International Journal of Innovative Inventions in Social Science and Humanities

ISSN(print): 3050-6921, ISSN(online): 3050-693X

Volume 03 Issue 08 August 2026

DOI: 10.58806/ijiissh.2026.v3i8n08

Page No: 1003-1009

Beyond Verification: How Blockchain Technology Challenges the Future Role of External Auditors

Dr. Gaduga Godwin, Esq

Lecturer at Accra Institute of Technology Adjunct Lecturer at Blue Crest University College

ABSTRACT

Blockchain technology records transactions on a distributed ledger that is cryptographically chained, replicated across independent nodes, and validated by consensus rather than by any single institution. Because the technology verifies that recorded transactions occurred and have not been altered, some commentators have concluded that it will make external auditors redundant. This article rejects that conclusion but takes the underlying disruption seriously. It argues that blockchain automates a narrow and historically labor-intensive slice of the audit, namely the verification of the existence, occurrence, and mathematical accuracy of recorded transactions, while leaving untouched the components of assurance that depend on professional judgment: valuation, accounting estimates, classification, completeness of off-chain events, related party identification, and going concern assessment. At the same time, the technology creates new objects that require assurance, including consensus protocols, cryptographic key management, smart contract code, and the oracles that connect ledgers to the physical world. The article examines the consequences for auditing standards, particularly the treatment of blockchain records as audit evidence, and for the education, skills, and business model of the profession. The external auditor's future role, it concludes, lies not in verifying transactions but in assuring the systems that now verify them, and in exercising the judgment that no ledger can encode.

ARTICLE DETAILS

Published On:
15 August 2026

KEYWORDS: Blockchain, External Audit, Assurance, Distributed Ledger Technology, Smart Contracts, Audit Evidence, Professional Judgment.

Available on:
https://ijiissh.com/

1. INTRODUCTION

Every few decades, a technology arrives that is said to make the external auditor unnecessary. Computerized bookkeeping was supposed to do it in the 1970s. Enterprise resource planning systems were supposed to do it in the 1990s. The claim has returned with unusual force in the case of blockchain, and this time it has a superficially compelling logic. If a transaction is validated by a decentralized network of computers, recorded on a ledger that no single party can alter, and visible to every participant in real time, what exactly is left for the auditor to verify? Proponents of the technology have described distributed ledgers as machines for producing trust without intermediaries (Casey & Vigna, 2018; Tapscott & Tapscott, 2016), and the external auditor is, on one reading, precisely the kind of trust intermediary the technology was designed to replace.

The auditing literature has responded to this provocation with a decade of scholarship that is now substantial enough to synthesize. Early conceptual work mapped the technology onto accounting and assurance processes and asked which audit procedures a shared ledger would render redundant (Dai & Vasarhelyi, 2017; Kokina et al., 2017). A more skeptical strand asked whether blockchains can serve an accounting purpose at all, given that a ledger can guarantee only the integrity of its own records and not their correspondence with economic reality (Coyne & McMickle, 2017). Later work turned to research agendas (Schmitz & Leoni, 2019), to the fit between the technology and existing auditing standards (Gauthier & Brender, 2021), and to systematic reviews of a literature that had grown quickly but unevenly (Han et al., 2023; Lombardi et al., 2022). Professional bodies produced their own assessments, generally concluding that the technology would transform rather than eliminate the audit (CPA Canada et al., 2017; Institute of Chartered Accountants in England and Wales [ICAEW], 2018).

This article builds on that literature but sharpens its central claim. The argument proceeds in three steps. First, blockchain genuinely automates part of the audit. The verification of recorded transactions, which has consumed a large share of audit fieldwork since the profession took its modern form, becomes largely mechanical when transacting parties share a single validated ledger.

Confirmations, reconciliations, and vouching of on-chain transactions lose much of their point. Second, and less comfortably for the technology's enthusiasts, the parts of the audit that blockchain cannot touch are the parts that were always hardest. A ledger cannot tell an auditor whether inventory recorded at cost is impaired, whether a receivable will be collected, whether a smart contract executed a transaction that lacked economic substance, or whether an entity will still exist in twelve months. Immutability, the technology's signature property, cuts both ways: a fraudulent entry validated onto a chain is preserved with the same cryptographic permanence as an honest one. Third, blockchain creates new things that need auditing. Consensus mechanisms, key custody arrangements, smart contract code, and the oracles that feed external data onto chains are all points at which assurance can fail, and none of them can be assessed without the auditor.

The phrase in the title, beyond verification, is meant in two senses. The audit profession must move beyond transaction verification because technology is absorbing that function. But assurance itself has always extended beyond verification, and the profession's survival depends on recognizing that its economic value never rested solely on ticking and checking. Power (1997) observed that the audit explosion of the late twentieth century was driven less by the mechanics of checking than by society's demand for rituals of comfort performed by credible, independent professionals. Blockchain changes the mechanics. It does not, by itself, satisfy the demand.

The article is organised as follows. Section 2 describes the technology in the terms that matter for assurance, distinguishing permissionless from permissioned architectures. Section 3 reconstructs the verification core of the traditional audit. Sections 4 and 5 examine, respectively, what blockchain automates and what it cannot verify. Section 6 identifies the new assurance objects the technology creates. Section 7 assesses the fit with existing auditing standards. Section 8 draws out the implications for professional skills, education, and the audit business model, with attention to the position of auditors in emerging economies. Section 9 concludes.

2. THE TECHNOLOGY, DESCRIBED FOR ASSURANCE PURPOSES

A blockchain is a ledger with three properties that distinguish it from a conventional database. It is distributed, meaning that identical copies are held by multiple independent nodes rather than by one custodian. It is append-only and cryptographically chained, meaning that each block of transactions incorporates a hash of the previous block, so that altering any historical record would change every subsequent hash and expose the tampering. And it is validated by consensus, meaning that new transactions are accepted onto the ledger only when the network's nodes agree, according to a defined protocol, that they are legitimate (Nakamoto, 2008). The practical consequence is that the ledger's integrity does not depend on trusting any single record keeper. Trust is placed instead in mathematics and in the assumption that a majority of validating power is honest.

Two design distinctions matter greatly for auditing, and much confusion in the popular debate stems from ignoring them. The first is the distinction between permissionless and permissioned chains. Bitcoin and Ethereum are permissionless: anyone may run a node, validate transactions, and read the ledger. Corporate deployments are almost invariably permissioned: a defined consortium of participants, for example a group of banks or the members of a supply chain, operates the nodes, and access is controlled. Liu et al. (2019) show that the two architectures present sharply different audit risk profiles. Permissionless chains achieve strong tamper resistance through the sheer scale and dispersion of their validating networks, but they expose transaction data publicly and offer no governance counterparty for the auditor to assess. Permissioned chains offer confidentiality and identifiable governance, but their consensus is only as trustworthy as the small group of institutions that operate the nodes, and a small group can collude.

The second distinction is between the ledger and the programmes that run on it. Smart contracts are pieces of code deployed on a blockchain that execute automatically when specified conditions are met (Szabo, 1997). A smart contract might release payment when a shipping oracle confirms delivery, or transfer collateral when a price feed crosses a threshold. Smart contracts are what make blockchains interesting for accounting, because they turn the ledger from a passive record into an active participant in transactions. They are also a distinct source of risk, because code can contain errors, and code that executes automatically executes its errors automatically as well (Rozario & Vasarhelyi, 2018).

One further clarification is needed. Blockchain records are better described as tamper-evident than as immutable. History can in principle be rewritten on a permissionless chain by an actor controlling a majority of validating power, and on a permissioned chain by agreement among the consortium. These are not theoretical curiosities. Majority attacks have been executed against smaller permissionless networks, and consortium governance rules typically contain provisions for correcting the ledger. The auditor who treats a blockchain record as unconditionally permanent has substituted a slogan for an assessment of control risk. What the technology actually offers is a very high, but measurable and architecture-dependent, cost of undetected alteration.

3. THE VERIFICATION CORE OF THE TRADITIONAL AUDIT

To see what blockchain threatens, one must be precise about what auditors do. The objective of a financial statement audit is to obtain reasonable assurance that the statements are free from material misstatement, and the auditor pursues that objective by testing management's assertions: that recorded transactions occurred, that all transactions that should have been recorded were recorded, that amounts are accurate, that transactions fall in the correct period, that assets exist and are controlled by the entity, that they are valued appropriately, and that everything is properly classified and presented. The International Standards on Auditing organise the

evidence-gathering effort around these assertions, and International Standard on Auditing (ISA) 500 requires the auditor to obtain sufficient appropriate evidence in support of them (International Auditing and Assurance Standards Board [IAASB], 2009).

In practice, a large fraction of fieldwork hours has always gone to a subset of these assertions: existence, occurrence, and accuracy. Junior auditors vouch recorded sales to invoices and shipping documents. Teams circularize banks and debtors to confirm balances. Reconciliations are performed between subsidiary ledgers and control accounts, between the entity's records and its counterparties' statements, between what was recorded and what the documents say happened. Sampling theory exists in auditing largely because complete verification of transactions was economically impossible, so the profession developed disciplined ways of examining a fraction and inferring the whole. This is the ticking and checking of professional folklore, and it is genuinely valuable work: it is how auditors have historically detected fictitious revenue, unrecorded liabilities, and simple error.

It is also, and this is the point, work whose value depends on a specific institutional fact: that each party to a transaction keeps its own records, and that those records can disagree. Double-entry bookkeeping disciplines a single entity's books internally, but nothing in conventional accounting infrastructure disciplines the relationship between one entity's books and another's. The auditor stands in that gap. Confirmation and reconciliation are meaningful precisely because the buyer's ledger and the seller's ledger are separate documents that might tell different stories. Remove the separateness, and much of the verification apparatus loses its object.

4. WHAT BLOCKCHAIN AUTOMATES

That is exactly what a shared ledger removes. When transacting parties record their dealings on a common blockchain, there are no longer two sets of books to reconcile. There is one record, validated at the moment of the transaction by a mechanism that neither party controls. Dai and Vasarhelyi (2017) describe this as the practical realization of triple-entry accounting: alongside each party's internal debit and credit sits a third, shared, cryptographically sealed entry that both are bound by. For transactions living on such a ledger, several familiar audit procedures become redundant or trivial. Confirmation letters to counterparties add nothing, because the counterparty's record is by construction identical. Reconciliations between the entity's ledger and the shared ledger can be performed by software continuously rather than by staff annually. Tests of mathematical accuracy are pointless where the validating protocol rejects arithmetically inconsistent entries.

Two further consequences follow. The first is the collapse of the sampling rationale for on-chain populations. Sampling was a concession to cost; when the entire transaction population is available in structured, machine-readable form on a ledger whose integrity is cryptographically assured, the auditor can test all of it. This continues a trajectory that predates blockchain, since the availability of complete digital populations was already pushing the profession from sampling toward full-population analytics (Alles, 2015). Blockchain strengthens the trajectory by adding integrity assurance to availability: the data is not only complete but demonstrably unaltered since recording.

The second consequence is temporal. An audit performed months after year-end is an artefact of evidence that had to be assembled, requested, and cross-checked. Where evidence is validated at the moment of the transaction, assurance can in principle be contemporaneous with the events it covers. Rozario and Vasarhelyi (2018) propose external audits built on smart contracts that execute audit tests automatically as transactions occur, flagging exceptions in real time and reserving human attention for what the rules cannot resolve. The joint report by CPA Canada, the American Institute of Certified Public Accountants, and the University of Waterloo reaches a similar conclusion: routine verification will increasingly be embedded in the transaction infrastructure itself, and the audit will reorganize around what remains (CPA Canada et al., 2017).

It would be a mistake to minimize the disruption this represents. Verification of recorded transactions is not a marginal audit activity; it is the activity around which audit methodology, staffing pyramids, and fee structures were built. Bonsón and Bednárová (2019) are right that the effect of widespread blockchain adoption on audit economics would be considerable, and the honest starting point for the profession is to concede that a real and substantial category of its historical work is being absorbed by infrastructure.

5. WHAT BLOCKCHAIN CANNOT VERIFY

The concession, however, has limits, and they are not incidental limits. They follow from what a ledger is. A blockchain validates that a recorded transaction is internally consistent, properly authorized by the relevant private key, and unaltered since recording. It cannot validate that the transaction corresponds to anything in the world. Coyne and McMickle (2017) put the objection early and precisely: a blockchain can ensure the integrity of its records, but it cannot ensure that those records were true when made. If a supplier records the delivery of goods that never left the warehouse, the chain will preserve that falsehood with perfect fidelity. The problem the profession has always called garbage in, garbage out is not solved by the technology. It is entrenched by it, because the garbage, once validated, becomes tamper-evidently permanent.

Consider where financial statement fraud actually lives. Fictitious revenue schemes typically involve genuine-looking documentation created by people with authority to create it. Management override, the fraud risk that auditing standards treat as present in every engagement, operates through the legitimate channels of the accounting system. On a blockchain, a manager with control of the entity's private keys is simply a user whose transactions validate. Collusion between counterparties, the classic defeat of the confirmation procedure, works even better on a shared ledger, because the colluding parties now jointly author a single

authoritative record instead of maintaining two records that an auditor might find inconsistent. Blockchain relocates fraud risk from the alteration of records, where the technology is strong, to the creation of records, where it is silent (Schmitz & Leoni, 2019).

Next, and decisively, there is valuation. The assertions that consume senior audit judgment are not existence and occurrence but valuation, estimation, and presentation. Whether a loan book is adequately provisioned, whether goodwill is impaired, whether inventory will sell above cost, whether a legal claim requires a provision, whether revenue from a long-term contract has been recognized in the right pattern: none of these questions is about what the ledger says. They are about what the future holds and what accounting standards mean, and they are answered with models, assumptions, and professional judgment. A blockchain records that an asset was acquired for a given consideration. It has nothing to say about what the asset is worth at the reporting date. As Yermack (2017) notes in the governance context, distributed ledgers change the observability of transactions, not the economics of the positions they create.

Third, completeness fails in a new way. The completeness assertion asks whether everything that should be in the ledger is in the ledger. A blockchain can demonstrate the completeness of its own history, but it cannot know about transactions conducted off it. An entity that transacts partly on-chain and partly off, which describes essentially every real entity for the foreseeable future, presents the auditor with a boundary problem: the chain is complete about itself and silent about everything else. Side agreements, off-ledger arrangements, and unrecorded liabilities remain exactly as invisible to a blockchain as they were to a bound ledger book.

Finally, there is the gap between cryptographic control and legal reality. Possession of a private key demonstrates the ability to transact with an asset. It does not demonstrate ownership in law. Keys can be held by custodians, shared within syndicates, stolen, or controlled by parties acting as nominees. The rights and obligations assertion, in other words, survives tokenization intact, and in some respects becomes harder, because the auditor must now connect a cryptographic fact to a legal one across systems that were not designed to speak to each other. Ghanaian law, to take one example the author knows well, gives legal recognition to electronic records through the Electronic Transactions Act, 2008 (Act 772), but recognition of a record is not adjudication of title, and no statute anywhere yet makes a ledger entry conclusive of beneficial ownership.

6. THE NEW OBJECTS OF ASSURANCE

If Section 5 described what blockchain leaves for auditors, this section describes what it adds. The technology does not merely shrink the audit; it relocates audit risk into new components, each of which someone must assess, and none of which management can credibly assess for itself.

The first is the consensus mechanism. The reliability of every record on a chain rest on the protocol by which nodes agree, and that protocol has an attack surface. On permissionless chains, the auditor must consider the concentration of validating power and the economic feasibility of majority attacks, which is a live question for smaller networks. On permissioned chains the question is starker and more familiar: who operates the nodes, under what governance agreement, with what provisions for amending history, and with what independence from the audited entity? A consortium chain operated by five subsidiaries of the client is, for assurance purposes, barely distinguishable from the client's own database, whatever its cryptographic dressing. Sheldon (2019) shows that the information technology general controls framework extends naturally to permissioned chains, but the extension requires the auditor to evaluate controls that sit outside the client, in the consortium and its technology providers, which raises questions of access and of the division of assurance labour that current practice has not settled. Smith and Castonguay (2020) make the broader governance point: the reliability of a consortium ledger is a product of the consortium's rules, and evaluating those rules is assurance work of a kind boards and audit committees are only beginning to demand.

The second is key management. Private keys are the sole instrument of authorization on a blockchain, which makes their custody the single most concentrated control in the system. Keys held on network-connected devices can be exfiltrated; keys held in cold storage can be lost; keys held by third-party custodians import the custodian's entire control environment into the client's risk profile. Appelbaum and Nehmer (2020) examine the compounding case, now the commercial norm, in which the blockchain itself is hosted on cloud infrastructure, so that the auditor confronts layered service providers, each with its own controls, beneath the ledger it is asked to rely on.

The third is smart contract code. When contractual performance is automated, the code is the transaction cycle, and errors in it are control deficiencies that execute themselves at machine speed. Assurance over smart contracts requires reading code, or reading the work of specialists who read code, and forming a view on whether the logic implements the commercial agreement and the applicable accounting treatment. The auditor must also grasp that deployed contracts are frequently unmodifiable, so that a discovered flaw cannot simply be patched, and the population of affected transactions may already be validated and final (Rozario & Vasarhelyi, 2018; Vincent et al., 2020).

The fourth is the oracle. Smart contracts act on external facts, prices, deliveries, temperatures, defaults, only as those facts are reported to the chain by oracles. The oracle is therefore the point at which the tamper-evident world of the ledger depends on the ordinary, corruptible world of data feeds. An attacker who cannot alter the chain does not need to; corrupting the input that the contract trusts achieves the same result. Oracle assurance, meaning evidence about the reliability, independence, and manipulation

resistance of external data sources, has no established methodology in auditing, and building one is among the most concrete research and practice needs the technology creates (Lombardi et al., 2022).

Vincent et al. (2020) draw the natural conclusion: assurance over the blockchain itself, its architecture, governance, and controls, is emerging as a service in its own right, plausibly delivered through third-party reporting frameworks analogous to service organization control reports, so that individual financial statement auditors can rely on a specialist's examination of the shared infrastructure. That model would reproduce, for consortium ledgers, the division of labour the profession already operates for payroll processors and cloud providers. Someone must still perform the underlying examination, and that someone is an auditor.

7. THE AWKWARD FIT WITH AUDITING STANDARDS

Auditing standards were written for a world of discrete entities, each with its own records, exchanging paper or its electronic equivalent. Blockchain strains several of their categories, and Gauthier and Brender (2021), examining the International Standards on Auditing against blockchain environments, find the fit workable in principle but awkward in application.

Begin with audit evidence. ISA 500 directs the auditor to consider the relevance and reliability of evidence, and the standard's guidance reflects a long-standing hierarchy in which evidence obtained from independent external sources is more reliable than evidence generated internally (IAASB, 2009). Where does a blockchain record sit? It is generated partly by the client, validated by third parties, and held simultaneously by everyone. It is neither a confirmation from an independent counterparty nor an internal record, but a hybrid whose reliability depends on the consensus architecture discussed above. The sensible answer is that the reliability of on-chain evidence is a function of the chain's governance and controls, assessed case by case, which is exactly the kind of answer the current standard permits but nowhere articulates. Auditors need guidance that maps consensus architectures onto evidence reliability, and standard setters have not yet supplied it.

ISA 315, as revised in 2019, requires the auditor to obtain an understanding of the entity's information technology environment, including the risks arising from the use of information technology, and it is flexible enough to reach blockchain in general terms (IAASB, 2019). What it does not contemplate is an information system whose critical controls are operated by a consortium that is not the audited entity, may not be a service organization in the contemplated sense, and may include the entity's own counterparties. The group audit and service organization frameworks each capture part of this situation and neither captures all of it. Nor do the standards address the auditor's position when the evidence trail runs through a permissionless network that offers no governance counterparty at all: there is no one to send an inquiry to, no controls report to obtain, only a protocol whose properties must be assessed as a matter of technical analysis.

Professional bodies have moved faster than standard setters, which is the historical pattern with technology. The CPA Canada and AICPA analysis remains the most direct practitioner treatment of how audit methodology absorbs the technology (CPA Canada et al., 2017), and the ICAEW (2018) report frames blockchain as removing the reconciliation burden while sharpening the demand for judgment on valuation and substance. These documents are guidance, not requirements. The gap between them and the binding standards is where engagement risk currently lives, because an auditor relying on a blockchain today must translate general evidence principles into specific technical assessments without an authoritative bridge. Regulators who wait for the technology to mature before addressing it should note that the entities adopting consortium ledgers include banks and exchanges, which is to say entities whose audits the public actually worries about.

8. REORIENTING THE PROFESSION

What follows for auditors, the firms that employ them, and the universities that train them? The answer divides into skills, structure, and geography.

The skills question is the least speculative. An auditor who cannot read a system architecture diagram, interrogate a full transaction population with analytical tools, or supervise a specialist's review of contract code will be confined to the shrinking part of the audit. This does not mean every auditor must become a cryptographer, any more than the rise of complex financial instruments meant every auditor became a quantitative analyst. It means the profession needs a cadre of technology-literate auditors and a much larger population capable of directing, evaluating, and integrating specialist work, which is itself a skill the standards already demand but education rarely teaches. Han et al. (2023) find the accounting curriculum lagging the research literature by years; the finding will surprise no one who teaches. The plausible curricular response is not a bolt-on blockchain course but the integration of data analytics, systems thinking, and code literacy into the auditing core, taught alongside, not instead of, the judgment disciplines of valuation, estimation, and skepticism that Section 5 showed to be the durable heart of the work.

The structural question concerns the economics of firms. Audit pricing has long rested on hours, and a disproportionate share of hours has rested on verification performed by junior staff. If infrastructure absorbs that work, the pyramid narrows at the base, the traditional training ground for judgment disappears with it, and fee models tied to effort face pressure from clients who can see that the effort has fallen. Firms will respond, as they responded to analytics, by repricing around risk and expertise rather than hours, and by selling new assurance products of the kind described in Section 6. The uncomfortable distributional fact is that building blockchain assurance capability requires investment that the largest firms can amortize across global networks and smaller firms

cannot, so the technology plausibly deepens concentration in an audit market that competition regulators in several jurisdictions already consider too concentrated. That is a policy problem, not merely a professional one.

The geographic question deserves more attention than the literature has given it. Discussion of blockchain and audit is written largely from jurisdictions with mature audit markets, but the technology's early corporate uses, trade finance, remittances, agricultural supply chains, and commodity provenance, run disproportionately through emerging economies. An auditor in Accra or Lagos may within a single portfolio serve a client whose records are handwritten and a fintech client whose transactions settle on a distributed ledger. Legal infrastructure is developing on a similar dual track: Ghana's Electronic Transactions Act, 2008 (Act 772) established the evidentiary standing of electronic records well before distributed ledgers were commercially relevant, and its Cybersecurity Act, 2020 (Act 1038) now regulates the security environment on which any ledger deployment depends, yet neither instrument, nor its counterparts elsewhere on the continent, speaks to consensus governance or the ownership status of on-chain assets. Professional bodies and universities in these jurisdictions face a choice between importing assurance methodologies developed elsewhere after they harden, or participating now in shaping standards for technologies their economies are already using. The second course is harder and better.

One thing does not change, and it is worth stating plainly because the automation narrative obscures it. Professional skepticism is not a procedure and cannot be encoded. The disposition to ask whether a validated transaction had substance, whether management's assumptions are self-serving, whether the pattern in the exceptions means something, is a human capacity exercised against evidence, whatever form the evidence takes. Blockchain will change what auditors look at. It will not change the fact that someone must know what to look for.

9. CONCLUSION

This article has argued that blockchain technology automates the verification of recorded transactions while leaving intact, and in places intensifying, the audit's dependence on professional judgment. The technology guarantees that records have not been altered; it cannot guarantee that they were ever true, that the assets they describe are worth their carrying amounts, that everything relevant was recorded at all, or that cryptographic control corresponds to legal ownership. At the same time, it introduces consensus protocols, key custody, smart contract code, and oracles as new components on which financial reporting reliability depends, and each of these requires exactly the independent, expert examination that external auditors exist to provide.

The threat to the profession is therefore real but misdescribed. Blockchain will not make auditors redundant. It will make a particular kind of audit practice redundant: the practice that equated assurance with the verification of transactions and staffed, priced, and taught accordingly. Firms that respond by defending verification hours will lose them anyway, and will watch technology companies build the assurance products described in Section 6 without them. Firms, standard setters, and educators that respond by moving the profession's centre of gravity toward systems assurance and judgment will find that the demand identified by Power (1997) has not weakened at all. Markets, regulators, and the public still require credible, independent professionals to stand behind financial information. The ledger has changed. The demand for someone answerable for its meaning has not.

For researchers, the agenda is concrete: methodologies for oracle assurance, evidence-reliability frameworks mapped to consensus architectures, empirical study of early blockchain-affected engagements, and the economics of assurance in consortium settings. For standard setters, the task is to close the gap between practitioner guidance and binding standards before adoption outruns both. For educators, including this author, the task is to produce graduates who can read a smart contract on Monday and challenge an impairment model on Tuesday. None of these tasks is beyond a profession that has absorbed every prior technology said to abolish it. But absorption is a verb. It requires the profession to act.

REFERENCES

1) Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. *Accounting Horizons, 29*(2), 439–449. https://doi.org/10.2308/acch-51067
2) Appelbaum, D., & Nehmer, R. A. (2020). Auditing cloud-based blockchain accounting systems. *Journal of Information Systems, 34*(2), 5–21. https://doi.org/10.2308/isys-52660
3) Bonsón, E., & Bednárová, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research, 27*(5), 725–740. https://doi.org/10.1108/MEDAR-11-2018-0406
4) Casey, M. J., & Vigna, P. (2018). *The truth machine: The blockchain and the future of everything*. St. Martin's Press.
5) Coyne, J. G., & McMickle, P. L. (2017). Can blockchains serve an accounting purpose? *Journal of Emerging Technologies in Accounting, 14*(2), 101–111. https://doi.org/10.2308/jeta-51910
6) CPA Canada, American Institute of Certified Public Accountants, & University of Waterloo Centre for Information Integrity and Information Systems Assurance. (2017). *Blockchain technology and its potential impact on the audit and assurance profession.* Chartered Professional Accountants of Canada.
7) Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems, 31*(3), 5–21. https://doi.org/10.2308/isys-51804

8) Cybersecurity Act, 2020 (Act 1038) (Ghana).
9) Electronic Transactions Act, 2008 (Act 772) (Ghana).
10) Gauthier, M. P., & Brender, N. (2021). How do the current auditing standards fit the emergent use of blockchain? *Managerial Auditing Journal, 36*(3), 365–385. https://doi.org/10.1108/MAJ-12-2019-2513
11) Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial intelligence: A literature review. *International Journal of Accounting Information Systems, 48*, Article 100598. https://doi.org/10.1016/j.accinf.2022.100598
12) Institute of Chartered Accountants in England and Wales. (2018). *Blockchain and the future of accountancy*. ICAEW Thought Leadership.
13) International Auditing and Assurance Standards Board. (2009). *International Standard on Auditing 500: Audit evidence*. International Federation of Accountants.
14) International Auditing and Assurance Standards Board. (2019). *International Standard on Auditing 315 (Revised 2019): Identifying and assessing the risks of material misstatement*. International Federation of Accountants.
15) Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: Emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting, 14*(2), 91–100. https://doi.org/10.2308/jeta-51911
16) Liu, M., Wu, K., & Xu, J. J. (2019). How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Current Issues in Auditing, 13*(2), A19–A29. https://doi.org/10.2308/ciia-52540
17) Lombardi, R., de Villiers, C., Moscariello, N., & Pizzo, M. (2022). The disruption of blockchain in auditing: A systematic literature review and an agenda for future research. *Accounting, Auditing & Accountability Journal, 35*(7), 1534–1565. https://doi.org/10.1108/AAAJ-10-2020-4992
18) Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
19) Power, M. (1997). *The audit society: Rituals of verification*. Oxford University Press.
20) Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with smart contracts. *The International Journal of Digital Accounting Research, 18*, 1–27. https://doi.org/10.4192/1577-8517-v18_1
21) Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: A research agenda. *Australian Accounting Review, 29*(2), 331–342. https://doi.org/10.1111/auar.12286
22) Sheldon, M. D. (2019). A primer for information technology general control considerations on a private and permissioned blockchain audit. *Current Issues in Auditing, 13*(1), A15–A29. https://doi.org/10.2308/ciia-52356
23) Smith, S. S., & Castonguay, J. J. (2020). Blockchain and accounting governance: Emerging issues and considerations for accounting and assurance professionals. *Journal of Emerging Technologies in Accounting, 17*(1), 119–131. https://doi.org/10.2308/jeta-52686
24) Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday, 2*(9). https://doi.org/10.5210/fm.v2i9.548
25) Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Portfolio/Penguin.
26) Vincent, N. E., Skjellum, A., & Medury, S. (2020). Blockchain architecture: A design that helps CPA firms leverage the technology. *International Journal of Accounting Information Systems, 38*, Article 100466. https://doi.org/10.1016/j.accinf.2020.100466
27) Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance, 21*(1), 7–31. https://doi.org/10.1093/rof/rfw074