2026 European Conference on Computing in Construction
Corfu, Greece
July 12–15, 2026

TRUST LAYERS FOR AUTOMATED BRIDGE MANAGEMENT USING BLOCKCHAIN AND SMART CONTRACTS

Leonardo Zunino[1], Valentina Gatteschi[1], Marco Domaneschi[1], Joan Ramon Casas[2], and Valentina Villa[1]
[1]Politecnico di Torino, Turin, Italy
[2]Universitat Politècnica de Catalunya, Barcelona, Spain

Abstract

Bridge management is increasingly automated through continuous monitoring, AI-based diagnostics, and digitally coordinated interventions. Yet, current workflows rarely provide end-to-end verifiability: sensor datasets, off-chain computations, and resulting maintenance decisions are difficult to audit across multiple stakeholders. This paper proposes a trust-layered architecture that combines decentralized storage, verifiable computation, and blockchain governance to make monitoring-to-action pipelines tamper-evident and reproducible. The paper discusses how smart contracts can orchestrate inspection and maintenance playbooks, while computation integrity can be certified via Trusted Execution Environments or zero-knowledge proofs. Trade-offs in scalability, privacy, and compliance are analyzed, outlining practical deployment patterns for bridge lifecycles.

Introduction

The ongoing digital transformation of civil infrastructure is reshaping how bridges are monitored, assessed, and maintained over their service life. In recent years, Structural Health Monitoring (SHM) systems have evolved from isolated sensing deployments into data-centric platforms capable of continuously observing structural response under real traffic and environmental variability. In parallel, advances in signal processing and Artificial Intelligence (AI) have increased the ability to extract damage-sensitive features, detect anomalies, and support condition-based and predictive maintenance strategies (An et al., 2019; Malekloo et al., 2022; Zinno et al., 2022; Jiménez Rios et al., 2023). Nevertheless, despite the growing availability of monitoring data and diagnostic tools, a persistent gap remains between ”sensing” and ”action”: monitoring outcomes do not automatically translate into traceable engineering decisions or timely interventions.

This gap is not only technical; it is also organizational and procedural. Bridge management workflows involve multiple stakeholders (owners, operators, engineers, authorities, contractors, technology providers) and multiple data sources (sensors, inspections, numerical models, maintenance records). In this multi-actor setting, it becomes difficult to ensure that the data used for diagnosis have not been manipulated, the diagnostic pipeline has been executed on the declared inputs, the decision logic applied to diagnostic results is consistent and auditable, and subsequent actions and approvals remain accountable years after the event. Conventional centralized data management solutions struggle to provide long-term integrity, verifiable provenance, and non-repudiation, especially when information must be exchanged across institutional boundaries and justified retrospectively.

Blockchain technology has been proposed as an enabling layer for tamper-resistant data governance and transparent process automation. Its core properties, immutability, distributed consensus, and the ability to execute smart contracts, provide mechanisms to register evidence, log events, and enforce pre-defined rules without relying on a single trusted intermediary (Christidis and Devetsikiotis, 2016; Casino et al., 2019; Khan et al., 2021; Liu et al., 2024). In the Architecture, Engineering, and Construction domain, blockchain-based approaches have been explored for documentation, contractual automation, and lifecycle information management (Turk and Klinc, 2017; Plevris et al., 2022; Christodoulou and Kalergis, 2024; Zhang et al., 2022, 2023; Adel et al., 2023; Villa et al., 2025; Gioberti et al., 2024; Romani et al., 2025), while, in the SHM field, several studies have considered blockchain to timestamp measurements, certify alarms, or coordinate stakeholders (Xu et al., 2021; Gordan et al., 2022; Gigli et al., 2022; Mariniello et al., 2025). These contributions confirm the potential of blockchain to improve trust and transparency; however, they also reveal a critical limitation: most frameworks implicitly assume that the off-chain computations that produce alarms and indicators are correct and faithfully executed. In detail, blockchain records can certify that an alert was registered, but they do not, by themselves, prove that the alert was obtained by executing the declared algorithm on the declared dataset.

This paper addresses the above limitation by proposing a methodological framework for trust-aware automated bridge management that spans the full path from sensing to intervention. The framework integrates: off-chain monitoring and diagnostics, decentralized or content-addressed storage for scalable data management, blockchain and smart contracts for governance and audit trails, and optional mechanisms for certifying algorithm execution (e.g., Trusted Execution Environments or cryptographic proofs). The objective is not to replace engineering judgment with automation, but to embed verifiability into the digital workflow so that data, computation, decisions, and actions

can be independently checked and retrospectively reconstructed. In this sense, the contribution of the paper is primarily architectural and methodological: it defines a design space of "trust layers" that can be combined to achieve different levels of accountability, performance, and decentralization depending on stakeholder needs and operational constraints.

The remainder of the paper is organized as follows. The next section introduces the end-to-end methodological framework connecting SHM evidence to intervention governance. Then, the core section discusses alternative trust layers and digitalization levels, comparing technologies and architectural options through a structured trade-off analysis and a summary table. Finally, discussion and conclusions outline practical implications and directions for future work.

Methodological Framework: From Sensors to Intervention

The proposed framework follows a design-oriented research approach aimed at structuring a conceptual solution to a recognized gap in current bridge management practice, rather than validating a specific algorithm or implementation. Its development builds on both the existing literature on SHM, digital twins, and blockchain-based infrastructures, and the authors' ongoing research on SHM-driven bridge management.

The resulting framework can therefore be interpreted as a synthesis of established knowledge and research-driven insights, organized into a layered architecture that maps identified trust gaps to corresponding technological mechanisms. This section introduces the resulting end-to-end framework as a technology-agnostic reference process from sensing to intervention, clarifying where trust issues typically arise and how they can be progressively addressed.

The framework starts with sensing and data acquisition. A bridge is monitored through a network of structural and environmental sensors, often complemented by inspections and operational records. These sources produce heterogeneous data. Raw signals, processed time series, extracted features, and supporting documents are generated at different rates and with different formats. For this reason, data are usually managed off-chain using scalable storage. A key point is that data must remain uniquely identifiable over time. In practice, this is achieved by associating each data batch and each derived artefact with a cryptographic fingerprint, so that the same content can always be referenced and checked.

After acquisition, data move through a diagnostic pipeline. Typical steps include cleaning, synchronization, normalization, feature extraction, and anomaly detection. The pipeline produces indicators and alerts that summarize the structural condition. At this stage, automation becomes attractive, but also fragile. If the input data are not reliable, or if the computation is not transparent, then the alert can be disputed and the whole chain loses credibility. This is one of the main motivations for introducing trust layers: not only to protect the final output, but to make the pathway from data to results verifiable.

Diagnostic outputs are then interpreted within a management workflow. The goal is not to turn algorithms into decision-makers. The goal is to connect monitoring evidence to consistent actions. A practical approach is to adopt clear response policies that map alerts to intervention intents, such as enhanced monitoring, rapid assessment, or emergency safeguards. These policies can be prepared offline and updated when needed. When a new alert arrives, the workflow selects the appropriate response and starts the corresponding process. The process includes notifications, deadlines, responsibilities, and approvals. The technical assessment and the final engineering judgement remain off-chain and under human control, especially for safety-critical cases.

Finally, the response is executed and documented. Inspection reports, images, calculations, and contractor deliverables are produced. These artefacts are typically too large and too diverse to be stored on a ledger. However, the framework assumes that they are still linked to the workflow through immutable references. In this way, the system can preserve an auditable trail that connects monitoring evidence, diagnostic outputs, response activation, approvals, and completion proofs.

Overall, the framework provides a simple reference model that separates computation and storage from governance and accountability. It also makes explicit where trust must be reinforced: data provenance, algorithm execution, decision logic, and action traceability. In the next section, these weak points are addressed through a set of digital trust layers that can be combined depending on cost, performance, privacy, and governance requirements. An overview of the framework and the position of the different trust layers along the monitoring-to-intervention pipeline is shown in Figure 1.

Trust Assumptions and Threat Model

The increasing digitalization of bridge monitoring and management implicitly introduces a set of trust assumptions that are often left unspoken. In traditional SHM-based workflows, trust is typically placed in data providers, algorithm developers, system operators, and centralized data platforms. While this model may be sufficient in controlled or single-organization settings, it becomes fragile when monitoring results are used to justify high-impact decisions, involve multiple stakeholders, or must be audited retrospectively.

One of the main risks concerns data integrity. Sensor measurements, processed signals, and derived indicators are usually stored and handled off-chain, often within proprietary platforms. Without explicit integrity guarantees, data can be altered, selectively filtered, or replaced without leaving clear evidence. Even unintentional errors, such as data loss, version mismatches, or undocumented preprocessing changes, can undermine confidence in the moni-

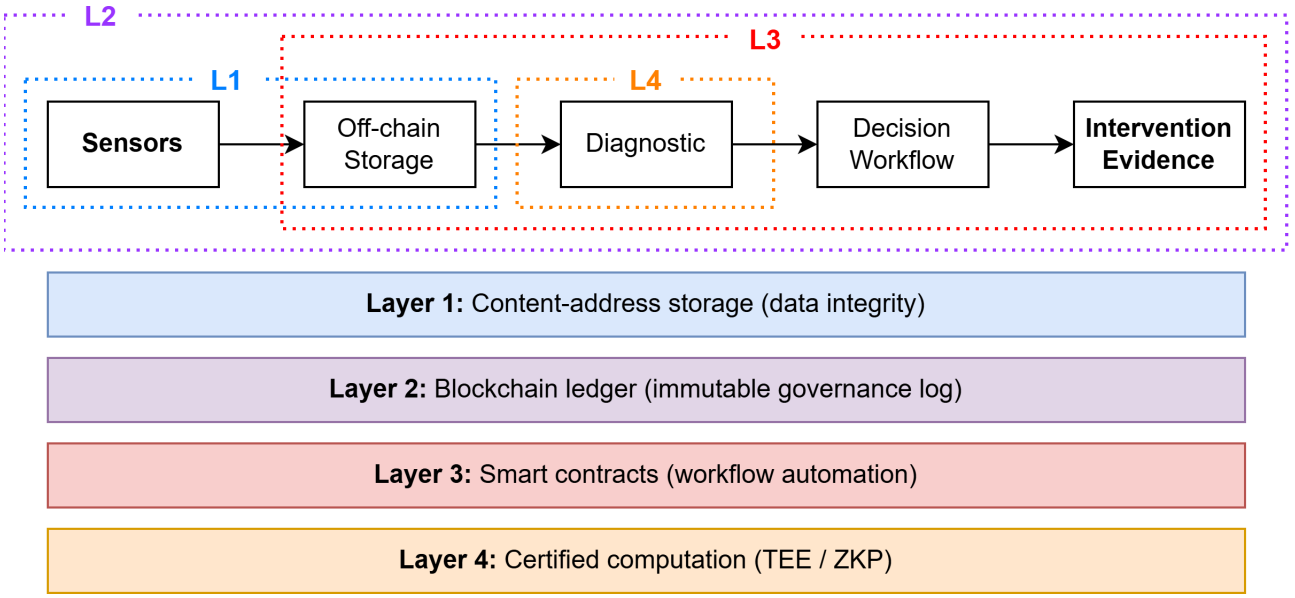

Figure 1: Monitoring-to-intervention workflow and associated trust layers.

toring results when decisions are questioned years later.

A second critical risk is related to opaque computation. Modern SHM pipelines increasingly rely on complex algorithms, including machine learning models and hybrid data-driven approaches. In many cases, the execution of these algorithms is not externally verifiable. Stakeholders must trust that the declared algorithm has been executed on the declared data, following the expected logic. When this assumption is violated, either by misconfiguration, software updates, or deliberate manipulation, the resulting alerts and indicators cannot be independently validated.

Disputes across stakeholders represent another relevant threat. Bridge management typically involves owners, operators, inspectors, engineers, contractors, and authorities, each with different responsibilities and incentives. When an alert triggers inspections, restrictions, or costly interventions, disagreements may arise regarding the correctness of the diagnosis, the timing of the alert, or the appropriateness of the response. In the absence of a shared and immutable audit trail, responsibility attribution becomes difficult and decisions may be contested.

Finally, retrospective accountability poses a long-term challenge. Bridge management decisions are often reviewed long after their execution, for example following incidents, legal disputes, or changes in ownership. At that point, personnel, software, and data platforms may have changed. Traditional monitoring systems rarely provide the guarantees needed to reconstruct the full chain from raw data to final action in a reliable and verifiable manner.

The trust layers introduced in the next section directly address these risks. Rather than assuming fully trusted actors or platforms, the proposed approach progressively reduces trust requirements by making data, computation, decision logic, and actions tamper-evident and auditable. Each layer targets specific weaknesses of traditional monitoring workflows and can be adopted independently or in combination, depending on the required assurance level.

Trust Layers and Digitalization Levels

Building on the reference workflow shown in Figure 1, this section discusses how different trust layers can be combined to strengthen specific stages of the process.

The central idea of the proposed approach is that bridge management digitalization can be equipped with a set of modular ”trust layers”, each providing additional guarantees in terms of integrity, transparency, and accountability. These layers should not be interpreted as mandatory components of a single fixed architecture, but as optional mechanisms that can be selectively adopted and progressively combined to achieve increasing levels of assurance.

In this sense, the framework is both modular and progressive: stakeholders may choose minimal configurations based on off-chain integrity and logging, or adopt more advanced layers (e.g., blockchain governance, smart contracts, or certified computation) depending on performance, privacy, interoperability, and governance requirements. This section introduces the resulting design space and discusses the associated trade-offs.

Layer 1: Content-addressed storage and integrity anchors (e.g., IPFS-like approach)

A first trust layer is achieved by separating data storage from trust in the storage provider. Content-addressed storage assigns a stable identifier to each dataset based on its content digest, enabling any party to verify that retrieved data match the declared identifier. This approach improves long-term traceability and supports distributed access while keeping heavy data off-chain. Limitations include data availability management (pinning/replication), access control design, and operational overhead when integrating with legacy data pipelines.

Layer 2: Blockchain ledger for immutable logs (public vs. consortium vs. private)

A blockchain ledger provides a tamper-resistant timeline of events, data anchors, and governance actions. From an architectural perspective, blockchain deployment can be interpreted along a single dimension with three main configurations: public, consortium, and private networks. Each configuration reflects a different trade-off between decentralization, performance, and governance.

- **Public blockchains** maximize transparency and third-party verifiability, but may raise concerns on transaction costs, throughput, and governance externalities.
- **Consortium / semi-private** networks balance decentralization and performance by restricting validators to identified organizations, improving scalability while preserving shared governance.
- **Private ledgers** provide high performance and administrative control but shift trust toward a single operator and may weaken independent verifiability.

In all cases, practical designs store only compact evidence on-chain (hashes, identifiers, proofs), while keeping datasets and detailed documents off-chain.

Layer 3: Smart contracts for automated and auditable workflows

Smart contracts implement transparent and deterministic rules that are executed on-chain and recorded immutably. In the proposed framework, they do not perform structural analysis or SHM computations, but act as a governance and orchestration layer connecting data, diagnostics, and management actions.

More specifically, different types of smart contracts can be introduced to support distinct functions along the workflow (Xu et al., 2021; Mariniello et al., 2025). These include:

- **Data validation and provenance contracts**, which register dataset identifiers and verify data integrity and quality before use;
- **Diagnostic certification contracts**, which record and validate the outputs of anomaly detection algorithms;
- **Response or workflow contracts**, which activate predefined management procedures based on alert conditions.

Within bridge management, these contracts enable the automation of governance logic, such as classification rules, response activation, deadlines and escalation paths, multi-signature approvals, and auditable milestone recording. For example, when an alert exceeds a predefined threshold, a smart contract may trigger a corresponding response playbook, notify responsible stakeholders, enforce time constraints, and require formal approvals before progressing to subsequent stages.

Importantly, the framework advocates *automation with oversight*: smart contracts formalize and enforce the decision process, but do not replace engineering judgement. All computationally intensive tasks and technical assessments remain off-chain, while smart contracts ensure that actions are consistent, traceable, and accountable across stakeholders.

Layer 4: Certified algorithm execution (TEE and ZKP as alternatives)

Even with data anchors and on-chain governance, a major trust gap remains if diagnostic computation is performed off-chain without verifiable execution. To reduce this gap, the framework introduces optional mechanisms to certify that a declared algorithm was executed on declared data:

- **Trusted Execution Environments (TEE)** provide hardware-isolated execution and remote attestation reports. They offer near-native performance and practical deployability, at the price of relying on hardware vendors and being potentially exposed to implementation and side-channel risks (Sabt et al., 2015).
- **Zero-Knowledge Proofs (ZKP)** can, in principle, provide cryptographic evidence that a computation was executed correctly with respect to its formal semantics, potentially without revealing proprietary details. They offer strong verifiability but may introduce substantial computational overhead and engineering complexity, especially for floating-point intensive pipelines and large datasets (Sun et al., 2021).

In this paper, these mechanisms are treated as part of a design space rather than a mandatory requirement: stakeholders may choose different layers based on the required assurance level and operational constraints.

Summary and trade-off table

The layered structure presented in this section directly reflects the methodological approach described above, where each trust layer corresponds to a specific class of trust gaps identified in the monitoring-to-intervention workflow. Table 1 summarizes the role of each technology and highlights typical advantages and limitations. The table is intended as a practical decision aid when assembling a trust-aware bridge management architecture.

Discussion

The proposed framework frames bridge management as a verifiable digital workflow rather than as a collection of disconnected tools. A key implication is that trust is not a binary property, but a configurable design choice. Different stakeholders and decision contexts require different assurance levels, and the framework allows these to be addressed without enforcing a single technological solution. For example, routine monitoring activities within a single organization may only require basic data integrity and logging mechanisms. In contrast, safety-critical decisions, contractual disputes, or regulatory reporting may benefit from stronger guarantees, such as immutable governance logs or certified computation. By separating the functional workflow from the trust layers, the framework supports incremental adoption and avoids unnecessary overhead where it is not justified.

The discussion also highlights a fundamental tension be-

Table 1: Trust layers and digitalization options: role, benefits, and limitations.

Layer / Technology	Primary contribution	Main limitations / trade-offs
Content-addressed storage (e.g., IPFS-like)	Integrity-by-design through content hashing; scalable off-chain storage; persistent references via content identifiers; facilitates distributed access and reproducible evidence chains.	Data availability management (pinning/replication) required; access control and confidentiality must be handled outside the storage layer; integration effort with existing pipelines.
Blockchain ledger (public)	Strong immutability and broad third-party verifiability; ideal for public audit trails and long-term non-repudiation.	Higher transaction costs and limited throughput; potential privacy concerns for metadata; governance and upgradeability depend on public ecosystem.
Blockchain ledger (consortium / semi-private)	Shared governance among identified participants; improved performance and easier alignment with regulatory/compliance constraints.	Less decentralization than public chains; requires formal consortium arrangements and operational coordination among validators.
Blockchain ledger (private)	High throughput and administrative control; straightforward integration inside a single organisation.	Trust is concentrated in the operator(s); weaker independent verifiability and reduced external auditability.
Smart contracts	Deterministic, auditable workflow logic: automate notifications, deadlines, escalation, multi-signature approvals and immutable event logs.	Correctness/bugs and upgrade governance are critical; legal and organisational alignment needed; smart contracts should orchestrate processes, not replace engineering judgement.
TEE-based execution certification	Hardware-isolated execution with remote attestation; near-native runtime performance; suitable for complex, floating-point-intensive pipelines.	Relies on hardware trust (vendor certificates); vulnerable to side-channel attacks and implementation flaws; attestation proves platform+binary, not full semantic correctness of the algorithm.
ZKP-based computation proofs	Cryptographic binding of input, computation and output; strong mathematical verifiability and optional privacy-preserving proofs.	Potentially very high proof-generation cost for large or floating-point workloads; engineering complexity and immature tooling for some classes of SHM algorithms.

tween transparency and operational constraints. While strong auditability improves accountability, it may conflict with privacy requirements, proprietary algorithms, or regulatory restrictions on data sharing. The proposed architecture mitigates this tension by relying on off-chain storage and selective on-chain anchoring, but careful system design remains essential to prevent sensitive information leakage while preserving verifiability.

Another important aspect concerns the role of automation. Although smart contracts enable deterministic and auditable workflows, they are not intended to replace engineering judgement. In the proposed framework, automation is used to enforce procedures, deadlines, and traceability, while technical assessments and final decisions remain under human control. This distinction is particularly important in bridge management, where safety considerations require conservative and accountable decision-making.

Finally, the comparison between Trusted Execution Environments and Zero-Knowledge Proofs illustrates that certified computation is technically feasible, but context-dependent. Hardware-based approaches currently offer a pragmatic balance between performance and assurance for complex SHM pipelines, while cryptographic proofs provide stronger theoretical guarantees at the cost of higher computational effort. The framework accommodates both approaches, allowing stakeholders to select the most appropriate option for their use case.

Conclusions

This paper proposed a trust-aware methodological framework for automated bridge management that spans the full path from sensing to intervention. The approach integrates scalable off-chain data handling with blockchain-based governance and introduces a layered view of digitalization, where additional "trust layers" can be progressively added to improve integrity, transparency, and accountability.

The core contribution of this paper is the definition of a structured design space and a comparative analysis of the main technologies that enable trust-aware digital workflows. These include content-addressed storage for data integrity, different blockchain deployment models, smart contracts for workflow governance, and mechanisms for certifying algorithm execution such as Trusted Execution Environments and Zero-Knowledge Proofs. By combining these components appropriately, bridge management systems can embed verifiability into digital processes while remaining adaptable to performance, privacy, and organizational constraints.

Future work will focus on several complementary directions. A first line of development concerns the extension of trust layers to additional stages of the infrastructure lifecycle, including sensor-level validation, inspection data certification, and the integration of digital twin updates within verifiable workflows.

A second research direction involves hybrid verification strategies. As zero-knowledge technologies mature and

hardware-based trusted execution evolves, combinations of TEE and cryptographic proofs may reduce trust assumptions while maintaining acceptable performance for data-intensive SHM applications. Evaluating these hybrid approaches in realistic operational settings remains an open challenge.

Further work is also needed to address interoperability and standardization. Integrating trust-aware workflows with existing monitoring platforms, asset management systems, and regulatory reporting processes requires well-defined interfaces and shared data models. Progress in this direction is essential to enable adoption beyond isolated pilots.

Finally, scaling the proposed framework from single assets to bridge networks represents an important step. Network-level deployment would enable coordinated risk assessment, prioritization of interventions, and transparent allocation of resources across multiple infrastructures, aligning the framework with the needs of infrastructure owners and public authorities.

Acknowledgments

Giorgio Marengo contributed to the conceptual development of this work in partial fulfilment of the requirements for his MSc degree in Industrial Production and Technological Innovation Engineering at Politecnico di Torino, under the supervision of the authors. His contribution is gratefully acknowledged.

This work was supported by MIUR - PRIN 2022 "BIO-RESTORE" [Prot. 202234HM8J, CUP E53C24002680006]; and it is part of the project "National Recovery and Resilience Plan-Next Generation EU" (PNRR-NGEU) which has received funding from the Italian Ministry of University and Research (MUR) – DM 629/2024.

References

Adel, K., Elhakeem, A., and Marzouk, M. (2023). Decentralized system for construction projects data management using blockchain and ipfs. Journal of Civil Engineering and Management, 29(4):342–359.

An, Y., Chatzi, E., Sim, S.-H., Laflamme, S., Blachowski, B., and Ou, J. (2019). Recent progress and future trends on damage identification methods for bridge structures. Structural Control and Health Monitoring, 26(10):e2416.

Casino, F., Dasaklis, T. K., and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and informatics, 36:55–81.

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE access, 4:2292–2303.

Christodoulou, D. and Kalergis, D. (2024). Leveraging blockchain for smart city resilience: Strengthening prevention and civil protection systems. Journal of Sustainable Development, Culture, Tradition, 3.

Gigli, L., Sciullo, L., Montori, F., Marzani, A., and Di Felice, M. (2022). Blockchain and web of things for structural health monitoring applications: A proof of concept. In 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), pages 699–702. IEEE.

Gioberti, L., Domaneschi, M., Villa, V. B., Chiaia, B. M., and Catbas, F. N. (2024). Blockchain technology conception in digital data collection for damage assessment and l.c.a. pages 1575 – 1582.

Gordan, M., Siow, P. Y., Deifalla, A. F., Ong, Z. C., Ismail, Z., and Yee, K. S. (2022). Implementation of a secure storage using blockchain for pca-frf sensor data of plate-like structures. Ieee Access, 10:84837–84852.

Jiménez Rios, A., Plevris, V., and Nogal, M. (2023). Bridge management through digital twin-based anomaly detection systems: A systematic review. Frontiers in Built Environment, 9:1176621.

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., and Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications, 14(5):2901–2925.

Liu, Y., He, J., Li, X., Chen, J., Liu, X., Peng, S., and Wang, Y. (2024). An overview of blockchain smart contract execution mechanism. Journal of Industrial Information Integration, 41:100674.

Malekloo, A., Ozer, E., AlHamaydeh, M., and Girolami, M. (2022). Machine learning and structural health monitoring overview with emerging technology and high-dimensional data source highlights. Structural Health Monitoring, 21(4):1906–1955.

Mariniello, G., Gragnaniello, C., and Asprone, D. (2025). Enhancing structural health monitoring data management and damage detection in digital twins with blockchain and smart contracts. Automation in Construction, 180:106558.

Plevris, V., Lagaros, N. D., and Zeytinci, A. (2022). Blockchain in civil engineering, architecture and construction industry: state of the art, evolution, challenges and opportunities. Frontiers in Built Environment, 8:840303.

Romani, N., de Caria, R., Restori, F., Domaneschi, M., Gatteschi, V., and Villa, V. B. (2025). A blockchain-based platform for real estate management. pages 534 – 542.

Sabt, M., Achemlal, M., and Bouabdallah, A. (2015). Trusted execution environment: What it is, and what it is not. In 2015 IEEE Trustcom/BigDataSE/Ispa, volume 1, pages 57–64. IEEE.

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., and Peng, X. (2021). A survey on zero-knowledge proof in blockchain. IEEE network, 35(4):198–205.

Turk, Ž. and Klinc, R. (2017). Potentials of blockchain technology for construction management. Procedia Engineering, 196:638–645.

Villa, V. B., Gioberti, L., Domaneschi, M., and Catbas, N. (2025). Conceptual advancements in infrastructure maintenance and management using smart contracts: Reducing costs and improving resilience. Buildings, 15(5).

Xu, J., Liu, H., and Han, Q. (2021). Blockchain technology and smart contract for civil structural health monitoring system. Computer-Aided Civil and Infrastructure Engineering, 36(10):1288–1305.

Zhang, X., Liu, T., Rahman, A., and Zhou, L. (2023). Blockchain applications for construction contract management: A systematic literature review. Journal of Construction Engineering and Management, 149(1):03122011.

Zhang, Y., Wang, T., and Yuen, K. V. (2022). Construction site information decentralized management using blockchain and smart contracts. Computer-Aided Civil and Infrastructure Engineering, 37(11):1450–1467.

Zinno, R., Haghshenas, S. S., Guido, G., and VItale, A. (2022). Artificial intelligence and structural health monitoring of bridges: A review of the state-of-the-art. IEEE Access, 10:88058–88078.