SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 7239-7245
Open Access. Online & Print

DOI: 10.5281/zenodo.19671556

THE RESILIENCE OF BANK GOVERNANCE IN THE ALGORITHMIC ERA: INTERNAL AUDIT BETWEEN SKILLS OBSOLESCENCE AND THE IMPERATIVE OF A HYBRID TRANSITION

ILLOUA AMANI Moctar, PhD Student[1*], EL BEKKALI Abdelhaq, Professor of higher education[1*]

Universiapolis - Université Internationale d'Agadir, Bab Al Madina, Qr Tilila, B.P. 8143, Agadir, Maroc, Affiliation ID: 60268804.

Received: 23/02/2026
Accepted: 01/04/2026

Corresponding Author: ILLOUA AMANI Moctar (Moctaramani@gmail.com)

ABSTRACT

This research examines the structural and paradigmatic mutation of the internal audit function in the face of the massive integration of distributed ledger technologies (Blockchain) and cognitive artificial intelligence (AI). Through an in-depth empirical analysis conducted on a targeted sample of n=156 decision-making professionals in the financial sector, this article highlights the legitimacy crisis currently faced by traditional control bodies, which are now confronted with the intrinsic opacity of automated systems. The quantitative results demonstrate that the obsolescence of auditors' technical skills is no longer merely an operational lag, but constitutes a direct systemic threat to bank governance and risk management. Drawing on continuous auditing and agency theories, this study conceptualizes and advocates for a radical hybridization of skills, coupled with an architectural overhaul of control frameworks, as a sine qua non condition to ensure the sustainability and ethics of institutions in an irreversible dematerialized financial ecosystem.

KEYWORDS: Internal Audit, Continuous Auditing, Blockchain, Artificial Intelligence, Skills Hybridization.

1. INTRODUCTION

The global banking and financial industry is currently undergoing a systemic mutation of unprecedented magnitude, characterized by an exponential dependence on algorithmic decision-making and the deployment of highly decentralized data architectures. As astutely highlighted by Gomaa et al. (2023), blockchain technology has definitively moved past the stage of a mere technophile niche innovation to establish itself as a distributed transactional database capable of redefining the very foundations of institutional trust.

By resolving the historical and costly problems of bank reconciliation through real-time shared ledgers, this technology disrupts the entire value chain of financial data. In this context of accelerated transformation, internal audit, which has historically established itself as the ultimate guarantor of security, compliance, and the fairness of financial statements, is colliding head-on with what we term the "digital wall." This conceptual wall represents the barrier, both cognitive and technical, that separates the classically trained auditor (primarily in accounting and finance) from the shifting, cryptographic reality of modern financial flows.

The paradox currently striking audit committees is striking: the more banking information systems become high-performing, agile, and capable of processing millions of transactions per nanosecond, the more internal control mechanisms seem to stagnate in analog paradigms inherited from the sampling practices of the 20th century. This asymmetry in velocity creates a vast operational gray area where algorithmic risks, such as credit scoring biases or conditional logic errors buried within smart contracts, can proliferate silently and without adequate supervision.

The transition towards advanced blockchain architectures certainly promises the cryptographic immutability of ledgers and absolute transactional transparency, but this promise cannot be institutionally kept without a strategic alignment of the human capital tasked with monitoring it. Internal audit must imperatively undergo a philosophical and methodological metamorphosis: shifting from an a posteriori verification function based on past anomalies to an a priori systemic supervision function, capable of interrogating and validating the software source code just as rigorously as the traditional general ledger (Appelbaum, Kogan, & Vasarhelyi, 2018).

The emergence and democratization of smart contracts further complicate and densify this control landscape. These computer protocols, which execute entirely autonomously when predefined mathematical or temporal conditions are met on a blockchain, are not merely harmless lines of code; they are, in essence, legal and financial commitments endowed with intrinsic executory force (Rozario & Thomas, 2019).

This software autonomy requires the auditor to transcend their role as a censor to become a true "auditor-technician," capable of evaluating the robustness of a decentralized architecture. The objective of this article is to demonstrate that technology, however powerful and disruptive it may be, cannot replace critical and professional human judgment, but must instead augment it through new, comprehensive digital literacy.

Faced with regulatory authorities (central banks, market authorities) increasingly equipped with advanced analytical tools known as Sup Tech (Supervisory Technology), the bank internal audit function can no longer afford to lag behind in institutional digitalization. Furthermore, the exponential cost of non-compliance and the proliferation of increasingly sophisticated cyberattacks compel executive boards to entirely rethink their extreme risk mapping.

A devastating attack on a decentralized finance protocol very often manifests itself through the subtle exploitation of a logical flaw in a smart contract vulnerability that traditional audit matrices, focused on classic access rights, and conceptually lack the capacity to detect (Sheldon, 2019). By rigorously exploring the widening gap between the relentless demands of algorithmic finance and the actual, measured skills of control departments, this article theorizes skills hybridization as the sole survival and legitimization mechanism for a profession currently teetering on the edge of obsolescence and hyper-automation.

2. LITERATURE REVIEW

2.1. Evolution of ledger technologies and the single truth paradigm

Contemporary academic literature generally agrees on segmenting technological evolution into several distinct phases, each impacting the theory and practice of the accounting function differently. While early conceptual work on blockchain merely debated, not without skepticism, the capacity of distributed ledgers to serve a genuine and rigorous accounting purpose (Coyne & McMickle, 2017), current research paradigms have resolutely shifted towards studying real-world, large-scale implementation.

The seminal work of Gomaa et al. (2023)

convincingly demonstrates that blockchain enables the creation of an ecosystem based on a "single truth" (Single-ledger entries). This involves a unique ledger entry, shared and validated simultaneously by multiple stakeholders, which effectively eradicates the structural problem of data reconciliation across departmental silos. For internal audit, this upheaval means that the traditional "audit trail" is no longer a linear chronological sequence of paper documents, but a pristine cryptographic chain requiring the deployment of entirely new algorithmic verification methodologies.

2.2. Smart contracts, audit by design, and automation

The native integration of smart contracts undeniably represents the new technological frontier in the automation of the audit function. Recent research by Guo, Zuo, & Li (2024) has empirically proven that complex and specific audit rules can now be coded and embedded directly into the architecture of smart contracts.

This approach, often referred to as Audit by Design, allows for the near real-time identification and blocking of suspicious transactions, flow anomalies, and common fraud schemes, even before the financial impact materializes. However, this extreme automation, as also theorized by Rozario & Thomas (2019), fundamentally reorganizes the value chain of the audit process. It irrevocably shifts the auditor's focus away from the tedious manual verification of supporting documents towards evaluating the architectural and semantic integrity of the underlying code.

2.3. Agency theory revisited by digital asymmetry and technological capture.

In the foundations of classical agency theory, the auditor intervenes to reduce the information asymmetry between the principal (the shareholders) and the agent (the management) by acting as an absolute trusted third party. However, the integration of complex algorithms introduces a new, particularly pernicious form of asymmetry: the one that arises between the IT system designer (data scientists and developers) and the financial auditor tasked with evaluating it.

As indicated and lamented by Betti & Sarens (2021), this asymmetry in technical knowledge creates a major risk of "technological capture." In this configuration, internal auditors, overwhelmed by the mathematical complexity of the models, end up validating the compliance of opaque systems out of blind dependence on IT experts. This structural dependence significantly weakens the critical independence that is consubstantial to the profession.

2.4. Big data, continuous auditing integration, and the RPA boundary

The absolute necessity of integrating advanced and comprehensive analytical procedures into the normative audit framework has been extensively documented. The work of Kuusinen, Hanna; Miettinen, Veera (2023) strongly emphasizes that Big Data integration is no longer an option, but a fundamental building block for proactive risk assessment.

This massive data ingestion capacity facilitates the long-awaited transition to continuous auditing, a theoretical concept powerfully defended by Eulerich & Kalinichenko (2018). These authors advocate for the definitive abandonment of periodic sampling in favor of exhaustive tests covering 100% of data populations, analyzed in real-time. Furthermore, academic literature requires drawing a clear conceptual distinction: Robotic Process Automation (RPA), which merely mimics human workflows based on strict rules (Moffitt, Rozario, & Vasarhelyi, 2018), must not be confused with advanced cognitive AI, which requires auditors capable of deconstructing probabilistic weights and unsupervised learning.

2.5. Ethical implications, algorithmic biases, and cybersecurity vulnerabilities

A critical dimension of this transition concerns the profoundly ethical and security-related implications of algorithmic auditing. Researchers Munoko, Brown-Liburd, & Vasarhelyi (2020) vigorously argue that delegating audit decisions to AI introduces major ethical dilemmas, particularly regarding the integration of latent discriminatory biases in Machine Learning and the lack of explanatory transparency. Concurrently, the study by No & Vasarhelyi (2017) demonstrates that cybersecurity has definitively left the exclusive perimeter of IT departments; internal auditors must now actively participate in the strategic evaluation of cybersecurity frameworks. Nevertheless, institutional resistance to this redefinition of roles remains tenacious. As aptly noted by Salah Ahmed Oraby (2024), the paradigm shift induced by blockchain disintermediation clashes daily with significant organizational inertia.

3. RESEARCH HYPOTHESES AND CONCEPTUAL MODELING

To move beyond mere theoretical observation, this empirical research was designed to test the statistical validity of the following hypotheses:

- H1: The proven obsolescence of bank internal auditors' technical skills is positively and significantly correlated with a measurable increase in undetected operational risk during compliance missions.
- H2: The intensity of resistance to technological and methodological change within audit departments is inversely proportional to the volume (in hours) and quality of continuous training in data science invested by the institution.
- H3: The perception of the internal auditor's legitimacy and authority by other business lines (Front-office, IT) is now directly dependent on their demonstrated technical mastery of the algorithmic tools deployed by the bank.

3.1. Research Methodology And Sample Parameters

To guarantee the rigor and external validity of our results, the study deploys a strict quantitative approach, based on a targeted and qualified sample of n=156 high-level professionals working in the banking and financial sector (Senior Auditors, Audit Managers, General Inspectors, and Chief Audit Executive - CAE). This deliberate restriction avoids dilution biases associated with responses from back-office employees not involved in complex risk control strategies.

The internal consistency reliability of our measurement instrument (a structured questionnaire on a 5-point Likert scale), evaluated by Cronbach's Alpha coefficient, displays a very solid score of \alpha = 0.89, attesting to the excellent consistency of the items. The methodological choice to limit to 156 respondents relies on a purposive sampling technique, exclusively targeting executives of systemic institutions currently engaged in massive digital transformation projects. All raw data processing was performed in the R statistical environment. The statistical significance threshold was strictly set at $p < 0.05$.

3.2. Detailed Analysis of Results: Internal Audit Facing The "Digital Divide"

The purely descriptive analysis of the collected data immediately reveals a particularly alarming structural flaw. Although 88% of respondents agree that blockchain and AI irreversibly redefine the ontology of their profession, only 14% of them declare themselves tangibly capable of planning and conducting an information system audit based on a distributed ledger without resorting to external IT assistance.

3.3. Pearson Correlation Matrix Modeling and Interpretation

We generated a Pearson correlation matrix to scientifically evaluate the cross-relationships between four fundamental latent variables : the measured level of continuous technical training (IT Training), the declared and evaluated capacity to detect complex algorithmic operational risks (Risk Detection), the perceived professional legitimacy within the bank (Legitimacy), and the index of resistance to new audit methodologies (Resistance).

Table 1: Pearson Correlation Matrix (n=156).

Variables	1. IT Training	2. Risk Détection	3. Legitimacy	4. Resistance
1. IT Training	1			
2. Risk Détection	0.68	1		
3. Legitimacy	0.54	0.61	1	
4. Resistance	-0.49	-0.38	-0.42	1

The statistical results unambiguously confirm the validity of hypothesis H1. There is a strong, highly significant positive correlation ($r = 0.68$, $p < 0.01$) between the intensity of the auditor's specific technical training and their ability to identify complex systemic risks buried in the code. Furthermore, organizational resistance to change shows a strong negative correlation with the level of IT training ($r = -0.49$), thereby validating hypothesis H2.

3.4. Analysis of variance (ANOVA) and measuring the impact of hybridization

To move beyond simple correlation and measure whether the performance gap in detecting algorithmic anomalies is statistically different depending on the auditor's initial academic background (Pure Accounting/Finance Profile vs. Hybrid Profile combining Finance and IT/Data Science), we conducted a one-way ANOVA.

Table 2: ANOVA Results - Detection Rate by Auditor Profile.

Source of variation	Sum of Squares (SS)	Degrees of Freedom (df)	Mean Square (MS)	F-value	P-value
Between Groups	412.35	1	412.35	45.82	$p < 0.001$
Within Groups (Error)	1385.12	154	8.99		
Total	1797.47	155			

Examining the ANOVA test confirms that the between-group variance is spectacularly significant with an F-value of 45.82 and $p < 0.001$. These figures irrefutably demonstrate that skills hybridization is not an abstract concept, but a predominant explanatory variable for the internal audit's capacity to secure the banking ecosystem. Auditors with a hybrid profile vastly outperform their classically trained counterparts in identifying, qualifying, and remediating algorithmic risks, fully justifying hypothesis H3.

4. DISCUSSION

Putting our quantitative results into perspective with the academic literature allows us to assert that skills hybridization is, to date, the only viable strategic path to guarantee the long-term resilience of bank governance. A "hybrid" auditor is not a software developer who does accounting, but rather an expert in global finance endowed with sufficient analytical background to converse as equals with artificial intelligence and the engineers who design them.

As aptly raised by Munoko, Brown-Liburd, & Vasarhelyi (2020), the profound ethical implications of using AI in audit processes require the establishment of a humanistic governance framework, where the human auditor retains their role as the ultimate moral supervisor. The spectacular results of our ANOVA prove mathematically that this supervision is pure fiction if it is not supported by a granular technical competence allowing the supervisor to understand what is being supervised.

This discussion must imperatively address the fundamental concept of "sovereignty of control." By choosing, out of convenience or lack of internal skills, to delegate the validation of their systems to "black box" off-the-shelf software or external IT consulting firms, banks effectively outsource the mastery of their own governance.

Internal audit must urgently reclaim this algorithmic sovereignty by actively involving itself in the very design of decentralized systems. As brilliantly demonstrated by Guo, Zuo, & Li (2024), the integration of audit rules directly into the core of smart contracts requires auditors to be integrated into project teams from the initial coding phase (Audit by Design), thus modifying their historical status as post-mortem verifiers to become co-architects of compliance.

Furthermore, in a financial environment where credit granting, client risk assessment, and high-frequency trading are massively delegated to machines, the mission of the hybrid auditor takes on an unprecedented societal dimension. They must ensure, through algorithmic stress tests, that machine learning models do not reproduce or amplify discriminatory biases. Institutional resilience is therefore no longer confined to the strict technical cybersecurity of the IT infrastructure (No & Vasarhelyi, 2017); it now encompasses Corporate Social Responsibility (CSR). Audit thus establishes itself as the ultimate guarantor of the financial institution's digital ethics.

4.1. Recommendations

- Faced with the imminence of an irreversible technological tipping point for the global financial system, boards of directors and audit committees must transcend mere statements of intent and adopt proactive, structural, and budgeted measures:
- Radical Curriculum and Recruitment Overhaul: Massively integrate data science, proficiency in exploratory analysis using Python/R, Solidity coding for smart contracts, and cybersecurity engineering into the prerequisites for CPA and internal audit certifications.
- Effective Transition to Continuous Auditing: By appropriating the foundational work of Eulerich & Kalinichenko (2018), abandon the obsolete culture of periodic statistical sampling in favor of analytical command centers ensuring 100% automated and exhaustive real-time monitoring.
- Creation of Algorithmic Ethics Cells: Banks must institutionalize independent control protocols dedicated exclusively to auditing cognitive AIs to prevent any drift related to discriminatory biases in automated decision-making.
- Restoration of Control Sovereignty: Prioritize the development of internal and proprietary

analytical audit tools. Only total mastery of the verification code allows for the maintenance of absolute independence from technological providers.

5. CONCLUSION

The massive integration of blockchain technology and artificial intelligence within financial architectures does not constitute a mere incremental evolution of IT tooling; it represents a paradigmatic rupture that shakes the epistemological and operational foundations of internal audit. This research has endeavored to demonstrate, through a rigorous empirical analysis conducted on 156 decision-making professionals, that the gap between the velocity of algorithmic systems and the stagnation of traditional control skills generates a major systemic vulnerability.

The quantitative results of our study unequivocally confirm our initial hypotheses: the technical obsolescence of auditors is directly correlated with a critical inability to detect complex risks, thereby paving the way for a dangerous "technological capture" by system designers.

Furthermore, the analysis of variance (ANOVA) made it possible to irrefutably quantify the redeeming impact of skills hybridization. The classically trained auditor, confined to a posteriori documentary verification, is condemned to validate "black boxes" whose probabilistic weightings and feedback loops they do not understand.

Conversely, the hybrid auditor, equipped with advanced digital literacy encompassing data science and an understanding of smart contract architecture, succeeds in restoring the information asymmetry inherent to agency theory. They thus become capable of transitioning towards a model of continuous auditing and Audit by Design, guaranteeing the sovereignty of institutional control.

Nevertheless, like any scientific endeavor, this research presents certain limitations inherent to its methodological design. The sampling choice, although relevant for targeting expert profiles, focuses on a restricted size (n=156) and a specific banking sector undergoing transformation. Moreover, the measurement of technical skills relies partly on declarative data, which can induce a social desirability bias, even though the anonymity guaranteed during data collection aims to minimize it.

These limitations constitute stepping stones for future academic investigations. It is now crucial for the community of accounting and management control researchers to broaden this field of study. Future research could lean towards longitudinal studies measuring the actual Return on Investment (ROI) of audit departments that have completed their hybridization.

Furthermore, the imminent emergence of quantum computing, capable of breaking the current cryptographic standards of blockchain, opens a new front of vulnerability that will require, very soon, rethinking the matrices of information systems auditing once again. Ultimately, this study reaffirms a timeless truth of governance: the resilience of an institution in the face of hyper-automation does not lie in blind delegation to algorithms, but in the continuous elevation of the critical consciousness and human expertise tasked with governing them.

REFERENCES

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2018). Analytical procedures in external auditing: A comprehensive literature survey and framework for external audit analytics. Journal of Accounting Literature, 40, 83-101. https://doi.org/10.1016/j.acclit.2018.01.001

Betti, N., & Sarens, G. (2021). Understanding the internal audit function in a digitalised business environment, Journal of Accounting & Organizational Change., 17 (2): 197–216. https://doi.org/10.1108/JAOC-11-2019-0114

Coyne, J. G., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? Journal of Emerging Technologies in Accounting, 14(1), 101-111. https://doi.org/10.2308/jeta-51910

Eulerich, M., & Kalinichenko, A. (2018). The Current State and Future Directions of Continuous Auditing Research: An Analysis of the Existing Literature. Journal of Information Systems, 32(3), 31-51. https://doi.org/10.2308/isys-51813,

Gomaa, A. A., et al. (2023). The Creation of One Truth: Single-Ledger Entries for Multiple Stakeholders Using Blockchain Technology to Address the Reconciliation Problem Journal of Emerging Technologies in Accounting, 20(1), 1-17

Guo, X., Zuo, Y., & Li, D. (2024). When auditing Meets Blockchain: A study on applying blockchain smart contracts in auditing. International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2025.100730.

Kuusinen, Hanna; Miettinen, Veera (2023) The Role of Data Analytics in Audit Risk Assessment.

https://urn.fi/URN:NBN:fi-fe2023050741634
Moffitt, K. O., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. Journal of Emerging Technologies in Accounting, 15(1), 1-10. https://doi.org/10.2308/jeta-10589
Munoko, I., et al. (2020). The ethical implications of using artificial intelligence in auditing. Journal of Business Ethics, 167(2), 209-234.
No, W. G., & Vasarhelyi, M. A. (2017). Cybersecurity and Continuous Assurance. Journal of Emerging Technologies in Accounting, 14(1), 1–12. https://doi.org/10.2308/jeta-10539
Rozario, A. M., & Thomas, C. (2019). Reengineering the audit with blockchain and smart contracts. Journal of Emerging Technologies in Accounting, 16(1), 21-35. https://doi.org/10.2308/jeta-52432
Salah Ahmed Oraby (2024). The Impact of Blockchain Technology on Accounting and Auditing, Functions: Evidence from Saudi Arabia. Pakistan Journal of Life and Social Sciences,
Sheldon, M. D. (2019). A primer for information technology general control considerations on a blockchain. Current Issues in Auditing, 13(1), A15-A29. https://doi.org/10.2308/ciia-52356