The Emergence of Trust as a Technical and Legal Concept

El surgimiento de la confianza como concepto técnico y legal

O surgimento da confiança como conceito técnico e jurídico

Alfonso Vicente [1] (*), Ariel Sabiguero [2]

Recibido: 10/03/2026 Aceptado: 22/06/2026

Summary. - This paper traces the historical transformation of trust from a social and moral virtue into a technical and legal construct. Drawing on historical epistemology, it reconstructs how computer science in the late twentieth century redefined trust as a property of systems, protocols, and credentials —and how this technical meaning later migrated into law through the concept of trust services. While no canonical definition of trust exists —neither across the social sciences nor within any of them— it is possible to identify recurring traits of what may be called the traditional concept of trust. Adapting from Luhmann, the paper defines trust as a subjective belief in the good future performance of someone or something upon which valuable resources or enterprises depend. It then shows how technical and legal redefinitions of the term displaced this relational and experiential meaning with notions of formal verification and institutional compliance. The argument proceeds in three movements: (1) Trust as a traditional concept, understood as a relational and emotive category; (2) Trust as a technical concept, understood as designed reliability and automated verification; and (3) Technological trust as a legal concept, in which states reimport the term to confer legitimacy upon infrastructures and accredited intermediaries. The discussion interprets this evolution as a case of semantic inversion: law now commands citizens to trust entities that were, in technical origin, conceived precisely to eliminate the need for trust. Following Stevenson, the emotive charge of the word endures across this migration, generating a political illusion where moral confidence fuses with mathematical certainty. Naming, as Hacking reminds us, is never neutral: when categories travel, they create new realities of belief and obligation.

Keywords: *Trust, Historical Epistemology, Philosophy of Computer Science, Philosophy of Technology, Digital Rights*.

(*) Corresponding author.

[1] Research Coordinator, Facultad de Ingeniería, Universidad de la Empresa (Uruguay), avicente@ude.edu.uy,
ORCID iD: https://orcid.org/0000-0003-3575-5326

[2] Research Coordinator, Facultad de Ingeniería, Universidad de la Empresa (Uruguay), asabiguero@ude.edu.uy,
ORCID iD: https://orcid.org/0009-0008-6759-0865

Memoria Investigaciones en Ingeniería, núm. 30 (2026). pp. 256-265
https://doi.org/10.36561/ING.30.17
ISSN 2301-1092 • ISSN (en línea) 2301-1106 – Universidad de Montevideo, Uruguay

Resumen. - *Este artículo rastrea la transformación histórica de la confianza desde una virtud social y moral a una construcción técnica y legal. Basándose en la epistemología histórica, reconstruye cómo la ciencia informática a finales del siglo XX redefinió la confianza como una propiedad de sistemas, protocolos y credenciales, y cómo este significado técnico posteriormente migró al derecho a través del concepto de servicios de confianza. Si bien no existe una definición canónica de confianza, ni en las ciencias sociales ni dentro de ninguna de ellas, es posible identificar rasgos recurrentes de lo que podría llamarse el concepto tradicional de confianza. Adaptando de Luhmann, el artículo define la confianza como una creencia subjetiva en el buen desempeño futuro de alguien o algo de lo que dependen recursos o empresas valiosas. Luego muestra cómo las redefiniciones técnicas y legales del término desplazaron este significado relacional y experiencial con nociones de verificación formal y cumplimiento institucional. El argumento procede en tres movimientos: (1) La confianza como un concepto tradicional, entendido como una categoría relacional y emotiva; (2) La confianza como un concepto técnico, entendido como confiabilidad diseñada y verificación automatizada; y (3) La confianza tecnológica como concepto legal, en la que los Estados reimportan el término para conferir legitimidad a infraestructuras e intermediarios acreditados. El análisis interpreta esta evolución como un caso de inversión semántica: la ley ahora exige a los ciudadanos confiar en entidades que, en su origen técnico, fueron concebidas precisamente para eliminar la necesidad de confianza. Siguiendo a Stevenson, la carga emotiva de la palabra perdura a lo largo de esta migración, generando una ilusión política donde la confianza moral se fusiona con la certeza matemática. El nombramiento, como nos recuerda Hacking, nunca es neutral: cuando las categorías viajan, crean nuevas realidades de creencia y obligación.*

Palabras clave: *Confianza, Epistemología histórica, Filosofía de la computación, Filosofía de la tecnología, Derechos digitales.*

Resumo. ***-*** *Este artigo traça a transformação histórica da confiança, de uma virtude social e moral para uma construção técnica e jurídica. Baseando-se na epistemologia histórica, reconstrói-se como a ciência da computação, no final do século XX, redefiniu a confiança como uma propriedade de sistemas, protocolos e credenciais —e como esse significado técnico posteriormente migrou para o direito por meio do conceito de serviços de confiança. Embora não exista uma definição canônica de confiança —nem nas ciências sociais nem em nenhuma delas—, é possível identificar traços recorrentes do que pode ser chamado de conceito tradicional de confiança. Adaptando Luhmann, o artigo define confiança como uma crença subjetiva no bom desempenho futuro de alguém ou algo, do qual dependem recursos ou empreendimentos valiosos. Em seguida, demonstra-se como as redefinições técnicas e jurídicas do termo substituíram esse significado relacional e experiencial por noções de verificação formal e conformidade institucional. O argumento prossegue em três movimentos: (1) Confiança como um conceito tradicional, entendida como uma categoria relacional e emotiva; (2) Confiança como um conceito técnico, entendida como confiabilidade projetada e verificação automatizada; e (3) Confiança tecnológica como um conceito jurídico, no qual os Estados reimportam o termo para conferir legitimidade a infraestruturas e intermediários credenciados. A discussão interpreta essa evolução como um caso de inversão semântica: a lei agora ordena aos cidadãos que confiem em entidades que foram, em sua origem técnica, concebidas precisamente para eliminar a necessidade de confiança. Seguindo Stevenson, a carga emotiva da palavra perdura durante essa migração, gerando uma ilusão política em que a confiança moral se funde com a certeza matemática. A nomenclatura, como Hacking nos lembra, nunca é neutra: quando as categorias viajam, elas criam novas realidades de crença e obrigação.*

Palavras-chave: *Confiança, Epistemologia Histórica, Filosofia da Ciência da Computação, Filosofia da Tecnologia, Direitos Digitais.*

1. Introduction. - Life presents an ineradicable uncertainty. We cannot be certain about the future, but having some expectations broadens the possibilities for action in the present [1]. Trust thus emerges as the fragile cement of social life. Philosophers, economists, and sociologists alike have treated it as the tacit foundation of cooperation and the antidote to uncertainty. Yet during the second half of the twentieth century, trust underwent an unnoticed semantic migration. The term that once denoted a moral and social relation among people —an ethically charged bond grounded in mutual recognition and expectation— began to be used to describe the secure communication of machines, systems, and institutions. Today, technical standards and legal instruments casually speak of trusted platforms, chains of trust, and Trust Service Providers as if these expressions carried a single, self-evident meaning. They do not. Their coexistence conceals an epistemic shift with profound consequences.

This paper explores how the meaning of trust was displaced from fuzzy human judgment to technical verification and legal prescription. It follows the method of historical epistemology, which treats categories not as timeless but as historically situated instruments of thought and governance. Our task is genealogical: to identify how trust was successively reconstituted as a technical and then a legal operator, and what remains of its traditional emotive and relational sense after these transformations. This reconstruction is necessarily selective. It does not claim to offer a complete or exhaustive genealogy of the technical concept of trust, but rather a preliminary sketch of its main transformations. A detailed genealogy of trust in computer science and law still remains to be written; if we attempt one here, it is only to illuminate the conceptual path by which a moral and social term came to designate mechanisms of verification and control. This approach is genealogical in method but realist in spirit: it examines how concepts evolve as instruments of understanding and coordination, without implying that reality itself is contingent upon their use.

While many disciplines employ the term without defining it, only a few thinkers have attempted to analyze its structure and social function in depth. Among them, Luhmann, Fukuyama, and Tilly stand out for treating trust as both a moral sentiment and a systemic prerequisite for cooperation. Fukuyama, in particular, emphasized its role as a cultural resource underlying economic prosperity and institutional stability [2].

We acknowledge at the outset that no canonical definition of trust exists. As Luhmann observed[3], is a concept "taken from common usage or from the traditional realm of discussion about ethics." [1] Nevertheless, a family resemblance can be discerned among usages that involve three core features: uncertainty, dependency, and value at risk. Building on this insight, we may propose an operational definition suited to our inquiry: Trust is a subjective belief in the good future performance of someone or something upon which valuable resources or enterprises depend.

This definition accommodates both interpersonal and technical contexts without erasing their difference. It highlights the forward-looking and relational nature of trust, as well as its vulnerability to disappointment. With this orientation, the argument proceeds in three parts: first, to reconstruct the traditional moral and relational uses of the term; second, to trace its technical transformation in computer science; and third, to analyze its legal codification in frameworks of electronic signatures and certification. The discussion then interprets this trajectory in light of Stevenson's theory of emotive meaning and Hacking's reflections on the performativity of categories.

2. Trust as a Traditional Concept. - Without aiming at a precise definition or deep analysis, trust, in its traditional sense, is not a substance but a relation. It presupposes a trinity: a subject A, an object B, and a domain X —the matter of dependence. A trusts B with respect to X. This relational structure can take multiple forms depending on what or whom is trusted: people, ideas, or artifacts.

Trust in people. To trust a person is to rely on their integrity, competence, or goodwill. It presumes moral character and social memory: past behavior grounds expectations of future conduct. Locke described trust as the foundation of

[3] We may owe Luhmann more than it seems at first glance; to do justice to his position, it is worth citing the following passage at length: "There is a question worth serious consideration of whether it is advisable [...] to employ terms and concepts taken from common usage or from the traditional realm of discussion about ethics. [...] The usefulness of the term, which resides in its uniqueness, will be lost, and its traditional range of meaning devalued." [1]

delegated authority [3], while Hume observed that "to perform promises is requisite to beget mutual trust and confidence in the common offices of life" [4]. Trust thus functions as the condition that makes cooperation possible —an invisible infrastructure sustaining promises, contracts, and institutions. This moral dimension extends into the economic sphere. Carl Menger emphasized that, before the establishment of legal tender, trust in the weight and purity of coined metal was a prerequisite for its transformation into money, and that confidence in the authenticity and backing of banknotes later became essential for their acceptance as currency [5]. Trust therefore mediates between personal conduct and systemic stability: it links moral reliability with the material instruments of exchange. In every case, trusting involves exposure to wrongdoing, error, and negligence —to use Charles Tilly's triad. As Tilly noted, "trust networks are vulnerable to malfeasance, error, and failure" and governments throughout history have sought to appropriate these networks for their own purposes. States, he argued, routinely insert themselves into existing circuits of interpersonal trust —families, guilds, religious communities— to channel loyalty and compliance [6]. This observation foreshadows the later appropriation of trust by legal institutions: the term's authority is borrowed from its moral and social roots.

Trust in ideas. To trust an idea or theory is to believe in its coherence and predictive power. Scientists "trust" a model to hold across contexts, much as citizens trust economic or political doctrines. Here trust functions as epistemic reliance: one wagers that a hypothesis will continue to work. This trust can be shaken by anomalies, falsification, or shifts in paradigm, yet it remains indispensable for coordinated action. Without some degree of epistemic trust, science itself would be paralyzed.

Trust in artifacts. We also trust artifacts —the ship that should not sink, the airplane that should not stall, the lock that should not yield, the banknote that should not lose value overnight, and even the encryption algorithm that should preserve our privacy. In each case, trust attaches to design, maintenance, and proper functioning rather than to character or belief. Yet even this apparently "objective" trust presupposes institutions: shipbuilders, engineers, manufacturers, and money issuers. Artifactual trust therefore links back to social trust; we rely on objects because we rely on those who make, certify, and supervise them. Some artifacts also generate feedback loops between performance and confidence. Money is a paradigmatic example: its value depends on collective expectations about its future stability[4], and those expectations in turn respond to the perceived integrity of the institutions that issue and manage it. As economic historians have shown, when the link between public trust and institutional discipline is broken —through repeated collusion between bankers and governments— confidence erodes, triggering crises and systemic instability [7].

Across these variations, trust remains an ethical and emotional relation. Following Stevenson, the term carries an emotive meaning: through historical usage, it elicits positive feelings of safety and solidarity. Stevenson wrote that "The emotive meaning of a word is a tendency of a word, arising through the history of its usage, to produce (result from) affective responses in people […] Such tendencies to produce affective responses cling to words very tenaciously." [8] To call someone —or something— "trusted" is thus not a neutral description but an invitation to approval. This emotive residue persists even when the term migrates into technical or legal contexts. It is precisely this persistence that allows later transformations of trust to borrow its moral prestige.

3. Trust as a Technical Concept. - The technical redefinition of trust did not result from a deliberate attempt to abolish human judgment. Rather, it emerged as an unintended consequence of efforts to design secure and reliable data interchange processes —a process that exemplifies the unintended results of human action. Engineers sought predictability, not philosophy; but in codifying procedures that displaced judgment onto verification, they altered the semantics of trust.

From reliability to verification: The Orange Book. The U.S. Department of Defense's Trusted Computer System Evaluation Criteria (1983), known as the Orange Book, introduced the notion of a Trusted Computing Base (TCB) —

[4] Of course, this is not to suggest that expectations operate in isolation from objective factors such as the money supply and the rate of monetary issuance. Rather, expectations reflect and amplify these underlying realities.

the ensemble of mechanisms responsible for enforcing a system's security policy [9]. Trust, here, refers not to belief but to evaluation: components are trusted because they have been tested and certified. Assurance becomes a property of code. In this framework, trust is ex ante (granted by certification) and binary (a module either passes or fails). The result is a technical ontology in which reliability replaces character as the object of confidence.

Mathematical trust: Diffie–Hellman and RSA. A more radical transformation came with public-key cryptography. The work of Diffie and Hellman in 1976 [10] and RSA in 1978 [11] replaced personal trust with computational security[5]. Communication between strangers became possible through the infeasibility of reversing a one-way function. What warranted confidence was not the honesty of participants but the computational hardness of certain problems. Trust was now quantified by probability. This new rationality, however, harbored a paradox. Ken Thompson's Turing Award lecture, "Reflections on Trusting Trust" (1984), revealed that even verified software could be compromised if the tools used to build it were tainted. Complete elimination of trust was impossible: every layer of verification presupposed another trusted foundation. Thompson's insight reintroduced epistemic humility —no system can certify its own trustworthiness [12].

Institutionalized trust: Kerberos, X.509, and PGP. In networked environments, trust became an institutional relation among entities mediated by cryptographic protocols. Kerberos (MIT, 1985–88) formalized the notion of a trusted third party: a Key Distribution Center that both clients and servers must accept as authoritative [13]. The X.509 standard (1988) defined a Certification Authority (CA) as an entity "trusted by one or more users" to issue certificates [14]. Here, trust was no longer a judgment, but a state variable propagated through a chain of trust. RFC 1422 (1993) codified these practices for Internet governance, establishing procedures for delegation and revocation [15]. Phil Zimmermann's Pretty Good Privacy (PGP, early 1990s) transformed trust into a distributed administrative practice: through its "web of trust," users could sign one another's keys with graded endorsements —unknown, marginal, or complete— converting the social gesture of recommendation into formal metadata [16]. Finally, Matt Blaze, Joan Feigenbaum, and Jack Lacy's seminal paper "Decentralized Trust Management" (1996) synthesized these trends by defining trust as a logical relation between policies and credentials [17]. Their PolicyMaker system introduced a new computational layer —trust management— distinct from authentication and authorization. At this point, trust had become an object of computation, managed and reasoned about by machines.

The cumulative result of these developments was a semantic inversion. In engineering, trust came to mean precisely the opposite of its traditional sense. It no longer signified a subjective belief under uncertainty, but the elimination of uncertainty through formal verification. The word survived, but its logic was reversed. These transformations not only redefined who or what could be trusted, but also what it meant to trust. In the traditional sense, trust was a subjective and graded disposition: A might trust B more than C, and such confidence could grow, decay, or be repaired. Within technical frameworks, by contrast, trust became an objective and absolute condition. To say that "A trusts B" now means that A possesses B's public key or accepts a certificate within a trust store —a state of configuration rather than conviction. The concept thereby loses its ordinal and experiential quality: one no longer trusts more or less, but simply does or does not. The subtle degrees of human reliance are compressed into a Boolean logic of authorization, where belief is replaced by compliance and assurance by attestation.

4. (Technological) Trust as a Legal Concept. - When law adopted the technical meaning of trust, the inversion deepened and spread. The European Directive 1999/93/EC on electronic signatures introduced the notion of certification-service providers and what it called "trusted" third parties, a terminology later consolidated in the eIDAS Regulation (910/2014) under the unified concept of Trust Service Providers (TSP). This framework established a model in which reliability was delegated to accredited intermediaries [18]. Many countries followed this pattern, translating the language of trust from engineering into law. Uruguay provides a particularly revealing example. Its Law 18.600 (2009) initially emphasized the principle of exclusive control of the private key by the signer —faithful to the original

[5] It's worth noting that computational security is often distinguished from unconditional security: the main difference is that unconditional security relies on mathematical principles to ensure invulnerability to any computational power, while computational security relies on the *difficulty* of solving computational problems for an attacker *using current technology*. For most practical problems, computational security is sufficient.

spirit of public-key cryptography, where the guarantee of authenticity depends precisely on the secrecy and non-delegability of that key [19]. However, in 2017, Law 19.535 amended the framework by adding Articles 31–33, which formally recognized TSPs and introduced the model of centralized key custody [20]. Article 31 created a Registry of TSPs within the national Certification Unit, authorizing them to offer services such as digital identification, timestamping, and the creation, verification, and validation of advanced electronic signatures with centralized custody. The same article obliges providers to "diligently safeguard the signer's key" —a formulation that, by avoiding the explicit phrase private key, leaves open whether legislators failed to grasp or deliberately ignored the contradiction: if a third party safeguards a private key, the key ceases to be private. Article 32 equates signatures performed under such centralized custody with the advanced electronic signature, granting them the same legal validity and effect. Article 33 further extends equivalence to digital identification mechanisms defined by the Certification Unit. In this way, what began as a framework grounded on individual cryptographic autonomy evolved into one of institutional delegation. A legal category of trusted providers thus emerged —entrusted not by personal confidence but by regulatory fiat. An engineering convention became a normative authority, reversing the logic of trust on which public-key infrastructures were originally founded. The concentration of such functions in accredited intermediaries marks a shift from decentralized verification to institutional monopoly over trust.

This transposition performs a double move. On the one hand, it borrows the aura of reliability from technical certification: if a system is "trusted" in engineering, it must be safe for legal purposes. On the other hand, it commands belief through legal authority: citizens must treat accredited providers as reliable by decree. What was once a description of protocol compliance becoming a prescription of civic confidence.

Our applied study shows the institutional consequences of this conflation. Analyzing Uruguayan TSPs under centralized key custody, we identified three systemic tensions:

Centralized custody vs. individual authorship. Centralized management of private keys contradicts the original principle of public-key cryptography —that only the signer controls the private key. One would not think it necessary to belabor this point, and yet, TSPs routinely hold and operate users' private keys. When a third party can sign "on behalf of" the user, authorship becomes legally presumed rather than technically guaranteed.

User flows and TLS dependence. Web-based signing often relies on Transport Layer Security (TLS) as a surrogate for trust, overlooking the fact that encrypted channels do not preclude compromise. TLS traffic can be intercepted by inspection proxies in controlled networks, but it can also be deciphered or replicated through other vectors —such as malware embedded in the user's browser that silently exfiltrates everything typed or displayed. In such conditions, the user's "intention to sign" becomes epistemically opaque: what the law presumes to be a legitimate and voluntary act may, in practice, be an instance of identity impersonation, not a genuine expression of will. We wish to be clear about what this study demonstrated. For a considerable period, it was theoretically possible for identity impersonations to occur by exploiting a combination of vulnerabilities and design decisions within the two TSPs accredited in Uruguay. While there is no public evidence of deliberate exploitation, comparable conditions may have existed or may still exist in other jurisdictions operating under similar centralized models of trust[6].

Fallback authentication paths. Many systems downgrade to weaker methods (e.g., password plus PIN) to improve accessibility. These exceptions erode the very assurances that justify the label "trusted."

From a historical-epistemological standpoint, these issues illustrate how the law reattaches the emotive force of trust to a framework that was originally meant to operate without it. The citizen is told to "trust" an infrastructure whose correctness depends on code and audit, not on virtue or intention. In many contexts, it is enforced and no alternative is provided. The result is an emotional surplus: the comforting word endures, but its referent has changed. The Uruguayan

[6] *These findings are based on the technical and legal analysis conducted in* "Let There Be Trust" *(2024), which examined the architecture and accreditation procedures of Uruguayan TSPs. The study identified theoretical vulnerabilities arising from the interaction between design decisions and regulatory assumptions. No evidence of actual exploitation was found, nor are such findings intended as allegations of misconduct.*

case thus condenses in miniature the broader epistemic inversion traced in this paper: law re-personalizes what technology had depersonalized, reattaching moral vocabulary to architectures of automation. What began as a security convention returns as a command of faith.

5. Discussion. - The genealogy of trust across moral, technical, and legal regimes exemplifies how categories migrate and mutate. What appears as continuity of language conceals a reconfiguration of knowledge and authority.

In moral life, trust is dialogical, fallible, and revocable. In technology, it becomes formal, testable, and binary. In law, it becomes prescriptive and hierarchical. The passage from one regime to another compress's judgment into verification and verification into compliance —a consequence not of deliberate design, but of the spontaneous evolution of technical practices seeking reliability. In this sense, the locus of trust migrated from the believing subject to the certified object —a shift from phenomenology to ontology, or from expectation to inscription. What was once a disposition of conscience becoming a property of systems, stored and turned executable in code.

To visualize this transformation, Table I summarizes the evolution of trust across the three regimes discussed in this study. Each regime redefines what counts as trust, the epistemic grounds on which it rests, and the kind of authority it legitimizes. The table makes explicit what the historical narrative implied: as the referential field shifts from lived experience to formal systems and then to legal frameworks, trust ceases to denote a relational practice and becomes a symbolic guarantee. Each regime retains traces of the previous one —experience informs design, design informs law— but the movement is one of abstraction and detachment. The table thus makes visible the semantic inversion at work: what began as belief under uncertainty ends as delegated certainty under regulation.

Regime	Referential Field	Form of Trust	Epistemic Basis
Traditional	Social / Moral	Learned, revocable confidence	Experience & reciprocity
Technical	Engineering / Cryptography	Designed reliability	Formal verification
Legal	Regulatory / Normative	Institutionalized assumption	Compliance & delegation

Table I. Genealogical evolution of the meanings of trust.

The conceptual trajectory outlined above invites a broader philosophical interpretation. This progression can also be read, following Feenberg, as the subsumption of moral judgment under technical rationality [21]. The translation of prudence into procedural control exemplifies what Ellul called technical rationality —a logic that replaces deliberation with operation and locates authority in artefacts rather than in virtue [22].

The persistence of emotive meaning. Following Stevenson —not in his emotivist ethics, but in his analysis of linguistic affect— the emotive meaning of trust —its tendency to produce positive affect— "clings tenaciously" to the word [8]. When legislators and standards bodies label a provider "trusted," they unconsciously reactivate this emotive charge. The label fuses two sources of legitimacy: (a) the moral warmth of social confidence, and (b) the technical aura of mathematical certainty. Together they generate what may be called the worst scenario for citizens: a command to trust backed by both ethical and epistemic authority. Doubt appears irrational, even disloyal.

Naming as performative act. As Ian Hacking reminds us, naming is never neutral. Categories do not merely describe the world; they organize practices and create new kinds of objects and people [23]. When the law adopts the technical term trust, it performs a double creation: it institutes the TSP as a legal actor and the trusting citizen as its correlative subject. What began as a convenience of language becomes a mechanism of governance.

Trust is also something learned —both individually and collectively. We acquire it through experience, through the success and failure of our expectations. In this sense, trust operates as a form of social learning: it evolves with practice, error, and correction. When transferred to technical or legal domains, however, this pedagogical dimension tends to

disappear. Yet law, as Aquinas already noted, has an instructive function: it teaches citizens not only what is permitted but also what is worthy of confidence [24]. In this broader sense, legal norms act as forms of testimony, signaling what a society should or should not trust [25].

Consequences and reform. The conflation of moral, technical, and legal trust affects accountability. When systems fail —through negligence or design flaws— responsibility disperses across opaque chains of certification. To correct this, both semantics and institutions must evolve toward greater proportionality between meaning and function.

Semantically, the label trusted should be replaced by descriptive attestations of assurance level and scope. Technically, systems should prioritize exclusive key control and auditable delegation over convenience-driven centralization. Legally, presumptions of authenticity should track what cryptographic proofs actually establish —that a key was used, not that a person intended its use. These reforms would restore proportion between words and realities.

6. Conclusion. - The historical trajectory of trust —from virtue to architecture to law— reveals a paradox at the heart of modern rationality. In seeking to eliminate uncertainty, we reproduce it under new forms. The systems built to automate belief still depend on belief in their operation; the laws written to enforce certainty still rely on trust in their interpreters. The dream of perfect assurance remains just that: a dream.

The technical redefinition of trust was not a conspiracy to remove judgment but an unintended consequence of attempts to formalize reliability. Yet once the law reimported the term, the consequences became political. By commanding citizens to “trust” infrastructures designed to make trust unnecessary, states combined the emotive resonance of moral virtue with the symbolic power of mathematics. The resulting hybrid —legalized trust— is both seductive and dangerous.

Recovering the relational and emotive dimensions of trust does not mean rejecting technology or law. It means acknowledging that trust cannot be decreed or computed; it must be earned —by people through conduct, by ideas through coherence, and by artifacts through transparent design. As Ferguson might put it, the most sophisticated systems remain products of human action, not of human design [26]. And as Hacking would remind us, the names we give them shape what we become capable of believing [23].

In the same way that we distinguish holographic signatures from digital signatures, we may start using digital trust (e-trust maybe) to avoid collisions on these abstractions, meaning and what to expect in the different identified contexts. In any case, to call something “trusted” is never innocent. It is a performative act that joins affect to authority. Recognizing this fact may be the first step toward disentangling the moral and technical strands of our digital infrastructures —and toward restoring the modest truth that no algorithm, however perfect, can relieve us of the burden of judgment. After all, there is no such thing as perfection in human things.

References

[1] N. Luhmann, Trust and Power. John Wiley & Sons, 2018.
[2] F. Fukuyama, Trust: The Social Virtues and the Creation of Prosperity. Free Press, 1995.
[3] J. Locke, The Second Treatise of Civil Government. Broadview Press, 2015.
[4] D. Hume, A Treatise of Human Nature. Oxford University Press, 2000.
[5] C. Menger, El dinero. Unión Editorial, 2013.
[6] C. Tilly, Trust and Rule. Cambridge University Press, 2005.
[7] J. Huerta De Soto, Money, Bank Credit, and Economic Cycles. Ludwig von Mises Institute, 2009.
[8] C. L. Stevenson, "The emotive meaning of ethical terms," in Logical Empiricism at Its Peak. Routledge, 2021, pp. 284–301.
[9] U.S. Department of Defense, Trusted Computer System Evaluation Criteria (TCSEC) (commonly known as the "Orange Book"). DoD Standard 5200.28-STD, National Computer Security Center, 1983.
[10] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.
[12] K. Thompson, "Reflections on trusting trust," Communications of the ACM, vol. 27, no. 8, pp. 761–763, 1984.
[13] J. G. Steiner, B. C. Neuman, and J. I. Schiller, "Kerberos: An Authentication Service for Open Network Systems," in Proceedings of the Winter USENIX Conference, 1988, pp. 191–202.
[14] ITU-T Recommendation X.509, Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, International Telecommunication Union, 1988.
[15] S. Kent, "Privacy Enhancement for Internet Electronic Mail: Part II – Certificate-Based Key Management," RFC 1422, Internet Engineering Task Force (IETF), February 1993.
[16] P. R. Zimmermann, The Official PGP User's Guide. MIT Press, 1995.
[17] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," in Proceedings of the IEEE Symposium on Security and Privacy (S&P), 1996, pp. 164–173.
[18] European Parliament and Council, "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures," 1999. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093. Accessed: 2025-10-13.
[19] República Oriental del Uruguay, "Ley N° 18.600: Documento Electrónico y Firma Electrónica Avanzada," 2009. Published in Diario Oficial on 21 September 2009. [Online]. Available: https://www.impo.com.uy/bases/leyes/18600-2009. Accessed: 2025-10-13.
[20] República Oriental del Uruguay, "Ley N° 19.535: Rendición de Cuentas y Balance de Ejecución Presupuestal Ejercicio 2016 (Artículo 28)," 2017. Published in Diario Oficial on 25 September 2017. [Online]. Available: https://www.impo.com.uy/diariooficial/2017/10/03/3 (carilla 7). Accessed: 2025-10-13.
[21] A. Feenberg, Questioning Technology. Routledge, 1999.
[22] J. Ellul, The Technological Society. A. A. Knopf, 1964 (orig. pub. 1954).
[23] I. Hacking, Historical Ontology. Harvard University Press, 2002.
[24] T. Aquinas, Summa Theologica, I–II, q. 95, a. 1.
[25] J. Lackey, Learning from Words: Testimony as a Source of Knowledge. Oxford University Press, 2008.
[26] A. Ferguson, An Essay on the History of Civil Society. Cambridge University Press, 1995 (original work published 1767).

Author contribution:
1. Conception and design of the study
2. Data acquisition
3. Data analysis
4. Discussion of the results
5. Writing of the manuscript
6. Approval of the last version of the manuscript

A.V. has contributed to 1, 2, 3, 4, 5 and 6.
A.S. has contributed to 1, 2, 3, 4, 5 and 6.

Acceptance Note: This article was approved by the journal editors Dr. Rafael Sotelo and Mag. Ing. Fernando A. Hernández Gobertti.