POLITECNICO DI TORINO
Repository ISTITUZIONALE

Blockchain-enabled bridge monitoring and maintenance

Original
Blockchain-enabled bridge monitoring and maintenance / Marengo, G., Zunino, L., Romani, N., Villa, V., Gatteschi, V., Domaneschi, M.. - (2026), pp. 3006-3013. (International Association for Bridge Maintenance and Safety IABMAS 2026 Orlando, Florida (US) 6–10 July 2026) [10.1201/9781003778677-363].

Availability:
This version is available at: 11583/3016071 since: 2026-09-29T13:54:49Z

Publisher:
CRC Press

Published
DOI:10.1201/9781003778677-363

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

(Article begins on next page)

14 November 2026

Moving Toward Smart, Resilient and Sustainable Bridges – Catbas, Frangopol & Yun (Eds)
© 2026 The Author(s), ISBN: 978-1-041-31173-7

Blockchain-enabled bridge monitoring and maintenance

G. Marengo, L. Zunino, N. Romani, V. Villa, V. Gatteschi and M. Domaneschi
Politecnico di Torino, Turin, Italy

ABSTRACT: The continuous digitalization of bridge monitoring systems has generated massive volumes of data, requiring secure, transparent, and verifiable mechanisms for their management and certification. This work explores the integration of blockchain technology into Structural Health Monitoring frameworks to enhance data reliability, traceability, and long-term sustainability in bridge management. A decentralized architecture is proposed that leverages public and immutable technologies to create a transparent and verifiable execution pipeline. Sensor data is stored on the InterPlanetary File System (IPFS), a peer-to-peer system that assigns each file a unique and immutable content identifier (CID). The algorithm can be executed using two different approaches: Trusted Execution Environments (TEE) and Zero-Knowledge Proofs (ZKP), analyzing their differences and use cases. The system aims to guarantee the authenticity and integrity of sensor data throughout the life cycle of the infrastructure, enabling automated maintenance actions and auditable decision-making processes through smart contracts. Beyond data certification, the approach supports the creation of a verifiable digital twin environment, where AI-driven diagnostics can be securely traced and validated. The proposed framework represents a step toward integrating advanced digital technologies within bridge management systems, providing a scalable and sustainable solution for resilient transport infrastructures.

1 INTRODUCTION

Civil infrastructures, and bridges in particular, are critical assets for the safety, economy, and development of modern societies. Service interruptions or sudden failures can propagate severe social and economic consequences over large geographical areas, as dramatically highlighted by recent bridge collapses such as the Polcevera viaduct in Genoa, Italy (Morgese et al. 2020, Domaneschi et al. 2020). These events have accelerated the demand for more reliable and proactive strategies for bridge management and maintenance.

Over the last decade, the digitalization of bridge management has been largely driven by the deployment of Structural Health Monitoring (SHM) systems. These data-driven frameworks rely on networks of sensors that continuously measure structural and environmental quantities, enabling condition-based and predictive maintenance strategies. Raw signals are pre-processed through noise reduction, synchronization, and normalization steps, and then analyzed by signal processing or machine learning algorithms to extract damage-sensitive features and indicators. Threshold-based criteria or statistical decision models are finally used to trigger alerts, inspections, or interventions (An et al. 2019; Malekloo et al. 2022).

While SHM systems significantly improve safety and reduce inspection costs, they also introduce new challenges related to data management and trust. The increasing volume of sensor data, the involvement of multiple stakeholders (owners, operators, contractors, technology providers), and the complexity of processing pipelines make it difficult to guarantee the integrity, traceability, and independent verifiability of the information used for decision-making. In many deployments, both data handling and algorithmic logic remain proprietary and opaque, preventing external auditors from reproducing the analyses or checking their correctness. This lack of

DOI: 10.1201/9781003778677-363
This chapter has been made available under a Creative Commons Attribution-Non Commercial-No Derivatives (CC BY-NC-ND) 4.0 International license.

transparency hinders the long-term certification of monitoring results and may undermine confidence in automated maintenance decisions.

Blockchain technology has emerged as a promising tool to address some of these issues. By providing an immutable and publicly verifiable ledger, blockchain can record key events, decisions, and infrastructure states through the execution of smart contracts, enabling tamper-proof audit trails and automated enforcement of maintenance policies (Christidis & Devetsikiotis 2016; Casino et al. 2019; Khan et al. 2021; Liu et al. 2024). Several recent works have proposed blockchain-based frameworks within the fields of engineering and construction (Turk & Klinc 2017; Li & Kassem 2021; Plevris et al. 2022; Gordan et al. 2022; Christodoulou & Kalergis 2024; Zhang et al. 2022; Adel et al. 2023; Zhang et al. 2023). In the specific context of infrastructure monitoring and asset management, the focus is mainly on storing hashed measurements, logging alarms, or implementing token-based incentive schemes (Gordan et al. 2021; Xu et al. 2021; Gigli et al. 2022; Mariniello et al. 2025). These approaches, however, typically assume that the off-chain pre-processing and damage detection algorithms are trusted. In practice, smart contracts only verify the final indicators or alarm levels, and no guarantees are provided about how these values have been computed from the raw sensor data.

This work addresses this critical gap by integrating verifiable computation mechanisms into the SHM pipeline. Raw and processed sensor data are stored on a decentralized file system, the InterPlanetary File System (IPFS). It assigns each file a unique and immutable content identifier (CID). The execution of the damage detection algorithm is made verifiable by means of either Trusted Execution Environments (TEE) or Zero-Knowledge Proofs (ZKP). Smart contracts deployed on a public blockchain validate the certified outputs against predefined thresholds to determine the structural condition and trigger maintenance actions. By cryptographically linking input data, algorithm execution, and output indicators, the proposed architecture turns the bridge monitoring and decision-making process into a transparent and auditable digital pipeline.

Two alternative approaches are investigated for the verifiable execution of the damage detection algorithm. In the first, the program runs inside a hardware-based TEE, which produces an attestation report proving that a specific binary has been executed on genuine confidential-computing hardware (Sabt et al. 2015). In the second, the computation is encoded in a zero-knowledge proof system, allowing a prover to convince verifiers that the algorithm has been correctly executed on a given dataset without revealing internal states or proprietary code (Sun et al. 2021). Each solution involves different trust assumptions, costs, and performance trade-offs, which are particularly relevant for real-world SHM deployments where algorithms are floating-point intensive and datasets can be large.

The main contributions of this paper are threefold. First, a decentralized and verifiable digitalization framework for bridge SHM is introduced, combining IPFS-based data storage, verifiable computation, and blockchain smart contracts to ensure end-to-end traceability and integrity of monitoring pipelines. Second, two design alternatives for certifying algorithm execution, based on TEE and ZKP, are analyzed and compared, discussing their applicability, limitations, and suitability for different stakeholders and use cases. Third, the framework is instantiated in a realistic case study, and a quantitative assessment of computational effort and on-chain costs is provided, illustrating the practical feasibility of the proposed approach.

The remainder of the paper is organized as follows. Section 2 introduces the problem setting and outlines the requirements of the proposed framework, together with the enabling technologies. Section 2.1 explores the framework design space and presents the alternative digitalization paths based on TEE and ZKP. Section 3 provides a practical, numerical, and computational analysis of the design alternatives, including cloud deployment and blockchain cost estimation. Finally, Section 4 discusses the implications of the results and concludes the paper.

2 PROBLEM SETTING AND REQUIREMENTS

SHM systems enable continuous and digital monitoring of bridge infrastructures, supporting corrective, preventive, and predictive maintenance strategies. These systems rely on networks of sensors that collect structural and environmental measurements, which are then processed through a multi-stage pipeline including noise reduction, synchronization, normalization, and damage detection algorithms. The outputs of this pipeline are finally compared against predefined thresholds to assess the structural condition and to trigger inspections or maintenance actions.

While this architecture improves safety and operational efficiency, it also introduces a critical dependency on the correctness of each processing stage. SHM pipelines involve multiple actor-sand heterogeneous technologies, and even minor errors or manipulations in the early stages of data handling or algorithm execution may propagate downstream, compromising the reliability of the final decision. In current deployments, data pre-processing and damage detection algorithms are typically executed off-chain and remain opaque to external stakeholders, preventing independent verification of both data integrity and computational correctness.

From a digitalization perspective, this lack of transparency represents a major limitation. Although blockchain-based solutions can ensure immutability and auditability of final decisions through smart contracts, they do not inherently guarantee that the off-chain computations producing the contract inputs have been executed correctly or on the declared data. As a result, trust is implicitly shifted from the blockchain to the off-chain computing infrastructure and algorithm provider.

To enable a fully digital and trust-minimized SHM pipeline, the following requirements must be satisfied. First, sensor data and intermediate results must be protected against tampering and remain uniquely identifiable over time, ensuring data integrity and long-term traceability. Second, the execution of damage detection algorithms must be verifiable by third parties, without requiring access to proprietary code or reliance on trusted operators. Third, input data, algorithm execution, and output results must be cryptographically bound, so that it is impossible to alter one component without invalidating the entire computation. Fourth, the system must support public auditability and non-repudiation, allowing stakeholders to independently verify past analyses and decisions. Finally, the solution must remain scalable and economically sustainable, avoiding excessive computational overhead or on-chain storage costs.

The framework proposed in this work is designed to address these requirements by combining decentralized data storage, verifiable computation techniques, and blockchain-based smart contracts. The following section explores the design space of the framework and discusses alternative digitalization paths for certifying algorithm execution, focusing on TEE and ZKP.

2.1 *Framework design space*

The proposed framework targets the digitalization and certification of the core computational stages of a SHM pipeline. The overall monitoring and maintenance process is composed of multiple interconnected phases, ranging from data acquisition to post-alert inspection and intervention planning. Not all of these phases are equally critical from a verification perspective, nor do they all require the same degree of digital certification.

The initial data-driven monitoring stage, which includes sensor deployment, signal acquisition, and basic validation of raw measurements, is considered outside the scope of this work. Similarly, the post-alert phase, encompassing detailed damage quantification, engineering assessment, and intervention planning, is not explicitly addressed. Although these phases could also benefit from blockchain-based certification mechanisms, the proposed framework focuses on the most critical segment of the pipeline: the execution of damage detection algorithms and the generation of certified indicators used for decision-making. A schematic overview of the proposed segment is shown in Figure 1.

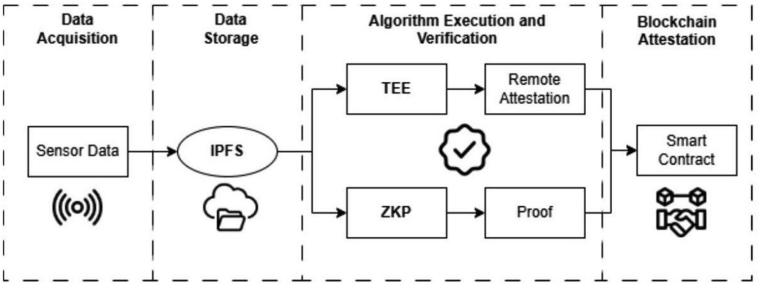

Figure 1. Overview of the proposed certification segment of the damage assessment pipeline.

Within this core segment, the framework introduces a fully decentralized and verifiable digitalization layer. Raw sensor data and intermediate processing results are stored on the IPFS, a peer-to-peer distributed storage system that ensures data integrity, availability, and contentaddressability through immutable CIDs. This approach enables all stakeholders to reference the exact datasets used in each analysis without relying on centralized repositories or trusted custodians.

The central design choice of the framework concerns the certification of algorithm execution. The objective is to provide third-party verifiable evidence that a specific damage detection algorithm has been executed correctly on a declared dataset, producing a given output, while preserving the confidentiality of proprietary code and models. To this end, two alternative execution paths are considered.

In the first path, the algorithm is executed inside a Trusted Execution Environment. The computation runs within a hardware-protected enclave, which isolates the execution from the operating system and other processes. Upon completion, the TEE produces a signed attestation report proving that a specific binary was executed on genuine confidential-computing hardware. This report can be independently verified and linked to the identifiers of the input and output data stored on IPFS.

In the second path, the correctness of the computation is certified using Zero-Knowledge Proofs. In this case, the execution of the damage detection algorithm generates a cryptographic proof attesting that the program was executed correctly on the declared inputs, according to its formal semantics, without revealing intermediate states or proprietary information. The resulting proof binds input data, computation, and output in a mathematically verifiable manner.

In both cases, the certified outputs are submitted to a blockchain-based smart contract together with cryptographic references to the processed data and execution proofs. The smart contract validates the received information, applies predefined threshold-based rules, and autonomously determines the structural status of the monitored asset. All events are permanently recorded on the blockchain, creating an immutable and publicly auditable history of analyses and decisions.

These alternative execution paths define the design space explored in this work. While both approaches satisfy the integrity, traceability, and auditability requirements introduced in Section 2, they differ significantly in terms of trust assumptions, computational overhead, scalability, and practical applicability. The next section provides a detailed analysis and quantitative comparison of the two approaches, highlighting their respective advantages and limitations in real-world SHM scenarios.

3 ANALYSIS OF DESIGN ALTERNATIVES

This section analyzes the alternative design paths introduced in Section 2.1 for certifying the execution of damage detection algorithms within the proposed framework. The objective is to assess their suitability with respect to the requirements defined in Section 2, focusing on trust assumptions, computational overhead, scalability, and practical applicability in real-world Structural Health Monitoring scenarios.

Both approaches aim to provide third-party verifiable evidence that an algorithm has been correctly executed while minimizing trust in the computing entity. However, certifying program execution alone is insufficient: it is also necessary to prove that the computation was performed on the declared input data and that the output is uniquely bound to that execution. Input, computation, and output must therefore be linked in an inseparable and verifiable chain. The following subsections analyze TEE and ZKP as alternative solutions to achieve this goal.

3.1 *Trusted Execution Environments*

Trusted Execution Environments are hardware-based technologies that allow programs to be executed within isolated and encrypted regions of a processor, commonly referred to as enclaves. This architecture ensures that the execution remains protected and inaccessible even to privileged software components such as the operating system or the hypervisor. In this work, the discussion focuses on enclave-based TEE solutions such as Intel SGX, while more

recent technologies, including Intel TDX and AMD SEV, extend similar protection guarantees to entire virtual machines.

The integrity of the execution is guaranteed through remote attestation. During this process, the processor computes a cryptographic hash of the program binary, known as a measurement, and generates a signed attestation report rooted in hardware-backed keys. This report can be independently verified against the certificates of the hardware manufacturer, providing evidence that a specific program has been executed on genuine confidential-computing hardware.

The primary advantage of TEE-based solutions lies in their efficiency. Programs execute with near-native performance, typically with an overhead ranging from 1.1x to 2x, while attestation reports are generated in the order of milliseconds and occupy only a few kilobytes. However, the trust model requires confidence in the hardware manufacturer, and vulnerabilities such as side-channel attacks have shown that these guarantees may be violated under certain conditions. Moreover, TEE-based attestation does not natively provide a mathematical binding between input data, program semantics, and output results.

3.2 *Zero-Knowledge Proofs for Verifiable Computation*

An alternative approach relies on Zero-Knowledge Proofs, cryptographic protocols that allow a prover to convince a verifier of the correctness of a statement without revealing additional information. In the context of verifiable computation, ZKP enable the generation of proofs attesting that a program has been executed correctly on a given input, according to its formal semantics.

Two main paradigms exist. zk-SNARK-based systems require the computation to be expressed as an arithmetic circuit written in domain-specific languages, where the circuit is public and only the execution trace (witness) remains private. More recent zkVM approaches allow developers to write programs in general-purpose languages such as Rust or C. In this case, the public circuit encodes the semantics of the virtual machine, while the program and its execution trace are embedded in the witness, preserving code confidentiality.

ZKP-based solutions provide strong security guarantees, as correctness is enforced by mathematical soundness rather than trust in external entities. Input data, computation, and output results are cryptographically bound, fully satisfying the verifiable computation requirements. However, these guarantees come at the cost of significant computational overhead. Proof generation can be several orders of magnitude slower than native execution, particularly for floating-point intensive algorithms and large datasets, which are common in SHM applications.

3.3 *Comparative analysis*

Table 1 summarizes the key differences between TEE- and zkVM-based approaches, highlighting the trade-offs between trust assumptions, performance, and verifiability.

Table 1. Comparison between TEE and Zero-Knowledge Virtual Machine Proof approaches.

Parameter	TEE	zkVM
Trust model	Hardware manufacturer	Mathematical/cryptographic
Execution overhead	1.1x-2x (up to 3x for enclave transitions)	100x - 1,000,000x
Proof generation time	$\sim$ ms	Seconds to hours
Proof size	$1-2$KB	KB-MB
Input-output binding	No (attestation only)	Yes (mathematical)
Code privacy	Full	Full (embedded in witness)
Known vulnerabilities	Side-channel attacks	Circuit or setup bugs
Hardware requirements	Required	Not required
Ecosystem maturity	High	Lower (rapidly evolving)

While ZKP-based solutions offer stronger theoretical guarantees by eliminating trust in external entities, their computational cost currently limits their applicability to complex SHM algorithms. Conversely, TEE-based solutions provide a pragmatic trade-off between efficiency and verifiability, at the cost of relying on hardware-backed trust assumptions.

3.4 *Application to a Realistic SHM Scenario*

To ground the comparison in a realistic application context, the proposed framework has been applied to the monitoring of the Yonghe Bridge (Zunino et al. 2025). Based on the analysis above, a TEE-based solution was selected to certify the execution of the data cleaning and damage detection algorithm. This decision is motivated by the characteristics of the application scenario: the algorithm involves floating-point intensive operations and large datasets, making zkVMbased solutions impractical due to excessive computational overhead (100x-10,000x) and proof generation times ranging from several seconds to hours.

In contrast, the TEE-based approach provides near-native execution performance and millisecondscale attestation times, satisfying the near-real-time requirements of the monitoring pipeline. To access the required confidential-computing hardware without dedicated infrastructure investments, a cloud-based virtual machine equipped with Intel SGX extensions was employed. The specifications of the VM are reported in Table 2.

Table 2. Specifications of the VM used for TEE deployment.

Parameter	Value
Cloud platform	Microsoft Azure
Region	Northern Europe
VM type	Standard DC4s_v3
Processor	Intel Xeon Platinum 8370C
Architecture	Ice Lake (3rd Gen Xeon Scalable)
Base frequency	2.8 GHz
vCPU	4 cores
RAM	32 GB
TEE technology	Intel SGX v2
EPC memory	Up to 16 GB
Operating system	Ubuntu 24.04 LTS
Hourly cost	$0.445/hour

After generating the execution proof through TEE remote attestation, the attestation report and the cryptographic references to the processed datasets are registered on-chain. The smart contract receives the certified output values together with the identifiers of the corresponding files stored on decentralized storage. The contract autonomously validates the results by counting the number of values exceeding predefined critical thresholds and classifies the structural condition into three levels: normal operation, inspection required, or urgent intervention.

Each execution generates a blockchain event with a timestamp, creating an immutable and publicly auditable record of the entire processing chain, from raw data to certified computation and final decision. To reduce transaction costs, large documents such as attestation reports are stored off-chain on decentralized storage, while only their cryptographic hashes are recorded on-chain. The gas consumption and associated costs of the on-chain operations are reported in Table 3, showing that both contract deployment and the periodic threshold evaluation incur negligible expenses on Ethereum mainnet.

Table 3. Deployment and transaction costs on Ethereum mainnet.

Operation	Gas used	Cost (ETH)	Cost (USD)
Contract deployment	805,162	0.0000354	$0.11
Threshold evaluation	307,657	0.0000135	$0.04
Total (example)	1,112,819	0.0000489	$0.15

Gas price: 0.044 Gwei - ETH price: $2,992 (measured at 23:00 CET on 2026-01-20)

Assuming a weekly monitoring execution with an average runtime of 1 hours, the annual operational cost of the system can be estimated as:

$$\text{Annualcost} = \underbrace{0.445 \times 52}_{\text{cloud VM}} + \underbrace{0.11}_{\text{Deployment}} + \underbrace{0.004 \times 52}_{\text{Transactions}} = \$25.33$$

The costs relating to the VM indicate a scenario of one hour of use per week with the creation and elimination of the VM.

These results indicate that the proposed framework is not only technically feasible but also economically sustainable. Even when deployed on a public blockchain, the operational costs remain negligible compared to traditional inspection campaigns, supporting the long-term adoption of verifiable and fully digital SHM pipelines.

4 DISCUSSION AND CONCLUSION

This paper has presented a blockchain-enabled framework for the digitalization and certification of SHM pipelines, with a specific focus on the verifiable execution of damage detection algorithms. By combining decentralized data storage, verifiable computation techniques, and blockchainbased smart contracts, the proposed approach addresses a key limitation of existing digital SHM solutions: the lack of transparency and auditability in off-chain data processing.

The analysis highlights that while blockchain technologies ensure immutability and traceability of final decisions, they do not inherently guarantee the correctness of the computations that generate those decisions. To bridge this gap, the framework introduces verifiable execution mechanisms that cryptographically link input data, algorithm execution, and output results, transforming the monitoring pipeline into a fully auditable digital process and reducing reliance on infrastructure operators or algorithm providers.

Two alternative design paths have been investigated. Zero-Knowledge Proofs offer the strongest theoretical guarantees, as correctness is enforced by mathematical soundness rather than trusted hardware. However, the computational overhead of current zkVM-based solutions makes them impractical for realistic SHM scenarios involving floating-point intensive algorithms and large datasets. Trusted Execution Environments, despite relying on hardware-backed trust assumptions, provide a pragmatic and efficient solution, enabling near-native performance and millisecondscale attestation times. The comparative analysis and application to a realistic monitoring scenario demonstrate that TEE-based approaches currently represent the most viable option for deploying verifiable SHM pipelines in practice.

An important outcome of the study is the demonstration that the proposed framework is not only technically feasible but also economically sustainable. The on-chain cost analysis shows that smart contract deployment and transaction fees on a public blockchain are negligible when compared to traditional inspection campaigns, even under continuous monitoring assumptions. This result supports the long-term adoption of blockchain-based certification mechanisms for infrastructure management without introducing prohibitive operational costs.

Despite these advantages, some limitations must be acknowledged. It is important to note that a TEE does not establish a cryptographic binding between an algorithm's output and its actual execution. Instead, it only ensures that the computation was performed within a private environment. As a result, there is no mathematical assurance that the produced output originates from the intended program. The reliance on Trusted Execution Environments introduces a dependency on hardware manufacturers and their security guarantees, which may be affected by undiscovered vulnerabilities or side-channel attacks. Moreover, the framework currently focuses on certifying the core damage detection stage, while other phases of the SHM lifecycle, such as sensor-level validation or post-alert damage quantification, are not explicitly addressed.

Future work will focus on extending the framework to additional stages of the monitoring and maintenance process, enabling a fully verifiable digital twin of the infrastructure. As zeroknowledge technologies mature and computational efficiency improves, hybrid approaches combining TEE and ZKP may further reduce trust assumptions while maintaining acceptable performance. The integration of advanced AI-based diagnostic models within a verifiable execution environment also represents a promising direction for enabling transparent and accountable decision-making in next-generation bridge management systems.

ACKNOWLEDGMENTS

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. & 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. & 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. & 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. & Devetsikiotis, M. 2016. *Blockchains and smart contracts for the internet of things*. IEEE Access 4: 2292–2303.

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

Domaneschi, M., Pellecchia, C., De Iuliis, E., Cimellaro, G.P., Morgese, M., Khalil, A.A. & Ansari, F. 2020. *Collapse analysis of the Polcevera viaduct by the applied element method. Engineering Structures* 214: 110659.

Gigli, L., Sciullo, L., Montori, F., Marzani, A. & 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): 699–702.

Gordan, M., Ismail, Z., Mohd Rahim, F. A., Chao, O. Z., Ibrahim, Z., Hashim, H. & Kiong, L. C. 2021. *Defining a conceptual framework for vibration-based damage detection platforms using blockchain*. Journal of Civil Engineering and Materials Application 5(1): 25–33.

Gordan, M., Siow, P. Y., Deifalla, A. F., Ong, Z. C., Ismail, Z. & 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.

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

Li, J. & Kassem, M. 2021. *Applications of distributed ledger technology (DLT) and blockchain-enabled smart contracts in construction*. Automation in Construction 132: 103955.

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

Malekloo, A., Ozer, E., AlHamaydeh, M. & 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. & 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.

Morgese, M., Ansari, F., Domaneschi, M. & Cimellaro, G.P. 2020. *Post-collapse analysis of Morandi's Polcevera viaduct in Genoa Italy. Journal of Civil Structural Health Monitoring* 10(1): 69–85.

Plevris, V., Lagaros, N.D. & 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.

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

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

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

Xu, J., Liu, H. & 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. & 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. & Yuen, K.V. 2022. *Construction site information decentralized management using blockchain and smart contracts*. Computer-Aided Civil and Infrastructure Engineering 37(11): 14501467.

Zunino, L., Casas, J.R. & Domaneschi, M. 2025. *Bridge damage assessment under traffic and environmental variability: A case study on Yonghe cable-stayed bridge*. Engineering Structures 343: 120965.