iBRICS
Journal of Multidisciplinary Study

Vol. 2, No. 1, 2026, Pg. 12-30

Blockchain in Accounting and Assurance: A Systematic Literature Review

Arya Samudra Mahardhika[1*], Rizki Ramadhani[2]
[1,2]Universitas Putra Bangsa, Kebumen, Indonesia
Email: arya@universitasputrabangsa.ac.id[1*], ramadhani362@gmail.com[2]

ABSTRACT

Blockchain has been presented as a remedy for fragmented ledgers, delayed reconciliation, and weak audit trails, yet the accounting literature often moves too quickly from technical immutability to claims about trustworthy reporting. This study reviews what the technology can change, which risks it leaves intact, and where the evidence remains thin. A systematic literature review was conducted using the Consensus scholarly index and PRISMA-informed screening. Eleven keyword combinations produced 110 records; after de-duplication, screening, and eligibility assessment, 37 peer-reviewed studies published between 2017 and 7 August 2026 were included. The corpus was coded by research design, accounting function, proposed mechanism, evidential basis, and reported limitation. Six themes emerged: shared validation and triple-entry accounting; continuous assurance; audit evidence and risk; governance and privacy; professional adoption; and sustainability reporting. The review finds credible support for faster reconciliation, stronger provenance, automated controls, and broader transaction testing. It does not support the stronger proposition that an immutable ledger makes the underlying economic event true or removes the need for professional judgment. Empirical studies instead show that blockchain may increase inherent and control risk when governance, data inputs, smart contracts, or access rights are poorly designed. The article contributes a conditional value model in which accounting gains arise only when on-chain integrity is joined to reliable data origination, permission governance, interoperability, standards, and competent human oversight. The resulting agenda shifts research away from generic benefit claims toward field evidence, control testing, and institution-specific implementation.

Keywords: accounting information systems; assurance; blockchain; systematic literature review; triple-entry accounting

INTRODUCTION

Accounting systems do more than store numbers. They establish who may record an event, which evidence is accepted, how counterparties reconcile differences, and when a record becomes authoritative. Conventional enterprise systems handle these tasks through controlled databases, contractual arrangements, and periodic verification. Blockchain changes that architecture by allowing several parties to maintain a synchronized record under an agreed validation protocol. The attraction for accounting is obvious: a shared ledger may reduce duplicated entry, shorten reconciliation, and preserve a traceable sequence of transactions (Dai & Vasarhelyi, 2017; Kokina et al., 2017). The danger is equally obvious but less often stated. A ledger can be internally consistent and still contain a false quantity, a manipulated valuation, or a transaction entered by a compromised identity. Immutability protects a record after acceptance; it does not prove that the economic event was represented correctly before acceptance (Coyne & McMickle, 2017).

This distinction separates useful accounting applications from technological rhetoric. Blockchain may improve the integrity and availability of transaction evidence, yet financial reporting still requires classification, estimation, consolidation, impairment judgments, and interpretation of standards. Likewise, an auditor may inspect a complete on-chain population and still need to test the reliability of external data, the logic of smart contracts, the governance of permissioned nodes, and management's estimates. Tan and Low (2019) therefore locate blockchain at the database-engine level of the accounting information system rather than treating it as a replacement for accounting. Schmitz and Leoni (2019) reach a similar conclusion for auditing: routine verification may contract, while governance, systems assurance, and professional judgment become more important.

The research field has expanded quickly but unevenly. Early work was largely conceptual, describing real-time reporting, triple-entry accounting, or automated assurance (Dai & Vasarhelyi, 2017; Rozario & Vasarhelyi, 2018). Later reviews mapped a broad and fragmented literature (Pimentel & Boulianne, 2020; Garanina et al., 2022; Bellucci et al., 2022). More recent empirical studies have begun to examine auditors' intentions, client risk, and organizational barriers. These studies complicate the earlier narrative. Dyball and Seethamraju (2021) report that blockchain-using clients may be perceived as riskier, while Akter et al. (2024) find that integration cost, limited knowledge, and uncertainty about benefits continue to obstruct adoption. Elmaasrawy et al. (2024) similarly show that better access to evidence can coexist with higher assessed inherent and control risk. The technology does not remove risk; it redistributes risk across code, data interfaces, identities, governance arrangements, and legal responsibility.

Several systematic reviews already exist, but three gaps remain. First, broad bibliometric maps tend to count themes without resolving contradictions between conceptual promises and practitioner evidence. Second, studies of triple-entry accounting, audit automation, cryptoassets, and sustainability reporting are often reviewed separately even though they depend on the same underlying control problem: whether a digital record can be linked to a valid economic event. Third, research published since 2023 offers enough empirical material to reconsider assumptions formed when nearly all studies were conceptual. A current synthesis is therefore needed, not to ask whether blockchain is 'good' for accounting, but to specify the conditions under which it produces reliable accounting and assurance outcomes.

This review addresses four research questions:

RQ1. Which blockchain mechanisms are proposed to alter recordkeeping, reporting, and accounting information systems?

RQ2. How does blockchain change audit evidence, audit procedures, and the assessment of audit risk?

RQ3. Which technical, organizational, professional, and institutional conditions shape adoption?

RQ4. What research designs are needed to move the field from plausible architectures to defensible evidence?

The study contributes in two ways. It integrates accounting and assurance around a conditional value model rather than a list of benefits and barriers. It also distinguishes ledger integrity from representational faithfulness. That distinction matters for practitioners: a technically valid block is an input to accounting assurance, not the final assurance conclusion. The remainder of the article reviews the conceptual foundations, explains the search and coding process, presents the thematic synthesis, and develops an agenda centered on implementations, controls, and institutional fit.

LITERATURE REVIEW

From shared ledgers to accounting records

A blockchain is an append-oriented ledger replicated across participating nodes. Transactions are grouped, cryptographically linked, and accepted according to a consensus or validation mechanism. Public and permissionless networks distribute participation widely; enterprise accounting applications more often assume permissioned networks in which participation, validation, and data visibility are governed. The distinction is not cosmetic. Accounting records contain commercially sensitive data, named counterparties, and transactions governed by contractual and regulatory duties. Wang and Kogan (2018) show that confidentiality-preserving transaction processing requires additional design features, including cryptographic techniques that limit what participants can see. Fullana and Ruiz (2021) accordingly treat privacy, governance, and integration as central features of a blockchain-enabled accounting information system rather than secondary implementation questions.

The strongest accounting argument concerns multiparty validation. When two entities record the same exchange in separate systems, differences are found through reconciliation. A shared record can reduce that duplication by allowing the parties to validate the transaction once and retain a common cryptographic receipt. McCallig et al. (2019) connect this architecture to representational faithfulness by drawing on independently held counterparty data. Yet the shared record is only as useful as the rules governing identity, authorization, measurement, and corrections. Bonsón and Bednárová (2019) warn that technical

immutability does not settle regulatory, privacy, or governance issues. The accounting significance of blockchain therefore comes from coordinated validation, not from decentralization as an end in itself.

Triple-entry accounting and event-level reporting

Triple-entry accounting (TEA) is the field's most persistent organizing idea. The phrase does not usually mean a third arithmetic side added to debit and credit. It refers to a cryptographically signed receipt or shared ledger entry that links the counterparties' records. Cai (2021) shows how this arrangement can reduce internal entries for selected accounts and create a common verification layer. Maiti et al. (2021) develop a future-oriented TEA framework, while Thies et al. (2023) find that the literature remains dominated by conceptual designs with very few evaluated implementations. TEA is therefore better understood as an interorganizational control architecture than as a replacement for double-entry bookkeeping.

A related claim is that blockchain supports event-level and near-real-time reporting. If transactions are validated continuously, financial information need not wait for month-end reconciliation before becoming available. Dai and Vasarhelyi (2017) connect this capability to continuous assurance; Yu et al. (2018) describe shorter reporting lags and new disclosure possibilities. But faster availability is not identical to faster recognition under accounting standards. Accruals, provisions, impairments, and fair values depend on estimates and reporting choices that are not resolved by transaction timestamping. Real-time records can accelerate the flow of evidence while financial statements remain periodic, interpretive products.

Audit automation, evidence, and professional judgment

The audit literature extends the shared-ledger argument into automated assurance. Smart contracts can execute specified procedures when predefined conditions are met. Rozario and Vasarhelyi (2018) propose smart-contract-supported audit procedures; Rozario and Thomas (2019) envision an external audit blockchain that coordinates evidence and reporting. Guo et al. (2025) advance the design discussion by examining how smart contracts may be applied in audit work. These proposals are credible for deterministic tests: authorization, three-way matches, limit checks, and the detection of exceptions in complete transaction populations. They are less persuasive for questions requiring intent, valuation, legal interpretation, or skepticism.

This creates a change in the object of assurance. Auditors must consider not only transactions but also consensus rules, node permissions, identity management, interfaces,

code changes, and data supplied by oracles or physical systems. Cryptoasset audits make the point clearly: proof that an address controls tokens does not by itself establish ownership, valuation, completeness, or the absence of undisclosed obligations (Hsieh & Brennan, 2022). Smith and Castonguay (2020) place these matters within accounting governance and internal control. Blockchain may enlarge the quantity of accessible evidence while simultaneously increasing the technical complexity of deciding whether that evidence is sufficient and appropriate.

Adoption, institutions, and sustainability reporting

Adoption research moves the literature from capability to use. Ferri et al. (2021) identify factors shaping Big Four auditors' intentions in Italy; Parmoodeh et al. (2023) report practitioner expectations and concerns in the United Arab Emirates; Anis (2023) documents perceived opportunities, competency requirements, and obstacles in Egypt. These studies show that adoption depends on expected usefulness, facilitating conditions, expertise, client readiness, and regulatory clarity. A technically feasible ledger can remain organizationally unattractive when it must be integrated with legacy systems, shared with reluctant counterparties, and governed across jurisdictions.

Sustainability reporting adds a different application. Blockchain can preserve provenance for supply-chain or environmental data, automate incentives, and reduce the ease with which a disclosure trail is altered. Almadadha (2024) links the technology to transparent environmental, social, and governance (ESG) reporting, while Niu et al. (2024) model blockchain-based incentives for disclosure quality. Zafra-Gómez et al. (2026) show that sustainability, TEA, traceability, and institutional governance are converging research clusters. Here too, provenance should not be confused with measurement validity. A durable record of a carbon estimate is still only as sound as the sensors, conversion factors, boundaries, and managerial assumptions that produced it.

METHOD

Review design and search strategy

The study used a systematic literature review because the evidence base contains several research designs and is not suitable for statistical meta-analysis. The review followed the reporting logic of PRISMA 2020 (Page et al., 2021) and the problem-driven review guidance described by Snyder (2019). The objective was explanatory synthesis: to compare how the literature moves from a technical property to an accounting claim, what evidence supports that move, and which boundary conditions are acknowledged.

Table 1. Review protocol

Element	Operational decision
Review question	How, and under what conditions, does blockchain alter accounting records, reporting, and assurance?
Discovery source	Consensus scholarly index; publisher and DOI metadata were used to check bibliographic identity.
Search date	7 August 2026.
Coverage	Peer-reviewed English-language journal studies published from 2017 through the search date.
Core terms	blockchain combined with accounting, audit, assurance, financial reporting, triple-entry, AIS, smart contract, audit evidence, governance, privacy, cryptoasset, or ESG.
Inclusion	Direct accounting or assurance relevance; identifiable journal record; sufficient methodological or conceptual substance for coding.
Exclusion	Non-accounting applications, editorials, duplicate versions, preprints without a journal record, and records lacking usable metadata.
Synthesis	Descriptive coding followed by mechanism-based thematic coding and comparison of claims with reported limitations.

Source: Author synthesis.

Eleven query combinations were executed. The retrieval interface returned the ten highest-ranked records for each combination, yielding 110 records before de-duplication. Repeated records were expected because central papers appeared under several combinations; 46 duplicates were removed. Title and abstract screening excluded 22 records that were outside accounting and assurance, were not peer reviewed, or lacked adequate bibliographic information. Forty-two reports received a full-record eligibility assessment. Five were removed because the accounting connection was incidental or because a more complete journal version of the same study was already retained. The final qualitative synthesis comprised 37 studies. Figure 1 records the selection decisions rather than presenting the sample as an exhaustive census of all blockchain research.

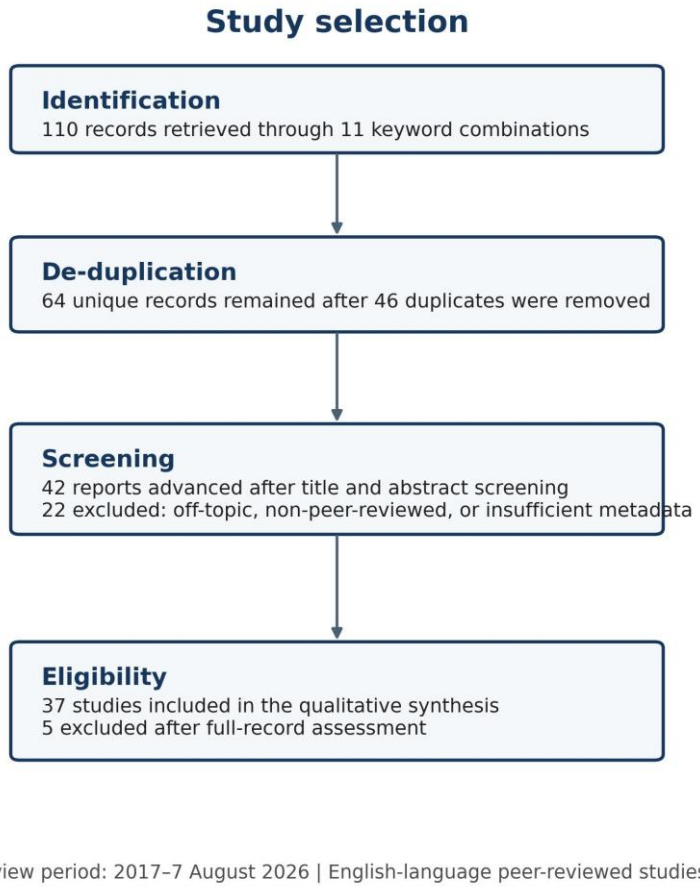

Figure 1. PRISMA-informed study selection

Source: Author synthesis based on the review search conducted on 7 August 2026.

Screening, quality appraisal, and coding

Each candidate was appraised on five questions: whether the source was a recognizable peer-reviewed journal; whether the accounting or assurance objective was explicit; whether the method or argumentative design was described well enough to evaluate; whether conclusions stayed within the evidence presented; and whether the study contributed a mechanism, observation, contradiction, or boundary condition. Conceptual work was not penalized for lacking a sample, but it had to make its assumptions visible. Empirical work had to identify its respondents, documents, cases, or analytical approach. This prevented technical novelty from being treated as evidence of accounting effectiveness.

First-cycle coding recorded year, country or setting, research design, accounting function, technology configuration, claimed benefit, risk, and type of evidence. Second-cycle coding grouped studies by mechanism rather than by vocabulary. For example, 'immutability,' 'tamper resistance,' and 'unalterable audit trail' were coded under record integrity; 'continuous audit,'

'real-time assurance,' and 'automated verification' were grouped under assurance timing and procedure. Contradictory findings were retained. When one article described stronger evidence and another reported higher audit risk, both were coded to distinguish evidence accessibility from evidence validity.

The method has two limitations. First, relevance-ranked retrieval favors visible and highly cited work; the review may omit papers that use different terminology or receive lower ranking. Second, abstract and metadata access varied across publishers, limiting article-level detail for several recent studies. These constraints make the results an analytically transparent synthesis of a defined corpus, not a claim of bibliographic completeness. The narrow search record is disclosed so that a later review can repeat the queries, broaden the databases, or test the coding against a larger sample.

RESULT AND DISCUSSION

Corpus profile: growth without methodological balance

The 37 studies show a field that is growing but still methodologically unbalanced. Publication activity rises after the foundational 2017 papers and peaks in 2024, when six studies in the corpus appeared. The decline in 2025–2026 should not be interpreted as contraction because the search year was incomplete and several recent records were available only as advance publications. Figure 2 shows the distribution used for the synthesis.

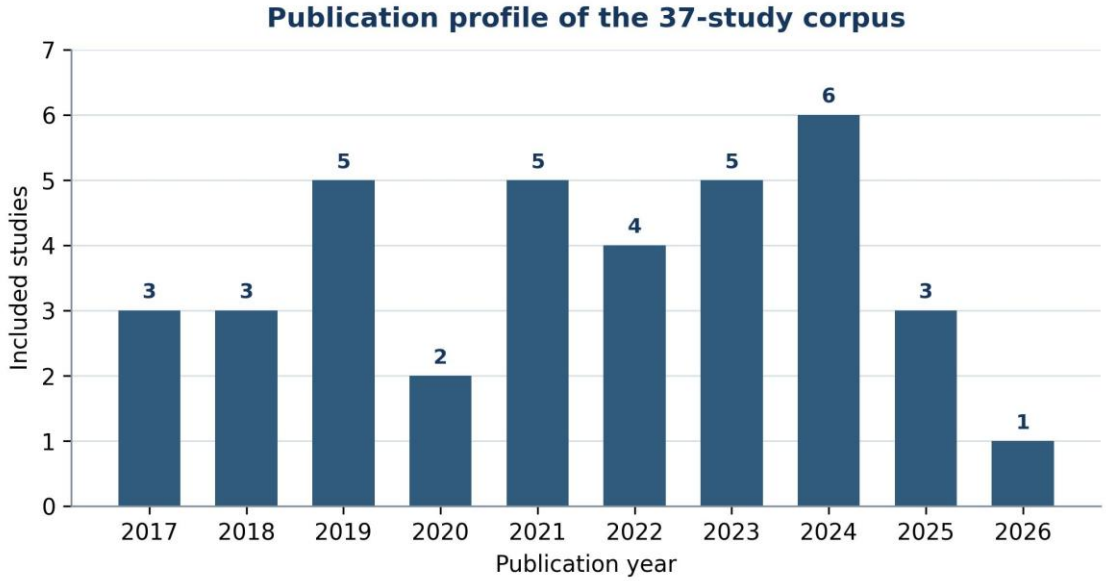

Figure 2. Included studies by publication year

Source: Author synthesis; years follow final issue metadata where available.

Table 2. Evidence profile of the included studies

Design family	n	Representative studies	Interpretive limit
Conceptual and design	15	Dai & Vasarhelyi (2017); Wang & Kogan (2018); Rozario & Thomas (2019); Maiti et al. (2021)	Clarifies architecture and mechanisms; cannot establish realized organizational effects.
Systematic, structured, or bibliometric review	12	Pimentel & Boulianne (2020); Lombardi et al. (2022); Bellucci et al. (2022); Georgiou et al. (2024)	Maps themes and gaps; often inherits the conceptual bias of the underlying literature.
Survey, interview, or mixed method	8	Ferri et al. (2021); Dyball & Seethamraju (2021); Anis (2023); Elmaasrawy et al. (2024)	Provides practitioner and adoption evidence; mostly cross-sectional and perception based.
Archival or content analysis	2	Bednárová et al. (2025); related corporate-report evidence	Shows actual disclosure and sector concentration; does not reveal internal system performance.

Source: Author synthesis.

Table 2 explains why strong language in this field must be handled carefully. Conceptual and review papers dominate. They are useful for specifying how a system might work, but their repeated appearance across later reviews can create the illusion of cumulative evidence. Empirical studies are increasing, yet most measure perceptions or intentions rather than implementation outcomes. Only a small portion of the corpus observes actual corporate disclosure or evaluates deployed architectures. The evidence base can therefore support claims of capability and perceived usefulness more confidently than claims of realized cost savings, fraud reduction, or audit-quality improvement.

Table 3. Characteristics and extracted contribution of the 37 included studies

Study	Design or setting	Primary focus	Contribution retained for synthesis
Dai & Vasarhelyi (2017)	Conceptual	Accounting and assurance	Proposes a real-time, verifiable accounting ecosystem and automated assurance.
Coyne & McMickle (2017)	Conceptual critique	Financial reporting	Shows that blockchain cannot by itself resolve the truth of off-chain assets and events.
Kokina et al. (2017)	Industry scan	Profession	Documents early accounting-firm activity and frames opportunities and limitations.
Wang & Kogan (2018)	Design and prototype	Transaction processing	Demonstrates privacy-preserving blockchain processing and continuous monitoring.
Rozario & Vasarhelyi (2018)	Conceptual design	Smart-contract audit	Explains how deterministic audit procedures could execute continuously.
Yu et al. (2018)	Conceptual	Financial accounting	Links blockchain to disclosure, governance, and shorter reporting lags.
Schmitz & Leoni (2019)	Structured review	Accounting and audit	Develops a research agenda around profession, governance, and assurance.
Tan & Low (2019)	Conceptual	AIS	Locates blockchain in the database engine while retaining accounting judgment.
Bonsón & Bednárová (2019)	Critical review	Accounting systems	Balances transformation claims against privacy, regulation, and governance issues.
McCallig et al. (2019)	Design study	Representational faithfulness	Uses multiparty security and shared data to strengthen reporting evidence.
Rozario & Thomas (2019)	Conceptual design	External audit	Proposes an external-audit blockchain with smart procedures.
Smith & Castonguay (2020)	Governance analysis	Control and assurance	Identifies data-integrity, counterparty, control, and governance responsibilities.
Pimentel & Boulianne (2020)	Literature review	Accounting practice	Organizes research across reporting, audit, cryptoassets, governance, and tax.
Cai (2021)	Multiple cases	Triple-entry accounting	Shows how a shared cryptographic receipt may reduce duplicated entries.

Ferri et al. (2021)	Survey; PLS-SEM	Auditor adoption	Finds technology-acceptance and facilitating-condition effects among Big Four staff.
Fullana & Ruiz (2021)	Critical review	AIS	Explains operational fit alongside governance, transparency, and security concerns.
Maiti et al. (2021)	Framework design	Triple-entry accounting	Develops an architecture linking blockchain and future accounting workflows.
Dyball & Seethamraju (2021)	28 interviews	Audit risk	Finds blockchain clients may carry amplified inherent and control risks.
Lombardi et al. (2022)	SLR; 40 articles	Auditing	Groups audit research into systems, smart contracts, and crypto-finance.
Garanina et al. (2022)	SLR and topic modelling	Accounting research	Shows a fragmented field and calls for stronger empirical and theoretical work.
Bellucci et al. (2022)	SLR; 346 records	Accounting practice	Maps accounting, crypto-finance, business models, and supply-chain themes.
Hsieh & Brennan (2022)	Issue analysis	Cryptoasset audit	Separates blockchain evidence from ownership, completeness, valuation, and legal risks.
Parmoodeh et al. (2023)	Practitioner interviews	Audit practice	Anticipates more automation but emphasizes skills, regulation, and implementation challenges.
Han et al. (2023)	Literature review	Blockchain and AI	Synthesizes event accounting, real-time reporting, TEA, and continuous audit.
Thies et al. (2023)	SLR	Triple-entry accounting	Finds TEA research is still overwhelmingly theoretical and rarely evaluated in practice.
Anis (2023)	Mixed method; Egypt	Accounting and audit	Documents perceived benefits, barriers, and required capabilities in an emerging economy.
Sheela et al. (2023)	Bibliometric/content review	Accounting and audit	Shows expansion of the literature but continuing concentration in conceptual themes.
Akter et al. (2024)	19 interviews; TOE	Accounting adoption	Finds knowledge gaps, legacy integration, cost, and unclear benefits constrain adoption.
Georgiou et al. (2024)	SLR; 75 studies	Accounting, audit, cryptoassets	Prioritizes skills, governance, independence, standards, and regulation.
Almadadha (2024)	Conceptual/KDD	Financial and ESG reporting	Connects blockchain provenance to transparency, security, and sustainability reporting.
Niu et al. (2024)	Principal-agent model	ESG disclosure	Models incentives for higher-quality disclosure while retaining data-quality assumptions.
Elmaasrawy et al. (2024)	Survey; 249 auditors	Accounting estimates	Finds better evidence collection alongside higher inherent and control risk.
Qader & Çek (2024)	Survey; 300 respondents	Audit quality	Reports perceived audit-quality gains from blockchain and AI use.
Guo et al. (2025)	Smart-contract application study	Audit automation	Extends continuous-audit designs toward programmable audit execution.
Bednárová et al. (2025)	1,409 reports; 337 firms	Corporate disclosure	Shows adoption remains early and concentrated in large financial and technology firms.
Ben Youssef et al. (2025)	Adoption study	Big Four audit	Tests intention to adopt and reinforces the role of organizational and normative factors.
Zafra-Gómez et al. (2026)	Bibliometric; 57 articles	AIS and sustainability	Identifies convergence among TEA, traceability, ESG, AI, and governance themes.

Source: Author synthesis.

Shared validation and triple-entry accounting

The first theme concerns reconciliation and the location of trust. In conventional interorganizational accounting, each party maintains its own authoritative record and later reconciles differences. Blockchain offers a shared validation layer that can reduce repeated matching. This is the practical core of TEA: the third element is a jointly verifiable receipt, not a third side of the accounting equation. Cai (2021), Maiti et al. (2021), and Thies et al. (2023) converge on that architecture even though they differ in detail. The potential gains are strongest where transactions are standardized, counterparties repeatedly exchange data, and the network has a clear rule for identity and validation.

The limits are just as important. TEA does not decide whether an expenditure should be capitalized, whether control over an asset has transferred, or whether a liability is complete. Those are accounting questions that require contracts, standards, and evidence beyond the cryptographic receipt. Coyne and McMickle (2017) make the strongest early critique: blockchain was designed to reach agreement about digital-state changes, not to authenticate every external fact represented by those changes. The synthesis therefore supports a narrower claim than much professional commentary. TEA can strengthen transaction agreement and provenance; it cannot make accounting judgments self-executing unless those judgments have first been reduced to rules, and many cannot be reduced without loss.

This distinction also changes how fraud risk should be described. An append-only ledger makes retroactive alteration more difficult, but manipulation may occur before entry, through collusion among authorized validators, through false identities, or through code that faithfully executes a biased rule. Fraud control shifts upstream. The relevant question becomes who controls data origination and governance, not merely who can edit the database after posting.

Continuous assurance and the redesign of audit work

The second theme is procedural automation. A blockchain exposes standardized, time-stamped transaction data that can be tested as it arrives. Smart contracts can apply deterministic procedures to the full population and flag exceptions. This improves coverage compared with periodic sampling and may shorten the distance between event, test, and response (Rozario & Vasarhelyi, 2018; Rozario & Thomas, 2019; Guo et al., 2025). Han et al. (2023) further argue that validated blockchain data can become a more dependable input for artificial-intelligence-assisted audit analytics.

Yet continuous testing should not be confused with continuous assurance over the financial statements as a whole. Many audit assertions depend on data outside the chain. Existence may require observation; rights and obligations may depend on legal interpretation; valuation often depends on models; and presentation depends on reporting frameworks. The auditor's work shifts from reperforming transaction matches toward assuring the system that produced and admitted the data. Node governance, access controls, private-key custody, smart-contract change management, interfaces, and oracle reliability become part of the audit domain. Automation removes some clerical work but creates a demand for systems specialists and clearer allocation of responsibility.

This shift may also change audit timing and reporting. If exceptions are detected continuously, annual reporting of a single pass/fail opinion looks increasingly detached from

the underlying monitoring process. The literature, however, offers little field evidence on whether users want continuous signals, how liability would be allocated, or how materiality should operate when exceptions arrive one by one. Continuous capability has advanced further than continuous-reporting institutions.

Audit evidence improves while audit risk may rise

The third theme resolves an apparent contradiction in the empirical literature. Better evidence and higher risk can occur at the same time. Dyball and Seethamraju (2021) find that practitioners view blockchain clients as potentially riskier because system novelty, governance, and technical complexity amplify inherent and control risk. Elmaasrawy et al. (2024) similarly report that auditors perceive improved collection of sufficient and appropriate evidence for accounting estimates, yet also assess higher inherent and control risk. These findings are not inconsistent. Blockchain can make a transaction trail more accessible while making the system that generates the trail harder to understand and control.

The distinction can be stated in audit terms. Evidence quantity increases when a complete population is available. Evidence reliability improves when identities, authorization, and consensus are well governed. But audit risk rises when the auditor cannot evaluate code, when data arrive through opaque interfaces, when key custody is weak, or when several organizations share responsibility without a clear control owner. Hsieh and Brennan (2022) demonstrate this problem in cryptoasset transactions, where control of a key, legal ownership, valuation, and completeness may diverge. Blockchain changes the evidence map; it does not collapse it into a single proof.

Survey evidence should also be read cautiously. Qader and Çek (2024) report positive associations between blockchain and perceived audit quality in Turkey. Such results establish professional expectations and organizational readiness, not causal improvement in detected misstatement. A stronger evidence base would compare matched engagements before and after implementation, examine audit adjustments and control deficiencies, or use regulator inspection outcomes. The present literature rarely reaches that level.

Governance, privacy, and the persistence of control

The fourth theme concerns governance. Permissioned accounting networks do not eliminate central authority; they distribute authority across rules for admission, validation, visibility, software updates, dispute resolution, and exit. Tan and Low (2019) note that accountants may cease to be the sole central authority while retaining responsibility for reporting policy and, in some cases, validation. Smith and Castonguay (2020) similarly emphasize that

organizations must redesign internal controls and counterparty-risk assessment. 'Decentralized' systems still require accountable decisions about who is allowed to do what.

Privacy is a structural tension. Auditability favors a durable, shareable trail; commercial practice favors restricted access and, in some jurisdictions, deletion or correction rights. Wang and Kogan's (2018) privacy-preserving design shows that these objectives can be reconciled only through additional architecture. Permissioning, encryption, zero-knowledge techniques, off-chain storage, and selective disclosure all reduce the simplicity of the original proposition. They also create new configuration risk. The most suitable accounting system may therefore be hybrid: a shared layer for proofs and selected events, with detailed or sensitive information retained off-chain under controlled access.

Corrections require similar care. Financial records must accommodate errors, reversals, changes in estimates, and legal orders. An immutable ledger does not prevent correction; it prevents silent deletion. The correction appears as a new entry linked to the original. This is valuable for traceability but can preserve sensitive or erroneous information indefinitely. Governance must define who can initiate a correction, how it is approved, and which view is presented to users.

Professional adoption: useful systems are not adopted by capability alone

The fifth theme is adoption. Ferri et al. (2021) show that auditor intention depends on expected usefulness, social influence, and facilitating conditions. Interviews in the United Arab Emirates and Egypt likewise identify skills, regulatory uncertainty, cost, and client preparedness as central concerns (Parmoodeh et al., 2023; Anis, 2023). Akter et al. (2024) provide the clearest empirical correction to technological enthusiasm: experts and accountants often cannot specify how blockchain would be used, how it would integrate with existing accounting systems, or whether its benefits justify the cost.

The network character of blockchain intensifies this problem. A firm receives limited value from a shared ledger when major counterparties, auditors, banks, or regulators remain outside the network. Adoption is therefore a coordination problem, not simply an information-technology purchase. Bednárová et al. (2025) find that reported use among large European-listed companies remains early and concentrated in financial and technology sectors and in countries with clearer strategies. This pattern is consistent with institutional readiness rather than universal diffusion.

The professional implication is not that accountants disappear. Tasks centered on data entry, reconciliation, and routine confirmation are exposed to automation. Tasks centered on

system design, control, valuation, governance, skepticism, and explanation become more valuable. Education should therefore combine accounting judgment with data architecture, access control, smart-contract logic, and the ability to interrogate automated evidence. Training limited to cryptocurrency terminology will not address the actual control work.

Sustainability reporting and the problem of trustworthy provenance

The sixth theme extends blockchain beyond financial transactions. ESG reporting often relies on data that cross organizational boundaries: supplier certifications, emissions measurements, origin records, and assurance statements. Blockchain can preserve provenance and make later alteration visible. Almadadha (2024) and Niu et al. (2024) show why this matters for accountability and incentives; Zafra-Gómez et al. (2026) confirm that sustainability reporting has become a distinct research cluster within blockchain accounting.

The same boundary applies. Provenance answers where a datum came from and how it moved. It does not answer whether a sensor was calibrated, whether organizational boundaries were chosen fairly, or whether a supplier had an incentive to misclassify an input. A blockchain may make greenwashing easier to trace after the fact, but it cannot prevent a misleading metric from being entered. Sustainability assurance therefore needs controls over measurement devices, estimation models, chain-of-custody rules, and data governance. In this setting, blockchain is most defensible as a provenance layer joined to independent verification.

Table 4. Mechanisms, benefits, and unresolved conditions

Theme	Mechanism	Supported benefit	Unresolved condition
Shared validation and TEA	Common cryptographic receipts reduce duplicated entry and reconciliation.	Faster agreement and stronger provenance.	Off-chain facts, accounting classification, and collusive input remain outside consensus.
Continuous assurance	Smart contracts test rules and flag exceptions as transactions arrive.	Population testing and shorter detection lag.	Judgment, materiality, legal interpretation, and reporting liability remain unresolved.
Audit evidence and risk	A complete ledger expands accessible evidence.	Traceability and standardized evidence improve.	Complexity can raise inherent and control risk even when evidence access improves.
Governance and privacy	Permissioning allocates validation, visibility, and change rights.	Clearer accountability when rules are explicit.	Hybrid designs add configuration risk; immutability may conflict with correction and privacy needs.
Professional adoption	Use depends on usefulness, skills, infrastructure, partners, and regulation.	Routine work may decline; advisory and systems assurance expand.	Network coordination, cost, legacy integration, and uncertain business value impede use.
ESG provenance	Shared traceability links measurements and supply-chain claims.	More durable non-financial evidence and chain of custody.	Sensors, estimates, boundaries, and incentives can still produce a durable falsehood.

Source: Author synthesis.

An integrative boundary model

Across the six themes, the same causal sequence appears. Technical properties enable accounting mechanisms; those mechanisms alter assurance work; and their value is moderated by boundary conditions. Figure 3 expresses that sequence. An append-only record can support a durable audit trail. Distributed validation can support shared transaction evidence. Cryptographic identity can support authorization. Programmable logic can support automated control. None of those properties, by itself, produces reliable financial reporting. Reliability arises only when data origination, permissions, change governance, interoperability, standards, and human competence align with the technical layer.

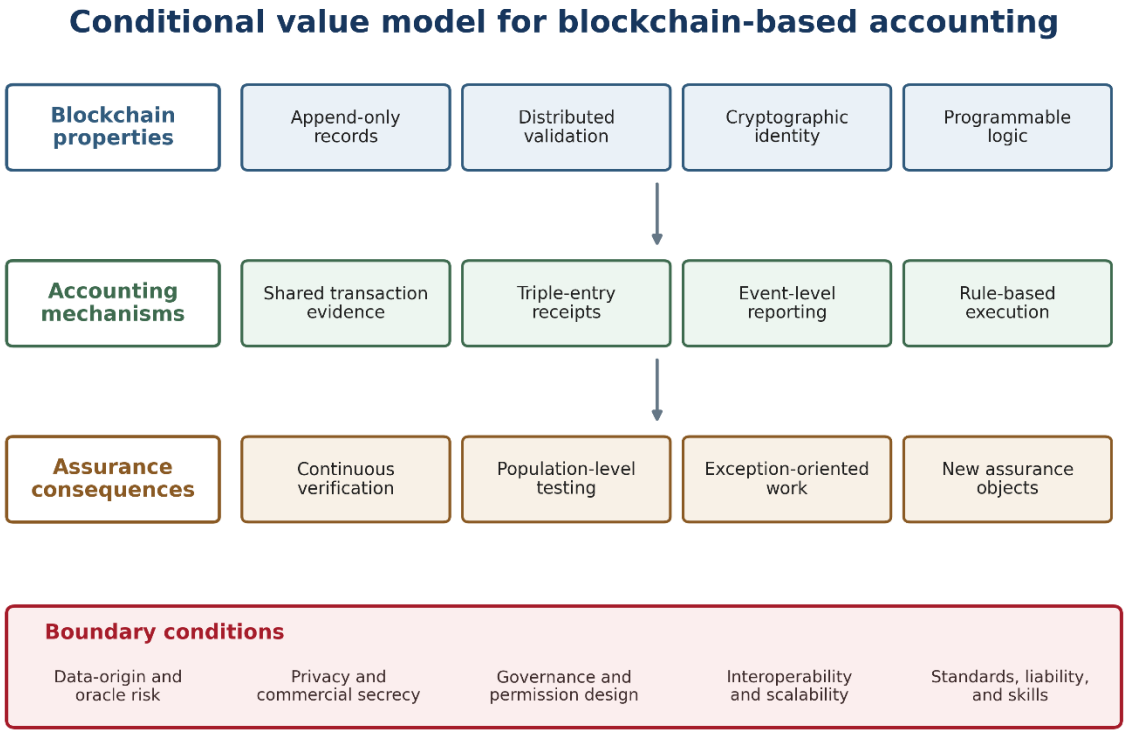

Figure 3. Conditional value model for blockchain-based accounting and assurance

Source: Author synthesis from the six review themes.

The model changes how implementation proposals should be evaluated. A proposal should not begin with the question, 'Where can we put a blockchain?' It should begin with a multiparty accounting problem: repeated reconciliation, disputed provenance, weak chain of custody, or delayed verification. The design must then identify which participants need a common record, what information belongs on-chain, who validates, how errors are corrected, how private data are protected, and which assertions remain outside the ledger. If a trusted database under one accountable owner solves the problem more simply, blockchain adds complexity without an accounting gain.

Research agenda

The review's final question concerns evidence. The field does not primarily need another generic list of benefits and barriers. It needs studies that expose blockchain designs to accounting failure modes. Table 5 sets out six priorities. Each priority links a question to a design capable of producing evidence rather than additional speculation.

Table 5. Evidence-oriented research agenda

Priority	Research question	Suggested evidence	Expected contribution
Implementation effects	Do deployed systems reduce reconciliation time, errors, closing lag, audit hours, or adjustments?	Longitudinal field studies; matched adopters and non-adopters; process logs and engagement files.	Separates realized outcomes from expected capability.
Data-origin controls	Which controls make off-chain data and oracle inputs reliable enough for financial or ESG reporting?	Control experiments; sensor and oracle failure tests; design-science evaluations with auditors.	Connects ledger integrity to representational faithfulness.
Audit-risk response	How should auditors alter risk assessment, materiality, sampling, and specialist use?	Engagement simulations, regulator inspection data, and comparative case studies.	Builds procedures suited to permissioned and hybrid ledgers.
Governance and liability	Who bears responsibility for validator failure, code defects, and disputed corrections?	Contract analysis, cross-jurisdiction comparison, and governance case studies.	Clarifies accountability in multi-organization systems.
Privacy-preserving assurance	Can selective disclosure satisfy audit evidence needs without exposing commercial data?	Prototype benchmarks, adversarial testing, and user experiments.	Tests the usability and control cost of privacy architecture.
Professional capability	Which combinations of accounting, audit, and technical expertise improve judgment?	Curriculum experiments, competency assessments, and team-composition studies.	Moves education research from attitude to task performance.

Source: Author synthesis.

Two design principles cut across the agenda. First, studies should specify the ledger type, governance model, data boundaries, and integration architecture. 'Blockchain adoption' is too broad a variable when public, consortium, permissioned, and hybrid systems distribute risk differently. Second, outcomes should be accounting outcomes. Transaction speed and hash integrity matter, but they are intermediate measures. Research should observe reporting error, control deficiency, audit effort, detected misstatement, decision usefulness, or assurance quality.

CONCLUSION

This review examined 37 peer-reviewed studies to determine what blockchain changes in accounting and assurance, what it leaves unresolved, and what evidence the field still lacks. The most defensible finding is narrower than the usual transformation narrative. Blockchain can strengthen shared transaction evidence, reduce reconciliation, preserve provenance, automate deterministic controls, and widen the population available for audit testing. These are meaningful capabilities. They can change the timing and organization of accounting work.

They do not make the underlying economic event true. Nor do they remove classification, estimation, ownership, valuation, privacy, governance, or legal questions. Empirical studies show that more accessible evidence can coexist with higher inherent and control risk. Adoption remains limited by cost, legacy integration, knowledge, counterparty participation, and standards. The central problem is therefore not whether a ledger is immutable. It is whether reliable data enter the ledger under accountable rules and whether accountants and auditors can evaluate the system around it.

The article's conditional value model captures that conclusion. Technical properties create value only through specific accounting mechanisms, and those mechanisms work only under boundary conditions: trustworthy data origination, appropriate permissions, privacy design, interoperability, institutional clarity, and competent oversight. For practice, this means starting with a multiparty accounting problem and testing whether blockchain offers a better control architecture than a conventional database. For research, it means leaving generic forecasts behind. Longitudinal implementations, control failures, audit files, governance disputes, and measurable reporting outcomes will tell the field more than another prediction that the profession is about to be disrupted.

REFERENCES

Akter, M., Kummer, T.-F., & Yigitbasioglu, O. (2024). Looking beyond the hype: The challenges of blockchain adoption in accounting. *International Journal of Accounting Information Systems, 53*, 100681. https://doi.org/10.1016/j.accinf.2024.100681

Almadadha, R. (2024). Blockchain technology in financial accounting: Enhancing transparency, security, and ESG reporting. *Blockchains, 2*(3), 312–333. https://doi.org/10.3390/blockchains2030015

Anis, A. (2023). Blockchain in accounting and auditing: Unveiling challenges and unleashing opportunities for digital transformation in Egypt. *Journal of Humanities and Applied Social Sciences, 5*(4), 359–380. https://doi.org/10.1108/JHASS-06-2023-0072

Bednárová, M., Bonsón, E., & Perea-Khalifi, D. (2025). The use of blockchain in European-listed companies: A content analysis of corporate reports. *The International Journal of Digital Accounting Research*.

Bellucci, M., Cesa Bianchi, D., & Manetti, G. (2022). Blockchain in accounting practice and research: Systematic literature review. *Meditari Accountancy Research, 30*(7), 121–146. https://doi.org/10.1108/MEDAR-10-2021-1477

Ben Youssef, W. A., Bouebdallah, N., & El Bouhali, M. (2025). Blockchain technology adoption intention among the Big Four audit firms. *The British Accounting Review*. Advance online publication.

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

Cai, C. W. (2021). Triple-entry accounting with blockchain: How far have we come? *Accounting & Finance, 61*(1), 71–93. https://doi.org/10.1111/acfi.12556

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

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

Dyball, M. C., & Seethamraju, R. (2021). The impact of client use of blockchain technology on audit risk and audit approach—An exploratory study. *International Journal of Auditing, 25*, 602–615. https://doi.org/10.1111/ijau.12238

Elmaasrawy, H. E., Tawfik, O. I., & Abdul-Rahaman, A.-R. (2024). Effect of audit client's use of blockchain technology on auditing accounting estimates: Evidence from the Middle East. *Journal of Financial Reporting and Accounting, 23*(2), 617–638. https://doi.org/10.1108/JFRA-08-2023-0499

Ferri, L., Spanò, R., Ginesti, G., & Theodosopoulos, G. (2021). Ascertaining auditors' intentions to use blockchain technology: Evidence from the Big 4 accountancy firms in Italy. *Meditari Accountancy Research, 29*(5), 1063–1087. https://doi.org/10.1108/MEDAR-03-2020-0829

Fullana, O., & Ruiz, J. (2021). Accounting information systems in the blockchain era. *International Journal of Intellectual Property Management, 11*(1), 63–80. https://doi.org/10.1504/IJIPM.2021.113357

Garanina, T., Ranta, M., & Dumay, J. (2022). Blockchain in accounting research: Current trends and emerging topics. *Accounting, Auditing & Accountability Journal, 35*(7), 1507–1533. https://doi.org/10.1108/AAAJ-10-2020-4991

Georgiou, I., Sapuric, S., Lois, P., & Thrassou, A. (2024). Blockchain for accounting and auditing—Accounting and auditing for cryptocurrencies: A systematic literature review and future research directions. *Journal of Risk and Financial Management, 17*(7), 276. https://doi.org/10.3390/jrfm17070276

Guo, X., Zuo, Y., & Li, D. (2025). When auditing meets blockchain: A study on applying blockchain smart contracts in auditing. *International Journal of Accounting Information Systems, 56*, 100730. https://doi.org/10.1016/j.accinf.2025.100730

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*, 100598. https://doi.org/10.1016/j.accinf.2022.100598

Hsieh, S.-F., & Brennan, G. (2022). Issues, risks, and challenges for auditing crypto asset transactions. *International Journal of Accounting Information Systems, 46*, 100569. https://doi.org/10.1016/j.accinf.2022.100569

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

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

Maiti, M., Kotliarov, I., & Lipatnikov, V. (2021). A future triple entry accounting framework using blockchain technology. *Blockchain: Research and Applications, 2*(4), 100037. https://doi.org/10.1016/j.bcra.2021.100037

McCallig, J., Robb, A., & Rohde, F. (2019). Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain. *International Journal of Accounting Information Systems, 33*, 47–58. https://doi.org/10.1016/j.accinf.2019.03.004

Niu, Y., Fu, Y., Liu, X., Harish, A. R., Li, M., & Huang, G. Q. (2024). Blockchain-based incentive mechanism for environmental, social, and governance disclosure: A principal-agent perspective. *Corporate Social Responsibility and Environmental Management, 31*(6), 6318–6334. https://doi.org/10.1002/csr.2916

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *PLoS Medicine, 18*(3), e1003583. https://doi.org/10.1371/journal.pmed.1003583

Parmoodeh, A. M., Ndiweni, E., & Barghathi, Y. (2023). An exploratory study of the perceptions of auditors on the impact of blockchain technology in the United Arab Emirates. *International Journal of Auditing, 27*(1), 24–44. https://doi.org/10.1111/ijau.12299

Pimentel, E., & Boulianne, E. (2020). Blockchain in accounting research and practice: Current trends and future opportunities. *Accounting Perspectives, 19*(4), 325–361. https://doi.org/10.1111/1911-3838.12239

Qader, K. S., & Çek, K. (2024). Influence of blockchain and artificial intelligence on audit quality: Evidence from Turkey. *Heliyon, 10*(9), e30166. https://doi.org/10.1016/j.heliyon.2024.e30166

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

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

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

Sheela, S., Alsmady, A. A., Tanaraj, K., & Izani, I. (2023). Navigating the future: Blockchain's impact on accounting and auditing practices. *Sustainability, 15*(24), 16887. https://doi.org/10.3390/su152416887

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

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Tan, B. S., & Low, K. Y. (2019). Blockchain as the database engine in the accounting system. *Australian Accounting Review, 29*(2), 312–318. https://doi.org/10.1111/auar.12278

Thies, S., Kureljusic, M., Karger, E., & Krämer, T. (2023). Blockchain-based triple-entry accounting: A systematic literature review and future research agenda. *Journal of Information Systems, 37*(3), 101–118. https://doi.org/10.2308/ISYS-2022-029

Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving blockchain-based transaction processing systems. *International Journal of Accounting Information Systems, 30*, 1–18. https://doi.org/10.1016/j.accinf.2018.06.001

Yu, T., Lin, Z., & Tang, Q. (2018). Blockchain: The introduction and its application in financial accounting. *Journal of Corporate Accounting & Finance, 29*(4), 37–47. https://doi.org/10.1002/jcaf.22365

Zafra-Gómez, E., López-Pérez, G., Sanz Martín, L., Navarro-Ruiz, M.-A., & Castillo, V. (2026). Blockchain and accounting information systems: Enhancing sustainability reporting with triple-entry accounting. *Revista de Contabilidad—Spanish Accounting Review*. Advance online publication.