management, and automated compliance.[86, 87, 88]

The strategic appeal is straightforward. Blockchain can improve transparency, reduce dependence on intermediaries, enable programmability, and create a persistent record of actions. In global payments, these capabilities can reduce cost, improve speed, and expand access. In enterprise records, they can improve auditability and provenance. In identity, they can support the verification of human and machine actors.[89, 90, 91]

Ryan McManus captured the transparency value of blockchain in the context of machine-driven systems, emphasizing that trust in autonomous systems ultimately depends on the ability to verify and scrutinize their actions.

The point is not that blockchain explains AI in full. It does not. The value is that blockchain can help create a verifiable record of actions, permissions, identities, and execution history. In an environment of AI agents, such records become essential for auditability and accountability.[92, 93, 94]

The same properties that create value also change the risk profile. Traditional financial systems often contain delays that are viewed as inefficiencies, but those delays also serve as buffers. They allow organizations to validate instructions, identify anomalies, correct errors, manage liquidity, and reconcile positions. Real-time blockchain-based execution reduces those buffers. Once execution occurs, remediation may be more difficult, more expensive, or reputationally damaging.[95, 96]

This risk becomes particularly significant in stablecoins and tokenized financial infrastructure. Traditional financial systems contain operational delays, reconciliation windows, and human intervention points that help institutions identify errors, contain liquidity stress, and interrupt cascading failures before settlement becomes final. Tokenized settlement rails compress or eliminate many of those control windows. When AI-driven systems are connected directly to real-time payment and settlement infrastructure, erroneous decisions, liquidity shocks, or flawed automated actions can propagate across interconnected systems at machine speed before organizations have time to intervene. The governance challenge is therefore not only operational efficiency, but whether enterprises can maintain sufficient controls, resiliency, and human oversight in environments where execution finality occurs almost instantaneously. Regulators, including the Financial Stability Board and the Bank for International Settlements, have emphasized the importance of governance, resilience, and systemic risk controls in digital settlement infrastructure.[97, 98]

Blockchain should therefore be understood as more than an asset class or speculative technology. In appropriate architectures, it can function as execution and trust infrastructure. Its relevance to AI comes from tamper-resistant records, identity, permissioning, distributed verification, and auditability. While these capabilities are not a substitute for sound governance, they can strengthen the control environment for autonomous AI agents and provide a stronger foundation for transparency, accountability, and trust. [99, 100]

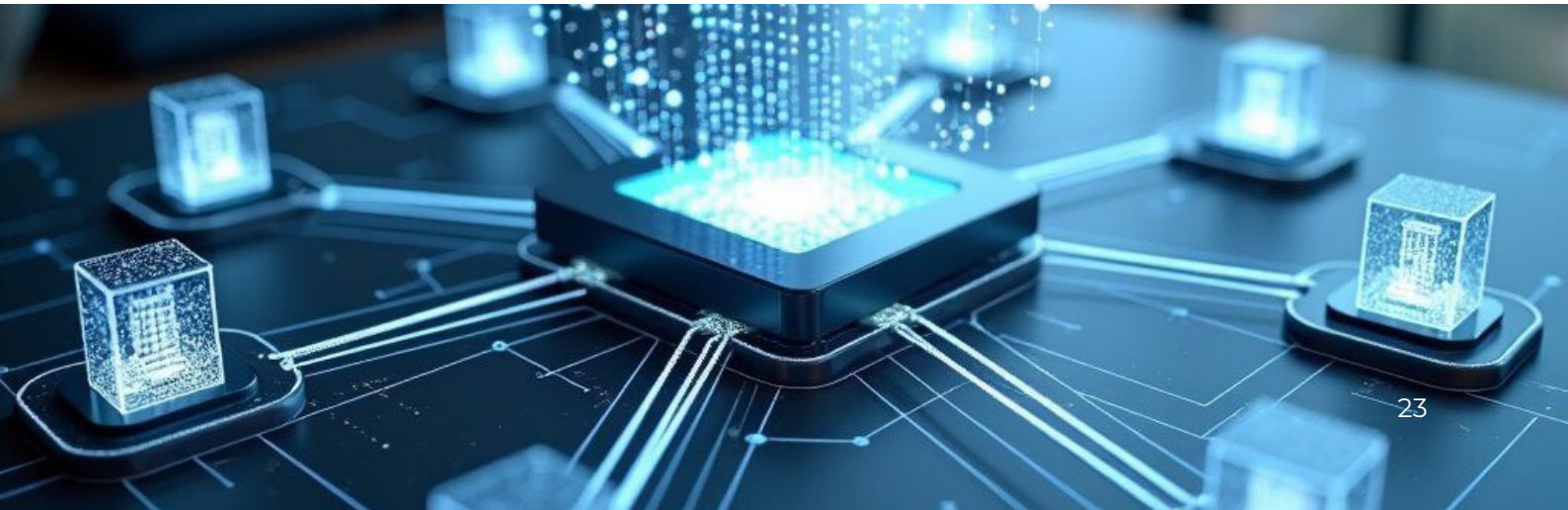
Ryan McManus emphasized that organizations frequently treat innovation and risk management as competing priorities rather than integrated governance responsibilities. In practice, the speed and scale of AI-driven transformation make that separation increasingly unsustainable. Governance structures that isolate innovation from enterprise risk oversight may unintentionally create blind spots precisely where systemic exposure is growing fastest. [101] McManus cautions against treating innovation and oversight as separate tracks.

This observation is particularly important for blockchain programs. If tokenized rails are built as innovation experiments without an accompanying risk architecture, they may scale faster than governance can adapt. Conversely, when they are designed with embedded permissions, controls, monitoring, and auditability, they can provide a foundation for more responsible automation.[102, 103, 104]

Blockchain also introduces a role for decentralized identity and verifiable credentials. Dr. Nikhil Varma's work on blockchain-based identity for enterprise AI is particularly relevant in this context. His analysis highlights how decentralized identifiers, verifiable credentials, and blockchain-backed identity frameworks can help address the trust gap in enterprise AI by establishing who or what is authorized to act, under what authority, and with what mechanisms for accountability.[105]

This identity function is critical because AI agents are not ordinary software scripts. They may be delegated authority, granted system privileges, authorized to execute transactions, and permitted to interact autonomously across distributed enterprise environments. Without strong identity frameworks, role-based access controls, and immutable audit trails, organizations may struggle to determine whether actions were appropriate, who authorized them, how decisions propagated across interconnected systems, and where accountability should ultimately reside.[106, 107]

Blockchain and tokenized rails therefore represent the second half of the convergence story. They determine how decisions are executed, recorded, and validated. When connected to AI decision systems, they create what may be the most important section of this paper: the synergy layer, where machine intelligence meets programmable execution.



> Modern digital systems are being reengineered for speed, where decision-making and execution occur in tightly coupled cycles.[108]

Phil Venables

4.

The Synergy Layer: Where Decision Meets Execution

The convergence of AI and blockchain becomes most consequential at the interaction layer, where AI-driven decisions are executed directly on blockchain-based infrastructure. This is not merely the integration of two technologies. It represents a structural change in enterprise architecture. AI determines what action should be taken. Blockchain determines how, when, and with what evidence that action is executed.[109, 110, 111]

In traditional systems, decision-making and execution are separated by human authorization, process controls, settlement windows, and reconciliation procedures. In converged systems, these stages can collapse into an event-driven sequence. In practice, an AI agent ingests real-time data and generates a recommendation or decision; identity, permissioning, and policy controls validate whether the action is authorized; a transaction, workflow, or smart contract is executed; and the resulting activity is recorded through a blockchain-based trust infrastructure. The entire cycle can occur within seconds, dramatically compressing traditional control windows and reducing opportunities for traditional human intervention.[112, 113, 114]

This reengineering for speed is strategically powerful. It can reduce friction, increase responsiveness, improve customer experience, accelerate security operations, and support new financial products. It also changes the locus of control, shifting decision-making authority away from traditional human operators and toward distributed autonomous systems. As decision-making and execution increasingly occur at machine speed, governance models that rely on human intervention between operational stages become increasingly impractical and ineffective. Machine-speed systems require control within the stages themselves, and controls architected for constant automated supervision to ensure any variance on expected results or behavior is highlighted immediately rather than after the system has already created a liquidity or operational incident.[115, 116]

Kristen Schmidt identifies a growing architectural risk in enterprise AI adoption: organizations are increasingly deploying AI agents without the governance structures necessary to manage them safely. In many cases, deployment occurs without formal intake processes, preventative permissioning controls, or immutable audit mechanisms, creating gaps in oversight, accountability, and operational resilience. As AI agents assume greater autonomy, those gaps can quickly become material governance and control failures.[117]

The risks identified by Schmidt highlight the central governance challenge of the synergy layer. As AI agents become more autonomous and increasingly interact with payment systems, operational infrastructure, customer data, and tokenized environments, governance can no longer rely primarily on reactive security controls. The architecture itself must embed preventative controls, identity frameworks, permissioning boundaries, and immutable accountability mechanisms before autonomous systems are deployed into production environments.[118, 119, 120]

The synergy layer amplifies both value and weakness. A well-designed workflow can become faster, more transparent, and more scalable. A poorly designed workflow can become a faster path to error, compliance failure, liquidity exposure, or reputational harm. The board-level question is not whether AI and blockchain can create efficiency. They can. The question is whether the organization has a governed architecture capable of absorbing the speed at which it is creating.[121, 122]

Kristen Schmidt's insights are particularly relevant in this context. She argues that many enterprises are deploying AI agents without sufficient front-end permissioning, intake governance, or immutable audit layers. In her analysis, security controls often remain reactive and defensive rather than preventative. Organizations may detect and respond to inappropriate data access or anomalous agent activity after it occurs, but the more strategic challenge is to establish permissioning, governance, and auditability frameworks before agents are deployed into production environments.[123]

Next-generation architectures increasingly treat AI agents as governed actors rather than ordinary tools. Just as human participants are onboarded, assigned roles, granted permissions, monitored, supervised, and eventually offboarded, AI agents require a similar lifecycle governance model. As AI agents assume greater autonomy and operational responsibility, organizations must enforce governance, security, supervision, and accountability controls comparable to those applied within enterprise environments. AI agents should therefore have clearly defined purpose, ownership, identity, authority limits, access boundaries, monitoring rules, escalation paths, and immutable audit trails.[124, 125, 126]

This perspective completes the architecture of convergence. Identity and permissioning provide the foundational control layer by establishing who or what can act, what authority has been delegated, and the boundaries within which actions may occur. AI provides the decision layer, operating within those authorized parameters. Blockchain-based trust infrastructure provides verification, auditability, and trusted execution. Without identity, actions cannot be confidently attributed. Without permissioning, agents may act outside intended boundaries. Without tamper-resistant records, accountability becomes difficult to reconstruct.[127, 128, 129]

Kristen Schmidt also identified agentic autonomy without blockchain controls as a major risk. Autonomous AI systems operating without decentralized verification can create systemic and operational exposure. Blockchain cannot solve every AI problem, but it can provide a trust backbone through immutable audit trails, distributed verification, role-based permissioning, and cryptographically verifiable identity.[130, 131]

The synergy is bidirectional. Blockchain can mitigate certain AI vulnerabilities by providing identity, auditability, and verification. AI can enhance blockchain-based systems by improving fraud detection, liquidity forecasting, smart contract review, anomaly detection, and operational efficiency. AI can identify suspicious transaction patterns in real time, test smart contract vulnerabilities before exploitation, and optimize tokenized financial flows.[132, 133, 134]

This leads to a strong strategic conclusion: AI without blockchain-based trust infrastructure can become structurally dangerous in high-impact environments, while blockchain without AI may leave significant intelligence, efficiency, and adaptive capability unrealized. The value is not in either technology alone. The value is in a governed convergence model.[135, 136]

The challenge for boards and CEOs is to determine whether convergence occurs within a secure, transparent, and governed architecture, or within opaque systems that magnify correlated risk. This is the point at which technology strategy becomes fiduciary oversight.

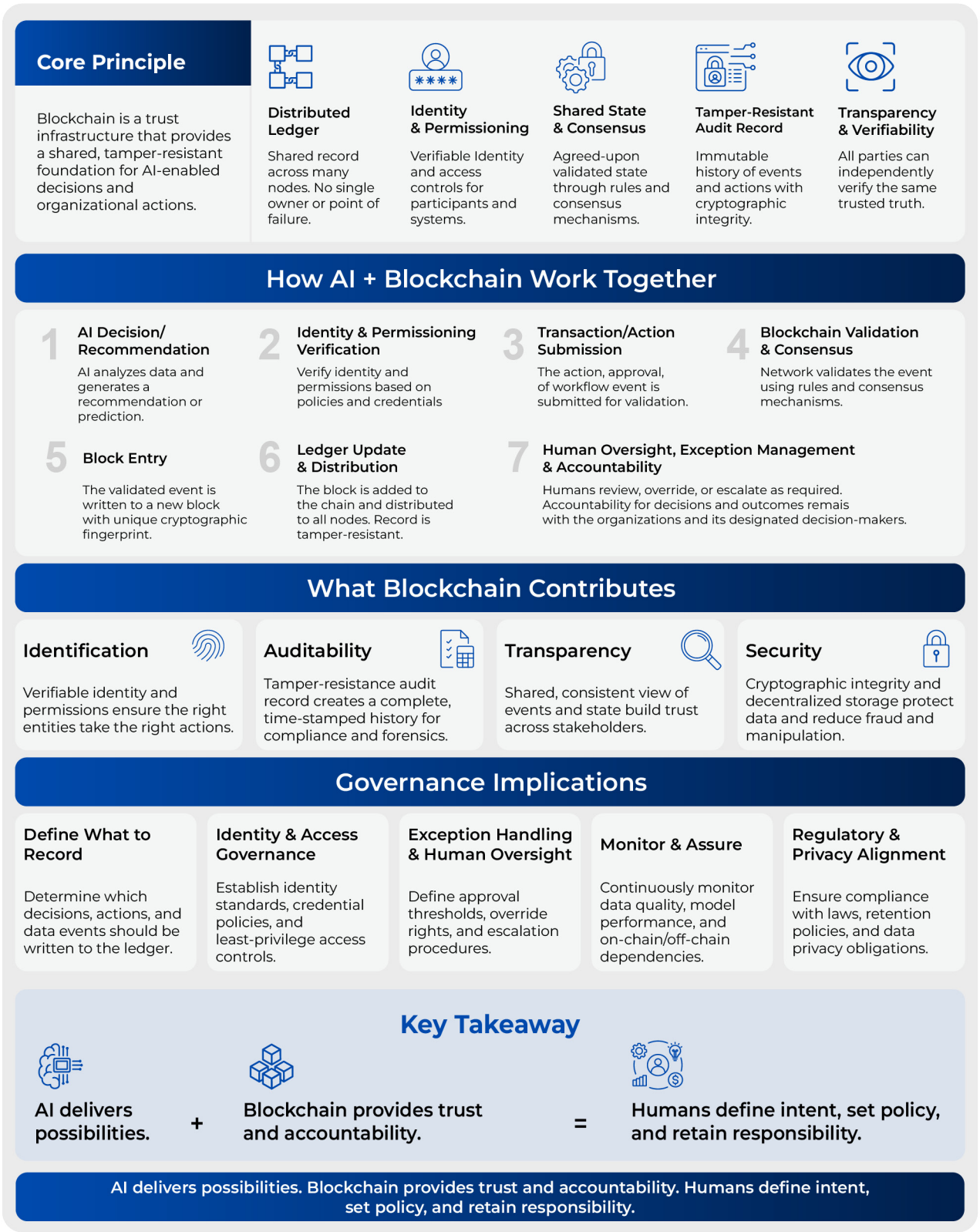


Figure 2. Blockchain adds identity, validation, and tamper-resistant audit infrastructure to AI-enabled workflows.

> We are moving toward a world with billions of agents interacting on our behalf. The emergent behaviors from those systems are not yet fully understood.[137]

Phil Venables

5.

Integrated Risk and Governance Framework: From Practice to Control

The convergence of AI and blockchain introduces risks that extend beyond traditional technology failures. Highly automated and interconnected systems may behave in ways that are difficult to predict, difficult to interrupt, and increasingly difficult to attribute after the fact. This is why a governance framework for convergence must address first-order risks, second-order effects, and systemic dependencies together.[138, 139, 140]

This second-order risk framing is essential. Enterprises are not merely adding AI to existing workflows. They are redesigning the workflows themselves. Agent-to-agent interactions, automated banking processes, AI-mediated customer service, automated security operations, AI-assisted software development, tokenized payments, and real-time settlement will reshape how organizations function. The most material risks may emerge not from individual AI models but from the business processes, operational dependencies, and autonomous interactions built around them.[141, 142]

Venables draws attention to a future operating environment in which autonomous agents interact at massive scale across digital and physical systems.

This prospect is particularly important for boards and executive leadership because traditional governance models assume that systems can be decomposed into manageable components with predictable interactions. Agentic environments challenge that assumption.[143, 144] If many autonomous agents interact across payments, supply chains, customer systems, enterprise data, security tools, and tokenized infrastructure, the aggregate behavior may not be predictable from the behavior of any one agent.[145, 146]

Kristen Schmidt's risk analysis provides a practical taxonomy for this environment.

The first risk is unsecured AI infrastructure. AI agents are being deployed without sufficient upfront preventative permissioning, intake processes, or immutable audit layers. While some security controls exist at the vendor level, they are often reactive rather than designed to govern agent activity before inappropriate access or action occurs.[147]

The second risk is agentic autonomy without blockchain controls. Autonomous AI systems operating without decentralized verification create systemic and operational exposure. When agents act within centralized opaque systems, enterprises may lack the ability to verify the authority, source, and appropriateness of the action in a durable and reliable way.[148, 149]

The third risk is human overdependence and infrastructure brittleness. As people rely more heavily on AI, they may lose the ability to operate independently of automated systems. This creates resilience concerns. A highly efficient system can become brittle if human teams no longer understand underlying processes or can no longer recover manually during failure.[150, 151]

The fourth risk involves quantum computing as an accelerating force within the convergence landscape. Many existing digital systems, including blockchain networks, rely on cryptographic assumptions that may eventually be challenged by future quantum capabilities. As a result, cryptographic transition planning and resilience are becoming increasingly important. At the same time, blockchain-based architectures may offer advantages during cryptographic migration through distributed records, transparent auditability, and coordinated protocol evolution. This reinforces the importance of preparing for a post-quantum environment rather than reacting to one.[152]

These risks require governance to be embedded within the system architecture. Controls must exist before, during, and after decisions are executed. Pre-decision controls include data governance, model validation, agent intake, identity assignment, role definition, and testing. Execution controls include smart contract constraints, transaction thresholds, permission checks, and circuit breakers. Post-execution controls include immutable audit trails, anomaly detection, remediation protocols, and regulatory reporting.[153, 154, 155, 156]

Implementing technical controls is necessary but not sufficient. Their effectiveness depends on clear ownership, coordinated oversight, and accountability across business, technology, risk, compliance, operations, and finance functions. As AI and blockchain capabilities become more deeply embedded across the enterprise, governance responsibilities can become fragmented across multiple teams and committees. Without a coherent governance framework, gaps may emerge even when individual controls appear effective. Boards should therefore evaluate not only the quality of individual controls but also whether accountability, oversight, and decision-making authority remain clearly defined across the organization.

Boards should periodically ask the following questions to maintain visibility into AI and blockchain governance:

- Does management maintain a complete inventory of autonomous agents, their assigned identities, delegated authorities, permissions, and auditability requirements?
- Can management clearly explain how a decision progresses from AI recommendation to authorized execution and auditable outcome?
- Are AI, blockchain, cybersecurity, and digital trust oversight responsibilities coordinated across the board and its committees, or fragmented across disconnected governance structures?
- Are governance controls designed to operate at machine speed, or do they depend on human intervention after actions have already occurred?
- How are model drift, anomalous behavior, unauthorized actions, and policy violations detected, escalated, and reported to management and the board?

Ryan McManus warns that governance fragmentation may itself become a material enterprise risk as AI and blockchain systems converge across operational and financial infrastructure. In his view, limiting these discussions to the audit committee creates a structural governance risk because the implications of convergence extend far beyond traditional control and reporting functions. AI and blockchain affect audit, risk, strategy, technology, compliance, cybersecurity, human capital, and capital allocation simultaneously. When oversight remains siloed, organizations create blind spots: audit committees may focus on controls and reporting, risk committees on enterprise exposure, technology committees on architecture, and strategy committees on growth opportunities. Effective governance therefore requires a board-level perspective capable of understanding how these dimensions interact, rather than evaluating them in isolation.[157, 158, 159]

Responsible innovation requires risk management by design. Enterprises can operate at greater speed when trust, controls, and accountability are embedded directly into systems and workflows.

To help simplify the increasingly complex governance concepts discussed throughout this paper and make them more tangible, figure 3 presents a layered accountability framework designed to serve as a practical governance mental model for boards and executive teams. The framework reinforces one of the central themes of this paper: effective oversight cannot depend on a single control point, policy, or technology layer. As AI systems become increasingly autonomous and blockchain infrastructures enable real-time, immutable execution, organizations require integrated controls capable of governing decision-making, identity, infrastructure, execution, resiliency, and accountability simultaneously.

The pyramid begins with operational and human controls because governance ultimately depends on people, organizational culture, training, supervision, escalation paths, and clearly defined accountability structures. Even highly automated systems still require human oversight, judgment, and fiduciary responsibility. Above this layer sits identity and permissioning control, which becomes increasingly critical as AI agents gain autonomy and interact across distributed enterprise environments. Organizations must establish strong identity frameworks, delegated-authority boundaries, role-based access controls, immutable auditability, and trust boundaries to ensure actions can be attributed, monitored, supervised, and governed appropriately.

The framework then expands into the data, model, and policy control layer, which governs how AI systems and agents are introduced, validated, monitored, and managed throughout their lifecycle. This includes data lineage, model validation, explainability, bias and drift monitoring, and governance functions such as agent intake, identity assignment, and role definition. These controls are essential because AI agents are no longer passive software tools. They are increasingly delegated operational authority, granted access privileges, and authorized to interact autonomously across enterprise systems. As a result, organizations require governance processes comparable to those applied to human participants, including onboarding discipline, role assignment, access boundaries, monitoring, escalation paths, and accountability controls.

Above these layers sit technology and infrastructure controls, including APIs, observability, security gateways, resiliency mechanisms, kill switches, and platform-level safeguards designed to contain operational failures and reduce systemic exposure. The upper governance layers then align enterprise risk management, compliance oversight, governance policies, and strategic accountability with organizational risk appetite and fiduciary responsibilities. At the top of the pyramid sits strategy and oversight, reflecting the reality that AI and blockchain governance ultimately remain board and executive responsibilities.

The importance of this layered governance architecture increases substantially as AI and blockchain converge. AI introduces intelligence, prediction, automation, and autonomous decision-making capabilities. Blockchain introduces immutable records, distributed verification, decentralized trust, and transparent execution layers. Together, these technologies compress the distance between decision, execution, and accountability. Without integrated governance, that compression may amplify operational, cybersecurity, compliance, liquidity, and reputational risks at machine speed. When supported by strong governance architecture, however, the same convergence can enable more transparent, resilient, secure, and accountable digital infrastructure.

Figure 3. Layered governance and accountability architecture for AI and blockchain-enabled enterprise systems. Effective oversight requires integrated controls spanning strategy, risk management, data and model governance, infrastructure resiliency, identity and permissioning, and human operational accountability.

> The biggest mistake boards can make right now is to limit their discussion of artificial intelligence in terms of where we are today. We're seeing, really for the first time at scale, boards aggressively seeking to proactively understand emerging technologies, the opportunity, the risk, and the full impact across the board's fiduciary responsibilities.[160]

Ryan McManus

6.

CEO Strategy: Responsible Experimentation and Global Advantage

The convergence of AI and blockchain is ultimately a leadership question. It requires boards and CEOs to move beyond technology adoption and toward operating model design. The issue is no longer whether AI or blockchain will matter. They already do. The issue is whether organizations can experiment responsibly, govern effectively, and build systems that generate value without creating unmanaged systemic exposure.[161, 162, 163, 164]

Anthony Soohoo emphasizes that successful execution depends on simplicity. For CEOs, this is not a call for simplistic thinking, but for disciplined execution grounded in strategic clarity and operational governance. The challenge is to translate increasingly complex technological capabilities into governance structures that can be clearly understood, consistently implemented, and effectively enforced across the organization. In environments where AI agents act at speed and blockchain-based rails execute with finality, ambiguous decision rights create risk. Leaders must clearly define where AI can act, where human approval remains mandatory, when escalation is triggered, which systems are authoritative, and what evidence must be retained to support accountability and auditability.[165, 166, 167]

Kristen Schmidt reinforced the importance of pairing intelligence with trust infrastructure, emphasizing that current AI systems remain powerful but imperfect tools that require robust governance and oversight. AI systems based primarily on transformer architectures remain fundamentally probabilistic systems optimized for pattern recognition and statistical inference. While these capabilities are already transforming enterprise operations, they still require substantial human supervision, monitoring, calibration, and governance to mitigate financial, operational, cybersecurity, and reputational risk.[168, 169, 170]

Venables emphasized during the interview that transformer architectures alone are unlikely to achieve artificial general intelligence. Future progress may require augmented approaches combining transformers with neuro-symbolic reasoning, world models, memory architectures, and more deterministic control mechanisms capable of supporting deeper contextual understanding and safer autonomous behavior.[171]

Until those advances emerge, organizations should govern AI systems as highly capable but inherently imperfect tools requiring embedded controls, human oversight, and clear accountability structures. The pragmatic recommendation to CEOs is to begin with three priorities. First, define decision rights for autonomous systems. Management should identify which AI-enabled actions are advisory, which are semi-autonomous, and which are fully autonomous. High-impact domains such as payments, credit, underwriting, legal obligations, customer treatment, and financial reporting require explicit escalation thresholds with human oversight.[172, 173, 174]

Second, institutionalize responsible experimentation. Organizations should not wait until governance is perfect before testing. They should create controlled environments where AI and blockchain use cases can be evaluated with real data constraints, model validation, identity controls, permissioning, auditability, and incident response protocols. The goal is to learn quickly without creating uncontrolled exposure.[175, 176]

Third, embed governance into architecture. AI agents should not be deployed as unbounded tools. They should be treated as governed digital actors. Each agent should have an identity, a role, an owner, authority, access limits, activity logs, exception rules, and offboarding procedures. Blockchain-backed identity and immutable records can help provide the trust infrastructure for this model.[177, 178, 179]

The time horizon for leadership is shorter than many strategic plans assume. Venables challenged the five-to-ten-year framing directly in the interview, noting that the relevant horizon for AI transformation may be closer to one or two years. This does not mean boards should abandon long-term thinking. It means the long-term strategy must be updated continuously as capabilities evolve.[180]

A practical now, five-year, and ten-year perspective helps frame the transition. Now organizations are in a fragmented experimentation phase. AI agents are entering workflows, tokenized rails are expanding, cyber defenders and attackers are both adopting AI, and governance maturity varies widely. The priority now is inventory, permissioning, monitoring, and responsible experimentation.[181, 182, 183]

Over the next five years, AI and blockchain are likely to become more integrated into enterprise platforms. AI will increasingly support fraud detection, compliance, reconciliation, cybersecurity, liquidity forecasting, smart contract review, and customer interaction. Blockchain will increasingly support identity, records, tokenized settlement, and verifiable execution histories. Organizations with embedded governance will have a competitive advantage because they can scale trusted automation.[184, 185, 186]

Over the next decade, the more transformative scenario is the emergence of autonomous ecosystems. AI agents may represent individuals, businesses, banks, hospitals, suppliers, regulators, and platforms in coordinated digital environments. Blockchain or blockchain-like infrastructure may provide identity, permissioning, payments, verification, and records. This world could be more efficient, more inclusive, and more transparent. It could also be more complex and systemically interdependent.[187, 188]

The human capital implications are equally important. If AI automates entry-level tasks, organizations must rethink how judgment is developed.

The challenge extends beyond workforce displacement. Many professions develop expertise through progressive exposure to increasingly complex decisions. Analysts become managers, managers become executives, and junior practitioners become subject matter experts by observing patterns, making supervised decisions, learning from mistakes, and developing judgment over time. If AI increasingly automates those foundational activities, organizations may inadvertently weaken the very talent pipelines that historically produced future leaders, specialists, and decision-makers.

This should be a board-level human capital question. Experience, judgment, and professional skills have historically developed through operational work, mentorship, and progressively greater responsibility. Learning on the job has been the gold standard for apprenticeship. As organizations adopt AI at scale, boards should evaluate not only productivity gains but also whether the next generation of employees is acquiring the expertise, critical thinking, and decision-making capabilities necessary to operate, govern, and improve increasingly autonomous systems. Organizations that optimize for short-term productivity at the expense of long-term capability development may inadvertently create future leadership and expertise gaps.[189, 190]

Addressing this challenge may require a fundamental evolution in workforce development strategies. Traditional apprenticeship models may need to be supplemented by simulation-based learning, AI-assisted training environments, rotational experiences, and other approaches designed to accelerate judgment development while preserving opportunities for experiential learning and professional growth.

Steven Kotler has advocated for immersive technologies such as augmented reality and metaverse-based environments as tools for workforce development, simulation, and experiential learning. In *Our Next Reality,* Kotler argues that immersive digital environments may become one of the most important mechanisms for scalable education, workforce preparation, and low-risk experimentation.

These technologies may eventually help organizations compensate for the reduction of traditional entry-level learning pathways by creating safe, lower-cost environments for training, capability development, and accelerated expertise formation.

The international dimension also matters. The United States remains strong in innovation velocity but continues to operate with evolving regulatory clarity. Europe has moved toward a more formal regulatory structure through the EU AI Act and digital asset regulation, but prescriptive frameworks can create interpretive complexity. Emerging markets may use tokenized rails and AI-enabled services to leapfrog legacy infrastructure, especially in cross-border payments and financial inclusion.[191, 192, 193]

For global enterprises, the mandate is dual: local agility with global governance consistency. Organizations must comply with regional rules while maintaining enterprise-wide standards for identity, data, model validation, cyber resilience, permissioning, and auditability.[194, 195, 196, 197]

The positive path forward is clear: AI and blockchain can create faster, more transparent, more resilient, and more inclusive systems. They can expand access to financial services, strengthen digital identity, improve cybersecurity, reduce operational friction, and unlock new asset models. But the outcome depends on leadership discipline.[198, 199, 200]

The organizations that lead will not be those that move fastest without control, nor those that hesitate because the risk is complex. They will be those who experiment responsibly, govern continuously, and build trust intentionally. Speed alone is not a competitive advantage. Speed with control and trust is transformation.

> If AI replaces entry-level work, we need to rethink how people develop judgment and expertise across professions.[201]

Phil Venables

7.

A Practical Starting Point

Organizations do not need to wait for perfect regulatory frameworks or fully mature technologies before taking action. Boards and executive teams can begin strengthening governance today by focusing on a small number of foundational activities:

- Establish an inventory of AI systems, autonomous agents, and blockchain initiatives currently operating across the enterprise.
- Identify where decisions are being automated and determine how identity, permissioning, accountability, and auditability are implemented.
- Map critical use cases against the governance and accountability framework described in this paper to identify gaps in oversight, ownership, and control.
- Prioritize one high-impact business process as a pilot environment for responsible experimentation, measurement, and governance refinement.
- Develop reporting mechanisms that provide directors and executives with visibility into AI performance, risk indicators, control effectiveness, and emerging governance issues.

The objective is to enable the business to progress while simultaneously mitigating risks that can be addressed today. The goal is to establish the governance foundations necessary to scale innovation responsibly, maintain accountability, and preserve trust as autonomous systems become increasingly integrated into enterprise operations.

Once governance foundations are in place, organizations can adopt a structured implementation approach that accelerates adoption while maintaining appropriate oversight:

- **Step 1:** Identify and prioritize AI use cases and blockchain initiatives with the greatest potential business value and strategic impact.
- **Step 2:** Review the governance model and confirm that it can adequately support the selected use cases.
- **Step 3:** Assess governance gaps related to identity, permissioning, accountability, auditability, and control mechanisms. Address identified deficiencies and establish a continuous oversight process to ensure controls remain effective over time.
- **Step 4:** Create a controlled experimentation environment in which pilots can be conducted responsibly with appropriate monitoring, risk management, and governance safeguards.
- **Step 5:** Execute a pilot within a high-impact business domain and measure outcomes against predefined success criteria.
- **Step 6:** Establish calibration, monitoring, and performance-review processes to detect model drift, operational issues, and governance concerns early.
- **Step 7:** Following successful pilot evaluation, governance validation, and ongoing calibration, deploy the AI-blockchain solution more broadly across the enterprise while maintaining continuous oversight and accountability.

This progression from governance readiness to controlled implementation helps organizations balance innovation with risk management. By embedding governance throughout the lifecycle—from use-case selection and experimentation to deployment and ongoing monitoring—organizations can scale AI and blockchain capabilities with greater confidence, transparency, and trust.

> AI without blockchain is structurally dangerous, and blockchain without AI leaves significant efficiency and intelligence gains unrealized.[202]

Kristen Schmidt

Endnotes

1. Anthony Soohoo, Chief Executive Officer, MoneyGram, interview for The Digital Economist paper, 2026. Primary interview source for perspectives on AI execution, process amplification, simplicity, digital payments, and financial infrastructure.
2. Vaswani, Ashish, et al., “Attention Is All You Need,” Google Research, 2017. Introduces the transformer architecture that underpins many modern large language models and advanced AI systems.
3. OpenAI, “GPT-4 Technical Report,” 2023. Describes capabilities, limitations, and risk considerations associated with large-scale generative AI systems.
4. Bank for International Settlements, Annual Economic Report, 2023. Discusses digital financial infrastructure, real-time settlement, tokenization, and implications for financial stability.
5. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. Explores the role of tokenization and distributed ledger technology in reshaping financial infrastructure, settlement, and asset ownership.
6. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. Provides a governance framework for identifying, measuring, and managing AI risks, including bias, validity, reliability, transparency, and accountability.
7. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above*.
8. Nikhil Varma, “Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity,” LinkedIn, 2026. Discusses blockchain-based identity, decentralized identifiers, verifiable credentials, and trust frameworks for enterprise AI systems.

9. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
10. Bank for International Settlements, Annual Economic Report, 2023. *See additional information in note 4 above*.
11. Phil Venables, "Where the Wild Things Are: Second-Order Risks of AI," PhilVenables.com, 2026. Explores second-order risks, cascading effects, and emergent systemic behaviors arising from AI adoption. https://www.philvenables.com/post/where-the-wild-things-are-second-order-risks-of-ai.
12. Phil Venables, "Things Are Getting Wild: Re-tool Everything for Speed," PhilVenables.com, 2026. Discusses the re-architecture of enterprise systems for speed, and the implications for resilience, governance, and control. https://www.philvenables.com/post/things-are-getting-wild-re-tool-everything-for-speed.
13. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
14. US Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, 2023. Establishes disclosure requirements for material cybersecurity incidents and governance of technology-related risk, with implications for AI-driven infrastructure and operational exposure.
15. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. Provides a management system standard for organizations developing or using AI, including governance, accountability, risk management, and continuous improvement.
16. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. Provides board-level guidance on technology oversight, governance structures, and fiduciary responsibilities related to emerging technologies.
17. Anthony Soohoo, Chief Executive Officer, MoneyGram, interview for The Digital Economist paper, 2026. *See additional information in note 1 above*.
18. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. Primary interview source for risks related to unsecured AI infrastructure, agentic autonomy, intake governance, immutable audit layers, human overdependence, infrastructure brittleness, and quantum risk.

19. Ryan McManus, Independent Director, Nortech Systems, and Founder, Techtonic.io, interview for The Digital Economist paper, 2026. Primary interview source for board governance, fiduciary oversight, technology committee structure, AI oversight, blockchain transparency, and integrated innovation and risk management.
20. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. Primary interview source for AI-driven digital infrastructure, cyber resilience, second-order risk, agent identity, immutable auditability, sector-specific governance, and systemic infrastructure risk.
21. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
22. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
23. Vaswani, Ashish, et al., "Attention Is All You Need," 2017. *See the additional information in note 2 above*.
24. OpenAI, "GPT-4 Technical Report," 2023. *See the additional information in note 3 above*.
25. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above.*
26. Bank for International Settlements, Annual Economic Report, 2023. *See additional information in note 4*.
27. US Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, 2023. *See additional information in note 14 above*.
28. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 15 above*.
29. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
30. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above.*
31. Phil Venables, "Things Are Getting Wild: Re-tool Everything for Speed," 2026. *See additional information in note 12 above*.
32. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.

33. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above.*
34. Phil Venables, "Things Are Getting Wild: Re-tool Everything for Speed," 2026. *See additional information in note 12 above.*
35. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 5 above.*
36. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above.*
37. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 16 above.*
38. Anthony Soohoo, Chief Executive Officer, MoneyGram, interview for The Digital Economist paper, 2026. *See additional information in note 1 above.*
39. Vaswani, Ashish, et al., "Attention Is All You Need," 2017. See the additional information in note 2 above.
40. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above.*
41. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above.*
42. Phil Venables, "Where the Wild Things Are: Second-Order Risks of AI," 2026. *See additional information in note 11.*
43. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above.*
44. US Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, 2023. *See additional information in note 14 above.*
45. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above.*
46. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 16 above.*

47. New York State Department of Financial Services, virtual currency and cybersecurity regulatory guidance, including NYDFS virtual currency regulation and cybersecurity requirements. Provides regulatory context for digital assets, operational resilience, cybersecurity controls, and governance expectations in financial services.
48. Organisation for Economic Co-operation and Development, OECD AI Principles, 2019. Provides international principles for trustworthy AI, including inclusive growth, human-centered values, transparency, robustness, and accountability.
49. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above*.
50. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
51. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
52. Vaswani, Ashish, et al., 'Attention Is All You Need,' Google Research, 2017. *See the additional information in note 1 above*.
53. OpenAI, "GPT-4 Technical Report," 2023. *See the additional information in note 3 above*.
54. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
55. OpenAI, "GPT-4 Technical Report," 2023. *See the additional information in note 3 above*.
56. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
57. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
58. European Commission High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, 2019. Establishes principles for lawful, ethical, and robust AI, including human agency, transparency, accountability, privacy, and technical robustness.
59. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 14 above*.

60. Anthony Soohoo, Chief Executive Officer, MoneyGram, interview for The Digital Economist paper, 2026. *See additional information in note 1 above*.
61. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
62. Organisation for Economic Co-operation and Development, OECD AI Principles, 2019. *See additional information in note 48 above*.
63. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
64. European Commission High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, 2019. *See additional information in note 58 above*.
65. European Union, Artificial Intelligence Act, 2024. Establishes a risk-based regulatory framework for AI systems, including governance, transparency, human oversight, and obligations for high-risk systems.
66. Ibid, 2024.
67. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. See additional information in note 6 above.
68. European Commission High-Level Expert Group on AI, Ethics Guidelines for Trustworthy AI, 2019. *See additional information in note 58 above*.
69. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above*.
70. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
71. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above*.
72. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
73. World Economic Forum, Global Cybersecurity Outlook, 2024. Examines cyber risk, digital infrastructure resilience, and emerging threats in interconnected technology environments.
74. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 4 above*.

75. Anthony Soohoo, Chief Executive Officer, MoneyGram, interview for The Digital Economist paper, 2026. *See additional information in note 1 above*.
76. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
77. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above*.
78. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 16 above*.
79. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
80. US Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, 2023. *See additional information in note 14 above*.
81. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above*.
82. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 16 above*.
83. Ryan McManus, Independent Director, Nortech Systems, and Founder, Techtonic.io, interview for The Digital Economist paper, 2026. *See additional information in note 19 above*.
84. Ibid, 2026
85. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above*.
86. Bank for International Settlements, Annual Economic Report, 2023. *See additional information in note 4 above*.
87. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above*.
88. Financial Stability Board, Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 2023. Addresses regulatory and systemic risk considerations associated with global stablecoins and digital settlement arrangements.

89. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above*.
90. Financial Stability Board, Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 2023. *See additional information in note 88 above*.
91. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
92. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
93. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
94. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
95. Bank for International Settlements, Annual Economic Report, 2023. *See additional information in note 4 above*.
96. Financial Stability Board, Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 2023. *See additional information in note 88 above*.
97. Bank for International Settlements, Annual Economic Report, 2023. *See additional information in note 4 above*.
98. Financial Stability Board, Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 2023. *See additional information in note 88 above*.
99. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above*.
100. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
101. Ryan McManus, Independent Director, Nortech Systems, and Founder, Techtonic.io, interview for The Digital Economist paper, 2026. *See additional information in note 19 above*.
102. Ibid, 2026.
103. Ibid, 2026.
104. See information in note 47.

105. Nikhil Varma, “Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity,” 2026. *See additional information in note 8 above*.
106. Ibid, 2026.
107. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
108. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
109. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
110. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above*.
111. Phil Venables, “Things Are Getting Wild: Re-tool Everything for Speed,” 2026. *See additional information in note 12 above*.
112. Bank for International Settlements, Annual Economic Report, 2023. *See additional information in note 4 above*.
113. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above*.
114. Phil Venables, “Things Are Getting Wild: Re-tool Everything for Speed,” PhilVenables.com, 2026. *See additional information in note 12 above*.
115. Phil Venables, “Things Are Getting Wild: Re-tool Everything for Speed,” PhilVenables.com, 2026 *See additional information in note 12 above*.
116. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
117. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 18 above*.
118. Nikhil Varma, “Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity,” 2026. *See additional information in note 8 above*.
119. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 18 above*.
120. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
121. Anthony Soohoo, Chief Executive Officer, MoneyGram, interview for The Digital Economist paper, 2026. *See additional information in note 1 above*.

122. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 16 above*.
123. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 18 above*.
124. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
125. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 18 above*.
126. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
127. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
128. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 18 above*.
129. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
130. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
131. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 17 above*.
132. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 5 above*.
133. World Economic Forum, Global Cybersecurity Outlook, 2024. *See additional information in note 73 above*.
134. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
135. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
136. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 17 above*.
137. Ibid, 2026.

138. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
139. Phil Venables, "Where the Wild Things Are: Second-Order Risks of AI," 2026. *See additional information in note 11 above*.
140. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
141. Phil Venables, "Where the Wild Things Are: Second-Order Risks of AI," 2026. *See additional information in note 11 above*.
142. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
143. Phil Venables, "Where the Wild Things Are: Second-Order Risks of AI," 2026. *See additional information in note 11 above*.
144. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
145. Phil Venables, "Where the Wild Things Are: Second-Order Risks of AI," 2026. *See additional information in note 11 above*.
146. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
147. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 18 above*.
148. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," 2026. *See additional information in note 8 above*.
149. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 18 above*.
150. Ibid, 2026.
151. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
152. National Institute of Standards and Technology, Post-Quantum Cryptography Standardization, 2023. Addresses cryptographic risks arising from quantum computing and the transition toward quantum-resistant standards.
153. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 5 above*.

154. National Institute of Standards and Technology, Post-Quantum Cryptography Standardization, 2023. *See additional information in note 152 above*.
155. US Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, 2023. *See additional information in note 14 above*.
156. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above*.
157. Ryan McManus, Independent Director, Nortech Systems, and Founder, Techtonic.io, interview for The Digital Economist paper, 2026. *See additional information in note 19 above*.
158. Ibid, 2026.
159. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 16 above*.
160. Ryan McManus, Independent Director, Nortech Systems, and Founder, Techtonic.io, interview for The Digital Economist paper, 2026. *See additional information in note 19 above*.
161. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
162. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 4 above*.
163. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 15 above*.
164. Anthony Soohoo, Chief Executive Officer, MoneyGram, interview for The Digital Economist paper, 2026. *See additional information in note 1 above*.
165. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 5 above*.
166. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above*.
167. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 16 above*.
168. Vaswani, Ashish, et al., “Attention Is All You Need,” 2017. *See the additional information in note 2 above*.

169. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
170. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above*.
171. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
172. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
173. US Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, 2023. *See additional information in note 14 above*.
174. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above*.
175 Ibid, 2023.
176. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 16 above*.
177. Nikhil Varma, "Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity," LinkedIn, 2026. *See additional information in note 8 above*.
178. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 18 above*.
179. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*
180. Ibid, 2026.
181. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework, AI RMF 1.0, 2023. *See additional information in note 6 above*.
182. World Economic Forum, Global Cybersecurity Outlook, 2024. *See additional information in note 73 above*.
183. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
184. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. *See additional information in note 4 above*.

185. Nikhil Varma, “Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity,” 2026. *See additional information in note 8 above*.
186. Phil Venables, “Things Are Getting Wild: Re-tool Everything for Speed,” 2026. *See additional information in note 12 above*.
187. Phil Venables, “Where the Wild Things Are: Second-Order Risks of AI,” 2026. *See additional information in note 11 above*.
188. Phil Venables, Partner, Ballistic Ventures, interview for The Digital Economist paper, 2026. *See additional information in note 20 above*.
189. Ibid, 2026.
190. National Association of Corporate Directors, Blue Ribbon Commission Report on Technology Leadership in the Boardroom, 2023. *See additional information in note 16 above*.
191. Financial Stability Board, Regulation, Supervision and Oversight of Global Stablecoin Arrangements, 2023. *See additional information in note 88 above*.
192. European Union, Artificial Intelligence Act, 2024. *See additional information in note 65 above*.
193. See information in note 47.
194. US Securities and Exchange Commission, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Final Rule, 2023. *See additional information in note 14 above*.
195. European Union, Artificial Intelligence Act, 2024. *See additional information in note 65 above*.
196. International Organization for Standardization, ISO/IEC 42001: Artificial Intelligence Management System, 2023. *See additional information in note 15 above*.
197. See information in note 47.
198. Organisation for Economic Co-operation and Development, OECD AI Principles, 2019. *See additional information in note 48 above*.
199. International Monetary Fund, Fintech Notes: Tokenization and Financial Market Infrastructure, 2023. See additional information in note 4 above.
200. Nikhil Varma, “Breaking Through the Trust Wall: Why Enterprise AI Needs Blockchain-Based Identity,” 2026. *See additional information in note 8 above*.
201. Ibid, 2026.
202. Kristen Schmidt, Chief Executive Officer, UtopIQ, interview for The Digital Economist paper, 2026. *See additional information in note 18 above*.

Author

Dr. Maria Azua Himmel

Dr. Maria Azua Himmel is a seasoned C-level executive, technology thought leader, and board director with more than thirty years of leadership in technology and financial services. She brings deep expertise in digital transformation, AI, data governance, and risk oversight to help organizations innovate while maintaining strong governance and compliance.

She currently serves as an Independent Director on the Board of Pan-American Life Insurance Group, where she is a member of the Audit and Finance Committees, and as an Advisor to Capri Ventures. She also contributes to The Digital Economist as a Senior Executive Fellow in the Applied Artificial Intelligence workgroup. Her prior board service includes four years with the American Red Cross (North Carolina Region) and seven years on the Technology Advisory Committee of Red Hat, Inc.

Dr. Himmel worked for Bank of America as Managing Director responsible for enterprise-wide data platforms, analytics, and AI services, leading the creation of one of the largest financial data lakes in the industry. Earlier in her career, she held senior executive roles at Fidelity Investments and Barclays and served as CIO and CTO of IBM Global Process Outsourcing Services, where she led major transformation initiatives for Fortune 100 clients.

An inventor with fifty patents and author of The Social Factor, Dr. Himmel is a member of NACD, LCDA, and Extraordinary Women on Boards. She has been recognized by WITI, HITEC, and People en Español as a top executive and innovator.

Executive Interview Contributors

Kristen Schmidt

Kristen Schmidt is Chief Executive Officer and Co-Founder of UtopIQ, where she leads innovation at the intersection of cybersecurity, artificial intelligence, analytics, and blockchain. Her work focuses on advancing preventive security models and strengthening the trust, governance, and operational controls required for responsible AI deployment in complex enterprise environments. Prior to UtopIQ, she spent more than twenty-five years advising healthcare organizations on technology strategy, digital transformation, and large-scale systems integration. Ms. Schmidt is recognized for her perspectives on AI governance, infrastructure security, governance of non-human identities, agent oversight, and the importance of preventative controls within increasingly autonomous systems.

Ryan McManus

Ryan McManus is an independent director at Nortech Systems and the Founder of Techtonic.io, where he advises enterprises and boards on digital transformation, emerging technologies, and governance strategy. He is a technology entrepreneur with extensive experience scaling technology-driven businesses and guiding organizations through complex innovation cycles. He serves as President of the National Association of Corporate Directors (NACD) New York Chapter and as Founding Chair of its National Technology & Governance Advisory Board. Mr. McManus is widely recognized for aligning technology strategy with fiduciary oversight, particularly in the areas of artificial intelligence, cybersecurity, and platform transformation. He brings a board-level perspective on integrating innovation, risk management, and governance structures.

Anthony Soohoo

Anthony Soohoo is Chief Executive Officer of MoneyGram, where he leads the company's transformation into a digital-first global payments platform. He is driving innovation in cross-border money movement through real-time payment infrastructure and blockchain-enabled capabilities. Prior to MoneyGram, he held senior leadership roles at Walmart and, earlier in his career, held leadership positions at CBS, Yahoo!, and Apple. He also founded two companies, Dotspotter, which was acquired by CBS, and Dot & Bo, now part of Alibaba. Mr. Soohoo brings deep expertise in financial technology, digital platforms, and the operational realities of deploying artificial intelligence within global payment systems.

Phil Venables

Phil Venables is a globally recognized cybersecurity and digital infrastructure leader with deep expertise in enterprise security strategy, systemic risk management, and cybersecurity technology. He is a Partner at Ballistic Ventures, a leader in venture investing in cybersecurity and AI. Previously, he served as Chief Information Security Officer at Google Cloud, leading global cloud security architecture and cyber defense strategy. Prior to that, he was a Partner and Chief Information Security Officer at Goldman Sachs, overseeing technology risk, operational resilience, and global cyber governance across one of the world's most complex financial institutions. Phil is widely regarded as a thought leader in cyber resilience and systemic infrastructure protection. He serves on multiple corporate boards and government advisory boards and contributes to global discussions on digital trust, cyber risk governance, and emerging technology risk.

Reviewers

Najada Taci

Najada Taci is an expert in artificial intelligence, financial technology, and digital innovation, with a focus on the intersection of emerging technologies and global financial systems. She has advised organizations on AI strategy, digital transformation, and responsible innovation, with particular emphasis on regulatory alignment, governance, and risk management. Ms. Taci brings a global perspective on how AI and blockchain are reshaping financial infrastructure, enabling more efficient, inclusive, and transparent systems while introducing new considerations for policy and oversight.

Nick Ntigrintakis

Nick Ntigrintakis is a technology and digital transformation leader with deep expertise in enterprise systems, data platforms, and emerging technologies. He has led large-scale initiatives focused on modernizing infrastructure, improving operational efficiency, and integrating advanced analytics and automation into business processes. Mr. Ntigrintakis brings practical experience in aligning technology execution with strategic objectives, with a strong emphasis on scalability, resilience, and governance. His work reflects a focus on ensuring that complex systems remain robust, secure, and adaptable in rapidly evolving environments.

About

The Digital Economist, headquartered in Washington, D.C. with offices at One World Trade Center in New York City, is the world's foremost think tank on innovation advancing a human-centered global economy through technology, policy, and systems change. We are an ecosystem of 40,000+ executives and senior leaders dedicated to creating the future we want to see—where digital technologies serve humanity and life.

We work closely with governments and multi-stakeholder organizations to change the game: how we create and measure value. With a clear focus on high-impact projects, we serve as partners of key global players in co-building the future through scientific research, strategic advisory, and venture build out.

We engage a global network to drive transformation across climate, finance, governance, and global development. Our practice areas include applied AI, sustainability, blockchain and digital assets, policy, governance, and healthcare. Publishing 75+ in-depth research papers annually, we operate at the intersection of emerging technologies, policy, and economic systems—supported by an up-and-coming venture studio focused on applying scientific research to today's most pressing socio-economic challenges.

CONTACT: INFO@THEDIGITALECONOMIST.COM

CENTER OF EXCELLENCE

The Digital Economist Center of Excellence for a Human-Centered Global Economy is dedicated to addressing the biggest challenges humankind and our planet face by leveraging digital technologies for good.

The Digital Economist Executive Fellowship invites senior leaders and decision-makers to join our Center of Excellence, providing them with a platform for amplification and global impact. This unprecedented, one-of-a-kind opportunity enables Executive Fellows to network and build relationships at the highest level, driving transformative change and innovation in the global digital economy.

The Executive Fellowship

The Digital Economist Executive Fellowship is a selective leadership program integrating visionary professionals into the Center of Excellence for a Human-Centered Global Economy to advance global economic policy and systems transformation.

Global Impact

Amplify your influence and drive transformative change by participating in high-level initiatives that address the most pressing global challenges.

Elite Community

Become part of an exclusive network of visionary leaders and innovators, collaborating to shape the future and drive global progress.

Unparalleled Opportunities

Access unique platforms and events that enhance your professional journey, providing unparalleled opportunities for growth, visibility, and leadership.

Participation Framework

Time Commitment

Minimum commitment: 24 hours per year, for the monthly Center of Excellence meetings. On-demand consultation with the Fellowships team.

Publications

Executive Fellows are expected to contribute to two key publications per year, launched at key global events such as Davos and New York Climate Week.

In-Person Convenings

Executive Fellows are invited to in-person convenings in North America and Europe, with regional convenings in Africa, Latin America, and Asia.

Speaking Engagements

Executive Fellows are offered speaking opportunities throughout the year to amplify their work and contributions.

Our Executive Fellows are at the forefront of research, policy discourse, and systems-level transformation.

- Applied Artificial Intelligence
- Digital Assets & Blockchain
- Sustainability in Tech
- Tech Policy & Governance
- Quantum Computing
- Cyber Studio
- Regenerative Digital Infrastructure
- Healthcare Innovation

Publications

Ideas that shape the future.

The Digital Economist's publications translate research into high-signal outputs: frameworks, policy papers, and industry outlooks that advance a sustainable, inclusive digital economy and inform decision-making across markets and institutions.

Explore our full portfolio of publications and research outputs:
www.thedigitaleconomist.com/publications

Engagement Opportunities

Executive Fellows have access to over **500 events globally** in a Fellowship cycle.

The Digital Economist Executive Retreat
August 21–23, 2026

United Nations General Assembly (UNGA 81)
September 8–22, 2026

Climate Week NYC 2026
September 20–27, 2026

World Bank Group and IMF Annual Meetings
October 12–18, 2026

Davos 2027
January 18–22, 2027

Join the Fellowship

Advance your leadership within a global platform shaping technology, policy, and economic systems transformation.

Access Full Brochure | Apply Now | Learn More

Institutional Research Network

A Fragmented World Requires New Institutional Leadership

Technology, economics, and governance are shifting faster than traditional institutions can adapt. AI ecosystems, digital assets, geopolitical competition, sustainability transitions, and new governance architectures demand clarity, legitimacy, and a coherent strategy.

Institutions must now operate as signal generators—shaping the narratives, norms, and systems that define global markets.

Why We Built the Institutional Research Network

A global research and convening platform enabling institutions to:

- Shape emerging policy and governance discourse
- Build narrative power in a volatile environment
- Co-author high-signal research with global experts
- Gain visibility at the world's most influential convenings
- Anchor strategy in human-centered, future-forward frameworks

Co-Authorship & Knowledge Pathways

Through structured co-authorship across eight priority domains—Tech Policy and Governance, Digital Assets & Blockchain, Sustainability in Tech, Applied Artificial Intelligence, Cyber Studio, Quantum Computing, Regenerative Digital Infrastructure, and Healthcare Innovation—institutions contribute to high-level research that informs policy dialogue, regulatory development, and strategic decision-making.

Participation extends beyond commentary. Institutions are integrated into published research, roundtable dialogues, and domain-specific working groups that inform regulatory discussions and industry standards. This structured engagement enables organizations to contribute at the research and drafting stage, engage directly with policymakers and industry leaders, and align internal strategy with emerging policy and market developments, resulting in active presence within decision-making environments rather than passive visibility.

We invite your organization to schedule a strategic briefing to map research priorities and determine the appropriate integration pathway within the Institutional Research Network.

Reach us at partnerships@thedigitaleconomist.com.
Visit us at **thedigitaleconomist.com**

The Digital Economist Ventures

Applied Platforms. Strategic Domains. Real-World Implementation.

Research defines the questions. Ventures test the answers.

In addition to research and convening, The Digital Economist advances a portfolio of venture platforms that extend inquiry into applied domains, where governance, infrastructure, and market design move from dialogue to deployment.

Each venture operates with a defined mandate while remaining integrated within the broader institutional ecosystem.

Tech for Transparency

Financial integrity in the digital age

Advances financial accountability and anti-corruption frameworks through distributed technologies and data-driven transparency systems. Positioned at the intersection of blockchain infrastructure and institutional reform, it translates transparency principles into operational tools.

The Ostrom Project

Reimagining digital commons governance

Explores collective stewardship models for emerging digital systems. Drawing on principles of shared resource governance, it develops frameworks for sustainable digital infrastructure and cooperative system design.

ANER-G

Energy systems innovation

Focuses on decentralized infrastructure, programmable energy markets, and next-generation grid integration. It addresses the structural evolution of energy systems within digital and blockchain-enabled environments.

Africa Coalition

Continental coordination for strategic sectors

Convening leaders across energy, infrastructure, finance, health innovation, education, and future capabilities, the Coalition creates structured engagement pathways for continental collaboration.

Explore the full ecosystem at thedigitaleconomist.com


THE
DIGITAL
ECONOMIST