Journal of Business
And Digital Strategy

SAH PUBLISHER

Vol. 1, No. 1, October 2026

Blockchain as a Strategy for Enhancing Transparency and Trust in Digital Business

Yulaikha Mar'atullatifah[1*], **Muhammad Anwar Fauzi**[2], **Bella Gusniar**[1]

[1]Universitas Sugeng Hartono, Indonesia

[2]PT Bank BPD DIY, Indonesia

**Corresponding author. Email: yulaikhaam@gmail.com*

Abstract. Digital business depends on transactions between parties who rarely meet, across platforms, firms and borders, so the capacity to see what has happened in a transaction and to rely on the parties behind it becomes a strategic resource. This paper examines blockchain technology as a strategy for enhancing transparency and trust in digital business, treating the two outcomes as distinct constructs rather than as synonyms. Transparency is understood here as the visibility, accessibility and integrity of records about products, transactions and obligations, while trust is understood as a willingness to be vulnerable to another party based on expectations of ability, benevolence and integrity. Drawing on a systematic review of the peer reviewed literature and on conceptual framework building, the paper analyzes four affordances of blockchain systems, namely immutability of records, provenance tracking, smart contract execution and disintermediation, and sets them against five structural limits, namely the oracle problem, the persistence of inaccurate input data, scalability and energy constraints, and unresolved questions of governance. Evidence from four application domains, covering supply chains, finance, certification and digital platforms, shows that documented value concentrates in multi party settings where records are shared, disputed or audit intensive, and that failures such as the TradeLens discontinuation trace back to governance and adoption problems rather than to cryptographic weaknesses. The paper therefore proposes a decision framework that tests whether a use case involves multiple writers, an absent or costly trusted intermediary, a need for a shared and tamper evident history, and data that can be verified at the point of entry, before blockchain is preferred over a conventional database. The Indonesian context shows why adoption strategy must separate the trading of crypto assets from enterprise blockchain deployment, which faces barriers of skills, infrastructure, legal fit and organizational readiness rather than prohibition.

Keywords: Blockchain; Transparency; Trust; Digital Business; Smart Contracts; Distributed Ledger Technology

Received October 2026 / Revised October 2026 / Accepted October 2026

This work is licensed under a Creative Commons Attribution 4.0 International License.

INTRODUCTION

Digital business reorganizes exchange around data. Orders, payments, shipments, certificates and service entitlements increasingly exist as records inside information systems, and the parties to a transaction often interact only through those records. This shift creates an enduring managerial problem. A buyer who cannot inspect a production process must decide whether to rely on the records that describe it. A platform that aggregates thousands of sellers must persuade users that ratings, settlements and product claims recorded on the platform deserve confidence. A regulator or an auditor who

receives reports from many firms must establish whether those reports were altered after the fact. In each case the difficulty is not a shortage of information but the credibility of information, because records held privately by one party can be edited, withheld or selectively disclosed by that same party. Transparency and trust therefore sit at the center of digital business strategy, and technologies that promise to manufacture both have attracted intense interest from firms, governments and researchers.

Blockchain is the most prominent of those technologies. The design published under the name Satoshi Nakamoto in 2008 proposed a peer to peer electronic cash system in which transactions are batched into blocks, linked cryptographically and validated by network consensus, so that a shared transaction history can be maintained without a central operator [1]. The architecture that generalizes this design combines a distributed ledger replicated across nodes, consensus protocols that agree on the state of the ledger, cryptographic hashing that makes later alteration evident, and, in later generations, programmable smart contracts that execute agreed rules automatically [2]. Research in business and information systems quickly recognized that the significance of the technology lies less in cryptocurrency than in this new way of organizing shared records among parties that do not fully trust one another [3]. A systematic review of blockchain based applications found reported deployments across finance, supply chain, healthcare, energy, public services and digital media, while also noting that many projects remained at pilot stage and that evidence of realized business value was still thin [4].

Despite this breadth of experimentation, the strategic conversation around blockchain often runs ahead of conceptual clarity. Promotional claims typically treat transparency and trust as a single undifferentiated benefit, as if making records visible automatically makes counterparties trustworthy, and as if a technology described as trustless removes the need for trust altogether. The scholarly literature gives reasons to resist both assumptions. Trust, in the established organizational literature, is a psychological state comprising the intention to accept vulnerability based on positive expectations of the intentions or behavior of another party, and it rests on perceptions of that party's ability, benevolence and integrity [5]. In electronic commerce, consumer trust has been modeled as a set of beliefs about an online counterpart's integrity, benevolence and competence, interacting with perceived risk to shape transaction intentions [6], and empirical work confirms that trust building mechanisms such as reputation systems, guarantees and institutional assurances materially influence online buying decisions [7]. Research on trust in technology adds that users also form trust judgments about the technology artifact itself, based on its functionality, helpfulness and reliability [8]. None of these constructs is reducible to the visibility of records. A ledger can be perfectly transparent and still record the promises of a dishonest firm, and a firm can be trustworthy while keeping commercially sensitive records private. Any serious strategy for using blockchain in digital business must therefore begin by separating the two constructs and asking which of them a given blockchain design actually changes.

A second reason for caution is that blockchain does not eliminate trust but redistributes it. A widely cited analysis of blockchain and trust in the sharing economy concludes that so called trust free systems rest on trust in the underlying protocol, in the developers who maintain it, in the interfaces through which users access it and in the institutions that stand behind tokens or records [9]. Institutional economics reaches a similar conclusion from another direction, arguing that blockchains are best understood as a new institutional technology that lowers the cost of maintaining shared ledgers and enforcing certain rules,

while still depending on surrounding legal and social institutions for the meaning and enforcement of what is recorded [10]. Reviews of business adoption likewise stress that the technology's benefits are conditional, emerging only where the structure of a business problem matches the structure of the technology, namely multi party processes with contested or duplicated records [11].

This paper develops that conditional argument into a strategy oriented account. It asks three questions. First, through which mechanisms do the affordances of blockchain, namely immutability, provenance, smart contracts and disintermediation, plausibly enhance transparency, and under what conditions does enhanced transparency support trust? Second, what structural limits, including the oracle problem, inaccurate input data, scalability, energy use and governance, constrain those mechanisms in practice? Third, how should managers decide whether a given digital business process warrants a blockchain at all, rather than a conventional database operated by a trusted party? To answer these questions the paper conducts a systematic literature review following established protocols for evidence synthesis in management and information systems research, and builds a conceptual framework that links affordances, conditions and outcomes. The framework is then examined across four application domains, namely supply chains, finance, certification and digital platforms, and is applied to the Indonesian context, where the regulatory treatment of crypto assets is frequently but mistakenly read as a judgment on enterprise blockchain as a whole. The contribution is threefold. The paper separates transparency from trust analytically and shows that blockchain acts directly on the first and only conditionally on the second. It consolidates documented benefits and documented failures into a single decision framework that managers can apply before investing. It also clarifies, for an emerging economy with a large digital market, which barriers to enterprise blockchain adoption are regulatory, which are legal in a broader sense, and which are organizational and technical.

METHODS

This study uses a systematic literature review combined with conceptual framework building. The review follows the logic of evidence based synthesis in management research, in which a research question is specified in advance, literature is identified through documented searches, sources are screened against explicit criteria, and findings are aggregated thematically rather than narratively cherry picked. The research questions stated in the introduction governed the search. Literature was sought in major scholarly databases and publisher platforms, principally Scopus and Web of Science as index sources and the digital libraries of Elsevier, Springer Nature, Wiley, Taylor and Francis, SAGE, Cambridge University Press and Oxford University Press, together with the ACM Digital Library and IEEE Xplore for foundational technical work. Search strings combined the core term blockchain or distributed ledger with transparency, trust, supply chain, smart contract, provenance, adoption and business model in title, abstract and keyword fields. The search window ran from 2008, the year of the Nakamoto white paper, to 2025, with an emphasis on the period after 2016 when peer reviewed business research on blockchain began to consolidate.

Inclusion criteria required that a source be peer reviewed or an authoritative primary document, that it address blockchain in an organizational, economic or managerial context rather than a purely cryptographic one, and that it contribute evidence or theory about transparency, trust, application value or adoption barriers. Foundational works on

the concept of trust published before the search window, notably the integrative model of Mayer, Davis and Schoorman and the electronic commerce trust models of Pavlou and of Kim, Ferrin and Rao, were included deliberately because the paper's first task is conceptual and these works define the constructs that blockchain research uses, often loosely. Exclusion criteria removed purely speculative commentary, vendor white papers without independent verification, and duplicate or superseded versions of the same study. Because this is a conceptual and strategic analysis rather than a meta analysis, the synthesis is thematic. Sources were coded against the affordances and limits named in the research questions, against application domain, and against the level at which trust was claimed to change, namely interpersonal, interorganizational, institutional or technological. Indonesian regulatory materials were drawn from official sources, including regulations of the Commodity Futures Trading Regulatory Agency (Bappebti), the Financial Services Authority (OJK) and statutes enacted by the Indonesian legislature, and were used only for the regulatory analysis, not as evidence of business outcomes.

The framework building step proceeded abductively. Affordances identified in the technical and review literature were mapped against the established components of trust, and the conditions under which each mapping holds were extracted from reported implementations, adoption studies and documented failures. Documented industry cases discussed in the paper, such as food traceability networks and the TradeLens shipping platform, are taken from the peer reviewed literature and from the companies' own public announcements as reported in reputable trade press, and are used illustratively to test the framework rather than as primary empirical data. No new empirical data were collected, and no claim in this paper rests on unpublished or unverifiable sources. The resulting framework is therefore offered as a decision aid grounded in the published record, with its limits stated as openly as its propositions.

RESULT AND DISCUSSION

3.1. Transparency and Trust as Distinct Constructs

The first finding of the review is conceptual. Transparency and trust are related but asymmetric constructs, and blockchain bears on them differently. Transparency, as the term is used in the supply chain and information systems literature, denotes the extent to which information about products, processes and transactions is visible, accessible and comprehensible to parties who did not produce it. Francisco and Swanson define the promise of blockchain for supply chains in exactly these terms, arguing that a distributed ledger makes transactions considerably more transparent than centralized systems because every authorized participant holds the same record and can inspect the history of an asset [12]. Trust, by contrast, is forward looking and relational. In the integrative model of Mayer, Davis and Schoorman, trust is a willingness to be vulnerable, arising from perceptions of a trustee's ability, benevolence and integrity, and it produces risk taking in the relationship rather than mere information receipt [5]. Pavlou's model of electronic commerce similarly treats trust as beliefs about a counterpart's integrity, benevolence and competence that, together with perceived risk, drive transaction intentions [6]. Kim, Ferrin and Rao show empirically that such trust beliefs significantly shape consumer decisions in online markets, partly by reducing perceived risk [7]. A record system can therefore increase transparency without increasing trust, if the actor revealed by the record is judged incompetent or self interested, and it can even decrease trust, if greater visibility exposes conduct that parties prefer not to see.

Blockchain's direct effect is on a specific component of this system. What a well designed ledger changes is the integrity and sharedness of records, which supports the integrity dimension of trustworthiness judgments and reduces one particular risk, namely the risk that a counterparty will rewrite history. It does not certify ability, since a firm can record its incompetence immutably, and it does not certify benevolence, since the ledger cannot reveal intentions. McKnight and colleagues' work on trust in specific technologies adds a further layer, since users must also trust the artifact itself, judging its functionality, helpfulness and reliability, so a blockchain deployment adds a new object of trust even as it modifies an old one [8]. Hawlitschek, Notheisen and Teubner systematize this point in their review of blockchain and trust in the sharing economy, showing that trust is displaced rather than abolished, moving from intermediaries toward code, platform operators, miners or validators, and oracles that feed external data into the system [9]. The strategic implication is significant. Firms should articulate blockchain investments as integrity and visibility infrastructure whose trust effects are indirect, mediated by the judgments users form about the actors and institutions around the ledger. Marketing language that promises trust itself overstates the mechanism and invites the disappointment documented in several adoption studies reviewed below.

3.2. Blockchain Affordances for Transparency and Trust

The technical literature describes blockchain as a combination of a replicated append only ledger, consensus protocols, cryptographic linking of blocks and digital signatures [2]. From these properties, four affordances recur across the review literature. The first is immutability, more precisely tamper evidence. Because each block contains a hash of its predecessor and copies of the ledger are held by many nodes, altering a past record requires rewriting subsequent blocks and convincing the network to accept the rewritten history, which consensus rules make impractical in a well distributed network [2]. Security surveys caution that this guarantee is probabilistic and conditional on network design, since attacks on consensus, on endpoints and on smart contract code are documented [13], but within its design assumptions the ledger provides a shared history that no single participant can quietly revise. For digital business this affordance targets audit and dispute costs. Records of delivery, inspection, payment or certification that are anchored on a shared ledger can be checked by all parties against the same version, reducing the reconciliation work that fragmented private databases impose.

The second affordance is provenance, the capacity to maintain a continuous, inspectable chain of custody for an asset. Kshetri's analysis of supply chain management identifies provenance and traceability among the key objectives blockchain can serve, since each transfer of an asset can be recorded as a transaction linked to earlier ones [14]. Montecchi, Plangger and Etter show how this works strategically in consumer markets, arguing that blockchain based provenance allows firms to substantiate claims about origin and production that would otherwise be cheap talk, thereby converting transparency into a signal consumers can use [15]. The third affordance is programmable execution through smart contracts. Cong and He model smart contracts as a force that expands the set of verifiable states on which contracts can be written, reducing certain contracting and enforcement costs while creating new ones [16]. In business process terms, Mendling and colleagues show that smart contracts can encode the control flow of interorganizational processes so that agreed steps execute and are recorded without a central coordinator [17]. The fourth affordance is disintermediation. By maintaining a shared record through consensus, blockchain can remove or weaken intermediaries whose business is the

custody of records, such as certain registries, clearing functions and escrow arrangements, and Beck and colleagues identify this reorganization of intermediation as the technology's core business significance [3]. Each affordance, it should be noted, is an affordance rather than an outcome. Whether immutability produces useful transparency depends on who may read the ledger, whether provenance produces trust depends on whether the recorded events were true when entered, and whether disintermediation produces value depends on whether the intermediary performed only record keeping or also absorbed risk, provided liquidity or enforced rules in ways the code does not replicate.

3.3. The Limits of Blockchain Based Transparency

The review literature is equally consistent about limits, and a strategy paper must weigh them at the same length as the affordances. The most fundamental is the oracle problem. A blockchain guarantees the integrity of data after it is written, but it cannot by itself guarantee that the data correspond to physical or institutional reality. Information about the offline world enters the ledger through sensors, human attestations or external data feeds collectively called oracles, and every one of those channels can err or be corrupted. Galvez, Mejuto and Simal Gandara make this point central to their assessment of blockchain for food traceability, noting that the reliability of the whole system depends on the reliability of data capture at each stage of the chain [18]. The colloquial form of the problem is garbage in, garbage out, except that blockchain adds a twist, because inaccurate data, once written, acquires the aura of immutable truth and becomes harder to correct than in a conventional database. Transparency of a false record is worse than opacity in one respect, since it manufactures confidence without warrant.

Three further limits are structural. Scalability remains constrained in public networks, where consensus mechanisms trade throughput and latency against decentralization, and even permissioned networks face integration and performance costs when transaction volumes grow [4], [19]. Energy consumption is a serious concern for proof of work networks, whose security model deliberately expends computation, although enterprise deployments typically use permissioned consensus with far lower energy demands, so the criticism applies unevenly across designs [11]. Governance is the least technical and most decisive limit. A shared ledger requires agreement on who may write, who may read, who validates, who pays, how errors are corrected, how the software evolves and how disputes are resolved, and these are institutional questions that cryptography cannot answer. Saberi and colleagues identify governance and organizational challenges among the principal barriers to blockchain adoption in sustainable supply chains [20], and Kouhizadeh, Saberi and Sarkis show through a structured analysis that adoption barriers are dominated by interorganizational and external factors, including the absence of standards and of regulatory clarity, rather than by the technology alone [21]. Finally, immutability itself can conflict with legal obligations, notably data protection regimes that grant rights of rectification and erasure, a tension that system designers must resolve through architectural choices such as keeping personal data off chain and anchoring only hashes on chain [22].

3.4. Application Domain: Supply Chain and Provenance

Supply chains are the most extensively documented application domain, because they combine exactly the conditions blockchain addresses, namely many parties, sequential custody of physical goods, fragmented records and high dispute and audit costs. Kshetri's early analysis mapped blockchain roles onto supply chain objectives including cost,

quality, speed, dependability, risk reduction, sustainability and flexibility, and illustrated them with cases ranging from provenance tracking of minerals to food safety [14]. Saberi and colleagues positioned blockchain within sustainable supply chain management, arguing that a shared and tamper evident record can support environmental and social claims that currently rely on costly certification intermediaries [20]. Min examined the resilience argument, contending that distributed records reduce single points of failure and information bottlenecks when supply networks are disrupted [23]. Reviews of the operations literature confirm sustained scholarly and industry attention while noting that most reported projects are pilots and that rigorous performance evaluation is scarce [24], [25]. Dutta and colleagues, reviewing blockchain in supply chain operations, catalog applications in traceability, quality assurance and logistics coordination alongside challenges of interoperability, data privacy and stakeholder alignment [24].

The documented flagship cases illustrate both the mechanism and its ceiling. In food supply chains, Tian's early design combined radio frequency identification with blockchain to record production, processing, warehousing, distribution and retail events for Chinese agri food chains, aiming to make traceability information trustworthy for consumers and regulators [26]. Retail led traceability networks built on the IBM Food Trust platform, joined by Walmart and other food companies, are documented in the literature as reducing the time needed to trace the origin of a food item from days to seconds in reported demonstrations, and as enabling more targeted recalls [15], [18]. These gains are gains in transparency in the strict sense used here, namely faster and more reliable access to an agreed history, and their trust effect runs through the integrity channel, since the record can no longer be quietly rewritten by the party whose product is under suspicion. The same literature is candid that traceability is only as good as the discipline of scanning and data entry at farms, packing houses and warehouses, which is the oracle problem in operational form [18]. The shipping industry's TradeLens platform supplies the necessary counterweight. Launched by Maersk and IBM in 2018 to digitize container shipping documentation on a permissioned blockchain, it attracted hundreds of ecosystem members yet was discontinued in November 2022, with the companies citing insufficient global industry collaboration and the failure to reach commercial viability. The technology functioned, but competitors were reluctant to build their operations on a platform associated with the largest carrier, data sharing incentives were misaligned, and governance of a supposedly neutral infrastructure by two dominant firms undermined the very trust the platform was meant to create. For strategy, TradeLens is the single most instructive case in the literature, because it demonstrates that the binding constraint on blockchain value is usually the governance of the consortium, not the quality of the ledger [21].

3.5. Application Domain: Finance, Certification and Digital Platforms

In finance, blockchain based systems target the reconciliation burden created when every institution keeps its own books. Shared ledgers promise a single golden record for settlement, syndicated lending, trade finance and post trade processing, and smart contracts promise automated execution of payment against verified delivery or documentary events [16]. Yermack's analysis of corporate governance shows a further financial application, since a transparent and current record of share ownership could transform proxy voting, shareholder activism and the identification of owners, while also creating new risks around privacy and the speed of stake building [27]. At the retail edge of finance, Parra Moyano and Ross demonstrate a concrete efficiency case, showing how

distributed ledger technology can optimize know your customer processes by allowing verified identity attestations to be shared among banks instead of duplicated by each [28], and Notheisen, Cholewa and Shanmugam prototype the trading of tokenized real world assets, illustrating how issuance and transfer of asset backed tokens can be organized on a ledger [29]. The limits identified in section 3.3 apply with full force here, since financial records carry legal finality requirements, privacy obligations and supervisory expectations that a ledger design must satisfy rather than bypass, and legal scholars warn that smart contracts interact awkwardly with doctrines of interpretation, mistake and remedy in contract law [30], [31]. Mik's detailed analysis concludes that the complexity of real world agreements, and the ambiguity of natural language obligations, place firm bounds on what can sensibly be automated [31].

Certification is a quieter but strategically important domain. Diplomas, professional licenses, product certifications and land or identity records are valuable precisely because third parties rely on them, and they are vulnerable to forgery and to slow manual verification. Anchoring certificate hashes on a blockchain allows any verifier to confirm that a presented document matches the record issued by the certifying body, without contacting that body and without the body retaining the ability to alter issued records retroactively. Ølnes, Ubacht and Janssen analyze such uses in government, identifying benefits for information sharing, auditability and fraud reduction in registries and benefit administration, while cautioning that benefits depend on process redesign and legal recognition rather than on the ledger alone [22]. The same logic extends to halal, organic and sustainability certification in supply chains, where Saberi and colleagues argue that shared records can strengthen the credibility of claims that consumers cannot verify directly [20]. Digital platforms form the fourth domain. Platform businesses intermediate between large numbers of buyers and sellers and monetize trust through reputation systems, payment guarantees and dispute resolution. Hughes and colleagues argue that blockchain could reconfigure platform value chains by letting participants carry portable reputation and transact under shared rules [32], while Morkunas, Paschen and Boon provide a managerial typology of how blockchain changes business models, from incremental record keeping improvements to fully decentralized marketplaces [33]. Angelis and Ribeiro da Silva add that adoption decisions follow perceived value drivers, including transparency and security, weighed against cost and complexity [34]. The sober reading of this literature is that incumbent platforms have weak incentives to disintermediate themselves, so blockchain in platform markets has advanced furthest where it supplies back office integrity, for settlement, content rights or credential portability, rather than where it promises to replace the platform outright.

3.6. A Strategic Framework: When Blockchain Adds Value and When a Database Suffices

Synthesizing the affordances, limits and domain evidence yields a decision framework that managers can apply before committing resources. The framework consists of five tests, and blockchain is indicated only when most of them are passed. The first test is multiplicity of writers. If a single organization writes all the records and others merely read them, a conventional database with access control and audit logging achieves the same result at lower cost, because there is no contested authorship for consensus to resolve [35], [36]. The second test concerns the trusted intermediary. Blockchain earns its complexity when no acceptable trusted third party exists, when the available intermediary is too costly, too slow or conflicted, or when participants refuse to cede control of the

record to a competitor, which was precisely the fault line in the TradeLens case. If a trusted and accountable operator is available and accepted, the operator's database is usually the rational choice. The third test is the need for a shared, tamper evident history. Blockchain adds distinctive value where records are disputed, audited, regulated or relied upon by parties outside the firm, so that proving a record was not altered is itself valuable, as in provenance, certification and settlement [14], [15]. Where records are internal and uncontested, tamper evidence buys little. The fourth test is verifiability at entry. Because of the oracle problem, blockchain should be preferred only where the events recorded can be captured reliably, through automated sensors, digitally native events such as payments, or attestation arrangements with accountable signers [18]. Processes whose critical facts are subjective or easily falsified at the point of entry will manufacture false confidence on chain. The fifth test is governance feasibility. Sponsors must be able to agree on validator membership, read and write permissions, error correction, cost sharing, data standards and exit arrangements before launch, since the literature shows interorganizational barriers dominate technical ones [21], [37]. A consortium that cannot settle these questions will reproduce the TradeLens outcome regardless of platform quality.

Two corollaries follow. First, where the tests are passed, permissioned architectures will usually fit enterprise needs better than public networks, because they offer known validators, privacy controls, higher throughput and accountable governance, at the price of weaker censorship resistance that most business processes do not require [19]. Second, the framework is deliberately conservative. It treats blockchain as one record keeping option among several, to be chosen when the structure of distrust in a process matches the structure of the technology, and it implies that many celebrated use cases, particularly single firm track and trace and internal workflow digitization, are database projects wearing blockchain branding. Passing the five tests does not guarantee success, but failing them predicts the pattern the literature repeatedly documents, namely technically competent pilots that stall at the boundary of the firm [10], [11], [38].

3.7. Adoption Barriers and the Indonesian Context

Indonesia gives the framework a demanding test, because it combines one of the world's largest digital consumer markets with regulatory arrangements that are frequently misunderstood. The central distinction is between crypto assets as traded instruments and blockchain as enterprise infrastructure. Indonesian law has treated crypto assets as tradable commodities rather than as currency. Bank Indonesia has consistently prohibited virtual currency as a payment instrument, while the Commodity Futures Trading Regulatory Agency, Bappebti, permitted and supervised crypto asset trading on the futures market, most comprehensively through Bappebti Regulation Number 8 of 2021, which set guidelines for physical trading of crypto assets including approved asset lists and exchange requirements [39]. The Financial Sector Development and Strengthening Law, Law Number 4 of 2023, then reclassified crypto assets as digital financial assets and mandated the transfer of supervision from Bappebti to the Financial Services Authority, OJK [40]. That transfer was implemented through Government Regulation Number 49 of 2024 and OJK Regulation Number 27 of 2024 on the organization of digital financial asset trading, and supervision formally moved to OJK in January 2025 [41]. The regulatory energy in this sequence is directed at consumer protection, market integrity and monetary sovereignty in asset trading. It neither prohibits nor specifically licenses the use of distributed ledgers inside firms for record keeping, traceability or settlement among known parties.

Enterprise blockchain in Indonesia therefore faces barriers that are real but different in kind from those facing crypto trading. The first is legal fit. Smart contract based processes must be reconciled with Indonesian contract law and with the electronic information and transactions framework, and records intended to serve as legal evidence must satisfy the requirements for electronic documents and signatures, questions on which the legal scholarship reviewed earlier urges caution [30], [31]. The second is data protection. Law Number 27 of 2022 on Personal Data Protection grants data subjects rights including correction and deletion, which collide with naive implementations of immutability and push designers toward off chain storage of personal data with on chain hashes [42]. The third is capability. Adoption studies in comparable emerging economies identify shortage of expertise, unclear return on investment, infrastructure gaps and resistance to interorganizational data sharing as leading barriers [43], [38], and Schuetz and Venkatesh show for India, a context structurally similar to Indonesia in income level and digital adoption patterns, that blockchain initiatives succeed where they are tied to concrete inclusion and process problems rather than to technology promotion [44]. The fourth barrier is ecosystem readiness. The framework of section 3.6 requires consortia, and Indonesian supply chains, dominated by small and medium enterprises with uneven digitization, cannot write reliable data to any ledger, conventional or distributed, until basic digital record keeping is in place, which is the oracle problem at national scale. Public sector exploration, including Bank Indonesia's publicly documented work on a digital rupiah under Project Garuda, signals institutional interest in distributed ledger concepts at the wholesale level, but retail payment applications remain a matter of monetary policy rather than enterprise strategy. For Indonesian firms, the practical implication mirrors the global evidence. Begin with processes that pass the five tests, such as export commodity traceability where foreign buyers demand verifiable provenance, interbank or intragroup reconciliation, and certification registries where forgery is a live problem, and treat regulatory compliance for any token or asset component as a separate workstream governed by the OJK regime rather than as a property of the ledger itself.

CONCLUSION

Blockchain is best understood not as a machine that produces trust but as an infrastructure that produces shared, tamper evident and inspectable records, and its strategic value in digital business follows from that narrower claim. The literature reviewed here shows that its affordances of immutability, provenance, smart contract execution and disintermediation act directly on transparency, understood as the visibility and integrity of records, and only indirectly on trust, which remains a human and institutional judgment about the ability, benevolence and integrity of counterparties, now supplemented by judgments about the technology itself. The same literature shows that these affordances are bounded by the oracle problem, by the persistence of false or careless data entry, by scalability and energy constraints that vary with design, and above all by governance, whose failure ended the most ambitious supply chain platform yet attempted. Managers should therefore subject every proposed deployment to five tests covering multiplicity of writers, the absence or cost of a trusted intermediary, the need for a tamper evident shared history, verifiability of data at entry and the feasibility of consortium governance, and should choose a conventional database whenever those tests are failed. In Indonesia, this discipline also requires separating the OJK supervised regime for crypto asset trading from enterprise ledger deployment, whose real obstacles are legal fit, data protection, skills and ecosystem digitization. Pursued under those conditions, blockchain can make

digital business more transparent in ways that support warranted trust. Pursued as a slogan, it will continue to generate pilots that the next literature review will record as abandoned.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[3] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain technology in business and information systems research," Business & Information Systems Engineering, vol. 59, no. 6, pp. 381-384, 2017, doi: 10.1007/s12599-017-0505-1.

[4] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and Informatics, vol. 36, pp. 55-81, 2019, doi: 10.1016/j.tele.2018.11.006.

[5] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," Academy of Management Review, vol. 20, no. 3, pp. 709-734, 1995, doi: 10.5465/amr.1995.9508080335.

[6] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," International Journal of Electronic Commerce, vol. 7, no. 3, pp. 101-134, 2003.

[7] D. J. Kim, D. L. Ferrin, and H. R. Rao, "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," Decision Support Systems, vol. 44, no. 2, pp. 544-564, 2008, doi: 10.1016/j.dss.2007.07.001.

[8] D. H. McKnight, M. Carter, J. B. Thatcher, and P. F. Clay, "Trust in a specific technology: An investigation of its components and measures," ACM Transactions on Management Information Systems, vol. 2, no. 2, pp. 1-25, 2011, doi: 10.1145/1985347.1985353.

[9] F. Hawlitschek, B. Notheisen, and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," Electronic Commerce Research and Applications, vol. 29, pp. 50-63, 2018, doi: 10.1016/j.elerap.2018.03.005.

[10] S. Davidson, P. De Filippi, and J. Potts, "Blockchains and the economic institutions of capitalism," Journal of Institutional Economics, vol. 14, no. 4, pp. 639-658, 2018, doi: 10.1017/S1744137417000200.

[11] J. Frizzo-Barker, P. A. Chow-White, P. R. Adams, J. Mentanko, D. Ha, and S. Green, "Blockchain as a disruptive technology for business: A systematic review," International Journal of Information Management, vol. 51, art. no. 102029, 2020, doi: 10.1016/j.ijinfomgt.2019.10.014.

[12] K. Francisco and D. Swanson, "The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency," Logistics, vol. 2, no. 1, art. no. 2, 2018, doi: 10.3390/logistics2010002.

[13] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, vol. 107, pp. 841-853, 2020, doi: 10.1016/j.future.2017.08.020.

[14] N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," International Journal of Information Management, vol. 39, pp. 80-89, 2018, doi: 10.1016/j.ijinfomgt.2017.12.005.

[15] M. Montecchi, K. Plangger, and M. Etter, "It's real, trust me! Establishing supply chain provenance using blockchain," Business Horizons, vol. 62, no. 3, pp. 283-293, 2019, doi: 10.1016/j.bushor.2019.01.008.

[16] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," The Review of Financial Studies, vol. 32, no. 5, pp. 1754-1797, 2019, doi: 10.1093/rfs/hhz007.

[17] J. Mendling, I. Weber, W. M. P. van der Aalst, J. vom Brocke, C. Cabanillas, F. Daniel, S. Debois, C. Di Ciccio, M. Dumas, S. Dustdar, A. Gal, L. García-Bañuelos, G. Governatori, R. Hull, M. La Rosa, H. Leopold, F. Leymann, J. Recker, M. Reichert, H. A. Reijers, S. Rinderle-Ma, A. S. Solti, M. Weske, and X. Xu, "Blockchains for business process management: Challenges and opportunities," ACM Transactions on Management Information Systems, vol. 9, no. 1, art. no. 4, 2018, doi: 10.1145/3183367.

[18] J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis," TrAC Trends in Analytical Chemistry, vol. 107, pp. 222-232, 2018, doi: 10.1016/j.trac.2018.08.011.

[19] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," Journal of Industrial Information Integration, vol. 13, pp. 32-39, 2019, doi: 10.1016/j.jii.2018.07.004.

[20] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," International Journal of Production Research, vol. 57, no. 7, pp. 2117-2135, 2019, doi: 10.1080/00207543.2018.1533261.

[21] M. Kouhizadeh, S. Saberi, and J. Sarkis, "Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers," International Journal of Production Economics, vol. 231, art. no. 107831, 2021, doi: 10.1016/j.ijpe.2020.107831.

[22] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," Government Information Quarterly, vol. 34, no. 3, pp. 355-364, 2017, doi: 10.1016/j.giq.2017.09.007.

[23] H. Min, "Blockchain technology for enhancing supply chain resilience," Business Horizons, vol. 62, no. 1, pp. 35-45, 2019, doi: 10.1016/j.bushor.2018.08.012.

[24] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," Transportation Research Part E: Logistics and Transportation Review, vol. 142, art. no. 102067, 2020, doi: 10.1016/j.tre.2020.102067.

[25] M. M. Queiroz, R. Telles, and S. H. Bonilla, "Blockchain and supply chain management integration: A systematic review of the literature," Supply Chain Management: An International Journal, vol. 25, no. 2, pp. 241-254, 2020, doi: 10.1108/SCM-03-2018-0143.

[26] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in Proc. 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Beijing, China, 2016, pp. 1-6, doi: 10.1109/ICSSSM.2016.7538424.

[27] D. Yermack, "Corporate governance and blockchains," Review of Finance, vol. 21, no. 1, pp. 7-31, 2017, doi: 10.1093/rof/rfw074.

[28] J. Parra-Moyano and O. Ross, "KYC optimization using distributed ledger technology," Business & Information Systems Engineering, vol. 59, no. 6, pp. 411-423, 2017, doi: 10.1007/s12599-017-0504-2.

[29] B. Notheisen, J. B. Cholewa, and A. P. Shanmugam, "Trading real-world assets on blockchain: An application of trust-free transaction systems in the market for lemons," Business & Information Systems Engineering, vol. 59, no. 6, pp. 425-440, 2017.

[30] A. Savelyev, "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law," Information & Communications Technology Law, vol. 26, no. 2, pp. 116-134, 2017, doi: 10.1080/13600834.2017.1301036.

[31] E. Mik, "Smart contracts: Terminology, technical limitations and real world complexity," Law, Innovation and Technology, vol. 9, no. 2, pp. 269-300, 2017, doi: 10.1080/17579961.2017.1378468.

[32] A. Hughes, A. Park, J. Kietzmann, and C. Archer-Brown, "Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms," Business Horizons, vol. 62, no. 3, pp. 273-281, 2019.

[33] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," Business Horizons, vol. 62, no. 3, pp. 295-306, 2019.

[34] J. Angelis and E. Ribeiro da Silva, "Blockchain adoption: A value driver perspective," Business Horizons, vol. 62, no. 3, pp. 307-314, 2019.

[35] M. Risius and K. Spohrer, "A blockchain research framework: What we (don't) know, where we go from here, and how we will know when we have succeeded," Business & Information Systems Engineering, vol. 59, no. 6, pp. 385-409, 2017, doi: 10.1007/s12599-017-0506-0.

[36] L. Hughes, Y. K. Dwivedi, S. K. Misra, N. P. Rana, V. Raghavan, and V. Akella, "Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda," International Journal of Information Management, vol. 49, pp. 114-129, 2019, doi: 10.1016/j.ijinfomgt.2019.02.005.

[37] S. Fosso Wamba and M. M. Queiroz, "Blockchain in the operations and supply chain management: Benefits, challenges and future research opportunities," International Journal of Information Management, vol. 52, art. no. 102064, 2020, doi: 10.1016/j.ijinfomgt.2019.102064.

[38] N. Kshetri, "Blockchain and sustainable supply chain management in developing countries," International Journal of Information Management, vol. 60, art. no. 102376, 2021, doi: 10.1016/j.ijinfomgt.2021.102376.

[39] Commodity Futures Trading Regulatory Agency (Bappebti), Regulation of the Head of Bappebti Number 8 of 2021 concerning Guidelines for the Implementation of Physical Market Trading of Crypto Assets on the Futures Exchange, Jakarta, Indonesia, 2021.

[40] Republic of Indonesia, Law Number 4 of 2023 concerning Financial Sector Development and Strengthening, Jakarta, Indonesia, 2023.

[41] Financial Services Authority (OJK), Regulation of the Financial Services Authority Number 27 of 2024 concerning the Implementation of Trading of Digital Financial Assets Including Crypto Assets, Jakarta, Indonesia, 2024.

[42] Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, Jakarta, Indonesia, 2022.

[43] M. M. Queiroz and S. Fosso Wamba, "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA," International Journal of Information Management, vol. 46, pp. 70-82, 2019, doi: 10.1016/j.ijinfomgt.2018.11.021.

[44] S. W. Schuetz and V. Venkatesh, "Blockchain, adoption, and financial inclusion in India: Research opportunities," International Journal of Information Management, vol. 52, art. no. 101936, 2020, doi: 10.1016/j.ijinfomgt.2019.04.009.