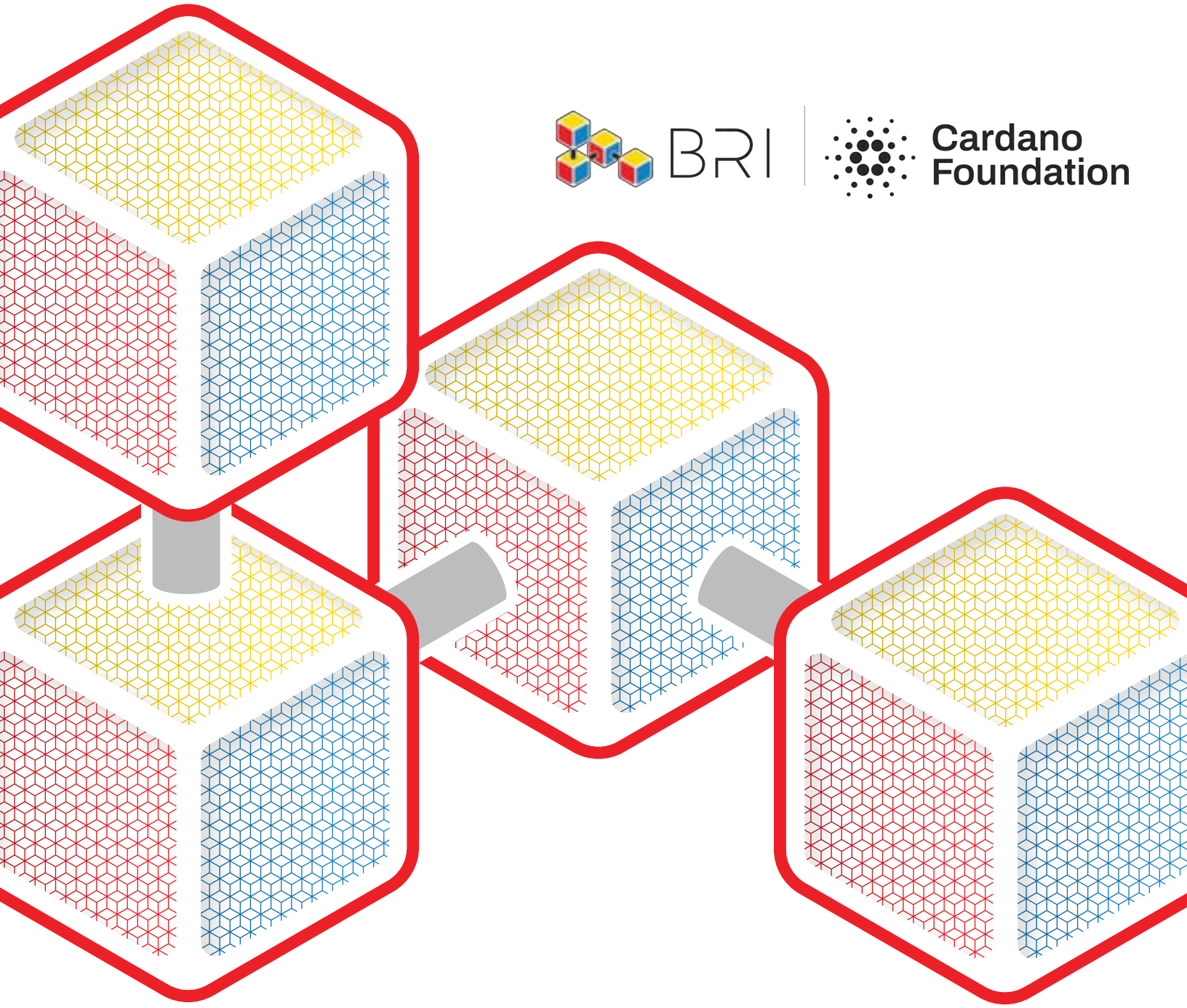


INTRODUCING DIGITAL TRUST INFRASTRUCTURE

The Foundation for the New Digital Economy

Douglas Heintzman, BRI

November 2025

A BRI BIG IDEA WHITE PAPER

Realizing the new promise of the digital economy

In 1994, Don Tapscott coined the phrase, "the digital economy," with his book of that title. It discussed how the Web and the Internet of information would bring important changes in business and society. Today the Internet of value creates profound new possibilities.

In 2017, Don and Alex Tapscott launched the Blockchain Research Institute (operating as BRI) to help realize the new promise of the digital economy. Our current program explores such critical areas as blockchain and artificial intelligence, identic AI, and digital infrastructure.

Our findings, conclusions, and recommendations are initially proprietary to our members and ultimately released to the public in support of our mission. To find out more, please visit www.blockchainresearchinstitute.org.

Contents

Cardano Foundation

Message from the CEO

The world of technology feels like it is moving very fast. The sheer volume of newsflow and updates means that the business leaders I meet often feel overwhelmed at the level of advancements they are supposedly to have made, whether it is in AI, blockchain, or cybersecurity.

It is easy to get wrapped up in headlines. Through my career in finance and now advanced blockchain technology as CEO of the Cardano Foundation, I understand that the real challenges and the hard work lie in the implementation. This is especially true in ever-growing industries with complex and sensitive data types such as finance, identity, and security.

Digital transformation is not a new term, but I truly believe we are now at a critical point in that journey where different factors and technological innovations, on seemingly independent paths, have converged into one interoperable ecosystem. This is what we call the New Digital Economy.

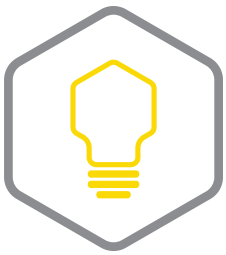
We are excited to launch this timely report with the BRI at the Cardano Summit in Berlin, among such esteemed executives from world leading enterprises and organizations.

Douglas Heintzman's work introduces not just the idea of *digital trust infrastructure* (DTI), but how actually to harness its potential using practical examples. Its success depends on balancing institutional trust with individual privacy, something that is core to the Cardano Foundation's mission.

A primary focus of the Cardano Foundation is to advance Cardano as a public infrastructure across a wide range of industries; we believe that it can deliver DTI in a business-friendly way.

I am looking forward immensely to the response this report receives from the business community and, even more so, how we work together to bring this technology into your organization and deliver real business benefits.

FREDERIK GREGAARD
Chief Executive Officer
Cardano Foundation



Foreword

We live in a time of historic disruption and equally historic opportunity. Around the world, our economic, social, and institutional systems—shaped for the industrial age—are straining under the weight of the digital era. In many countries, a consensus is emerging among business and political leaders: we must build a more resilient and independent economy, but not an isolated one. Too often, however, the solutions on offer amount to incremental tweaks to an aging, resource-driven or industrial age model.

To achieve long-term prosperity, national sovereignty, and meaningful productivity gains, I've argued for some time that we must go deeper. Our leaders of businesses, governments, and nongovernmental organizations must do what their counterparts are already doing in Estonia, Finland, Germany, and the Netherlands in the European Union, in Japan, Singapore, and South Korea, and in the United Arab Emirates: retooling our economy from the ground up, rethinking not only what we produce but how our society functions.

This means rethinking infrastructure—not just the roads, bridges, and power grids of the past, but the digital systems that now underpin economic activity, democratic governance, and individual empowerment. Just as the railroads connected the country in the 19th century, and power grids lit up the 20th century, something we've named the *digital trust infrastructure* (DTI) will define the 21st.

"This is a comprehensive and deeply thoughtful blueprint for building the foundational layers of a digital enterprise and society."

DON TAPSCOTT
EXECUTIVE CHAIRMAN
BRI

That's why I'm delighted to introduce this new white paper by Doug Heintzman, developed in collaboration with the Cardano Foundation. It's a comprehensive and deeply thoughtful blueprint for building the foundational layers of a digital enterprise and society, one that puts trust, autonomy, and innovation at the center.

This isn't theoretical, although there has been no overall conceptual framework and language to describe this new thinking until this paper. The components of this new infrastructure already exist. What's also missing is the coordination, architecture, and vision to pull them together into a public utility for the digital age. Doug's work does exactly that.

The paper introduces a five-layer DTI architecture. Each layer builds upon the last to create a coherent, secure, and inclusive system.

Layer one is the trusted data fabric, the base of the entire stack. It consists of truth anchors and zero-knowledge proofs, which allow individuals and institutions to prove claims without exposing underlying data. This enables a shift away from institutional silos and toward a decentralized, privacy-preserving flow of verified information.

Layer two is digital identity. I'd argue that this is the most important building block of digital citizenship. It includes decentralized and autonomous identifiers, verifiable credentials, and verifiable

presentations. These tools allow individuals to present only the data relevant to a context, reducing surveillance risk and boosting control. The identity layer also includes trust registries, compliance standards, a complete *decentralized identity* (DID) life cycle, and alignment with privacy regulations, all of which give people real ownership over their digital selves.

This isn't an abstract ideal. In healthcare, for example, patients could control and share their own records across systems and borders, contribute anonymized data to research, or license data commercially, always within an ethical and secure framework.

Layer three addresses authoritative registries and data exchange layers, including trusted oracles—bridges to external data—and open data exchange protocols. These allow institutions to securely share validated data across sectors, powering everything from supply chain integrity to pandemic response.

Layer four introduces digital payments and programmable value. Imagine a public payment system where money flows peer-to-peer, instantly and securely, with logic and rules embedded directly into the transaction. This could take the form of a central bank digital currency or a regulated stablecoin. Either way, the goal is to reduce friction, expand financial inclusion, and build a value layer for digital commerce that works as a public good.

Layer five presents a bold but essential idea: universal basic intelligence. Artificial intelligence is no longer a niche tool; it's becoming an ever-present digital companion. Without intervention, AI could become a new fault line in society, supercharging a small elite while leaving the majority behind. Doug calls for every citizen to have access to a trusted, secure, personalized AI agent, trained on their data and working on their behalf.

In the second part of the paper, Doug examines how this architecture rolls out across key sectors: finance, healthcare, education, supply chains, public services, and emerging implementations. He shows how DTI is not just a set of technologies but a framework for real-world transformation.

"Artificial intelligence is no longer a niche tool; it's becoming an ever-present digital companion."

DON TAPSCOTT
EXECUTIVE CHAIRMAN
BRI

Finally, the third part explores design and deployment. How do we move from concept to implementation? What does governance look like in a decentralized environment? Doug presents a road map, starting with local pilots, then scaling to national, and eventually cross-border ecosystems. He outlines public-private partnership models, security by design, AI trustworthiness, change management, and digital sovereignty.

The conclusion is clear: we must act now. Digital trust infrastructure isn't just a strategy for technology—it's an economic, social, and democratic imperative. It offers concrete enterprise and ecosystem benefits, but it also offers us something greater: another chance to realize a fairer, smarter, more resilient digital society.

We have the tools. We have the knowledge. What we need is the will.

This paper is a call to action. Please read it not just as a proposal, but as a blueprint for any nation ready to lead in the global digital economy and for any company ready to collaborate in building it.

DON TAPSCOTT
EXECUTIVE CHAIRMAN
BRI

Idea in brief

- Businesses increasingly rely on digital tools, but today's tools often fall short. They are slow, costly, fragmented, and prone to fraud. Centralized models create single points of failure and increase risk of vendor lock-in. Compliance, trust, and interoperability remain major challenges.

- *Digital trust infrastructure* (DTI) shifts how organizations handle data. Instead of the traditional "collect and store" model, DTI takes a "request and verify" approach with verification, privacy, and accountability built in from the start. It replaces fragmented digital identity systems with a shared foundation for trust across the digital economy.

- DTI is a layered, vendor-neutral approach built on open standards. It includes:

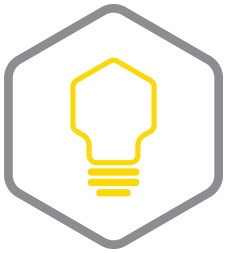
  - A trusted data fabric secured by cryptographic proofs.
  - Portable digital identities and credentials for people, organizations, and devices.
  - Authoritative registries of verified participants.
  - Programmable value systems that automatically trigger payments or actions when conditions are met.
  - *Artificial intelligence* (AI) that operates only on verified, trustworthy data.

DTI implementation depends on balancing institutional trust with individual privacy. Clear governance, roles, standards, and trust registries are essential.

- The success of DTI implementation depends on balancing institutional trust with individual privacy. Clear governance, roles, standards, and trust registries are essential. To prevent fragmentation and maintain interoperability, open standards must connect systems so that participants can exchange data across jurisdictions and platforms.

- DTI delivers tangible benefits: faster onboarding, lower fraud and compliance costs, seamless verification across borders, and more resilient operations.

- Together, these elements make trust an infrastructure-level capability that organizations, governments, and individuals can use to coordinate with confidence.



Introduction

Over the past decade, digital transformation has become central to business strategy. According to McKinsey, 90 percent of companies are pursuing some form of digital transformation, yet 70 percent of these initiatives fail to deliver expected results.[1]

History shows that transformative technologies achieve their greatest impact only when they evolve into infrastructure: shared systems that reduce friction and increase predictability and collaboration at scale. Roads, railways, and telecommunication networks illustrate how infrastructure allows coordinated activity far beyond what any single organization can achieve alone.

In the digital era, trust plays the same foundational role as those networks. DTI turns uncertainty into reliability. It allows organizations to verify identities, entitlements, and data without unnecessarily exposing sensitive information. As Dr. David A. Jaffray, senior vice president and chief technology and digital officer of the University of Texas MD Anderson Cancer Center, observed, "The big business truth is that no one knows what truth is anymore."[2] This lack of a common understanding of truth severely compromises commerce and undermines trust. By embedding verification, privacy, and accountability into digital systems, DTI reduces friction and lowers the cost of compliance, with seamless cross-industry and cross-border collaboration.

"The big business truth is that no one knows what truth is anymore."

DR. DAVID A. JAFFRAY
Senior Vice President and Chief Technology and Digital Officer
University of Texas MD Anderson Cancer Center

Today's digital systems often rely on "collect and store" models that are slow, costly, and vulnerable to fraud. Business leaders face a dilemma: they need digital tools for efficiency and growth, yet existing systems frequently fail to provide trustworthy, interoperable, and privacy-preserving solutions. Centralized models create single points of failure and increase dependence on specific vendors, while inconsistent standards slow collaboration and innovation.

DTI offers a new approach. Instead of hoarding data, organizations can "request and verify" information on demand. Portable credentials, machine-verifiable proofs, and shared trust frameworks make sure that parties exchange only the right data, in the right context, with built-in safeguards for privacy and compliance.

Early examples of large-scale *digital public infrastructure* (DPI)—such as India Stack, MOSIP, and Estonia's X-Road—demonstrate how open, interoperable platforms can make identity, payments, and data exchange accessible at a national scale.[3] These systems reduce transaction costs, improve access, and provide a foundation for innovation. DTI builds on and extends these lessons for enterprise and cross-border transactions. It combines verified digital identities, authoritative registries, programmable value systems, and AI-driven insights into a layered architecture that makes digital interactions inherently reliable.

This white paper guides business leaders, policymakers, and strategists through the DTI landscape. Its goals are to:

1. Explain DTI in practical terms by outlining its core building blocks and design choices;
2. Demonstrate its business and policy value through real-world examples;
3. Offer guidance on how to implement DTI at scale; and
4. Connect these insights to evolving regulatory and international frameworks.

Part 1 maps the DTI stack and shows how trusted data fabric, digital identity, authoritative registries, programmable payments, and embedded intelligence work together to move decisions and value with confidence.

Part 2 highlights sectoral applications of DTI and demonstrates how it is already transforming industry—finance, healthcare, education, supply chains, and public services—and what is possible as adoption scales.

Finally, Part 3 provides practical guidance on designing and deploying DTI. It covers governance, security, operational practices, and cross-jurisdictional policy considerations that keep systems trustworthy, scalable, and effective.

At its core, DTI is about coordination. It gives organizations a means of proving who they are, what they are entitled to do, and whether information is current, without exposing more than necessary. This level of coordination transforms compliance from a costly afterthought into a real-time process and makes collaboration across industries programmable, auditable, and resilient.

Embedding trust into digital infrastructure has tangible business benefits. Leaders can expect faster onboarding, lower fraud and compliance costs, seamless cross-border verification, and greater resilience against regulatory, vendor, or cyber risks. The premise is simple but transformative: trust becomes infrastructure for coordination at digital speed on a global scale.

The key idea is simple: trust becomes an infrastructure-level capability so that businesses can coordinate with confidence.

Part 1: The DTI stack

A trusted digital economy requires more than faster networks or bigger databases; it needs a mechanism that assures the trustworthiness of information wherever it travels. The foundation of DTI is a trusted data fabric that secures identities, transactions, and other records with verifiable proofs, so that information from

multiple sources can reliably integrate. Distributed ledgers provide tamper-evident integrity; different entities can verify facts across organizational boundaries.

At the core of DTI is a trusted data fabric that secures identities, transactions, and other records with verifiable proofs so that information from multiple sources can integrate reliably.

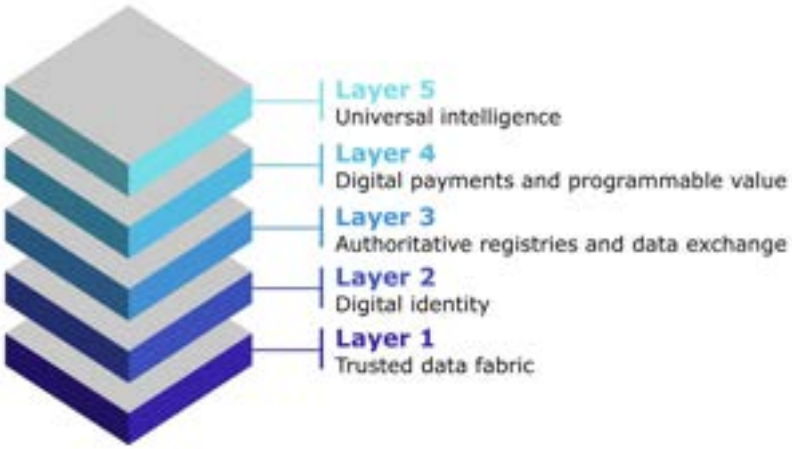
Built on the trusted data fabric are layers that secure and preserve private interactions. With *decentralized identifiers* (DIDs) and verifiable credentials, people, businesses, and devices can prove who they are and what they are authorized to do. Registries and data exchange protocols govern flows of information. Programmable value systems allow automated payments or conditional transfers. AI strengthens the stack by detecting anomalies, managing risk, and supporting decision-making, all powered by verified, high-integrity data.

This section explores each layer of the DTI stack (Figure 1). It introduces the role of each component, key design choices, and the trade-offs that enterprises face when implementing them. These layers form a coherent architecture, which organizations can use to exchange information and value at digital speed on a global scale while maintaining trust, security, and regulatory compliance.

Layer 1: A trusted data fabric

A trusted data fabric draws on diverse data sources, combining their distinct strengths. Government databases increase the reliability of the trusted data fabric through institutional reputation and legal enforcement: regulation requires parties to validate information, and regulatory compliance and oversight deter tampering. Regulated institutions (e.g., banks and hospitals) manage sensitive data such as payments or health records. Technology platforms (e.g., Google, Facebook, and Amazon) play a complementary role by verifying identities, managing large volumes of user data, and acting as custodians of "extended identity" in the digital economy. *Distributed ledger technology* (DLT), including blockchain, adds a decentralized, tamper-evident layer for digital interactions across industries beyond cryptocurrency.

Figure 1: Layers of the DTI stack



The trusted data fabric underpinning DTI combines these sources to deliver verifiable services across enterprise systems, government records, *Internet of Things* (IoT) devices, registries, credentialing platforms, and AI ecosystems. Traditional databases (e.g., those used to record transactions or store images) are typically selected for performance or cost efficiency, and they remain the backbone of most enterprises. However, their trustworthiness depends largely on the managing organization's reputation or regulatory oversight, thereby limiting their effectiveness in distributed, multi-jurisdictional environments. Solutions are emerging to address these limitations. "While you can't drop legacy cores," said Ian Putter, chief evangelist at Aurachain, "you can fix data outside the system and build the new data fabric."[4] This approach allows organizations to strengthen trust without replacing their existing systems.

"While you can't drop legacy cores, you can fix data outside the system and build the new data fabric."

IAN PUTTER
Chief Evangelist
Aurachain AG

Truth anchors

Distributed ledger technologies act as "truth anchors" to strengthen these existing data stores. Ledger systems provide tamper-evident time stamps, consensus-based ordering, and immutable references, so that no single entity can alter records unilaterally. The ledger itself typically does not store the underlying data; instead, authorized parties use it to publish attestations, event logs, and cryptographic proofs, such as digital signatures or *hashes*.

A modern trust architecture integrates rather than replaces existing systems. Proprietary databases continue to store operational data when privacy, scale, and performance matter most. Permissioned blockchains, operated by vetted consortia, support secure and controlled collaboration among enterprises and government agencies. Permissionless blockchains, on the other hand, serve as neutral public anchors for information, so that no single participant can alter shared facts. Interoperability comes from a clear division of labor. Systems of record maintain detailed data, whereas blockchains store cryptographic proofs that verify authenticity, timing, and integrity. This approach lowers onboarding costs, simplifies reconciliation, accelerates audits, and improves overall reliability.

A modern trust architecture connects *rather than* replaces *existing systems.*

Such a hybrid model balances governance with risk control. Sensitive information (e.g., personally identifiable information, trade secrets, or pricing) remains in secure databases under legal and contractual protection. Blockchains record tamper-evident "fingerprints" of this data, along with status signals such as "valid," "revoked," or "expired," and maintain version-controlled policies. Permissioned networks deliver enterprise-grade throughput and accountability, while permissionless networks offer neutrality and global transparency. This approach provides shared assurance without requiring all parties to use the same platform or vendor.

By anchoring off-chain data such as registries, records, or credentials to a distributed ledger, organizations across jurisdictions can independently verify claims without exposing sensitive information or mandating system uniformity. By sharing this layer of trust,

enterprises, governments, and regulators can validate integrity, preserve privacy, and maximize flexibility.

Several industries are already taking this truth-anchoring approach. In supply chains, it improves traceability, product authenticity, and compliance with ethical sourcing standards. For example, DLT-based solutions such as IBM's Food Trust enhance food safety and transparency, and Singapore's TradeTrust simplifies cross-border trade.[5] In financial services, DLTs streamline audits, secure payments, and support trade financing. For example, on J.P. Morgan's Kinexys Liink network, banks can validate account details before sending payments.[6] In health care, parties use DLT to manage and share patient data securely. The Synaptic Health Alliance, which includes Humana, UnitedHealth Group/Optum, and MultiPlan, uses a permissioned ledger to coordinate provider-directory updates across member systems.[7] And Estonia's e-government platform uses the truth-anchoring model to time-stamp and preserve the integrity of records across health, land, and business registries.[8]

In each case, the same principle applies: by anchoring trust to the fabric of digital interactions, organizations can reduce friction, simplify compliance, and create new opportunities for efficiency and growth.

By anchoring trust to the fabric of digital interactions, organizations can reduce friction, simplify compliance, and create opportunities for efficiency and growth.

Zero-knowledge proofs

An essential feature of a blockchain-based truth anchor is its ability to support *zero-knowledge proofs* (ZKPs). ZKPs allow one party to prove that a statement is true without revealing the underlying data. Within a DTI, this means sensitive records can be transformed into privacy-preserving yes/no answers: a business can prove that a supplier is not sanctioned, a user is over 18 years of age, or a device is certified, while sensitive data (e.g., date of birth, supplier name, device type or series number) remains with its owner.

This approach reduces data exposure and breach risk, limits the information organizations must store and audit, and gives regulators verifiable evidence that participants are following rules. ZKPs pair naturally with verifiable credentials and trust registries for real-time, policy-aware checks across organizations and jurisdictions. With this foundation, ZKPs enhance privacy, security, and compliance in identity verification and deliver assurance without sharing unnecessary data, both of which are essential to digital identity.

Layer 2: Digital identity

After establishing a trusted data fabric, digital identity becomes the core building block of DTI. It connects people, organizations, devices, and AI agents to accountable actions and verifiable rights, so that every credential, policy check, and payment can be trusted, attributed, and privacy-preserving across networks and jurisdictions. Digital identity is the entry key to participation: it determines who can access services, exercise rights, and transact across organizational and national boundaries.

Today, digital ID remains fragmented, and many implementations carry risks. As Jonathan LLamas, vice president of decentralized strategy at WISeKey, observed, "Government atomic identity underpins democracy, but online the big platforms have become the authority, a conflict of interest."[9]

"Government atomic identity underpins democracy, but online the big platforms have become the authority, a conflict of interest."

JONATHAN LLAMAS
Vice President of Decentralized Strategy
WISeKey SA

The economic potential of a secure, privacy-preserving, and widely accepted digital ID system is substantial. In 2019, the McKinsey Global Institute estimated that, depending on adoption rates and interoperability, universal digital identity coverage could unlock between 3 percent and 13 percent of global gross domestic product by 2030.[10]

From health care eligibility and school enrollment to cross-border payments, remote work, and social benefits, the ability to assert identity quickly, privately, and reliably is essential. Governments worldwide are advancing digital ID programs. In India, people use Aadhaar to access subsidies, welfare programs, financial services, and mobile-based services.[11] The European Union (EU) is developing the EU Digital Identity Wallet to support cross-border transactions and give residents control over their personal data, including what they share with public and private entities.[12] Estonia's e-ID system and Singapore's Singpass are very advanced.[13] In Australia, myGov and myID have formed a federation of accredited providers; citizens can securely access over 80 federal and state government services.[14]

Bhutan's National Digital Identity (NDI) program exemplifies the new wave of privacy-preserving, standards-based identity systems worldwide. It takes a standards-based approach to building trust in digital interactions, expanding inclusive access to services (i.e., particularly in remote districts), and reducing costs. Launched nationwide in October 2023 under the Digital Drukyul flagship, the program adopted *self-sovereign identity* (SSI) principles to give users control over their identities when accessing digital services.[15] Officials expect NDI to curb fraud, corruption, and resource leakage, and to cut administrative processing times across government departments by up to 60 percent over the next three years.[16]

Components of identity

Think of digital identity as operating in layers, each one adding more confidence and context.

In the digital era, identity is not just "identification." Instead, identity is better understood as a set of trusted claims about an individual, organization, or device that can be securely shared and instantly verified. Think of digital identity as operating in tiers, each tier adding greater confidence and context.

1. **Core identity** is the foundation. It is the basic link between a subject and an identifier, strong enough for high-stakes use cases such as a passport or government-issued ID.

2. **Structured entitlements** add authoritative information from trusted sources. These might include professional licenses, academic degrees, payroll records, or credit histories.

3. **Contextual reputation** reflects the social and behavioral signals we use to make decisions about trust. It includes things like ratings, endorsements, professional profiles, and even digital content. While these signals are not authoritative on their own, they shape an individual's reputation.

4. **Operational identity**, or the "identic" tier, introduces a software-based AI agent owned by the user that can act on their behalf.[17] This agent holds a decentralized identifier, cryptographic keys, and a digital wallet. Within this layer:

    a. *Mandate credentials* prove the agent is authorized to act on behalf of the user;

    b. *Capability credentials* specify what the agent is allowed to do, such as querying records, authorizing payments, or sharing data, and within what limits; and

    c. *Operational attestations* provide transparency about the agent itself, such as its software version or AI model build.

With this layered approach to identity, users are not just proving but acting upon identity, automating processes, reducing fraud, and sharing only the data needed.

With this tiered approach, users are not just proving identity but acting upon it, automating processes, reducing fraud, and sharing only the necessary data with the right parties at the right time.

Centralized and decentralized identity models

How we issue, store, and use identity can shape everything from customer experience to cybersecurity risk, and even a company's ability to innovate and enter new markets. Digital identity systems generally fall into centralized or decentralized categories, which differ in how they manage, verify, and control identities.

Most of today's digital identity systems are centralized. Examples include government *electronic IDs* (eIDs), enterprise login systems, online banking credentials, and single sign-on systems run by big tech companies. In this model, a single identity provider issues and manages the identity, acting as an intermediary that verifies users in all transactions.

Centralized identity models have clear advantages. They are simple and familiar, offering an easy experience for end users and system administrators alike. They scale efficiently because they are built on mature, reliable platforms that businesses have trusted for decades. They also benefit from clear rules of the road, including well-established liability, compliance, and audit frameworks that give enterprises confidence when using them.

However, centralized systems also carry well-known limitations. Because everything depends on a single provider, they represent a single point of failure. If that provider is hacked or goes offline, every account linked to it could be at risk. Centralized models also

tend to create "walled gardens," locking digital identities within a single domain. Moving them across jurisdictions or platforms often requires custom agreements, expensive integrations, or even re-registration. Finally, when organizations tie identities to one vendor or government, they face lock-in risk and may have limited leverage to negotiate changes or exit the relationship.

Decentralized systems give users more control over their own data, which can help build trust and meet growing privacy expectations.

Creators of decentralized identity models designed them to address many of the limitations of traditional, centralized systems. Instead of depending on a single authority, they let individuals and organizations own and manage their own identifiers and credentials. This approach brings identity closer to the user, so that the user can move seamlessly across platforms, borders, and business relationships. Several open-source networks have already deployed self-sovereign digital identity solutions. For example, individuals and organizations can use the Cardano Foundation's Veridian platform to manage their digital identities, verifiable credentials, and data with greater control and privacy.[18]

For business leaders, the benefits are significant. Decentralized systems give users more control over their own data, which can help build trust and meet growing privacy expectations. Users can selectively disclose only the information required for a transaction. Because decentralized systems are built on open standards, they can support seamless interoperability across multiple domains and reduce dependency on any single vendor.

That said, decentralized identity systems are not without challenges. First, since they rely on cryptographic keys that users control, losing those keys can mean losing access. That is a risk that robust recovery mechanisms can mitigate. Second, the user experience is still maturing, and onboarding processes can be complex for those unfamiliar with concepts like digital wallets. Third, lack of interoperability among competing DID methods, credential formats, and protocols can also fragment the ecosystem and hinder adoption. Finally, important governance questions remain: who accredits issuers of credentials, who is liable when a party uses false credentials, and how do parties resolve disputes across national or legal boundaries?

In practice, most ecosystems are moving toward a hybrid approach that combines the best of both worlds.

In practice, most business ecosystems are moving toward a hybrid approach that combines the best of both models. Centralized systems still serve as a foundation because they are widely trusted, easy to scale, and governed by well-established legal frameworks. On top of this foundation, governments and enterprises are beginning to layer decentralized credentials so that users can carry their verified information across platforms and share only what's necessary for each interaction. The result is a model that balances institutional trust and stability with individual privacy and flexibility.

Decentralized identifiers and autonomous identifiers

Digital identifiers apply not only to individuals but also to organizations, devices, and autonomous agents. A hospital, a

logistics firm, a sensor in a shipping container, or a policy-bound software agent needs the ability to authenticate, assert capabilities, and perform verifiable actions in the digital economy.

In fact, verifying the identity of a counterparty is critical in almost every business transaction. However, the process is often slow, costly, and prone to errors. Confidence in identity reduces fraud, streamlines onboarding, and expedites service delivery. When trust is lacking, interactions can stall, disputes can arise, and operational costs can increase.

"Payments and onboarding are still the biggest pain. … If we verified signatory rights up front, many disputes would vanish."

DR. FLORIAN HERZOG
Chair, Founder, and Chief Technology Officer
Deon Digital AG

Traditional centralized digital ID systems help address some of these challenges, but they are imperfect and often create friction. According to Dr. Florian Herzog, founder, chair, and chief technology officer of Deon Digital in Zurich, "Payments and onboarding are still the biggest pain. Cross-border wires get held for weeks for [anti-money laundering] even when the counterparty is fine."[19] He added, "A frequent fraud trick is signing without legal authority. … If we verified signatory rights up front, many disputes would vanish."

Standardized DIDs and *autonomous identifiers* (AIDs) resolve many of these challenges. DIDs are globally unique, cryptographically verifiable identifiers controlled directly by a person, organization, or device, without the need for a central registry. For example, a coffee producer can assign a unique DID to batches of coffee beans. Registering that DID on a blockchain within the trusted data fabric creates a permanent, tamper-evident record of origin and movement of those coffee beans. As the batches of beans move through the supply chain, each participant can verify its role using its own DID, with transparency and accountability at every step. This record can help the coffee company quickly resolve disputes about origin or authenticity of its beans, give auditors a verifiable trail of transactions, and demonstrate compliance with regulations governing food safety, labor standards, or sustainability claims.

Autonomous identifiers *are self-certifying, meaning other parties can confirm their integrity using only the identifier itself and its associated cryptographic information.*

AIDs take this a step further. They are self-certifying, meaning their integrity can be confirmed using only the identifier itself and its associated cryptographic information. This feature makes them particularly valuable when parties must establish trust directly, without consulting an external system. For example, a smart thermostat provisioned with an AID at the time of manufacturing could identify itself to a home hub, establish a secure channel, and operate without querying a central database. The same principle applies to AI-powered identic agents. An identic agent acting on behalf of a person could receive an AID upon creation, use it to sign transactions, and participate in governance within a *decentralized autonomous organization* (DAO). Other members of the DAO, whether human or digital, could then cryptographically verify that an authorized agent truly originated all actions.

Together, digital and autonomous identifiers serve as the core of digital trust. Each makes identity not only verifiable, but portable and interoperable across networks.

Verifiable credentials: Signed, temper-evident claims

Verifying identity is only part of the trust equation. Equally important is knowing what counterparties are authorized to do and what claims they can make. In business transactions, leaders need to know who a person is and whether the person's claims about roles, qualifications, or permissions are reliable. This is the role of verifiable credentials.

Verifiable credentials are cryptographically signed and tamper-evident assertions issued by a trusted authority about a person, organization, device, or agent.

A *verifiable credential* is a cryptographically signed and tamper-evident assertion issued by a trusted authority about a subject, whether that subject is a person, organization, device, or agent. Holders of verifiable credentials store them securely, typically in a digital wallet so that they can present them whenever a party needs verification. Because they are cryptographically protected, parties can validate information instantly without relying on paper documents, emails, or manual checks.[20]

Verifiable credentials can cover a spectrum of information. They may represent core identity attributes (e.g., a legal name linked to a national ID) or more specific claims (e.g., "licensed to practice medicine until 2026"), which speed verification, preserve privacy, and comply with legal and governance requirements. They are also essential for establishing a person's "authority to sign" in transactions.

In corporate contexts, verifiable credentials help to confirm authority in business transactions. For example, knowing who can legally sign contracts or commit corporate resources is critical. A *signatory credential*, issued by a recognized authority such as a company secretary or corporate registry, provides this assurance.[21] It verifies the individual's identity, specifies the individual's authorized actions (e.g., this person may approve contracts up to a certain value), and confirms the validity period of that authority.

For enterprises, verifiable credentials have three powerful characteristics. First, they are *portable*: their holders can use them across organizations and jurisdictions without complex integrations. Second, they are *privacy-preserving*: their holders share only the information necessary. Third, they are *machine-verifiable*: other parties can confirm their authenticity, issuer authority, and status almost instantaneously. With these capabilities, organizations can reduce fraud, simplify operations, and rely on digital claims in real time.

A verifiable presentation is a specific, verifiable proof that answers a question about a party without exposing unrelated information.

Verifiable presentations: Context-specific proofs

In most transactions, parties need not reveal all details behind a credential. What they usually need is a specific, verifiable proof that answers a question without exposing unrelated information. This is the role of a *verifiable presentation*.

Using a verifiable presentation, the holder of one or more verifiable credentials can assemble and share a subset of information, or a

cryptographic proof derived from those credentials, in response to a request from a verifier.[22]

While a verifiable credential represents signed, tamper-evident data, the verifiable presentation is a dynamic, context-specific proof created for a particular interaction. Examples include a digital boarding pass to prove eligibility for duty-free shopping, or an age-related credential that shows whether a person is at least 18 years old, but not how old, let alone an exact birthdate. The ability to generate these context-specific proofs gives individuals and organizations greater control over what they disclose, when, and to whom.

Verifiable presentations are especially valuable when parties must aggregate complex assertions involving multiple credentials. For example, a digital product passport may combine material attestations, facility certifications, and transport records. Using verifiable presentations, auditors can trace the chain of trust and verify compliance without accessing sensitive raw data such as detailed bills of materials.

Verifiable presentations also streamline regulatory oversight. Rather than submitting entire datasets, organizations can demonstrate compliance with specific policies, such as "all suppliers are ISO 14001 certified" or "beneficial ownership screening was performed on [specific date]," while minimizing exposure of personal data or sensitive information.

For DTI, this selective disclosure is essential. Standardization of data models and interaction patterns for verifiable credentials and verifiable presentations makes for interoperability across systems, simplifies adoption at scale, and allows enterprises to confidently integrate verifiable digital claims into everyday business processes.

"What stops someone from creating a fake ID? Platforms can let anyone claim an identity; issuer trust must be verifiable. ... Trust registries are the missing link in digital ID."

ILÁN MELÉNDEZ
Ecosystem Lead, LNet Inter-American Development Bank

Trust registries and compliance

Ilán Meléndez, ecosystem lead for LNet (formerly LACChain) at the Inter-American Development Bank, identified a critical issue with digital credentials: "What stops someone from creating a fake ID? Platforms can let anyone claim an identity; issuer trust must be verifiable."[23]

A trust registry *is an authoritative list of approved issuers of decentralized credentials along with the legal basis for their authority.*

Identifiers, credentials, and presentations become operationally meaningful only when their issuers are trusted. The key question is, who has authority to issue or vouch for what? Trust registries provide that answer. As Meléndez noted, "Trust registries are the missing link in digital ID" and a central focus of LNet.[24]

A *trust registry* is an authoritative list of approved issuers along with the legal basis for their authority. These registries make decentralized credentials reliable and verifiable at scale, particularly in regulated environments. For example, a registry might list licensed banks, government agencies, or accredited certification authorities.

Using standardized and machine-readable registries, agents or wallets from different vendors or jurisdictions can interoperate while complying with local rules.

This allows verifiers to distinguish authoritative credentials from self-asserted claims. Real-world examples are already emerging:

- *EU Electronic Identification, Authentication, and Trust Services* (eIDAS) provide a machine-readable record of qualified trust service providers across Europe.[25]
- *Global Legal Entity Identifier Foundation* (GLEIF) maintains the global registry of Legal Entity Identifiers, so that verifiers can confirm the legitimacy of corporate entities.[26]
- *LNet* (formerly LACChain and LACNet) builds registries for issuers across Latin America and the Caribbean, anchoring legal and compliance frameworks into digital credentials.[27]

Regulators can also mandate inclusion in trust registries. For instance, *anti-money laundering* (AML) or *know-your-customer* (KYC) providers may be required to register so that only entities meeting legal and supervisory standards are recognized. Registries also serve as auditable reference points, where verifiers prove that an issuer was in good standing when issuing a credential.

With standardized and machine-readable registries, wallets, agents, and verifiers from different vendors or jurisdictions can interoperate while respecting local compliance rules. In effect, decentralized credentials are usable and governable at scale.

The DID life cycle

The life cycle of a DID includes three main stages. The first stage is *issuance*, during which the subject (e.g., a person, a company) or its administrator generates the identifier along with its cryptographic keys. When necessary, the subject may also undergo identity assurance and link the identifier to authoritative records, such as a company registry or a legal entity identifier, thereby establishing a trusted foundation.

The second stage is *credential use*. The holders can use these identifiers to present associated verifiable credentials and verifiable presentations in business transactions. Verification involves confirming that a trust registry recognizes the issuer, validating credential integrity, checking for revocation, and applying relevant policy or compliance rules so that counterparties can confidently rely on the claims presented.

The third stage is *revocation and rotation*. Cryptographic keys can be rotated or recovered if necessary, and any revocation or updates are recorded in tamper-evident, auditable systems. These records may reside either directly on a blockchain or in off-chain storage anchored to a blockchain within the trusted data fabric, providing a permanent and verifiable trail of identity changes.

Throughout this life cycle, digital identities remain secure, verifiable, and adaptable over time. They also lay the groundwork for the next challenge: protecting privacy and ensuring sovereignty.

Privacy, data sovereignty, and regulation

The principle of minimal disclosure is central to DTI and important in meeting privacy and regulatory requirements.

The principle of minimal disclosure is central to DTI and especially important when addressing privacy and regulatory requirements. With DTI, enterprises can more easily adopt privacy-by-design practices such as data minimization, purpose binding, and user control over disclosure.

These practices must align with global and regional frameworks such as the EU General Data Protection Regulation (GDPR), eIDAS regulation, and sector-specific laws like the US Health Insurance Portability and Accountability Act (HIPAA).[28]

DTI technologies also create an opportunity to revisit and modernize existing regulations. For example, MD Anderson's Dr. Jaffray suggested that "HIPAA has to be re-examined; de-identification is clearly flawed," and that health care needs to shift toward a consent-based model with selective disclosure.[29]

By standardizing identity models that support verifiable, selective presentations, DTI can enhance productivity while still preserving privacy and sovereignty. Personally identifiable information (PII) remains securely within governed systems, while only cryptographic proofs are anchored to decentralized ledgers rather than centralized records.

Practical digital identity in DTI

A robust digital identity ecosystem delivers tangible benefits across stakeholders, from policymakers and business leaders to enterprise architects and compliance and risk teams.

In most real-world implementations of DTI, the most effective approach will be hybrid. Governments, regulators, banks, and other authoritative entities will continue to issue high-assurance credentials, but as verifiable ones bound to DIDs. This model preserves the legal legitimacy of issuers and the privacy, portability, and flexibility for holders in everyday use. A policy engine makes sure that each transaction applies the principle of least privilege and discloses only the minimal proof required.

A robust digital identity ecosystem delivers tangible benefits across stakeholders. For policymakers, it balances rights-preserving portability with stronger regulatory oversight, reduces the cost of gathering evidence, improves institutional governance, and enhances auditability. For business leaders, digital identity reduces friction in transactions, cuts fraud risk, and accelerates onboarding of customers and partners; organizations can move faster and operate more efficiently. For those who oversee enterprise architecture, it minimizes vendor lock-in, automates policies, and simplifies integration across multiple systems and ecosystems. Compliance and risk teams also benefit: digital identity reduces unnecessary

exposure of sensitive data, streamlines compliance workflows, and aligns privacy protections with regulatory requirements.

A digital identity ecosystem built on open standards with strong governance shifts identity from a static, one-time verification step to a dynamic control surface. Organizations, devices, and agents can collaborate securely at scale while preserving their privacy, sovereignty, and auditability. Confidence in a counterparty's identity and credentials is essential to business transactions, as is confidence in the veracity of the information conveyed.

A digital identity ecosystem built on open standards with strong governance shifts identity from a static, one-time verification step to a dynamic control surface.

Layer 3: Authoritative registries and data exchange layers

Confidence in data accuracy is key to reducing friction in transactions. The trusted data fabric can guarantee that information has not been altered, but it cannot verify that the parties providing the information are trustworthy. Authoritative registries and data exchange layers address this gap by validating the source of the data and making sure that parties can share it reliably across trusted networks.

Authoritative registries

In contrast to trust registries of those authorized to issue or verify credentials, authoritative registries serve as definitive sources of truth for critical data. Curated by trusted stewards such as government agencies, regulatory bodies, or industry associations, these registries maintain legally recognized records about entities, licenses, credentials, products, and other regulated assets. Authoritative registries act as root record keepers within the DTI; they provide verified datasets that parties can reliably reference across ecosystems. Examples include national business registries that track incorporation and legal status, professional licensing boards for doctors, lawyers, or engineers, the Legal Entity Identifier system for corporate identity, and sector-specific registries for product codes, health procedures, or property ownership.[30]

Authoritative registries warrant data accuracy and legal validity, whereas trust registries confirm authorization to issue credentials.

While some authoritative registries may also function as trust registries by publishing issuer signing keys, their roles are distinct. Authoritative registries warrant data accuracy and legal validity, whereas trust registries confirm authorization to issue credentials.

Oracles: Trusted bridges to external data

Where registries establish who and what can be trusted, oracles determine how trusted data flows *into* digital ecosystems. Oracles act as trusted digital bridges that pull external, off-chain data into blockchain or DTI ecosystems in a way that preserves data integrity and verifiability.

By signing, time-stamping, and anchoring external data, oracles assure integrity and help systems to respond dynamically to updates.

Traditionally used in blockchain contexts, oracles supply real-world inputs such as exchange rates, shipment updates, or IoT sensor readings to smart contracts, to automate actions such as buy or sell orders, messages to customers, or adjustments to thermostats. Within DTI, oracles expand this functionality by linking authoritative external data sources, like national registries, licensing authorities, customs databases, or regulated IoT networks, into the trusted data fabric. By signing, time-stamping, and anchoring external data, oracles provide integrity assurance and allow systems to respond dynamically to real-time updates, such as revoked licenses or updated sanctions lists.

Oracles work in tandem with trust registries and authoritative registries to provide reliable, up-to-date information and trigger event-driven processes, adaptive automation, and real-time compliance. Those capabilities are essential to such sectors as finance, health care, logistics, and public services.

Data exchange layers

Once data is verified and made available, *data exchange layers* (DELs) make sure it moves securely and efficiently across systems. DELs form the connective framework of DTI, for secure, policy-compliant data sharing across jurisdictions, sectors, and platforms. By standardizing complex system interactions into standardized interfaces, DELs allow trusted data to flow between government agencies, enterprises, and regulated ecosystems while preserving data sovereignty.

An example of a DEL in practice is X-Road, a secure data exchange system between private and public sector organizations.[31] X-Road is currently used in Estonia and Finland, with other countries considering adoption.[32] Another example is HL7 FHIR (i.e., fast health care interoperability resources), a widely used standard for exchanging health care data.[33] These implementations highlight how well-governed interoperability layers can combine legal trust frameworks with technical enforcement to deliver reliable, cross-domain data sharing.

DELs must meet the highest security standards. That means safeguarding the integrity and authenticity of data, encrypting information in transit and at rest, implementing strong authentication and role-based access control, and validating endpoints against trusted sources. Without these safeguards, DELs could become systemic vulnerabilities within an otherwise secure DTI. When designed correctly, however, DELs facilitate reliable, scalable, and compliant data exchange and form the backbone for trusted digital ecosystems across industries.

Layer 4: Digital payment systems and programmable value

With "programmable money," parties can embed policies into payments to reduce fraud, lower reconciliation costs, and automate just-in-time, rules-compliant transactions at scale.

The next layer of DTI consists of *digital payment systems*, where verifiable data translates into economic action (Table 1). These systems move value between parties in a secure, automated, and regulation-compliant manner. They make what is often called "programmable money" possible. By integrating identity and credentials into payment workflows and validating them against trust registries, these systems execute payments only when predefined rules and conditions are satisfied. Parties can set conditional disbursements, comply with AML/KYC before funds move, and confirm recipients against approved trust lists. Embedding these policies into payment systems reduces fraud, lowers reconciliation costs, and supports just-in-time, rules-compliant financial automation at scale.

Table 1: Typology of digital payment systems

Type	Description	Examples
RTGS (Real-time gross settlement)	Central-bank-run systems for high-value, real-time interbank settlements	Fedwire (US), TARGET2* (EU), Clearing House Automated Payment System (CHAPS, UK), BOJ-NET‡ (Japan)
Instant retail payments	Always-on, low-latency account-to-account transfers with features like aliasing and QR-based initiation	SEPA Instant (EU), FedNow (US), RTP (US), UPI (India), Pix (Brazil), NPP (Austria), Interac (Canada)
Automated clearing house (ACH)/batch networks	Deferred settlement systems for payroll, bills, and mass payouts, often programmable via rule engines	ACH (US), Single Euro Payments Area (SEPA), Credit/Debit (EU)
Card schemes	Global consumer networks with built-in dispute resolution, tokenization, and strong identity integration	Visa, Mastercard
Mobile money/e-money	Stored-value accounts for retail payments and remittances, typically offered outside traditional banks	M-Pesa (Kenya), Airtel Money, licensed electronic money institution (EMIs)
CBDCs	Digital fiat issued by central banks; may be account- or token-based, with features like offline use and privacy protections	Digital yuan (China), e₹ (India), Sand dollar (Bahamas)
Stablecoins and regulated tokenized money	On-chain fiat equivalents backed by reserves; support programmable, global, 24/7 settlement	USD Coin (USDC), USD Tether (USDT), tokenized deposits

**Trans-European automated real-time gross settlement express transfer system; ‡ Bank of Japan Financial Network System*

Digital payment rails

Regulated tokens (e.g., some stablecoins and CBDCs) are better positioned to meet enterprise and policy requirements today for large-scale adoption.

Modern digital payment rails are designed to be programmable, auditable, continuously available, and inclusive. Users can program smart disbursements, escrows, trade settlements, and other policy-driven transfers. They can audit cryptographic proofs rather than bulk personal data. The rails operate reliably 24/7 around the globe to improve cash flow certainty and operational security. At the same time, verifiable logs and selective disclosure strengthen regulatory assurance. Over time, these capabilities may support new financial products and give governments better tools for macroeconomic policy.

The global payments sector is already immense. In 2023, traditional networks, including ACH, Visa, Mastercard, and SWIFT, processed $1.8 quadrillion in value across 3.4 trillion transactions.[34] While these networks are mature, robust, and scalable, they still face challenges, such as dependence on third-party operators, vulnerability to fraud, limited programmability, and continued exclusion of unbanked populations in some regions. As DTI evolves, token-based, programmable platforms offer complementary alternatives that expand flexibility, security, and automation in payments.

Central bank digital currencies (CBDCs) and stablecoins, when combined with DIDs and verifiable credentials, offer policy-aware transfers, automated compliance with regulations, low-latency disbursements, and strong privacy protections. These features align directly with the goals of DTI, to facilitate trustworthy, compliant, privacy-preserving, and interoperable transfers of value.

In contrast, most cryptocurrencies are currently less suited to serve as DTI payment rails, largely because of volatility, uncertain regulatory treatment, and unclear liability frameworks. Regulated tokens, including some stablecoins and CBDCs, are better positioned to meet enterprise and policy requirements today and provide a more reliable foundation for large-scale, trusted adoption. This assessment may evolve as new models for governance, compliance, and liability frameworks emerge.

The potential of programmable money

When parties use programmable money in social programs, for example, they can study program performance without exposing participants' personal details.

With programmable value exchanges, funds can move in controlled, automated, and policy-compliant manner. For example, a government could issue farmers subsidies that are restricted to approved purchases, such as farm equipment or fuel. By using digital credentials, trust registries, and programmable currency, governments can disburse public funds conditionally to eligible recipients in a secure, targeted, and fully auditable way.

The process begins with enrollment, during which a trusted government authority (e.g., a department of agriculture) issues each eligible farmer a digital credential that verifies details such as income, residency, and primary crop type. Farmers store these

credentials securely in their digital wallets and use them for all subsequent transactions. After enrollment, a treasury or regulated financial institution allocates funds to participants as programmable digital currency, such as a CBDC or stablecoin. Transactions occur only when specific conditions are met. The trusted government authority can embed policy rules into the system so that only verified recipients receive funds, to spend only at authorized merchants within a defined time frame.

When recipients make a purchase, their digital wallet discloses only the proof needed to verify eligibility for a subsidy and keeps other personal details private. Simultaneously, merchants validate their authorization without exposing unnecessary information. Smart contracts automatically execute the transaction after cross-checking both parties against trust registries and revocation lists. Once all verification conditions are met, the transaction settles instantly on a digital ledger or through a synchronized real-time payment system.

At every stage, oversight is built in. Regulators and supervisory bodies can audit compliance in real time using cryptographically verified proofs. They can also study aggregated, anonymized data to gauge program performance without exposing personal details. The result is faster, more accurate delivery of public support, reduced fraud and administrative costs, full auditability, and greater certainty for recipients and merchants. Because this system relies on standards-based, interoperable infrastructure, it can scale efficiently across programs and jurisdictions.

Real-world implementations of programmable money are emerging. For example, organizations are already using the Monetary Authority of Singapore's Purpose-Bound Money (PBM) protocol, which attaches programmable conditions to digital money such as CBDCs, tokenized bank deposits, or stablecoins, to restrict their use for specific purposes. The system is currently being tested in commercial-scale trials.[35]

Layer 5: Universal basic intelligence

Universal basic intelligence *is an emerging concept that several interviewees highlighted as potentially important to the future evolution of DTI.*

Universal basic intelligence (UBI) is an emerging concept that several interviewees highlighted as potentially important to the future evolution of DTI. In the context of DTI, UBI broadly refers to enhancing the creative process, data analysis, risk assessment, and decision-making capabilities of individuals, systems, and AI agents through accessible AI tools and resources. UBI serves two primary functions within DTI. First, as a cognitive backplane, it underpins fraud detection, data verification, cybersecurity, and systemic resilience across the digital stack. Second, as a service layer, it delivers a suite of generalized AI capabilities that can seamlessly integrate with diverse systems and workflows.

These capabilities include question-and-answer information retrieval systems that help small businesses identify partners and navigate licensing processes. Summarization and classification tools

In the context of DTI, UBI *broadly refers to enhancing the creative process, data analysis, risk assessment, and decision-making capabilities of individuals, systems, and AI agents through accessible AI tools and resources.*

streamline compliance reporting, while risk-scoring mechanisms support insurers and financial operators. Other uses include anomaly detection for cybersecurity analysts and real-time situational awareness tools to enhance supply chain performance.

UBI functions as an adaptive intelligence fabric capable of interpreting, reasoning, and learning across domains, data types, and contexts rather than specific use cases. Models deployed within a jurisdiction's DTI are trained on local, domain-specific data, so that they operate fluently within that environment's legal, regulatory, and cultural context. Policy engines operate alongside AI to preserve contextual integrity by evaluating consent, purpose, jurisdiction, and data retention so that automated actions remain lawful and proportionate.

Trust in AI output is critical. To achieve trust, parties need a clear, verifiable record of the data used to train the AI, the methods applied to process that data, the model itself, and the evaluations the model has undergone. Metadata linking AI outputs to their underlying data can be anchored in the trusted data fabric with cryptographic time stamps, for transparency and auditability. Governance registries track model details, risk classifications, and independent testing results, continuously monitor bias or drift, and trigger fallback mechanisms or human review when necessary. AI outputs can also include provenance tokens that reveal which data and rules were used to generate the result, as well as the methods used to consult external information.

Although many implementation details are still immature, this approach aligns with emerging regulatory frameworks such as the European Union AI Act, the US National Institute of Standards and Technology AI Risk Management Framework (NIST AI RMF), and International Standards Organization standards. Together, for auditability, these frameworks answer critical questions such as

Table 2: Comparison of the old model with the new one

Design choice	**Old infrastructure** *"Collect and store" model*	**Digital trust infrastructure** *"Request and verify" model*
Storage	Centralized databases	Distributed trust fabrics
Identity	Share personal data	Verify proofs
Interoperability	Vendor lock-in	Open standards
Compliance	After-the-fact enforcement	Real-time audit/verification
Security	Potential fraud exposure	Cyrptographic assurance

who approved the model, what data could the model access, which safeguards were applied, and which evaluations did it pass?

DTI takes the model of a domain-trained AI deployed as shared infrastructure across functions and scales it to ecosystems and the broader economy.

The potential of universal AI is evident in organizations adopting an intelligence-as-a-fabric model. Sanofi, the French multinational pharmaceutical and health care company, offers a useful case in point. Its enterprise AI platform, plai, delivers an AI-driven, 360-degree view across operations for roughly 100,000 employees and adapts to diverse contexts. As Miguelina Matthews, Sanofi's head of external liaison, noted in a conversation with *Biopress Online*, the system delivers "real-time, user-friendly data visualizations" that "reinforce decision-making 24/7."[36] With this quality audit function, Sanofi can prioritize high-risk areas that pose the greatest threat to product integrity and patient safety. Plai dynamically adjusts delivery schedules, assists in anticipating deviations, managing complaints, and drafting product-quality reviews, and helps investigators identify potential root causes of quality issues that might otherwise have gone unnoticed.[37]

DTI extends the model of domain-trained AI from serving as shared infrastructure across organizational functions and scales it to coordinate and deliver insight across entire industries and economies.

Part 2: Sectoral applications of DTI

The vision of a fully integrated DTI is still emergent, but its potential is already apparent. Early deployments in financial services, health care, supply chains, and telecommunications show how digital identity, verifiable credentials, and trusted data-sharing frameworks deliver measurable business value. These early initiatives move DTI from theory to practice and provide operational benefits today as well as a blueprint for broader adoption.

Finance and payments

"Payments internationally through banks are still a hassle. You have to wait and continuously look for the money, and so on."

DR. FLORIAN HERZOG
Chair, Founder, and Chief Technology Officer
Deon Digital AG

Financial services have been among the earliest adopters of DTI, with good reason: compliance costs are soaring. According to LexisNexis, global spending on AML/KYC, sanctions screening, and reporting surpassed $206 billion in 2023.[38] These rising costs reflect an expanding web of regulations, labor-intensive manual reviews, and the escalating expense of advanced compliance technologies.

The stakes for failure are equally high. In 2024, TD Bank paid $3.09 billion in penalties for systemic shortcomings in its AML program. The year before, Binance reached a major settlement with US authorities over sanctions violations and AML lapses. In 2022, Danske Bank forfeited more than $2 billion to the US Department of Justice, the Securities and Exchange Commission, and Denmark's Special Crime Unit after misleading US banks about illicit fund flows through its Estonian branch.[39]

Compliance requirements lead to delays and expense, especially in multi-jurisdictional situations. As Dr. Herzog explained, "Payments internationally through banks are still a hassle. You have to wait and continuously look for the money, and so on."[40]

The UBO is the person who ultimately benefits when an institution initiates a transaction.

DTI offers quite a different approach. Rather than moving money first and reconciling later, DTI embeds compliance into the transaction flow itself so that makes it possible to confirm that parties have met all regulatory requirements before funds ever leave the treasury. For example, a company initiating a supplier payment can trigger an automated request for proofs of incorporation, tax status, and sanctions clearance through an open-standard protocol. The supplier's digital wallet returns a verifiable package of proofs, revealing only the necessary facts, that a trusted authority verified the supplier as the *ultimate business owner* (UBO) on a given date and that the UBO was not on a sanctions list.[41] Other trusted issuers registered in a recognized trust framework have signed other proofs in the supplier's package.

If the parties meet all conditions, then settlement occurs instantly. If there is a mismatch or missing proof, then funds go automatically into a programmable escrow account while parties resolve the issue. Each step in the process is time-stamped, cryptographically verifiable, and ready for audit. DTI not only reduces compliance costs but also accelerates settlement, improves liquidity management, and builds regulator confidence by cutting false positives and increasing transparency.

The pattern applies far beyond supplier payments. Trade finance, collections, refunds, and any process, where parties must satisfy rules before any value moves, can benefit from the same approach. Singapore's COSMIC platform exemplifies the model: it allows banks to exchange risk signals securely under regulatory oversight and dramatically improving AML effectiveness.[42] Similarly, Europe's rollout of the European Digital Identity (EUDI) Wallet demonstrates how verifiable credentials can simplify onboarding, payments, and e-signatures at scale.[43] Together, these initiatives illustrate how DTI transforms compliance from a costly, after-the-fact burden into a streamlined, automated, real-time capability that creates competitive advantage.

DTI transforms compliance from a costly, after-the-fact burden into an automated, real-time capability that creates competitive advantage.

Health care and pharmaceuticals

Health care is one of the sectors where the benefits of DTI are emerging fast. The UK National Health Service (NHS) has introduced a Digital Staff Passport that uses verifiable credentials to recognize professional qualifications and employment histories across hospitals and regions.[44] The passport has shortened onboarding for clinicians moving between organizations, boosted staff satisfaction, and enhanced patient safety by requiring staff to keep credentials up to date. At the same time, the NHS is laying the digital groundwork for trusted data-fabric-based audit trails to secure patient data integrity and simplify compliance with privacy regulations.[45] As

these examples show, digital trust mechanisms can solve pressing workforce and data challenges while building out the DTI for patient-controlled data sharing.

In healthcare, billing is a major area where DTI could transform outcomes.

The need for trusted health data systems has never been greater. In its *Cost of a Data Breach Report 2025*, IBM reported that health care continues to face the highest breach costs of any sector, averaging $7.42 million per incident.[46] According to the report, attackers value patient information because they can exploit it for identity theft, insurance fraud, and other financial crimes.[47] But risks to patient privacy are only one part of a broader challenge. Dr. Jaffray of MD Anderson identified billing as a major area where DTI could transform outcomes: "Billing is a huge one," he noted.[48] "In the United States, billing to the federal government inaccurately is fraud." He argued that privacy regulations such as HIPAA must evolve toward a consent-first data economy, one that gives patients, care teams, and labs control over what data is shared, for what purpose, and for how long.

Dr. Jaffray also underscored the importance of governing AI in health care: "Think of AI as a drug. Even if certified, deployment needs oversight inside the hospital."[49] IBM echoed this concern in its finding that attackers are increasingly targeting AI models and applications, taking advantage of underdeveloped security controls.[50]

DTI helps address these challenges in three critical ways. First, provenance-rich data can make billing more accurate and fraud easier to detect. Second, consent can become a portable, verifiable credential. Rather than burying patient consent in forms, patients could issue their consent digitally, scope it to a specific purpose, and revoke it at any time. Labs and providers could request only the minimum patient data needed, such as proof of coverage or an allergy indicator, without exposing anyone's full medical history. Finally, health care organizations could use verifiable audit trails to track when and how AI was deployed, to make sure users were applying algorithms safely, transparently, and in line with regulatory expectations.

DTI could also help secure the pharmaceutical supply chain by detecting counterfeit drugs, speeding up recalls, and reducing administrative burdens.

DTI could also play a pivotal role in securing the pharmaceutical supply chain. The World Health Organization estimated that one in 10 medicines in low- and middle-income countries was falsified or substandard, resulting in more than $30 billion in losses annually.[51] The Pacific Research Institute estimated that the global counterfeit drug trade was worth between $200 billion and $431 billion annually.[52] A DTI-enabled supply chain would make provenance visible at every stage: manufacturers could issue verifiable credentials for batch origin and site licenses; IoT sensors could record temperature and custody events with cryptographic signatures; distributors and pharmacies could verify these credentials at each transfer point; and regulators could reconstruct provenance from tamper-evident records without accessing sensitive patient or commercial data. The result would be fewer counterfeit drugs, faster recalls, and cleaner near-real-time audits that reduced administrative burden and improved public safety.

Together, these capabilities point toward a health care system where trust is built into the infrastructure. Patients gain meaningful control over their data. Providers reduce administrative friction and liability. Regulators shift from after-the-fact enforcement to continuous assurance. And the system becomes more resilient, more efficient, and more patient centered.

Education and training

"Many institutions are not using open standards for credentials. … The technology is there; it's a matter of diffusion and university policy."

DR. HORST TREIBLMAIER
Professor and Head
School of International Management
Modul University Vienna

Education and workforce development face a common problem: credentials move far more slowly than skills do. When verifying a degree, license, or employment history takes weeks or months, especially across borders, it slows hiring, creates skill mismatches, and hurts productivity. A 2025 study of countries in the Organization for Economic Cooperation and Development found that reducing credential delays and skill mismatches could raise national productivity by three to four percent on average.[53]

This is not just an employer problem. Educational institutions themselves often suffer from inefficiencies tied to outdated technology. Dr. Horst Treiblmaier, full professor and head of the School of International Management at Modul University Vienna, told us, "Many institutions are not using open standards for credentials … we verify every semester; the technology would solve it."[54] He added, "The technology is there; it's a matter of diffusion and university policy."[55]

With DTI, universities, professional bodies, and employers could address these problems by issuing verifiable, portable credentials directly to a worker's lifelong digital identity wallet. A nurse applying for work in a new jurisdiction, for example, could instantly present a digitally authenticated degree, an active professional license, and a verified work history, all bundled within a single, tamper-proof credential package. A human resources (HR) system could validate these credentials automatically against trusted registries, grant provisional authorization in minutes, and continue background checks in parallel, all shortening the time to hire dramatically while preserving compliance.

Early pilots of the EU Digital Product Passport have shown strong results: audits are faster, counterfeiting is reduced, and asset recovery is more efficient at the end of a product's life.

Integration of DTI also advances models of training and hiring. With microcredentials, workers can prove specific competencies quickly, helping employers match talent to emerging needs. Because credentials are revocable and time-bound, outdated or irrelevant claims naturally expire, preserving privacy in the process. The result is a labor market that operates at digital speed and is compliant, verifiable, and rights-preserving by design.

Supply chain and logistics

Supply chains are increasingly turning to trust frameworks to verify products and the information attached to them. The EU Digital Product Passport, for instance, requires manufacturers to link verifiable data on origin, sustainability, and compliance directly

DTI makes supply chain provenance programmable. Producers can link each product or batch to a digital twin with an open identifier; and supply chain members can record key events such as inspection and shipping as signed attestations.

to goods, starting with sectors such as textiles and electronics. Early pilots have already shown strong results: audits are faster, counterfeiting has declined, and asset recovery at the end of a product's life has become more efficient. For example, Tesla has traced 100 percent of the cobalt in its electric vehicle batteries to the Kamoto Copper Company in the Democratic Republic of Congo, while Audi has traced over 10 percent of its battery materials to Hungarian suppliers and more than 13 percent to Chinese suppliers.[56] The stakes are high: according to an OECD–EU Intellectual Property Office report, the global market for counterfeit goods in 2019 was valued at $464 billion, with the European Union importing €119 billion worth of fake products.[57]

The challenges that DTI can address go beyond counterfeiting. Products today may involve conflict minerals, forced labor, or carbon-intensive production. According to a 2022 Greenhouse Gas Protocol report, Scope 3 emissions (i.e., the indirect carbon emissions generated across a company's supply chain and product life cycle) can represent more than 90 percent of a company's total carbon footprint, yet these emissions are among the hardest to measure and manage.[58]

Regulators are responding: the European Union now requires companies to verify that commodities are free from child labor and that products sold within the region do not contribute to deforestation or environmental degradation. "We have about 3,000 suppliers. How can you ensure that none of them uses child labor?" an automotive executive asked Dr. Treiblmaier who was researching supply chains.[59] That is the real-world challenge.

DTI makes such supply chain provenance programmable. Each product or batch can be linked to a digital twin with open identifiers, while key events such as manufacturing, inspection and shipping, are recorded as signed attestations. Buyers can automate payments based on verified milestones, releasing funds partially upon lab certification and in full upon delivery confirmation. Customs authorities, banks, and auditors can access the same cryptographically secured proofs without exposing sensitive trade secrets, and parties can resolve disputes automatically with evidence attached.

This approach accelerates cash flow, reduces delays, and opens new opportunities for finance and insurance based on verifiable, event-level risk. By connecting physical goods to verifiable digital credentials for emissions, repair, recycling, and more, businesses gain a foundation for circular-economy incentives and digitized environmental, social, and governance compliance. Governments benefit as well, with a scalable, auditable system that supports sustainability goals and strengthens customs enforcement. In short, DTI transforms supply chains into transparent, accountable, and digitally empowered networks that deliver both operational efficiency and trust.

Government and public services

Governments have become one of the leading adopters of elements of DTI. Many countries have introduced digital IDs, built trusted data repositories, and mandated standards that align with DTI principles. Yet adoption remains uneven, both across regions and within agencies, leaving significant room for progress. As Chief Data Officer Stephen Burt of the Government of Canada observed, "If the government starts to prioritize [the right pieces] with a bit of political impetus, we could move quite a bit faster."[60]

"If the government starts to prioritize [the right pieces] with a bit of political impetus, we could move quite a bit faster."

STEPHEN BURT
Chief Data Officer
Government of Canada

One of the most promising public-sector applications of DTI is the verification and management of eligibility for government programs. Zurich-based Dr. Florian Herzog of Deon Digital noted that, with Switzerland's newly approved digital ID, citizens could prove who they are, and providers could query the system, "Is this person eligible to do this?"[61]

When eligibility is conveyed inefficiently or incompletely, traditional programs suffer two kinds of errors: inclusion errors (i.e., where funds go to the wrong recipients) and exclusion errors (i.e., where eligible individuals are prevented from receiving benefits). Inclusion errors attract headlines and can result in substantial waste. For example, the *PBS News Hour* reported that more than $280 billion in COVID-19 relief funds went to fraudsters.[62] Though less visible, exclusion errors such as bureaucratic hurdles, identification requirements, or long waiting lists can leave large numbers of people without access to essential support.

DTI offers a solution by making eligibility verifiable and portable. Government agencies can issue credentials such as proof of residency, income level, or disability status that individuals present selectively via their digital wallet when needed. For example, after a natural disaster, a citizen can prove residence in an affected area or income below a certain threshold. Merchants can verify their authorization to accept aid disbursements. The government can deliver funds via programmable payments, restricted by merchant type and expiration date, and can monitor such delivery in real time through dashboards that rely on verifiable data rather than bulk personal information. If some entity challenges a decision, then government officials can review the relevant policy and evidence and provide redress while preserving the integrity of the system.

DTI offers a solution to inclusion errors (i.e., where funds go to the wrong recipients) and exclusion errors (i.e., where eligible individuals are prevented from receiving benefits) by making eligibility verifiable and portable.

The result is faster, fairer service delivery with fewer leaks and a fundamental shift from audit-by-paperwork to audit-by-proof. By embedding trust and verification into the infrastructure itself, governments can boost operational efficiency, safeguard public resources, and strengthen citizen confidence.

Emerging DTI implementations

Beyond government service delivery, several large-scale pilot projects are demonstrating the potential of DTI and yielding practical lessons for broader deployment. In Latin America, LNet, led by

the Inter-American Development Bank Group's IDB Lab, supports experiments in digital identity, cross-border verifiable credentials, and tokenized money.[63] In Europe, the European Blockchain Services Infrastructure aims to facilitate the portability of credentials across borders, so that individuals and businesses can interact seamlessly across countries.[64] China has invested heavily in state-led platforms such as the Blockchain-based Service Network, which facilitates business licensing and supply chain tracing, as well as municipal hubs like the Shanghai Blockchain Hub, which supports trade, taxation, and customs operations.[65] Conceptual initiatives such as China's Belt and Road blockchain infrastructure explore multi-country platforms for logistics, trade finance, and document provenance.[66] Meanwhile, smart-city pilots in Singapore, Dubai, and Shenzhen are experimenting with DTI for business licensing, trade documentation, and service payments.

Governance frameworks are as important as the technology itself because they provide the rules, oversight, and accountability needed for trust.

Although China's investments reflect a high degree of formalization, outcomes and lessons remain somewhat opaque. Across other pilots, common patterns are emerging that can inform future DTI implementations. A seamless user experience and ability to move credentials and status with individuals are essential for adoption. Creators must build in interoperability from the start to prevent silos and support smooth cross-platform functionality. Governance frameworks are just as important as the technology itself because they provide the rules, oversight, and accountability needed for trust. Hybrid public-private models are becoming the norm and balance the strengths of government authority with private-sector innovation. Open standards reduce vendor lock-in and accelerate adoption. Institutional capacity, sustained funding, and training are equally critical to scaling these initiatives effectively.

Taken together, these pilots demonstrate that DTI is moving from concept to practice. They provide both inspiration and practical lessons that can guide enterprises, governments, and consortia as they build the next generation of DTI.

Part 3: DTI design and deployment

Governance, legitimacy, and trust

DTI requires coordinated governance that spans technologies and jurisdictions. Without clear governance, trust will be fragmented and adoption will stall.

Effective DTI design depends on more than just technology. It also requires governance structures to warrant legitimacy and build trust. Governance is what transforms a collection of technologies into reliable infrastructure. Roads, telecommunications networks, and payment systems became trusted public utilities not only because of engineering quality or technical standardization, but because governance established shared rules, oversight mechanisms, and accountability structures. This instills confidence and accelerates adoption.

For DTI to have legitimacy and widespread adoption, its governance must be rooted in standards and regulation. The challenge is that DTI requires coordinated governance that spans technologies (e.g., identity, credentials, data fabrics, payments, and AI) as well as jurisdictions. Without clear governance, trust will remain fragmented, and adoption will stall.

Legitimacy comes from transparency, inclusiveness, and responsiveness. Governance dashboards can display uptime, incident logs, policy changes, and participation.

At the heart of effective governance are rules, roles, and stakeholders. Rules may be encoded in policies or smart contracts, but they must remain interpretable within legal, cultural, and regulatory contexts. Roles define who issues credentials, who holds them, who verifies them, and who manages registries and oversight. Stakeholders include governments that confer legitimacy, businesses that drive innovation, and civil society groups that safeguard rights and inclusion. DTI governance must balance these elements so that the system can function globally across sectors while preserving trust and legitimacy.

One central challenge is reconciling overlapping and sometimes conflicting claims to rights and sovereignty. Governments seek control over identity and registries, individuals want privacy and agency over their personal data, and businesses need predictability around liability, intellectual property, and enforcement. Commercial platforms often prioritize efficiency or data collection over other interests, but DTI supports balance. Regulators can verify cryptographic proofs rather than collect bulk data. Individuals can selectively disclose information, and trust registries can link verifiable events to legal entities for accountability. Those responsible for oversight can view audit trails anchored in tamper-evident data fabrics without exposing sensitive information. In this way, accountability is built into, not bolted onto, the system.

Legitimacy comes from governance processes that are transparent, inclusive, and responsive. Governance dashboards can provide visibility into uptime, incident logs, policy changes, and participation. Redress mechanisms such as automated error correction, arbitration panels, and clear escalation paths give users confidence that the system works fairly. Portability and exit options allow credentials and data to move between providers without vendor lock-in. Inclusive design means multilingual interfaces, accessibility features, and meaningful participation for affected communities.

DTI can also build on existing governance tools in sectoral domains and standards bodies, including trust registries, assurance frameworks, conformance tests, and dispute resolution processes. Today, these mechanisms are fragmented. To serve as a foundation for a new global economy, they must be integrated across sectors and jurisdictions. This includes cross-border recognition of credentials, schema harmonization, continuous oversight, AI provenance and model governance, secure recovery, and safeguards against monopolistic control. Integrated governance creates a cohesive, trusted global infrastructure; fragmented systems risk slowing adoption.

Interoperability is critical. As Ismael Arribas, president of the Data Economy Association and standards specialist at LNet (formerly LACChain), observed, "We need standards de jure."[67] For DTI to operate as a legitimate and resilient public utility, it must move beyond informal technical conventions toward legally supported standards. This does not freeze innovation but provides a framework through which regulators and standards organizations can guide adoption nationally and internationally. Smaller jurisdictions and globally connected industries feel this need most acutely. Dr. Clara Guerra of Liechtenstein's Office for Digital Innovation emphasized how legitimacy in digital systems ultimately depended on cooperation and mutual recognition across borders. "International integration is mandatory for us," she said.[68] Such integration provides the legal and regulatory foundation that makes verifiable data and programmable workflows binding, auditable, and recognized across borders.

"International integration is mandatory for us."

DR. CLARA GUERRA
Director
Office for Digital Innovation
Government of Liechtenstein

A practical example of governance in action is a CBDC consortium like Project Acacia in Australia.[69] Unlike traditional systems where central banks, commercial banks, and payment providers operate separately, a consortium model creates shared governance. Central banks retain authority over issuance and monetary policy. Commercial banks and fintechs distribute wallets, manage onboarding with verifiable credentials, and enforce policy rules such as transaction limits or sanctions compliance. Supervisors receive real-time compliance signals through cryptographically signed attestations rather than delayed batch reports. Users benefit from redress mechanisms that resolve disputes, such as frozen accounts, without undermining systemic trust. This model transforms a payment system into a trusted public utility that balances efficiency, sovereignty, and accountability.

Lessons learned from digital public infrastructure

DTI is not being built from scratch. Across the globe, governments and regions have already deployed large-scale DPI that demonstrates both what works and what to avoid. These programs show that trusted digital identity, secure data exchange, and modern payment systems can operate reliably at a national scale. DTI builds on these lessons, extending them into a model that is ready for enterprise use and cross-border application. Here are a few examples:

Across the globe, governments and regions have already deployed large-scale DPI that demonstrates what works and what to avoid.

- **India Stack** offers a comprehensive suite of national *application programming interfaces* (APIs) for identity verification, digital payments, and secure document exchange.[70] It shows that open APIs, modular architecture, and consent-based data sharing can scale to serve more than a billion users, offering a model of digital infrastructure that is both efficient and inclusive.
- **MOSIP** is a *modular open-source identity platform* adopted across Africa and Asia.[71] Its design demonstrates how modular, sovereign architectures can reduce vendor lock-in and encourage innovation. At the same time, the platform highlights that achieving broad inclusion requires options for offline use and low-bandwidth environments.

- **X-Road** is a secure data-exchange layer that links government and private sector services. Its design emphasizes keeping data at its source, sharing proofs instead of raw records, and complementing technical trust with a strong legal framework.[72] This combination strengthens security, auditability, and reliability for users.

- **EUDI wallet** provides an interoperable framework for citizens and businesses across the European Union. It illustrates that legal mandates drive adoption, while design factors, such as user experience, certification, and inclusivity, are essential for building trust and engagement.[73]

With pilots, teams can track repeatability and reliability of performance across issuers, holders, verifiers, and registries.

Together, these examples provide practical guidance for building DTI. Open standards, modular building blocks, data minimization, policy-aware wallets, and cross-border interoperability are achievable today. Applied at scale, these principles can make DTI a secure and trusted foundation for both public and private sectors worldwide.

From pilots to scale

Shaped by lessons from existing DPI implementations, DTI rollouts will likely follow a familiar growth path. This progression typically unfolds across three stages, from local pilots to cross-border ecosystems.

Stage 1: Local or sector pilots

Early initiatives start with targeted pilots in high-value sectors, such as small business lending. These projects test performance across issuers, holders, and verifiers, using conformance checks and playbooks to ensure repeatability and trust.

Stage 2: National and regional rollouts

Successful pilots scale into national and regional deployments supported by published credential profiles, standardized assurance levels, and onboarding toolkits. API-first design, policy alignment, and enforceable standards such as those in India Stack, MOSIP, and EU digital ID pilots, can prevent fragmentation and lower integration costs.

Stage 3: Cross-border ecosystems

As governance and standards mature, cross-border corridors enable interoperability among jurisdictions and sectors. Examples include EUDI wallets linking with global banks or customs authorities recognizing shared product passports, although institutional trust and liability remain the hardest problems to solve.

Successful DTI rollouts share three key traits. First, clear ownership of rule books, trust registries, and change management processes

buoys stability and accountability across the system. Second, conservative data practices protect sensitive personal information by keeping it off-chain and promptly updating revocations, which reduce risk and build trust. Third, agile iteration allows teams to continuously improve by tracking metrics such as onboarding time, false positives, settlement speed, and audit effort, providing transparency and measurable progress for all stakeholders.

"You're not going to succeed with this kind of infrastructure without public-private partnerships."

IAN PUTTER
Chief Evangelist
Aurachain AG

Public-private partnership models

Industry experts consistently underscored that strong *public-private partnerships* (PPPs) were essential for building successful DTI. Joseph Bradley, CEO of TONOMUS, described PPPs as "the first pillar," noting that government should act as a protector rather than an operator.[74] Ian Putter of Aurachain put it simply: "You're not going to succeed with this kind of infrastructure without public-private partnerships."[75] In DTI, each stakeholder brings distinct value:

- *Governments* provide legitimacy, legal guardrails, funding, authoritative identity attributes, and often serve as major users of the infrastructure.
- *Industry* contributes technology, distribution capabilities, innovation, and additional funding.
- *Civil society* helps prioritize fairness, usability, and public trust. As Dr. Suelette Dreyfus of the University of Melbourne observed, efforts must "bring civil society along, resource them, and make them stakeholders from the start."[76]

Successful PPPs share several key traits. First, with co-governance, multistakeholder boards can operate with clear rule books, defined membership criteria, incident response protocols, and transparent budgeting. Second, funding models are blended; they combine public budgets, development banks, philanthropy, and private investment. As initiatives scale, modest user fees can sustain operations, while open-source approaches with certification support local vendors and reduce dependance on single vendors. Finally, procurement policies prioritize open standards, data portability, and conformance certification, while reference implementations and test tools help smaller firms to participate fully and fairly.

Builders must design security into DTI from the start and take a zero-trust approach.

Key success factors

Security by design

Trust is the core attribute of DTI. For broad adoption, design security must be built into DTI from the start and take a zero-trust approach with mutual authentication, least-privilege access, and hardware-backed keys wherever possible. Separating governance and policy functions from operational data exchange reduces risk exposure and maintains service performance.

Tamper-evidence and auditability must also be built into the foundation. Logs, policies, and trust lists should be anchored to verifiable ledgers, while wallets, registries, and agents are distributed only as signed, traceable builds so that any compromise can be detected, investigated, and remediated quickly.

Finally, the infrastructure must also have a clear playbook when issues occur. If credentials are compromised, then status lists must be updated in real time and checked before transactions continue. If an AI agent is compromised, then its keys must be rotated, its access revoked, and all events logged for review. In case of a policy breach, software versions must be frozen or rolled back, advisories issued, and remediation verified by operators.

True resilience requires preparation for geopolitical and operational shocks. Enterprises will adopt DTI more easily if it aligns with their existing security models.

True resilience requires preparation for geopolitical and operational shocks. That means sovereign and multi-cloud deployments, offline verification with cached credentials, and clear resynchronization procedures so that systems can continue operating even under degraded conditions. Enterprises will adopt DTI more readily when it aligns with their existing security models. Secure gateways, policy enforcement, rate limiting, and revocation caching improve resilience and fit seamlessly into enterprise practices.

The cryptographic landscape is evolving rapidly, with quantum computing a significant challenge. As Ismael Arribas of the Data Economy Association observed, "We need to harden the cryptography now. We need post-quantum robustness. It is extremely important to scale up."[77] A practical road map starts with cataloging existing algorithms, moves to hybrid signatures, then adds support for rotating and re-issuing high-value credentials. The road map should require certified endpoints to meet post-quantum standards within three years.

The bottom line: security is the foundation of trust. DTI must be continuously hardened, fully auditable, and prepared for any threats.

Making AI trustworthy

AI adoption is outpacing governance. Executives are launching pilots to capture productivity gains, while organizational controls, security patterns, and legal frameworks lag.

The universal intelligence layer of DTI will interpret signals from across the stack and turn them into action. When combined with trusted identity, verifiable credentials, policy engines, and authoritative data registries, AI can reason over provenance-rich information, automate compliance checks, and personalize experiences without compromising confidentiality or control. This means copilots that verify a supplier's certification before drafting a contract, contact-center agents that disclose only the attributes needed to resolve a case, and analytics that can trace conclusions back to signed evidence. The stronger the authenticity, authorization, and auditability of the underlying data, the more confidently AI can deliver value. But that confidence depends on governance evolving just as quickly.

Alarmingly, but perhaps predictably, adoption is outpacing governance. Business leaders are launching pilots to capture

productivity gains faster than organizational controls, security patterns, and legal frameworks can adapt. This lag creates both opportunity and risk: rapid wins on one side, and opaque vendor practices on the other. Slowing innovation is not the answer. The priority is to pair deployment with standards and guardrails that clarify who may run which models, on what data, under what policies, and with what accountability.

DTI must treat AI as a first-class participant in the trust stack. AI agents should operate with verifiable identities, credentials, and proofs, just like people, organizations, and devices.

A practical cornerstone is provenance: knowing what data went into a model and how it has evolved over time. As Dr. Guerra said, "AI only becomes trustworthy if it consumes trustworthy data."[78] By recording cryptographic fingerprints and usage rights of training sets in a tamper-evident log, enterprises can prove what sources were used, whether sensitive records were masked, and when fine-tuning occurred. *Fine-tuning* refers to the process of adapting a pre-trained AI model to perform a new, specific task by training it on a smaller, specialized dataset. This approach allows auditors to track lineage, detect drift, and connect hallucination patterns to specific data or vendors. It also supports responsible commercialization: suppliers can prove that licenses are honored, while buyers can verify that models comply with sector-specific regulations; for example, by confirming that protected attributes are excluded in lending or that synthetic data is used when required. Provenance transforms AI governance from a stance of "trust us" to one of "verify once, use widely."

DTI must also treat AI as a first-class participant in the trust stack. Agents and services should operate with verifiable identities, credentials, and proofs, just like people, organizations, and devices. Dr. Herzog raised an important question: "With agents, who's responsible when something goes wrong?"[79] The answer is clear accountability. An AI agent initiating a payment, accessing patient data, or filing a regulatory report should present proof of who controls it, what it is authorized to do, and whether it has followed the required policy steps. With these proofs, systems can enforce least privilege across APIs, maintain auditable trails for regulators, and interoperate safely with other systems across firms and borders. AI agents can also discipline the market: customers and partners favor models and agents with stronger assurances, reducing risk and integration cost.

The bigger challenge is organizational, not technical. Success depends on aligning stakeholders, training teams, and rolling out in phases.

The path forward is clear: govern AI where it operates, within the DTI. Pair adoption with enforceable policies, insist on provenance logs for training data, and require that AI agents carry verifiable identities and permissions. If executed well, AI will evolve from a productivity tool to a trusted, accountable participant in the digital economy.

Change management and systems integration

For DTI to scale, it must work seamlessly with the systems enterprises already rely on. This means connecting DTI to existing business software, such as financial systems, customer databases, HR platforms, and other data tools, so that credentials and trust

signals can flow automatically without disrupting daily operations. Open interfaces, real-time updates, and built-in policy checks ensure that employees and partners can continue using familiar roles and workflows while benefiting from verifiable, trustworthy data.

The bigger challenge is organizational, not technical. Success depends on aligning stakeholders, training teams, and rolling out in phases. Early corridors, such as bank-supplier networks, hospital-insurer clusters, or export lanes, are the best proving grounds. Clear migration paths, backward compatibility, and visible early wins build confidence and momentum.

Sovereignty is essential. Governments must retain control of identity policies, data protection, critical registries, and incident response.

Governance and change management are equally important. Programs that publish standards early, invest in training, and maintain transparency on performance tend to scale faster and earn greater trust. Funding should be linked to measurable outcomes, and safeguards must prevent any single vendor or government entity from creating lock-in.

Ultimately, DTI becomes real when technology is embedded in institutions and deployed through repeatable, standards-based practices. Organizations that treat integration and change management as strategic priorities will lead the way, moving first from pilots to national rollouts, and then to trusted cross-border ecosystems.

Digital sovereignty and cross-jurisdictional interoperability

In an increasingly interconnected digital economy, sovereignty is essential. Governments must retain control of identity policies, data protection, critical registries, and incident response. At the same time, global commerce, migration, finance, health, and climate action all require digital services that work seamlessly across borders. The policy challenge is to distinguish what must remain local, such as laws, oversight, and redress, from what should be standardized, such as data formats, discovery protocols, and verification methods.

A practical path forward is layered cooperation. Countries can maintain their own assurance levels and accreditation processes while agreeing to recognize one another's trust lists and minimum controls, much like the mutual acceptance of passports or driver's licenses. Organizations and individuals can present verifiable credentials using global standards such as the World Wide Web Consortium's DIDs, verifiable credentials, and verifiable presentations allowing their cryptographic proofs to be validated anywhere without moving any underlying personal data.

Organizations can express policy frameworks as machine-readable code, so that verifiers apply the exact rule set in place at the moment of decision.

Instead of moving large volumes of sensitive data across borders and compromising the privacy of residents, transaction decisions can rely on cryptographic evidence (e.g., digital signatures, time stamps, and revocation checks) for trustworthy verification and to satisfy data localization rules. Organizations can express policy frameworks

as machine-readable code, so that verifiers apply the exact rule set in place at the moment of decision; and outcomes are transparent, auditable, and consistent across jurisdictions.

To make digital proofs legally enforceable, governments and trust frameworks need formal standards that have been adopted into law or regulation. These standards define the rules for verifiable credentials, wallets, and verification systems, similar to how the EU eIDAS framework sets legally binding standards for electronic identities. A conformance registry managed by a neutral authority such as a government agency, standards body, or accredited third-party auditor, can list the wallets, verifiers, and registries that meet these standards. Such a registry provides transparency so that stakeholders can independently verify compliance; only certified systems carry formal legal recognition. Measurable accountability checkpoints, such as mandatory periodic audits, certification renewal cycles, and real-time reporting of revocations or compliance breaches, help maintain trust so that digital infrastructure remains dependable and legally enforceable across jurisdictions. This approach balances flexibility for innovation with legal certainty, giving organizations confidence that others will recognize and trust their DTI internationally.

By rethinking and automating the antenna permit application process on a blockchain, Italy streamlined it from three weeks to a couple of hours.

Rethink and automate

As a word of caution, Dr. Treiblmaier recounted Italy's blockchain-based system for streamlining antenna permit applications. A government official had told him, "It's not enough to take an existing solution and put it on a blockchain. That did not work; you need to rethink and automate the process." By doing so, the official added, "They reduced the time for applying from three weeks to a couple of hours."[80]

Identity is best delivered through a hybrid model that combines high-assurance issuers, verifiable credentials, selective disclosure, and policy engines.

DTI is an enabler and a catalyst. With DTI, enterprises can streamline operations internally and across value chains, automate routine work, and lift productivity. Instead of collecting files, emailing screenshots, and rechecking data at every step, systems can request small proofs of facts and act when those checks pass. A new supplier, for example, can present a verified business credential and tax status, which triggers automatic onboarding and account setup. No manual review. In finance, invoices flow straight through, from purchase order, price match, and delivery record to automatic payment. Only exceptions need human attention. In customer operations, verified identity and eligibility can unlock services instantly and generate audit logs. The result is fewer handoffs, fewer errors, faster cycle times, and lower operating costs. Such results show that DTI enhances not only security but also operational efficiency.

Conclusion

Clear rules, defined roles, trust registries, and accountability turn technology into reliable infrastructure across jurisdictions and sectors.

Four major themes emerged from the research. First, DTI will shift enterprise operations from a "collect and store" model to a "request and verify" model, moving trust from application add-ons to shared infrastructure. Powering this transformation is a layered, hybrid architecture that combines a trusted data fabric for tamper-evident integrity, portable digital identity and credentials, authoritative and trust registries, programmable value, and AI that acts only on verified data. Together, these components form a neutral, standards-based stack that balances institutional assurance with individual privacy and cross-border interoperability. Evidence from finance, health care, supply chains, education, and public services shows that these patterns are already delivering value and creating repeatable playbooks across sectors.

Second, identity is best delivered through a hybrid model that combines high-assurance issuers, verifiable credentials, selective disclosure, and policy engines. This approach preserves portability and privacy and maintains clear lines of accountability.

Third, AI belongs *inside* the trust stack. Provenance of training data, model registries, and governed access make AI auditable and fit for high-stakes workflows in regulated domains.

Finally, governance is the flywheel. Clear rules, defined roles, trust registries, and transparent accountability turn technology into reliable infrastructure that can operate across jurisdictions and sectors.

Getting identity right reduces integration cost and vendor dependency and improves customer and workforce experience through selective disclosure and portable credentials.

Several industries are at the forefront of scaling DTI. Driven by regulatory pressure, fraud reduction, and tokenized payment pilots, the financial service sector is likely to lead. Telecom, travel, and education are also emerging as early adopters, with faster onboarding and microcredential verification delivering measurable gains. Health care adoption will likely accelerate as consent-based data management and AI governance reduce risk and speed decisions at the point of care. Manufacturing, shipping, and logistics will likely experience larger changes in the medium term through product passports, provenance tracking, and AI-enabled optimization. Together, these early adopters show how DTI can translate trust into measurable efficiency and growth across sectors.

Enterprise and ecosystem benefits

The business outcomes are clear: lower fraud and compliance costs, faster onboarding across organizations, seamless interoperability across partners and borders, lower friction in value transfer, better decision-making, and greater value creation from provenance-rich data.

Executives can expect near-term gains as verification becomes real-time and policy-aware rather than after the fact. Processes that once required manual checks will deliver audit-ready evidence by default, reducing overhead and risk. Cross-border coordination will improve as decisions rely on cryptographic proofs rather than bulk data transfers, as enterprises engage in compliant, privacy-preserving collaboration with partners and regulators.

Embedding programmability at the value layer unlocks precise disbursements, automated escrow, and event-driven settlement, to improve liquidity, reduce reconciliation, and drive new business models. Getting identity right cuts integration costs and vendor dependency and improves customer and workforce experience through selective disclosure and portable credentials.

Early steps for leaders

Across sectors, the playbook is consistent: adopt shared governance and standards; treat distributed ledgers and enterprise databases as complementary sources of truth; invest early in DIDs, verifiable credentials, and verifiable presentations; apply AI broadly; make proofs and revocations real-time; and prepare for emerging security threats, including post-quantum cryptography. To move from concept to results, focus on these critical steps:

Organizations can realize tangible benefits such as faster onboarding and settlement, lower fraud and compliance costs, audit-ready evidence on demand, workflows that interoperate across partners, and a resilient, vendor-neutral foundation for growth and new services.

1. **Target high-friction processes.** Identify one or two workflows where verification or onboarding is slow, costly, or error-prone, such as KYC or know your business, supplier onboarding, supplier qualification, or employee credentialing. Define clear metrics to measure success, including time to approval, verification pass rates, fraud losses, and audit effort. Use these key performance indicators (KPIs) to guide pilots and scaling decisions.

2. **Establish the minimal trust stack.** Adopt an interoperability profile using verifiable credentials and decentralized identifiers with real-time status events. Deploy a verifier API that connects to digital wallets and a trust registry, and anchor proofs to a neutral source of truth without storing personal data.

3. **Publish a pilot rule book.** Define roles, accepted credentials, revocation service levels, evidence retention, and liability. Express these rules in legal terms and in machine-readable policy so automated systems, auditors, and human stakeholders can enforce them consistently.

4. **Make AI accountable now.** Require provenance logs for training data, register model permissions, and enforce least-privilege agent behavior.

Leaders who begin planning and piloting today will influence the standards their ecosystems adopt tomorrow and capture the compounding benefits of trusted data, trusted identity, and trusted value at scale.

5. **Procure for interoperability.** Mandate open standards, conformance testing, crypto-agility, and post-quantum readiness to avoid vendor lock-in and costly rewrites.

6. **Go live with the target processes.** Replace PDFs, emails, and other manual proofs with digital verifiable credentials. Use selective disclosure or ZKPs where privacy or regulatory requirements apply. Maintain append-only decision logs and real-time revocation events. If AI agents are involved, maintain a registry to track models, permissions, and audit history.

7. **Test and expand.** Run cross-partner pilots using shared KPIs. Require conformance to standards in procurement. Establish a governance cadence with quarterly updates, crypto-agility, post-quantum readiness planning, and independent audits for controlled, measurable, and resilient scaling.

The practical takeaways for leaders are simple: start small, measure results, and scale carefully; focus on shared governance, clear standards, and security built in from day one; and avoid siloed, proprietary approaches that create lock-in or limit interoperability.

With a disciplined, stepwise approach, leaders can embed trust into operations, reduce risk, and open new opportunities for value creation across their networks.

Why act now

Organizations that act early to standardize identity, credentials, and presentations, operationalize governance, and treat AI as a verifiable participant in transactions, will turn compliance into a source of resilience and competitive advantage. The path forward is direct: select a corridor, measure outcomes, iterate, and scale through shared rulebooks and trust registries.

DTI is not a moonshot; it is a disciplined evolution toward programmable, auditable collaboration across industries and borders. Leaders who start planning and piloting today will not only define the standards their ecosystems adopt tomorrow but also capture the compounding benefits of trusted data, trusted identity, and trusted value at scale.

Acknowledgments

We are deeply grateful to the business and policy leaders who generously shared their time, candor, and expertise in interviews that informed this report. Executives, academics, regulators, technologists, and civil society representatives from finance, health care, supply chains, education, and public administration across multiple jurisdictions, offered practical insights that sharpened our framework, highlighted real-world constraints and potentials, and shaped the recommendations.

We especially thank the following individuals:

» Ismael Arribas, President, Data Economy Association of Spain; and Standards Specialist, LNet

» Joseph M. Bradley, Chief Executive Officer, TONOMUS, Saudi Arabia

» Stephen Burt, Chief Data Officer, Government of Canada

» Dr. Suelette Dreyfus, Researcher and Senior Lecturer, School of Computing and Information Systems, University of Melbourne, Australia

» Dr. Clara Guerra, Director, Office for Digital Innovation, Government of Liechtenstein, Liechtenstein

» Dr. Florian Herzog, Founder, Chair, and Chief Technology Officer, Deon Digital AG, Switzerland

» Dr. David A. Jaffray, Senior Vice President and Chief Technology and Digital Officer, University of Texas MD Anderson Cancer Center, United States

» Jonathan LLamas, Vice President, Decentralized Strategy, WISeKey, Switzerland

» Ilán Meléndez, Ecosystem Lead, LNet, Costa Rica

» Ian Putter, Chief Evangelist, Aurachain AG, Switzerland

» Dr. Horst Treiblmaier, Full Professor and Head, School of International Management, Modul University Vienna, Austria

We acknowledge the many other experts whom we interviewed in related research initiatives and podcasts, whose perspectives and insights contributed significantly to the thinking in this report.

About the author

Douglas Heintzman is chief catalyst at the BRI, where he collaborates with members around the world to guide them on their Web3 transformation journeys. Throughout his career, he has focused on disruptive technologies and their influence on business strategy, organizational design, and enterprise innovation. His leadership experience spans roles as an entrepreneur, founder, chief executive officer, chief operating officer, strategy executive, and management consultant.

Doug is also the CEO and co-founder of Syncura, a company specializing in cognitive AI process automation. Prior to this, he spent 25 years at IBM, primarily as a global strategy executive. He has served as a policy advisor and expert witness for the European Commission as well as the Canadian and US governments and provided guidance on technology policy, standards, and intellectual property.

Doug previously chaired the selection committee for the NSERC Synergy Awards for Innovation. He holds five patents. In addition, he serves on the boards of several companies and nonprofit organizations and advises numerous startups on innovation strategy and governance.

About the Cardano Foundation

The Cardano Foundation is an independent, Swiss-based, not-for-profit organization tasked with advancing Cardano as a public digital infrastructure across a wide range of industries. The Foundation works to anchor the Cardano blockchain as a utility for financial and social systems, thus empowering the digital architects of the future. It also develops infrastructure tooling, strengthens operational resilience, and drives diversity of on-infrastructure use cases as well as the development of sound and representative governance. For more information, visit https://cardanofoundation.org.

About the BRI

In 2017, Don and Alex Tapscott founded the Blockchain Research Institute (operating as the BRI) following the success of their bestselling book, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*.

BRI brings together a diverse community of business leaders, policymakers, researchers, and scholars to grasp and guide the transformative power of emerging technologies in shaping a prosperous digital future. Our mission is to empower organizations with the knowledge and insights they need to turn emerging technologies into strategic advantage.

From 2017 to 2023, our syndicated research programs explored the strategic impact of blockchain across industries and managerial functions. We facilitated global discussions and produced case studies, white papers, research briefs, roundtable reports, infographics, videos, webinars, and the podcast "What's on Tap?"

As demand for syndicated research shifted, BRI evolved its model to focus on custom research, tailored education, and expert advisory services such as workshops and ecosystem roundtables designed to help clients solve complex challenges and seize new opportunities.

Today, our work continues to inform business and government leaders worldwide, shaping digital strategies and policies at the highest levels. Guided by a platform-agnostic approach, BRI has upheld its steadfast commitment to objectivity, neutrality, and rigor, supplying businesses and governments with clear, actionable insights to navigate the next era of the digital economy. We invite you to join us as we work toward building a prosperous digital future for all: https://www.blockchainresearchinstitute.org/contact-us/

Research management

Don Tapscott – Co-Founder and Executive Chairman
Kirsten Sandberg – Editor-in-Chief
Alisa Acosta – Director of Research and Education

Others in the BRI leadership team

Joan Bigham – BRI Fellow
Andrew Facciolo – Director of Client Experience
Douglas Heintzman – Chief Catalyst
Roya Hussaini – Director of Administration
Jody Stevens – Director of Finance
Alex Tapscott – Co-Founder

Notes

1. "What Is Digital Transformation?" *Insights*, McKinsey & Co., 7 Aug. 2024, https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-transformation, accessed 18 Oct. 2025.
2. Dr. David Jaffray, interviewed via Zoom by Douglas Heintzman, 29 Aug. 2025.
3. India Stack, *IndiaStack.org*, https://indiastack.org/; MOSIP, "A Digital Public Good for Identity," https://www.mosip.io/, accessed 22 Oct. 2025.
4. Ian Putter, interviewed via Zoom by Douglas Heintzman, 23 Sept. 2025.
5. Matt High, "Supply Chain Insight: Inside IBM's Food Trust Blockchain System," *Supply Chain Digital*, BizClik Media Ltd., 17 May 2020, https://supplychaindigital.com/technology/supply-chain-insight-inside-ibms-food-trust-blockchain-system;, "About TradeTrust," *TradeTrust*, Infocomm Media Development Authority, Government of Singapore, last updated 22 July 2025, https://www.imda.gov.sg/how-we-can-help/digital-utilities/tradetrust, both accessed 18 Oct. 2025.
6. "Kinexys Liink: Permissioned Payments Information Network," J.P. Morgan, JPMorgan Chase & Co., n.d., https://www.jpmorgan.com/kinexys/liink, accessed 10 Oct. 2025.
7. "About Synaptic Health Alliance," Synaptic Health Alliance, n.d., https://www.synaptichealthalliance.com, accessed 10 Oct. 2025.
8. "KSI Blockchain Provides Truth Over Trust," *e-Estonia*, Estonian Business and Innovation Agency, 2 June 2022, https://e-estonia.com/ksi-blockchain-provides-truth-over-trust/, accessed 18 Oct. 2025.
9. Jonathan LLamas, interviewed via Zoom by Douglas Heintzman, 14 Aug. 2025.
10. Olivia White, et al., "Digital Identification: A Key to Inclusive Growth," *Insights*, McKinsey Global Institute, 17 April 2019, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth, accessed 18 Oct. 2025.
11. Alan Gelb and Anit Mukherjee, *Building on Digital ID for Inclusive Services: Lessons from India*, CGD Note, Center for Global Development, 13 Sept. 2019, https://www.cgdev.org/sites/default/files/building-digital-id-inclusive-services-lessons-india.pdf, accessed 18 Oct. 2025.
12. "What Are EU Digital Identity Wallets?" *The Wallet*, European Commission, n.d., https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/791609471/What+is+the+Wallet, accessed 10 Oct. 2025.
13. e-Estonia, "ID-card – Estonia's e-ID: The Cornerstone of a Seamless Digital Society," Estonia Business and Innovation Agency, https://e-estonia.com/solutions/estonian-e-identity/id-card/; and Singpass, "Your Improved Digital ID to Make Life Easy," Government of Singapore, https://www.singpass.gov.sg/main/, as of 18 Oct. 2025.
14. "Digital ID," *MyGov*, Australian Government, last updated 4 July 2025, https://my.gov.au:443/content/mygov/en/about/help/digital-id.html, accessed 18 Oct. 2025.
15. Jigme Tenzing, "Digital Drukyul: An ICT Masterplan for Bhutan," *DRUK Journal*, 2020, https://drukjournal.bt/digital-drukyul-an-ict-masterplan-for-bhutan/; Pallavi Sharma and Eric Drury, "Bhutan National Digital Identity and ToIP Digital Trust Ecosystems," Case Study, Trust Over IP Foundation, 21 May 2024, https://trustoverip.org/wp-content/uploads/Case-Study-Bhutan-NDI-National-Digital-Identity-ToIP-Digital-Trust-Ecosystems-V1.0-2024-05-21.ext_.pdf, accessed 18 Oct. 2025.
16. Lu-Hai Liang, "Bhutan Upgrades Digital Identity Wallet, Including Liveness and P2P Chat," *Biometric Update.com*, Biometrics Research Group Inc., 16 July 2025, https://www.biometricupdate.com/202507/bhutan-upgrades-digital-identity-wallet-including-liveness-and-p2p-chat, accessed 18 Oct. 2025.
17. Joseph M. Bradley and Don Tapscott, *You to the Power of Two: Redefining Human Potential in the Age of Identic AI*. (Dallas, TX: BenBella Books, 2025), https://www.amazon.com/You-Power-Two-Redefining-Potential/dp/1637747845.
18. Cardano Foundation, "Veridian: A NextGeneration Digital Identity Platform," *Cardano Foundation Blog*, Cardano Foundation, 3 April 2025, https://cardanofoundation.org/blog/veridian-digital-identity-platform, accessed 18 Oct. 2025.
19. Dr. Florian Herzog, interviewed via Zoom by Douglas Heintzman, 21 Aug. 2025.
20. World Wide Web Consortium, *Verifiable Credentials Data Model v2.0*, W3C Recommendation, 15 May 2025, https://www.w3.org/TR/vc-data-model-2.0/#what-is-a-verifiable-credential, accessed 18 Oct. 2025.

21. HID Global, "PIV Configuration and Management Use Case: ActivID CMS v6.0," Documentation, *HID Global*, https://docs.hidglobal.com/activid-cms-v6.3/operator/api-sdk/piv-toolkit/piv-config-and-mgmt-use-case.htm, accessed 18 Oct. 2025.
22. World Wide Web Consortium, "Verifiable Presentations," *Verifiable Credentials Data Model v2.0*, W3C Recommendation, 15 May 2025, https://www.w3.org/TR/vc-data-model-2.0/#verifiable-presentations, accessed 18 Oct. 2025.
23. Ilán Meléndez, interviewed via Zoom by Douglas Heintzman, 22 Aug. 2025.
24. Ilán Meléndez, interviewed via Zoom by Douglas Heintzman, 22 Aug. 2025.
25. European Commission, "eIDAS Regulation," *Shaping Europe's Digital Future*, Directorate-General for Communications Networks, Content, and Technology, 5 May 2025, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation, accessed 20 Oct. 2025.
26. Global Legal Entity Identifier Foundation (GLEIF), "Identifying Organizations – the Legal Entity Identifier (LEI)," GLEIF, https://www.gleif.org/en/organizational-identity/introducing-the-legal-entity-identifier-lei; and "This is GLEIF," a not-for-profit foundation incorporated by the Financial Stability Board under the laws of Switzerland, https://www.gleif.org/en/about/this-is-gleif, accessed 18 Oct. 2025.
27. "About LNET," LNET Global, https://lnet.global/about-lnet/; and "Documentation," LNET Global, https://lnet.global/documentation/, as of 18 Oct. 2025.
28. GDPRInfo, "General Data Protection Regulation (GDPR): Legal Text," *GDPR.eu*, European Union, https://gdpr-info.eu/; "What is GDPR, the EU's new data protection law?" *GDPR.eu*, European Union, https://gdpr.eu/what-is-gdpr/; and US Department of Health & Human Services, "HIPAA for Professionals," HHS.gov, https://www.hhs.gov/hipaa/for-professionals/index.html, as of 20 Oct. 2025.
29. Dr. David Jaffray, interviewed via Zoom by Douglas Heintzman, 29 Aug. 2025.
30. Global Legal Entity Identifier Foundation (GLEIF), "Identifying Organizations – the Legal Entity Identifier (LEI)," GLEIF, https://www.gleif.org/en/organizational-identity/introducing-the-legal-entity-identifier-lei, accessed 22 Oct. 2025.
31. "X-Road: The free and open-source data exchange solution," MTÜ Nordic Institute for Interoperability Solutions and Estonian Information System Authority, https://x-road.global/, as of 18 Sept. 2025.
32. Yogesh Hirdaramani, "Estonia's XRoad: Data Exchange in the World's Most Digital Society," *GovInsider*, 21 March 2024, https://govinsider.asia/intl-en/article/estonias-x-road-data-exchange-in-the-worlds-most-digital-society, accessed 20 Oct. 2025.
33. "Welcome to FHIR," HL7 FHIR v. 5, https://www.hl7.org/fhir/, accessed 18 Oct. 2025.
34. Philip Bruno, et al., "Global Payments in 2024: Simpler Interfaces, Complex Reality," *Insights*, McKinsey & Co., 18 Oct. 2024, https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-in-2024-simpler-interfaces-complex-reality, accessed 18 Oct. 2025.
35. Monetary Authority of Singapore, Purpose-Bound Money White Paper, https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/purpose-bound-money-whitepaper; and Shikhar Gupta, "OKX Singapore Launches Stablecoin Payments at GrabPay Merchants," *The Business Times*, SPH Media Limited, Co., 30 Sept. 2025, https://www.businesstimes.com.sg/wealth/crypto-alternative-assets/okx-singapore-launches-stablecoin-payments-grabpay-merchants, accessed 18 Oct. 2025.
36. "A Year in, Sanofi's Journey with Plai AI Is Aiding Quality Decisions: A Conversation with Miguelina Matthews," *BioProcess Online*, VertMarkets Inc., 30 Aug. 2024, https://www.bioprocessonline.com/doc/a-year-in-sanofi-s-journey-with-plai-ai-is-aiding-quality-decisions-0001, accessed 18 Oct. 2025.
37. "A Year in, Sanofi's Journey with Plai AI Is Aiding Quality Decisions: A Conversation with Miguelina Matthews," *BioProcess Online*, VertMarkets Inc., 30 Aug. 2024, https://www.bioprocessonline.com/doc/a-year-in-sanofi-s-journey-with-plai-ai-is-aiding-quality-decisions-0001, accessed 18 Oct. 2025.
38. Forrester Consulting, *True Cost of Financial Crime Compliance Global Study 2023*, LexisNexis Risk Solutions, 26 Sept. 2023, https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report, accessed 18 Oct. 2025.
39. Mažvydas Miliauskas, "AML Fines: Recent Most Famous Cases," AMLYZE, 17 May 2024, https://amlyze.com/aml-fines/, accessed 18 Oct. 2025.
40. Dr. Florian Herzog, interviewed via Zoom by Douglas Heintzman, 21 Aug. 2025.
41. SWIFT, "What is an Ultimate Beneficial Owner (UBO)? Know Your Customer (KYC)," SWIFT.com, https://www.swift.com/risk-and-compliance/know-your-customer-kyc/ultimate-beneficial-owner-ubo, accessed 22 Oct. 2025.

42. COSMIC stands for "collaborative sharing of money laundering/terrorism financing (ML/TF) information and cases." See "COSMIC," Anti-Money Laundering Regulations, Monetary Authority of Singapore, last updated 18 Oct. 2024, https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic, accessed 10 Oct. 2025.

43. "EU Digital Identity Wallet," European Commission, n.d., https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/overview, accessed 10 Oct. 2025

44. "Digital Staff Passport," National Health System, United Kingdom, n.d., https://digital.nhs.uk/services/digital-staff-passport, accessed 10 Oct. 2025.

45. NHS Digital, "Audits of Data Sharing Agreements," National Health System Digital, https://digital.nhs.uk/services/data-access-request-service-dars/data-sharing-audits; "Cross Organization Audit and Provenance," NHS Developer, https://developer.nhs.uk/apis/gpconnect-0-7-0/integration_cross_organisation_audit_and_provenance.html; and GP Connect specifications for developers, NHS Digital, https://digital.nhs.uk/services/gp-connect/develop-gp-connect-services/specifications-for-developers, all accessed 20 Oct. 2025.

46. IBM and Ponemon Institute LLC, *Cost of a Data Breach Report 2025: The AI Oversight Gap*, IBM Corp., 30 July 2025, mod. 5 Sept. 2025, https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91, accessed 18 Oct. 2025.

47. IBM and Ponemon Institute LLC, *Cost of a Data Breach Report 2025: The AI Oversight Gap*, IBM Corp., 30 July 2025, mod. 5 Sept. 2025, https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91, accessed 18 Oct. 2025.

48. Dr. David Jaffray, interviewed via Zoom by Douglas Heintzman, 29 Aug. 2025.

49. Dr. David Jaffray, interviewed via Zoom by Douglas Heintzman, 29 Aug. 2025.

50. IBM and Ponemon Institute LLC, *Cost of a Data Breach Report 2025: The AI Oversight Gap*, IBM Corp., 30 July 2025, mod. 5 Sept. 2025. , https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91, accessed 18 Oct. 2025.

51. "Substandard and Falsified Medical Products," World Health Organization, 3 Dec. 2024, https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products, accessed 18 Oct. 2025.

52. Henry I. Miller and Wayne Winegarden, *Fraud in Your Pill Bottle: The Unacceptable Cost of Counterfeit Medicines*, Issue Brief, Pacific Research Institute Center for Medical Economics and Innovation, Oct. 2020, https://www.pacificresearch.org/wp-content/uploads/2020/10/CounterfeitMed_F.pdf, accessed 18 Oct. 2025.

53. There are 38 member countries in the Organization for Economic Cooperation and Development (OECD). Pietro Garibaldi, Pedro Gomes, and Thepthida Sopraseuth, "Output Costs of Education and Skill Mismatch in OECD Countries," *Economics Letters*, 250 (April 2025), https://doi.org/10.1016/j.econlet.2025.112278; and OECD, "Members and Partners," https://www.oecd.org/en/about/members-partners.html, accessed 18 Oct. 2025.

54. Dr. Horst Treiblmaier, interviewed via Zoom by Douglas Heintzman, 24 Aug. 2025.

55. Dr. Horst Treiblmaier, interviewed via Zoom by Douglas Heintzman, 24 Aug. 2025.

56. Rithika Thomas, "Early Examples of EU Digital Product Passports in Action," *ABI Research*, Allied Business Intelligence Inc., 23 April 2024, https://www.abiresearch.com/blog/digital-product-passports-examples, accessed 18 Oct. 2025.

57. OECD and European Union Intellectual Property Office, *Global Trade in Fakes: A Worrying Threat*, 22 June 2021, https://doi.org/10.1787/74c81154-en, accessed 18 Oct. 2025.

58. *Scope 3 Frequently Asked Questions*, Greenhouse Gas Protocol, June 2022, https://ghgprotocol.org/sites/default/files/2022-12/Scope%203%20Detailed%20FAQ.pdf, accessed 18 Oct. 2025.

59. Dr. Horst Treiblmaier, interviewed via Zoom by Douglas Heintzman, 24 Aug. 2025.

60. Stephen Burt, interviewed via Zoom by Douglas Heintzman, 25 Aug. 2025.

61. Dr. Florian Herzog, interviewed via Zoom by Douglas Heintzman, 21 Aug. 2025.

62. Richard Lardner, Jennifer McDermott, and Aaron Kessler, "How Billions in COVID-19 Pandemic Relief Aid Was Stolen or Wasted," *PBS News Hour*, NewsHour Productions LLC, 14 June 2023, https://www.pbs.org/newshour/politics/how-billions-in-covid-19-pandemic-relief-aid-was-stolen-or-wasted, accessed 18 Oct. 2025.

63. LNet is a rebranding that combines LACChain and LACNet. "LACChain and LACNet Are Now LNet, a Global Platform for Trusted Digital Innovation," *IDB Lab News*, Inter-American Development Bank Group, 29 Sept. 2025, https://bidlab.org/en/news/lacchain-and-lacnet-are-now-lnet-global-platform-trusted-digital-innovation, accessed 18 Oct. 2025.

64. Directorate-General for Communications Networks, Content and Technology, "European blockchain services infrastructure," *Shaping Europe's Digital Future*, European Commission, 9 July 2025, https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure, accessed 27 Oct. 2025.

65. Anoosh Kumar, "China's Blockchain Playbook: Infrastructure, Influence, and the New Digital Order," *CSIS Blog*, Center for Strategic and International Studies, 5 May 2025, https://www.csis.org/blogs/strategic-technologies-blog/chinas-blockchain-playbook-infrastructure-influence-and-new; and Shanghai Municipal People's Government, "Shanghai Set to Expand Blockchain Applications," *English.Shanghai.gov.cn*, 9 April 2025, https://english.shanghai.gov.cn/en-Latest-WhatsNew/20250409/ed9cdef341ee475690fdcf5a73ce65f3.html, accessed 27 Oct. 2025.

66. Zoltan Vardai, "Chinese Gov't Launches Public Blockchain Infrastructure Platform with Conflux Network," *Cointelegraph*, 1 April 2024, https://cointelegraph.com/news/chinese-govt-public-blockchain-conflux, accessed 27 Oct. 2025.

67. Ismael Arribas, interviewed via Zoom by Douglas Heintzman, 1 Sept. 2025.

68. Dr. Clara Guerra, interviewed via Zoom by Douglas Heintzman, 15 Sept. 2025.

69. RBA, "Project Acacia: RBA and DFCRC announce chosen industry participants and ASIC provides regulatory relief for tokenized asset settlement research project," media release, Reserve Bank of Australia, 10 July 2025, https://www.rba.gov.au/media-releases/2025/mr-25-18.htm.

70. India Stack, *IndiaStack.org*, https://indiastack.org/, accessed 22 Oct. 2025.

71. MOSIP, "A Digital Public Good for Identity," https://www.mosip.io/, accessed 22 Oct. 2025.

72. "XRoad: Interoperability services," eEstonia.com, https://e-estonia.com/solutions/interoperability-services/x-road/.

73. European Commission, "European Digital Identity (EUDI) Regulation: From digital identification to digital Wallet," *Shaping Europe's Digital Future*, last modified 15 July 2025, https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation, accessed 22 Oct. 2025.

74. Joseph Bradley, interviewed via Zoom by Douglas Heintzman, 28 July 2025.

75. Ian Putter, interviewed via Zoom by Douglas Heintzman, 23 Sept. 2025.

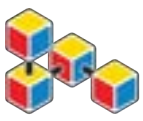
76. Dr. Suelette Dreyfus, interviewed via Zoom by Douglas Heintzman, 24 Sept. 2025.

77. Ismael Arribas, interviewed via Zoom by Douglas Heintzman, 1 Sept. 2025.

78. Dr. Clara Guerra, interviewed via Zoom by Douglas Heintzman, 15 Sept. 2025.

79. Dr. Florian Herzog, interviewed via Zoom by Douglas Heintzman, 21 Aug. 2025.

80. Dr. Horst Treiblmaier, interviewed via Zoom by Douglas Heintzman, 24 Aug. 2025.



blockchainresearchinstitute.org

cardanofoundation.org