STABILITY

PROOF INFRASTRUCTURE

Learning to Trust in an Era of Information Superabundance

07 July 2025

PROOF INFRASTRUCTURE

Executive Summary

The world is drowning in data, but thirsting for trust.

Information superabundance, accelerated by generative AI, is breaking society's traditional framework of "Trust Infrastructure" - trust based on self-verification, authority, and reputation - which can no longer scale to verify truth, source, or integrity of such massive volumes of data.

Proof Infrastructure offers a solution: a novel overlay of digital communications where all data is untampered and independently provable without relying on centralized platforms or intermediaries.

From AI transparency and content authenticity to supply chain integrity and fraud prevention, Proof Infrastructure uses provability to make trust scalable, programmable, and ultimately to become a built-in feature of digital communications, rather than a manual and subjective afterthought.

Only proof is scalable enough to meet society's fundamental need for information it can trust.

Proof Infrastructure is the way forward.

1. The Truth About Trust

A well-functioning society relies on trust.

But it's impossible for each person to verify every piece of information before relying on it, so "outsourcing" verification is necessary. The traditional infrastructure ("Trust Infrastructure") by which society outsources verification of truth, source, or integrity of data has barely changed through history. It is built around two primary mechanisms:

1. Authority: Historically this would have meant the educated class wielding social authority, such as monarchs, nobles, and religious leaders. In today's world, it refers to governments, regulators, and standards bodies, which impose legal obligations, enforce disclosures, investigate wrongdoings, and vouch for the truth or accuracy of information

issued by them. This model relies on central authority and assumes a manageable volume of data.

2. Reputation: Institutions, brands, platforms, and individuals become trustworthy based on accumulated credibility, success, and past performance. Trust is earned slowly, lost quickly, and is subjective and non-transferable. Private sector intermediaries such as Google, Meta, and Microsoft act both as stewards of the world's information, vouching for the integrity of data held by them, and as de facto gatekeepers of truth, moderating information flow and algorithmically influencing the information to which users have access.

1.1 AI as an Accelerant

The emergence of artificial intelligence ("AI") is hyper-accelerating the need for trust. AI is expected to generate nearly 50% of the world's data by 2025 and by some estimates up to 90% by 2026, transforming data from a byproduct of human activity into an autonomous, high-velocity output of machines. Humanity has never existed in an era defined by non-human exponential data creation until now.

Trust Infrastructure, while effective in the industrial and early digital eras, is ill-suited to establishing the truth of billions of AI-generated texts, images, decisions, or transactions per day - let alone in real time, across borders, and without human supervision.

1.2 The Trust Crisis

The limitations of Trust Infrastructure are a fundamental bottleneck.

As data volume explodes, the time and cost required to verify any single item of information increases. Without scalable proof mechanisms, trust becomes delayed, unreliable, or infeasible. Individuals can no longer tell what's real, companies can no longer vouch for the accuracy of what they consume or publish, and regulators fall increasingly behind. Society risks defaulting to distrust. This is the "Trust Crisis".

If the record numbers of scams, misinformation, and deepfakes are any indication, we may already be on our way. We can see the Trust Crisis manifesting today in multiple ways:

- Information pollution and distrust

  The flood of content, including misinformation and disinformation, overwhelms users' ability to distinguish signal from noise. This erodes confidence in digital platforms, journalism, science, and even interpersonal communication. Americans' trust in the media is at an all-time low and trust in science and scientists has declined.
- Widespread fraud

  Synthetic identities, deepfakes, forged documents, and data manipulations become trivial to produce and hard to refute. Criminals and bad actors can exploit the opacity and ambiguity of unverifiable data to impersonate, mislead, or manipulate at massive scale. As of 2021, fraud resulted in global losses amounting to approximately 6.4% of global GDP - around US $5.38 trillion.
- Social fragmentation

  With no objective anchor for truth, societies fracture into epistemic silos - groups of people who trust different sources, believe in different facts, and lose the ability to agree on reality itself. This weakens democratic processes, public health efforts, and collective responses to global crises. According to the Pew Research Center, Democrats both use and trust a wide range of news sources, while Republicans rely on a narrower and more concentrated group of sources, with up to a 20% overlap in news sources used by both.

In short, we are racing toward a world drowning in data but thirsting for trust.

To meet this moment, society must shift from the Trust Infrastructure model of *assumed trust*, based on authority or reputation - to a post-trust societal model of *provable trust*, where the authenticity, origin, and integrity of data can be independently verified by anyone, anywhere, at any time.

This is the premise of Proof Infrastructure: to evolve past the limitations of trust as an unscalable social construct, making it a highly-scalable technical capability woven into the very fabric of digital communications.

2. Understanding Proof Infrastructure

Proof Infrastructure represents a foundational shift in how trust is established in the digital world. Rather than relying on authority or reputation, Proof Infrastructure enables trust through technical guarantees built on cryptographic verification and public transparency.

Fundamentally, Proof Infrastructure answers the question: *Can this piece of data be independently verified as true, authentic, and untampered, without requiring me to trust the source?*

In other words, trust becomes an objective, verifiable property of any datum, rather than being dependent on social constructs like authority and/or reputation.

2.1 What is Proof Infrastructure?

Proof Infrastructure is a technological overlay that allows any digital data, including documents, transactions, digital files, actions, or events, to be verifiably:

- Authentic: It comes from a legitimate source.
- Untampered: It has not been altered since its creation.
- Traceable: Its origin, history, transformations, states, and other properties attaching to the datum can be audited.
- Portable: The abovementioned properties can be independently validated anywhere, without reference to centralized authorities or closed software systems.
- Provable: It embeds proofs such as digital signatures, attestations, and cryptographic commitments.

Notably, Proof Infrastructure decouples provability from software interfaces. Provability is embedded at the infrastructure level, making it universally accessible and verifiable regardless of the front-end tooling or platforms used.

2.2 Implementation

Proof Infrastructure can be accomplished through a combination of technologies, including but not limited to:

- Digital signatures: Proving that data was issued by a specific entity or under a specific cryptographic key.
- Cryptographic hashing: Proving that data remains unchanged since it was signed or recorded.
- Immutable ledgers (e.g. blockchains): Recording when and in what order data was created or modified.
- Zero-Knowledge Proofs, Privacy-Preserving Attestations: Proving facts about data without revealing or having sight of the data itself.
- Decentralized Identifiers and Verifiable Credentials: Where identification or credentials are relevant, providing such identity and credentials that are independently verifiable and resistant to forgery.

Proof Infrastructure can also be implemented at multiple layers:

- Content Layer: Embedding proof into the data itself, such as watermarking, metadata, and cryptographic tags.
- Transmission Layer: Proving data transmission was secure, authenticated, and untampered, as well as details of the transmission such as time-stamping, devices, and transmission pathways.
- Storage Layer: Ensuring stored data is verifiable, traceable, and immutable, and being able to prove that the stored data has not been modified.
- Computation Layer: Recording and verifying computational steps, including AI inference and decision-making.
- Interaction Layer: Capturing interactions between systems, agents (including AI Agents), or users, proving the authentication to carry out those interactions, and proving the authenticity of those transactions.

2.3 What Proof Infrastructure Isn't

Proof Infrastructure is not:

- Content moderation

  It is not intended to assess whether information is correct, ethical, or appropriate. In any event, the point is not that all digital communications (or in society, more broadly) must be true - fiction, for example, enriches society. Proof Infrastructure therefore must accommodate false data, but enable anyone to determine themselves whether the information can be trusted based on the data's accompanying properties. *Note: An exception to this may be where, in specific scenarios, such as where the content itself is deterministic, the content itself may be proved.*
- A trust score

  It does not assign scores or ranks to establish reputation. It proves *what* happened, *when*, and where applicable, *who* did it. It does not say *how much* someone should be believed.
- A blockchain

  Blockchains may contribute to the architecture, but Proof Infrastructure is a broader concept synthesizing various technologies and principles to achieve scalable provability as a fundamental property of data, to be used as a foundation for trust.
- Subjective

  It is not opinion-based or subjective. It is entirely deterministic, ensuring that each datum is provable with consistent outcomes no matter how many times the proof is executed and irrespective of the prover.

2.4 Why Proof > Trust

Trust Infrastructure is slow to scale because authority and reputation are inherently:

- Opaque: Trust is granted by each person subjectively based on sentiment, it is non-neutral and can hold biases.
- Centralized: Dependent on government authorities or reputable private entities, it is difficult for individuals, new entities, AI Agents, and small businesses to elicit the same levels of trust.

- Slow to establish/develop: It takes years for governments to set up regulatory bodies and for private entities to build trusted reputations.
- Non-exhaustive: Authorities and private entities may only vouch for data issued by and relevant to them, but will not vouch for all data. Consequently, there are entire clusters of data-types that Truth Infrastructure does not address or support.

Proof Infrastructure changes that by offering:

- Speed: Proof Infrastructure can be implemented immediately, because it is a technological innovation, and proofs themselves are immediate and machine-verifiable, enabling real-time or near-real-time decision-making.
- Scale: Proof can be embedded into trillions of data transactions, creating global infrastructure for digital communications, and enabling provability regardless of the volume of data generated.
- Objectivity: Proof is not biased by sentiment, it's just math - fact-based and objective.
- Neutrality: Verifications can be independently performed and proofs work the same way no matter who performs the verification, making proofs absolutely neutral.

When a tech giant runs a global marketing campaign claiming to care about your privacy, you shouldn't need to take them at face value. They should be able to prove it.

2.5 Proof Makes Trust Programmable

Where Proof Infrastructure is implemented, developers can build systems that only process data with valid proofs. For example:

- AI Agents would prove that they only process data with proven provenance.
- AI Agents would only interact with other AI Agents that have proven that they only process data with proven provenance.
- AI Agents would have auditable records to prove what processes they use to process data, and through this, be able to prove that they are consistent in how they apply such processes.

- Humans looking at AI Agent outputs would be able to trust - but more importantly, prove - that the outputs have been made based on reliable processes and data with proven provenance.

Just as encryption made privacy programmable, Proof Infrastructure makes trust programmable.

3. Examples Where Proof Infrastructure Can Succeed Where Trust Infrastructure Fails

Below are some key areas in which Proof Infrastructure fills much-needed gaps that traditional Trust Infrastructure fails to address.

3.1 Artificial Intelligence, Generative AI, and Agentic AI

By 2026, most data is anticipated to be AI-generated, with some estimating that AI will be responsible for up to 90% of data generation.

As AI systems, particularly Generative AI and Agentic AI, become increasingly embedded in our lives, the need for provability across the AI lifecycle becomes paramount. Without the ability to independently verify what an AI system did, why it did it, how it was trained, and whether its output is consistently reliable, trust in AI outcomes will remain tenuous.

Proof Infrastructure provides the foundation to embed accountability, transparency, and verification into AI systems by enabling cryptographic attestation of every significant stage of AI development, deployment, and action, including metadata associated with each action.

Proof Infrastructure can enable:

- proof of input integrity by using verifiable logs of input data (e.g. prompts, sensor inputs, or user commands) to enable downstream users or regulators to confirm that outputs were generated in response to specific, known inputs without revealing sensitive or proprietary content.

- proof of model provenance and training data for foundational models or fine-tuned LLMs, by recording metadata about datasets used, model versioning, and training procedures, in a tamper-proof and publicly auditable format. This supports transparency, enables challenges arising from training data to be resolved more quickly (e.g. IP infringement), and can help identify AI bias or other risks stemming from training data.
- reconstruction and verification of AI decision-making paths by logging inference processes, chains of reasoning, memory retrieval, API/tool calls, sub-agent interactions, intermediate states, and other internal processes, providing verifiable and much-needed transparency and insight into AI reasoning.
- AI-to-AI trust. As AI Agents interact, collaborate, and make decisions on behalf of humans or organizations, they need a way to verify each other's claims, capabilities, and compliance. Proof Infrastructure acts as a substrate allowing AI Agents to publish verifiable claims and proofs such as proof of competency, reputation, resource use, or task execution, and enables secure, trustless inter-Agent cooperation.
- users, creators, and regulators to distinguish between human and machine generated content by embedding attestations directly into digital files or assets to prove their provenance, authorship (AI or human), and integrity. As is mentioned in other sections of this whitepaper, this capability helps combat issues like disinformation, misinformation, and fraud.
- proof of model use, versioning, and deployment context, including details like configuration, environmental context (e.g. hardware, runtime, prompt templates), and usage restrictions. This information would allow AI providers and customers to conduct AI model analysis internally, and provide real-time transparency to counterparties and regulators conducting audits.

Proof Infrastructure shines a light on the black box of AI operations, and ensures that AI is not just powerful but provably trustworthy.

3.2 Content Authenticity

The explosion of digital content creation significantly amplifies challenges around verifying authenticity, authorship, and ownership.

Copyright infringement, unauthorized distribution, and plagiarism not only lead to substantial financial losses, but also undermine trust, discourage creators, and inhibit innovation across creative industries. Media and entertainment piracy alone will account for an estimated $75 billion in lost revenue globally for 2025 and is expected to reach $125 billion by 2028, with piracy increasing annually at nearly 11%.

Proof Infrastructure can be a robust tool:

- Enabling anyone to distinguish software-generated data from data generated by real users or hardware. By creating transparency around the use of generative AI, actors can enjoy stronger personality rights and productions can manage digital assets more efficiently.
- Enabling provable authorship and originality. In particular, this democratizes the creative industry by empowering independent creatives (who lack the resources of large production houses and studios) to affordably obtain and submit indisputable proof to enforce or defend against intellectual property infringement claims.
- Empowering media industries such as Hollywood and the music industry to securely track and verify the distribution of movies, scripts, screenplays, soundtracks, and other creative assets, dramatically reducing losses from piracy and unauthorized distribution. Additionally, rights-holders can monitor contracts and royalties more transparently and efficiently, enhancing their ability to verify and collect accurate royalties.

By embedding trust directly into creative content, Proof Infrastructure can reduce infringement, enhance the protection and empowerment of artists and creators, and promote sustainable growth across the entire creative industry spectrum - from Hollywood studios and major music labels to individual creators and emerging digital platforms.

3.3 Supply Chain and Logistics

The global supply chain industry is worth $9 trillion, of which approximately $15.5 billion is spent annually on paper-based bills of lading alone - a 2,000 year old technology that remains in use because paper documents are non-fungible.

However, paper documents still suffer from risks such as fraud/forgery, loss, damage, and destruction. They also attract other negative externalities such as the environmental impact of posting them around the world and time spent on their transit.

Digital documents have generally suffered from fungibility. While blockchain technology has enabled non-fungible digital documentation, crypto and wallet-based infrastructure has been too complex for mass adoption.

Proof Infrastructure could be used to:

- demonstrate and prove non-fungibility, immutability, various states of the trade document such as ownership/possession/retirement, and as supporting documentation for insurance claims ;
- demonstrate and prove other properties relating thereto including tracking data for shipments, customs declarations, sourcing information, food and safety declarations such as ingredients and allergens;
- eliminate loss, destruction, and fraud; and
- lower negative externalities such as time, cost, environmental impact, and improve the processing speed for insurance and other claims;

all while remaining independently verifiable by authorized parties such as regulators or end-consumers.

3.4 Gaming and Esports

The global gaming market is estimated to reach over $503 billion in 2025, up from $396 billion in 2023. Gaming culture has long prided itself on gaming being a great equalizer, transcending race, religion, social background, and nationality - a space where skill is the sole and ultimate determinant of success.

Nevertheless, gaming faces significant challenges related to trust, asset authenticity, cheating, and fraud. As the gaming ecosystem becomes increasingly digital, online, and asset-driven, fairness and control over in-game assets become more challenging to manage.

On the esports front, global esports is estimated to be worth $2.89 billion in 2025, growing at an annual rate of 20.9%. In the United States alone, universities awarded over $16 million to attract top esports talent in 2020, and 130 universities offer esports scholarships as of 2022. But hacking, bot usage, and exploits compromise game fairness and undermine the integrity of scholarships and scholastic admissions for players.

Proof Infrastructure can be used to:

- Authenticate game data and esports events by providing cryptographic proof of game state changes, player actions, and server events, dramatically reducing cheating opportunities
- Enable verifiable fairness in e-sports tournaments and gaming leaderboards, reinforcing trust among players and spectators alike.

Gamers also grind hard for in-game assets - unique skins, rare weapons, seasonal awards, rare materials for crafting, competition badges, each a mark of skill and dedication. Some of these may be tradable for real-world money via marketplaces operated by game publishers. Current digital infrastructures typically provide limited verifiable ownership or transferability of such assets, and may even be subject to fraudulent duplication or other exploits.

Proof Infrastructure would enable:

- Game developers and publishers to transparently and securely manage virtual marketplaces, creating a trustworthy and fair digital economy via immutable, cryptographically verifiable records of asset creation, ownership, trade history, and authenticity, and elimination of duplication, theft, and fraud on the virtual marketplaces. If done correctly, this would not impact the in-game economies that have been carefully designed and implemented.
- Verifiable proof of ownership to follow players across platforms and even across compatible games, essentially letting them take their in-game assets from one game to another, thereby increasing player engagement and long-term loyalty.

3.5 Finance

The financial sector is built on trust between institutions, clients, regulators, and markets. Yet, despite extensive regulation, traditional financial systems are plagued by opacity, inefficiencies, and remain susceptible to fraud. Meanwhile, compliance costs are sky-high - financial institutions globally spend over US $206.1 billion per year on compliance alone.

Proof Infrastructure offers a transformative opportunity to embed provability into financial data, transactions, and operations, making trust scalable, transparent, and real-time. In particular, Proof Infrastructure can enable:

- Real-time transaction integrity by cryptographically signing and time-stamping every transaction, enabling participants, auditors, and regulators to verify its authenticity and order of execution. This reduces settlement disputes and strengthens systemic resilience.
- Zero-knowledge proofs of financial institution reserves and solvency without revealing confidential or sensitive customer information.
- Financial institutions generate authentic and cryptographically verifiable logs of regulatory compliance activities (e.g. KYC/AML checks, risk assessments, trade executions) for real-time or on-demand non-intrusive audits and compliance/regulatory reporting, while reducing audit costs.
- Digital signatures and verifiable credentials to prevent identity theft, document forgery, and transaction tampering, helping to prevent and mitigate fraud across a spectrum of financial services including loan applications, insurance claims, and cross-border payments.
- Financial assets to be tokenized with embedded proofs of ownership, authenticity, and transfer history, opening up new asset classes and enhancing existing ones with embedded proofs of ownership, authenticity, and transfer history.
- Use of AI in the financial sector to be tracked and proven. As AI systems become embedded in operations such as trading, credit decisions, and customer interactions, Proof Infrastructure can record input data, model decisions, and inference logic to prove AI outputs and output consistency, improve AI explainability, and demonstrate compliance with AI governance frameworks.

Proof Infrastructure provides a way to reduce information asymmetry in the finance sector without sacrificing privacy or operational efficiency, and ultimately empowers the financial sector to move beyond “Trust me, I’m a bank” towards a future of provable finance.

3.6 Digital Identity

According to a report published in December 2024 by the United Nations Children’s Fund (”UNICEF”), 20% of children worldwide under the age of 5 remain unregistered and lack a legal identity.

In relation to children under the age of 1, UNICEF reports:

> *Today, 53 million infants lack a birth certificate: This includes 37 million babies who are unregistered and 16 million whose births are reported as registered but who lack proof in the form of a birth certificate.*
> *- The Right Start in Life: Global levels and trends in birth registration*

Identity is foundational to all societal interaction. Without it, our existence is real only to ourselves, and our claim to an identity (any identity) can’t be verified or trusted by others.

The United Nations 2030 Agenda for Sustainable Development recognizes the importance of identity under Sustainable Development Goal 16, and in particular target 16.9 which calls for the provision of legal identity for all human beings by 2030.

But there is no universal standard of identity management. Implementation of identity management processes and systems is autochthonous to each country. In the digital space, identity management systems traditionally rely on centralized login providers, siloed government databases, and/or proprietary credentials. Consequently, identity management processes and systems suffer from fragmentation and limited interoperability.

The United Nations Commission on International Trade Law’s (“UNCITRAL”) Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (”MLIT”) provides a principles-based and technologically neutral legal foundation for cross-border recognition of identity management and trust services, including in digital form.

MLIT-compliant identity management and trust service providers would enable interoperable and cross-border recognition of identity.

In fact, many of the principles articulated in the Guide to Enactment of the UNCITRAL MLIT closely align with Proof Infrastructure concepts, such as:

Reliable and independent verification of identity:

> *4. The growth of online commercial activities is built on trust – and needs to be supported by a continued sense of trust – in the electronic environment. One important component of that trust is the ability to identify each party in a reliable manner, especially in the absence of any prior in-person interaction.*

Proving data associated with, and metadata of, a datum:

> *6. Another important component of online trust is the ability to rely with sufficient confidence on the quality of data, which underpins data exchanges. Trust services that provide assurance on qualities of a data message such as its origin, its integrity and the time of processing of a certain related action have emerged as solutions to provide that confidence.*

The need for Proof Infrastructure (described as a “trust framework”) and participants to Proof Infrastructure (described as an “identity federation”):

> *56. [Identity Management (”IdM”)] service providers, subscribers, relying parties and other entities concerned may agree to operate under compatible policies, standards and technologies, which are specified in system rules, so that credentials provided by each participating IdM service provider can be understood and trusted by all participating relying parties. This arrangement may be referred to as “identity federation”, and the system rules, which are of a contractual nature, as a “trust framework”. Identity federation may contribute to increasing the number of users and of applications sharing the same IdM services, which, in turn, may reduce costs, thus ensuring long-term sustainability.*

Proof Infrastructure (or the “trust framework” in MLIT parlance) complements the MLIT by enabling identity to be defined as a set of objective, deterministic, and provable properties, and enabling these properties to be proven without requiring disclosure of a data subject’s full identity:

- Authentic: The identity and its claims are digitally signed by a trusted issuer such as a government authority, with clear provenance and integrity guarantees.
- Tamper-evident: Any modification to identity data or metadata invalidates the cryptographic proof.
- Portable and interoperable: Identity proofs can be presented and verified independently of the original issuer or system that created them. Open standards (e.g. OpenID4VCI, W3C Verifiable Credentials v2.0, etc) can enable interoperability across platforms and jurisdictions.
- Privacy-centric: Technologies such as zero-knowledge proofs enable users to prove only selected and relevant attributes of a data subject (e.g., X is a real person, X is over 21, X is has a valid driver’s license for specified vehicles, X is a citizen of a specified country, etc) without revealing the full details of the data subject’s identity.

These properties are valuable in a variety of identity-centric scenarios such as:

- Supra-national identification: Cryptographically proven identity documents, such as driver’s licenses, passports, and other forms of national IDs, issued by one country can be independently authenticated by another country and granted legal recognition.
- KYC/AML compliance: Financial institutions can directly rely on verifiable credentials issued by government authorities, reducing onboarding times and the need for third party intermediaries.
- e-Government services: Verifiable credentials issued by government authorities can be used for cross-border access of e-Government services. For example, if a citizen of one country owes taxes in two countries, they could use the same identity credentials to access tax portals of both countries.
- Travel and immigration: Digital identity credentials can be used for seamless cross-border identity verification by reducing reliance on physical documents, speeding

up security checks and immigration/customs clearances, and detecting and eliminating forged documents.

By ensuring that identity data can be provably verified rather than merely trusted, Proof Infrastructure advances the goals of the MLIT by laying the foundation for a global identity ecosystem that is more secure, privacy-centric, and legally interoperable.

3.7 Healthcare

The healthcare industry faces critical challenges in maintaining trust, ensuring accuracy, and protecting patient privacy.

Medical errors are the third-leading cause of death in the United States, after heart disease and cancer, and are estimated to cause more than 250,000 deaths per year in the United States alone]. Errors can arise from a combination of factors, including inaccurate or inaccessible patient data across public and private healthcare networks.

Fraudulent activities such as falsified medical records or counterfeit pharmaceuticals further threaten patient safety and public health.

Proof Infrastructure can be applied in healthcare to:

- Create immutable medical records, including medical history, treatments, prescriptions, and diagnoses, to significantly reduce medical errors stemming from data inaccuracies or unauthorized alterations. Healthcare providers can confidently rely on the authenticity of medical data, leading to better patient outcomes.
- Enable traceability and verification of drugs, enabling pharmaceutical companies, doctors, patients, and regulators, to easily and independently verify the authenticity of drugs at any time.
- Ensure the integrity of clinical trial data by recording and verifying for transparency, accountability, and authenticity of research results. This verification method supports quicker and more reliable regulatory approvals.
- Record and verify patient/trial subject's Informed Consent, ensuring that healthcare organizations demonstrably comply with global privacy regulations such as the EU's

General Data Protection Regulation ("GDPR"), and Good Clinical Practice ("GCP") standards in clinical trials.

- Enable real-time regulatory compliance by allowing regulators and healthcare providers to independently verify compliance and audit trails in real-time or at their convenience, saving time and costs.

3.8 Education and Work Experience

Verification of educational credentials and professional experiences is fundamental for employment, higher education admissions, and professional certifications. However, resume fraud is widespread. It undermines institutional integrity, workplace efficiency, and career opportunities. Resume fraud is estimated to cost employers $600 billion annually.

Traditional verification methods, which are often manual, slow, costly, and susceptible to inaccuracies, can no longer adequately support the need for trust in credentials.

Proof Infrastructure can be applied in this space to:

- Enable academic institutions to issue degrees, certifications, and transcripts in an immutable, cryptographically verifiable format, which can be independently validated by employers, educational institutions, and professional bodies.
- Enable individuals to share verified records of their education, skills, and work experiences seamlessly across multiple platforms and jurisdictions, simplifying job applications and speeding up background and credential checks.
- Enable verification of micro-credentials such as online courses and professional training.
- Create immutable and verifiable employment records, including details about roles, responsibilities, and duration of employment, to improve hiring accuracy.
- Enable educational institutions to demonstrate admittance standards, and employers to demonstrate hiring standards and employment regulation compliance, transparently and verifiably.

3.9 Combating Misinformation and Disinformation

Misinformation and disinformation represent some of the most critical threats facing society today.

Misinformation may or may not have malicious intent, and may or may not be propagated as part of a political agenda. Its insidious twin, disinformation, is the deliberate spread of falsehoods to intentionally undermine the national security of a nation.

Both erode trust in institutions, up-end political processes, and negatively impact public safety.

The rapid and unchecked spread of misinformation and disinformation, exacerbated by social media, automated bots, and increasingly realistic generative AI, creates an urgent need to prove data comprehensively at-scale.

Proof Infrastructure is a potent tool in combating misinformation by embedding provability directly into all digital information. In particular, Proof Infrastructure can be used to:

- Ensure that every piece of digital published content, such as news articles, reports, or official announcements (e.g. government-issued announcements), is immutably associated with its verified source. Users, platforms, and regulators can independently verify origin and authenticity. For individuals, this also reduces susceptibility to misinformation and scams. According to 2024 estimates, scams cost consumers over $1 trillion globally, with US victims having the highest losses at $3,520 per scam victim.
- Enables misinformation to be more rapidly traced and managed, by providing transparency of the spread and origin of the misinformation.
- Reduce deepfakes and other risks associated with AI-generated content, by providing cryptographic proof of original, authentic media and its source. Proof Infrastructure can even be encoded into firmware to allow anyone to prove whether media was software-generated (e.g. AI software) or hardware-generated (e.g. a sensor recording a real-life event).

3.10 Evidence in Court

The ease with which anyone can now generate convincing deepfakes calls the trustworthiness of all digital evidence into question and poses significant challenges to evidentiary value.

Professor Daniel W. Linna Jr. *et al* writes:

> *There is no foolproof way today to classify text, audio, video, or images as authentic or AI generated, especially as adversaries continually evolve their deepfake generation methodology to evade detection. Thus, the generation and detection of fake evidence will continue to be a cat and mouse game. These are not challenges of a far-off future, they are already here. Judges will increasingly need to establish best practices to deal with a potential deluge of evidentiary issues.*
> - *Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases*

An article by the Illinois State Bar Association titled "*Deepfakes in the Courtroom: Problems and Solutions*" further outlines these challenges.

Higher standards are required to ensure that factual data generated by AI systems is accurate and can be relied upon by the Courts, and that non-factual data such as deepfakes are identifiable and rendered inadmissible. Provability is more important than ever to uphold the fair and equitable administration of justice.

Proof Infrastructure in this space would enable:

- an auditable and immutable record of chain-of-custody, ensuring that the exact origin and time of creation of digital evidence, as well as every access, edit, or transfer of evidence, is logged and verifiable through an auditable and immutable record of chain-of-custody
- systems to flag or exclude content created or altered by generative AI.
- AI processes to be recorded and inspected for reliability, and AI-based data analyses to be compared against the recorded process to ensure that the analyses are consistent with the process and sufficiently reliable so as to hold evidentiary value.

4. Challenges

While Proof Infrastructure offers a transformative framework, some complex challenges remain. We set these out below. Proof Infrastructure is a novel concept. Accordingly, this list is non-exhaustive and more challenges may emerge.

4.1 Immutability

The value of immutability is well understood and needs no restating. However, because data once written cannot be retracted nor erased, specific challenges arise relating to personal data, confidential information, illegal content, and human error.

- Personal Data: Individuals have a right of correction under most privacy laws, and a right of erasure under privacy laws of certain jurisdictions. An immutable record of data would not permit correction or erasure.
- Confidential Information: As with Personal Data, Confidential Data once written cannot be retracted nor erased.
- Illegal content: In cases where criminal or harmful content is embedded into a proof or committed on-chain, immutability prevents removal.
- Human error: Accidental or incorrect entries could become permanent, even if demonstrably inaccurate or harmful.

These concerns may be mitigated by:

- Off-chain commitments: Generally, all data (including personal data and confidential information) should be hashed and stored off-chain, and only the cryptographic proof recorded immutably. This enables verifiability without exposing the underlying data.
- Chained rectifications: Updates or corrections can be layered on top of the original record as cryptographically-linked events, preserving transparency while delivering the updated information.
- Front-end controls: Since users interact with Proof Infrastructure through front-end interfaces, front-end providers should build safeguards to prevent the display or

propagation of illegal content or blacklisted content while leaving the underlying proofs intact.

4.2 Personal Data Protection

Beyond the challenges of immutability, global privacy laws still apply to regulate the collection, processing, disclosure, and handling of personal data. Key challenges of data privacy compliance include:

- Unintentional data exposure: Pseudonymization could lead to re-identification under certain conditions.
- Regulatory unfamiliarity: Supervisory authorities may not be familiar with cryptographic techniques such as verifiable credentials, zero-knowledge proofs, and homomorphic encryption, or anonymization techniques such as differential privacy. This may complicate compliance strategies for businesses.[1]

These considerations are not unique to Proof Infrastructure - in fact they are common to all, and users of Proof Infrastructure are ultimately responsible for complying (and demonstrating compliance) with applicable data privacy laws.

4.3 Data Storage

Data storage for Proof Infrastructure should be robust. As adoption of Proof Infrastructure scales, persistent proof records and other data stored in connection with Proof Infrastructure will increase storage overheads. There is no centralized “authority” or party responsible for storing data relating to proofs - it would be for each participant in the Proof Infrastructure to store the proofs relating to the data they wish to prove. However, careful data classification can help optimize this cost, and not all data may require permanent storage.

4.4 Environmental Impact

Every day, there are approximately:

[1] That said, some regulators are taking a proactive approach to cryptography for privacy regulation - for example, the Singapore Personal Data Protection Commission has released a Guide to Basic Anonymisation which covers technical considerations relating to anonymization techniques in some detail.

- 13.1 trillion HTTP requests (caa 2019)
- 8.5 billion Google searches (caa 2022)
- 333 billion emails sent (caa 2022)
- 24 billion text messages sent (caa 2022)
- And countless other social media postings, streaming requests, IoT signals, CDN/API calls, and backend service interactions.

The volume of internet transactions in 2025 is likely to be substantially higher, and at least in the tens of trillions per day.

Proof Infrastructure must contend not only with recording that enormous volume of transactions across the entirety of all digital communications including the internet - it should ideally also have no greater environmental impact than an ordinary large internet service.

For reference, Microsoft and Google each consumed 24 TWh of electricity in 2023.

4.5 Barriers to Adoption

The current ecosystem of blockchains is fragmented, leading to siloed systems and (i) a lack of interoperability; or (ii) high levels of complexity required to create compatibility between protocols.

Cryptocurrencies also act as barriers to adoption, introducing:

- regulatory risks such as anti money laundering and securities risks
- technical and integration complexity
- administrative and change management challenges such as wallet management, user training and adoption, and risk of mismanagement of corporate funds by wallet administrators
- competing incentives, resulting in protocols throttling throughput to maximize gas fees, and deprioritizing enterprise utility in favor of crypto value enhancement and market capitalization.

A high speed, high throughput, public blockchain protocol without cryptocurrency and wallet dependencies, and which can provide straightforward API integrations, would significantly remove barriers to adoption.[2]

4.6 Public Policy, Legal, and Regulatory Concerns

Proof Infrastructure aligns with growing global demands for transparency, auditability, and security, but laws and regulations may struggle to keep pace with novel technical paradigms.

To address this:

- Governments, standards bodies, and international institutions should be engaged early to develop new legal doctrines and policy around provable data.
- Proofs, smart contracts, and other technical processes may need to be accompanied by declarations or legally binding attestations that translate their meaning for non-technical stakeholders. Supplementary information such as context, applicable compliance rules (e.g. specific laws or codes of conduct), and statements of intent, would also help to provide richer understanding around raw proofs.

5. Defining the Future

We are entering an era defined not by information scarcity, but by Information Superabundance - much of it autonomously generated and instantaneously distributed. In such an environment, trust cannot be assumed, inherited, or manually granted.

It must be proven.

Proof Infrastructure represents a fundamental change from systems that rely on *who* says something, to systems that prove *what*, *when*, *where*, and *how* it was said, irrespective of the speaker.

Provability enables trust to scale with Information Superabundance, not collapse under it.

[2] In this regard, Stability's Global Trust Network is to our knowledge the only blockchain meeting such requirements.

As Proof Infrastructure becomes a native overlay of digital communications, like TCP/IP or HTTPS, its effects will compound:

1. Proof will make trust programmable: Developers will be able to embed provability directly into applications, platforms, and protocols.
2. Entities will be able to credentialise their data: Businesses, AI Agents, individuals - organizations of all sizes whether private or public, reputed or new and unknown - will be able to prove their data and claims relating thereto, rather than merely making “trust me” assertions.
3. Users will be empowered: Individuals can exercise agency in deciding what to trust because proofs can be independently verified.

Proof Infrastructure will not replace Trust Infrastructure - it supplements Trust Infrastructure by adding a technical overlay that allows all digital data to be provable, thereby removing any pressure for Trust Infrastructure to underwrite it.

Those who adopt Proof Infrastructure will not only lead the next generation of digital services - they will help define the next generation of communication itself.

If you would like more information on Proof Infrastructure and real world implementations, or if you’re a developer and want to get up and running in minutes, please contact us at contact@stabilityprotocol.com or visit our website at http://stabilityprotocol.com/.