

Security as a Strategic Asset: A Decentralized, Transparent, and Tokenized Framework for Digital Protection

María Paula González ^{1,2}, Walter Agüero ^{1,3}

¹ Universidad Siglo 21, Argentina, paula.gonzalez@ues21.edu.ar, walter.aguero@ues21.edu.ar

² Universidad Nacional del Sur, Argentina, mpg@cs.uns.edu.ar

³ Universidad Nacional de Villa Mercedes, Argentina, wfaguero@unvime.edu.ar

Abstract– *This paper examines the transition from traditional, reactive cybersecurity models toward a strategic paradigm in which security functions as a value-generating organizational asset within the digital economy. To operationalize this shift, it introduces the Decentralized, Transparent, and Tokenized (DTT) Strategic Security Framework, an original conceptual model that integrates blockchain architectures, verifiable transparency mechanisms, and tokenization processes to redefine digital protection. The framework articulates how decentralization enhances systemic resilience by reducing single points of failure, transparency strengthens accountability and regulatory trust through immutable auditability, and tokenization enables the economic activation of security-related artifacts such as credentials, access rights, and verifiable proofs. Drawing on illustrative international and Argentine case studies across high-value sectors—including finance, energy, logistics, agroindustry, technology, and Small and Medium-Sized Enterprises—the paper illustrates how early adoption of DTT principles may improve operational integrity, support compliance, and enable trust-based business models. The main contribution of this work is the presentation of a structured and replicable framework that bridges technical feasibility with strategic and economic rationale, offering organizations a pathway to reposition security from a defensive cost center toward a potential source of tangible and intangible value. The findings suggest that DTT-aligned security architectures can strengthen resilience, enhance market differentiation, and support sustainable digital transformation, particularly in emerging economy contexts.*

Keywords: *blockchain, tokenization, strategic security, decentralized architectures, Argentine case studies*

I. INTRODUCTION AND MOTIVATION

In today's data-driven and hyper-connected digital economy, cybersecurity has evolved from a purely defensive function to a critical enabler of trust, competitiveness, and innovation. Traditional security models—characterized by centralized control, reactive mitigation, and limited transparency—struggle to address the growing complexity of distributed infrastructures, emerging cyber-risks, and the increasing demand for verifiable digital integrity. As global markets adopt decentralized architectures and token-based economic models, the strategic relevance of security expands

beyond protection to become a potential generator of economic and operational value.

Recent studies emphasize that conceptualizing security as a strategic investment strengthens brand reputation, indicates regulatory alignment, and accelerates digital transformation initiatives. However, most organizations still lack a structured methodology to operationalize this transition and continue treating security as a cost center rather than a value-creating asset. This gap is even more pronounced in emerging economies, where resource constraints, legacy systems, and fragmented governance hinder the adoption of advanced protection models.

To address this challenge, this paper introduces the Decentralized, Transparent, and Tokenized (DTT) Strategic Security Framework. This original contribution provides a conceptual and actionable model that integrates decentralization for systemic resilience, transparency for verifiable accountability, and tokenization for monetization of security-related assets. By unifying technical feasibility with business rationale, the DTT Framework offers organizations a replicable pathway to transform digital protection into a strategic asset with tangible and intangible value.

This study adopts a conceptual and qualitative research approach aimed at developing a structured framework for understanding the strategic role of cybersecurity in contemporary digital ecosystems. Rather than relying on empirical validation, the work is grounded in the analytical integration of existing literature, institutional reports, and industry practices related to blockchain, decentralized architectures, and tokenization. The use cases presented throughout the paper are illustrative in nature and are intended to exemplify how the principles of decentralization, transparency, and tokenization are being adopted across different sectors and organizational contexts, rather than to provide exhaustive or statistically validated evidence. This approach enables the identification of emerging patterns and supports the conceptualization of security as a value-generating asset.

Accordingly, the contribution of this work should be understood as conceptual and integrative, aiming to provide a structured framework for interpreting emerging trends rather

than delivering empirically validated results. The remainder of this article is structured as follows: Section 2 presents the DTT Framework and its core principles. Section 3 analyzes strategic applications and use cases across high-value global and Argentine sectors. Section 4 situates the model within the state of the art. Section 5 discusses recommendations and future research directions. Finally, Section 6 presents the conclusions of the study.

II. PROPOSED FRAMEWORK: SECURITY AS A STRATEGIC ASSET

This section presents the central contribution of this work: the Decentralized, Transparent, and Tokenized (DTT) Strategic Security Framework. As shown in Fig. 1, the DTT Framework explicitly defines synergistic outcomes at the intersections of its three pillars, giving rise to Auditable Accountability (Decentralization + Transparency), Verified Asset Trading (Transparency + Tokenization), and Autonomous Ecosystems (Decentralization + Tokenization).

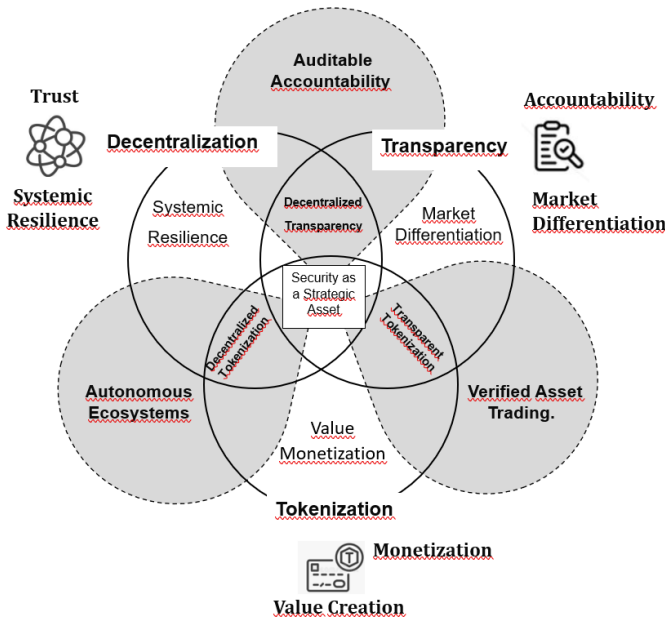


Fig 1. The proposed Decentralized, Transparent, and Tokenized (DTT) Strategic Security Framework.

The core innovation emerges at the central intersection, where these dynamics converge to operationalize Security as a Strategic Asset. This integrated approach addresses the current gap between isolated tactical experiments and the absence of a coherent strategic vision for security. Unlike existing initiatives concentrated in high-value niches (e.g., the Canton Network), the DTT Framework offers a replicable pathway for organizations to transition from defensive security spending toward value-generating security models, providing a robust methodological foundation that emphasizes measurable economic benefits, market access, and operational resilience.

While Fig. 1 presents the DTT Framework as an integrated model, the following subsections articulate the specific contribution of each principle and examine how their combined effect establishes the foundations for systemic resilience, verifiable trust, and security-driven value creation across diverse organizational and industrial contexts.

2.1. Decentralization for Systemic Resilience

As illustrated in Fig. 1, decentralization contributes to the center of the DTT Framework by sustaining the conditions under which security-relevant events can be reliably maintained and participate in the emergence of Security as a Strategic Asset.

In particular, the contribution of decentralization lies in distributing trust, authority, and validation across multiple nodes so that critical processes remain available and tamper-resistant under adverse or adversarial conditions, especially in environments where disruptions, failures, or coordinated attacks carry significant economic and regulatory impact. By reducing exposure to single-point failures and limiting dependency on centralized intermediaries, decentralization mitigates structural fragility and sustains the continuity and integrity of security-relevant operations.

2.2. Transparency as a Foundation for Verifiable Trust

Within the DTT Framework, transparency is incorporated as a strategic enabler of verifiable trust, rather than as a mere mechanism for increased visibility. Its contribution lies in transforming security-relevant actions, controls, and processes into artifacts that can be independently validated by multiple stakeholders. This capability is essential for repositioning security as a value-generating function, as it allows organizations to externalize trust and demonstrate integrity without relying on centralized authorities or subjective assurances.

As shown in Fig. 1, transparency contribution materializes through the emergence of auditable accountability at the intersection of the framework. By reducing information asymmetry and enabling independently verifiable evidence of compliance and integrity, transparency lowers regulatory friction, supports cross-organizational collaboration, and strengthens credibility in environments where demonstrable trust is a prerequisite for market participation and competitive differentiation.

2.3. Tokenization as a Mechanism for Security-Driven Value Creation

Tokenization adds a distinct economic dimension to the DTT Framework, allowing security-derived artifacts—such as verified credentials, certifications, or traceability proofs—to become actionable within digital markets and governance processes, as depicted in Fig. 1. Indeed, tokenization

contribution lies in operationalizing trust, compliance, and verification beyond their traditional role as internal controls, enabling them to function as transferable and programmable resources within digital ecosystems. Indeed, in this model, security is no longer confined to risk mitigation but becomes directly aligned with innovation and business incentives.

By providing monetization, interoperability, and automated governance, tokenization completes the transition of security from a defensive expenditure into a driver of sustainable business models and strategic differentiation.

Taken together, Section 2.1, Section 2.2 and this Section, contributions illustrate how security evolves—within the DTT Framework—from a protective function to a strategically exploitable asset.

III. USE CASES AND STRATEGIC APPLICATIONS

This section examines how the principles of decentralization, transparency, and tokenization articulated in the DTT Strategic Security Framework manifest in real-world contexts. Through illustrative international and Argentine use cases across multiple sectors and organizational scales, it explores adoption patterns in blockchain-enabled security models and derives indicative strategic implications for operationalizing security as a value-generating asset. The cases presented in this section are illustrative and do not necessarily represent full or integrated implementations of the DTT Framework. Instead, they highlight partial or evolving adoption patterns of decentralization, transparency, and tokenization across different sectors. Their purpose is to provide qualitative insights into how security-related capabilities may be reinterpreted as potential sources of operational and economic value, rather than to offer exhaustive or empirically validated evidence.

3.1. SECTORAL APPLICATIONS OF THE DTT FRAMEWORK

This subsection adopts an illustrative approach to show how organizations combine decentralization, transparency, and tokenization to reposition security from a defensive function to a strategic asset. In global financial and technology ecosystems, leading institutions such as JPMorgan Chase and Santander, together with cloud and technology providers including Google, Amazon, and Microsoft, have incorporated blockchain-based architectures to strengthen transactional integrity, digital identity, and data protection [1]-[5]. These initiatives indicate that decentralized and auditable infrastructures can enhance security while reducing operational inefficiencies and enabling scalable digital services. In several cases, tokenization mechanisms are employed to represent credentials, access rights, or certifications as verifiable digital assets, reinforcing the economic dimension of trust and compliance.

Similar dynamics are observed in energy, telecommunications, and supply-chain-intensive sectors. Corporations such as Shell and Enel have adopted blockchain solutions to certify renewable energy generation and market attributes, while telecommunications operators including Vodafone and Telefónica have applied distributed ledgers to optimize roaming management and network services. In supply-chain contexts, initiatives involving Carrefour, Nestlé, and IBM Food Trust illustrate how end-to-end traceability and immutable records support regulatory compliance, market access, and stakeholder confidence. Across these sectors, transparency and auditability operate as strategic resources rather than as purely operational safeguards [6]-[11].

In the Argentine context, organizations such as BBVA Argentina, fintech platforms like Ualá, technology firms including Globant, and energy initiatives explored by YPF Luz demonstrate an incremental but consistent pattern of adoption. These experiences illustrate how verifiable digital records and, in some cases, tokenization are used to enhance transactional security, certify origin and quality, and integrate local actors into global value chains. Although constrained by regulatory and economic factors, these cases show how DTT principles can be adapted to emerging economy environments [12]-[15].

For Small and Medium-Sized Enterprises, adoption is most feasible through blockchain- and security-as-a-service models, sectoral consortia, and pre-configured solutions for identity management, billing, and traceability. Both globally and in Argentina, such approaches reduce entry barriers and allow SMEs to transform security from a sunk cost into a commercial enabler, supporting contract acquisition, compliance with international standards, and access to markets that require demonstrable trust [16]-[18].

Public sector initiatives provide complementary conditions through regulatory clarity, technical standards, and interoperable infrastructures. International organizations such as ENISA and NIST, together with Argentine institutions including the National Cybersecurity Directorate, INTI, and AFIP, contribute to environments in which decentralized, transparent, and tokenized security models can scale effectively [16]-[22]. Taken together, these public and private initiatives illustrate how the DTT Framework offers a coherent lens for understanding the transition of security from a defensive expenditure into a strategic asset across organizational scales and institutional contexts.

3.2. ADOPTION RECOMMENDATIONS AND STRATEGIC IMPLICATIONS

Building on the cross-sectoral case studies presented above, this subsection identifies recurring adoption patterns and strategic implications across different organizational scales. Rather than prescribing universal solutions, the recommendations reflect how decentralization, transparency, and tokenization are being operationalized in practice to enable security to function as a value-generating asset.

For Small and Medium-Sized Enterprises, the cases suggest prioritizing scalable and cost-effective adoption pathways such as blockchain- and cybersecurity-as-a-service models, sectoral consortia, and standardized templates for traceability, compliance, and digital certification [18] [20]. These approaches lower technical complexity and upfront investment while enabling SMEs to externalize trust and participate in verifiable digital ecosystems.

For large enterprises, the strategic impact of DTT-aligned security models is maximized when blockchain-based mechanisms are embedded into core operational and governance structures rather than implemented as isolated pilot projects. Consistent application across supply chains, data governance architectures, identity systems, and customer engagement processes enables these organizations to leverage decentralization, transparency, and tokenization as sources of differentiation and value creation.

Governments and public entities play a central role in shaping the conditions under which DTT-aligned security models can scale. Clear regulatory frameworks, shared technical standards, and interoperability protocols are decisive for secure and economically viable applications of blockchain-based protection mechanisms. Public administrations may further contribute through direct adoption in public procurement, digital identity, tax and customs processes, and critical infrastructure protection, supported by incentives, public-private partnerships, and pilot programs [19] [25].

Beyond operational considerations, integrating decentralization, transparency, and tokenization within a unified security-as-an-asset framework has significant ethical and governance implications. Decentralization mitigates risks associated with excessive concentration of power and promotes more equitable participation in governance. Transparency embeds verifiable accountability into digital processes, reducing opportunities for corruption, misuse, or hidden bias. Tokenization enables explicit and enforceable rights related to data ownership, access privileges, and compliance certifications. These properties reinforce established standards and policy frameworks such as ISO/IEC 27001, ISO/IEC 27701, the NIST Cybersecurity Framework, and OECD data governance principles, as well as international guidelines for trustworthy AI [18], [25].

Importantly, the DTT Framework does not aim to extend or optimize traditional cybersecurity metrics, which are typically centered on risk mitigation, threat detection, or incident response. Instead, it introduces a complementary evaluative perspective focused on dimensions that are not captured by conventional approaches. In this sense, the framework shifts the analytical focus from measuring protection effectiveness to assessing how security contributes to value creation, trust externalization, and market enablement. As a result, direct comparison with traditional security evaluation models is limited, as the DTT approach operates on qualitatively different dimensions.

From an analytical perspective, the transition from security as a cost center to a value-generating asset may be assessed through a set of indicative dimensions aligned with the DTT Framework. These include: (i) resilience indicators, such as reduction of single points of failure and system recovery capacity; (ii) transparency indicators, including auditability of transactions and verifiability of compliance processes; (iii) tokenization indicators, such as the number and diversity of tokenized security-related assets (e.g., credentials, certifications, or access rights); and (iv) value-oriented indicators, including improvements in regulatory efficiency, reduction of compliance costs, enhanced market access, and increased stakeholder trust. While these indicators are not intended as standardized metrics, they provide an initial structure for evaluating the extent to which security contributes to organizational value creation within DTT-aligned architectures.

IV. RELATED WORK

Existing literature on cybersecurity and digital protection has traditionally framed security as a defensive and risk-mitigation function. Widely adopted frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 focus on identifying threats, defining technical and organizational controls, and ensuring compliance with security standards [23], [24]. Even contemporary architectural paradigms like Zero Trust Architecture formalize continuous verification and least-privilege access [25], but still conceive security primarily as control enforcement rather than as an economic or strategic asset.

More recent contributions attempt to expand this view by linking cybersecurity to organizational strategy and investment decisions. Security-by-design approaches and risk-based economic models argue that security can enhance resilience and long-term sustainability when embedded into governance and decision-making processes [26]. Quantitative approaches such as FAIR-based risk assessment and ROSI-oriented investment models further support this shift by framing cybersecurity expenditures in economic terms [27]. Nevertheless, these approaches largely remain within centralized or semi-centralized architectural assumptions and continue to treat security primarily as a mechanism for loss reduction rather than as a generator of new value streams.

In parallel, a growing body of literature examines blockchain technologies and decentralized trust architectures as alternatives to centralized security models. Research and institutional reports highlight how distributed ledgers can enhance transparency, immutability, and auditability in domains such as digital identity, supply-chain management, and financial transactions [16]. Within this stream, self-sovereign identity (SSI) and W3C specifications—for Decentralized Identifiers (DID) and Verifiable Credentials (VC)—redistribute trust and enable tamper-evident, privacy-preserving attestations across ecosystems supply-chain management, and financial transactions [28],

[29]. However, these contributions are often presented as technical solutions or sector-specific applications, without explicitly connecting decentralized security mechanisms to strategic or economic value creation.

Tokenization-focused work extends the discussion beyond infrastructure by analyzing how digital representations of assets, rights, and credentials enable programmability, automation, and new governance models. While policy and industry analyses emphasize efficiency, liquidity, and market design [30], they rarely connect tokenization explicitly to cybersecurity architectures or conceptualize security itself as an asset that can be monetized, exchanged, or leveraged strategically.

Policy-oriented and institutional literature underscores the importance of enabling conditions for advanced security models. Regulatory and governance studies emphasize the need for clear legal frameworks, shared technical standards, and interoperability to support trusted digital infrastructures [16]. As noted by [26], insufficient regulatory alignment tends to reinforce a defensive interpretation of security, constraining its evolution into a high-value organizational capability. Despite their relevance, these policy frameworks typically address governance and compliance challenges without proposing an integrated architectural model that operationalizes value-driven security.

Industry-driven initiatives and consortium-based networks—such as large-scale financial blockchain infrastructures—demonstrate that decentralized and shared security architectures can operate at scale in high-value environments. While these initiatives validate the feasibility of decentralized trust and compliance mechanisms, they are generally confined to specific sectors and do not offer a transferable strategic framework applicable across heterogeneous industries, organizational sizes, or emerging economies.

In contrast to the existing approaches across organizational scales, the DTT Strategic Security Framework integrates decentralization, transparency, and tokenization into a unified model explicitly oriented toward value creation. Rather than treating cybersecurity controls, decentralized infrastructures, and token-based mechanisms as separate or incremental enhancements, the framework conceptualizes their intersection as the means through which security transitions from a defensive cost center to a strategic, value-generating asset. By bridging insights from cybersecurity frameworks—as the ones depicted on [24] or [26]—strategic security investment models, decentralized identity standards like the ones described at [28] or [29], and tokenization literature [30], this work addresses a gap in the state of the art: the lack of a coherent and replicable methodology for operationalizing security as a strategic asset across sectors and regional contexts. In this sense, the DTT Framework is not intended to replace existing cybersecurity evaluation models but to complement them by introducing a new analytical perspective centered on value creation and trust externalization.

V. CONCLUSIONS AND FUTURE WORK

The findings of this work suggest that blockchain, tokenization, and emerging crypto-industry models have the potential to redefine the role of security in digital ecosystems—shifting it from a reactive safeguard toward a driver of competitiveness and economic value. By structuring protection models around decentralization, transparency, and tokenization, organizations may not only reduce vulnerabilities but also open new opportunities for market participation, strengthen stakeholder confidence, and enable the creation of verifiable digital assets.

While individual applications of these principles already exist across different sectors, the strategic novelty lies in integrating them within a single, coherent framework. This integration magnifies their impact: decentralization provides systemic resilience, transparency fosters trust and regulatory alignment, and tokenization directly converts trust and compliance into revenue streams. The case of the Canton Network illustrates the feasibility of such integration in financial contexts, but its underlying logic is equally adaptable to sectors such as energy, logistics, or agroindustry. From a policy perspective, governments and regulatory bodies play a critical role in enabling this paradigm shift. Clear legal frameworks, interoperability standards, and support for pilot programs can accelerate adoption, particularly in emerging economies where SMEs often face barriers to implementing advanced protection models. Future research should explore three key directions:

- i. Cross-sectoral frameworks — studying how the integrated model of decentralization, transparency, and tokenization can be adapted to different industries with specific compliance and market conditions.
- ii. Economic modelling — developing quantitative methods to measure the direct and indirect value generated by treating security as an asset.
- iii. Interoperability architectures — designing technical standards that allow security-tokenized assets to operate seamlessly across platforms, jurisdictions, and regulatory environments.

By moving beyond the traditional view of security as a cost and embracing it as a strategic, value-generating asset, organizations—whether in global markets or the Argentine context—can position themselves for sustainable growth in an increasingly interconnected, competitive, and risk-exposed world.

ACKNOWLEDGMENTS

This paper was founded by research project XXX (omitted for Blind Review) financed by XXX (omitted for Blind

Review) of the XXX (omitted for Blind Review) of the XXX (omitted for Blind Review)

REFERENCES

- [1] JPMorgan Chase & Co., “Onyx Digital Assets Platform,” JPMorgan, 2023. [Online]. Available: <https://www.jpmorgan.com/onyx>
- [2] Banco Santander S.A., “Blockchain Solutions for International Payments,” Santander Group, 2023. [Online]. Available: <https://www.santander.com/en/innovation/blockchain>
- [3] Google Cloud, “Decentralized Identity and Verifiable Credentials,” Google Cloud Documentation, 2024. [Online]. Available: <https://cloud.google.com/solutions/decentralized-identity>
- [4] Amazon Web Services, “Blockchain and Distributed Ledger Technologies on AWS,” AWS Whitepaper, 2023. [Online]. Available: <https://aws.amazon.com/blockchain/>
- [5] Microsoft Corporation, “Blockchain and Decentralized Identity on Azure,” Microsoft Azure Documentation, 2023. [Online]. Available: <https://learn.microsoft.com/en-us/azure/architecture/blockchain/>
- [6] Shell plc, “Blockchain-Enabled Certification of Renewable Energy,” Shell Sustainability Report, 2023. [Online]. Available: <https://www.shell.com/sustainability.html>
- [7] Enel S.p.A., “Digital Traceability and Blockchain for Energy Markets,” Enel Innovation Report, 2023. [Online]. Available: <https://www.enel.com/innovation>
- [8] Vodafone Group Plc, “Blockchain Applications in Roaming and Telecommunications,” Vodafone Technology Report, 2022. [Online]. Available: <https://www.vodafone.com/business/iot/blockchain>
- [9] Telefónica S.A., “Blockchain for Network Security and Digital Services,” Telefónica Tech Report, 2023. [Online]. Available: <https://www.telefonicatech.com>
- [10] IBM Corporation, “IBM Food Trust: Blockchain for Food Traceability,” IBM White Paper, 2022. [Online]. Available: <https://www.ibm.com/blockchain/solutions/food-trust>
- [11] Nestlé S.A., “Enhancing Supply Chain Transparency with Blockchain,” Nestlé Digital Transformation Report, 2023. [Online]. Available: <https://www.nestle.com/innovation/blockchain>
- [12] BBVA Argentina, “Blockchain and Digital Security Initiatives,” BBVA Corporate Report, 2024. [Online]. Available: <https://www.bbva.com.ar>
- [13] Ualá, “Tokenization and Secure Digital Payments,” Ualá Technology Blog, 2024. [Online]. Available: <https://www.uala.com.ar/blog>
- [14] Globant S.A., “Blockchain-Based Digital Transformation Projects,” Globant White Paper, 2023. [Online]. Available: <https://www.globant.com/technology/blockchain>
- [15] YPF Luz, “Blockchain and Transparency in Renewable Energy Initiatives,” YPF Luz Innovation Report, 2024. [Online]. Available: <https://www.ypf luz.com>
- [16] European Union Agency for Cybersecurity (ENISA), “Blockchain Cybersecurity and Governance,” ENISA Report, 2023. [Online]. Available: <https://www.enisa.europa.eu/topics/blockchain>
- [17] World Economic Forum, “Tokenization and the Future of Digital Trust,” WEF White Paper, 2024. [Online]. Available: <https://www.weforum.org/reports/tokenization>
- [18] Organisation for Economic Co-operation and Development (OECD), “Digital Security Risk Management for SMEs,” OECD Report, 2023. [Online]. Available: <https://www.oecd.org/digital/security/>
- [19] National Institute of Standards and Technology (NIST), “Blockchain Technology Overview,” NIST Internal Report 8202, 2023. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8202.pdf>
- [20] European Union Agency for Cybersecurity (ENISA), “Blockchain Interoperability and Standards,” ENISA Report, 2022. [Online]. Available: <https://www.enisa.europa.eu/publications/blockchain-standards>
- [21] Administración Federal de Ingresos Públicos (AFIP), “ARCA Platform and Digital Traceability in Foreign Trade,” AFIP, Argentina, 2023. [Online]. Available: <https://www.afip.gob.ar>
- [22] Instituto Nacional de Tecnología Industrial (INTI), “Digital Traceability and Industry 4.0 Initiatives,” INTI Report, Argentina, 2024. [Online]. Available: <https://www.inti.gob.ar>
- [23] Y. Li and Q. Liu, “A comprehensive review of cyber-attacks and cybersecurity: Emerging trends and recent developments,” Energy Reports, vol. 7, pp. 8176–8186, 2021.
- [24] J. Kaur and K. R. Ramkumar, “Recent trends in cybersecurity: A review,” Journal of King Saud University – Computer and Information Sciences, vol. 34, no. 8, pp. 5766–5781, 2022.
- [25] National Institute of Standards and Technology (NIST), “Zero Trust Architecture,” NIST Special Publication 800-207, 2020. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-207>
- [26] P. Radanliev, “Digital security by design,” Security Journal, vol. 37, no. 4, pp. 1640–1679, 2024.
- [27] Y. He, T. Xin, and C. Luo, “Enhancing cybersecurity investment with FAIR-ROSI,” Information Systems Frontiers, 2025.
- [28] World Wide Web Consortium (W3C), “Decentralized Identifiers (DID) v1.0,” W3C Recommendation, Jul. 2022. [Online]. Available: <https://www.w3.org/TR/did-core/>
- [29] World Wide Web Consortium (W3C), “Verifiable Credentials Data Model 1.1,” W3C Recommendation, Nov. 2022. [Online]. Available: <https://www.w3.org/TR/vc-data-model/>
- [30] Organisation for Economic Co-operation and Development (OECD), “Tokenisation of Assets and Potential Implications for Financial Markets,” OECD Publishing, 2023. [Online]. Available: <https://www.oecd.org/finance/financial-markets/tokenisation-of-assets-and-potential-implications-for-financial-markets.htm>
- [31] S. J. Greenwald, “What is the old security paradigm?,” in Proc. Workshop on New Security Paradigms, 1998, pp. 107–118.
- [32] P. Sharma and H. Gupta, “Emerging Cyber Security Threats and Security Applications in the Digital Era,” in Proc. ICRITO 2024, IEEE, pp. 1–6.