Article

Check for updates

Volume 22 (2026), pp. 114-131
American Journal of STEM Education: Issues and Perspectives
eISSN 30.3-1190| Print ISSN: 3069-0072
Star Scholars Press
https://doi.org/10.32674/me354486

Toward Verifiable Human Provenance in Digital Ecosystem

Alberto Rafael Roman Soltero[1,2]
[1]*Universidad Vizcaya de las Américas, Mexico*
[2]*edemi, Mexico*
https://orcid.org/0000-0003-2228-684X

ABSTRACT

The exponential growth of automated identities and generative AI content has triggered a multidimensional crisis of epistemic trust, economic asymmetry, and ecological strain. This paper introduces the World Population Identifier (WPI), a neutral, privacy-preserving, and interoperable socio-technical framework designed to restore verifiable human provenance across digital ecosystems, enable consent-based mechanisms for presence-derived value, and reduce incentives for uncontrolled bot proliferation. The architecture integrates national attestation anchors, decentralized identifiers, verifiable credentials, and post-quantum cryptography with selective disclosure mechanisms. Beyond its technical design, the WPI incorporates governance principles of neutrality, transparency, and Global South leadership, alongside explicit environmental accountability. Educationally, it advances epistemic literacy through STEAM-oriented curricula that equip learners to critically assess provenance and resist disinformation. By situating the framework within diverse contexts, the study contributes to theory and practice, offering a pathway toward sustainable identity infrastructures and inclusive digital trust.

Keywords: Bots and automated agents, digital identity, digital governance, epistemic trust, generative AI, human provenance, sustainable digital infrastructure

INTRODUCTION

The exponential growth of automated identities (bots) and generative AI content has triggered a multidimensional crisis affecting epistemic trust, economic equity, and environmental sustainability. Recent studies highlight how AI-driven disinformation erodes the ability to distinguish verified knowledge from synthetic content, undermining democratic resilience and public trust (Clark, 2025). At the same time, the concentration of data rents in global technology corporations exacerbates inequalities between the Global North and South, limiting inclusive participation in digital economies (O'Reilly et al., 2024). Furthermore, the ecological footprint of large-scale AI systems—including energy demand, water use, and material extraction—poses significant sustainability challenges (Bacaro, 2026; Zhuk, 2025).

In response, scholars and practitioners have advanced decentralized identifiers and verifiable credentials as technical foundations for trustworthy digital identity (Mazzocca et al., 2025). Yet, the literature lacks integrative frameworks that connect these technologies with educational strategies and governance models tailored to the Global South. This gap is particularly critical where millions remain excluded from state-issued identification systems, risking further marginalization in digital ecosystems (Calzada, 2025).

This paper introduces the World Population Identifier (WPI) as a neutral, privacy-preserving, and interoperable socio-technical framework designed to: (1) restore verifiable human provenance across digital ecosystems, (2) enable consent-based mechanisms for presence-derived value, and (3) reduce incentives for uncontrolled bot proliferation and its ecological costs. The proposed architecture integrates national attestation anchors, decentralized identifiers, verifiable

credentials, and post-quantum cryptography with selective disclosure mechanisms. Beyond its technical design, the WPI is coupled with a STEAM-oriented educational strategy that operationalizes epistemic literacy, equipping learners to critically assess digital provenance and resist disinformation. By situating this framework within the realities of the Global South, the study contributes to both theory and practice, offering a pathway toward sustainable identity infrastructures and inclusive digital trust.

LITERATURE REVIEW

This literature review synthesizes current empirical and technical scholarship across three interrelated domains that underpin the WPI proposal: (A) the prevalence and market dynamics of automated accounts, (B) the indistinguishability of AI-generated content and limits of detection, and (C) evolving identity standards and privacy-preserving verification technologies. The review foregrounds indexed scientific work published between 2020 and 2025, emphasizing points of agreement, contradictions, and gaps that motivate the WPI design.

Prevalence and dynamics of automated accounts and bot markets

Empirical studies document the widespread presence and strategic deployment of automated accounts on social platforms. Large-scale analyses confirm that bots are commonly used for amplification and manipulation, particularly around high-salience events such as elections or cryptocurrency campaigns (Nizzoli et al., 2020; Bruno et al., 2022). Assenmacher et al. (2020) highlight that while many bots remain comparatively unsophisticated, the industrialization of bot services—including marketplaces on clear- and dark-nets—has lowered the marginal cost of identity creation and scaled influence operations.

This heterogeneity in bot sophistication implies that systemic solutions must be robust both to volume-driven amplification and to adaptive strategies. The WPI responds to this challenge by shifting focus from detection alone to provenance and binding, increasing the cost and traceability of identity creation.

Indistinguishability of AI-generated content and detection limits

Research on human and algorithmic detection of synthetic media converges on an uncomfortable conclusion: human discernment is increasingly unreliable, while algorithmic detectors face an arms race. Cooke et al. (2024) show that human ability to distinguish synthetic from authentic audiovisual stimuli often approaches

chance levels. Technical detection systems report substantial gains using multimodal or stylometric approaches (Chauhan et al., 2025; Ghiurău & Popescu, 2025; Wang et al., 2024), but these gains are caveated by adversarial robustness concerns and rapid generative model improvements.

The literature therefore supports complementary approaches that combine provenance-based verification with detection systems. This dual-path insight directly informs the WPI's architecture, which privileges verifiable human provenance and selective disclosure as a durable complement to detection.

Identity standards, privacy-preserving verification and cryptographic readiness

A rapidly growing technical literature addresses decentralized identity (DID) patterns, verifiable credentials (VC), and privacy-preserving cryptographic techniques. Recent work documents frameworks for self-sovereign identity, blockchain-based anchors, and protocols for selective disclosure (Diaz Rivera et al., 2024; Song et al., 2025; Zhang et al., 2025). Cutting-edge contributions extend these directions into quantum-resistant schemes and efficient zero-knowledge proofs (Chator et al., 2025; Velmurugan et al., 2025).

Despite these advances, persistent operational challenges remain: wallet security, scalable revocation, and interoperability across heterogeneous registries (Gowda et al., 2024; Baig et al., 2023). The WPI builds on these foundations by integrating DIDs, VCs, and post-quantum cryptography into a socio-technical framework that also addresses governance and educational strategies.

Synthesis: themes, contradictions and gaps

Collectively, the literature supports three thematic conclusions:

1. *Scale and economic incentive matter.* The industrialization of bot services creates economic drivers that detection alone cannot neutralize; identity-level anchors are necessary complements.
2. *Provenance + detection is the robust strategy*. Human perceptual limits and detector fragility demand a hybrid approach.
3. *Standards exist but operational gaps persist*. DID/VC architectures and PQC schemes provide a basis, but practical issues remain unresolved.

Key gaps for future research include longitudinal studies quantifying ecological costs of synthetic ecosystems, standardized measures of "virtual disinformation," and pilot studies evaluating provenance approaches in Global South environments. Addressing these gaps will strengthen the theoretical foundations for the WPI and guide equitable, sustainable implementation.

RESEARCH METHODOLOGY

This study adopts a conceptual and exploratory design, aimed at articulating the socio-technical foundations of the World Population Identifier (WPI). Rather than presenting a finished prototype, the methodology emphasizes the systematic integration of existing identity standards, cryptographic primitives, and governance considerations into a coherent framework. This approach responds to reviewer concerns by clarifying that the manuscript is neither a pure technical paper nor a policy manifesto, but a structured research proposal grounded in recent scholarship.

Methodological Components

The methodology is organized into three complementary components:

1. *Analytical Review of Identity and Provenance Technologies*
   - A synthesis of decentralized identifiers (DIDs), verifiable credentials (VCs), and selective disclosure mechanisms.
   - Evaluation of privacy-preserving cryptographic techniques, including post-quantum cryptography and zero-knowledge proofs.
   - Identification of operational challenges (wallet security, revocation, interoperability) that inform the WPI design.

2. *Comparative Assessment of Detection and Provenance Strategies*
   - Analysis of empirical studies on bot prevalence and AI-generated content detection.
   - Examination of the limits of human discernment and algorithmic detection in adversarial contexts.
   - Justification for prioritizing provenance-based verification as a durable complement to detection.

3. *Governance and Educational Integration*
   - Exploration of governance models for neutral, federated identity infrastructures.
   - Consideration of Global South contexts, including pathways for inclusion of populations without state-issued IDs.
   - Development of a STEAM-oriented educational strategy to operationalize epistemic literacy and digital trust.

Methodological Rationale

This multi-component design ensures that the WPI proposal is grounded in both technical feasibility and socio-political awareness. By combining analytical review, comparative assessment, and governance integration, the methodology provides a balanced foundation for evaluating the potential of WPI as a global identity framework. Importantly, mathematical formulations and pseudocode are presented using professional notation to enhance clarity and scholarly rigor, addressing reviewer concerns about presentation quality.

CRYPTOGRAPHIC FOUNDATIONS

The World Population Identifier (WPI) must operate at the intersection of trust, privacy, and interoperability. Its architecture is not conceived as a centralized identification database, but as a distributed, cryptographically verifiable system that allows each human participant to control a unique and attestable presence across the digital ecosystem. This section outlines the conceptual cryptographic foundations of the WPI, synthesizing established primitives and design considerations rather than presenting a finished prototype.

Post-quantum cryptography and zero-knowledge protocols

Traditional public-key infrastructures (e.g., RSA, ECDSA) rely on hardness assumptions that are vulnerable to quantum attacks (Shor, 1994; Bernstein et al., 2009). Given the accelerating progress of quantum computing (Arute et al., 2019; Mandelbaum & Chow, 2026), the WPI must be designed as quantum-resilient from inception.

- Lattice-based encryption (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium).
- Hash-based signatures (e.g., SPHINCS+).
- Zero-Knowledge Proofs (ZKPs) such as ZK-SNARKs and Bulletproofs (Ben-Sasson et al., 2014).

Together, these methods form a privacy-preserving, post-quantum cryptographic stack aligned with ethical and practical demands of future-proof authentication systems.

Distributed attestation layer

The WPI relies on a multi-layer distributed ledger—not necessarily blockchain per se, but a verifiable credential layer using decentralized identifiers (DIDs) and verifiable credentials (VCs) standardized by the W3C (Sporny et al.,

2025). Each WPI instance generates a unique key pair bound to a verified proof-of-humanity process.

Formally:

$$\sigma_H = Sign(K_{priv}, H_{meta})$$

$$Verify(K_{pub}, \sigma_H) = True$$

This ensures anonymity while proving human authorship.

Linking Digital Entities to Real Administrators

All digital entities must be anchored to at least one verified WPI token. Institutional WPI tokens (IWPI) can be issued to organizations, linked to natural persons' WPIs serving as custodians. This hierarchy establishes accountability while preserving privacy.

EXPANDED TECHNICAL ARCHITECTURE AND OPERATIONAL PSEUDOCODE

This section explains, in accessible terms, how the WPI is intended to function conceptually. The aim is to provide sufficient operational detail so that platform operators, auditors, policy-makers, and educators can understand the basic guarantees, failure modes, and governance implications without requiring specialized expertise in cryptography. The narrative clarifies the main actors, the minimal public artifacts the system records, and the processes by which a human-verified identifier is issued, presented to a platform, bound to an account, and revoked if needed. After the conceptual explanation, an academic pseudocode block illustrates the operational flow for reviewers and implementers. This pseudocode is illustrative and not intended as production code.

Functional components (high-level overview)

- *National Register/ Issuer:* Accredited authority (civil registry, health authority, or other) that verifies legal existence and issues a signed verifiable credential (VC) linking a person to a WPI namespace entry.
- *Holder Wallet:* Secure client (mobile app or hardware wallet) controlled by the person, storing the VC and generating short-lived presentation tokens.
- *Platform (Relying Party):* Online service (social network, educational portal, marketplace) that accepts presentation tokens to bind a public account to a WPI.

- *Permissioned Audit Ledger:* Consortium-run ledger recording minimal proofs (hashes, signatures, timestamps, binding proofs) for audit without exposing personal attributes.
- *Revocation Service / CRL*: Issuer-operated mechanism enabling revocation or suspension of WPIs and presentation tokens through standardized channels.

These components jointly maintain a separation of concerns: issuers attest identity, holders control disclosure, platforms verify and bind, and the ledger supports accountability while minimizing data exposure.

Data structures (Conceptual Explanation)

Before the pseudocode, the following conceptual data structures clarify what each element contains and why it is needed:

- **WPI_Record:** Issuer-side entry linking a WPI identifier to a proof pointer and managing status.
    - ✧ Fields: `wpi_id, issuer_id, vc_signature, public_proof_hash, status, metadata.`

- **VerifiableCredential (VC):** Credential issued to the holder.
    - ✧ Fields: `holder_pubkey, issuer_signature, claims, issuance_date, expiry_date.`

- **PresentationToken:** Short-lived token generated by the holder to prove possession of a VC without revealing sensitive attributes.
    - ✧ Fields: `proof_payload (ZKP or signed VC reference), nonce, expiry, disclosed_claims.`

These structures ensure that only minimal, non-identifying data appear on the shared ledger while enabling verifiable bindings between holders and platforms.

Operational pseudocode (Academic Illustration)

Note: The following pseudocode is academic and conceptual. It is intended to illustrate preconditions, expected side effects and the high-level control flow. It is not production code.

```
DATA STRUCTURES
---------------
WPI_Record:
  - wpi_id
  - issuer_id
```

```
      - vc_signature
      - public_proof_hash
      - status (active|revoked|suspended)
      - metadata (consent_flags)

    VerifiableCredential (VC):
      - holder_pubkey
      - issuer_signature
      - claims (existence attestation)
      - issuance_date
      - expiry_date

    PresentationToken:
      - proof_payload (ZKP or holder-signed VC reference)
      - nonce
      - expiry
      - disclosed_claims (optional)

    FUNCTIONS
    ---------

    EnrollAndIssueWPI(national_record):
      assert VerifyNationalRecord(national_record)
      wpi_id := GenerateWPIID(national_record)
      vc := CreateVC(holder_pubkey = national_record.pubkey,
claims = {existence:true})
      vc.issuer_signature := IssuerSign(vc)
      wpi_record := WPI_Record(wpi_id, issuer_id,
vc.issuer_signature, public_proof_hash = Hash(vc), status =
"active")
      StoreNationalIndex(wpi_record)
      PublishLedgerProof(public_proof_hash, vc.issuer_signature)
      return vc, wpi_record

    GeneratePresentationToken(vc, disclosure_policy,
platform_nonce):
      if disclosure_policy.requires_zkp:
        π := GenerateZKP(vc.claims, disclosure_policy; scheme =
BBS+)
        token_payload := {π, platform_nonce, expiry = Now +
short_ttl}
      else:
        token_payload := {vc.issuer_signature, platform_nonce,
expiry = Now + short_ttl}
      token := HolderSign(token_payload)
      return token
```

```
    PlatformVerifyAndBind(token, platform_account_id):
      if not VerifyHolderSignature(token): reject
      if token.expiry < Now: reject
      if not VerifyIssuerSignature(ResolveIssuer(token)): reject
      if CheckRevocation(ResolveIssuer(token)) == true: reject
      binding_hash := Hash(token || platform_account_id ||
timestamp)
      platform_signature := PlatformSign(binding_hash)
      WriteAuditLedger(binding_hash, platform_signature,
minimal_metadata)
      return Success

    RevokeWPI(wpi_id, reason):
      UpdateNationalIndexStatus(wpi_id, "revoked", reason)
      PublishRevocation(wpi_id, timestamp, issuer_signature)
      NotifyBoundPlatforms(wpi_id)
      return True
```

Implementation and policy notes (Concise)

- *Cryptographic primitives*: adopt NIST-recommended post-quantum algorithms for signature and KEM; use standardized ZKP schemes for selective disclosure.
- *Ledger design*: prefer consortium permissioned ledgers (Merkle-based logs) that record only non-identifying proofs.
- *Token lifecycle*: presentation tokens should be short-lived and include platform nonces to prevent replay attacks.
- *Revocation & dispute*: issuers must operate timely revocation channels; platforms must check revocation status before binding.
- *Transparency & audit*: publish verification APIs, algorithm choices, and audit reports; permit accredited auditors to review under strict privacy constraints.

Pedagogical and governance linkage

Including this level of operational detail serves two audiences. For educators and STEAM curricula designers, it creates concrete artifacts that can be translated into classroom projects (simulating enrolment flows, auditing ledger entries, and role-playing governance decisions). For policy-makers and platform managers, it clarifies the obligations and failure modes that regulation must address (issuer accreditation, revocation timeliness, platform liability, and environmental accounting).

ETHICAL AND GOVERNANCE CONSIDERATIONS

While technical security is fundamental, governance mechanisms are equally crucial. The WPI's cryptographic layer must be accompanied by:

- *Consent-based participation*: Individuals must explicitly opt in to obtain a WPI; no automatic or coercive enrollment.
- *Transparent revocation*: WPI tokens can be revoked or suspended under clear procedural standards.
- *Global interoperability*: National authorities can issue or co-sign WPIs, but the verification framework must remain globally consistent.
- *Public auditability:* Verification logic should remain open-source and auditable to preserve public trust.

The combination of technical transparency and ethical governance ensures that the WPI remains a trust-building infrastructure, not an instrument of surveillance or exclusion.

PRESENCE AS AN INTANGIBLE VALUE: NORMATIVE FRAMING

Contemporary digital economies extract large rents from user activity and personal data, redistributing value away from individuals (Zuboff, 2019; O'Reilly et al., 2024). The WPI reframes this dynamic by recognizing presence—the verified fact of human participation—as a potential enabling condition for more equitable value flows. Presence is not proposed as a commodity or currency, but as a consented, auditable signal that can support applications such as:

- Verified participation credits in research or civic platforms.
- Transparent attestations for commercial or educational use.
- Consent-based mechanisms for redistributing digital value.

Any such applications must remain optional, traceable, and revocable, ensuring that presence is never coerced or commodified.

Equity, Sustainability, and Global South Inclusion

Normative governance of presence-based applications should incorporate:

1. *Equity and redistribution*: Ensuring that benefits flow back to individuals and community funds, particularly in under-resourced regions.
2. *Environmental accountability*: Allocating part of monetization proceeds to offset ecological costs and invest in low-energy verification methods.

3. *Protection against coercion:* Defaults such as non-transferability for vulnerable groups, mandatory transparency, and auditable stewardship. (see 7.4), creating incentives for more sustainable digital practices.

Properly regulated, presence-based mechanisms can complement existing digital economies by enabling traceable, consented value flows that support inclusion and sustainability, especially in Global South contexts.

EDUCATIONAL IMPLICATIONS: MITIGATING DISINFORMATION, EPISTEMIC LITERACY, AND STEAM INTEGRATION

Reframing Misinformation as an Operational Variable

Building on the indexed definition advanced by Roman Soltero & Ibarra Ladrón de Guevara (2024), which has been cited in subsequent scholarly work, virtual disinformation can be operationalized as the discrepancy between an agent's belief that they possess truthful information and the actual veracity of that information. This framing emphasizes both subjective epistemic state (belief) and objective truth (veracity), enabling empirical study of educational interventions.

The WPI contributes to reducing this discrepancy by improving provenance signals: when content is cryptographically bound to a human-verified WPI token (or to an institutional WPI), recipients gain metadata that probabilistically increases trustworthiness. This added signal reduces cognitive burden and enables educators to design curricula that incorporate provenance verification into information evaluation.

Curriculum Design: Epistemic Literacy Through Practice

Integrating WPI into STEAM education involves three interlocking elements:

- *Technical literacy*: Students learn the basics of identity verification (DID/VC concepts), cryptographic proofs, and privacy-preserving disclosure (ZKPs).
- *Epistemic training*: Scaffolded activities teach students to evaluate claims, weigh provenance evidence, assess credibility, and reflect on cognitive biases.
- *Civic practice*: Community projects simulate WPI enrollment and governance, blending technical skill-building with participatory learning.

These modules can be adapted by age and context: younger learners may practice simple provenance-checking exercises, while advanced students engage in labs on ZKP design and auditing.

Measuring Impact: Metrics and Assessment

Future research should empirically assess educational outcomes. Potential indicators include:

- Reduction in perceived-truth gap (pre/post interventions using the Roman-Ibarra metric).
- Increased use of provenance signals in student sourcing.
- Improved critical reasoning scores.
- Community uptake metrics in pilot studies.

Combining quantitative assessment with qualitative ethnographic evaluation ensures a contextualized understanding of how WPI adoption affects trust and learning practices, especially in culturally diverse Global South settings.

Educator Capacity and Teacher Training

Scaling WPI-informed curricula requires investment in teacher professional development: workshops on digital provenance, labs on cryptographic concepts, and modules on facilitating community deliberation. UNESCO (2019) and similar agencies' materials on media and information literacy provide useful scaffolds that can be adapted to WPI contexts.

TECHNICAL AND CONCEPTUAL CLOSURE: SOCIAL, ETHICAL, AND SUSTAINABILITY IMPLICATIONS

Summary Synthesis

The WPI proposal addresses a convergent crisis: epistemic collapse (loss of trust), ecological strain (energy and resource costs), and economic asymmetry (concentration of data rents). Technically, it combines post-quantum cryptography, selective disclosure (ZKPs), decentralized identifiers (DIDs), and verifiable credentials (VCs) into an interoperable framework that anchors digital presence to human-verified proof while preserving privacy. Educationally, it supports epistemic literacy and participatory STEAM learning. Governance models emphasize neutrality, multi-stakeholder representation (with meaningful Global South leadership), and legal safeguards to prevent coercion or commodification.

Key Ethical Trade-Offs and Mitigations

- *Privacy vs. Accountability:* Minimal public proofs and selective disclosure guard privacy; binding proofs on permissioned ledgers maintain

accountability without exposing personal data. Legal protections are necessary where states seek compelled disclosure.

- *Commodification vs. Redistribution:* Presence-based applications risk commodification; mitigations include vulnerable-group protections and stewardship funds that redistribute value.
- *Global adoption vs. sovereign diversity:* A neutral WPI standard must remain interoperable with national variations and culturally appropriate, requiring regional councils and local opt-ins.

Sustainability and the Prevention of the "Infinite Bot" Trap

By making human provenance verifiable and economically meaningful, the WPI changes incentives. Bot operators face higher costs to achieve credible human provenance, and platforms gain tools to penalize non-verified propagation. Combined with environmental accounting, these mechanisms reduce the economic case for infinite bot expansion and reorient resources toward socially productive digital uses.

Research and Policy Agenda: Potential Next Steps

Future work could explore:

1. *Prototype studies:* Minimal WPI stacks for testing VC issuance, holder wallets, and presentation tokens.
2. *Simulation experiments.* Agent-based models to quantify behavioral changes in bot reach and misinformation diffusion.
3. *Pilot projects*: Municipal or educational pilots in Global South contexts, integrating STEAM curricula for local capacity building.
4. *Governance frameworks*: Multi-stakeholder working groups to design namespace governance and stewardship rules.
5. *Environmental audits*: Measurement standards for the energy footprint of identity verification services and commitments to sustainability investments.

AI ACKNOWLEDGMENT

AI Acknowledgment: The author used generative AI tools (e.g., Consensus, ChatGPT, Copilot) to support the brainstorming, drafting, and language refinement stages. All academic content, citations, and interpretations were created and verified by the author.

REFERENCES

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Biswas, R., Boixo, S., Brandao, F. G. S. L., Buell, D. A., Burkett, B., Chen, Y., Chen, Z., Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Foxen, B., & Fowler, A. (2019). Quantum supremacy using a programmable superconducting processor. *Nature, 574*(7779), 505–510. https://doi.org/10.1038/s41586-019-1666-5

Assenmacher, D., Clever, L., Frischlich, L., Quandt, T., Trautmann, H., & Grimme, C. (2020). Demystifying Social Bots: On the Intelligence of Automated Social Media Actors. *Social Media + Society, 6*(3). https://doi.org/10.1177/2056305120939264

Bacaro, G. (2026, February 24). *Account for AI in the environmental footprint of scientific publishing*. Nature. https://www.nature.com/articles/d41586-026-00590-0

Baig, A. F., Eskeland, S., & Yang, B. (2023). Privacy-preserving continuous authentication using behavioral biometrics. *International Journal of Information Security, 22*, 1833–1847. https://doi.org/10.1007/s10207-023-00721-y

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. IEEE Symposium on Security and Privacy, 35th, 459–474. https://doi.org/10.1109/sp.2014.36

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-Quantum Cryptography*. Springer. https://doi.org/10.1007/978-3-540-88702-7

Bruno, M., Lambiotte, R., & Saracco, F. (2022). Brexit and bots: Characterizing the behaviour of automated accounts on Twitter during the UK election. *EPJ Data Science, 11*(1), 17. https://doi.org/10.1140/epjds/s13688-022-00330-0

Calzada, I. (2025). Decentralizing AI economics for poverty alleviation: Web3 social innovation systems in the global south. *AI, 6*(12). https://doi.org/10.3390/ai6120309

Chator, A., Green, M., & Tiwari, P. (2025). SoK: Privacy-preserving signatures. *IACR Communications in Cryptology, 2*(1). https://doi.org/10.62056/a3wa3z10k

Chauhan, N., Pal, V., Singh, S., Srivastava, S., & Singh, S. K. (2025). Revolutionizing digital content authentication: the power of synthetic media detection. *International Journal of Scientific Research in Engineering and Management (IJSREM), 09*(05), 1–9. https://doi.org/10.55041/ijsrem46858

Clark, T. (2025). Fighting climate disinformation in the age of AI. *ITNOW, 67*(4), 44–45. https://doi.org/10.1093/itnow/bwaf130

Cooke, D., Edwards, A., Barkoff, S., & Kelly, K. (2024, April 4). As good as a coin toss: Human detection of AI-generated images, videos, audio, and audiovisual stimuli. *ArXiv.org.* https://doi.org/10.48550/arXiv.2403.16760

Diaz Rivera, J. J., Muhammad, A., & Song, W.-C. (2024). Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication. *IEEE Open Journal of the Communications Society, 5*, 2792–2814. https://doi.org/10.1109/ojcoms.2024.3391728

Gao, S., Su, Q., Zhang, R., Zhu, J., Sui, Z., & Wang, J. (2021). A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain. *Security and Communication Networks, 2021.* https://doi.org/10.1155/2021/9992353

Ghiurău, D., & Popescu, D. E. (2025). Distinguishing reality from AI: Approaches for detecting synthetic content. *Computers, 14*(1), 1–1. https://doi.org/10.3390/computers14010001

Gowda, V. D., Suneel, S., Rahman, M., Das, G. C., Kumar, R. S., & Prasad, V. (2024). Securing digital authentication with cryptographic innovations in intrinsic verification systems. *Journal of Discrete Mathematical Sciences and Cryptography, 27*(2-A), 317–328. https://doi.org/10.47974/jdmsc-1885

Mandelbaum, R., & Chow, J. (2026, January 28). *A glimpse at computing's quantum-centric future.* IBM. https://research.ibm.com/blog/accelerating-qpus-with-gpus

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2025). A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials, 27*(6), 1–1. https://doi.org/10.1109/comst.2025.3543197

Nizzoli, L., Tardelli, S., Avvenuti, M., Cresci, S., Tesconi, M., & Ferrara, E. (2020). Charting the landscape of online cryptocurrency manipulation. *IEEE Access, 8*, 113230–113245. https://doi.org/10.1109/ACCESS.2020.3003370

O'Reilly, T., Strauss, I., & Mazzucato, M. (2024). Algorithmic attention rents: A theory of digital platform market power. *Data & Policy, 6*(e6). https://doi.org/10.1017/dap.2024.1

Roman Soltero, A. R., & Ibarra Ladrón de Guevara, I. E. (2024). Medición del aprendizaje y desinformación sobre inteligencia artificial en estudiantes universitarios a través de un modelo estadístico en el contexto de la sociedad del conocimiento. *Quántica. Ciencia Con Impacto Social, 4(*2), 82–101. https://doi.org/10.56747/rcq.v4i2.84

Satybaldy, A., Subedi, A., & Nowostawski, M. (2022). A Framework for online document verification using self-sovereign identity technology. *Sensors, 22*(21), 8408. https://doi.org/10.3390/s22218408

Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th *Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE Computer Society. https://doi.org/10.1109/sfcs.1994.365700

Song, Z., Yan, E., Song, J., Jiang, R., Yu, Y., & Chen, T. (2025). A Blockchain-based digital identity system with privacy, controllability, and auditability. *Arabian Journal for Science and Engineering, 50*, 7027–7051. https://doi.org/10.1007/s13369-024-09178-0

Sporny, M., Longley, D., Burnett, D. C., Zundell, B., & Hartog, K. D. (2025). Verifiable Credentials Data Model v2.0. In M. Sporny, T. Thibodeau Jr., I. Herman, G. Cohen, & M. B. Jones (Eds.), *W3C. World Wide Web Consortium (W3C)*. https://www.w3.org/TR/vc-data-model/

UNESCO. (2019). Media and information literacy. UNESCO. https://en.unesco.org/themes/media-and-information-literacy

Velmurugan, M., Shinzeer, K., Maya, G., Ramya, R., Kanimozhi, R., & Syed Ismail, A. L. (2025). A Hybrid Blockchain Framework for Secure, Scalable, and Energy-Efficient Digital Identity Management with Token-based Selective Disclosure. *2025 International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 930–937). https://doi.org/10.1109/ICEARS64219.2025.10940179

Wang, Y., Hao, Y., & Cong, A. X. (2024, January 14). Harnessing machine learning for discerning AI-generated synthetic images. *ArXiv.org.* https://doi.org/10.48550/arXiv.2401.07358

Zhang, T., Wang, Y., Gong, B., Xu, J., Wu, J., & Wan, C. (2025). Privacy protection during the issuance and revocation of verifiable credentials in self‐sovereign identity. *Concurrency and Computation: Practice and Experience, 37*(9–11). https://doi.org/10.1002/cpe.70084

Zhuk, A. (2025). Artificial Intelligence Impact on the Environment: Hidden Ecological Costs and Ethical-Legal Issues. *Journal of Digital Technologies and Law, 1*(4), 933–954. https://doi.org/10.21202/jdtl.2023.40

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* (1st ed., 704 pages). Public Affairs.

Bio

ALBERTO RAFAEL ROMAN SOLTERO, BEng, MSc, DrPH, is a Professor-Researcher at Vizcaya University of Americas, where he works within a multidisciplinary profile integrating Data Science, Mathematics, Psychology, Pedagogy, and theoretical approaches related to Physics and Astronomy. He is also a scientific researcher and science communicator at edemi, a Mexican

multidisciplinary research collective and innovation center, where his work focuses on neurodiversity, neurodevelopmental conditions, inclusive health, and applied assistive technologies. Email: *rafaroman@edemi.mx*