frontiers | Frontiers in Blockchain

TYPE Mini Review
PUBLISHED 30 October 2025
DOI 10.3389/fbloc.2025.1682474

OPEN ACCESS

EDITED BY
Akhilesh Thyagaturu,
Arizona State University, United States

REVIEWED BY
Musawer Hakimi,
Osmania University, India

*CORRESPONDENCE
Leonardo Juan Ramírez López,
ljramirezl@unbosque.edu.co

RECEIVED 08 August 2025
ACCEPTED 20 October 2025
PUBLISHED 30 October 2025

CITATION
Ramírez López LJ, Parra Chavarro DA and Hernandez Huertas YA (2025) Digital citizenship: Challenges and uncertainty in applying blockchain.
Front. Blockchain 8:1682474.
doi: 10.3389/fbloc.2025.1682474

Digital citizenship: Challenges and uncertainty in applying blockchain

Leonardo Juan Ramírez López*,
Danniel Alejandro Parra Chavarro and
Yeison Andres Hernandez Huertas

OSIRIS & BIOAXIS research group, Universidad El Bosque, Bogotá, Colombia

Digital citizenship in Colombia is a strategic priority to modernize public services through secure, transparent, and citizen-centered interactions. The national model combines Digital Authentication, the Digital Citizen Folder, a Digital Wallet, and Digital Signature under the regulatory framework led by the Ministry of ICT. Yet adoption has been limited by mistrust, especially concerns about information security, identity theft, and limited control over personal data. This article is a narrative Mini-review that offers a curated synthesis of recent literature on blockchain for digital identity, authentication, and citizen data management, drawing on representative studies indexed in Scopus, ScienceDirect, and Google Scholar. Prior work suggests that distributed ledgers can enhance immutability, auditability, and data sovereignty, and that Self-Sovereign Identity (SSI) with verifiable credentials and decentralized identifiers can enable selective disclosure and stronger user control. However, persistent challenges include scalability and cost, governance and interoperability with legacy systems, and regulatory alignment, which temper expectations. Taken together, the literature indicates that blockchain can be a viable complement to Colombia's digital government ecosystem when implemented through permissioned or hybrid designs, aligned with open standards and embedded in robust legal and institutional frameworks. Under these conditions, blockchain-based approaches may help rebuild trust and foster broader adoption of citizen-oriented digital services.

KEYWORDS

digital citizenship, blockchain, public services, digital identity, digital government, security

1 Introduction

Colombia's digital transformation strategy emphasizes digital identity, interoperability, and online citizen services. Accordingly, the Ministry of Information and Communications Technologies (MinTIC) defines digital citizenship as the outcome of citizens' digital and productive evolution, highlighting blockchain's capacity to ensure traceability and immutability of personal data. However, as of 29 December 2022, only 1,101,133 digital ID cards were issued, revealing obstacles such as fragmented authentication mechanisms, non-intuitive user interfaces, and distrust regarding data security (Misión de Observación Electoral, 2023).

By comparison, Chile's ClaveÚnica platform supports over 14.4 million users and 1,730 procedures, while Uruguay's national digital ID provides a standardized

authentication framework. Moreover, adoption models like TAM and UTAUT demonstrate that perceived security, ease of use, and digital literacy critically influence citizens' intentions to engage with online government services. In Colombia, significant segments of the population report inadequate training for digital procedures, underscoring gaps in digital skills (Gobierno de UruguayAGESIC, 2023; Gobierno de ChileMinisterio Secretaría General de la Presidencia, 2022).

Internationally, systems such as the European Digital Identity (EUDI) Wallet, India's Aadhaar, and Estonia's X-Road illustrate large-scale digital identity infrastructures (not necessarily blockchain). In parallel, blockchain-based, SSI-oriented pilots explore verifiable credentials, decentralized identifiers, and selective disclosure to enhance security, portability, and user control in specific contexts. A synthesis of 103 digital government studies (2003–2020) reports failure rates of approximately 60%–85%, often due to gaps between architectural design and implementation (Baheer et al., 2020). Accordingly, assessing Colombia's progress should triangulate scientific evidence, international best practices, and local user considerations; regional experiences such as Uruguay's national digital ID illustrate feasibility at scale (Gobierno de UruguayAGESIC, 2023).

1.1 Legal framework

Colombia bases its digital citizenship model on a solid legal framework. First, Law 527 of 1999 recognized the validity of electronic communications and signatures, thereby establishing the principles of integrity and non-repudiation in digital environments (Congreso de Colombia, 1999). Next, Law 962 of 2005 and Decree 2364 of 2012 granted qualified electronic signatures full legal equivalence to handwritten signatures, while defining cryptographic security requirements and their evidentiary value (Congreso de Colombia, 2005; Presidencia de la República de Colombia, 2012). Subsequently, Decree 1078 of 2015 unified all ICT regulations in a single compendium, setting common standards for digital identity, electronic signatures, and online public services (Presidencia de la República de Colombia, 2015). More recently, Decree 767 of 2022 formally introduced the concept of the digital citizen and articulated the principles of interoperability, security, privacy, and data sovereignty that govern Digital Authentication, the Digital Citizen Folder, the Digital Wallet, and the Digital Signature (Presidencia de la República de Colombia, 2022).

To operationalize these services, Decree 620 of 2020 laid down detailed technical guidelines for security, encryption, and identity management, guaranteeing access control and transaction traceability for Digital Authentication and the Citizen Folder (Presidencia de la República de Colombia, 2022). Moreover, Resolution 2160 of 2020 specified interoperability standards for the Citizen Folder, while Resolution 1254 of 2021 established assurance levels and risk management criteria for strong online user authentication (MinTIC, 2020; MinTIC, 2025). Taken together, this comprehensive set of regulations safeguards integrity, confidentiality, informed consent, and auditability, thereby strengthening citizen trust and fostering the widespread adoption of digital citizenship in Colombia.

1.2 Digital citizenship

Considering the previously presented definition by the Ministry of Information and Communications Technologies (MinTIC), first, it justifies the concept of digital citizenship as the result of citizens' digital and productive transformation in response to the challenges of the digital economy, with the ultimate goal of accelerating that transformation in the coming years (MinTIC, 2025). Moreover, this vision is explicitly framed by the National Policy on Digital Citizen Services (Decree 767 of 2022), whose primary objective is to establish an effective digital identity architecture as the fundamental infrastructure that enables secure interaction between the State and its citizens (Presidencia de la República de Colombia, 2022).

Unlike broader, more theoretical definitions, the MinTIC proposal explicitly links digital citizenship to tangible service transformation processes: it integrates Digital Authentication, the Digital Wallet, the Digital Citizen Folder, and the Digital Signature as interconnected mechanisms that foster a more secure, transparent, and citizen-controlled experience (Barrios Tao and Díaz Pérez, 2025; Ministerio de Tecnologías de la Información y las Comunicaciones, 2025a). In particular, it underscores the productive and technological empowerment of citizens. To that end, incorporating blockchain into this ecosystem emerges as a strategic way to overcome current challenges of interoperability and public trust. Indeed, the transparency, decentralization, and tamper-resistance that blockchain offers reinforce the Ministry's principles of data sovereignty and personal data control. Consequently, citizens could retain full control over their digital credentials, while enjoying secure validation by both public and private actors (Barrios Tao and Díaz Pérez, 2025).

Historically, the notion of digital citizenship has evolved alongside Information and Communication Technologies (ICT), shifting from traditional physical credentials to digital certificates and biometric authentication (Barrios Tao and Díaz Pérez, 2025; MinTIC, 2023b). This shift responds to rising demands for security, globalization, and service digitalization, which collectively imposes the need for new identity models. Therefore, recognizing the digital citizen entails not only proactive participation in these digital spheres but also the cultivation of digital skills and the exercise of rights within a secure online environment, all in alignment with the current regulatory framework.

1.3 Blockchain

Blockchain technology consists of a distributed database in which transactions are recorded in blocks linked by cryptographic techniques. Specifically, it offers record immutability, decentralized information storage, and end-to-end transaction traceability (Ministerio de Tecnologías de la Información y las Comunicaciones, 2023a; Cagigas et al., 2021). Consequently, networks based on distributed trust can complement and, in some cases, replace traditional centralized systems, thereby reducing risks of fraudulent tampering and single-point failures. In the public sector, recent reviews show that blockchain can boost operational efficiency, auditability, and inter-agency coordination; however, significant challenges persist around technical scalability

and network governance models (Cagigas et al., 2021; Pauletto, 2021).

Moreover, combining blockchain with the Self-Sovereign Identity (SSI) model enables users to control their personal credentials directly, without relying on a single central authority. Thus, each citizen decides what information to share and with whom (Stockburger et al., 2021; Wang and De Filippi, 2020; Guggenberger et al., 2023). For instance, Estonia's X-Road (a non-blockchain data exchange layer) illustrates secure, large-scale digital public services; in parallel, blockchain-based, SSI-oriented pilots have been explored in other contexts. Additionally, several studies document SSI pilots in domains such as European public transport and commercial KYC processes, where credentials are automatically validated via smart contracts (Stockburger et al., 2021; Guggenberger et al., 2023; Lan and Jiang, 2024).

In Colombia, the State Blockchain Reference Guide identifies the technology as a strategic resource for ensuring transparency, traceability, and data integrity, specifically recommending permissioned blockchains to balance openness with the protection of sensitive data (Ministerio de Tecnologías de la Información y las Comunicaciones, 2023a; MinTIC, 2023c). Furthermore, national policy stresses that blockchain adoption must be accompanied by clear interoperability standards and a supportive legal framework, particularly Law 1581 on personal data protection and the digital verification mechanisms introduced by Decree 767 of 2022 (Congreso de Colombia, 2005; Presidencia de la República de Colombia, 2022). Despite the early stage of Colombian blockchain initiatives, the existing regulatory environment already offers concrete opportunities to prototype digital authentication services, citizen wallets, and digital portfolios, thereby positioning blockchain as a central enabler of the country's digital citizenship ecosystem.

2 Background and thematic focus

2.1 Focus on blockchain

Over recent decades, digital identity has evolved from password-based systems and security questions to advanced solutions that use biometrics and encryption (Robles Carrillo, 2024). This shift occurs because the rapid expansion of electronic commerce and the digitalization of public services defmand stronger security safeguards (Pauletto, 2021).

Established models such as eIDAS in the European Union and Aadhaar in India already demonstrate that large-scale digital systems can provide secure access to governmental and financial procedures (Pauletto, 2021). However, both still depend on centralized infrastructures that create single-point failures, making them susceptible to cyberattacks and to conflicts with personal data protection regulations (Karasek and Wojciechowicz, 2021; Anand and Brass, 2021).

In Colombia, initiatives such as the Digital Identity Card and Digital Citizen Services aim to improve identification efficiency and reduce fraud, yet they face two major limitations:

- First, limited interoperability between state and private platforms complicates cross-validation of identities (Karasek and Wojciechowicz, 2021).
- Second, continued reliance on centralized servers heightens vulnerability to fraud and identity theft (Anand and Brass, 2021).

Consequently, these shortcomings have encouraged exploration of alternative technologies, notably blockchain, which offers a more secure and decentralized approach to digital identity management (Schlatt et al., 2022).

Blockchain is a technology that stores information in distributed, immutable ledgers managed by multiple independent nodes, thereby reducing the risk of a single-point failure (Pinto et al., 2022). Moreover, its key properties are immutability, which prevents unauthorized alteration of stored data (Pinto et al., 2022); decentralization, which distributes custody of information among independent nodes and reduces failure risk; and traceability, which enables complete and secure audits of every recorded operation (Secinaro et al., 2021). Consequently, these features have been shown to significantly reduce fraud and operational costs in processes such as Know Your Customer (KYC) (Schlatt et al., 2022).

2.1.1 About self-sovereign identity (SSI)

The blockchain-based SSI model enables users to control their digital credentials directly, without intermediaries, and to decide what information to share and with whom (Hünseler and Pöll, 2023). Specifically, its advantages are twofold: selective privacy, where the user reveals only the attributes required for each transaction, thereby preserving privacy (Hünseler and Pöll, 2023); and portability, where a single credential can serve multiple domains, including government, finance, and healthcare, so repetitive registration is no longer necessary (Schlatt et al., 2022). Blockchain has been piloted and applied across multiple domains:

- Government: Estonia's X-Road (a non-blockchain data-exchange layer) demonstrates secure, large-scale digital public services; in parallel, blockchain-based SSI pilots have been explored in specific contexts (Secinaro et al., 2021).
- Financial sector: Smart-contract-supported KYC has been reported to streamline verification and reduce fraud in specific deployments (Schlatt et al., 2022).
- Healthcare: Pilot projects explore privacy-preserving access to medical records and border-control scenarios (Xu, 2023).

These examples illustrate the potential of blockchain to enhance security and transparency in digital identity management, while real-world adoption remains contingent on governance, interoperability, and cost.

- Challenges: Despite these advantages, several hurdles remain.
- Scalability. Public blockchains tend to slow down and become costly when transaction volumes surge (Mishra et al., 2022).
- Regulation. A clear, harmonized legal framework for blockchain and digital identity is still lacking (Anand and Brass, 2021).
- Interoperability. Integrating blockchain networks with legacy platforms and databases is complex (Karasek and Wojciechowicz, 2021).

For instance, blockchain's inherent immutability can clash with regulations such as the European Union's "right to be forgotten"

under the General Data Protection Regulation (Anand and Brass, 2021).

In Colombia, blockchain deployment remains at an early stage; nevertheless, experts recommend hybrid or permissioned models governed jointly by public bodies, private firms, and academia (Schlatt et al., 2022). Domestic pilots exploring decentralized KYC and SSI solutions already signal growing interest within Colombia (Schlatt et al., 2022; Pava Díaz et al., 2023).

2.2 Focus on digital citizenship and citizen identity

The evolution of digital government infrastructures continues to show persistent gaps between theory and practice. For instance, Baheer et al. reviewed 103 studies published from 2003 to 2020 and found little consensus on architectural concepts; as a result, between 60 percent and 85 percent of digital government projects fail because of shortcomings in planning and ICT infrastructure (Baheer et al., 2020). In the identity domain, Hilowle et al. surveyed 203 Australian users under the theory of planned behavior and revealed that limited security trust and low cybersecurity awareness are critical barriers to mass adoption of digital identity systems (Hilowle et al., 2024). Meanwhile, Ruiu et al. assessed the use of biometric data in eIDAS and emphasized the need for robust regulatory frameworks, namely GDPR and eIDAS itself, plus cross-national interoperability to safeguard fundamental rights (Ruiu et al., 2024). Locally, López Solano and Castañeda documented collaboration between the National Civil Registry and IDEMIA, noting innovations such as the electronic identity card and digital wallets, yet warning about risks of technological dependency and disputes over data sovereignty (López Solano and Castañeda, 2024). Taken together, these studies underscore the importance of approaches that integrate technological, human, and regulatory factors, illustrating how public-private partnerships can inform blockchain-based digital citizenship design in Colombia (Stockburger et al., 2021; Semenzin et al., 2022).

Recently, scholarship has shifted toward Self-Sovereign Identity (SSI) and blockchain solutions. For example, Stockburger et al. showed with a European public-transport prototype that SSI improves interoperability among operators, replacing multiple cards and enhancing security and transparency (Stockburger et al., 2021). Moreover, Cagigas et al. observed that although 61.2 percent of blockchain publications in 2019 focused on cryptocurrencies, later work highlights public-service applications that deliver efficiency, traceability, and better inter-institutional coordination, even though scalability and regulatory uncertainty remain challenging (Cagigas et al., 2021). Similarly, Wang and De Filippi demonstrated that SSI reduces exposure of sensitive data through selective credential disclosure, thereby advancing economic inclusion in projects such as Kiva in Sierra Leone and Building Blocks in Jordan (Wang and De Filippi, 2020). In addition, Semenzin et al. analyzed the Estonian experience, noting tensions between public and permissioned blockchains and stressing the need for strong legal foundations (Semenzin et al., 2022). At the European level, Guggenberger et al. reported that only half of EU member states use compliant eIDs; they estimated a pan-European SSI system would cost more than 600 million euros and proposed design principles to enhance scalability, interoperability, and privacy (Guggenberger et al., 2023).

From a technical standpoint, Lan and Jiang presented a blockchain algorithm that cut computational cost by 55.5 percent and raised the security index from 12.5 to 22 (Lan and Jiang, 2024), whereas Abu Bakar et al. introduced the "digital pheromone," achieving 100 percent uniqueness for smartphone user identities (Abu Bakar et al., 2024). Cases beyond Europe, such as Aadhaar in India, show gains in inclusion and service access (Mira et al., 2020) but also highlight privacy and social-exclusion risks (Addo and Senyo, 2021). Latin American experiences, notably Uruguay's Digital ID, confirm the feasibility of unique credentials at national scale (Gobierno de UruguayAGESIC, 2023). Methodologies employed range from perception surveys (Tan et al., 2023) and structural-equation models of adoption (Addo, 2022) to blockchain simulations of efficiency and security (Zulkifli and Abidin, 2025). Looking ahead, prospective SSI systems for Colombia must secure citizen autonomy (Xin et al., 2022), comply with both local and international regulations (He, 2022), ensure interoperability across public and private entities, and foster digital inclusion that avoids marginalizing vulnerable groups (Robles Carrillo, 2024).

3 Discussion

International experiences in digital identity point to convergent design principles: minimal data on-chain, robust revocation, and standardized verifiability. These principles are transferable to Colombia because they are consistent with the country's legal and policy frameworks on digital identity and public services. Reference implementations and policy trajectories in the European Digital Identity initiative and regional programs illustrate feasibility at scale (Table 1), while the high failure rates documented in digital government projects underscore the need to close the design–implementation gap through governance and evaluation (Baheer et al., 2020; European Commission, 2025; Gobierno de UruguayAGESIC, 2023).

Reconciling blockchain immutability with rights to erasure and correction requires a minimal-on-chain architecture aligned with Colombian regulation. Personally identifiable information should remain off-chain in institutional repositories or user wallets, with the ledger storing only non-invertible references such as salted hashes, credential identifiers, and content-addressable pointers. Lifecycle controls should prioritize revocation lists or status registries over block editing; selective disclosure and privacy-preserving proofs can limit data exposure and correlation risks. These safeguards are coherent with data-protection and sectoral requirements and can be operationalized within permissioned or hybrid networks under clearly assigned controller and processor roles and auditable processes (He, 2022; Karasek and Wojciechowicz, 2021; Presidencia de la República de Colombia, 2012; Presidencia de la República de Colombia, 2015; MinTIC, 2020).

On the scale, self-sovereign identity (SSI) introduces organizational, and human-factors risks. Evidence highlights consumer concerns and adoption frictions, the importance of responsible innovation governance, and the role of human-centered cybersecurity practices for national ID systems. In

TABLE 1 Integration of blockchain in citizen identity.

Project/ country	Architecture (Type)	Primary Purpose	Data sovereignty and privacy implications	Relevance for Colombia
Aadhaar (India)	Centralized national eID (non-blockchain)	Social inclusion and access to services	Inclusion at scale, but privacy and state-control concerns (Mira et al., 2020; Addo and Senyo, 2021)	Not aligned with SSI; limited replicability under Colombia's data-protection approach (MinTIC, 2020)
Digital ID (Uruguay)	Federated system	Access with unique credentials	Strong governance and interoperability via national platform (Gobierno de UruguayAGESIC, 2023)	Viable with integration into state services (Ministerio de Tecnologías de la Información y las Comunicaciones, 2025a)
Sovrin/SSI (Europa/Global)	Blockchain + SSI (DID/VC)	Total user control over credentials	High data protection through decentralization and selective disclosure (Stockburger et al., 2021; Wang and De Filippi, 2020)	Promising model with local regulatory adjustments (MinTIC, 2023b)
Estonia	Non-blockchain data-exchange layer (government interoperability; X-Road)	Efficient public administration	Limited transparency, high interoperability (Semenzin et al., 2022)	Reference for interoperability infrastructure, but centralized (MinTIC, 2023a)
Building Blocks (UN/WFP)	Permissioned blockchain (Ethereum)	Beneficiary verification and traceability	Protection and auditability in humanitarian contexts (Wang and De Filippi, 2020)	Applicable in vulnerable and social sectors (MinTIC, 2020)

Colombia, inclusion and digital literacy remain salient and should be addressed through assisted issuance and verification, recovery options, and multilingual usability testing (Hünseler and Pöll, 2023; Anand and Brass, 2021; Hilowle et al., 2024; Barrios Tao and Díaz Pérez, 2025; MinTIC, 2025).

Governance and architecture choices should therefore emphasize permissioned, or hybrid ledgers governed by a public consortium with a regulator or auditor node, interoperable with open conformance profiles used internationally. Initial domains with clear public value include education and health or social-program attestations, which can be implemented with personal data off-chain and verifiable status on-chain. Evaluation should prioritize operational metrics such as verification latency, uptime, revocation timeliness, and cost per verification over aggregate adoption claims (Schlatt et al., 2022; Pinto, Ferreira da Silva and Moro, 2022; European Commission, 2025).

This review is narrative and prioritizes conceptual and regulatory relevance over exhaustiveness. The literature remains uneven across technical, legal, and socioeconomic strands, and several deployments are reported as pilots without longitudinal evaluation, which motivates further comparative and field research on performance, cost, recovery flows, and fairness outcomes in the Colombian context (Secinaro et al., 2021; Pava Díaz, Páez Méndez and Niño Vásquez, 2023).

Author contributions

LR: Writing – review and editing, Funding acquisition, Writing – original draft, Data curation, Validation, Conceptualization, Methodology, Supervision. DP: Writing – review and editing, Investigation, Validation, Formal Analysis, Supervision, Data curation, Visualization, Writing – original draft, Conceptualization. YH: Investigation, Writing – review and editing, Methodology, Formal Analysis, Writing – original draft, Data curation, Validation, Conceptualization, Visualization.

Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

Abu Bakar, A., Shariff, A. R. M., Huei, C. J., and Fadilah, S. I. (2024). The digital pheromone: building digital identity of smartphone users based on time-varying multivariates. *ICT Express* 10, 981–988. doi:10.1016/j.icte.2024.07.008

Addo, A. (2022). Orchestrating a digital platform ecosystem to address societal challenges: a robust action perspective. *J. Inf. Technol.* 37 (4), 359–386. doi:10.1177/02683962221088333

Addo, A., and Senyo, P. K. (2021). Advancing e-governance for development: digital identification and its link to socioeconomic inclusion. *Gov. Inf. Q.* 38, 101568. doi:10.1016/j.giq.2021.101568

Anand, N., and Brass, I. (2021). Responsible innovation for digital identity systems. *Data and Policy* 3, e35. doi:10.1017/dap.2021.35

Baheer, B. A., Lamas, D., and Sousa, S. (2020). A systematic literature review on existing digital government architectures: state of the art, challenges, and prospects. *Adm. Sci.* 10 (2), 25. doi:10.3390/admsci10020025

Barrios Tao, H., and Díaz Pérez, V. (2025). Inclusión, alfabetización y bienestar para la ciudadanía digital: Brasil-Colombia (2016-2023). *Collectivus* 12 (1). doi:10.15648/collectivus.vol12num1.2025.4387

Cagigas, D., Clifton, J., Diaz-Fuentes, D., and Fernandez-Gutierrez, M. (2021). Blockchain for public services: a systematic literature review. *IEEE Access* 9, 13904–13921. doi:10.1109/ACCESS.2021.3052019

Congreso de Colombia (1999). "Ley 527 de 1999: Mensajes de datos, comercio electrónico y firmas digitales,". Bogotá. Available online at: http://www.secretariasenado.gov.co/senado/basedoc/ley_0527_1999.html.

Congreso de Colombia (2005). Ley 962 de 2005. *D. Of.* 46.299 (25 July 2005). Available online at: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1671809.

European Commission (2025). *Identidad digital europea*. Brussels: European Commission. Available online at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_es.

Gobierno de Chile, Ministerio Secretaría General de la Presidencia (2022). Digitalización del Estado: más de 14,4 millones de personas ya tienen su ClaveÚnica, con la cual pueden acceder a 1.730 trámites de manera online. Available online at: https://www.gob.cl/noticias/digitalizacion-del-estado-mas-de-144-millones-de-personas-ya-tienen-su-claveunica-con-la-cual-pueden-acceder-a-1730-tramites-de-manera-online/.

Gobierno de Uruguay, AGESIC (2023). *No tan distintos: estonia, Uruguay y el gobierno digital*. Montevideo: AGESIC. Available online at: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/no-tan-distintos-estonia-uruguay-y-el-gobierno-digital.

Guggenberger, T., Kühne, D., Schlatt, V., and Urbach, N. (2023). Designing a cross-organizational identity management system: utilizing SSI for the certification of retailer attributes. *Electron. Mark.* 33 (3), 3. doi:10.1007/s12525-023-00620-z

He, Z. (2022). When data protection norms meet digital health technology: china's regulatory approaches to health data protection. *Comput. Law and Secur. Rev.* 47, 105758. doi:10.1016/j.clsr.2022.105758

Hilowle, M., Yeoh, W., Grobler, M., Pye, G., and Jiang, F. (2024). Improving national digital identity systems usage: human-centric cybersecurity survey. *J. Comput. Inf. Syst.* 64 (6), 820–834. doi:10.1080/08874417.2023.2251452

Hünseler, M., and Pöll, E. (2023). "Promises and problems in the adoption of self-sovereign identity management from a consumer perspective," in *Privacy and identity management*. Editors F. Bieker and J. Meyer (Cham: Springer), 671, 85–100. doi:10.1007/978-3-031-31971-6_8

Karasek, I., and Wojciechowicz, I. (2021). Reconciliation of anti-money-laundering instruments and European data-protection requirements in permissionless blockchain spaces. *J. Cybersecurity* 7 (1), tyab004. doi:10.1093/cybsec/tyab004

Lan, F., and Jiang, Y. (2024). Optimization exploration of digital identity authentication algorithm based on blockchain. *Appl. Math. Nonlinear Sci.* 9 (1), 20241704–20241716. doi:10.2478/amns-2024-1704

López Solano, J., and Castañeda, J. D. (2024). "A promising playground": IDEMIA and the digital ID infrastructuring in Colombia. *Inf. Commun. and Soc.* 27 (15), 2669–2685. doi:10.1080/1369118X.2024.2302995

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) (2023a). *Guía de referencia de blockchain en el Estado colombiano*. Bogotá: MinTIC. Available online at: https://gobiernodigital.mintic.gov.co/692/articles-161810_pdf.pdf.

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) (2025a). Centro de Innovación Pública Digital: proyectos. *Gob. Digit.* Available online at: https://gobiernodigital.mintic.gov.co/portal/Centro-de-Innovacion-Publica-Digital/Proyectos/#data=%7B%22filter%22:%22412569%22,%22page%22:1%7D.

MinTIC (2020). Resolución 2160 de 2020. Diario Oficial 51.729. Available online at: https://gobiernodigital.mintic.gov.co/692/articles-272983_res_2160_2020.pdf.

MinTIC (2023b). *Estrategia de gobierno digital en Colombia*. Bogotá: MinTIC. Available online at: https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf.

MinTIC (2023c). *Plan Estratégico Institucional 2023–2026: conectividad y tecnología para cambiar la vida*. Bogotá: MinTIC. Available online at: https://www.mintic.gov.co/portal/715/articles-334069_recurso_4.pdf.

MinTIC (2025). "Ciudadanía digital," in *Bogotá: MinTIC*. Available online at: https://colombiatic.mintic.gov.co/679/w3-propertyvalue-36666.html.

Mira, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M., and Sharma, R. (2020). Realizing digital identity in government: prioritizing design and implementation objectives for aadhaar in India. *Gov. Inf. Q.* 37, 101442. doi:10.1016/j.giq.2019.101442

Mishra, A., Alzoubi, Y. I., Anwar, M. J., and Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: an evidence from seven nations. *Comput. and Secur.* 120, 102820. doi:10.1016/j.cose.2022.102820

Misión de Observación Electoral (MOE) (2023). "La implementación de la cédula digital en Colombia,". Bogotá.

Pauletto, C. (2021). Blockchain in international e-government processes: opportunities for recognition of foreign qualifications. *Res. Glob.* 3, 100034. doi:10.1016/j.resglo.2020.100034

Pava Díaz, R. A., Páez Méndez, R. V., and Niño Vásquez, L. F. (2023). A bibliometric study of scientific production on self-sovereign identity. *Ing. Colomb.* 28, 204–218. doi:10.14483/23448393.19656

Pinto, F., Ferreira da Silva, C., and Moro, S. (2022). People-centered distributed-ledger-technology–IoT architectures: a systematic literature review. *Telematics Inf.* 70, 101812. doi:10.1016/j.tele.2022.101812

Presidencia de la República de Colombia (2012). Decreto 2364 de 2012. *D. Of.* 48.135. Available online at: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=50583.

Presidencia de la República de Colombia (2015). Decreto 1078 de 2015: Único Reglamentario TIC. *D. Of.* 49 (23 July 2015). Available online at: https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=77888.

Presidencia de la República de Colombia (2022). Decreto 767 de 2022: Política de Gobierno Digital. *Bogotá*. Available online at: https://gobiernodigital.mintic.gov.co/692/articles-272977_Decreto_767_2022.pdf.

Robles Carrillo, M. (2024). Digital identity: an approach to its nature, concept, and functionalities. *Int. J. Law Inf. Technol.* 32 (1), eaae019. doi:10.1093/ijlit/eaae019

Ruiu, P., Saiu, S., and Grosso, E. (2024). Digital identity in the EU: promoting eIDAS solutions based on biometrics. *Future Internet* 16 (7), 228. doi:10.3390/fi16070228

Schlatt, V., Sedlmeir, J., Feulner, S., and Urbach, N. (2022). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. *Inf. and Manag.* 59 (7), 103553. doi:10.1016/j.im.2021.103553

Secinaro, S., Dal Mas, F., Brescia, V., and Calandra, D. (2021). Blockchain in the accounting, auditing and accountability fields: a bibliometric and coding analysis. *Account. Auditing and Account. J.* 35 (9), 168–203. doi:10.1108/AAAJ-10-2020-4987

Semenzin, S., Rozas, D., and Hassan, S. (2022). Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia. *Policy and Soc.* 41 (3), 386–401. doi:10.1093/polsoc/puac014

Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., and Avital, M. (2021). Blockchain-enabled decentralized identity management: the case of self-sovereign identity in public transportation. *Blockchain Res. Appl.* 2 (2), 100014. doi:10.1016/j.bcra.2021.100014

Tan, K. L., Chi, C. H., and Lam, K. Y. (2023). Survey on digital sovereignty and identity: from digitization to digitalization. *ACM Comput. Surv.* 56 (3), 1–36. doi:10.1145/3616400

Wang, F., and De Filippi, P. (2020). Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion. *Front. Blockchain* 2, 28. doi:10.3389/fbloc.2019.00028

Xin, Y., Dilanchiev, A., Ali, M., Irfan, M., and Hong, Y. (2022). Assessing citizens' attitudes and intentions to adopt e-government services: a roadmap toward sustainable development. *Sustainability* 14, 15183. doi:10.3390/su142215183

Xu, B. (2023). *Privacy-aware biometric blockchain-based e-passport system for automatic border control (PhD thesis)*. Lancaster, United Kingdom: Lancaster University. doi:10.17635/lancaster/thesis/2110

Zulkifli, F., and Abidin, R. Z. (2025). Identity in the digital age: an investigation of Malaysian perspectives on technology and privacy. *J. Adv. Res. Appl. Sci. Eng. Technol.* 43 (2), 120–135. doi:10.37934/araset.43.2.120-135